VITEL

Osemintrideseta delavnica o telekomunikacijah
Thirtyeight workshop on telecommunications

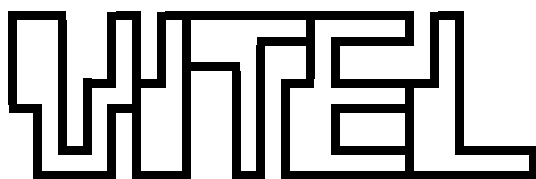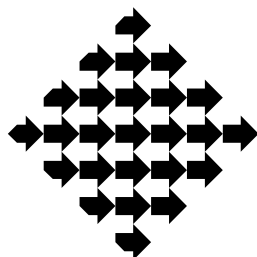# OBLAČNO ZASNOVANA OMREŽJA

CLOUD NATIVE NETWORKS

5. in 6. junija 2023
5 and 6 June 2023

Slovensko društvo za elektronske komunikacije
Elektrotehniška zveza Slovenije

SLOVENSKO DRUŠTVO ZA ELEKTRONSKE KOMUNIKACIJE
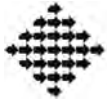ELEKTROTEHNIŠKA ZVEZA SLOVENIJE

VITEL

Osemintrideseta delavnica o telekomunikacijah
38th Workshop on telecommunications

OBLAČNO ZASNOVANA OMREŽJA
CLOUD NATIVE NETWORKS

ZBORNIK REFERATOV
PROCEEDINGS

5. in 6. junija 2023   Bled, Slovenija

38. delavnica o telekomunikacijah VITEL

ZBORNIK REFERATOV

38 Workshop on Telecommunications VITEL

PROCEEDINGS

Programski in organizacijski odbor delavnice
Programme and organizing committee

Ana Robnik

Boštjan Batagelj

Ivica Kranjčević

Katja Mohar Bastar

Nikolaj Simič

Tomi Mlinar

Vesna Prodnik

Zgodovina delavnic o telekomunikacijah VITEL
History of Workshops on Telecommunications VITEL

1993: 1. *ISDN omrežja in storitve v Sloveniji*, Brdo pri Kranju
1994: 2. *Mobilne in brezvrvične telekomunikacije*, Brdo pri Kranju
1995: 3. *Podatkovna omrežja in storitve v Sloveniji*, Brdo pri Kranju
1995: 4. *Načrtovanje, upravljanje in vzdrževanje komunikacijskih omrežij*, Brdo pri Kranju
1997: 5. *Varnost in zaščita v telekomunikacijskih omrežjih*, Brdo pri Kranju
1997: 6. *Zbliževanje fiksnih in mobilnih omrežij ter storitev*, Brdo pri Kranju
1998: 7. *Telekomunikacije in sprejetje Slovenije v Evropsko unijo*, Brdo pri Kranju
1999: 8. *Omrežja IP, internet, intranet, ekstranet*, Brdo pri Kranju
1999: 9. *Upravljanje omrežij in storitev*, Brdo pri Kranju
2000: 10. *Mobilnost v telekomunikacijah*, Brdo pri Kranju
2001: 11. *Dostop do telekomunikacijskih storitev*, Brdo pri Kranju
2002: 12. *Poslovne telekomunikacije*, Ljubljana
2002: 13. *Kakovost storitev*, Brdo pri Kranju
2003: 14. *Varnost v telekomunikacijskih sistemih*, Brdo pri Kranju
2003: 15. *Mobilni internet*, Brdo pri Kranju
2004: 16. *Pametne stavbe*, Brdo pri Kranju
2005: 17. *Telefonija IP (VoIP)*, Brdo pri Kranju
2005: 18. *Storitev trojček = Triple play*, Ljubljana
2007: 19. *Brezžični širokopasovni dostop*, Brdo pri Kranju
2007: 20. *Optična dostopovna omrežja*, Brdo pri Kranju
2008: 21. *Povsem IP–omrežja*, Brdo pri Kranju
2009: 22. *Širokopasovna mobilna omrežja*, Brdo pri Kranju
2009: 23. *Konvergenčne storitve v mobilnih in fiksnih omrežjih*, Brdo pri Kranju
2010: 24. *Prehod na IPv6*, Brdo pri Kranju
2011: 25. *Internet stvari*, Brdo pri Kranju
2011: 26. *Komunikacije in računalništvo v oblaku*, Brdo pri Kranju
2012: 27. *Telekomunikacije in zasebnost,* Brdo pri Kranju
2012: 28. *Pametna mesta,* Brdo pri Kranju
2013: 29. *Infrastruktura za izpolnitev digitalne agende in kaj po tem – primer Slovenije;* Brdo pri Kranju
2014: 30. *Omrežja prihodnosti,* Brdo pri Kranju
2015: 31. *Kritična infrastruktura in IKT,* Brdo pri Kranju
2016: 32. *Pametna omrežja informacijske družbe,* Brdo pri Kranju
2017: 33. *Omrežja 5G za digitalno preobrazbo,* Brdo pri Kranju
2018: 34. *Zaupanja vreden internet,* Brdo pri Kranju
2019: 35. *Uporabna vrednost interneta vsega,* Brdo pri Kranju
2021: 36. *Vloga tehnologije 5G v vertikalah in vloga vertikal v omrežju 5G, Zoom*
2022: 37. *Povečanje odpornosti kritične infrastrukture z uporabo naprednih rešitev IKT, Zoom*

Zgodovina mednarodnih simpozijev VITEL
History of International Telecommunication Symposium VITEL

1992:	*VITEL*, Ljubljana
1994:	*Subscriber Access*, Ljubljana
1996:	*Broadband Communications Prospects and Applications*, Ljubljana
1998:	*Mobility and Convergence Communication Technologies*, Ljubljana
2000:	*Technologies and Communication Services for the Online Society*, Ljubljana
2002:	*NGN and Beyond*, Portorož
2004:	*Next Generation User*, Maribor
2006:	*Content and Networking*, Ljubljana
2008:	*DVB–T and MPEG4*, Bled
2010:	*Digital Television Switchover Process*, Brdo pri Kranju

Uvodnik

Naslovna tema 38. delavnice o telekomunikacijah – oblačno zasnovana omrežja – se je ponudila kar sama. Desetletja smo poznali telekomunikacijska omrežja, ki so bila (in mnoga še vedno so) zgrajena načrtno, za javne ali zasebne potrebe, omogočala so govorne in/ali podatkovne komunikacije, zmogljivost opreme je bilo treba načrtovati pred postavitvijo, nadgrajevalo se jo je v desetletnih ciklih in nadgradnje niso bile poceni, varnost v takšnih sistemih (predvsem zaščita pred prisluškovanjem) je bila omejena, varstvo osebnih podatkov pa sploh ni bila tema, o kateri bi se pogovarjali. V dobrem desetletju so se stvari pomembno spremenile. Pomembnejši, ne pa vedno tudi zanesljivejši del telekomunikacijske opreme, je programska oprema, ki krmili delovanje strojne opreme oziroma omrežja. Strojna oprema se je minimizirala na zelo zmogljiv računalnik, ki ga poganjajo aplikacije. Razen minimalne strojne opreme – radijskih oddajnikov in komunikacijskih terminalov, je vse ostalo programje, ki se ga lahko spreminja in posodablja na daljavo kadarkoli in glede na trenutne potrebe. Omenjeni deli strojne opreme morajo biti na točno določenih lokacijah, vse ostalo lahko pa je lahko kjerkoli, le da je priklopljeno na zmogljiv internet, ki mora biti vedno na voljo. In tako pridemo do oblaka, oblačnih storitev in oblačnih omrežij, ki so v 21 prispevkih z vseh zornih kotov opisani v tem zborniku.

V uvodnem prispevku Marka Štefančiča so povzeti trendi, ki so aktualni za ponudnike komunikacijskih storitev. Sledi prispevek Urbana Sedlarja, ki pojasnjuje sodobne oblačne infrastrukture in poleg ostalega omenja, da moramo skrbeti tako za fizični kot virtualni nivo oblačnega omrežja. Prvega lahko zaupamo nekomu drugemu (storitev je lahko infrastruktura, platforma ali programska oprema), pri drugem pa nam pomaga ustrezna orkestracija. Kako je z zasebnostjo v oblaku, kako definiramo upravljavca podatkov in kako podatke zavarujemo, pa je tema prispevka Jelene Burnik. Oblačna infrastruktura je skupek kompleksnih (večinoma) virtualnih enot, ki se povezujejo in upravljajo na različne, povečini standardizirane načine. Te opisujejo prispevki Roberta Korošca, Aljaža Omana in Aleša Grosa. Tretji sklop prispevkov pokrivajo predstavniki treh največjih globalnih ponudnikov informacijsko-komunikacijske infrastrukture in oblačnih rešitev, ki stavijo na oblačno infrastrukturo tako pri hrambi podatkov, računski moči, kot pri sestavi omrežij na jedrnem in dostopovnem delu.

Uvodno predavanje drugega dela zbornika se osredotoča na uporabnika in ugotavlja, da etika ne dohaja razvoja tehnologije, kjer se zlahka dogajajo zlorabe zbranih podatkov in pojasnjuje odgovornost kreatorjev tehnologij. Sledijo prispevki Davida Jelenca, Uroša Majcna in Borisa Škrlja o varnostnih tveganjih, ki jih prinašajo oblačna omrežja in kako varno preiti na oblačno zasnovana kontejnerska omrežja. Matjaž Beričič predstavlja dobre prakse upravljanja oblačno zasnovanega javnega omrežja 5G, Urban Zaletel s soavtorji pa obdeluje oblačno zasnovana zasebna omrežja 5G. Jure Jerman opisuje izzive, s katerimi se soočajo meteorološke službe doma in po svetu, ko vpeljujejo oblačne tehnologije v svoje procese. Oblačno zasnovani poslovni procesi v proizvodnem podjetju je tema, ki jo v prispevku obdeluje Andrej Črepinšek, Izidor Žontar in Miran Ficko pa pojasnjujeta, kako obvladujejo infrastrukturo v zavarovalnici. Zadnji sklop prispevkov se posveča oblačnim storitvam v javni upravi, državni oblak obdeluje Igor Bohinc in občinski oblak Peter Geršič. Prvi ugotavlja, da je čas za posodobitev državnega oblaka, slednji pa opozarja, da na nacionalni ravni manjka strateški razvoj oblačne infrastrukture na lokalni ravni.

Končamo lahko z mislijo, da izbran nabor prispevkov celovito zajema prednosti in slabosti oblačno zasnovanih omrežij. Poleg podrobne obravnave tehnoloških izzivov pa mnogi od njih v središče dogajanja postavljajo uporabnika in se sprašujejo o etičnih in moralnih dilemah sodobnih tehnologij. Le s takšnim pristopom pa lahko zagotovimo, da bo tehnologija zares v korist človeštva in ne obratno.

dr. Tomi Mlinar   Bled, 5. junija 2023
Slovensko društvo za elektronske komunikacije

Foreword

The topic of the 38th telecommunications workshop is cloud-based networks. For decades we talked about telecommunication networks that were (and many still are) built by design, for public or private needs, they enabled voice and/or data communications, the capacity of the equipment had to be planned before the actual installation, it was upgraded in ten-year cycles and upgrades were not cheap, security in such systems (especially protection against eavesdropping) was limited, and the protection of personal data was not even a topic to discuss. In just over a decade, things have changed significantly. A more important, but not always reliable part of the telecommunications equipment is the software that controls the operation of the hardware or the network. The hardware has been minimized to a very powerful application-driven computer. Except for the minimal hardware - radio transmitters and communication terminals, everything else is software that can be changed and updated remotely, at any time and according to current needs. Except for the mentioned pieces of hardware, which must be in specific locations, everything else can be geographically anywhere, as long as it is connected to a powerful Internet, which must always be available. And so we come to the cloud.

Marko Štefančič's introductory article summarizes the trends that are of interest to providers of communication services. Follows an article by Urban Sedlar, who explains modern cloud infrastructures and, among other things, mentions that we must take care of both the physical and virtual level of the cloud network. The first can be entrusted to someone else (the service can be infrastructure, platform or software), and the second is managed by appropriate orchestration. How is with privacy in the cloud, how do we define a data manager and how do we secure data, is the topic of Jelena Burnik's contribution. Cloud infrastructure is a set of complex (mostly) virtual units that are connected and managed in different, mostly standardized ways. These are described in the contributions of Robert Korošec, Aljaž Oman and Aleš Gros. The third set of articles is covered by representatives of the three largest global providers of information and communication infrastructure and cloud solutions, which rely on cloud infrastructure both for data storage and computing power, as well as for the construction of core and access networks.

The introductory lecture of the second part of the proceedings focuses to the user and notes that ethics does not keep up with the development of technology, where misuse of collected data easily occurs and that responsibility lies with the creators of technologies. Then follow articles by David Jelenc, Uroš Majcen and Boris Škrlj on the security risks brought by cloud networks and how to safely switch to cloud-based container networks. Matjaž Beričič presents good practices of cloud-based public 5G network management, while Urban Zaletel and co-authors work on cloud-based private 5G networks. Jure Jerman describes the challenges that meteorological services are facing when introducing cloud technologies into their processes. Cloud-based business processes in a manufacturing company is a topic covered in the article by Andrej Črepinšek, and Izidor Žontar and Miran Ficko explain how they manage the infrastructure in an insurance company. The last set of contributions is devoted to cloud services in public administration, state cloud is processed by Igor Bohinc and municipal cloud by Peter Geršič. The former notes that it is time to modernize the national cloud, while the latter warns that there is a lack of strategic development of cloud infrastructure at the local level at the national level.

We can conclude that the selected set of articles comprehensively covers the advantages and disadvantages of cloud-native networks. In addition to the detailed descriptions of technological challenges, many of them put the user at the center of the action and ask questions about the ethical and moral dilemmas of modern technologies. Only with such an approach can we ensure that technology will really serve humanity.

Dr. Tomi Mlinar   *Bled, 5 June 2023*
Slovenian Electronic Communications Society

Kazalo prispevkov
Table of Contents

5. 6. 2023

VITEL

6. 6. 2023

PRISPEVKI

ARTICLES
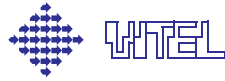
5. 6. 2023

Ključni tehnološki trendi za ponudnike komunikacijskih storitev v letu 2023

Top technological trends for communication service providers in 2023

Marko Štefančič

Gartner Slovenija & Central Asia

POVZETEK

Glavni tehnološki trendi za ponudnike komunikacijskih storitev za leto 2023 izpostavljajo najpomembnejše tržne silnice in interne iniciative, ki so letos v ospredju pozornosti telekomunikacijskih ponudnikov. Vsi analizirani tehnološki trendi so medsebojno povezani in vplivajo tako na tehnologijo kot tudi na poslovanje podjetij. Prispevek predstavlja šest ključnih tehnoloških trendov, njihove vplive na posamezne organizacije in trge telekomunikacijskih in digitalnih storitev ter možne odzive ponudnikov komunikacijskih storitev.

SUMMARY

The main technological trends for communication service providers for 2023 highlight the most important market channels and internal initiatives that are at the forefront of the attention of telecommunications providers this year. All analysed technology trends are interconnected and affect both technology and business operations. The paper presents six key technological trends, their impact on individual organizations and the markets of telecommunications and digital services, as well as the possible responses of communication service providers.

avtor večjega števila člankov in prispevkov o IKT ter soavtor knjige. Za uspešno delo v Gartnerju je prejel več nagrad in priznanj. Marko Štefančič je študiral na Ekonomski fakulteti v Ljubljani. Na Edinburgh Business School Univerze Heriot-Watt v Edinburghu je prejel naziv Master of Business Administration (with distinction).

ABOUT THE AUTHOR

Marko Štefančič is the regional director and principal of Gartner for Slovenia and Central Asia, where he is responsible for business management, strategic planning and cooperation with key customers and users of Gartner's services in the region. He has been working with Gartner for more than 20 years in various functions, mainly in the field of sales and business development.

In the market of information technologies and solutions, Marko Štefančič has more than 25 years of rich experience, both in leadership and management, marketing, consulting and sales. He is also the author of a large number of articles and papers on ICT and co-author of a book. He received several awards and recognitions for his successful work at Gartner.

Marko Štefančič studied at the Faculty of Economics in Ljubljana. He received the title of Master of Business Administration (with distinction) at the Edinburgh Business School of Heriot-Watt University in Edinburgh.

O AVTORJU

Marko Štefančič je regijski direktor in principal Gartnerja za Slovenijo in Centralno Azijo, kjer je zadolžen za upravljanje poslovanja, strateško načrtovanje ter sodelovanje s ključnimi strankami in uporabniki Gartnerjevih storitev v regiji. Z Gartnerjem sodeluje že več kot 20 let v različnih funkcijah, predvsem na področju prodaje in razvoja poslovanja.

Na trgu informacijskih tehnologij in rešitev ima Marko Štefančič več kot 25 let bogatih izkušenj, tako z vodenjem in upravljanjem, marketingom, svetovanjem in prodajo. Je tudi

2023 Top Tech Trends for Communication Service Providers

June 2023

Gartner

Next 5 Years for Communication Service Providers
Eight Impact Factors Covering External and Internal Business Environments

Market Demand Attributes

Product Characteristics

Technology Requirements

Industry Structure

Organizational Strength

Capital Inflow Characteristics

Geopolitical Developments

Regulatory Expansion

Gartner

3 Probable Futures Depend on 3 Sets of Forces

CSPs Response to the Collection of Forces Will Likely Determine Their Future State(s)

Communications as LEADING Industry

Leading / driving influence on industry and society through ecosystems, going beyond connectivity services.

Communications as INSULAR Industry

Low / limited influence on industry and society beyond incremental enhancement of connectivity. CSPs remain mainly as a data transport entity.

Communications as EMBEDDED Industry

Invisible but proactive impact on industry and society through exposure of data and functionalities, embedded in others' products.

We can expect a CSP in multiple probable future states across their lines of businesses.

Gartner

2023 Tech Trends of Significance for CIOs/CTIOs

Cloud-native network operations become imperative

AI/ML use-case adoption multiplies across operations

Looming threat of recession sharpens accountability
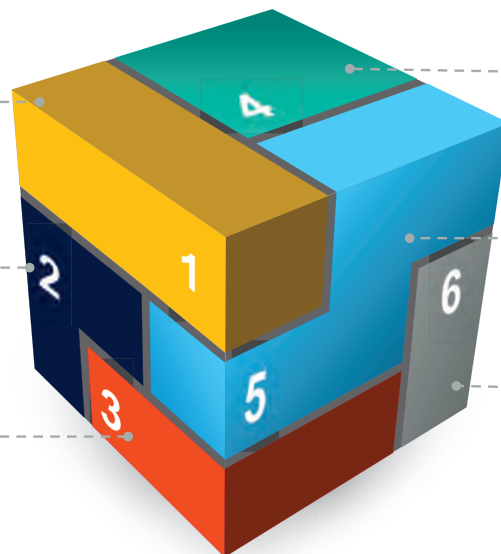
Intelligent automation is a critical pillar for CX improvement

Measurement, visibility and observability become key priorities

CSPs push for "TechCo" ambitions

Gartner

Cloud-Native Network Operations Become Imperative

CSPs worldwide are increasingly embracing cloud technologies as a critical enabler of their digital transformation strategy. Cloud native is an emerging set of design and operational principles that guide the implementation of cloudified software applications and network functions. It builds upon existing best practices for planning, developing, integrating, testing, minoring and governing software across the entire life cycle management. Leveraging the cloud-native principle for network operations is an imperative to realize the vision of a flexible, scalable and agile telecom cloud infrastructure.

Signals ⚑

- Rising demand for containerized applications and network functions by CSPs, particularly for new 5G investments
- Growing availability of cloud-native capabilities in network functions from NEPs for all domains of the network infrastructure
- Expanding use of private, public and hybrid multicloud platforms by CSPs beyond noncritical network functionality

Strategic Planning Assumptions

- By 2025, cloud-native platforms will serve as the foundation for more than 90% of new digital initiatives by CSPs — up from less than 25% in 2021.

Gartner

Cloud-Native Influences People, Process & Tech

As-a-service delivery model | Loosely coupled services | Continuous delivery & integration

Platform Services

Infrastructure

Fusion teams creating & managing cloud native platforms — Open APIs — Standardized and highly automated
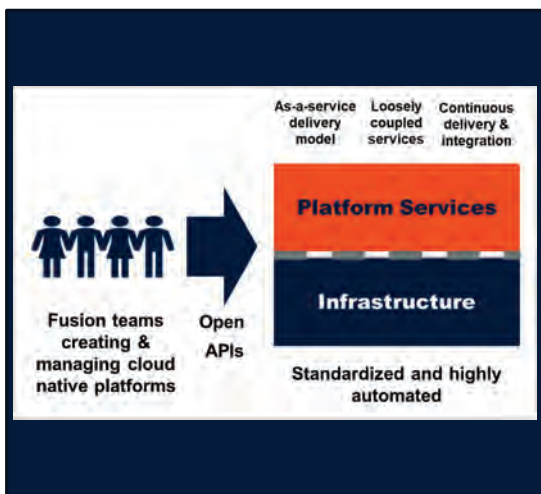
Recommended Response

- Identify business objectives, key stakeholders and adoption KPIs for the cloud-native network operations platform, keeping end-user needs in mind to ensure accessible and intuitive platform capabilities.

- Assess cloud-native needs though a comprehensive assessment of business processes, technologies and change management considerations. Ensure that security, risk and compliance issues are addressed upfront.

- Create an implementation roadmap using a phased approach that aligns efforts and resources with desired business outcomes. Use an MVP approach to ensure early impact and reduce implementation risks.

- Monitor performance and make improvements to the plan. Cloud-native applications and services can be complex and require iterative development and maintenance to maximize their utility.

Gartner

AI/ML Use-Case Adoption Multiplies Across Operations

CSP operations is a notably complex aspect of the business. There are various factors that affect CSPs' performance in this area. A synchronized approach among all business units (BUs) is one of those factors. In recent time, the utilization of AI/ML solutions has shown positive results in optimization of various business functions. Enhancing customer experience (CX), customer retention and cost optimization are some of the priorities. While CSPs have gained some success with CX initiatives, especially in the consumer segment, they are still facing challenges in achieving operational excellence and revenue growth for the majority across various market segments.

Signals ⚑

- As per the 2023 Gartner CIO and Technology Executive Survey, the demand for AI/ML is increasing, and it is most likely technology to be implemented by 2025. One reason for this is the market perception for AI/ML, which is more toward cost reduction.
- Increased budget distribution among BU leaders, as opposed to previous central budget authority, is making them more independent to have autonomy over their digital initiatives within their BUs.

Strategic Planning Assumptions

- By 2025, 35% of CSPs will deploy an AI platform to build their organization-level analytics strategy as compared to 5% at the end of 2022.
- By 2025, at least 40% of BU-operations in CSPs will be digitized and automated using AI/ML solutions as compared to 15% at the end of 2022.

Gartner

Fix the Fundamentals to Scale AI Use to AIOps

Data Source 1 → Data Source 2 → Data Source 3 → Data Source 4 → Data Source 5 → AI Platform → Unified Data Storage / Data Processing / Data Reporting / ML Tools
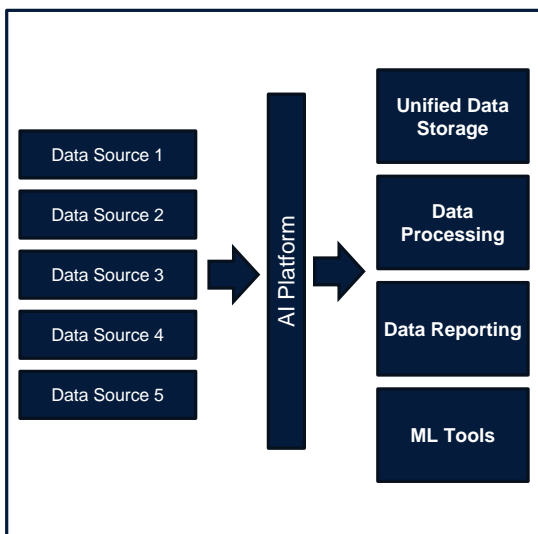
Recommended Response

- Develop a mindshare with other C-suite executives to craft an organizationwide data governance and data management policy enabling wider utilization of AI/ML.

- Formulate a decision-making criteria for different types of AI sourcing mechanisms, such as AI embedded in vendor solutions, horizontal AI platforms, hyperscale's offerings and their own investment.

- Select strong and most immediate AI/ML use cases. Initial plan can focus on specific use cases and applications. However, ensure that the current plan is scalable to incorporate your long-term goals, which should include end-to-end service provisions.

- Start with small projects where you have simple but clear goals. The requirements for such projects would be simple algorithms, which would be easier to start with.

- Enhance your data quality and data strategy by unifying data sets and maintaining data clarity and completeness. Where data is not complete, explore the use of synthetic data.

8

Gartner

Looming Threat of Recession Sharpens Accountability

With the looming threat of recession and other economic headwinds, CSP CIOs are increasingly required to deliver business objectives in a shorter timeframe. This necessitates closer collaboration with a line of business leaders.

Thriving CIOs can showcase and promote increased accountability for investments and time to market to their leadership teams and board.

Signals ⚑

- CSPs' ability to battle inflation with price increases is no longer a feasible option given recession and consumer sentiment, making efficiency the key driver for CSPs to deliver their 2023 results.
- Real purchasing power of IT budgets will be reduced in many markets, even though in terms of constant currency Gartner forecasts telecommunication companies IT spend will continue to grow in single digits (with growth shrinking from 6.0% in 2022 to 5.4% in 2023).

Strategic Planning Assumptions

- By 2024, CIOs focusing on projects with 12- to 18-month business impact will be fully funded while long-term projects struggle with business case approvals.

Gartner

To Thrive During the Looming Recession Phase

SPM

- Align with business priorities
- Accelerate cost optimization
- Plan skills and resources in advance
- Accelerate digitalization and automation
- Assess and minimize impact on contracts

Recommended Response ▤

- Align all initiatives closely with the line of business leaders to make sure that technical projects are fully aligned with the business priorities and that business teams are prepared to utilize the new technical capabilities being rolled out fully.

- Use a strategic portfolio management (SPM) system to reprioritize the existing portfolio and plan additional initiatives.

- Check the cost optimization efforts to see if any current or planned initiatives can be accelerated and can deliver a big enough impact in a timely fashion.

- Plan the needed resources and skills well in advance; a looming threat of recession is also a good time to hire critical skills and build new capabilities.

- Work together with the operational teams to assess the current level of digitalization and automation, and develop a roadmap to accelerate.

- Proactively check the main contracts for possible impacts from inflation or currency fluctuations, and work together with sourcing teams to minimize the impact.

Gartner

Intelligent Automation Is a Critical Pillar for CX Improvement

While customer experience has been one of CSPs' main focus areas for differentiation, challenges persist across customer journeys. The complexity of business and operational processes, together with siloed IT and data systems, is often the root cause of poor customer experience. Intelligent automation addressing both business and operational processes across the different teams and IT systems is emerging as an approach to improve CX, along with employee experience in a total experience paradigm. By providing consistent, contextually aware automated digital customer interactions and network operations, as well as enhanced tools for employees supporting customers, intelligent automation is driving improved CX metrics in companies and industries that have implemented it.

Signals ⚑

- CSPs continue to focus on improving CX but are limited by siloed solutions, processes and component-level IT focus. Tech companies that use automation as a key pillar of customer engagement rank higher than CSPs on CX metrics.
- Composable architectures, and open APIs, combined with RPA and low-code/no-code process automation tools, enable focusing on intelligent automation without complex companywide digital transformation.

Strategic Planning Assumptions

- By 2025, CSPs with intelligent automation in place for business and operational processes will outperform their peers measured by both CX and efficiency benchmarks by a minimum of 20%.

Gartner

Leverage CX Goals for Enhancing Automation

Identify drivers of dissatisfaction

Map E2E processes

Identify KPIs

Use intelligent automation
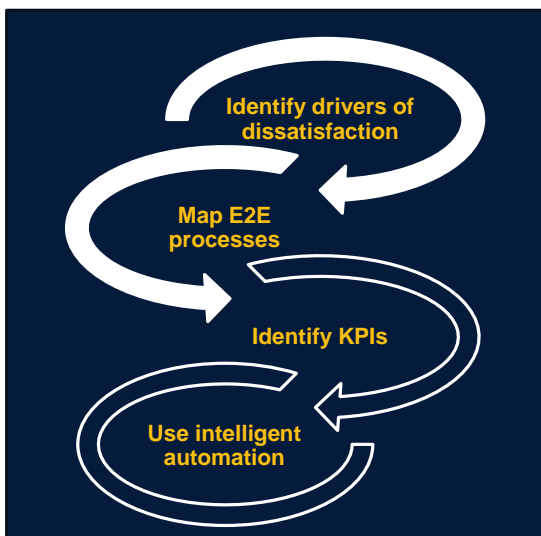
Recommended Response

- Identify key pain points in current business processes driving customer and employee dissatisfaction.

- Map the intersection between IT systems and the different teams across end-to-end business processes.

- Identify the digital outcome KPI measurements to be used to quantify and track progress in customer experience, employee experience and efficiency.

- Execute digital transformation projects to improve CX/TX by using intelligent automation for the selected business and operational processes.

- Plan the organizational and people aspects of the change to make the automation journey positive for employees, including necessary training or reskilling.

12

Gartner

Measurement, Visibility and Observability Become Key Priorities

Visibility refers to availability of relevant data and some insights into a localized process or system. On the other hand, observability allows systems to be "seen" and their behavior to be understood in a broader/holistic context.

CSPs' technology stack and supplier relationships are getting more complex. A larger part of the infrastructure and applications is outside of IT control. Traffic and data volumes are increasing. Traditional regulatory compliance requirements get more dynamic. ESG, energy and security compliance emerge. Yet budgets are tight, and IT should lead. Measurement, visibility and observability become a key strategic goal and tool for CSP IT next-generation value.

Signals ⚑

- Leading CSPs have increasing interest in analytics, AI and end-to-end services and the network view.
- Going beyond monitoring for known problems and toward mining insights from data as digital business brings with it unknown issues.
- CSPs' CX goals along with hyperautomation, cloud, security, ecosystem play, regulatory demands and product complexities are increasing the need for visibility and observability.

Strategic Planning Assumptions

- By 2025, 80% of tier-1 CSPs will treat monitoring, visibility and observability as a dedicated initiative for their operations, up from 30% in 2023.
- By 2023, smaller CSPs have emerged as the industry leaders in real-world measurement, visibility and observability due to their organizational agility.

Gartner

Consider a Framework to Deal With Many Needs
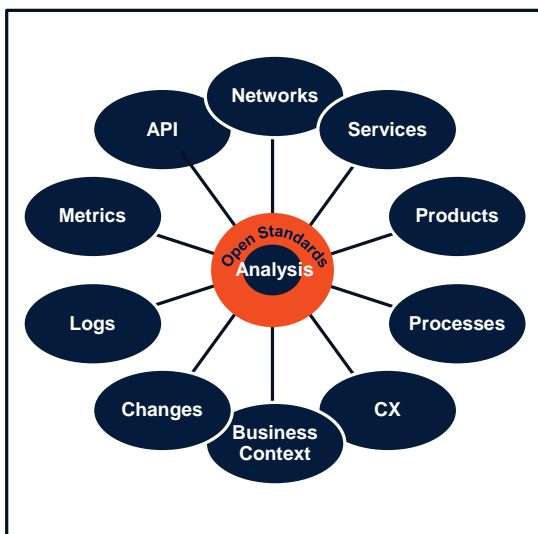
Recommended Response

- Fix your data management and governance practices to suit the goals of measurement, visibility and observability. It will aid other strategic initiatives such as AIOps, hyperautomation and others.

- Start proving ROI with solutions to problems that existing silo solutions cannot fix. For example, connect deployment and service assurance to avoid service impact to fiber customers in a multitenant building; or value for regulatory, ESG and energy.

- Start tearing down the organizational obstacles by working more closely with the enterprise risk function.

- Make visibility and enabling observability a key element of sourcing criteria for applications and infrastructure, and increase application and infrastructure uptime.

- Start to move to business observability by using AIOps to analyze correlations across the datasets generated by multiple monitoring tools. The correlations indicate opportunities to bridge organizational siloes.

- Consider business observability as a culture change agent by improving visibility and understanding of the interrelated nature of digital business problems. Everybody benefits if everybody contributes.

Gartner

CSPs Push for "TechCo" Ambitions

Digital technologies and their impact on society, customers and organizations have influenced many companies to pursue the goal of becoming a technology company (TechCo). Such companies include many CSPs, considering the significant influence of technologies such as cloud, containerization and AI on development process, network, operations and products. In addition, competition with tech giants such as hyperscalers has further buttressed the goal of some CSPs toward TechCo. However, there is no one common, clear and shared definition of TechCo, and CSPs have their own, and often fuzzy, definition of TechCo.

Signals ⚑

- Increasing investments and efforts to hire software engineering talent and train others in the organization
- Insourcing of manpower in many initiatives to gain control over technology change
- Development of select systems (such as customer journey layer, service orchestration layer, AI/ML, etc.) by many CSPs

Strategic Planning Assumptions

- By 2025, TechCo ambitions of 70% of CSPs will dampen because of lack of a shared vision and unclear outcomes.
- By 2025, TechCo goals will diversify talent sourcing in 50% of CSPs, up from 10% in 2022.

Gartner.

Clarity of Goal and Outcome Is Paramount

Business Objectives	Business Outcomes
As-Is Situation/Tech Competence	

↓

TechCo Definition

↓ ↓

What (Areas of Operations)	How (Ways of Working)
Governance Mechanism and KPIs	
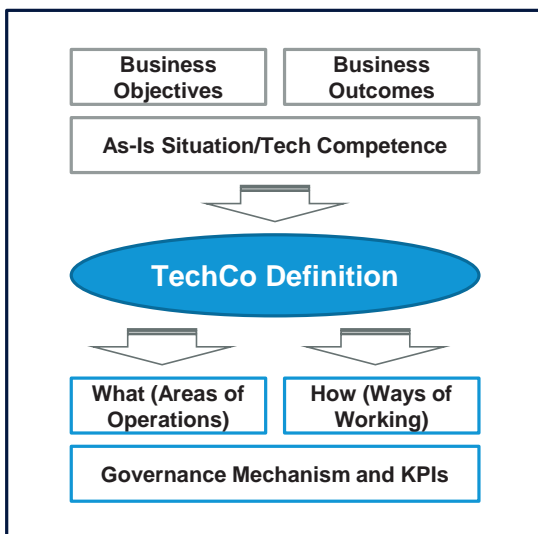
Recommended Response

- Define a common, unified and clear definition of TechCo for your organization. Ensure that you have full buy-in from the CEO and CFO.

- Work with other stakeholders (business units, HR, L&D and others) to develop a shared goal and ways of working.

- Focus on discovery and validation of customer needs. Use the lens of customer experience and competitive differentiation together while identifying objectives and outcomes associated with TechCo ambition.

- Assess current competence levels, not just in the present context of business requirements but considering the next five to seven years.

- Develop a set of principles to assess ideas, and make a checklist to test every idea, considering: Can it really contribute to differentiation for your business, can you do application development best for yourself, can you maintain a system better than partners?

- Ensure that you can provide a long-term career path and appropriate compensation in the technology workforce. If doubtful, reassess your plan.

Gartner.

Top Priorities & Technologies in Telecom in 2023
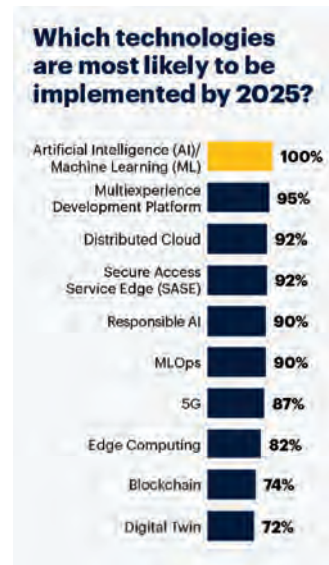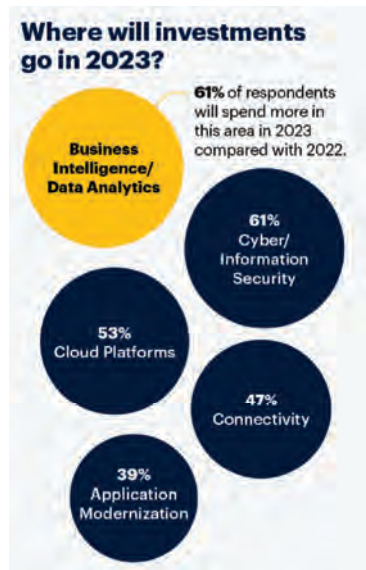
Source: 2023 Gartner CIO and Technology Executives Survey: telecom CIOs and executives

Gartner

Recommended Gartner Research

▷ **CSP Digital Transformation and Innovation Primer for 2023**
Amresh Nandan

▷ **Routes to the Future for CSP CIOs: Invest in Platform Capabilities to Shape Business**
Mentor Cana, Amresh Nandan, Mike Edholm

▷ **Routes to the Future for CSP Product Leaders: Balance Ecosystem, Innovation and Optimization**
Mike Edholm, Amresh Nandan, Mentor Cana

▷ **2023 CIO and Technology Executive Agenda: Navigating the Triple Squeeze for CSPs**
Amresh Nandan, Susan Welsh de Grimaldo

▷ **Infographic: Top Priorities, Technologies and Challenges in Telecom in 2023**
Amresh Nandan, Susan Welsh de Grimaldo

▷ **Predicts 2023: CSP Technology and Operations Strategies**
Amresh Nandan, Susan Welsh de Grimaldo, Juha Korhonen, Kosei Takiishi, To Chee Eng

▷ **Objectives and Principles for OSS Architecture Evolution in CSPs**
Amresh Nandan, Mentor Cana

▷ **Objectives and Principles for Assurance Architecture Evolution in CSPs**
Amresh Nandan, Susan Welsh de Grimaldo

▷ **Research Roundup: Top Technology Trends for CSPs in 2022**
Mentor Cana, Amresh Nandan

Gartner

Sodobne oblačne infrastrukture

Modern cloud infrastructures

Urban Sedlar

Univerza v Ljubljani, Fakulteta za elektrotehniko

POVZETEK

Računalništvo v oblaku predstavlja fleksibilen in stroškovno učinkovit način za dostop do računskih, hrambnih in omrežnih kapacitet. V tem predavanju so predstavljene osnovne koncepte računalništva v oblaku, vključno s storitvenimi modeli (infrastruktura, platforma in programska oprema kot storitev), možnostmi za uvedbo (javni, zasebni in hibridni oblak) ter njihovimi ekonomskimi implikacijami in potencialom za lock-in. Pojasnjeni so infrastrukturni vidiki, od virtualizacije do orkestracije in osvetljene sodobne prakse za njihovo upravljanje (DevOps, DevSecOps, Infrastructure as Code). V predavanju se dotikamo tudi sodobnih trendov, ki vključujejo t.i. brezstrežniško (serverless) računalništvo, rob oblaka (edge computing) in večoblačna okolja.

SUMMARY

Cloud computing represents a flexible and cost-effective way to access computing, storage and network capacities. This lecture introduces the basic concepts of cloud computing, including service models (infrastructure, platform, and software-as-a-service), deployment options (public, private, and hybrid cloud), and their economic implications and potential for lock-in. Infrastructure aspects are explained, from virtualization to orchestration, and modern practices for their management (DevOps, DevSecOps, Infrastructure as Code) are highlighted. In the lecture, we also touch on modern trends, which include the so-called serverless computing, edge computing and multi-cloud environments.

O AVTORJU

Dr. Urban Sedlar je raziskovalec in predavatelj na Fakulteti za elektrotehniko Univerze v Ljubljani. Ukvarja se s področjem informacijsko komunikacijskih tehnologij, zlasti s kibernetsko varnostjo, računalništvom v oblaku in sistemi za kritične komunikacije. Sodeluje pri več evropskih in nacionalnih projektih ter je soavtor 7 patentov in številnih člankov v uglednih revijah.

ABOUT THE AUTHOR

Dr. Urban Sedlar is a researcher and lecturer at the Faculty of Electrical Engineering of the University of Ljubljana. He deals with the field of information and communication technologies, especially with cyber security, cloud computing and systems for critical communications. He participates in several European and national projects and is the co-author of 7 patents and numerous articles in reputable journals.

Sodobne oblačne infrastrukture

dr. Urban Sedlar
Fakulteta za elektrotehniko
Univerza v Ljubljani

Vsebina

- Uvod
- Storitveni modeli
- Infrastrukturni vidiki
- Namestitvene možnosti
- Upravljanje
- Ekonomika in lock-in
- Sodobni trendi

Sodobni informacijski sistemi
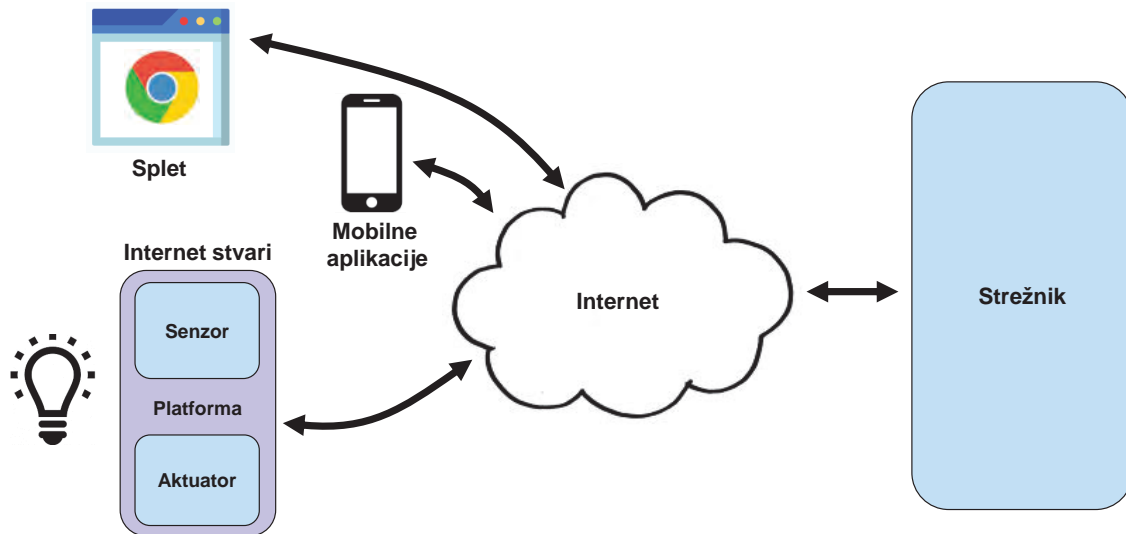
Strežnik kot osnovni gradnik oblaka

- Računalnik (x86, v zadnjih letih tudi ARM; populraen tudi GPU za ML)
- Operacijski sistem
  (najpogosteje Linux/FOSS,
  zaradi stroška licenc)

SOHO verzija   **Datacenter verzija**

Strežnik kot osnovni gradnik oblaka

- Sodobne potrebe nas pripeljejo do podatkovnega centra
  - Veliko strežnikov + vsa potrebna infrastruktura
  - Ponudniki imajo lahko nekaj 100 do nekaj milijonov strežnikov

Omrežje

Napajanje

Diskovje   ILO

25 U
=
111 cm

© Laboratory for Telecommunications, Faculty of Electrical Engineering

Pojavijo se številne težave

- Upravljanje s fizično infrastrukturo
  - Layer 1 problemi: napajanje, hlajenje, povezljivost, menjava pokvarjenih delov, odvisnost SW/HW (watchdog, gonilniki,...), fizično varovanje

- Kako menjamo fizično infrastrukturo brez prekinitve storitve
  - Virtualizacija: uvedba koncepta virtualnega strežnika
  - Abstrakcija (decoupling) med *softwarom* in *hardwarom*

- Upravljanje z virtualno infrastrukturo
  - Zdaj moramo stvarem slediti na 2 layerjih! (fizično + virtualno)
  - Tu nam bosta pomagali: orkestracija in abstrakcija (PaaS/SaaS/FaaS/BaaS)

- Računalništvo v oblaku poskuša rešiti vse naštete težave

© Laboratory for Telecommunications, Faculty of Electrical Engineering

Operativna definicija

- Oddaljen dostop do strežnikov poznamo že desetletja
  - Kaj je zdaj drugače
- Sodobna definicija računalništva v oblaku
  - NIST (National Institute of Standards and Technology)
  - »model za **zagotavljanje omrežnega dostopa do** deljenega nabora **računalniških virov** (kamor sodijo omrežja, strežniki, diskovni prostor, aplikacije in storitve), ki jih je mogoče **hitro pripraviti za uporabo in hitro sprostiti**, oboje z minimalnim trudom in **z minimalno interakcijo ponudnika storitve**«

- Poznamo več modelov

Modeli računalništva v oblaku

- **Infrastruktura kot storitev (IaaS)**
  - V najem bomo dali virtualne strežnike ali kontejnerje
- **Platforma kot storitev (PaaS)**
  - V najem bomo dali *vire* za razvoj in poganjanje aplikacij
- **Programsko opremo kot storitev (SaaS)**
  - V najem bomo dali računovodski software z web gui
- Back-end kot storitev (BaaS)
  - V najem bomo dali HTTP REST API-je in pripadajoč client SDK
  - Da razvijalec ne potrebuje svojega strežnika
- Function as a Service (FaaS)
  - T.i. serverless computing; v oblaku deployamo samo funkcijo
  - Npr. Python koda, ki ima REST API

λ

Infrastruktura

- Ne samo fizični strežniki
- Temveč tudi vsa podporna oprema
  - Omrežna oprema, diskovna polja, sistem za varnostne kopije, klima, UPS

- Obratovalni stroški
  - Elektrika, hlajenje, omrežna povezljivost, vzdrževanje

- V podatkovnih centrih definiramo metriko PUE (Power Usage Effectiveness)
  - Kakšen delež vse energije porabi računalniška oprema
  - Amaterske rešitve imajo slabo razmerje, skupno > 2 W na Watt (overhead >100%)
  - Vodilni ponudniki dosežejo PUE faktor 1.1 ali manj (overhead <10%)

© Laboratory for Telecommunications, Faculty of Electrical Engineering

Primer: Google PUE

Vir: Google
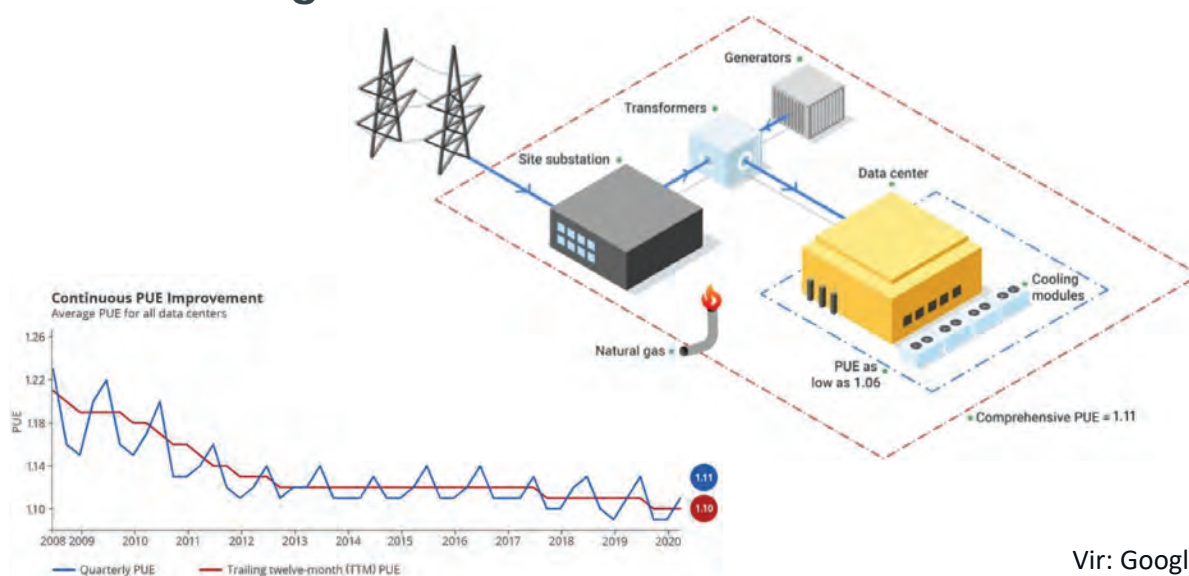
© Laboratory for Telecommunications, Faculty of Electrical Engineering

Primer: Amazonova strojna oprema

Vir: Amazon

Virtualizacija in kontejnerizacija

Kontejner vs. VM

- Ključna razlika
    - Kontejnerji so manjši in imajo manj režije

Lastnost	VM	Kontejner
Upravljalec	Hipervizor	Jedro OS
Jedro	Lastno jedro	Deljeno s hostom
Vzpostavitev	Nekaj minut	Nekaj sekund
Velikost slike	Od nekaj GB	Od nekaj MB
Zamenljivost	Nizka	Visoka
Stopnja izolacije	Visoka	Nizka
Uporabnost za monolitne aplikacije	Dobra	Slaba
Režija		Do 2-3x manjša

Koncept PaaS

⚠️ **Pozor: Total lock-in!**
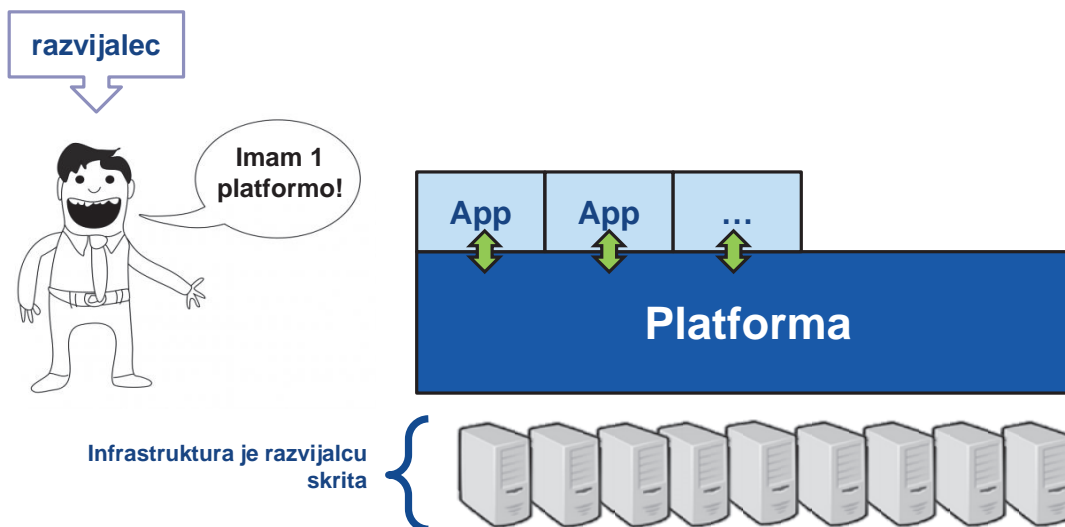
razvijalec

Imam 1 platformo!

App   **App**   **...**

Platforma

Infrastruktura je razvijalcu skrita {

Koncept SaaS
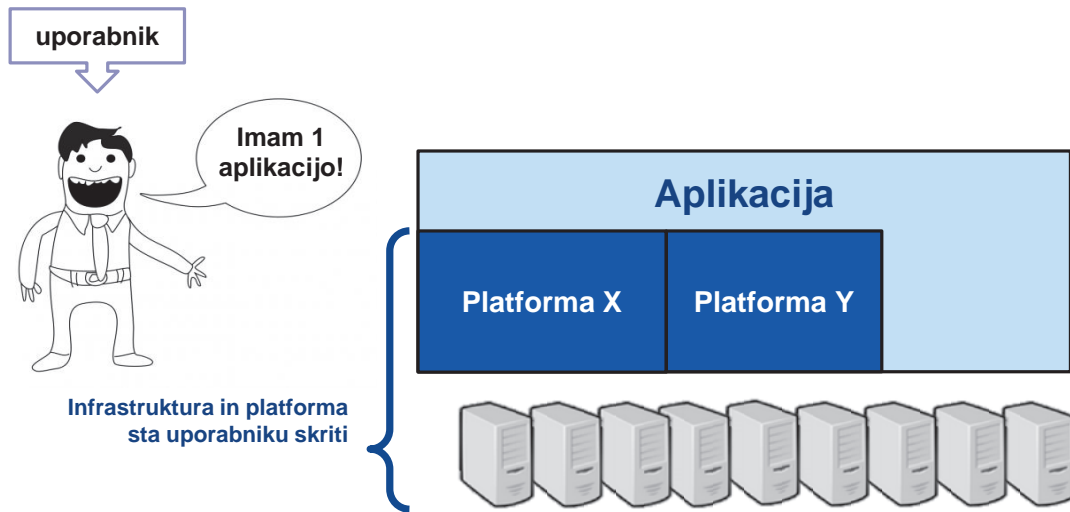
Koncept BaaS

⚠ Pozor: Total lock-in!

- Primer: Google Firebase
  - Najem back-enda
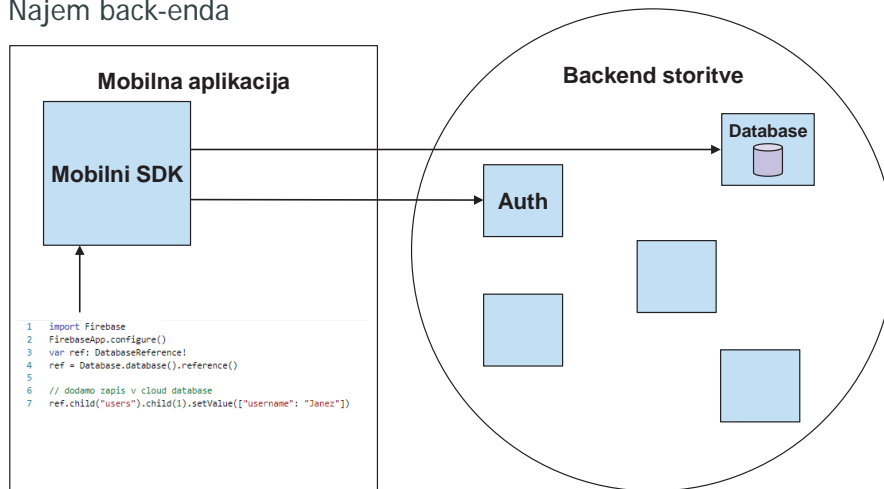
Serverless computing

⚠️ **Pozor: Delni lock-in!**

- Pretvarjamo se, da strežnika sploh ni
  - "So samo funkcije v vakuumu, ki imajo API vmesnike"

Strežnik

```
//JavaScript
function sum(a,b) {
    return a+b;
}
```

Odjemalec ← http://server.com/sum/7/3 →
← {result: 10}

```
#Python
def prod(a,b):
    return a*b
```
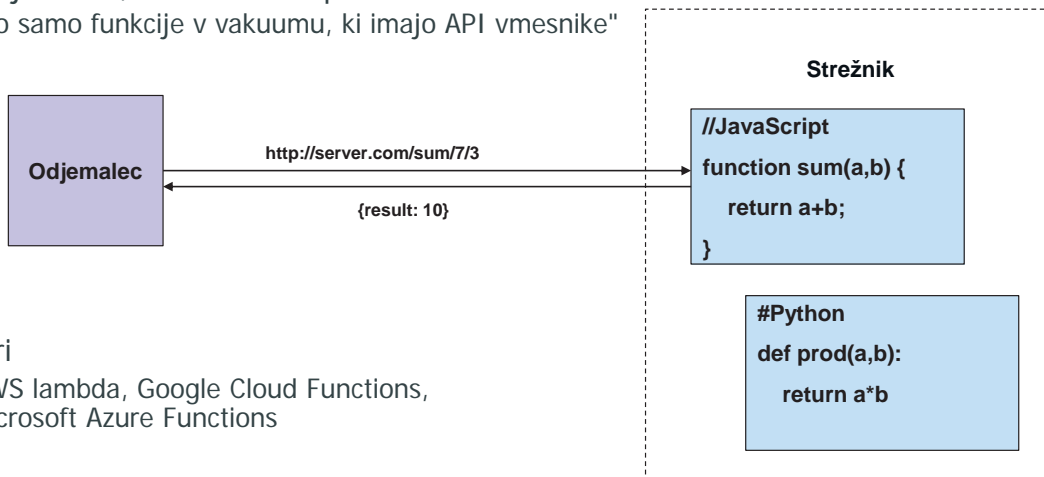
- Primeri
  - AWS lambda, Google Cloud Functions, Microsoft Azure Functions

© Laboratory for Telecommunications, Faculty of Electrical Engineering

Kaj je funkcija v FaaS modelu

- Osnovne lasnosti
  - Počne eno stvar
  - Kratkotrajna oz. minljiva
  - Nima internega stanja → *stateless*
  - Podpira skaliranje
  - Jezik in okolje nista pomembna (definiran je le API)
- Delno ujemanje s konceptom mikrostoritve
  - Vhod (REST API zahteva)
    ⬇
    izhod (REST API odgovor)

Short-lived
Functions
Single-purpose

FaaS
Stateless
Ephemeral
Auto-scaling

Long-lived
Microservices
Multi-purpose
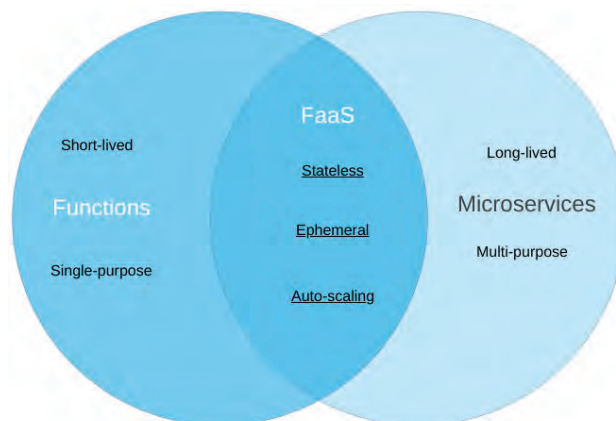
© Laboratory for Telecommunications, Faculty of Electrical Engineering

Modeli namestitve (deployment models)

- Zasebni oblak – HW pod našo kontrolo
  - Strežniki + virtualizacija (VMWare, KVM, ProxMox)
  - Ne nujno v hiši – možna kolokacija v podatkovnem centru
- Javni oblak – HW pod kontrolo ponudnika
  - Zaseganje in sproščanje preko API vmesnikov
- Hibridni oblak
  - Kombinacija privatnega in javnega
  - Možna večja fleksibilnost glede varovanja podatkov in skalabilnosti
- Večoblačno okolje
  - V zadnjem času vedno pogostejša možnost za visoko razpoložljivost
  - Izogib "single point of failure"

© Laboratory for Telecommunications, Faculty of Electrical Engineering

DevOps in CI/CD

- Beseda DevOps
  - Kombinacija razvoja programske opreme in
  - administracije sistemov (Operations)
- Gremo v smeri čim večje avtomatizacije
  - manjša možnost človeške napake
  - Hitrejši cikli izdajanja programske opreme

- Včasih:
  - **Razvoj** (in svn commit)
  - Prevajanje
  - Testiranje (lokalno)
  - Pakiranje
  - Namestitev
  - Konfiguracija
  - Spremljanje delovanja

- Danes
  - **Razvoj** (in git commit + push)
  - Prevajanje → samodejno
  - Testiranje → samodejno
  - Pakiranje → samodejno
  - Namestitev → samodejno
  - Konfiguracija → iz YAML-a
  - Spremljanje delovanja → samodejno

© Laboratory for Telecommunications, Faculty of Electrical Engineering

CI/CD – povratna zanka

- Continuous integration (nenehna / nepretrgana integracija)
- Continuous deployment (nenehno / nepretgano nameščanje)
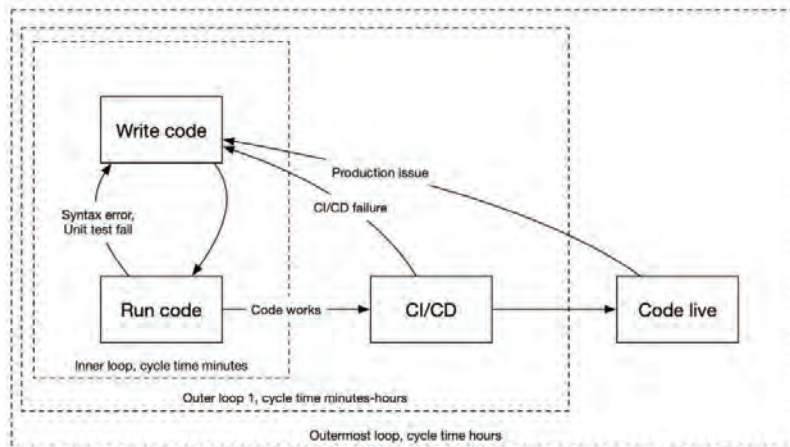
Vir: https://erikbern.com/2021/04/19/software-infrastructure-2.0-a-wishlist.html

Pot do orkestracije

- Ročno upravljanje strežnikov / VMjev / kontejnerjev
  - ni skalabilno
- Avtomatizacija procesa
  - Večina platform daje na voljo API vmesnike (VmWare, OpenStack, AWS,...)
  - Primeri: Ansible, Puppet, Chef, skriptni jeziki
  - Pogosto ponovljive operacije "poskriptamo"
  - Česar ne poskriptamo, se ne zgodi.
- Prava orkestracija
  - Sistem se mora "zavedati" (razumeti) samega sebe
  - Primeri: Docker Swarm, Kubernetes
  - "Infrastructure as code" – navodila za orkestratorje
  - Self-healing: če en strežnik odpove, se mora vsebina preseliti na drugega
  - Autoscaling: avtomatsko skaliranje glede na metrike obremenjenosti
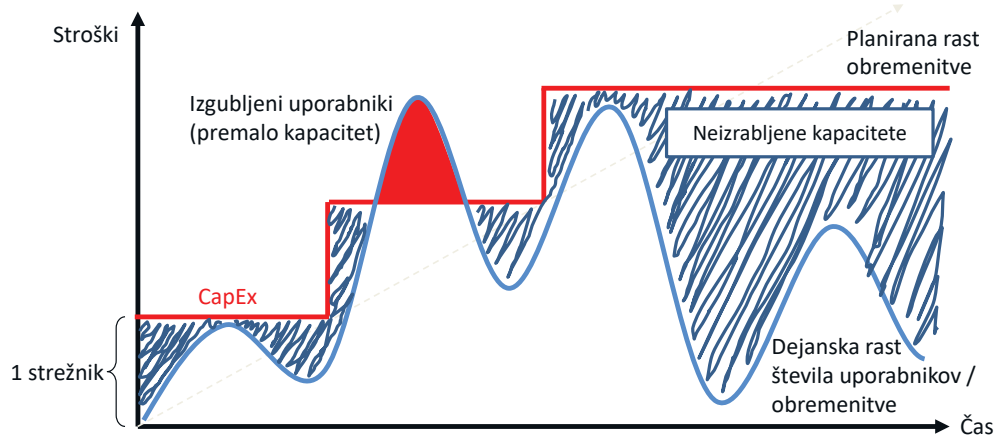
Stroškovni vidik: CapEx vs. OpEx

- CapEx: investicije (npr. nakup opreme)
- OpEx: obratovalni (sprotni) stroški (npr. "naročnina 5 EUR / mesec")

Stroškovni vidik: CapEx vs. OpEx

- CapEx: investicije (npr. nakup opreme)
- OpEx: obratovalni (sprotni) stroški (npr. "naročnina 5 EUR / mesec")

Skriti stroški

- Tudi pri privatnem oblaku so obratovalni stroški
  - Elektrika, vzdrževanje, varnostne kopije, najem prostora, varovanje

Vir: https://sapongcp.eu/sap-and-finops-next-steps/
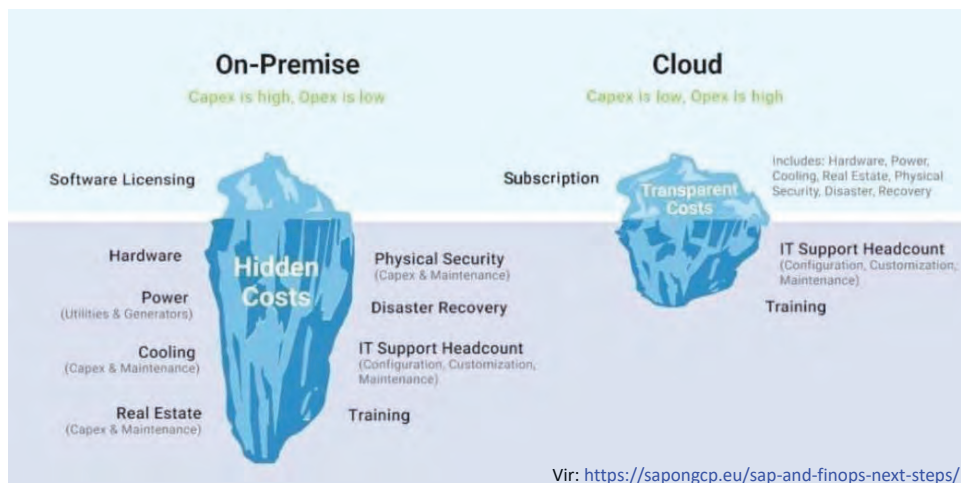
© Laboratory for Telecommunications, Faculty of Electrical Engineering

Kdo upravlja z infrastrukturo?

https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

© Laboratory for Telecommunications, Faculty of Electrical Engineering

Večoblačni sistemi

- Sistem namestimo na več oblačnih ponudnikov
- Opremo moramo spraviti v eno logično omrežje
    - Npr. preko site-to-site VPN
- Danes obstajajo ponudniki, ki vso logistiko že naredijo za nas
    - Amazon, Cast.AI
- Možen dodaten nivo finančne optimizacije
    - avtomatska uporaba trenutno najcenejše infrastrukture
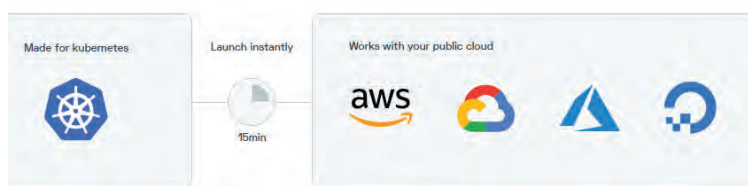
Varnost

- Marsikdo vam bo hotel prodati dejstvo, da je oblak *de facto* varen
    - Toda: dobite to kar plačate

- Primer: požar v OVHcloud, Strasbourg
    - Vse varnostne kopije shranjene on-site in izgubljene

- Primer: Amazon
    - Fizično varovanje podatkovnih centrov
    - Snowmobile: tovornjak za transport velikih podatkov + oboroženo spremstvo

Perimeter Layer

AWS data center physical security begins at the Perimeter Layer. This Layer includes a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures. Scroll down to learn more about the types of security measures we have in place within the Perimeter Layer of the data centers we operate around the world.

Druge sodobne paradigme

Splet

Internet stvari

Senzor

Platforma | CPU

Aktuator

Mobilne aplikacije

Internet

Megla (Fog)
Procesiranje in hramba podatkov blizu uporabnika oz. na robu omrežja (edge)

Dropbox

Procesiranje in hramba podatkov _neposredno na končni napravi_

Rosa (Dew)

Strežnik

Strežnik

Oblak (Cloud)

Strežnik

© Laboratory for Telecommunications, Faculty of Electrical Engineering

Hvala za pozornost!

urban.sedlar@fe.uni-lj.si

LTFE Laboratorij za telekomunikacije | IKT Katedra za informacijske in komunikacijske tehnologije | Univerza v Ljubljani Fakulteta za elektrotehniko

© Laboratory for Telecommunications, Faculty of Electrical Engineering

VITEL

Zasebnost v oblaku

Privacy in the cloud

Jelena Burnik

Republika Slovenija, Urad informacijskega pooblaščenca

POVZETEK

Sodobnega življenja, poslovanja, šolanja, pa tudi druženja si skoraj ni več mogoče predstavljati brez uporabe storitev vsaj kakega od znanih komercialnih oblačnih ponudnikov. Marsikaj nam oblak olajša, s sabo pa prinaša tudi tveganja za varstvo osebnih podatkov, ki so povezana z razpršenostjo podatkov in različnimi lokacijami njihove obdelave. V prispevku bomo poskusili odgovoriti na naslednja vprašanja: Kako dobro nam gre z varovanjem zasebnosti in osebnih podatkov v oblaku? Katera so tveganja? Na katere določbe zakonodaje o varstvu osebnih podatkov moramo biti še posebej pozorni? Kaj kaže praksa Informacijskega pooblaščenca?

SUMMARY

It is almost impossible to imagine modern life, business, schooling, and socializing without using the services of at least one of the well-known commercial cloud providers. The cloud makes many things easier for us, but it also brings with it risks for the protection of personal data, which are related to the dispersion of data and the various locations of their processing. In this article, we will try to answer the following questions: How well are we doing with protecting privacy and personal data in the cloud? What are the risks? Which provisions of the legislation on the protection of personal data should we pay particular attention to? What does the practice of the Information Commissioner show?

O AVTORJU

Dr. Jelena Burnik je vodja mednarodnega sodelovanja in nadzora pri Informacijskem pooblaščencu (IP), kjer koordinira področje čezmejnega sodelovanja IP pri inšpekcijskem nadzoru ter sodelovanje IP v Evropskem odboru za varstvo podatkov. Informacijskemu pooblaščencu se je pridružila leta 2008, ukvarja se predvsem s problematiko varstva osebnih podatkov pri sodobnih informacijsko komunikacijskih storitvah in digitalnem marketingu, čezmejnim sodelovanjem nadzornih organov, prenosu podatkov v tretje države, certificiranjem in aktivnostmi dvigovanja zavedanja o varstvu osebnih podatkov. Kot državna nadzornica za varstvo osebnih podatkov je Informacijskega pooblaščenca zastopala v številnih telesih, delovnih skupinah in projektih, med drugim v Delovni skupini iz člena 29 ter pri Svetu Evrope, v mreži GPEN, Delovni skupini za digitalno izobraževanje Global Privacy Assembly, Svetu za varno rabo interneta. Koordinirala je več evropskih projektov, v katerih je Informacijski pooblaščenec sodeloval kot partner v konzorciju (projekt CRISP o certificiranju varnostnih produktov in storitev in ARCADES o izobraževanju o zasebnosti v šolah) oziroma kot edini izvajalec (projekt iDecide za dvigovanje zavedanja o varstvu osebnih podatkov).

ABOUT THE AUTHOR

Dr. Jelena Burnik is the head of international cooperation and control at the Information Commissioner, where she coordinates the field of cross-border IP cooperation in inspection control and IP cooperation in the European Data Protection Board. She joined the Information Commissioner in 2008 and deals primarily with issues of personal data protection in modern information and communication services and digital marketing, cross-border cooperation of supervisory authorities, data transfers to third countries, certification and activities to raise awareness of personal data protection. As the national supervisor for the protection of personal data, she represented the Information Commissioner in numerous bodies, working groups and projects, including in the Working Group referred to in Article 29 and at the Council of Europe, the GPEN network, the Global Privacy Assembly Working Group for Digital Education, the Safe Use Council internet. She coordinated several European projects in which the Information Commissioner participated as a partner in a consortium (the CRISP project on the certification of security products and services and the ARCADES project on privacy education in schools) or as the sole contractor (the iDecide project to raise awareness of personal data protection).

Zasebnost v oblaku?

dr. Jelena Burnik
VITEL, 2023

Kako zasebno je v oblaku?

– Tveganja za VOP

– Ključna pravila

– Kaj prinaša ZVOP-2

– Kaj kaže praksa IP

Varstvo osebnih podatkov
&
računalništvo v oblaku

Nekatera tveganja z vidika VOP

— Razdelitev odgovornosti za VOP med različnimi: **kdo so upravljavci podatkov?**

— Tipske informacije in dogovori – neenakost moči

— Ali ima upravljavec podatkov pravno podlago, da hrani/obdeluje podatke v oblaku (nejasne lokacije, tretje države)

— Informiranje

— Zavarovanje podatkov

— **Prenos podatkov v tretje države**

Pravila varstva osebnih podatkov

Splošna uredba o varstvu podatkov (GDPR)

- načela, razdelitev vlog, pravne podlage, zavarovanje, prenos podatkov v tretje države

Novi Zakon o varstvu osebnih podatkov (ZVOP-2)

- sledljivost obdelave podatkov, omejitve prenosa podatkov izven RS, poznavanje lokacij, uveljavljanje pravic posameznikov, globe!

Temeljna načela varstva osebnih podatkov

Zakonito, pošteno in pregledno

Le za določene in zakonite namene

Minimalen nabor podatkov

Točni in posodobljeni

Omejeni roki hrambe

Zavarovanje

Odgovornost upravljavca

Definicija vlog: kdo so upravljavci podatkov?
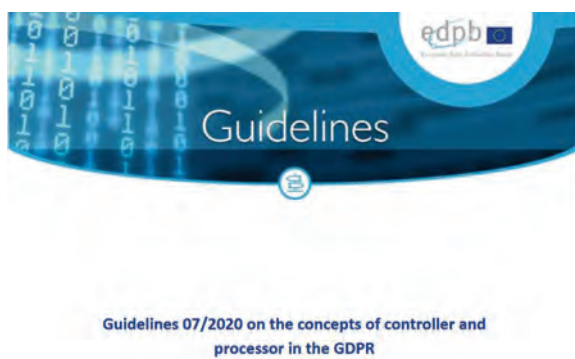
Pogodbeni obdelovalci
Skupni upravljavci
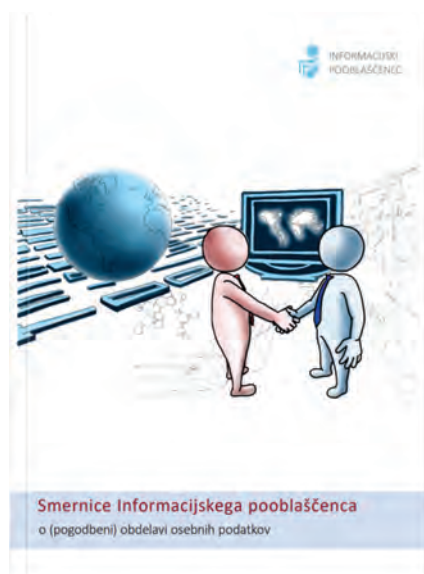
Skupni upravljavci

IZ PRAKSE IP: Ponudnik oblačne storitve in klient sta lahko skupna upravljavca!

Pravne podlage za obdelavo osebnih podatkov

- Ključno za upravljavce, kliente

- Splošna uredba o varstvu osebnih podatkov, ZVOP-2
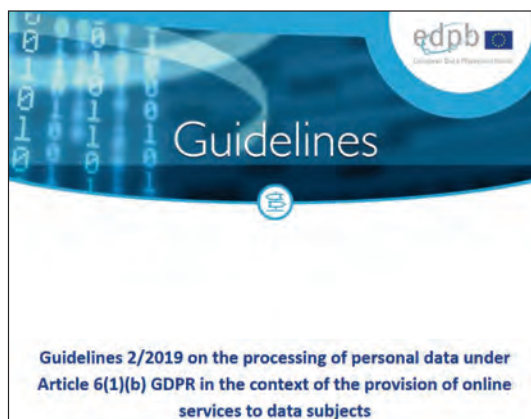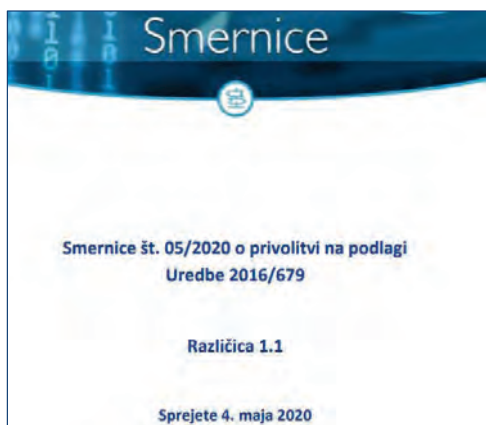
Obvestilo o obdelavi OP

Širši nabor informacij, ki jih je treba sporočiti posamezniku (13. člen)
— informacije o upravljavcu in DPO (če obstaja)
— nameni obdelave in pravna podlaga za obdelavo
— kadar je pravna podlaga zakoniti interes, tudi navedba zakonitega interesa
— uporabniki OP
— prenos podatkov v tretje države

Dodatno tudi :
— roki hrambe ali merila za roke hrambe
— informacije o pravicah posameznikov in pravici do preklica privolitve
— pravica do pritožbe k IP
— obstoj profiliranja, razlogi zanj, posledice

In še:
v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku, kar velja zlasti za vse informacije, namenjene posebej otroku

Zavarovanje podatkov

— vgrajeno varstvo osebnih podatkov, zasebnosti prijazne začetne nastavitve

  od začetka razvoja produktov in storitev

— poročanje o incidentih v zvezi z osebnimi podatki

Prenosi podatkov v tretje države po t. i. sodbi Schrems II

- Poglavje V Splošne uredbe – cilj je zagotoviti enako raven varovanja podatkov tudi pri prenosu iz EU v tretje države

- Dolžnost in odgovornost upravljavca podatkov!

- Podlage za prenos podatkov:
  - Odločitev o ustrezni ravni varovanja podatkov v državi
  - Uporaba zaščitnih ukrepov (standardne klavzule EK, zavezujoča poslovna pravila, certificiranje…)
  - Izjeme (privolitev, pogodba, prenos v javnem interesu… Zelo omejeno)

Po sodbi Schrems II

Smernice EDPB o dopolnilnih ukrepih

- KORAK 1: preglejte prenose

- KORAK 2: poiščite pravo podlago za prenos

- KORAK 3: preverite, ali ta podlaga v konkretnih okoliščinah dejansko pomeni ustrezno varstvo

- KORAK 4: sprejmite dopolnilne ukrepe (tehnične: kriptiranje, psevdonimizacija ipd., pogodbene, organizacijske)

- KORAK 5: uveljavite procesne spremembe (spremembe pogodb?)

- KORAK 6: ocenjujte stanje v rednih intervalih

Kaj je novega v ZVOP-2

Pri obdelavi v oblaku ne spreglejte:

- dnevniki sledljivosti

- varovanje nekaterih ključnih zbirk občutljivih podatkov (omejitve lokalizacije, hrambe izven RS)

- pravne podlage in omejitve (specialne določbe)

- pravice posameznikov in njihovo uresničevanje (do izbrisa, prenosljivosti, seznanitve, itd.)

- globe

Integrirane oblačne storitve in platforme

Integrated cloud services and platforms

Robert Korošec

Oracle Slovenija

POVZETEK

V prispevku je predstavljena "Oracle Cloud Infrastructure (OCI)", ki je oblačna platforma podjetja Oracle. Ponuja infrastrukturne storitve, upravljane platformne storitve in poslovne aplikacije v oblaku. Posebna pozornost je posvečena poslovnim uporabnikom, kjer se morajo aplikacije izvajati v visoko razpoložljivem in zelo zmogljivem okolju.

OCI je na voljo v več oblikah, primarno kot javni oblak, lahko pa se uporabi kot hibriden oblak za komercialni ali vladni sektor.

SUMMARY

The paper presents "Oracle Cloud Infrastructure (OCI)", which is the cloud platform of Oracle. It offers infrastructure services, managed platform services and business applications in the cloud. Special attention is paid to business users, where applications must run in a highly available and high-performance environment.

OCI is available in several forms, primarily as a public cloud, but can be used as a hybrid cloud for the commercial or government sector.

O AVTORJU

Robert Korošec je od leta 1999 zaposlen v podjetju Oracle Software, kjer je delal kot svetovalec za Oracle baze podatkov in Oracle Exadata sisteme. V zadnjem letih deluje na področju Oracle Cloud platforme, primarno na uporabi oblačnih baz podatkov, prediktivne analitike in analize velepodatkov (BigData).

ABOUT THE AUTHOR

Robert Korošec has been employed at Oracle Software since 1999, where he worked as a consultant for Oracle databases and Oracle Exadata systems. In recent years, he has been working in the field of the Oracle Cloud platform, primarily on the use of cloud databases, predictive analytics and BigData data analysis.

ORACLE

Oracle Cloud Infrastructure

A secure, high-performance platform for all your workloads

Robert Korošec
Oracle

Complete cloud services

24 PUBLIC AND GOVERNMENT REGIONS / EXADATA CLOUD AT CUSTOMER / AZURE

2

Deploy in our public, government, or sovereign regions

AMSTERDAM
LONDON • STOCKHOLM
NEWPORT • FRANKFURT
PARIS • ZURICH
TORONTO
CHICAGO • MONTREAL
ASHBURN
MADRID • SERBIA
MILAN
SAN JOSE
PHOENIX
MOROCCO • MARSEILLE
MEXICO 2
QUERÉTARO
ISRAEL 2
JERUSALEM
SAUDI 3
JEDDAH • DUBAI
RIYADH
ABU DHABI
MUMBAI
HYDERABAD
CHUNCHEON
SEOUL • TOKYO
OSAKA
COLOMBIA
VINHEDO
SÃO PAULO
SINGAPORE
SANTIAGO
CHILE 2
JOHANNESBURG
SYDNEY
MELBOURNE

- ■ 35 Commercial
- ○ 7 Commercial Planned
- ☐ 2 Sovereign Planned
- ■ 7 Government
- ■ 12 Microsoft Azure Interconnect

100% renewable energy by 2025

$16B+
Cloud Applications
Cloud Infrastructure
run rate

57%
cloud infrastructure
consumption growth

42
cloud regions

$8.2B
CapEx in the
last 12 months

3   Copyright © 2023, Oracle and/or its affiliates

Oracle Cloud + Microsoft Azure Interconnect
Multicloud solution

ORACLE + ■ Microsoft

Customer Premises Equipment | Customer Data Center

FastConnect/VPN | ExpressRoute/VPN

ORACLE Cloud Infrastructure

■ Microsoft Azure

VCN | vNet

Autonomous DB / Exadata | Enterprise Applications | FastConnect | ExpressRoute | Microsoft Applications | Azure Services

ORACLE CLOUD INFRASTRUCTURE (Ashburn) | MICROSOFT AZURE (US East region)

Copyright © 2021, Oracle and/or its affiliates.

✓ Microsoft Azure and Oracle Cloud are **interconnected today**, so you can migrate and run mission-critical enterprise workloads across clouds

✓ **FastConnect and ExpressRoute** direct connection with 2 millisecond latency and no intermediate service provider required

✓ **Unified identity and access** management via single sign-on with automated user provisioning to easily manage resources across clouds

✓ **Collaborative support** of workloads across clouds, for example, custom and Oracle Applications on Azure with Oracle Database cloud services – connect best-in-class services across clouds

✓ **Available Now:** Ashburn, San Jose, Vinhedo, Toronto, London, Frankfurt, Amsterdam, Tokyo

✓ **Coming Soon:** Government, Asia, Europe regions

Or deploy OCI cloud services exactly where you need them

Connectivity Partners

Equinix Multicloud

Megaport Multicloud

Colt Multicloud
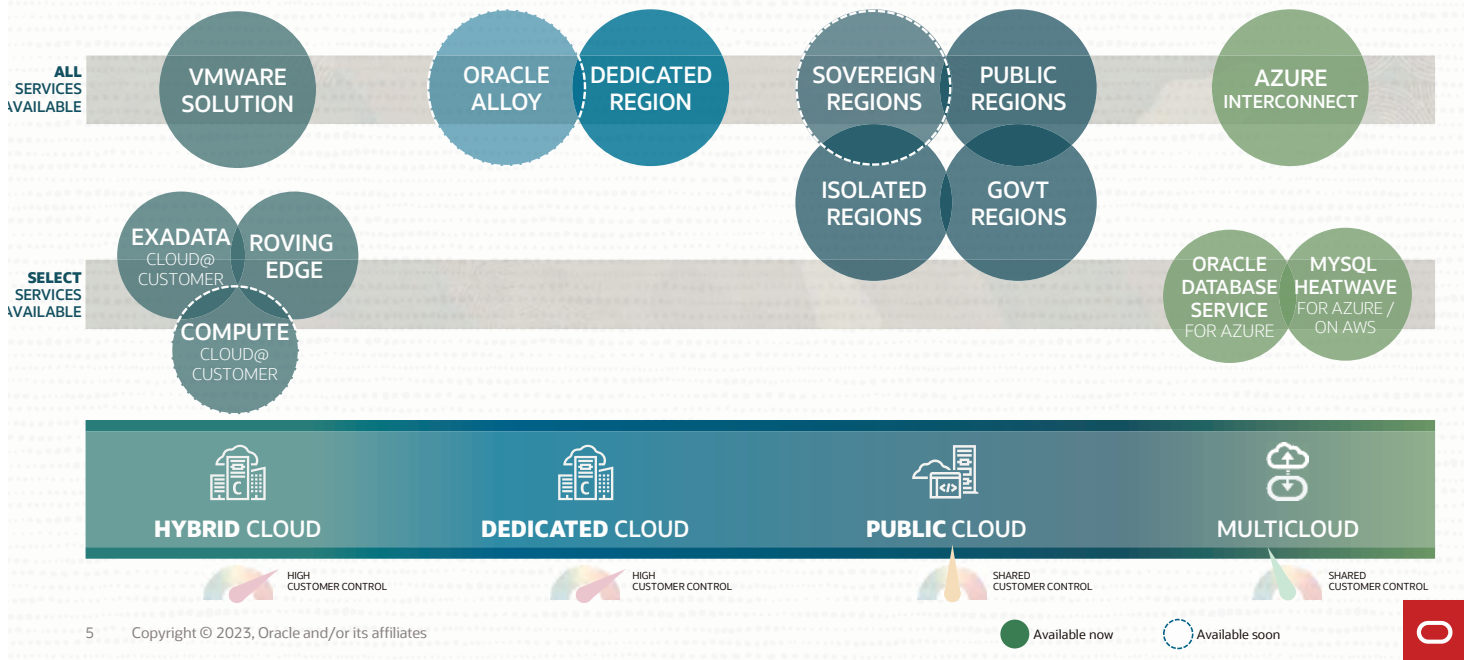
- In the diagrams, few of our largest connectivity partners are shown: Equinix, Megaport, and Colt
- Connections to other clouds from OCI is quick and easy to establish through our FastConnect partners.
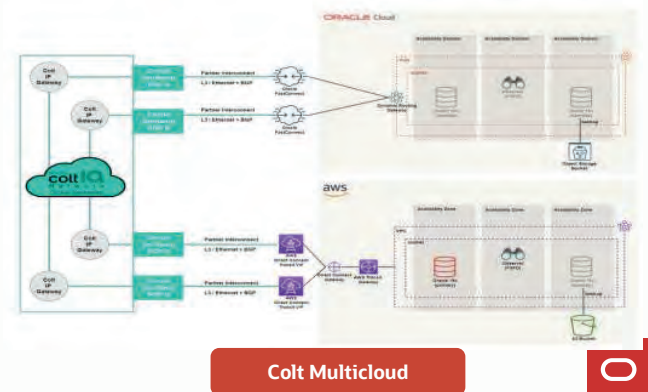
IaaS

Compute

Compute services for any enterprise use case

Bare Metal	VMs	Containers	Functions
• Instance isolation • Highest IOPS • High throughput • Low latency	• Flexible sizing • Security-hardened hypervisor • Burstable instances • Preemptible instances • Dense IO and dedicated host	• Managed Kubernetes • Bare metal option • Self-healing clusters	• Pay only for usage • Serverless • Container-native • Open source

AMD EPYC	Intel Xeon	Ampere (Arm)	NVIDIA GPUs

Local Attached Storage	Remote Attached Storage
NVMe SSDs Up to 51.2 TB Millions of IOPS	NVMe Block Volumes up to 1 PB 32 TB / volume 225 IOPS / GB

OCI Compute meets the demands of all workloads

Modern Distributed Application

AI/ML Training, DNA Sequencing, Crash simulation

AI/ML Inferencing, HPC, 3D Rendering

Enterprise Application Servers, Big Data

Enterprise Web & Application Servers

Development

Burstable

VM Standard E2.1.Micro — AMD — 1 — 1 GB — FREE

VM Standard A1.Flex — AMPERE — 1-80 — 1-512 GB — $0.01/hr /core

VM Standard E3.Flex — AMD — 1-64 — 1-1024 GB — $0.025/hr /core

VM Standard 3.Flex — intel — 1-32 — 1-512 GB — $0.054/hr /core

VM Standard E4.Flex — AMD — 1-64 — 1-1024 GB — $0.025/hr /core

BM Standard A1 — AMPERE — 160 — 1024 GB — $0.01hr /core

BM Standard 3 — intel — 64 — 1024 GB — $0.027/hr /core

BM Standard E4 — AMD — 128 — 2048 GB — $0.0125/hr /core

Flexible—choose your CPU cores and memory

Available to run on dedicated hosts

VM DenseIO E4.Flex — AMD — 8-32 — 128-512 GB — $0.0319/hr /core

VM Optimized 3.Flex — intel — 1-18 — 1-256 GB — $0.027/hr /core

VM GPU3 — intel NVIDIA V100 — 6-24 — 90-360 GB — $2.95+/hr

BM Optimized 3 — intel — 36 — 512 GB — 100 Gbps RDMA — $0.027/hr /core

BM GPU4 — AMD NVIDIA A100 — 64 — 2048 GB — 1.6 Tbps RDMA — Coming soon

BM DenseIO E4 — AMD — 128 — 2048 GB — $0.06375 /hr /core

Represents CPU cores (not threads or vCPUs)

Inter-node network with RDMA running on RoCE (< 1.5 µs latency)

Complete storage portfolio, with consistently fast performance

DATA LAKE, RICH MEDIA, LOGS, BACKUP, ARCHIVE

ENTERPRISE APPLICATIONS, DATABASES, GPU, CONTAINERS, APPLICATION LIFECYCLE

ANALYTICS, OLTP, HPC, CONTAINERS, KUBERNETES

€36/TB/mo.
25.000 IOPS, 480MB/s

Standard €21/TB/mo.
Archive €2.2/TB/mo.

Object & Archive Storage
Limitless capacity
Native & S3 APIs, HDFS,
encryption, storage lifecycle,
WORM, 10TB max object size

File Storage
Network NVMe SSD file storage
150 MB/s per TB
Scales to exabytes, NFS, NLM,
snapshots, encryption

Block Volumes
Network NVMe SSD block storage
Up to 32 TB volumes
Up to 1 PB/host
Up to 225 IOPs,
2,680 MB/s per volume
Snapshots, scheduled backups,
clones, grouped clones,
encryption, online performance &
capacity scaling
Performance SLA

X7 Bare metal Dense IO
51 TB
NVMe SSD
5M IOPS
Performance SLA

X9 Bare metal Dense IO
3.84 TB
NVMe SSD
100 Gbps RDMA

X7 VM Dense IO
6.4-25.6 TB
NVMe SSD
1.8M IOPS
Performance SLA

Free

Storage Gateway
NFS, at rest and inflight
encryption, configurable cache

Free

Data Transfer Service
HDD or 150TB appliance, encryption

Networking

High fidelity virtual networks and connectivity

Inbound Traffic is Free

Outbound Traffic is free < 10TB/mo. €7/TB for >10TB

Free

VCN	FastConnect	Load Balancing
Fully configurable subnets, routing, firewalls Default IPSec VPN 25Gb network infrastructure Public IP	Dedicated, SLA backed connectivity No data transfer charges 42 carriers worldwide	Choice of TCP, HTTP, HTTP/2 Flexible, autoscaling End-to-end SSL TLS encryption Network Load Balancer

First Free, 10Mb/s

Free

Service Gateways, VPNs	DNS	WAF
Private access without traversing internet Full range of IaaS/PaaS services covered	<30ms response time Global load balancing Traffic management Network health checks	Access Control Policies OWASP, XSS, Rate Limiting

Free

1.000.0000 req. €0.73

Oracle Linux, Windows, Ubuntu and RHEL on OCI

Shielded Instances
Defends against boot level attacks

- Hardened firmware security on bare metal hosts and Virtual Machines to defend against boot level attacks
- Supports Secure Boot, Measured Boot, and Trusted Platform Module (TPM)
- Aligns to Oracle Security Principles for
- Adding AMD E4 and Intel X9 shapes; and Windows Credential Guard

Workloads

- Secure Boot and TPM are available on Bare Metal and Virtual Machine instances across most workloads.
- Measured Boot is available on VM instances across most workloads

More Information

Introducing shielded instances for OCI Compute (oracle.com)
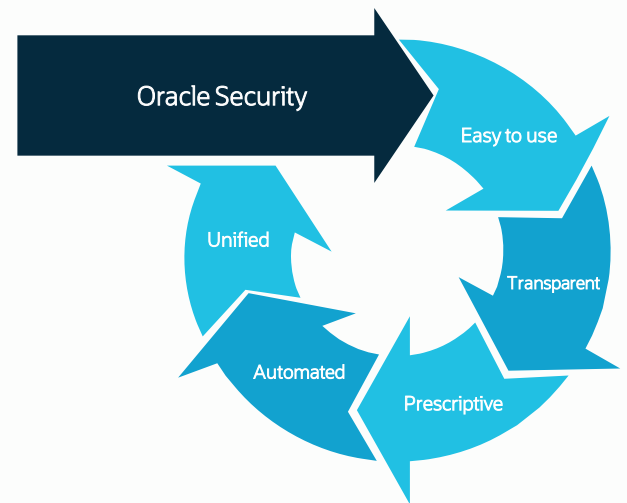
Confidential Computing
Advanced security to protect your data, included for free

- Protects data-in-use by encrypting it in memory with enhanced isolation using AMD Secure Encrypted Virtualization (SEV)
  - Data in memory isolated via encryption keys
  - No code change required for onboarding
  - Minimal performance impact across most workloads
  - Available at low or no cost to eliminate security tradeoffs

Workloads

- Enterprise workloads that process sensitive or confidential data requiring extra security protection for data-in-use.
- Workloads that leverage AMD shapes (E3 and E4)

"The new OCI E3 and E4-based confidential VMs, help to enable a higher assurance of data control as customers transition their workloads to the cloud while delivering the modern security features and impressive performance of AMD EPYC processors."

Lynn Comp
Corporate Vice President, Cloud Business Unit, AMD

Containers, Kubernetes, Functions

Where do I run workloads in OCI?

| run anything | | run containers | | run code |

OCI Compute	**OCI Container Engine for Kubernetes (OKE)**		**OCI Container Instances**	**OCI Functions**
	with Managed Nodes	**with Virtual Nodes**		
Best for:	**Best for:**	**Best for:**	**Best for:**	**Best for:**
• Requirement to control operating system	• Requirement to control operating system • Per-node pricing	• Fully managed infrastructure • Per-pod pricing	• Teams who don't know Kubernetes • Fully managed infrastructure	• Fully managed infrastructure • Short lived executions
Use cases	**Use cases:**	**Use cases:**	**Use cases:**	**Use cases**
• Non-containerized workloads • Windows workloads • Legacy applications • Per-server licenses	• Any containerized applications • Stateful workloads • GPU workloads	• Any containerized applications • Spiky workloads • Jobs, Batch • Stateful (roadmap) • GPU (roadmap)	• Any containerized applications • Ephemeral workloads (media/data processing, batch) • Dev/Test environments	• Event-driven code execution • Simple API implementation • Extend cloud services capabilities

Control, more operations ⟷ Agility, less operations

Pay for committed resources ⟷ Pay for usage

Where do I run workloads in OCI? - Containers

run containers

OCI Container Engine for Kubernetes (OKE)

with Managed Nodes   **with Virtual Nodes**

OCI Container Engine for Kubernetes (OKE)		OCI Container Instances
with Managed Nodes	**with Virtual Nodes**	

Best for: (Managed Nodes)
- Requirement to control operating system
- Per-node pricing

Use cases: (Managed Nodes)
- Any containerized applications
- Stateful workloads
- GPU workloads

Best for: (Virtual Nodes)
- Fully managed infrastructure
- Per-pod pricing

Use cases: (Virtual Nodes)
- Any containerized applications
- Spiky workloads
- Jobs, Batch
- Stateful (roadmap)
- GPU (roadmap)

OCI Container Instances

Best for:
- Teams who don't know Kubernetes
- Fully managed infrastructure

Use cases:
- Any containerized applications
- Ephemeral workloads (media/data processing, batch)
- Dev/Test environments

Control, more operations → Agility, less operations

Pay for committed resources → Pay for usage

17   Copyright © 2023, Oracle and/or its affiliates | Confidential: Internal/Restricted/Highly Restricted

---

OCI Container Instances

- **Flexible compute to run even demanding workloads**
  - Select preferred compute shape
  - Flexibility to allocate all CPU/memory provided by the underlying compute shape
  - 15 GB ephemeral storage included

- **Simple and fast launch**
  - Easy launch using Console, CLI, API, Terraform
  - One or more containers per instance
  - Pull images from OCIR or external registry
  - Optional configuration – graceful shutdown, restart policy, environment variables, startup options, resource throttling etc.

- **Security, networking and observability**
  - Strong isolation – no sharing of kernel, resources across instances
  - Secure communication through VCN with option to assign public IP
  - IAM access control using resource principal
  - Built-in metrics and logs

Container 1 | Container 2
App A
Container 1
App B
Container Instance | Container Instance
Hypervisor
Host

■ Oracle managed
□ Customer managed

18   Copyright © 2023, Oracle and/or its affiliates | Confidential: Internal/Restricted/Highly Restricted

OKE Virtual Nodes

Kubernetes Control Plane	Kubernetes Application & Services Pods, Services, Persistent Volumes, Secrets, RBAC, Quotas, HPA & VPA
etcd	Kubernetes Data Plane Upgrade Cordon/drain, software update
API Server	
Controller Manager	Compute Resources Scaling
Scheduler	Compute Resources Management OS patching, Compliance, Monitoring, Repair

🟧 Oracle managed
🟩 Customer managed

Virtual Nodes deliver a **serverless Kubernetes experience**

- Simplified Kubernetes operations

- Flexibility to support your application requirements

- Cost Optimization

PaaS - Databases

CUSTOMER MANAGED

Oracle Database on Compute
VM/Bare Metal
Data Guard
Auto TDE

Oracle Database Cloud Service
VM/Bare Metal
RAC
Data Guard
Auto TDE
Automated backup, patching

MySQL Service
100% built and managed by MySQL team
Optimized for OCI
HeatWave: unique integrated high perf analytics engine
1/3 the cost of Amazon RDS

MANAGED

Oracle Exadata
Extreme performance
Base – Full rack
RAC
ADG
IORM
Cloud Service/
Cloud@Customer

ORACLE NoSQL Database

NoSQL Service
JSON documents, columnar, or key-value data model
Instant scaling
Transaction consistency
Lower cost than AWS DynamoDB

AUTONOMOUS

Autonomous Database
Auto-scaling, Auto-tuning, Auto-patching

ADW
Serverless or dedicated
Spatial, graph, ML
SQL Developer

ATP
Serverless or dedicated
APEX

JSON
Serverless
Simple document APIs
ACID transactions

Database

The most comprehensive, resilient, high performing database services

CONTROL   AUTOMATION

Oracle Autonomous Database
Under the hood – A converged database

- **Multitenant** for Efficient, Agile Database Clouds
- **AutoML** for simple integrated Machine Learning
- **In-Memory** for Database Acceleration
- **Native JSON** for Document Data
- **In-Memory Ingest** for Fastest IoT
- **Cloud SQL** for integrating Object Store Data Lake
- **Persistent Memory Store** for Lowest Latency
- **Spatial and Graph** for Mapping and Social Networks
- **Licence**
  - Subscription (Licence Included), €1,25 €/OCPU/hour => 930/month
  - BYOL, €0,3 /OCPU/hour => 223€/month
    - DB EE -> 2 OCPUs (<16 OCPUs; RAC otherwise)
      ◦ DB EE -> Active DataGuard BYOL for Autonomous Dataguard
    - DB SE2 -> 4 OCPUs (max 8 OCPUs, i.e 2 DB SE2 CPU licences)

Multitenant

Machine Learning

In-Memory Analytics

JSON

Persistent Memory

In-Memory IoT

Spatial& Graph

Cloud Integration
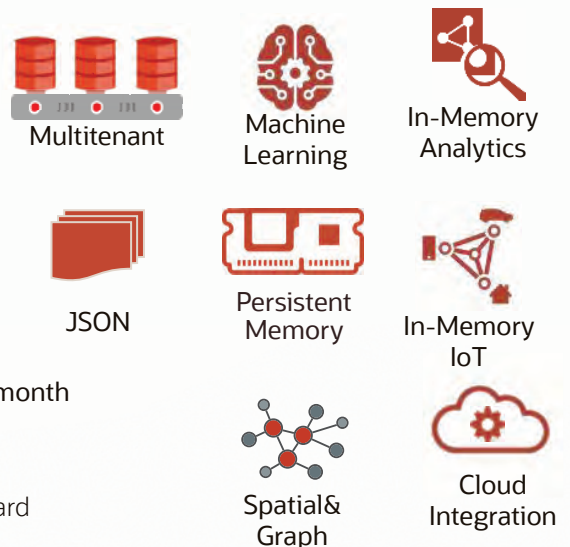
MySQL is the #1 Open Source Database

Jan 2023	Rank Dec 2022	Jan 2022	DBMS	Database Model	Jan 2023
1.	1.	1.	Oracle ✚	Relational, Multi-model 🛈	1245.17
2.	2.	2.	MySQL ✚	Relational, Multi-model 🛈	1211.96
3.	3.	3.	Microsoft SQL Server ✚	Relational, Multi-model 🛈	919.39
4.	4.	4.	PostgreSQL ✚	Relational, Multi-model 🛈	614.85
5.	5.	5.	MongoDB ✚	Document, Multi-model 🛈	455.18

DB-ENGINES

MySQL HeatWave

The *only* MySQL service with a native massively-scalable query accelerator
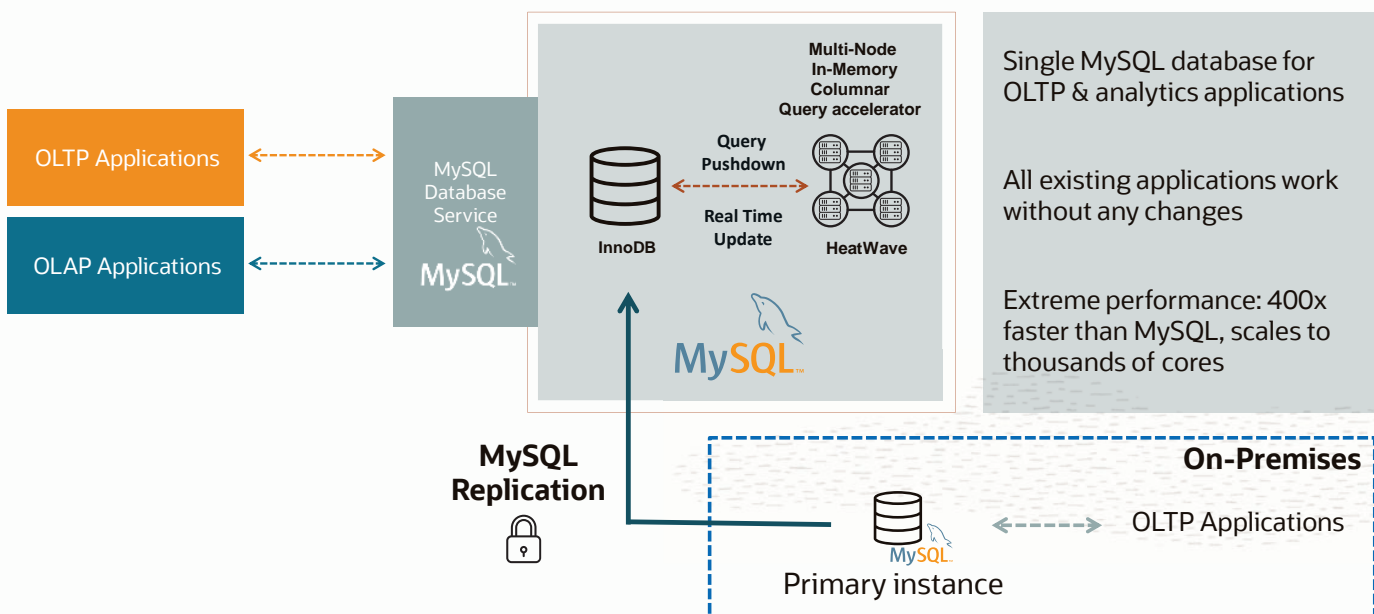
OLTP Applications

OLAP Applications

MySQL Database Service

Multi-Node In-Memory Columnar Query accelerator

Query Pushdown

Real Time Update

InnoDB   HeatWave

Single MySQL database for OLTP & analytics applications

All existing applications work without any changes

Extreme performance: 400x faster than MySQL, scales to thousands of cores

MySQL Replication

On-Premises

OLTP Applications

Primary instance

PaaS – BigData & AI

Data Lakehouses on OCI

Open & flexible: analyze any database, any application, from anywhere

Data Lakehouse on OCI

Data sources

Any Database

Any Application

Any Cloud

Any Events/Sensors

Managed Open Source

Big Data Service (Cloudera or ODH)
OCI Data Flow (Apache Spark)
OCI Streaming (Kafka)
OCI Search (OpenSearch)

Data Movement

Data Integration
GoldenGate

Data Stores

Object Storage
Relational Data

AI services for automation, prep, and prediction

Data Warehouse

Autonomous Data
Warehouse
MySQL HeatWave

Data Definition & Discovery

Data Catalog

Data target

Any BI Tool

Machine Learning
& Data Science

Any Application

Development

Modern application development on OCI

	Containers, Serverless and Functions	API Management, Streaming, and Messaging Services	Artificial Intelligence (AI) and Data Services	Monitoring and Observability
Dev Productivity	Native DevOps Experience + Freedom of Choice with Integrated Ecosystem			
Operations Reliability	Open Frameworks, 100% Upstream Compatible			
	Autonomous Operations			
	Shared Data Services			
	Flexible Infrastructure, Storage & Networking: any size, any workload, anywhere			
	IAM, Security & Governance across the SDLC			
	From always-free developer tier to hyperscale – on a single platform			

Containers, Serverless, and Functions-based Development

Broad set of OCI services

Container Engine for Kubernetes (OKE)
Managed Kubernetes service to simply and securely deploy and operate applications at scale

Serverless Kubernetes with Virtual Nodes capability for OKE
Eliminate the operational burden and learning curve around managing K8s clusters' infra. to accelerate cloud-native adoption.

Container Instances
Instantly run containers without managing any servers

Functions
Create, run and scale serverless event-driven apps

Container Registry
Container images and Helm repository with OOTB security scanning

Service Mesh
Secure, observe, and connect your microservices with no app code changes

Observability & Management
OOTB APM, logging, monitoring, ML-driven insights enable end-to-end visibility and management

Modern App Frameworks
Micronaut, Helidon, Springboot, GraalVM, more enable you to modernize Java apps and build new services

---

API Management, Streaming, and Messaging Services

Broad set of OCI services

API Gateway
Managed, HA API frontend for securely exposing, managing and connecting to API services

API Developer Portal
Coming soon! Discover, monitor, and share APIs with internal teams or the broad developer ecosystem

API Design
Design and develop APIs with fast prototyping and validation, based on OpenAPI

Serverless APIs
Functions triggered on-demand, eliminating infrastructure operations

API Security and Governance
Ensure authorization, routing, mTLS, rate limit, monitoring, and quota policies

Streaming & Queueing
Real-time, serverless, Kafka-compatible event streaming and REST/STOMP-based queueing for asynchronous, autoscaling, secure messaging

Workflow   COMING SOON
Simplify the design and execution of new apps, automation flows, and orchestration of microservices or OCI services - with a serverless, low-code visual workflow engine

Events & Notifications
Respond to CloudEvents-compatible resource changes. Trigger Email, SMS, functions, other webhooks notifications

Broad set of OCI services

Artificial Intelligence and Data Services

Managed AI services with pre-built models enable infusing your existing apps with AI – no experience necessary

Oracle Digital Assistant

Add chatbots to your website, mobile apps, and business applications

OCI Language

Sophisticated text analysis at scale—including sentiment analysis, key-phrase extraction, and classification

OCI Speech

Automatic speech recognition (ASR) and highly accurate transcription of audio/video files across languages

OCI Vision

Use computer vision to detect visual anomalies, automatically classify images, extract text from docs, and more

OCI Anomaly Detection

Anomaly detection models that flag critical incidents for sensor data processing, fraud detection, and more

OCI Forecasting

Time-series forecasts using ML and statistical algorithms—predict demand, budget, revenue, and resources

Machine Learning

Full lifecycle ML service (data prep, labeling, training, inference, visualization) and in-DB ML

Data Services & Blockchain

Autonomous Databases, OSS MySQL, OpenSearch, Data Lakes, Lakehouse services, Blockchain, and more

---

Broad set of OCI services   **Flexibility & Integrated Ecosystem**

Native DevOps Experience

Along with Freedom of Choice and an Integrated Ecosystem

CI/CD

Run declarative serverless CI/CD pipelines to easily automate your end-to-end delivery

Resource Manager

Automate infrastructure-as-code with **Terraform-**as-a-service

Secured Deployments

Easily deploy to private K8s clusters or VMs

Native Dev Environment

Git repos, CI/CD pipelines, Artifact Repo, Container Registry, Cloud IDE, Cloud Shell, and more

Integrated Ecosystem

Connect the tools you're already using: GitHub, GitLab, Jenkins, **Ansible**, Rancher, EFK, Spinnaker, more

Low Code Development

Visual Builder Studio, APEX, Blockchain Builder enable non-developers to extend & create new interfaces for your business apps

Reference Architectures

Cloud-Native opinionated templates and workflows get you started quickly with DevOps services

Modern App Frameworks

Micronaut, Helidon, Springboot, GraalVM, more enable you to modernize Java apps and build new services

Terraform   ANSIBLE
GitHub   GitLab
paloalto NETWORKS   TREND MICRO
FÜRTINET   PagerDuty
cybereason   TANIUM
JFrog   servicenow
RANCHER   DATADOG   Grafana
HELM   Spinnaker

Work how you like:

GUI, CLI, API, SDKs

Solution Design: Kubernets Application with Serverless AI
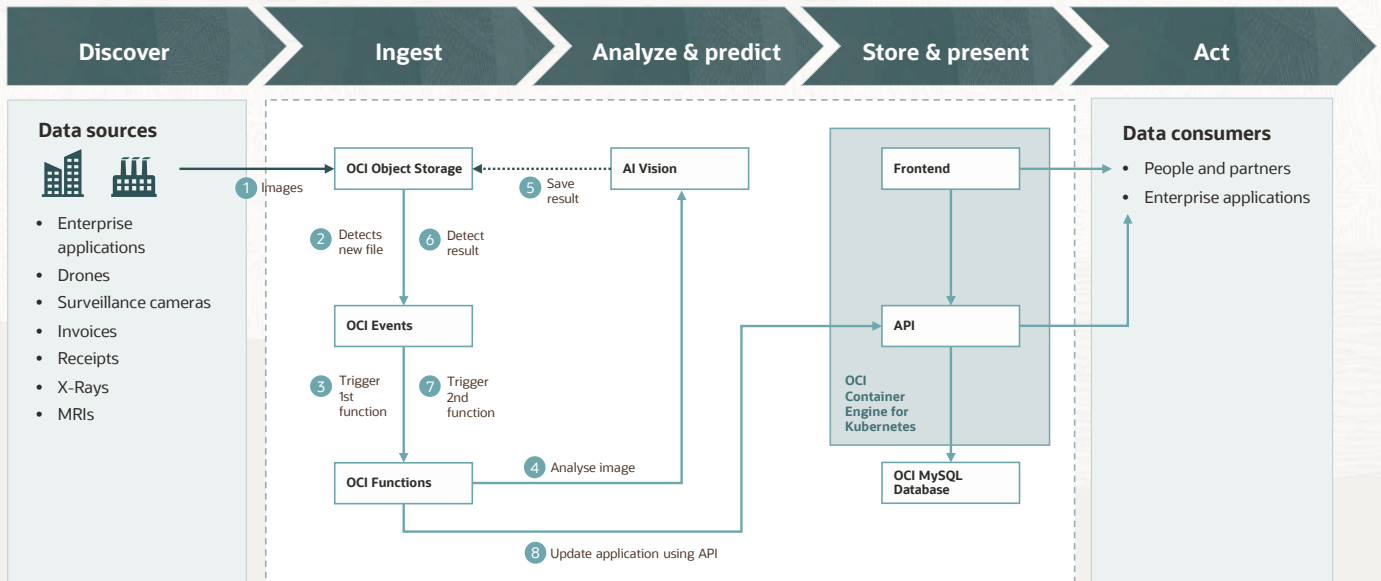
Oracle
Security,
Cloud Observability
and Management Platform

New cloud security services and enhancements

Compliance - EMEA

[Date]
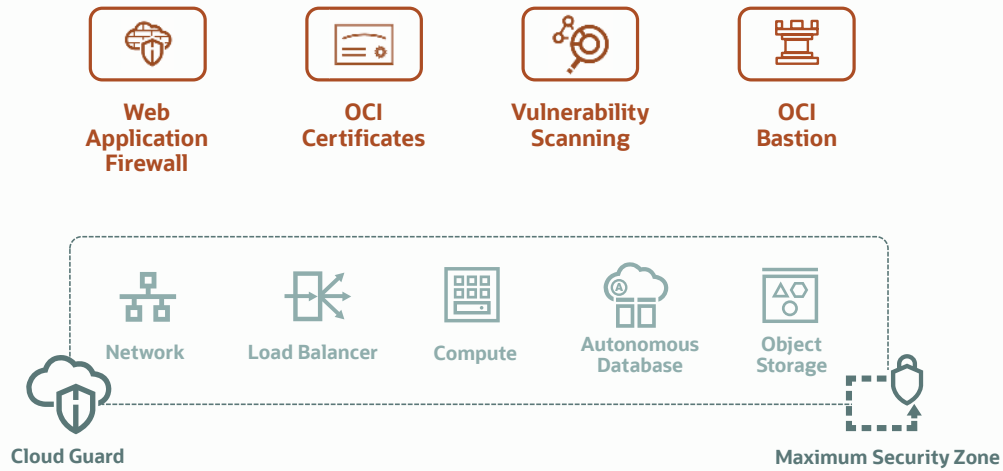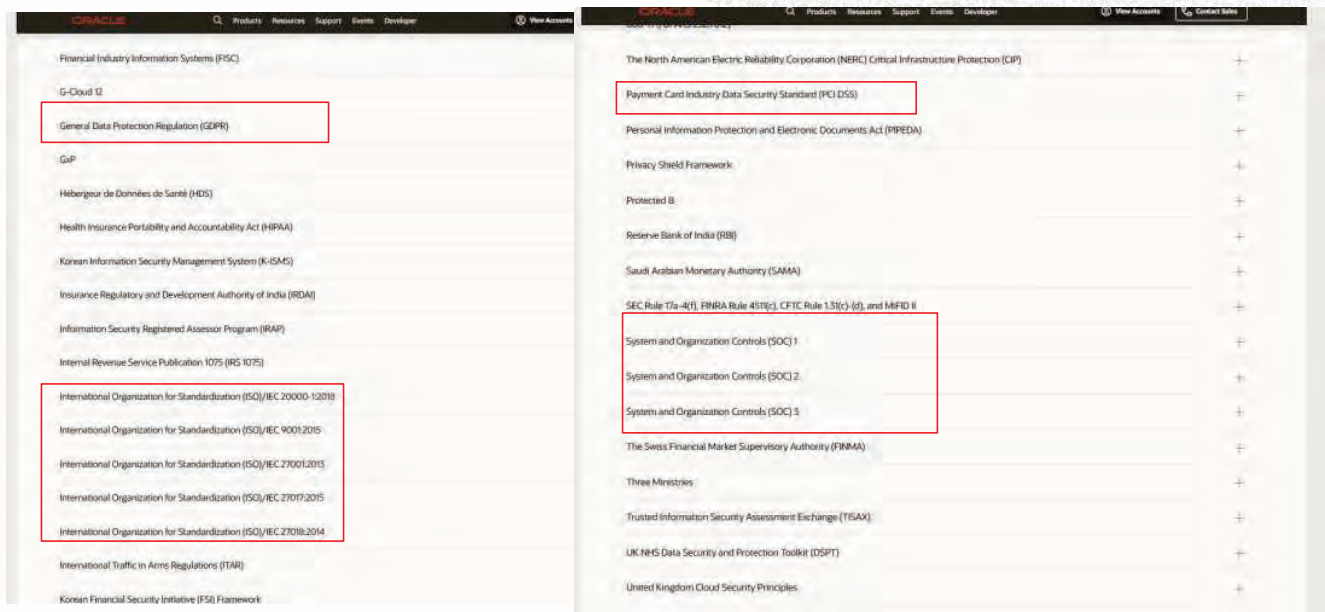
Observability Overview
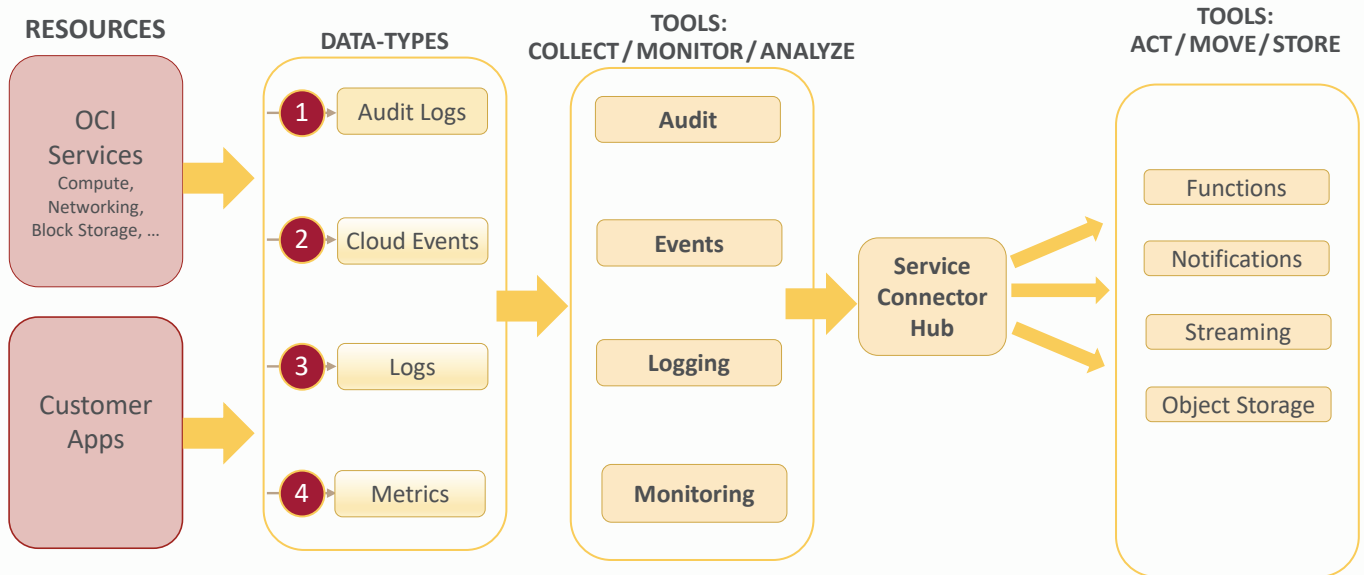
Application Performance Monitoring

Distributed tracing

- Full capture and analysis of all traces fine-grained problem diagnostics
- Compatible with OpenTracing and OpenTelemetry

Real User monitoring

- Measures end-user performance from browser to application
- Deep monitoring with in-context drill-downs from browser events across tiers

Synthetic monitoring

- Pre-defined monitors from global vantage points for proactive monitoring

Server monitoring

- Performance, availability and load analysis with rich set of server, and transaction metrics

Custom dashboards

- Create your own visualizations including data from other Observability & Monitoring Services

Oracle Logging Analytics: Overview

Proactive, repeatable, and automated problem detection and rapid troubleshooting

Smart analytics with Machine Learning
- Cluster and time series analysis & outlier detection
- Transaction sequencing, aggregation and rollup of potential issues
- Multi-dimensional data exploration

Intuitive data visualization and organization capabilities
- Analyze and visualize based on entity relationship
- In-context drill down for troubleshooting

Out-of-box knowledge contents
- Rich collection (250+) of parsers and knowledge enrichment for Oracle and non-Oracle stacks
- Error categorization

Dashboards for monitoring and reporting
- Create custom dashboard using user created widgets

Simple pricing
- Pay for what you store

39   Copyright © 2021, Oracle and/or its affiliates   5/31/2023
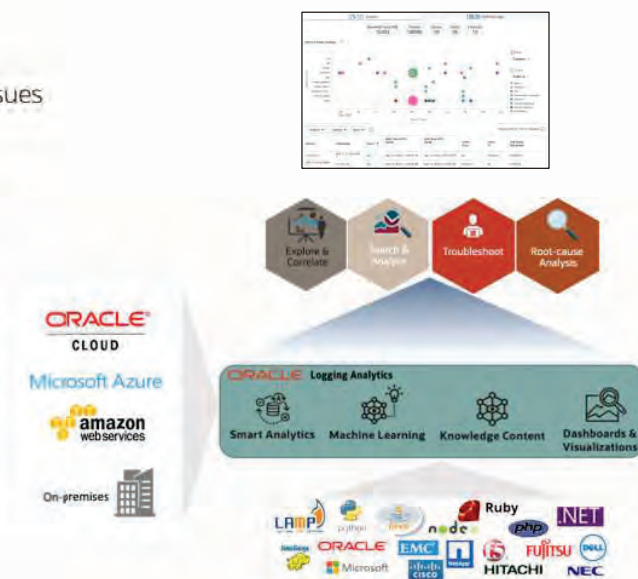
ORACLE

Pogled v prihodnost poslovnih aplikacij in kako to spreminjata OpenShift in DevSecOps

Look at the future of enterprise applications and how OpenShift and DevSecOps are changing it

Aljaž Oman

Smartis, informacijski sistemi, d. o. o.

POVZETEK

Prispevek se osredotoča na poslovne aplikacije ter njihovo delovanje v modernih hibridnih oblačnih okoljih. Posebej obravnavamo uporabo platforme OpenShift in pristopov DevSecOps pri razvoju in upravljanju aplikacij. Predstavljeno je, kaj so hibridna okolja in zakaj so pomembna za poslovne aplikacije. Osredotočamo se na platformo OpenShift in pojasnimo, kako lahko pomaga pri razvoju, upravljanju in skaliranju aplikacij ter kako se uporablja koncepte oblačno zasnovanih omrežij. V drugem delu je obravnavan DevSecOps pristop pri razvoju in upravljanju aplikacij, kaj je DevSecOps in zakaj je pomemben za poslovne aplikacije. V prispevku so predstavljena tudi orodja in prakse, ki jih uporabljamo pri DevSecOpsu, kot so CI/CD, avtomatizacija testiranja, nadzor nad konfiguracijo, orkestracija ter nadzor nad zmogljivostjo in delovanjem poslovnih aplikacij.

SUMMARY

The paper focuses on business applications and their operation in modern hybrid cloud environments. It specifically addresses the use of the OpenShift platform and DevSecOps approaches in application development and management. It introduces what hybrid environments are and why they are important for business applications. It focuses on the OpenShift platform and explains how it can help develop, manage, and scale applications, as well as how cloud-based networking concepts are used. The second part discusses the DevSecOps approach to application development and management, what DevSecOps is and why it is important for business applications. The paper also presents the tools and practices we use in DevSecOps, such as CI/CD, test automation, configuration control, orchestration, and performance and performance control of business applications.

O AVTORJU

Aljaž Oman je tehnični strokovnjak, ki se ukvarja s tehnologijami podatkovnih centrov že več kot desetletje. V zadnjih dveh letih pa se aktivno ukvarja z DevOps v podjetju Smartis. Študiral je na Fakulteti za elektrotehniko v Ljubljani, kjer je pridobil temeljna znanja, ki so mu omogočila vstop v svet informacijskih tehnologij. Med svojo karierno potjo je sodeloval v številnih projektih v Sloveniji kot tudi v tujini. Ima širok spekter znanja in izkušenj z upravljanjem različnih tehnologij, kot so VMware vSphere, NSX, vSAN, RedHat, OpenShift, Kuberebtes, CI/CD, ima pa tudi VCIX certifikacijo za VMware Datacenter.

ABOUT THE AUTHOR

Aljaž Oman is a technical expert who has been dealing with data center technologies for more than a decade. In the last two years, he has been actively involved in DevOps at Smartis. He studied at the Faculty of Electrical Engineering in Ljubljana, where he acquired basic knowledge that enabled him to enter the world of information technologies. During his career, he participated in many projects in Slovenia as well as abroad. He has a wide range of knowledge and experience in managing various technologies, such as VMware vSphere, NSX, vSAN, RedHat, OpenShift, Kubernetes, CI/CD, and also has VCIX certification for VMware Datacenter.

Pogled v prihodnost poslovnih aplikacij in kako to spreminjata OpenShift

Aljaž Oman, Smartis d.o.o.

Uvod v Red Hat OpenShift

- orkestracija kontejnerjev
- razvojno okolje
- upravljanje življenskega cikla aplikacij
- integracija in razširljivost
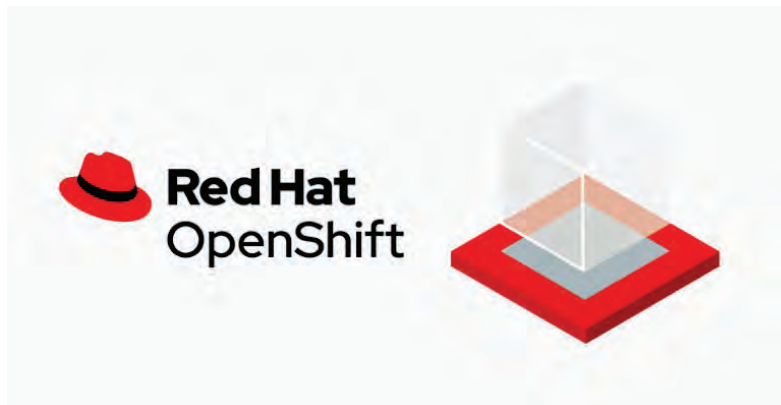
Arhitektura

- namespace, deployment, pod, service, route
- master, worker, infra nodes
- proxy, load balancer
- operatorji
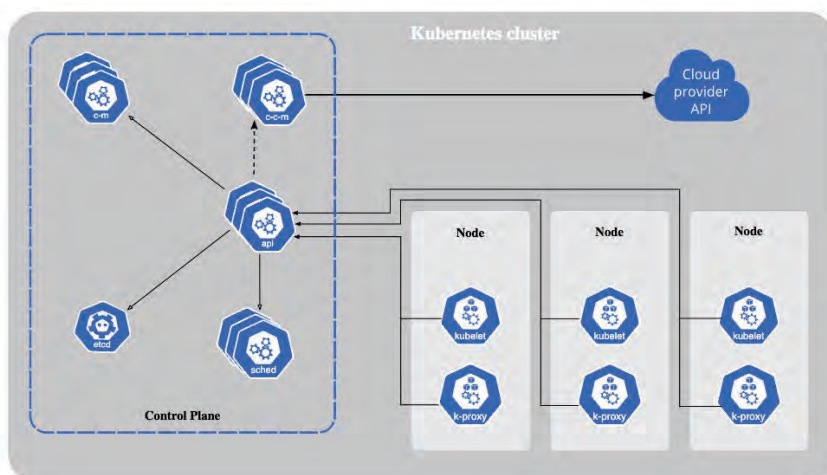
Kontejnerizacija

- izolacija
- skalabilnost in učinkovitost virov
- hiter razvojni cikel
- prenosljivost
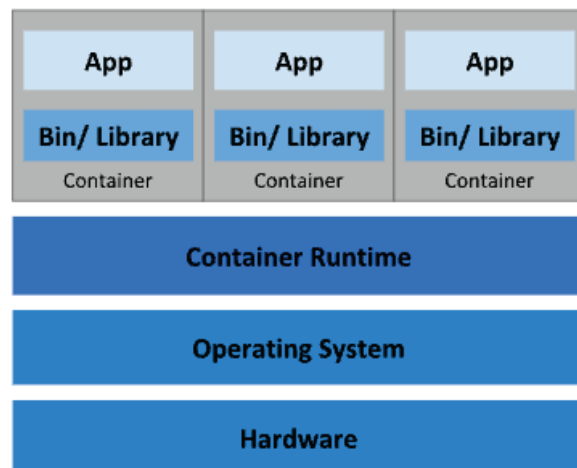
Prednosti

- enostavno upravljanje
- avtomatizacija in orkestracija
- skalabilnost
- varnost
- podpora

Primer iz prakse

- uporaba OpenShift
- arhitektura
- avtomatizacija
- kaj smo se naučili?

Vprašanja?

Vrednost hibridnega oblaka in mikrostoritev - hitra in učinkovita dostava storitev

The value of hybrid cloud and microservices: deliver services with speed and efficiency

Aleš Gros

IBM

POVZETEK

Današnji poslovni in tehnološki izzivi zahtevajo dinamičen odziv in sprejemanje. Stare, monolitne aplikacije zahtevajo čas in veliko dela za zagotavljanje novih funkcij in sprememb ter se ne morejo učinkovito odzvati na te dinamične zahteve. Za zagotavljanje učinkovitega in hitrega odziva so razvite mikrostoritve in hibridne rešitve v oblaku.

SUMMARY

Today's business and technology challenges requires dynamic response and adoptions. Old, monolithic based applications require time and a lot of work to deliver new functions and changes and are not able to efficiently response on those dynamic requirements. To provide efficient and fast response, microservices and Hybrid cloud-based solutions are developed.

O AVTORJU

Aleš Gros je v podjetju IBM vodja ekipe *Client Engineering*, ki je zadolžena za izvajanje t.i. projektov *Proof of Experienced* za področje Vzhodne Evrope. Aleš se je po študiju telekomunikacij pridružil podjetju Smart Com, kjer je svojo profesionalno pot začel na področju Lokalnih računalniških omrežij. Kmalu zatem se je v podjetju IBM podal v svet računalniških sistemov, kjer je prehodil pot od podpornega inženirja za velike računalniške sisteme do arhitekta IT sistemov. Pot je nadaljeval v podjetju EMC, kjer je delal kot tehnološki svetovalec za ključne stranke in tudi vodil lokalno pisarno. Leta 2011 se je ponovno pridružil podjetju IBM na delovnem mestu IT arhitekta za ključne stranke. Od takrat je delal na različnih mednarodnih in lokalnih delovnih mestih in projektih, kot so arhitekt na področju velikih računalniških sistemov, arhitekt zadolžen za razvoj globalnih sistemskih integratorjev, vodja arhitektov na področju Centralne in Vzhodne Evrope, vodja strokovnjakov za razvoj partnerjev na področju Vzhodne Evrope itd. V tem času je nabral veliko izkušenj na različnih področij in je tudi certificiran Open Group Distinguished Architect.

ABOUT THE AUTHOR

Aleš Gros is the head of the Client Engineering team at IBM, which oversees implementing the so-called Proof of Experienced projects for Eastern Europe. After studying telecommunications, Aleš joined the company Smart Com, where he began his professional career in the field of Local Computer Networks. Soon after, he ventured into the world of computer systems at IBM, where he worked his way up from a support engineer for large computer systems to an IT systems architect. He continued his career at EMC, where he worked as a technology consultant for key customers and managed the local office. In 2011, he re-joined IBM as an IT Architect for key customers. Since then, he has worked in various international and local positions and projects, such as architect in the field of large computer systems, architect in charge of the development of global system integrators, head of architects in the area of Central and Eastern Europe, head of specialists for partner development in the area of Eastern Europe, etc. During this time, he has accumulated a lot of experience in various fields and is also a certified Open Group Distinguished Architect.

The value of hybrid cloud and microservices: deliver services with speed and efficiency

—

Aleš Gros; IT Arhitekt ....
ales.gros@si.ibm.com
Tel: +386 40 456 880

Skladno s GDPS pravili za poslovne namene dovoljujem in se veselim uporabe mojih kontaktnih podatkov ☺

IBM

Our customers have declared three core imperatives

Resiliently
Respond To Change

1 - **IT will become decentralized, open, secure**

Flexibly
Optimize Productivity

2 - **Automation will fuel the future of work**

Intelligently
Operate & Engage

3 - **Winners will scale the value of data with AI**

2

The great digital shift

10 years of digitization
in under **one** year

34%
2020

16% 2019

% of business channels
replaced by digital

Consumer and
employee
expectations
demand reliable
digital
experiences

© 2021 IBM Corporation   Source: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/five-fifty-the-quickening

McKinsey
& Company

3

Leaders must modernize to achieve business transformation and agility

Accelerate innovation
and efficiency to unlock
immediate value
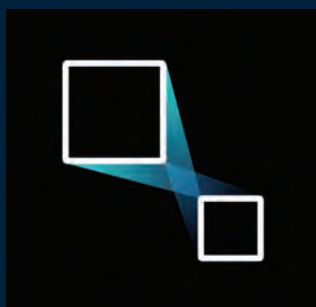
Integrate and extend
applications, data, and
services across your
environment

Manage and secure
applications and data
consistently and at
scale

IBM

Heterogenous

Data Explosion

IT Complexity

Digital Automation

Talent & Skills

Edge   Traditional On-premise(s)   Data Explosion   Multiple Public Clouds   SaaS

~25% workloads in '25   ~25% workloads in '25   ~50% workloads in '25

Skills and talent: teams are stretched, as they are fighting for workloads to their preferred stack.

Vertical Hybrid Cloud

| Application 1 | Data 1 | Application 2 | Data 2 | Application 3 | Data 3 | Application 4 | Data 4 |

Services 1   Services 2   Services 3   Services 4

Governance 1   Governance 2   Governance 3   Governance 4

Established Enterprise Stack   Cloud Stack 1 (Private)   Cloud Stack 2 (Public)   Cloud Stack 3 (Public)

Platform 1   Platform 2   Platform 3   Platform 4

Infrastructure 1   Infrastructure 2   Infrastructure 3   Infrastructure 4

Skills 1   Skills 2   Skills 3   Skills 4

Traditional   Private Cloud   Public Cloud

Speed: Time to market (Business), Time to production (ITDev), Time to change (ITOps).
Innovate: New business models (Business), New technology (ITDev), New platforms (ITOps).
Agility: Business resiliency (Business), DevOps pipelines (ITDev), GitOps automation (ITOps).
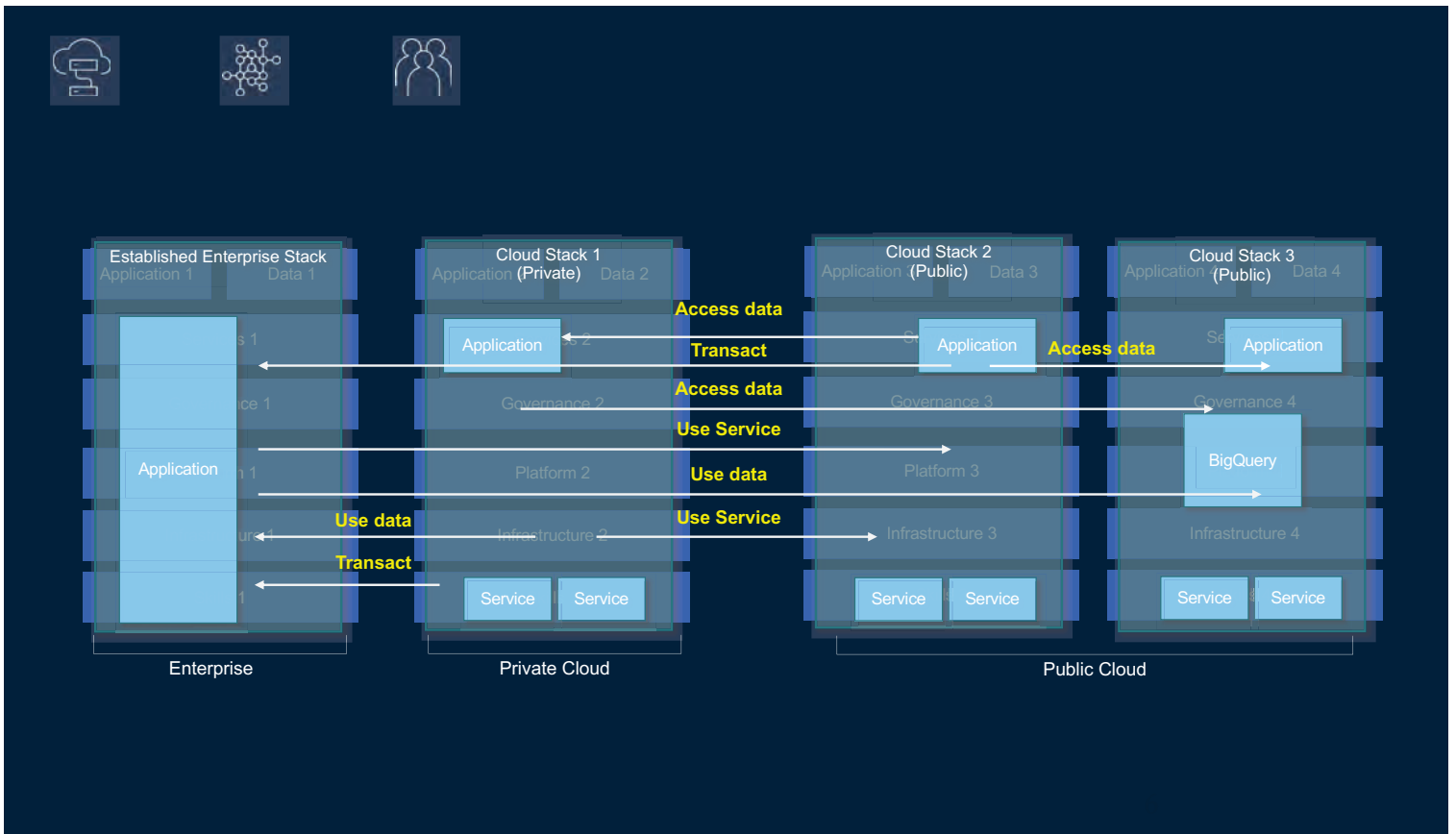
Monolith vs Microservices
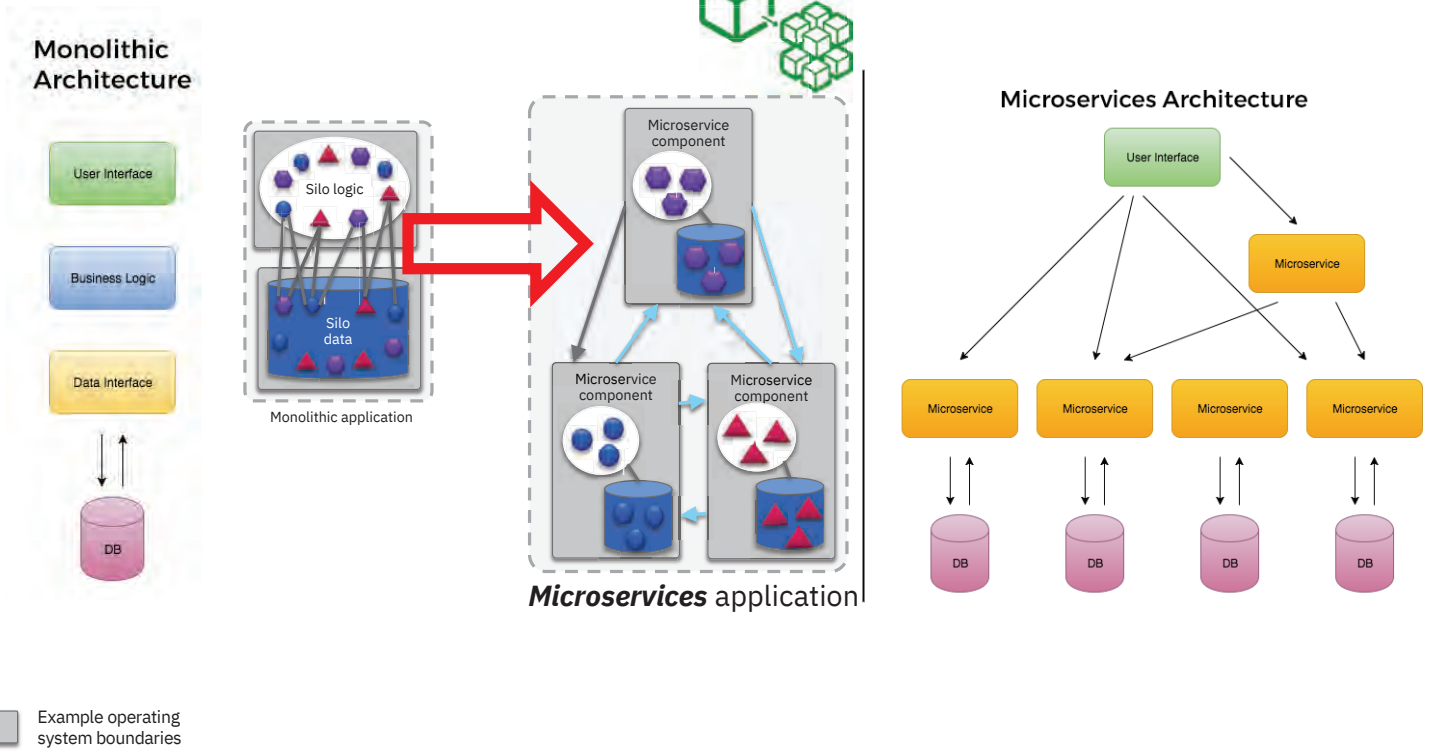
Containers vs Virtualization
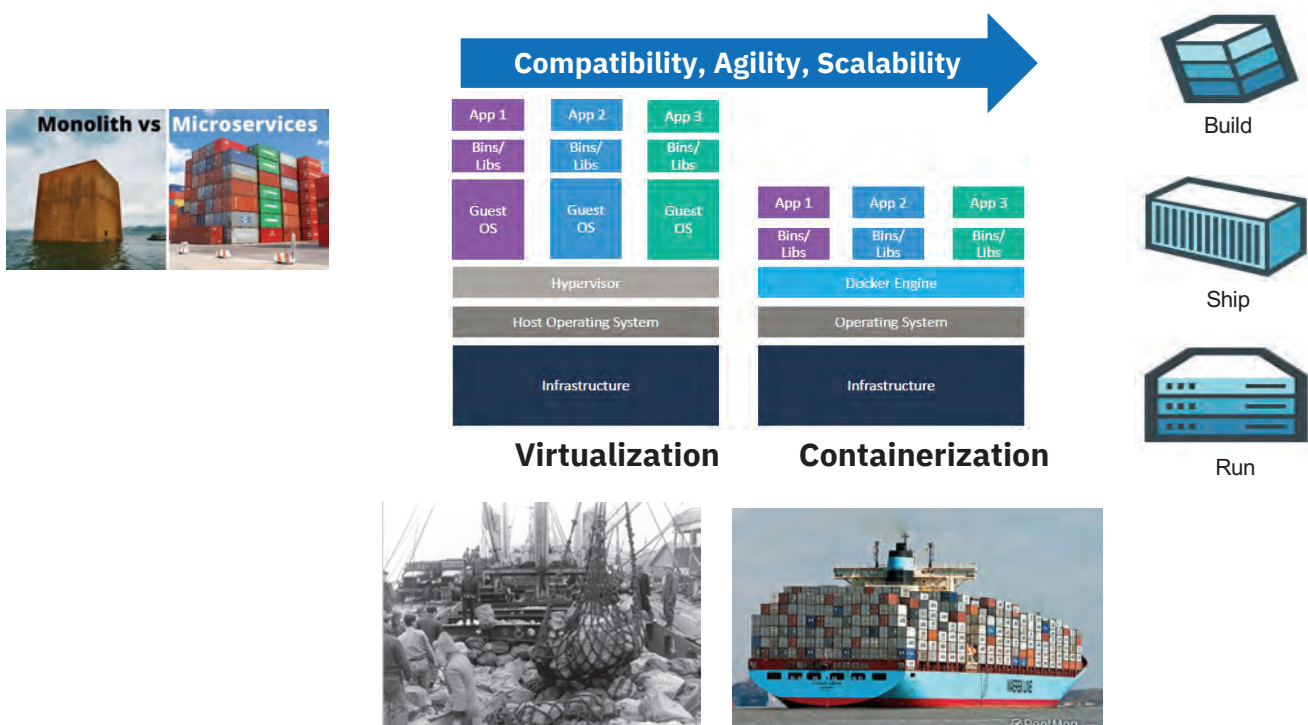
Microservices flexibility, independence, openness, knowledge …
… run where it is needed (appropriate)
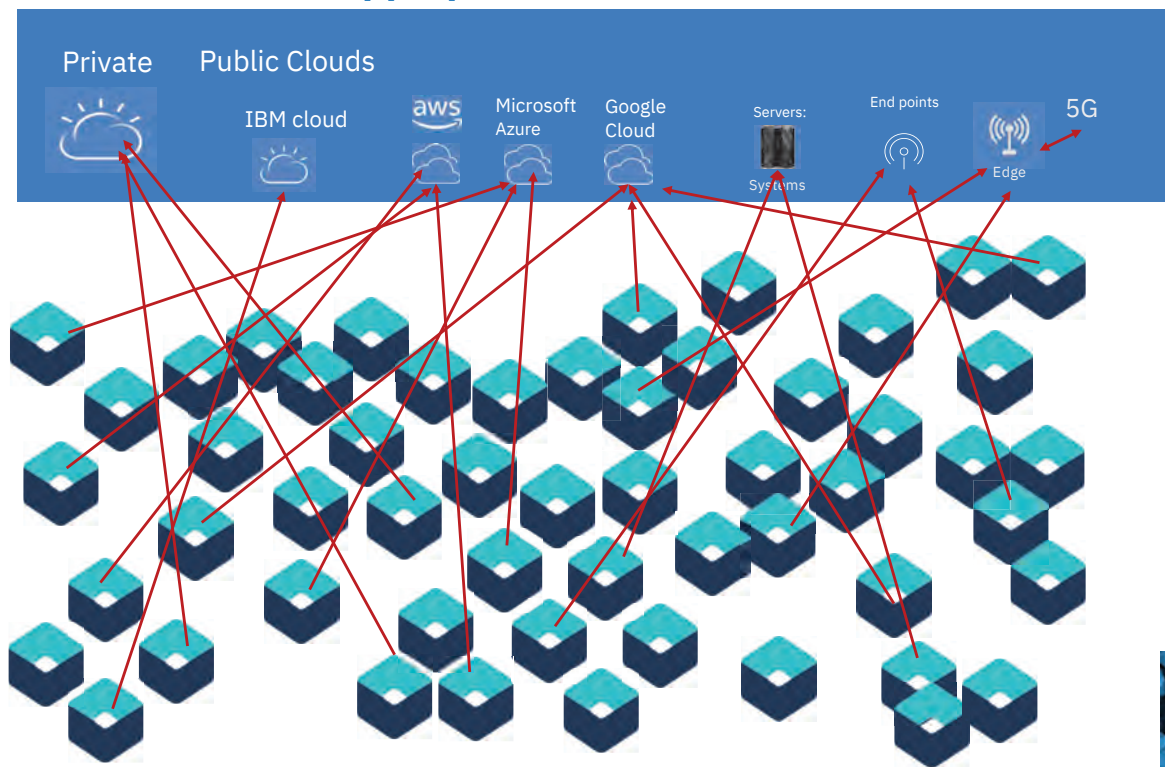
Any specific value of Microservices in Telecommunications?

....
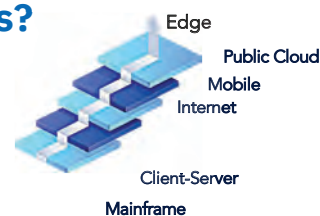
5G & Edge – next big step after/based on Cloud?
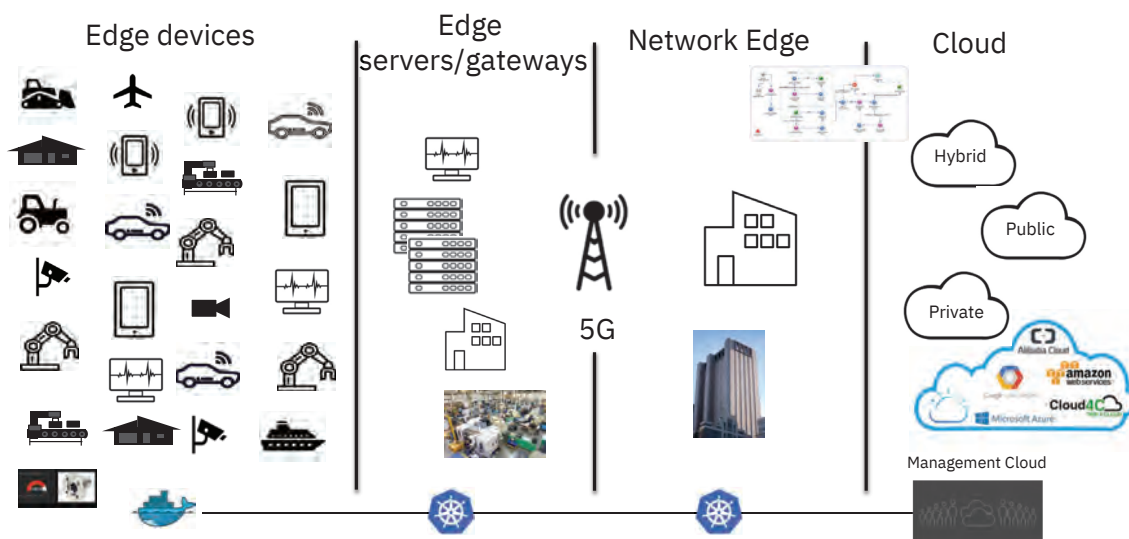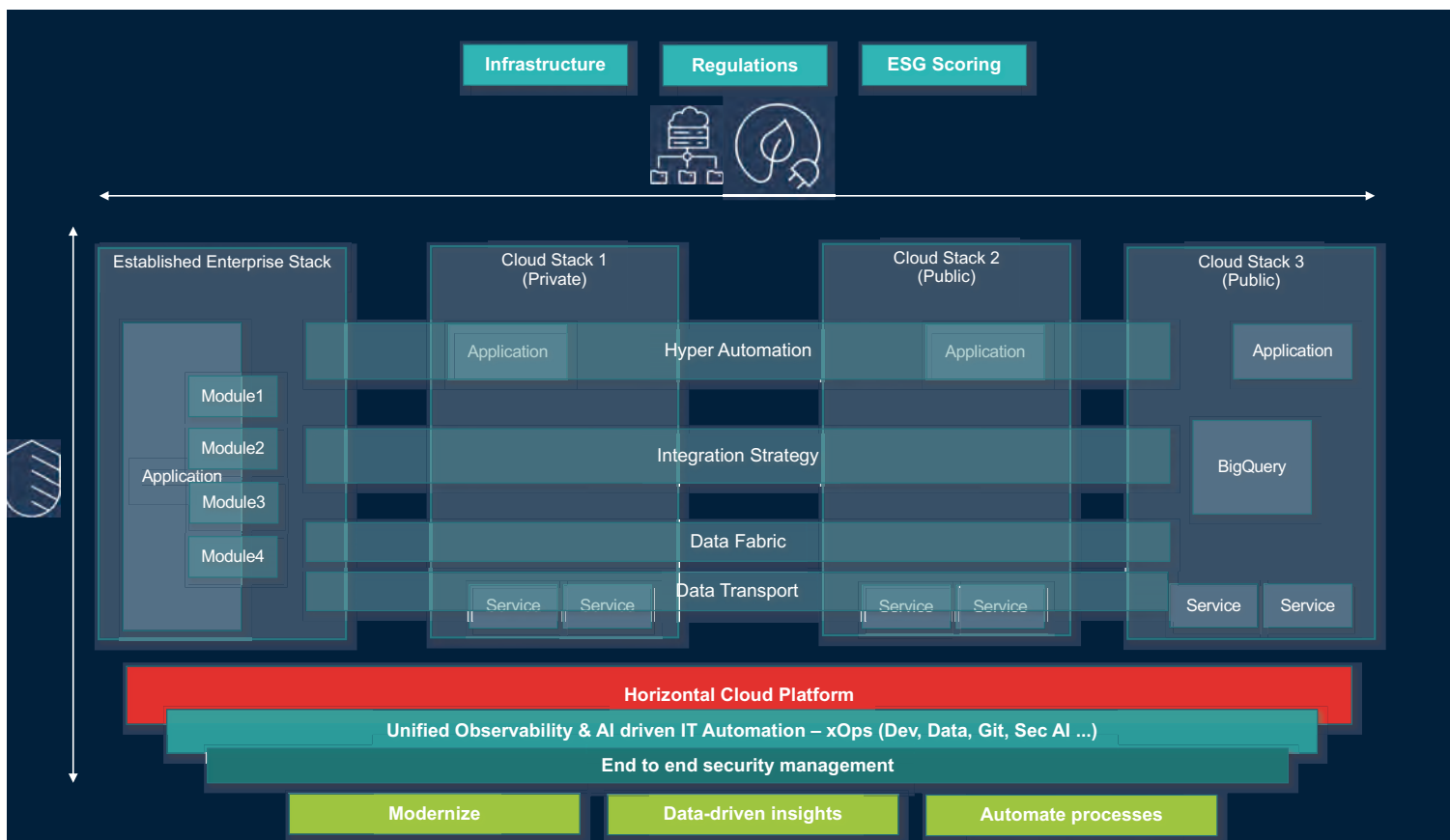
Agility, Speed and Innovation

A new era of business reinvention is dawning. Organisations are facing an unprecedented convergence of technological, social and regulatory forces. As **artificial intelligence (AI), automation, Internet of Things (IoT), blockchain and 5G become pervasive**, their combined impact will reshape standard business architectures. The 'outside-in' digital transformation of the past decade is giving way to the 'inside-out' potential of data exploited with these exponential technologies. We call this **next-generation business model the Cognitive Enterprise.**

Normalize and streamline
Speed (create-deploy-change)
Modular (Microservices, APIs, Events)
Containers (Speed, efficiency, automated)
Secure (build-in, regulated, marketplace)

Kako lahko omrežni operaterji izkoristijo storitve v oblaku za omogočanje nove storitvene arhitekture

How network operators can leverage Cloud services to enable new service architecture

Tamas Boday

Huawei Technologies

POVZETEK

Oblačno zasnovana infrastruktura je temelj za digitalno preobrazbo podjetja. Podjetja izkoriščajo digitalne zmogljivosti za hitro izboljšanje neprekinjenega poslovanja in odkrivanje priložnosti za večjo učinkovitost v spreminjajočih se okoliščinah. Inovacije in integracijske zmogljivosti celotnega sklada v oblaku pospešujejo posodobitev aplikacij. Gradnja oblaka je temelj za inteligenten svet z vseprisotnim oblakom in prodorno inteligenco. Model Huawei Cloud Pangu je pionir nove paradigme za razvoj umetne inteligence v industrijskem obsegu.

SUMMARY

The Cloud native infrastructure is the foundation for enterprise digital transformation. Enterprises leverage digital capabilities to rapidly improve business continuity and identify opportunities for increased efficiency under changing circumstances. Full stack cloud native innovation and integration capabilities accelerate application modernization. Building the cloud is a foundation for an intelligent world with ubiquitous cloud and pervasive intelligence. Huawei Cloud Pangu models - pioneering a new paradigm for industrial scale AI development.

na Univerzi v Obudi in Central European University v Budimpešti. Specializiran je za področje interneta stvari in digitalizacijo v industriji. Prepričan je, da je premostitev vrzeli med tehnologijo in poslovanjem Prepričan je, da je premostitev vrzeli med tehnologijo in poslovanjem ključni dejavnik uspeha za vse akterje v industriji.

ABOUT THE AUTHOR

Tamas Boday is the Director of Integrated Solutions at Huawei Technologies Hungary and the Adriatic region. Boday completed his studies in electrical engineering, majoring in telecommunications and holds a diploma in management in finance (corporate strategy) and an MBA (technology management and innovation). He is a visiting lecturer at the University of Obuda and the Central European University in Budapest. He specializes in the field of Internet of Things and digitization in industry. He believes that bridging the gap between technology and business is a key success factor for all players in the industry.

O AVTORJU

Tamas Boday je Direktor integriranih rešitev v podjetju Huawei Technologies Madžarska in regiji Adriatik. Boday je zaključil študij elektrotehnike, smer telekomunikacije in ima diplomo iz managementa v financah (področje korporacijske strategije) ter MBA (tehnološko upravljanje in inovacije). Je gostujoči predavatelj

Unleash Digital with Everything as a Service

Huawei Cloud Overview Presentation

HUAWEI
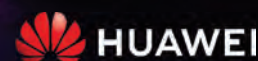
Using Digital to Cope with Uncertainties

Smart factory	Accurate weather forecast	Drug R&D	Remote office	Smart logistics
USD10 million reduction in costs	**4-hour forecast in 1 km² area**	Years → **Months**	5 million → **300 million**	**5x** efficiency
Smart production, with automatic analysis and adjustment of cement production line parameters	By leveraging 5G + AI, weather maps and radar data become more accurate.	AI-assisted drug design accelerates lead drug screening and discovery.	Remote collaboration and cloud office increase the number of teleworkers in China.	Unmanned warehouses and AI-powered logistics robots automate the process of storing goods.
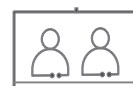
Enterprises leverage digital capabilities to rapidly improve business continuity and identify opportunities for increased efficiency under changing circumstances.

2   Huawei Confidential   **HUAWEI**

Make the Leap, Take the Lead
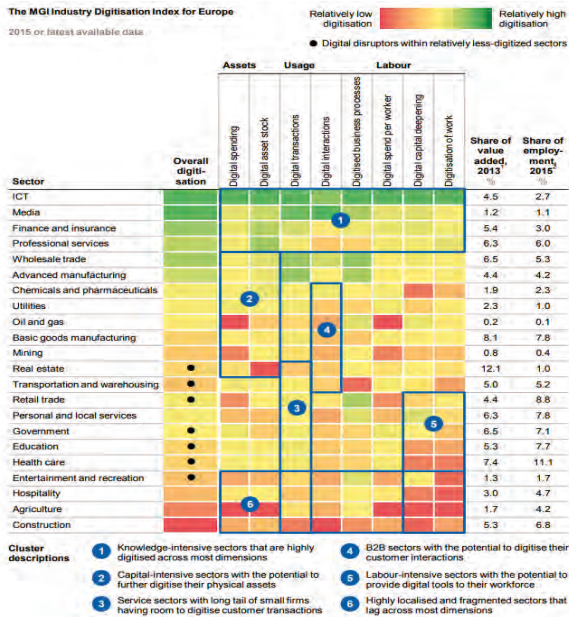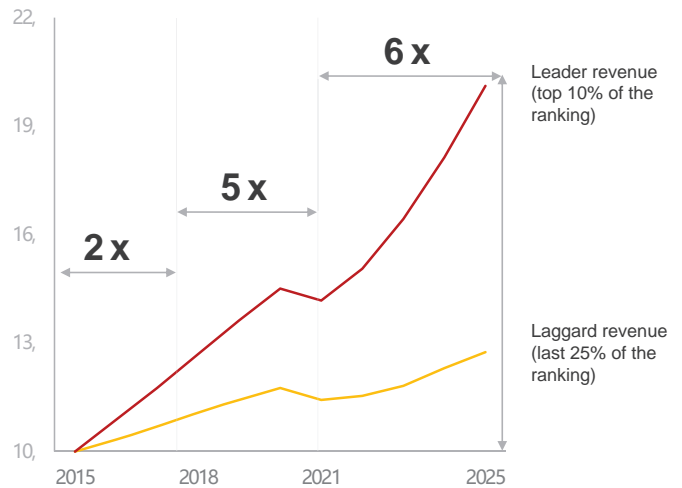
Source: Huawei MI, Accenture, McKinsey & Company

3   Huawei Confidential

To Embrace Digital, Application Modernization Is a Must

Application modernization has benefited thousands of enterprises

62 %
higher IT productivity thanks to modernized applications

88 %
CIOs see application modernization an effective method to significantly improve customer experience

Sources: IDC, Forrester

The capability of introducing and integrating new technologies becomes the bottleneck of enterprise digital transformation

3 years
needed to truly integrate new tech with business

VS

10+ types
of tech, including cloud computing, big data, social networking, mobility, next-generation security, AR/VR, IoT, AI, robotics, 3D, and blockchain

Source: Digital platform white paper by IDC

Modernized applications
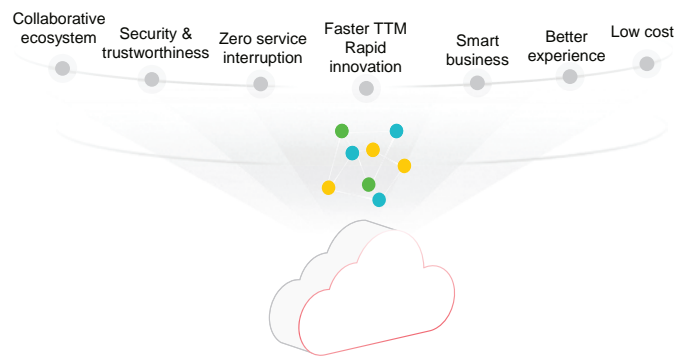
Collaborative ecosystem · Security & trustworthiness · Zero service interruption · Faster TTM Rapid innovation · Smart business · Better experience · Low cost

Full-stack cloud native innovation and integration capabilities accelerate application modernization

4   Huawei Confidential

Unleash Digital with Everything as a Service

Building the cloud foundation for an intelligent world with ubiquitous cloud and pervasive intelligence

5   Huawei Confidential

Infrastructure as a Service: Building One Global Infrastructure of Storage, Compute, and Network Resources

29 Regions

78 availability zones

2800 CDN nodes

CloudOcean — < 50 ms
Guizhou, Inner Mongolia, Anhui, Singapore, Ireland

CloudSea — < 10 ms
Beijing, Shanghai, Guangzhou, Hong Kong, Thailand, Indonesia, the UAE, South Africa, Brazil, Argentina, Mexico...

CloudLake — < 5 ms

Latency circle

6   Huawei Confidential

Cloud Native Infrastructure: The Foundation for Enterprise Digital Transformation

...   ...

Cloud native infrastructure

Ubiquitous Cloud Native Services (UCS)

Cloud Container Engine (CCE Turbo) Scheduling policies for hybrid deployment: resource utilization 100%↑	**Cloud Container Instance (CCI)** Scalability: 4000Pods/30s	Industry-leading serverless container service, free from infrastructure O&M

Cloud native compute Performance 20%↑ with the latest compute instance C7n	**Cloud native storage** Ultra-fast cloud disk, 2 million IOPS, and 100 µs latency	**Cloud native networking** Global traffic scheduling, hitless service reconstruction

QingTian architecture
Software-hardware synergy, full offloading of virtualization | Enclaves for zero host tampering
| Intelligent scheduling for optimal performance

- **No. 1** in China by **comprehensive strength of** cloud native **containers** in 2022
- **No. 1** in China by **container market share** in 2021/2022H1
- **The only** CNCF founding member **from Asia**
- Kata Containers **founding member +** Architecture Committee member

...

7   Huawei Confidential   **HUAWEI**

Technology as a Service for Faster Application Modernization

Traditional applications

Professional developers

Difficult to use and manage data

TTM in months

Monolithic applications

Runtime security

Single-node with MTTR in days

Service 1   Service 2   ...

Composable delivery

| Low-code development | API lifecycle management | Hybrid application integration | ... |

Data & AI

| Data governance | AI development | Digital content production | ... |

DevOps

| Software development | Desktop IDE | Observable O&M | ... |

Service-oriented architecture

| FunctionGraph | Cloud Service Engine (CSE) | Application Service Mesh (ASM) | ... |

Security & trustworthiness

| Software supply chain security | Cloud security brain | Host Security Service (HSS) | ... |

Resilience

| Multi-site high availability | Global load balancing | Pressure testing | ... |

Citizen + professional developers

Digital and intelligent decision making

TTM in just days

Microservice/Serverless

Full lifecycle security

Multi-active with MTTR in just minutes

Modernized applications

Transform cutting-edge technologies into cloud services to avoid reinventing the wheel

8   Huawei Confidential   **HUAWEI**

DataArts: Data Development and Governance with Data-AI Convergence

	Data development (IDE) **DataArts Studio**			Government

Data lifecycle

GaussDB

Data Migration	Data Storage	Data Conversion	Data Analysis, Prediction & Visualization	Data Sharing	Data Application & Enablement
CDM/CDL/DIS /DRS/ROMA FDI	LakeFormation /OBS	DataArts Studio	DWS/MRS/DLI/CSS/GES/ CloudTable/DLV/MLS/LTS	EI Gallery /TICS/EDS	RTD

IoT data   Messages   Files
...

Finance

Carrier

Enterprise

Internet

Data governance (catalog/quality/security/...)
DataArts Studio

16+ Years

Huawei's best practices in digital transformation

30+

Integration of disparate data source

10x +

Development efficiency improvement

Helps Xinyi Glass build an intelligent, data-driven control center

> **Intelligent dashboard**
> Decision-making support

> **Digital factory**
> 3D visualization

> **AI-driven innovation/optimization**
> Cold cutting

"Horizontal comparison & vertical optimization"

Tens of millions

RMB saved in gas costs annually

1 week → **1 hour**

preparation of monthly operational reports

IT & OT data convergence

Unified data collection

9   Huawei Confidential

HUAWEI

ModelArts: Efficient AI Development and Simplified AI Implementation

20,000+

Prefabricated models

40%+ ↑

Training efficiency

E2E AI platform

Continuous iteration

Industry UseCases

Visual quality inspection	Production scheduling	Sound detection	Workwear identification	Intelligent sales	...

General Suites

NLP suite	OCR suite	Vision suite	Speech suite	...

ModelArts (Lite | Edge | Standard)

Workflow   Constant collaborative iteration

Data labeling	Data processing	Model training	Model evaluation	Application generation	Application evaluation	Inference deployment	Service monitoring

Data preparation	**Development environment**	**Training**	TrainTurbo	**Inference**	InferTurbo

Resource Scheduling	DataTurbo

Compute frameworks	MindSpore	TensorFlow	PyTorch	Ray	DeepStream	MediaPipe	...

10   Huawei Confidential

Quickly build smart construction site SaaS services based on ModelArts

widya

- Develop once, deploy anywhere
- AI implementation efficiency improved by **30 times**, making construction sites safer

Sound suite helping protect Palawan rainforest

- Easy to use tutorials, easy to get started
- Model accuracy > 99%; recall rate > 95%

HUAWEI

Huawei Cloud Pangu Models: Pioneering a New Paradigm for Industrial Scale AI Development

Pangu models

Multimodal model

Scientific computing model

CV model (3 billion parameters)

NLP model (100 billion parameters)

Pre-trained models

Generalize Replicate

Scenario 1 ▸ Model 1
Pipeline

Scenario 2 ▸ Model 2
Pipeline

Scenario 3 ▸ Model 3
Pipeline

Pre-training → Fine-tuning and deployment

← Iteration ←

Large network
Hundreds of billions of parameters

Robust network architecture
10% higher overall performance

Good generalization capability
10x more scenarios covered

11 Huawei Confidential

Safe, efficient, intelligent coal mining with Pangu mining model, with no or only a small staff

Applied to **4,000+ mines in China, 18 mine operation APIs**, covering digging, extraction, transportation, communication, and more

Transportation
API for detecting foreign objects on conveyor belts
API for identifying belt deviation
......

Foreign object recognition precision
98%+

Faster inspection
10x to 100x
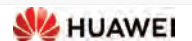
HUAWEI

CodeArts: More Agile App Development

| Microservices | Web apps | Mobile/Mini apps | Serverless apps | Embedded apps |

Security & trustworthiness

CI/CD CodeArts Pipeline

CodeArts Req → CodeArts IDE → CodeArts Repo → CodeArts Check → CodeArts Build → CodeArts TestPlan → CodeArts Artifact → CodeArts Deploy → O&M

CodeArts

30+ Years
Huawei R&D practice

1B+
lines of code

20+
mainstream programming languages and development frameworks
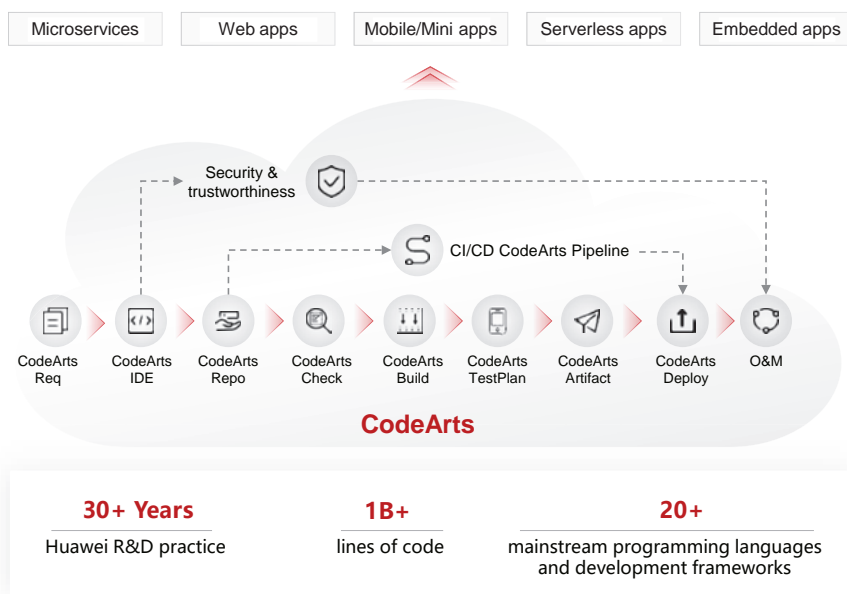
Deppon's Transformation

DEPPON EXPRESS

CodeArts Fully Covers:

| Code and data security | Quality control |
| Process standardization | Service automation |

750+
services developed via pipeline

80%
more test cases on average

71.74% ▾
fewer code defects

80+
Business systems migrated to the cloud

In Just 6 Months

12 Huawei Confidential

HUAWEI

MetaStudio: Faster Digital Content Production on the Cloud

| Socialization/Entertainment | E-commerce | Smart cities | Building design | Interior design | Education/Training | TV/Variety shows | Culture/Tourism | ... |

Joint solutions with ecosystem partners
Virtual human production | Virtual livestreaming | 3D space | Virtual-physical integration

Input
Optical cage scanning of multiple groups of images

Modeling
3D model generation

Simulation
Authenticity of the motion of materials such as hair and clothing

Control
Body and face control

Rendering
Virtual content presentation (Color, position, and brightness)

Compositing
Integration of virtual and real content

Output
Video of virtual-physical integration

Asset management

MetaStudio

Infrastructure (computing/storage/network, etc.)

Virtual ambassador for carriers

中國移動 China Mobile

JOY-E

JOY-E, China Mobile Hong Kong

- Embracing cutting-edge technologies and building a corporate image that is more appealing to Generation Z customers
- Providing intelligent customer services and serving as docent in the customer service center of AICC

13   Huawei Confidential

🏵 HUAWEI

Huawei Cloud Security: Safeguarding Services with Systematic Construction and Constant Operations

One center
Intelligent operation

10,000+ security baselines
600+ check items

Huawei Cloud CSIRT
30+ years of experience

300+ detection models
100+ automated playbooks

Real-time posture awareness

SecMaster

Threat detection & response

Log analysis engine

Response policy management
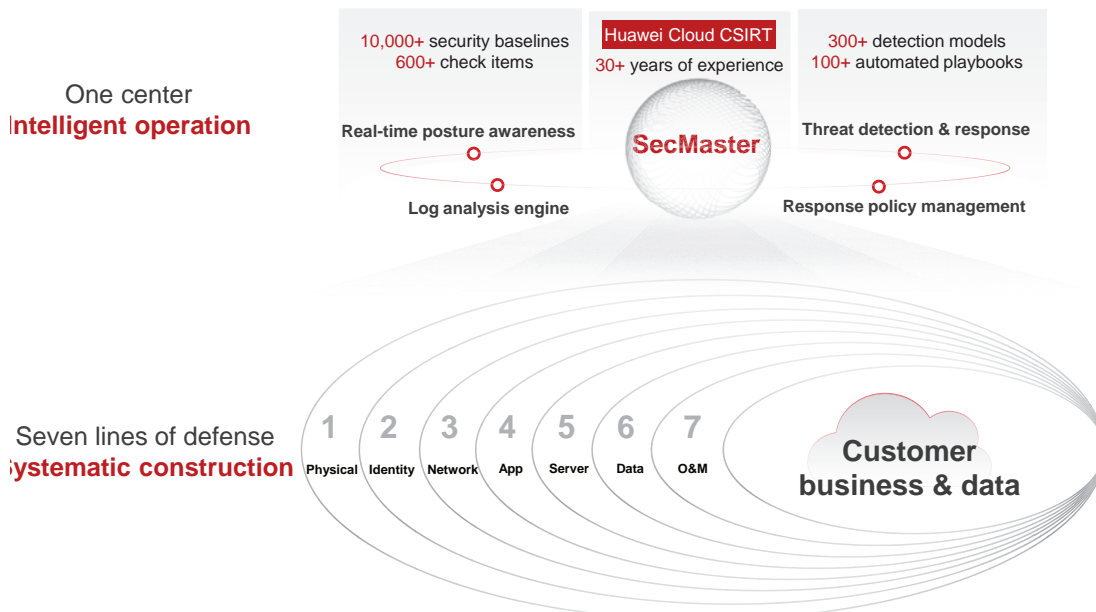
Intelligent security operation

- AI-assisted alarm handling, closing 99% alarms within 5 minutes
- MDR expert service with 10x⬆ operation efficiency

Cloud-native security services

- Services working together to dynamically respond to changes
- Border protection → Comprehensive defens

Seven lines of defense
Systematic construction

1 Physical 2 Identity 3 Network 4 App 5 Server 6 Data 7 O&M

Customer business & data

Unified security architecture

- Fragmented → Unified management, and distributed prevention & control
- Assembled solution → Service-oriented, dedicated security solution

14   Huawei Confidential

🏵 HUAWEI

Cloud Migration Path Planning: Helping Enterprises Move to the Cloud and Use the Cloud

Moving resources to the cloud

Reluctant

How to secure data
How to generate value

Cloud infrastructure planning

Blueprints | Cloud security | O&M | DR | Migration | More

Moving applications to the cloud

Disoriented

Which applications to migrate
How to smoothly migrate them

Cloud app planning

Migration path | Integration architecture | Technical architecture | O&M | More

Effective cloud usage

Inexperienced

How to use new tech
How to combine cloud with services

Tech on demand and digital transformation planning

AI | Big data | Multimedia | Digital content ecosystem | More
Data management systems | Data technology platforms | Data application scenarios | More
Insights and gap analysis | Digital vision and targets | Transformation blueprint and architecture | Implementation path | Digital governance | More

Beibu Gulf Port Group embraced digital operations on the right cloud

北部湾港集团
BEIBU GULF PORT GROUP

Container toting cycle at port

Shortened by **13%**

New land-sea corridor Freight time reduced by

1 day

15   Huawei Confidential

HUAWEI

Helping More Enterprises Explore the Global Market

10+ self-owned media with **hundreds of millions of MAUs**
36,000+ third-party media

Traffic aggregation

Boosting for global business

Security & compliance

90% payment scenarios
900+ logistics providers

Enterprise service

120+ global security compliance certifications
20+ compliance packages

Smart localization

Application acceleration

Text translation in **50+** languages
Detection of **100+** languages

2,800+ CDN nodes
20% routing acceleration

MINOVATE

Cross-border payment | Advertising service | Message notification

Cross-region collaborative development for **hundreds of millions of** users
Reaching **58+ million** Huawei users

giikin

Intelligent image cropping | Image synthesis | Image resizing

20x higher ads design efficiency
50% higher click conversion rate

Based on Huawei's own security compliance practices, local operation experience in 170 countries and regions, and a rich global ecosystem, Huawei Cloud provides one-stop and consistent experience for enterprises to expand the global market from multiple dimensions, such as security compliance, global acceleration, traffic aggregation, intelligent localization, and enterprise services.

16   Huawei Confidential

HUAWEI

Deepening Cloud-Cloud Collaboration to Help Enterprises Create Greater Value

Capability collaboration | **Joint operations** | **Business promotion** | **Content collaboration**

Third-party clouds

Huawei Mobile Services | BP&IT Cloud

Vehicle Cloud | **Huawei Cloud**

Cloud native | AI | Data intelligence | Multimedia | Collaborative office | Koo series | HMS Core | AGC

Games

Apps

AppGallery

Huawei Ads

Pre-installation of apps

Video   Music

Reader   Browser

Education Center

Huawei Cloud: The fatigue and distraction detection algorithm reduces the driving incident rate by **38.6%.**
HMS: promotion on Huawei AppGallery and CDP-based precision marketing for **3+ million** daily orders during peak period

Huawei Cloud & Huawei Mobile Services: custom red envelopes SMS with KooMessage
HMS: smart messaging for **10x higher** CTR

17   Huawei Confidential

Inclusive AI for a Better Planet

Eco-acoustic monitoring system based on cloud and AI

Partner: RAINFOREST CONNECTION

RFCx API @ Huawei Cloud and AI

AI-based sound recognition of gunshots, chainsaws, and vehicles

Solar powered acoustic equipment collecting ambient sounds in real time

Each device covers 7 square kilometers

Illegal logging and poaching

Send alarm notifications
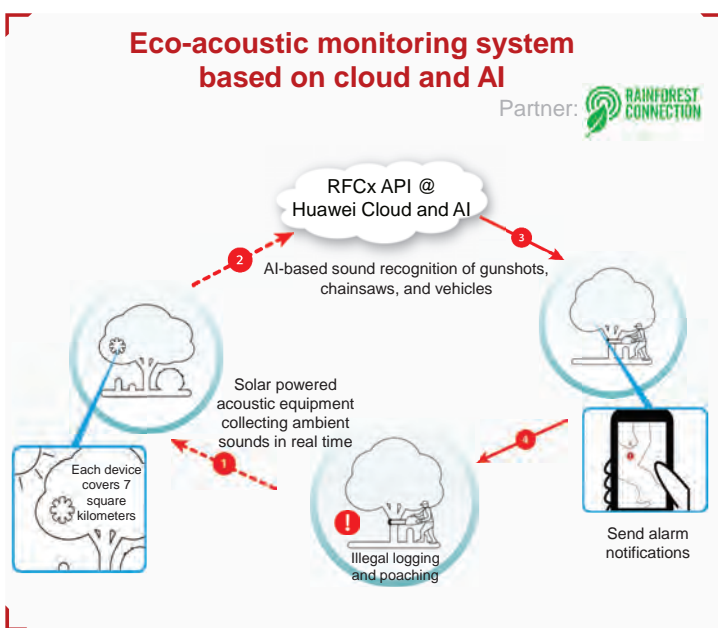
Due to illegal logging, poaching, and unreasonable land use, **420 million hectares** of forest have disappeared worldwide.

Online/Offline acoustic monitoring terminal

Real-time data transmission to the cloud platform

AI-based identification of poaching/species sounds

15 countries

37 protection areas

120,000 hectares
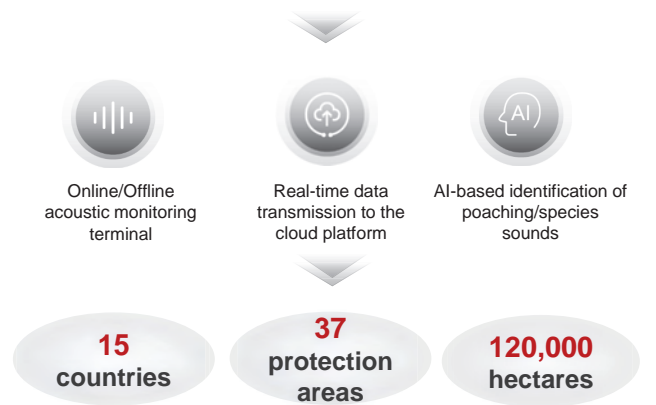
Costa Rica, Philippines, Ireland, Greece, Chile, Malaysia, United Kingdom, Italy, Austria, Mexico, Poland, Colombia, Ecuador, Finland, Croatia

18   Huawei Confidential

A Green Smart Data Center

Gui'an Huawei Cloud Data Center

- Natural ventilation: ambient air cooling
- High-density liquid cooling: heat removal from chips
- AI-aided optimization: energy efficiency up by 5% to 8%
- Silicon-based semiconductor instead of copper: Efficiency of the entire power supply improves from 93% to 95.5%.
- Heat recycling

Annual average PUE	Annually saved	Carbon emission reduced
1.12	**1.01 billion** kWh	**810,000+** tons

Ericssonovo radijsko dostopovno omrežje v oblaku

Ericsson Cloud RAN

Csaba Novak

Ericsson

POVZETEK

V zadnjih letih je opazno povečano zanimanje za virtualizacijo in tehnologije, ki izvirajo iz oblaka. To velja tudi za 5G radijska dostopovna omrežja (RAN). To zahteva izpolnjevanje različnih potreb po bolj odpornih, odprtih, trajnostnih in inteligentnih mobilnih omrežjih. Dolgoročno si predstavljamo, da bo vse, čemur lahko koristi delovanje v oblaku, delovalo v oblaku. *Cloud RAN* v osnovi pomeni ločitev programske opreme osnovnega pasu RAN in strojne opreme osnovnega pasu RAN, kjer je funkcionalnost osnovnega pasu RAN v obliki programja. Programi se lahko izvajajo na kateri koli zmogljivi komercialni strojni opremi, z ali brez integriranih pospeševalnikov, z uporabo orodij in procesov, ki izvirajo iz oblaka, za upravljanje programske in strojne opreme. Vse več je zanimanja za razširitev domene radijskega dostopovnega omrežja v oblak, kar v veliki meri velja že za IT in jedrno omrežje. Ericssonova rešitev za avtomatizacijo je precej več kot le upravljanje storitev in orkestracijo v skladu z načeli *Open RAN* za upravljanje in avtomatizacijo v oblaku, odprtih in namensko zgrajenih RAN.

SUMMARY

We are seeing an increased interest in virtualization and cloud-native technologies with 5G Radio Access Networks (RAN) and beyond, that promise to meet diverse and varied needs for more resilient, open, sustainable, and intelligent mobile networks. In the long run, we envision that everything that can benefit from running in the cloud, will be running in the cloud. Cloud RAN, at its most fundamental level, is a separation of the RAN baseband software and the RAN baseband hardware, where baseband RAN functionality is delivered as pure software. This software can run on any capable commercial off-the-shelf hardware, with or without integrated accelerators, using cloud-native tools and processes to manage both software and hardware. There has been an increasing interest in extending the movement to the cloud from the IT and Core network domains to the RAN. Ericsson´s automation solution is going beyond Service Management and Orchestration functionalities in line with Open RAN principles for management & automation across Cloud, Open and Purpose-built RAN.

O AVTORJU

Csaba Novák (1977. Budimpešta) je vodilni strokovnjak za 5G pri podjetju Ericsson Srednja in Evropa. Magistriral je iz elektrotehnike na Tehnološki univerzi v Budimpešti in opravljal doktorski študij na Oddelku za širokopasovne komunikacijske sisteme – raziskovanje širokopasovnih radijskih tehnologij z razpršenim spektrom, sistemov kodiranja CDMA in sprejemnikov za ublažitev motenj. Na to temo je objavil številne publikacije. Magistriral je iz ekonomskih znanosti na Univerzi Corvinus, kjer je študiral transformacijo vrednostnih verig v omrežja, ki ustvarjajo vrednost na trgu mobilnih komunikacij B2B. Podjetju Ericsson Madžarska se je pridružil leta 2006, danes pa je zadolžen za razvoj omrežja 5G in prodajo v regiji.

ABOUT THE AUTHOR

Csaba Novák (1977. Budapest) is the lead 5G expert for Ericsson's Central-European customer unit. He acquired his MSc in electrical engineering at the Budapest University of Technology, and pursued PhD studies at the Department of Broadband Communication Systems – researching broadband spread spectrum radio technologies, CDMA coding systems and interference mitigation receivers, having numerous publications in the topic. He received his MSc in economic sciences at Corvinus University, studying the transformation of value chains into value creating networks in mobile communications B2B market. He joined Ericsson Hungary in 2006, today he is supporting 5G network evolution and sales in the region.

Ericsson Cloud RAN

Csaba Novák,
Network Products

VITEL Conference – Bled, Slovenia   2023-06-05

Key terminology

Open RAN
- Industry term for Open radio access network architecture
- RAN with separation between HW and SW with open interfaces
- Virtualization allowing multiple vendor products to work together in one network

O-RAN
- Refers to the O-RAN Alliance
- an industry initiative for additional disaggregation and openness in RAN
- Its main objective is to create global standard specifications

Cloud RAN
- Run on COTS hardware
- Deployed on Public or Private cloud
- New requirement – end to end orchestration, assurance and security

Purpose- built
- Bundled RAN SW and HW
- Tightly integrated and optimized deployment
- Higher energy efficiency and capacity

Centralized RAN
- Large part of the RAN processing is done at a hub for multiple antenna sites

Distributed RAN
- All RAN processing for each site is done locally at the antenna site

Cloud native
- SW , HW and LCM in cloud building blocks
- Container based microservice architecture
- Container orchestration
- CI/CD practices for SW creation

History: in old 2013 times...

- Centralized RAN has long been existing
- Baseband hotels already in 3G

2023-06-05 | Public | Page 3 of 23

Cloud RAN drivers

Unified automation

– Increased level of automation of network operations

– Improved operational efficiencies and capabilities

– Introduction of CI/CD for resilient and secure network

Unified automation · Cloud Economics

Drivers

Enterprise use cases
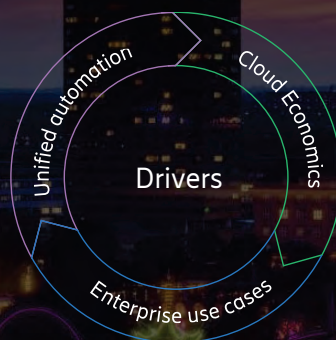
Cloud Economics

– Flexibility to choose the hardware and cloud infra

– Reuse existing IT infra to scale compute resources for RAN

– Deployment flexibility with disaggregation

Enterprise use cases

– 5G private networks

– Cost optimized indoor solution

– Reuse operational processes already in place

– On-prem deployment option

Cloud RAN vision

| Power efficient with best performance | Empower local and global ecosystems | Automated cross-domain operations | Enable new cloud opportunities |
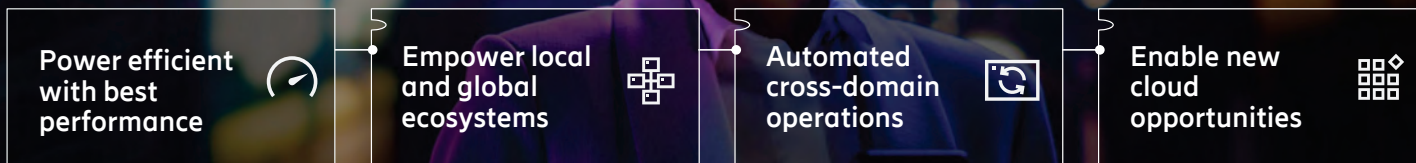
What Ericsson Cloud RAN is?

Purpose Built RAN (Ericsson Radio System)

- **Integrated HW and SW** as one system.
- **Purpose-built Custom Silicon** based HW

Central Unit — Distributed Unit

RAN Compute

Radio, Antenna

▼ ▼ ▼ Virtualized ▼ ▼ ▼

Cloud RAN

- **HW & SW disaggregated**
- **HW on General-purpose processing** (Commercial Off-the-shelf – COTS)
- Integration, verification and lifecycle are managed separately

Central Unit   Distributed Unit

Cloud Platform (CaaS / PaaS)

Generic Hardware (COTS)

Radio, Antenna

2023-06-05 | Public | Page 6 of 23

Cloud RAN deployment options

	Cell site	Far-edge	Near-edge	Data center
Purpose-built RAN Cloud RAN option 1	Baseband RU, vDU, vCU			RAN management
3GPP R15 HLS Cloud RAN option 2	RU, vDU		vCU	RAN management
Cloud RAN option 3	RU	vDU vCU		SMO
Cloud RAN option 4	RU	vDU	vCU	SMO

| 2023-06-05 | Public | Page 9 of 23

Enabling Bluefield Cloud RAN deployments

Bluefield deployment
Introduction of new technology into an existing footprint

Cloud Link

Cloud RAN

RAN Compute

CU

Ericsson Cloud Link

DU

Ericsson spectrum sharing for shared 4G/5G spectrum

Carrier Aggregation for 5G SA and to extend midband coverage

Common CU

Cloud RAN CU

RAN Compute

Ericsson Cloud Link

DU

Cloud native higher layers + joint mobility and user plane
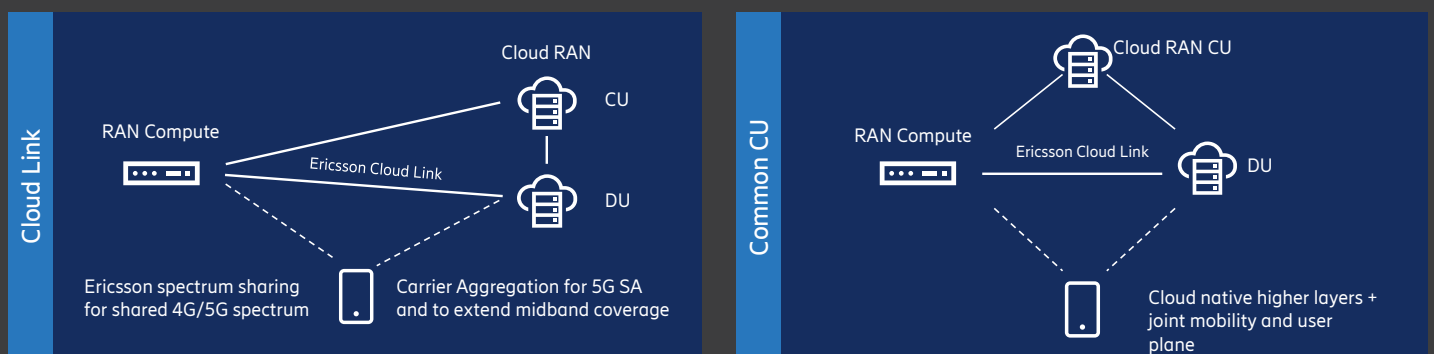
Bluefield deployments will enable CSPs to seamlessly evolve towards cloud native technologies and open network architectures with greater deployment flexibility

| 2023-06-05 | Public | Page 12 of 23

Ericsson Cloud RAN update — Q1 2023

First live site covering all 5G frequency bands

First data call in commercial network

Intel Xeon 4th generation launch

30+
Customer engagements

Portable software enables compute diversity

Ericsson Cloud RAN SW

intel®

AMD

NEW

Independent L1-L3 stack

Common acceleration architecture DPDK and BB dev standardization

Open RAN — Open Hardware — Freedom of choice

2023-06-05 | Public | Page 14 of 23

Cloud RAN—ecosystem overview Q1 2023

	Monitoring	Collaborating	Technology	Partners Solution
CPU, accelerator, NIC	MARVELL Qualcomm arm Mellanox TECHNOLOGIES	NVIDIA	AMD XILINX	intel.
Servers	Quanta Computer SUPERMICRO ODM manufactures	zt Systems	DELL	Hewlett Packard Enterprise
AI platforms			NVIDIA	
Platform as a Service				CLOUD NATIVE COMPUTING FOUNDATION
Containers as a Service	openSUSE vmware Dedicated networks		WNDRVR	RED HAT OPENSHIFT Container Platform
Hyperscalers	IBM Cloud	aws A		

2023-06-05 | Public | Page 15 of 23

What is SMO (Service Management and Orchestration) in O-RAN architecture
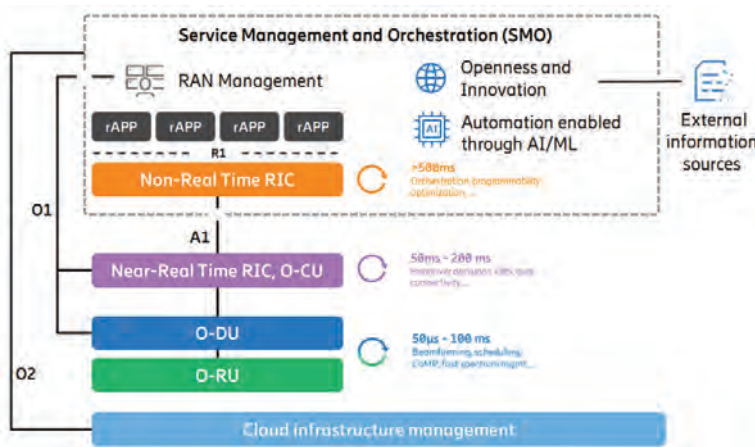
Key benefits of the SMO framework

- Multi-vendor with shorter TTM
  - Faster deployment and orchestration of new services
- TCO reduction
  - manages multi-vendor physical and cloud-RAN and management applications
  - automates the deployment of itself and applications into multi-cloud
  - may be integrated into CSP's existing multi-OSS environment
- Innovation and openness :
  - facilitates innovation through rApps ecosystem
- User experience optimization:
  - extends RAN automation with fast loop (1 sec loop)
  - uses non-RAN data to enrich end user's QoE
  - automates RAN provisioning, optimization and healing

O-RAN ecosystem is using the potential OPEX saving as a market disruption

Ericsson intelligent RAN automation with rApps

■ Network evolution
improves network, energy, and service performance, and enables new revenues

■ Network deployment
handles provisioning and life cycle management of complex networks

■ Network optimization
offers intelligent autonomous functions to optimize customer experience and ROI

■ Network healing
ensures service continuity and resolution of basic and complex incidents

■ Automation and AI foundation
enables faster TTM for — and trust in — high performance AI and automation use cases by means of openness and flexibility

| Network evolution |
| Network deployment | Network optimization | Network healing |
| Automation and AI Foundation |
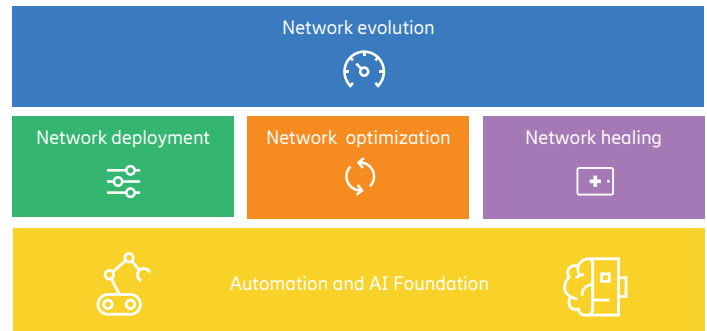
Zero-touch engineering and operations by means of AI
Combine simplification with improved performance, spectral utilization, energy efficiency, security and evolved network architecture

| 2023-06-05 | Public | Page 17 of 23

ericsson.com/cloud-ran

Industrijsko 5G in robno računalništvo v oblaku: osnova industrijskega digitalnega prehoda

Industrial 5G and edge cloud computing: The base of the industrial digital transition

Andrea Del Core

Nokia

POVZETEK

Industrijske zasebne kampusne platforme 5G in platforme robnega računalništva v oblaku so bistvenega pomena za aktiviranje inovativnih industrijskih procesov avtomatizacije in digitalizacije. Kritični procesi za svoje delovanje zahtevajo lastnosti, ki so primerljive s tistimi v kabelskih sistemih, prav tako pa tudi zanesljivost delovanja, kibernetsko varnost. mobilnost in razširljivost. Razpoložljivost podatkov in njihova obdelava sta novo sredstvo za izboljšanje učinkovitosti, produktivnosti in trajnosti ter zahtevata namenske platforme, ki upoštevajo omejitve tehnologij.

SUMMARY

Industrial private campus 5G and edge cloud computing platforms are essential for activation of innovative automation and digitalization industrial processes. Mission and business critical processes require, cable like performance, reliability and cyber security of data processing together with campus mobility and pervasiveness of connections. Industrial Campus Data availability and their processing are the new industrial asset to develop efficiency, productivity and sustainability and require dedicated platforms respecting operation technologies industrial constraints.

Industrije 4.0. Od januarja 2023 je zadolžen za vse industrijske vertikale v Italiji in jugovzhodni Evropi. Njegove dejavnosti se osredotočajo na povečanje konkurenčnosti in trajnosti industrijskih vertikal, ki z vpeljavo platform za upravljanje podatkov lahko podprejo ustvarjanje popolnoma integriranih dobavnih verig, hitre ozaveščene procese odločanja ter učinkovito in trajnostno delovanje.
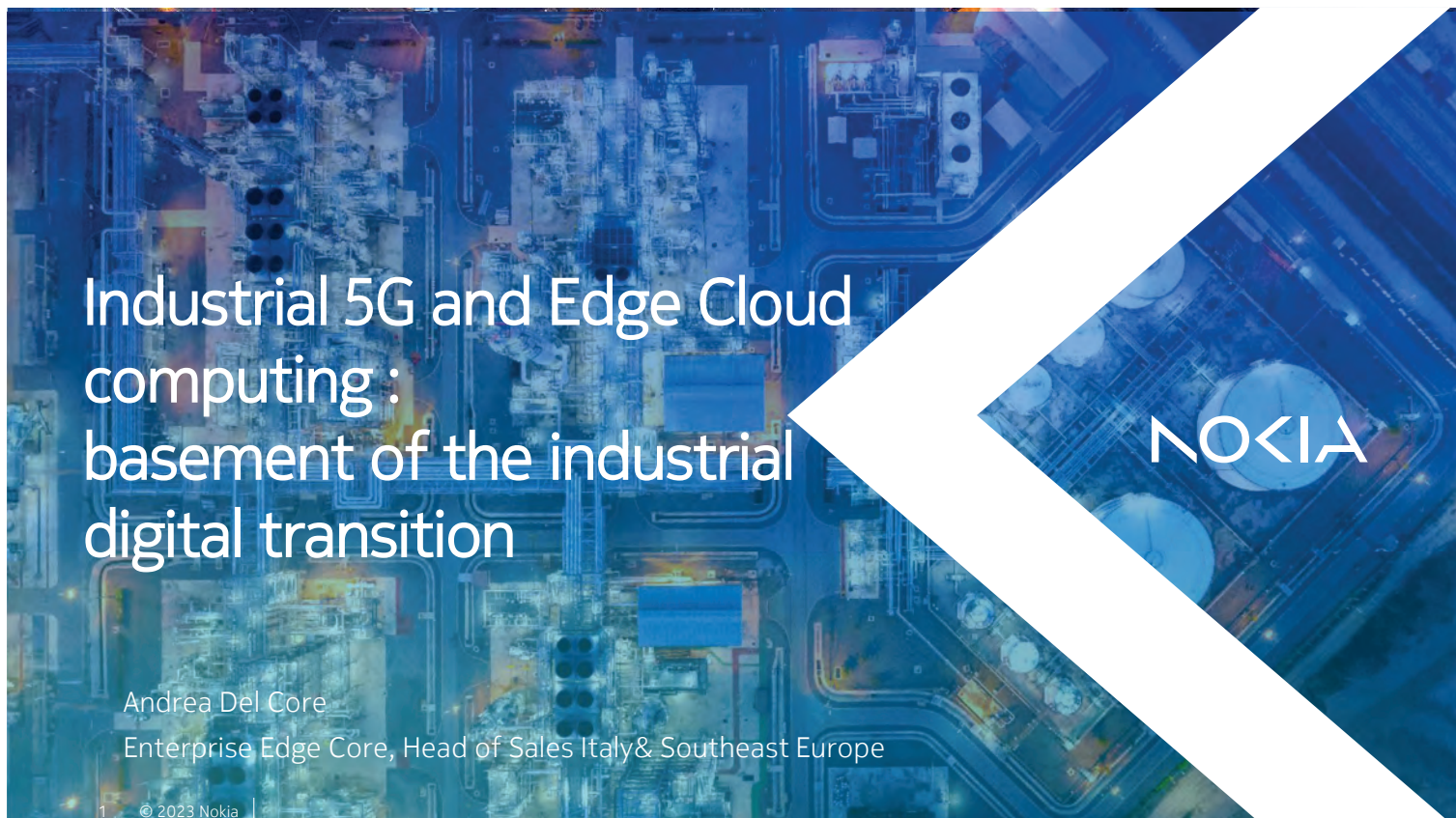
ABOUT THE AUTHOR

Andrea Del Core graduated in Telecommunications Engineering at the Politecnico di Milano. He is Head of Sales Nokia Enterprise Campus Edge in Italy and Southeast Europe. With 25 years of experience in the ICT sector, he has developed his professional career covering product management, partner management, sales management, and accounting roles in international global contexts. In March 2020 Andrea Del Core has got the responsibility of developing the Italian manufacturing market for Nokia with the aim of providing services and solutions that maximize the return on I4.0 investments. Since January 2023 he has extended his activity perimeter to all the industrial verticals for Italy and Southeast Europe. The focus of his activities is to increase the competitiveness and sustainability of industries verticals injecting data management platforms could support generation of fully integrated supply chains, quick aware decision-making processes, efficient and sustainable operations.

O AVTORJU

Anrdea Del Core je diplomiral iz telekomunikacijskega inženiringa na Politehniki v Milanu. Je vodja prodaje za Nokia Enterprise Campus Edge v Italiji in jugovzhodni Evropi. Ima 25 let izkušenj v sektorju IKT. Svojo poklicno kariero je razvijal na področju produktnega upravljanja, partnerskega upravljanja, prodaje in zastopanja v mednarodnem okolju. Marca 2020 je Del Core prevzel odgovornost za razvoj italijanskega trga za Nokio s ciljem zagotavljanja storitev in rešitev, ki povečujrjo donosnost naložb v sektorju

Industrial 5G and Edge Cloud computing : basement of the industrial digital transition

Andrea Del Core
Enterprise Edge Core, Head of Sales Italy& Southeast Europe

NOKIA

1   © 2023 Nokia

On the cusp of the 4th industrial revolution
...and this is happening NOW

Investment in ICT

30%   70%

Share of GDP

70%   30%

■ Physical industries   ■ Digital industries

0.7%

2.7%

Annual productivity growth
(15-year average)

Source: The Technology CEO Council
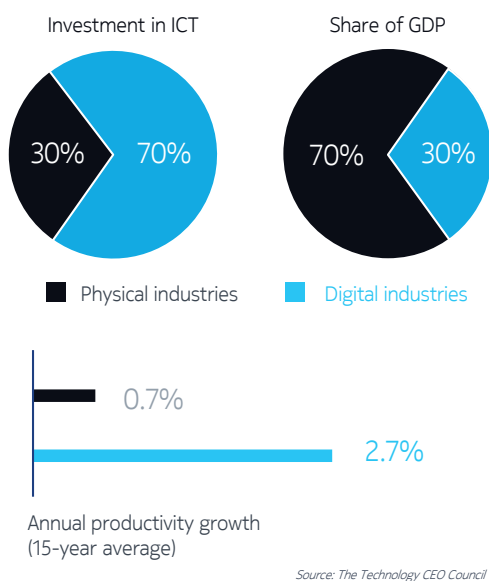
Confluence of key technologies enablers create the perfect environment for Industry 4.0

Edge computing

IoT   Hybrid cloud

°C

Industry
4.0

AR/VR/MR   Artificial
                                            intelligence

Robotics
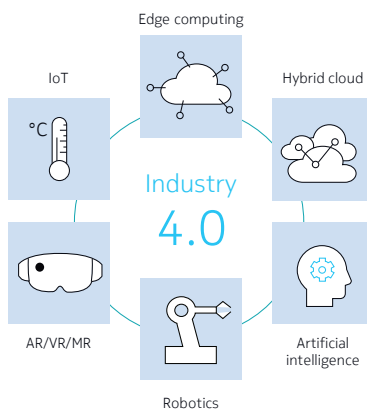
>70%

enterprise are investing in IIoT today

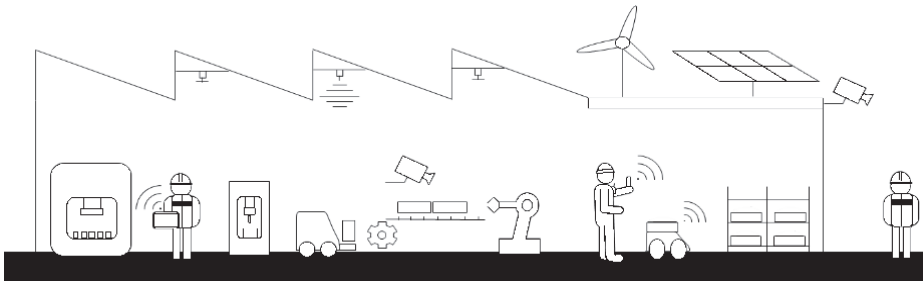*https://www.pwc.pt/pt/temas-actuais/pwc-apresentacao-iot.pdf*

49%

IT are reporting working closer with OT on IoT projects (32% in 2018)

451 research - Internet of Things, Organizational Dynamics 2019

NOKIA

2   © 2023 Nokia

Industrial plants are mostly brownfield campuses
With complex connectivity and compute environments

Heterogenous & fragmented compute environments

- Data stays in the machine
- Value of data not extracted
- Multiple compute units, even for single asset often not orchestrated
- Multi-OS environments
- Legacy compute units
- Legacy applications
- Different compute types: Machine PLCs, Machine control PC, etc...

Heterogenous connectivity environments

- Multiple fixed / wireless connectivity layers
  - Multiple Wi-Fi wireless networks (from different vendors)
  - Multiple low power sensors technology networks
  - Legacy voice network
- Mix of L2 industrial protocols
- Many unconnected assets

3   © 2023 Nokia

NOKIA

Industry 4.0 will deliver massive increase in productivity & economic value creation

Enhance efficiency	Increase agility	Better decision	Increase worker safety & productivity	Sustainability
with process automation	to meet fast changing requirements	making via intelligent insights		efficiency helps lower environmental impact

...all this while maintaining asset heavy industries "Must-have" needs

Continuous operation	Safety	Security

4   © 2023 Nokia

NOKIA

Safety, Productivity and Efficiency Technologies for Manufacturing

Tackling Industry 4.0 transformation steps
with Nokia end-to-end Industry digitalization solution
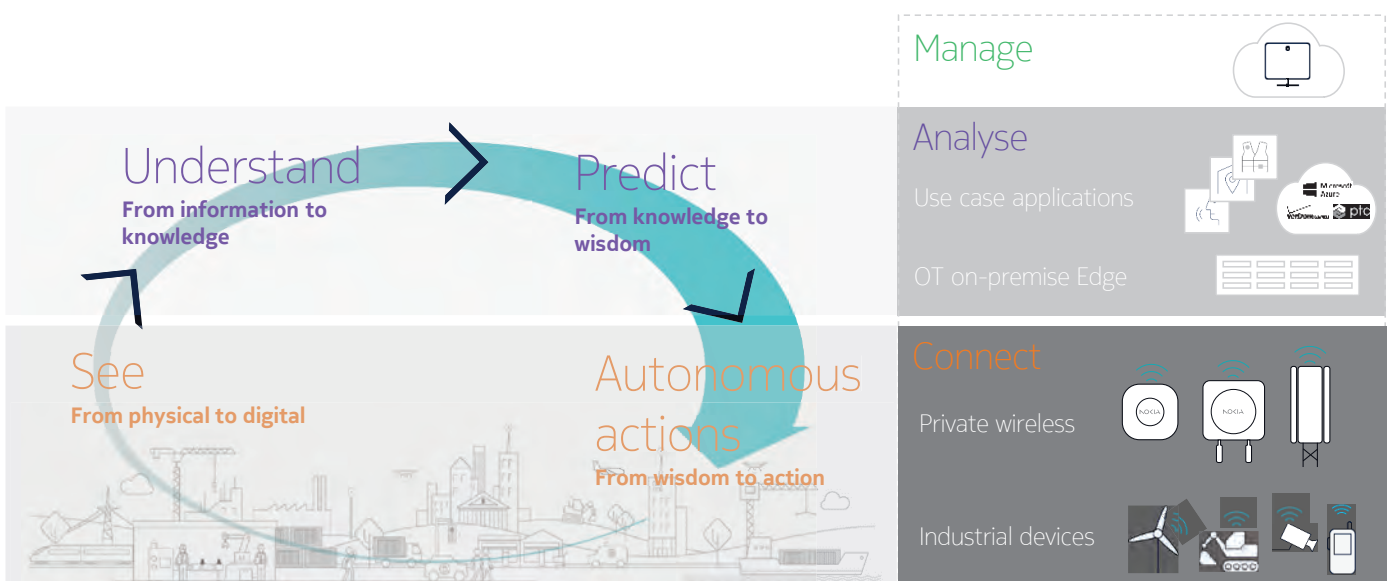
One platform for industrial digitalization
Accelerate I4.0 transformation with private wireless, edge, apps, cloud and Solution-aaS

Reliable & deterministic performance wireless connectivity for digitalization of OT assets and workers, and future autonomous actions

OT low latency edge OT app processing Application enablement (own/3rd P)

Expose APIs, edge data lake and integrate with worlds leading digital ecosystems and solution providers

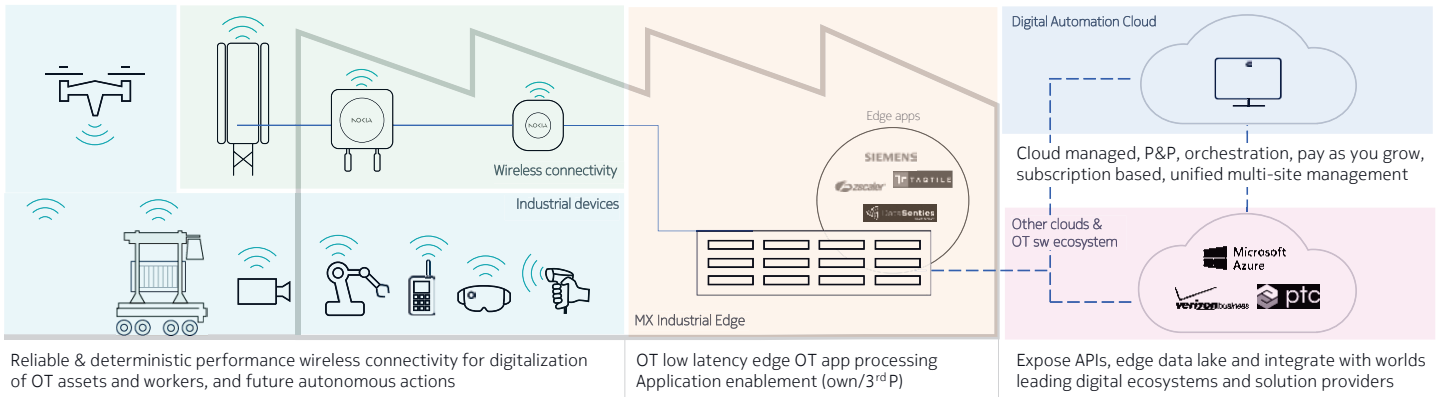| ++ | Industrial Devices & associated apps | Connectivity | OT Edge Compute AAS, Campus data lake | Own OT applications & Industrial connectors | 3rd party apps marketplace & cloud apps partners | Productivity platforms | Northbound & Webscale connectors | ++ |

7   © 2023 Nokia

NOKIA

5G Mobile Industrial Private Network
As-a-service application platform for private wireless connectivity and automation

Accelerate your digital transformation with a proven on-premise edge solution and industrial-grade private wireless connectivity
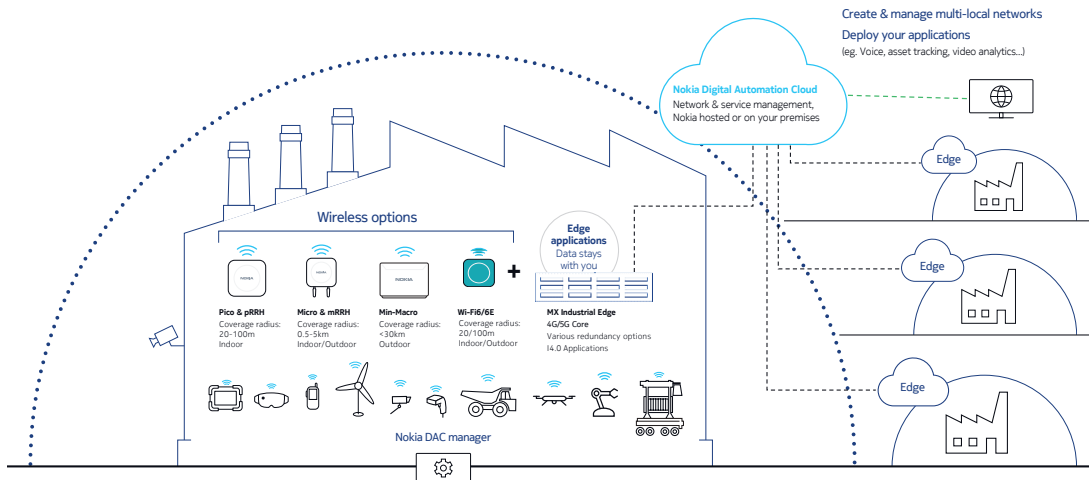
Easy to deploy
- Plug-and-play connectivity, devices, and applications
- Licensed and unlicensed spectrum
- Operation handled from the cloud by experts

Scalable
- pWaaS inherent low upfront cost
- pWaas allows for massive scaling
- Multi-site deployment
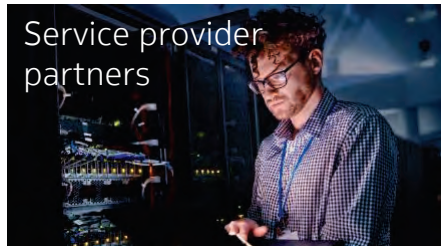- Adding 5G is mostly a software upgrade

With reliability and data confidentiality
- Hybrid edge cloud
- Confidential data kept on site
- Local processing of data for critical applications

8   © 2023 Nokia

NOKIA

Nokia collaborating with entire ecosystem to drive Industry 4.0

Service provider partners

Expertise in building & operating mobile network or public clouds, spectrum partners

System integrators & Consulting

Deeper industry expertise and specialised channel to market

Broadening the sphere of influence

Industrial bodies and ecosystem partners

Kick starting the industry with more LTE and future 5G industrial connected things

9   © 2023 Nokia

NOKIA

Nokia recommends to start with an early and small Proof-of-Concept, grow in use cases and deployment on demand and scale up with new 5G features

Scale-Up
(12-24 months)

Full plant, cross-country deployments that also consider ecosystem partners, supply chain, retailers etc.

Full use case range also using private wireless 5G features of the future, i.e.
- Cloud robotics and co-robots
- Digital twin real-time simulation
- Wireless safety applications

Financing through a multi-year business case (ROI) including IT/ business departments and partners

Deployment
(9-12 months)

Domino effect with additional 3-5 use cases for multiple factory halls and outdoor plants

New use cases leveraging more features of private wireless networks and 5G technology, i.e.
- Worker augmentation and VR
- Voice, video and video analytics
- Drones and digital twin

Financing through line budgets with a step-by-step investment plan

Proof-of-Concept
(6-12 months)

1-2 initial use cases in one part of the campus, factory or plant

Known, maybe already existing use cases are upgraded to private wireless and/or 5G, i.e.
- Automated guided vehicles
- IoT sensor retrofitting for machines
- Connected worker tablets

Financing OPEX-based through strategic or innovation funding with some broader investment picture

START NOW. | START SMALL. | GROW BIG.

Business Transformation: Organization l Processes l Backbone l Content l ...

10   © 2023 Nokia

NOKIA
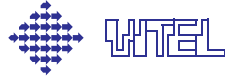
PRISPEVKI

ARTICLES

6. 6. 2023

Uporabniki, storitve in oblak

Users, services and the cloud

Andrej Košir

Univerza v Ljubljani, Fakulteta za elektrotehniko

POVZETEK

V prispevku soočamo pametne storitve za končne uporabnike z rešitvami v oblaku v povezavi z etiko in varovanjem osebnih podatkov. Razvoj pametnih storitev na področju pametnih domov, pametnih mest, tehnološke podpore starejših in drugje temelji na zbiranju občutljivih podatkov uporabnikov. Razvoj etike ne dohaja razvoja tehnologije in tehnoloških zmožnosti zlorabe teh podatkov. Kaj pričakujemo v prihodnosti? Kakšna je vloga in odgovornost kreatorjev tehnologije?

SUMMARY

In this paper, we confront smart services for end users based on cloud solutions in connection with ethics and protection of personal data. The development of smart services in the field of smart homes, smart cities, technological support for the elderly and elsewhere is based on sensitive user data. The development of ethics does not keep up with the development of technology and the technological capabilities of abusing this data. What do we expect in the future? What is the role and responsibility of technology creators?

O AVTORJU

Andrej Košir je redni profesor na Fakulteti za elektrotehniko Univerze v Ljubljani in vodja Laboratorija za uporabniku prilagojeno komunikacijo in ambientno inteligenco. Dejaven je na raziskovalnih področjih modeliranja uporabnikov in personalizacije, socialno inteligentnih pametnih sistemov, tehnološke podpore starejših, načrtovanja uporabniških poskusov ter razvoja etike na področju pametnih sistemov.

ABOUT THE AUTHOR

Andrej Košir, PhD, BSc math is a full professor at the Faculty of Electrical Engineering, University of Ljubljana. He is head of User-adapted communications and ambient intelligence lab, and IEEE senior member. He is active in a broad research field including: user modelling and personalization, socially intelligent smart systems, and experimental design.

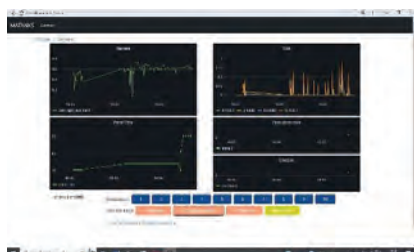# Uporabniki, storitve in oblak

Andrej Košir
andrej.kosir@fe.uni-lj.si

Pametni sistemi

Vir: projekt "Merjenje matematične anksioznosti"

Vir: project SHERPA https://www.project-sherpa.eu/

Vir: projekt "Merjenje multimedijske izpostavljenosti"

Kaj imajo ti projekti skupnega?

Implementacija v oblaku

Občutljive podatke uporabnikov

ICT   LUCAMI

Kaj so naloge in izzivi pametnih sistemov

Segmentacija uporabnikov in persone ('yourneys')

Situacijsko zavedanje

Umetna socialna inteligenca, multimodalna komunikacija

Ciljne storitve (pokrivajo konkretne scenarije)

ICT   LUCAMI

Za to "pamet" potrebujemo

Podatke nosljivih senzorjev (zapestnice, …)
Podatke uporabe sistemov (pametni dom, telefon, avto, …)
Podatke socialnih omrežij

Visoko zmogljivo računalništvo
Algoritmi
Učinkovita integracija – **oblak**

ICT   LUCAMI

Primer: pametni dom za starejše

1. Na osnovi realih podatkov in razvojnih pilotov
   1. Segmentacija in persone
   2. Storitve po segmentih in personah
   3. Situacijsko zavedanje: kateri konteksti, kako jih avtomatsko pridobiti
   4. Socialna inteligenca pametnega doma
   5. Senzorji in aktuatorji: socialno inteligentni robot
2. Integracija v kompletno storitev:
   - Oskrba s strani ponudnika
   - Enovita storitev, dostopna za širok krog (viri)

ICT   LUCAMI

Kdo varuje uporabnike: etika?

Kaj preprečujemo: **zlorabo občutljivih podatkov.**

Nekateri vidiki etike in varovanja

- Etična nevtralnost tehnologije
- Humova giljotina: tehnologija ne bo rešila etike
- Bistvo etičnosti storitve:
  Uporabnik pozna in razume kaj se dogaja z njegovimi podatki

- Anonimizacija in deanonimizacija
- GDPR, ZVOP-2, etične komisije, komisija za preprečevanje korupcije

ICT   LUCAMI

Etična presoja raziskav in projektov

Koga varujejo etične komisije?

Zakaj so vloge tako zapletene?

Kdo je odgovoren za izvajanje zahtev etičnih komisij?

ICT   LUCAMI

Relevantni dogodki v preteklosti (1)

1. Tehnologija ni več etično nevtralna
2. Gumb [STRINJAM SE] ne velja več
3. Google in drugi velikani zaprejo razvoj pred javnostjo
   1. Akademija: odpira
   2. Tehnološki velikani: zapirajo
4. GDPR nadomesti "Data Protection Directive"

ICT   LUCAMI

Relevantni dogodki v preteklosti (2)

5. Google 2019: Advanced Technology External Advisory Council: ukinjen po dobrem tednu dni.
6. Prehod na programsko definirana oprema komunikacijskih sistemov in proizvajalci, povezanimi z državnimi politikami
7. Uporabne inteligentne storitve:
   - oskrbni robot za starejše
   - Avtonomna vozila, …
8. Etični svetovalci na EU projektih

ICT   LUCAMI

Oblak in varovanje podatkov: nasprotnika

Storitev v oblaku ⟷ varovanje občutljivih podatkov

Obdelava v oblaku ⟷ obdelava na robu

Zlivanje uporabniških računov ⟵ → varovanje občutljivih podatkov

Sila v isto smer

Etično ravnanje lahko prispeva k izogibanju slabega mnenja uporabnikov

Prihodnost – razvoj (1)

1. Razvoj oblakov, ki jim etična presoja "zaupa"
   1. Izvedljiv nadzor
   2. Zaupanje nadzoru
2. Razvoj računalništva na robu
   1. Občutljivi podatki ne zapustijo senzorja
   2. Racionalnost strojne opreme računalništva na robu
3. Razvoj varovanja podatkov in deanonimizacija
   1. Deanonimizacija na velikih podatkih
   2. Težko natančno opredeliti

Prihodnost – razvoj (2)

4. Veliki ponudniki vstopijo v razvoj pametnih sistemov

5. Merjenje uporabnikov: nosljivi senzorji se umaknejo analizi podatkov

6. Analiza velikih podatkov da nove občutljive podatke (vključno z deanonimizacijo)

7. Razvoj etike podatkov in uporabnikov:

    1. Odgovori na sodobne izzive: varuje in omogoča razvoj. Pravna podlaga, ki nadomesti "uporabnik ve in razume" za ranljive skupine (trenutne postavke so same neetične)

    2. Ne nadzoruje le raziskav, ampak tudi vse projekte in produkte

ICT   LUCAMI

Prihodnost – izzivi (1)

1. **Razvojni piloti v realnem okolju**

2. Merjenje realnih učinkov storitev (npr. neodvisnost bivanja, učinki na dolgi rok)

3. Segmentacija uporabnikov, načrtovanje storitev po segmentih

4. Situacijsko zavedanje, razvoj umetne socialne inteligence

ICT   LUCAMI

Prihodnost – izzivi (2)

4. Razvoj etike: pravna podlaga, ki nadomesti "uporabnik ve in razume" za ranljive skupine (trenutne postavke so same neetične)

5. Generativni modeli in ChatGPT: generični pogovorni agent, algoritmi za kompleksne naloge

6. Tehnologija ima **družbeno odgovornost**: oskrba starejših, ranljive skupine

7. Preizkus za družbo: **varovanje ranljivih skupin**

ICT   LUCAMI

Varnostni izzivi računalništva v oblaku

Security challenges of cloud computing

David Jelenc

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko

POVZETEK

Računalništvo v oblaku prinaša mnoge prednosti, a hkrati odpira mnoga varnostna vprašanja: narava oblačnih storitev je, da se podatki često hranijo na oddaljenih lokacijah in do njih dostopa preko javnih omrežij, kar odpira dodatne možnosti zlorabam. V prispevku predstavimo, kako je pri računalništvu v oblaku skrb za varnost deljena med ponudnikom in uporabnikom, katere so tipične varnostne grožnje in kako jih naslavljamo ter kako se te s časom spreminjajo.

SUMMARY

Cloud computing introduces many benefits, but also raises many security concerns: the nature of cloud services is such that data is often stored in remote locations and accessed through public networks, which opens additional opportunities for malicious actors. In this paper, we show how in cloud computing the provider and the user share the security responsibility, what are typical cloud computing threats and how they are addressed, and how their dynamics change with time.

O AVTORJU

David Jelenc je doktoriral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani s temo Kvalitativne metode za obvladovanje zaupanja. Na UL FRI deluje kot asistent in vodi vaje pri več predmetih. Njegovo raziskovalno področje je na stičišču informacijske varnosti, računalniških komunikacij ter umetne inteligence.

ABOUT THE AUTHOR

David Jelenc received his doctorate at the Faculty of Computer Science and Informatics of the University of Ljubljana with the topic Qualitative methods for managing trust. At UL FRI, he works as an assistant and leads exercises in several subjects. His research area is at the intersection of information security, computer communications and artificial intelligence.

VARNOSTNI IZZIVI RAČUNALNIŠTVA V OBLAKU

VITEL 2023

David Jelenc, UL FRI

david.jelenc@fri.uni-lj.si

1

UVOD

- Niso vsi oblaki enaki.
- Z varnostnega vidika je smotrna obravnava glede na
    - model <u>namestitve</u> in
    - model <u>storitve</u>.

2

NAMESTITVENI MODEL

- Določa kako so viri, storitve in infrastruktura strukturirani, organizirani in deljeni.
- Vrste:
    - Javni;
    - Skupnostni;
    - Zasebni;
    - Hibridni.

3

JAVNI OBLAK

- Infrastruktura v lasti zunanjega ponudnika, storitve dostopne vsem.
- Konsolidirani in med različnimi uporabniki deljeni računski viri, kjer lahko vsak uporabnik dostopa le do svojih.
- Ni stroška investicije v začetno infrastrukturo, operativni stroški so predvidljivimi.
- Podatke zaupamo ponudniku.
- Amazon, Rackspace, Google, Microsoft, IBM …

4

SKUPNOSTNI OBLAK

- Infrastruktura v lasti več organizacij.
- Storitve dostopne omejenemu naboru uporabnikov.
- Podobna delitev virov kot v javnem oblaku, a prilagojena skupnosti.
- Pogosto za zdravstvene, znanstvene ali vladne organizacije z namenom delitve stroškov.

5

ZASEBNI OBLAK

- Infrastruktura v lasti organizacije in namenjena lastnim potrebam.
- Mora podpirati koncepte računalništva v oblaku.
- Tipično se nahaja v lastnih prostorih.
- Omogoča lažji nadzor nad varnostjo, zahteva upravljanje oblaka.

6

HIBRIDNI OBLAK

- Kombinacija dveh ali več namestitvenih tipov.
- Pogosto kombinacija javni–zasebni: del se izvede na javnem oblaku, del pa na zasebnem zaradi
  - varnostnih pomislekov,
  - nižanja zakasnitev,
  - ali drugih posebnih zahtev.
- Pogosta vmesna točka pri prehodu na (javno) oblačno infrastrukturo.
- Zahtevnejša integracija.

7

STORITVENI MODEL

- Določa ponudbo virov in nivo njihove abstrakcije.
- Vrste (glavne):
  - Infrastruktura kot storitev;
  - Platforma kot storitev;
  - Programska oprema kot storitev.

8

INFRASTRUKTURA KOT STORITEV (IAAS)

- Oskrba računskih, podatkovnih in omrežnih kapacitet.
- Uporabnik prejme navidezni stroj z želenimi kapacitetami in sam upravlja z operacijskim sistemom in ostalo programsko opremo.
- Ponudnik upravlja z hipervizorjem, strojno opremo, omrežno in električno infrastrukturo.
- Zmožnost poganjanja poljubnih delovnih bremen.

9

PLATFORMA KOT STORITEV (PAAS)

- Ponudnik dodatno ponudi in upravlja še z operacijskim sistemom, izvajalnim okoljem in različnim aplikacijskimi storitvami.
- Uporabnik ima nadzor nad podatki, razvito aplikacijo in nekaterimi nastavitvami izvajalnega okolja.
- Omogoča hitro namestitev aplikacij razvitih z uporabo programskih jezikov in orodij *ponujenih s strani ponudnika*.

10

PROGRAMSKA OPREMA KOT STORITEV (SAAS)

- Celotno vzdrževanje in izvajanje aplikacije je v domeni ponudnika.
- Uporabnik uporablja aplikacijo in zanjo *plačuje*.
- Aplikacijo v celoti vzdržuje ponudnik, uporabnik priskrbi podatke in poslovne procese.
- Office 365, GMail, Facebook, Salesforce CRM, Twitter, LinkedIn …

11

OBLAKOV JE VEČ

- Obveznosti ponudnika in uporabnika storitve so odvisne od namestitvenega in storitvenega modela – vsaj 12 kombinacij:
  - 4 namestitveni modeli,
  - 3 storitveni modeli.
- Podobno je tudi obveznost zagotavljanja varnostnih storitev odvisna od omenjenih kombinacij.

12

DELJENA SKRB ZA VARNOST

- Ponudnik in uporabnik vsak zagotavljata varnostne storitve skladno z namestitvenim in storitvenim modelom (angl. shared security responsibility):
  - 12 kombinacij zložimo v 4.

Lokalno	IaaS	PaaS	SaaS
Aplikacije	Aplikacije	Aplikacije	Aplikacije
Podatki	Podatki	Podatki	Podatki
Izvajalno okolje	Izvajalno okolje	Izvajalno okolje	Izvajalno okolje
Vmesna programska oprema	Vmesna programska oprema	Vmesna programska oprema	Vmesna programska oprema
Operacijski sistem	Operacijski sistem	Operacijski sistem	Operacijski sistem
Virtualizacija	Virtualizacija	Virtualizacija	Virtualizacija
Strežniki	Strežniki	Strežniki	Strežniki
Shramba	Shramba	Shramba	Shramba
Omrežje	Omrežje	Omrežje	Omrežje

▢ Varnost zagotavlja uporabnik   ▢ Varnost zagotavlja ponudnik

- Deljena skrb je slabo razumljena: le 43 % vprašanih pravilno poda najpogostejšo razdelitev deljene odgovornosti pri IaaS (Oracle and KPMG Cloud Threat Report, 2018).

13

ŽELENE VARNOSTNE STORITVE

- Zaupnost (tajnost).
- Celovitost.
- Razpoložljivost.
- Neovrgljivost.
- Overjanje.
- Avtorizacija.
- Nadzor dostopa.

14

VARNOSTNE GROŽNJE V OBLAKU

- Grožnja: karkoli lahko povzroči škodo sistemu.
- Identificiramo jih sistematično:
  - z uporabo modela za identifikacijo groženj,
  - na podlagi preteklih varnostnih incidentov,
  - izkušenj.

15

MODEL STRIDE

- Model za identifikacijo groženj.
- Z njim analiziramo vsako komponento računalniškega sistema, tako da se vprašamo, ali so omenjene grožnje mogoče, in če, kako:
  - **Spoofing.** Potvarjanje izvora sporočil.
  - **Tampering.** Neavtorizirano spreminjanje podatkov, sistemov in procesov.
  - **Repudiation.** Ovrgljivost, odsotnost beleženja.
  - **Information disclosure.** Neavtorizirano razkritje podatkov.
  - **Denial of service.** Ohromitev storitve.
  - **Elevation of privilege.** Pridobitev privilegiranega dostopa z namenom izrabe sistema.

16

OCENA TVEGANJA

- Vsaki grožnji *g* pripišemo **tveganje** kot kombinacijo verjetnosti, da grožnja nastopi, in negativnega učinka, ki ga tako uresničenje prinese:

$$R(g) = P(g) \cdot I(g)$$

- Na oceno verjetnosti vplivajo:
  - vektor napada (potencialni napadalci in zahtevnost),
  - ranljivosti (pogostost in zaznavnost).
- Ocena učinka uspešnega napada je organizacijsko pogojena (tehnični učinek, poslovni učinek).

17

PRIMERI SEZNAMOV TVEGANJ

OWASP Cloud Top 10 Risks (2019)

1. Odgovornost in razpolaganje s podatki.
2. Federacija uporabniških identitet.
3. Pravni vidiki in regulatorna skladnost.
4. Skrb za neprekinjeno poslovanje in odpornost.
5. Uporabniška zasebnost in sekundarna uporaba podatkov.
6. Integracija storitev in podatkov.
7. Večnajemniška in fizična varnost.
8. Analiza incidentov in digitalna forenzika.
9. Varnost infrastrukture.
10. Razkritje testnih okolij.

OWASP Cloud-Native Application Security Top 10 (2021)

1. Ne varne nastavitve storitev, vsebnikov in orkestracij.
2. Dovzetnost na napade z vrivanjem.
3. Pomanjkljivo overjanje in avtorizacija.
4. Cevovod CI/CD in napake oskrbovalne verige programske opreme.
5. Nezavarovana shramba tajnih vrednosti.
6. Permisivne in nezadostne omrežne politike.
7. Uporaba komponent z znanimi ranljivostmi.
8. Neskrbno ravnanje z viri.
9. Nezadostne omejitve računskih virov.
10. Neučinkovito spremljanje in beleženje.

CSA Top Threats to Cloud Computing (2022)

1. Pomanjkljivo upravljanje identitet, poverilnic, dostopa in ključev.
2. Nezavarovani uporabniški in programski vmesniki API.
3. Napačne nastavitve storitev in nezadosten nadzor nad spremembami.
4. Odsotnost varnostne arhitekture in strategije za prehod v oblak.
5. Odsotnost varnih praks pri razvoju programske opreme.
6. Uporaba nezavarovanih virov tretjih oseb.
7. Sistemske ranljivosti.
8. Nenamerno razkritje podatkov v oblaku.
9. Napačne nastavitve in izraba funkcij serverless in vsebniških bremen.
10. Organiziran kriminal, napadalci in skupine APT.
11. Kraja podatkov iz oblačne shrambe.

TVEGANJA POVEZANA Z OVERJANJEM IN AVTORIZACIJO

- Overjanje in avtorizacija sta tipično centralizirana zato je toliko bolj pomembno, da sta implementirana pravilno. Pogoste napake:
  - Uporaba šibkih gesel, ključev, žetonov, zgolj enofaktorskega overjanja.
  - Dodeljevanje in odstranjevanje uporabniških vlog ni usklajeno z dejanskimi kadri in ne sledi načelu minimalnega potrebnega privilegija.
  - Napačno nastavljen ali odsoten nadzor dostopa.
- Tveganja:
  - CR.2: Federacija uporabniških identitet.
  - CSA.1: Pomanjkljivo upravljanje identitet, poverilnic, dostopa in ključe.
  - CSA.2: Nezavarovani uporabniški in programski vmesniki API.
  - CNAS.3: Pomanjkljivo overjanje in avtorizacija.

19

TVEGANJA POVEZANA Z VARNOSTJO OBLAČNE INFRASTRUKTURE

- Podatki v oblaku pripadajo različnim uporabnikom in morajo biti ustrezno ločeni.
- Ponudnik mora dobro vzdrževati, posodabljati in varovati lastno infrastrukturo.
- Za zaupanje je dobro, da je ponudnik o tem transparenten.
- Tveganja:
  - CR.7: Večnajemniška in fizična varnost.
  - CR.9: Varnost infrastrukture.
  - CSA.7: Sistemske ranljivosti.
  - CSA.11: Kraja podatkov iz oblačne shrambe.

20

TVEGANJA SPECIFIČNA RAČUNALNIŠTVU V OBLAKU

- Fizična lokacija strežnikov je podvržena lokalni zakonodaji, zato jo mora ponudnik upoštevati, uporabnik pa se je zavedati.
- Ponudnik utegne podatke v oblaku uporabiti za dodatne namene (npr. podatkovno rudarjenje); pri tem mora biti transparenten.
- Posebnosti oblačnih storitev odpirajo nove možnosti napadalcem: napad z ohromitvijo denarnice (angl. denial of wallet attack).
- Tveganja:
  - CR.3: Pravni vidiki in regulatorna skladnost.
  - CR.5: Uporabniška zasebnost in sekundarna uporaba podatkov.
  - CSA.9: Napačne nastavitve in izraba funkcij serverless in vsebniških bremen.
  - CSNA.8: Napačno ravnanje z viri.
  - CSNA.9: Nezadostne omejitve računskih virov.
  - CSNA.10: Neučinkovito spremljanje in beleženje.
- **Trend**: narašča tveganje za grožnje, katere morajo naslavljati uporabniki, tveganja za grožnje, katera naslavljajo ponudniki, se zmanjšujejo.

21

ZAKLJUČEK

- Pri računalništvu v oblaku je skrb za varnost deljena med ponudnikom in uporabnikom: meje odgovornosti morajo biti jasne.
- Grožnje pretijo tako ponudnikom kot uporabnikom.
- Trendi kažejo, da postajajo uporabniki storitev šibkejši člen: naraščajo tveganja, za katera so zadolženi uporabniki, dočim tveganja, ki bremenijo ponudnika, postajajo manj izrazita.

22

VIRI

1. Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions. The Journal of Supercomputing, 2020.
2. Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan. A Comprehensive Survey on Security in Cloud Computing, Procedia Computer Science, 2017.
3. Cloud Security Alliance. Top Threats to Cloud Computing – the 'Pandemic Eleven', 2022.
4. Oracle, KPMG. Oracle and KPMG Cloud Threat Report 2020, Addressing Security Configurations Amidst a State of Constant Change, 2020.
5. Oracle & KPMG, Demystifying the Cloud Shared Responsibility Security Model. Oracle and KPMG Cloud Threat Report 2020 series, Volume 2, 2020.
6. Ludovic Petit. OWASP Cloud Top 10: Top 10 Cloud Security Risks, 2019. https://owasp.org/www-pdf-archive/OWASP_Cloud_Top_10.pdf
7. Open Web Application Security Project. (10. 5. 2023). OWASP Cloud-Native Application Security Top 10. https://owasp.org/www-project-cloud-native-application-security-top-10

23

Izzivi pri varnem prehodu na kontejnerska, oblačno zasnovana okolja Kubernetes in SSDLC

Challenges in safely transitioning to containerized, cloud-native Kubernetes and SSDLC environments

Uroš Majcen, Jože Orehar

S&T Iskratel

POVZETEK

Sestava ranljivosti aplikacij se je spremenila zaradi prehoda z monolitnih aplikacij na *cloud-native* aplikacije, vendar testiranje varnosti aplikacij temu ni sledilo, zato je varnost *cloud-native* aplikacij ogrožena. V tej predstavitvi bomo raziskali, kako so se ranljivosti razvile pri prehodu z monolitnih na *cloud-native* aplikacije in mikrostoritve. Videli bomo, kako se izvajajo izvorne ranljivosti v oblaku in kako so videti kot ranljivi tokovi in ne le statična napaka. V praktičnem delu pa si bomo ogledali postopke in orodja, ki omogočajo višjo stopnjo varnosti aplikacij in rešitve.

SUMMARY

The composition of application vulnerabilities has changed due to the transition from monolithic applications to cloud-native applications, but application security testing has not kept up, so the security of cloud-native applications is at risk. In this presentation, we will explore how vulnerabilities have evolved in the transition from monolithic to cloud-native applications and microservices. We'll see how cloud native vulnerabilities are implemented and how they look like vulnerability streams rather than just a static bug. In the practical part, we will look at procedures and tools that enable a higher level of application and solution security.

O AVTORJIH

Uroš Majcen je direktor oddelka za kibernetsko odpornost in vodja SOC v družbi S&T Iskratel. Ima več kot 25 let izkušenj na področju varnostnih rešitev, nadzornih sistemov in upravljanja. Je certificiran strokovnjak za SIEM in varnost ter sodelavec nacionalne zakonodaje o informacijski varnosti.

Jože Orehar je vodja oddelka DevOps za rešitve v oblaku z več kot 25-letnimi izkušnjami in bogatim strokovnim znanjem na področju virtualizacije in oblačno zasnovanih rešitev. Je strokovni vodja ekip Oblačne rešitve, razvoj in izvedba ter sodeluje pri pripravi rešitev, zasnovanih na oblaku. Usposobljen je za načrtovanje in implementacijo visoko razpoložljivih (HA) in geografsko porazdeljenih (GEO) arhitektur. Navdušen je nad odprtokodnimi tehnologijami in spodbuja sodelovanje pri razvoju rešitev. Sodeluje s Fakulteto za računalništvo in informatiko v Ljubljani ter sodeluje pri evropskih raziskovalnih projektih, ki so osredotočeni na rešitve v oblaku.

ABOUT THE AUTHORS

Uroš Majcen is the director of the cyber resilience department and head of the SOC at S&T Iskratel. He has more than 25 years of experience in the field of security solutions, control systems and management. He is a certified SIEM and security expert and contributor to national information security legislation.

Jože Orehar is the head of the DevOps department for cloud solutions with more than 25 years of experience and extensive expertise in the field of virtualization and cloud-based solutions. He is a professional leader of Cloud solutions, development and implementation teams and participates in the preparation of cloud-based solutions. He is skilled in the design and implementation of high availability (HA) and geographically distributed (GEO) architectures. He is passionate about open source technologies and encourages collaboration in the development of solutions. He collaborates with the Faculty of Computer Science and Informatics in Ljubljana and participates in European research projects focused on cloud solutions.

s&t ISKRATEL

Izzivi pri varnem prehodu na kontejnerska, cloud native okolja Kubernetes+SSDLC

Orehar, Majcen Maj 2023

Izzivi pri varnem prehodu na kontejnerska, cloud native okolja Kubernetes+SSDLC

Jože Orehar
S&T Iskratel
Vodja oddelka Razvoj in izvedba
Oblačne rešitve

Uroš Majcen
S&T Iskratel
Direktor področja kibernetske odpornosti

> 25 let
Varnostne rešitve, nadzorni sistemi, upravljanje

Glavne izkušnje
Varnostne storitve in rešitve SOC

> 20 let
Virtualizacijske in oblačne rešitve

Glavne izkušnje
Virtualizacijske in oblačne rešitve, DevSecOps, HA/GEO arhitekture

s&t ISKRATEL

1

Agenda

Cloud-Native Varnost v teoriji (Orehar)
– Aplikacije in Ranljivosti
– Aplikacijska varnost – pristop
– Ocena ranljivosti: Cloud-Native pristop

Cloud-Native Varnost v praksi (Majcen)
– Odgovor na ta izziv: SSDLC - Secure Software Development LifeCycle
– SAST, DAST, SCA
– Izkušnje S&T Iskratel pri SSDLC

s&t ISKRATEL   2

Aplikacije in Ranljivosti

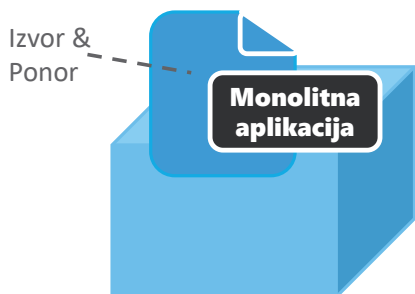## So sedaj Porazdeljene

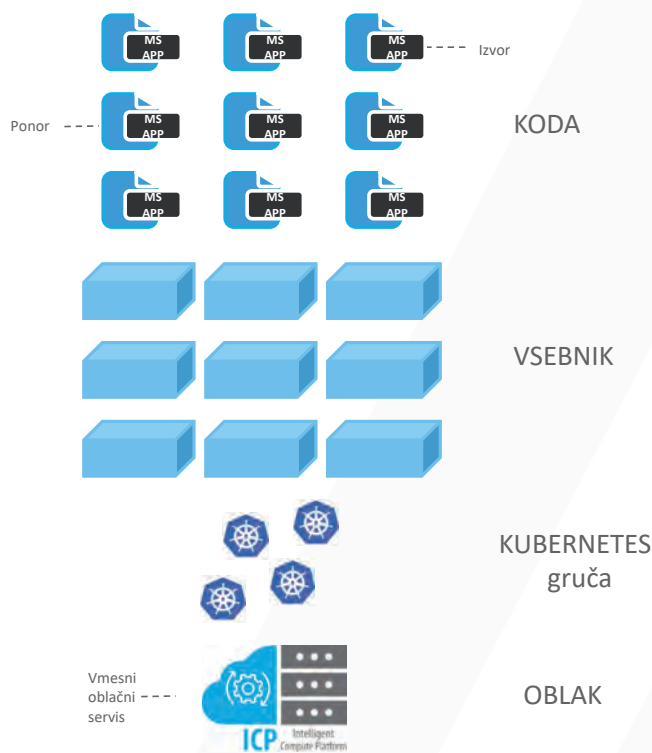Monolitna | Lokalne ranljivosti   Oblačno zasnovana | Porazdeljene ranljivosti

s&t ISKRATEL   3

Infrastruktura je pomembna

Monolitna | Lokalne ranljivosti

KODA

VSEBNIK

KUBERNETES
gruča

OBLAK

Oblačno zasnovana | Porazdeljene ranljivosti

Aplikacijska varnost - pristop

- **Analiza ranljivih tokov**
  - odkrivajte ranljive tokove, ki se raztezajo čez več mikro storitev in infrastrukturnih plasti

- **Validacija ranljivosti**
  - osredotočite se na funkcije in module, ki so v uporabi

- **Verifikacija javne izpostavljenosti**
  - dajte prednost javno izpostavljenim in dostopnim ranljivostim in skrivnostim

Ocena ranljivosti: Oblačno zasnovan pristop

Analiza odprte kode, tuje koda in lastne kode

SAST/SCA/BINARY SCANNING

Zberemo vse potencialne ranljivosti iz nameščene kode in tujih programskih paketov

Sledenje toku aplikacije

Application context

Sledimo toku aplikacije od izvora, ki je odprt v internet, do ranljive vrstice kode znotraj mikro servisa

Konfiguriranje infrastrukture

Cloud context

1. pridobimo konfiguracije iz plasti gruče, vsebnika in oblaka
2. dodamo dodatna izpostavljena tveganja (npr. dodatna dovoljenja)
3. dodamo tveganja dostopnosti interneta

Preračunajte resnost

Results

Preračunamo resnost z namenom osredotočenja na ranljivosti, ki jih je mogoče izkoriščati

s&t ISKRATEL   6

Najpomembnejše ugotovitve

1. Moderni Sodobni problemi zahtevajo **moderne sodobne rešitve**

2. Tveganja, povezana z varnostjo cloud-native oblačno zasnovanih aplikacij, se razvijajo, kar zahteva **posodobljene metode testiranja varnosti**

3. Različna **orodja,** zasnovana za nadzor, se lahko uporabljajo tudi za sledenje ranljivostim

4. **Možnost opazovanja in nadzora** je ključnega pomena za izboljšanje varnosti pri razvoju sodobne programske opreme

s&t ISKRATEL   7

Odgovor na ta izziv: SSDLC - Secure Software Development LifeCycle

— Življenjski cikel varnega razvoja
   programske opreme je sestavljen
   iz petih faz:
  — Izdelava/zbiranje in pregled zahtev
  — Načrtovanje
  — Razvoj
    • Static Application Security Testing
    • Software Composition Analysis (SCA)
      orodja
  — Verifikacija
  — Upravljanje in evolucija

Vir: https://snyk.io/

Dobre prakse SSDLC

— Izobraževanje razvijalcev
  — Smernice za varno kodo (Secure code guideline)
  — Uspodabljanje za varnno kodo (Secure code training)
— Jasne in natančne zahteve
— Upoštevanje rasti
  — Rast zahtev
  — Rast kode
  — Rast razvojnih ekip
— Upoštevanje tudi drugih iniciativ: DevSecOps
— Največji problemi se rešujejo takoj

Static application security testing (SAST)

Statično testiranje varnosti aplikacije - 5 vrst analize SAST

01	Configuration analysis	• Checks the application configuration files. • Ensures that the configuration is aligned with security practices and policies, such as defining a default error page for the web application.
02	Semantic analysis	• Tokenization and examination of syntax, identifiers, and resolving types from code • SAST tools are able to analyze a particular code within its context, such as detecting SQL injections through *.executeQuery().
03	Dataflow analysis	• Tracks the data flow through the application to determine if input is validated before use. • Determines whether data coming from insecure source such as a file, the network or user input is cleansed before consumption.
04	Control flow analysis	• Checks the order of the program operations to detect potentially dangerous sequences such as race conditions, secure cookie transmission failure, uninitiated variables, or misconfigurations of utilities before use.
05	Structural analysis	• Examines language-specific code structures for inconsistencies with secure programming practices and techniques. • Identifies weaknesses in class design, declaration and use of variables and functions • Identifies issues with generation of cryptographic material and hardcoded passwords.

Vir: https://snyk.io/

s&t ISKRATEL   10

Razlike med testiranji varnosti aplikacije: SAST, DAST, SCA

SAST - Static application security testing ,
DAST- Dynamic Application Security Testing
SCA - Software Composition Analysis

Vir: https://snyk.io/

s&t ISKRATEL   11

Preverjanje ranljivosti v različnih fazah SDLC

Stage	Description	Cost	Feedback	Completeness
Local	Great for debugging and building up knowledge among developers but requires individual developer action, and no way to enforce	Medium	Fast	Low
CI/CD	Great as a gate, fast feedback for developers, requires per-pipeline implementation which will depend on how standardized pipeline management is in your organization. Possibly counter productive for low severity issues breaking the build, so need other feedback cycles as well.	Medium	Fast	Variable
Registry	Often a single owner, so easy to integrate and covers all first-party images, no matter how they were built. Potentially noisy because images may be unused.	Low	Medium	Medium
Production	An accurate picture of what you're running, including third-party content, but potentially slow feedback cycles to development teams and the risk vulnerabilities can be exploited in running applications.	High	Slow	High

s&t ISKRATEL

12

Izkušnje S&T Iskratel pri SSDLC

— Ekipa za SSDLC

— Delo na lastnih projektih in na trgu

  — Preverjanja

  — Procesi in metodologije

  — Avtomatizacija

  — Orodja

  — Analize

s&t ISKRATEL

13

About **S&T Iskratel**

EU-based service- and comprehensive **ICT** solutions provider for the **digitalisation** of **industries**. Solutions tailored to **customers' needs**. Products designed in our **own R&D** and **manufacturing centres**.

We generated	We deliver solutions in	We serve
€143	**50+**	**1,200+**
million	countries	customers
revenue in 2021	worldwide and we can respond in your time zone	in 50 countries worldwide

We invest more than	Our team counts	We leverage
€13.5	**1,000+**	**75**
million	employees	years
in engineering, research and development	in 10 countries	of experience and innovation

s&t ISKRATEL

Thank You for Attention

s&t ISKRATEL

Ericssonov odgovor na izzive oblačno zasnovanih tehnologij

Ericsson answer to Cloud native challenges

Boris Škrlj

Ericsson

POVZETEK

Predavanje poudarja pomembnost oblačno zasnovanih tehnologij v segmentu telekomunikacij. Opisani so trenutni trendi in rešitve, ki omogočajo vzpostavitev skalabilnih, odpornih in upravljivih telekomunikacijskih sistemov ter tudi novih scenarijev uporabe in storitev.

SUMMARY

The lecture emphasizes the importance of cloud-native technologies in the telecommunications segment. Current trends and solutions are described, which enable the establishment of scalable, resilient and controllable telecommunication systems, as well as new scenarios of use and services.

O AVTORJU

Boris Škrlj je strokovnjak na področju telekomunikacij z več kot 25-letnimi izkušnjami v panogi. Sodeloval je pri razvoju mobilnih omrežij in prispeval k napredkom od prve (1G) do pete (5G) generacije. Boris že več kot 15 let deluje v podjetju Ericsson, kjer trenutno opravlja funkcijo vodje tehničnih rešitev za osrednjo evropsko regijo.

ABOUT THE AUTHOR

Boris Škrlj is an expert in the field of telecommunications with more than 25 years of experience in the industry. He participated in the development of mobile networks and contributed to advances from the first (1G) to the fifth (5G) generation. Boris has been working at Ericsson for more than 15 years, where he currently holds the position of head of technical solutions for the central European region.

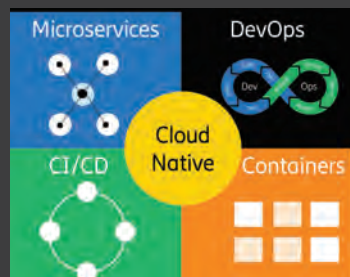# Ericsson answer to Cloud native challenges

Vitel presentation

Boris Škrlj   Ericsson   2023-06-06
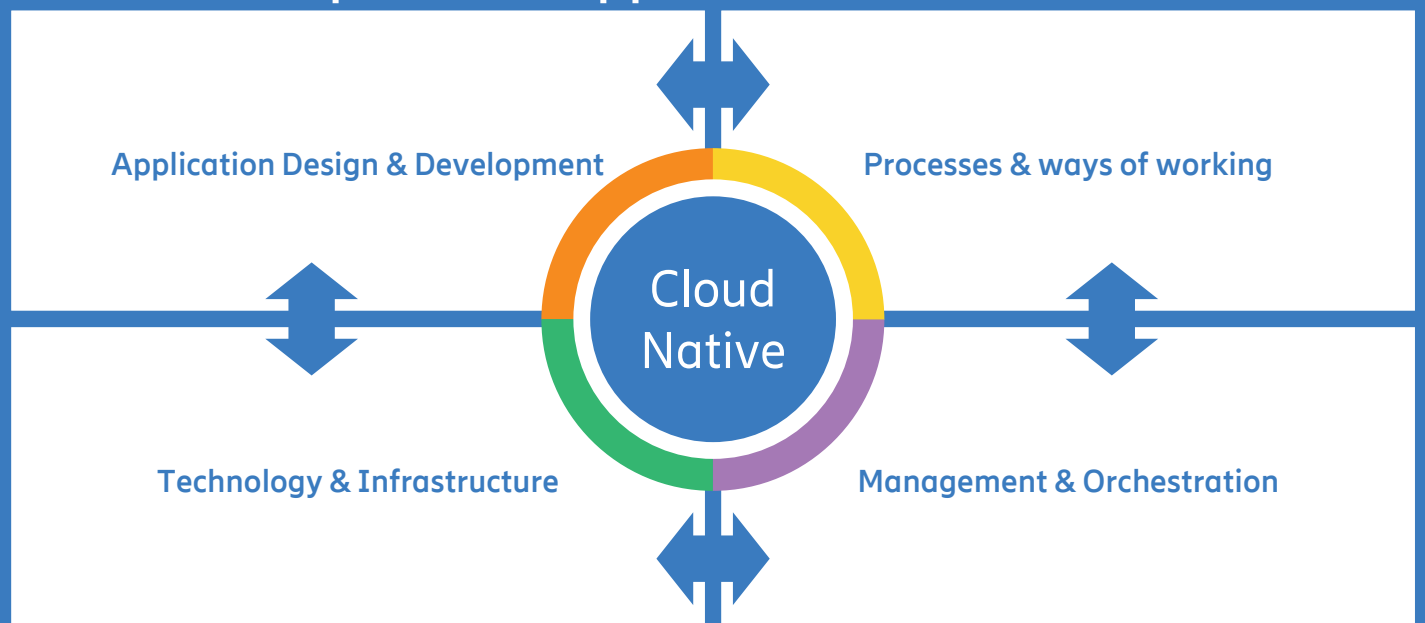
Cloud Native Paradigm Shift

Cloud native is a paradigm shift both from technical and commercial perspective. With the rapid cycles on microservices, we need to fundamentally think different on our business flow in new use cases to stay relevant and competitive.

Road to Cloud Native

PNF   VNF   CNF

Vision for Cloud Native Transformation
Across cloud platform, applications and MANO

Application Design & Development   Processes & ways of working

Cloud Native

Technology & Infrastructure   Management & Orchestration

5G - Bringing benefits to people, business and society

Key drivers

- ■ Sustainability
- ■ Quality of life
- ■ Efficiency
- ■ Productivity
- ■ Safety

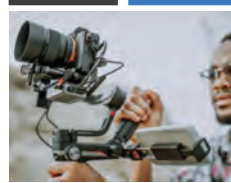Affordable, lightweight, power efficient AR glasses...

No cable, no heavy backpacks for remote VR training...

Enhanced fast interactive cloud gaming experience...
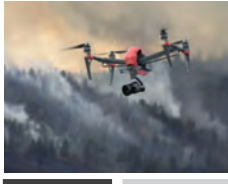
Mobile cameras for high quality Media Production...

Sustainable Cooperative intelligent transport systems...

Flexibility, mobility and lower costs for Industry 4.0...

Automated and remote operations for port efficiency...

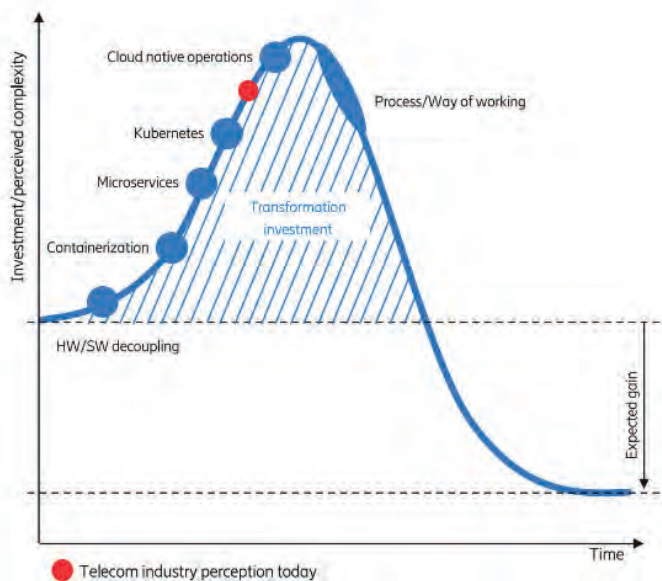Remotely controlled drones for logistics, public safety...

Remotely controlled machines for convenience, safety...

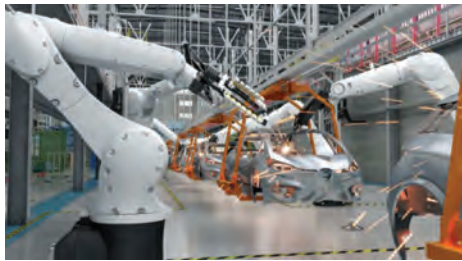Remotely controlled driving as backup for autonomous...

Boris Skrlj | A | 2023-06-06 | Ericsson answer to Cloud native challenges | Ericsson Confidential

The telecom industry cloud native transformation curve

Boris Skrlj | A | 2023-06-06 | Ericsson answer to Cloud native challenges | Ericsson Confidential

Addressing the opportunity of digital transformation for consumers and enterprise

|	
Network developer	Deployment and operation of network infrastructure and connectivity
Service enabler	Providing digital platforms offering value-enhancing digital capabilities
Service creator	Expansion of digital services offering beyond connectivity using own capabilities and extended partnerships

The role of CSPs in the value chain

| 2023-06-06 | Page 7

APIs enabled by a global network platform opens new opportunities to monetize networks
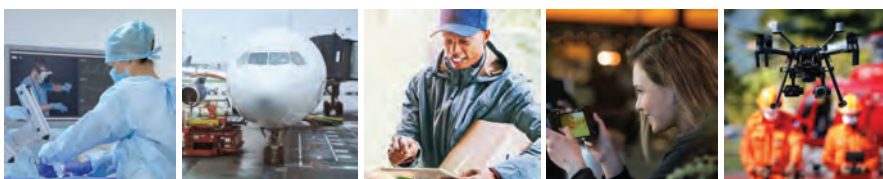
Communications APIs

Messaging   Voice   Video

Network APIs

Authentication   QoS   Location

Global network platform

APIs empower developers, simplify application creation, and optimize performance
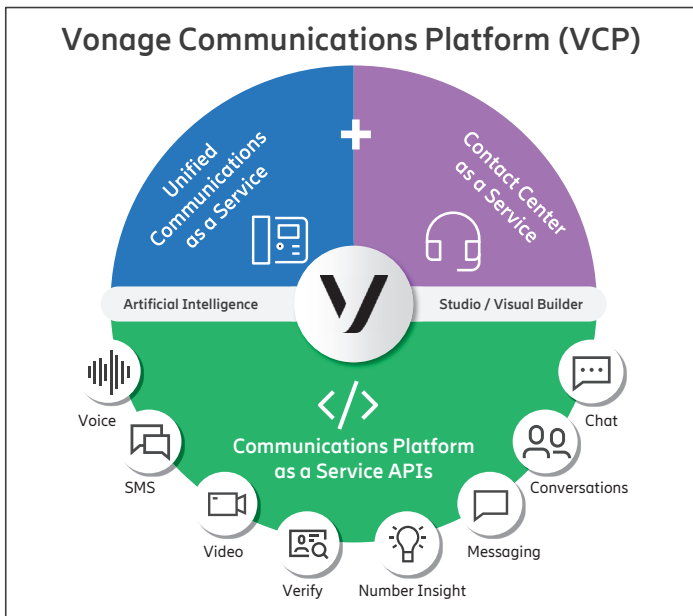
High speed & Low latency   Reliability   Wireless edge solutions   Security   Network slicing

Worldwide 4G and 5G networks

| 2023-06-06 | Page 8

The potential for 5G APIs

Vonage Communications Platform (VCP)
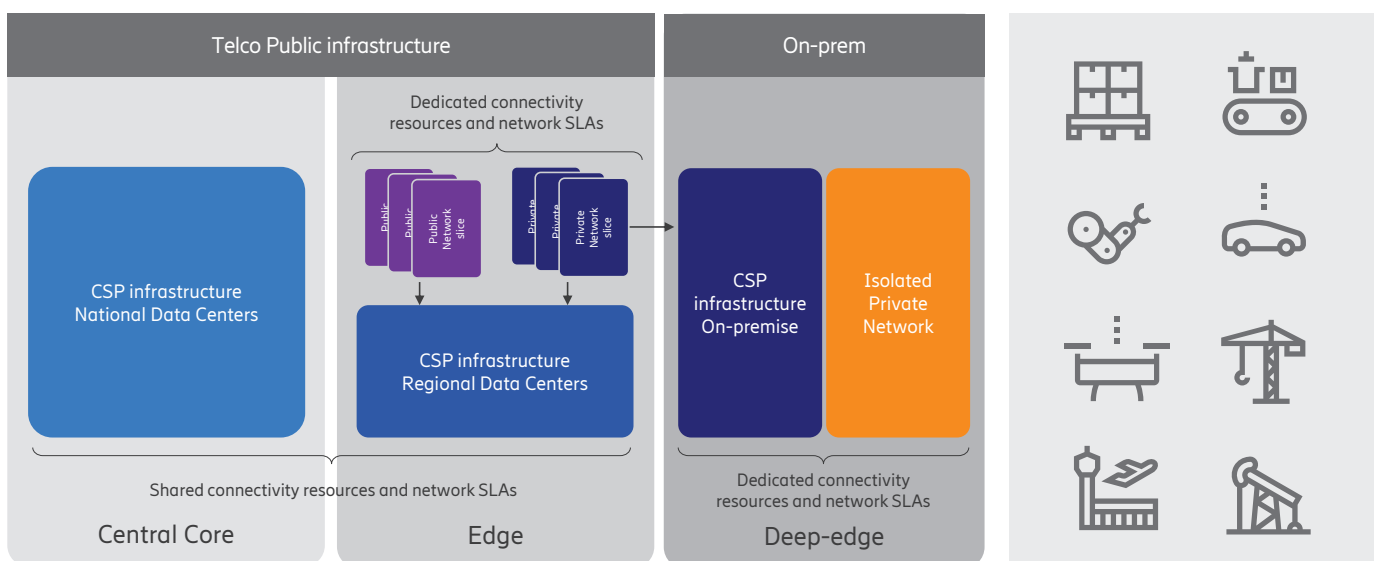

UCaaS & CCaaS

Unified Communications as a Service (UCaaS) provides metal PBX phone system replacement along with collaboration tools

Contact Center as a Service (CCaaS) CCaaS provides cloud contact center
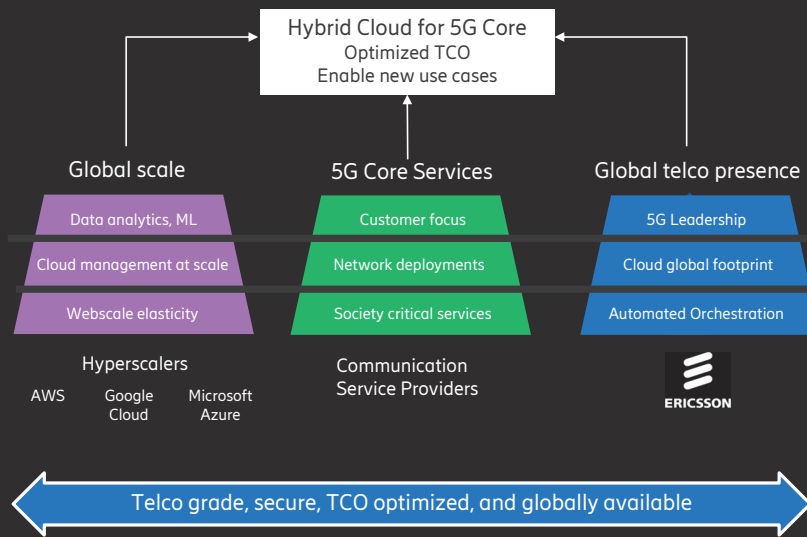
CPaaS/ API

Communications Platform as a Service (CPaaS) is the platform on which developers can program communication functions into their applications via programmable Communications APIs.

| 2023-06-06 | Page 9

Connectivity: getting closer to the end user

Hybrid Cloud for 5G Core

Hybrid Cloud for 5G Core
Optimized TCO
Enable new use cases

Global scale
- Data analytics, ML
- Cloud management at scale
- Webscale elasticity

Hyperscalers
AWS   Google Cloud   Microsoft Azure

5G Core Services
- Customer focus
- Network deployments
- Society critical services

Communication Service Providers

Global telco presence
- 5G Leadership
- Cloud global footprint
- Automated Orchestration
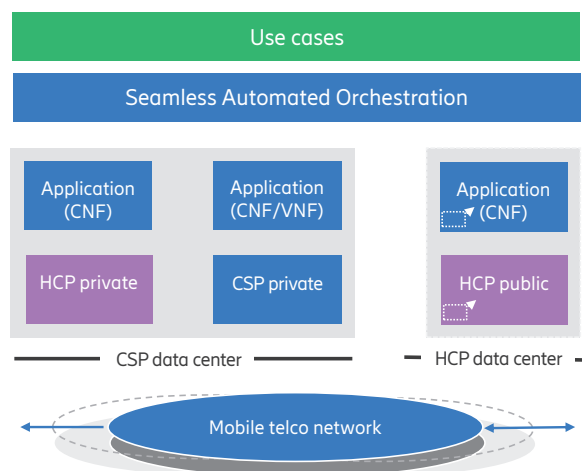
ERICSSON

Telco grade, secure, TCO optimized, and globally available

Enabling 5G Core Hybrid Cloud use cases

Leverage HCP Private capabilities and focus on:

- Utilizing existing CSP operating model with minimal impact on processes and tools
- Compliance with data sovereignty
- Low latency on edge deployments
- Earlier live readiness and global availability

Use cases

Seamless Automated Orchestration

Application (CNF)   Application (CNF/VNF)   Application (CNF)

HCP private   CSP private   HCP public

CSP data center   HCP data center

Mobile telco network

Leverage HCP Public capabilities and focus on:

- Explore elasticity for services which benefit from on-demand capacity.
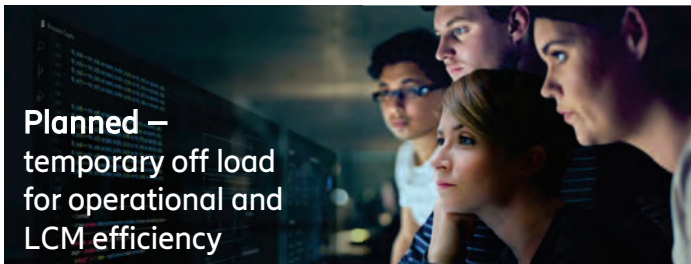- Adopt an evolved operational model
- Enable new revenue streams

Evolved services   Automation   Sustainability   Climate change   Resilience   Regulations

Hybrid cloud use cases – HCP public

Planned

Unplanned

Planned –
additional capacity
for local event

Unplanned –
burst capacity
for emergency incident

Planned –
temporary off load
for operational and
LCM efficiency

Unplanned -
additional capacity
for regional disaster
recovery

2023-06-06 | Page 13

Cloud Native Paradigm Shift

Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds.

Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach.

These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil

Varnostni izzivi in dobre prakse upravljanja omrežij 5G na osnovi oblačnih tehnologij

Security challenges and good practices of 5G network management based on cloud technologies

Matjaž Beričič

Telekom Slovenije

POVZETEK

V drugi polovici tega desetletja bo 5G nedvomno nosilna tehnologija javnih mobilnih komunikacij. Ob tem se postopoma uvaja tehnologija 5G SA, ki predvsem v jedrnem delu temelji na oblačnih (cloud-native) tehnologijah, bo pa tudi temelj napovedanega razmaha zasebnih mobilnih omrežij za posebne potrebe vertical, vezanih na pokritost, zanesljivost, varnost in učinkovitost digitalne transformacije. Ob tem je potrebno sistematično obravnavati paleto varnostnih groženj, s katerimi se soočajo omrežja 5G, pri čemer se lahko naslonimo na različne standardne in varnostne okvire, ki se uveljavljajo kot pomoč celovitemu obvladovanju varnostnih tveganj v omrežjih 5G, še posebej ob uporabi spodaj ležečih oblačnih tehnologij. Pri načrtovanju in upravljanju je potrebno upoštevati znane, po možnosti standardizirane dobre prakse, jih spremljati in razvijati, kot vedno pa je ključno vlagati v znanje in ustrezna sodobna informacijska orodja za uspešno spopadanje z novimi izzivi, ki jih razvoj novih tehnologij prinaša. ENISA v tem smislu podaja dobro osnovo, pričakujemo pa tudi čim prej jasen okvir certifikacije opreme 5G, tako za javna kot za zasebna omrežja 5G.

SUMMARY

In the second half of this decade, 5G will undoubtedly be the carrier technology of public mobile communications. At the same time, 5G SA technology is gradually being introduced, which is primarily based on cloud-native technologies in its core but will also be the basis of the predicted expansion of private mobile networks for the special needs of the vertical, related to coverage, reliability, security and efficiency of digital transformation. At the same time, it is necessary to systematically address the range of security threats faced by 5G networks, whereby we can rely on various standard and security frameworks that are being implemented to help comprehensively manage security risks in 5G networks, especially when using the underlying cloud technologies. When planning and managing, it is necessary to consider known, preferably standardized good practices, monitor and develop them, and as always, it is crucial to invest in knowledge and appropriate modern information tools to successfully deal with the new challenges that the development of new technologies brings. In this sense, ENISA provides a good basis, and we also expect a clear certification framework for 5G equipment as soon as possible, both for public and private 5G networks.

O AVTORJU

Matjaž Beričič je leta 1998 na Fakulteti za elektrotehniko Univerze v Ljubljani doštudiral elektrotehniko in telekomunikacije, leta 2006 pa je s tega področja tudi magistriral. Ves čas je poklicno aktiven na področju mobilnih in fiksnih komunikacijskih tehnologij. V tem obdobju je deloval v različnih vlogah s področja upravljanja, načrtovanja in vodenja projektov ali organizacij s področja mobilnih omrežij, jedrnih omrežij, sistemov za upravljanje zmogljivosti ter razvoju storitev omrežij pri operaterjih Simobil, Mobitel in v skupini Telekom Slovenije. Od decembra 2022 je direktor Dostopovnih omrežij v Telekomu Slovenije.

ABOUT THE AUTHOR

In 1998, Matjaž Beričič completed his studies in electrical engineering and telecommunications at the Faculty of Electrical Engineering of the University of Ljubljana, and in 2006 he also obtained a master's degree in this field. He is professionally active all the time in the field of mobile and fixed communication technologies. During this period, he worked in various roles in the field of management, planning and management of projects or organizations in the field of mobile networks, core networks, capacity management systems and development of network services at operators Simobil, Mobitel and in the Telekom Slovenije group. Since December 2022, he has been the Director of Access Networks at Telekom Slovenije.

Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij
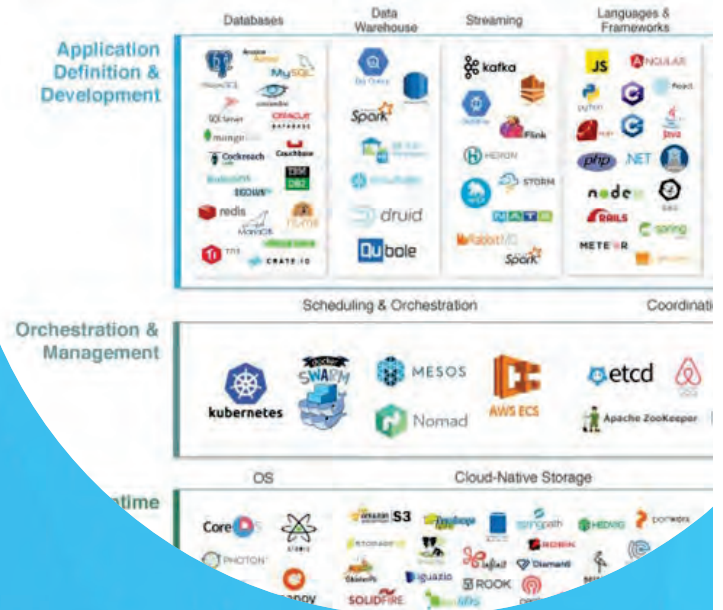
VITEL
Oblačno zasnovana omrežja
junij 2023

mag. Matjaž Beričič

1   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije

5G v javnih in zasebnih oblačno zasnovanih omrežjih

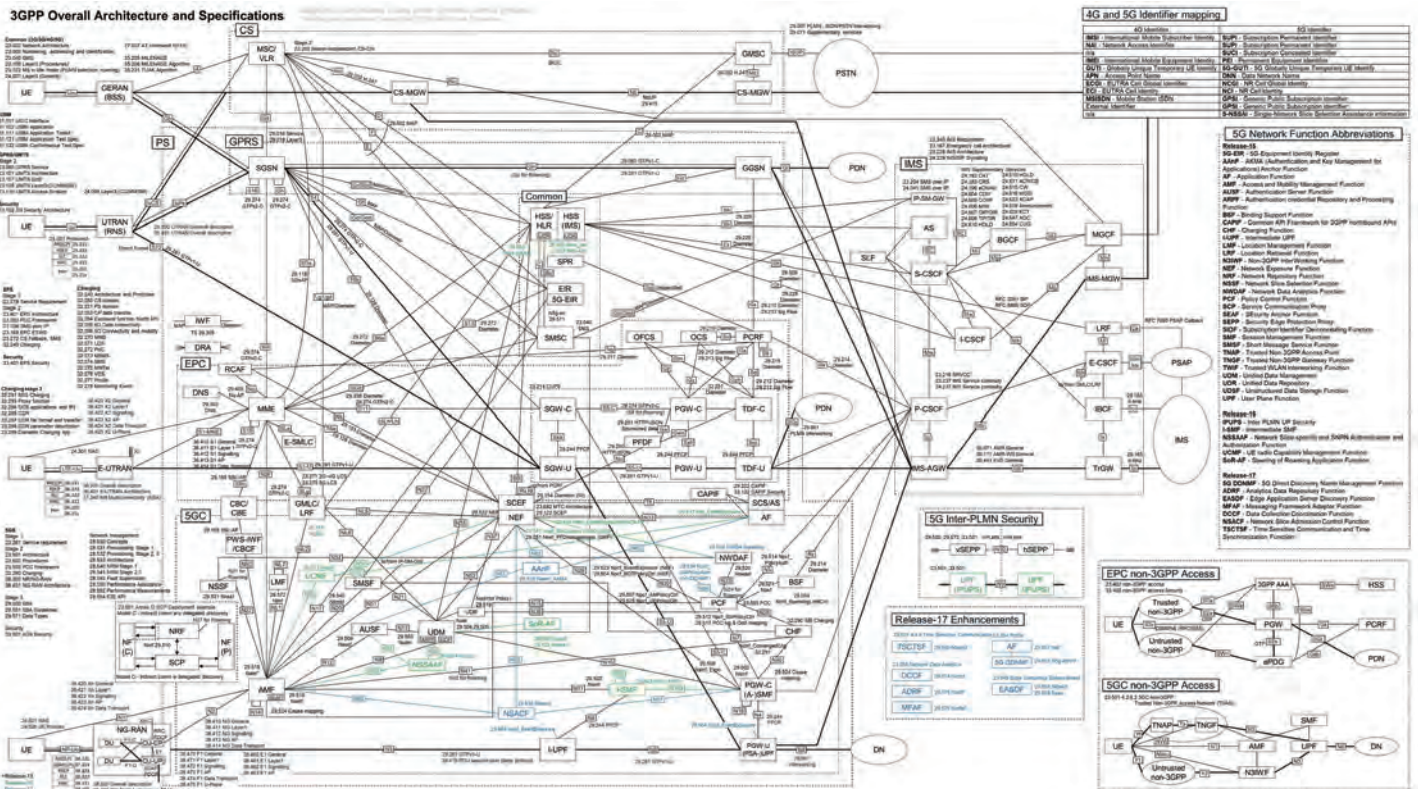**Paleta groženj s katerimi se soočajo 5G omrežja**

Varnost v 5G standardih

NFV varnost v 5G – izzivi in dobre prakse

2   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije

3   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij
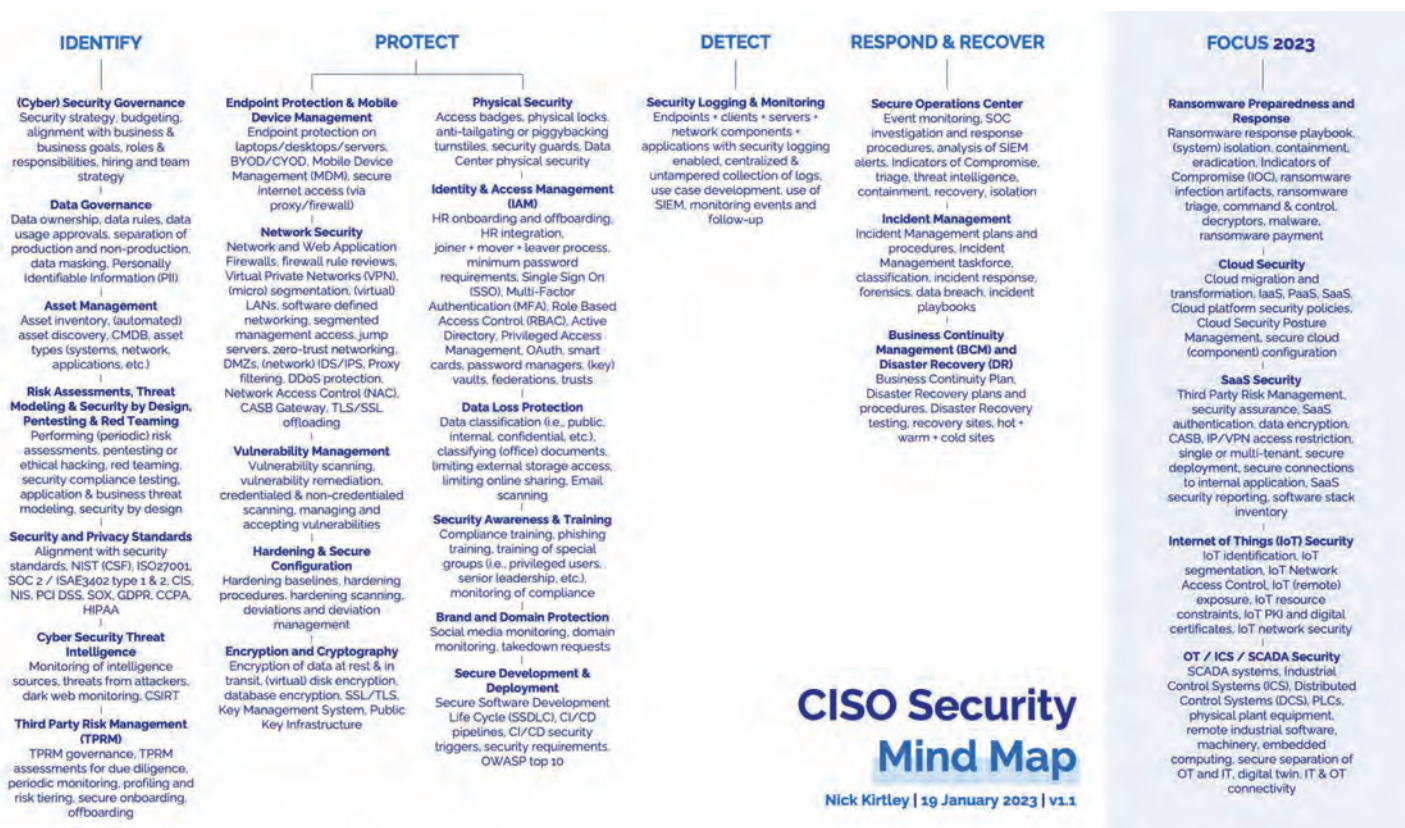
TelekomSlovenije
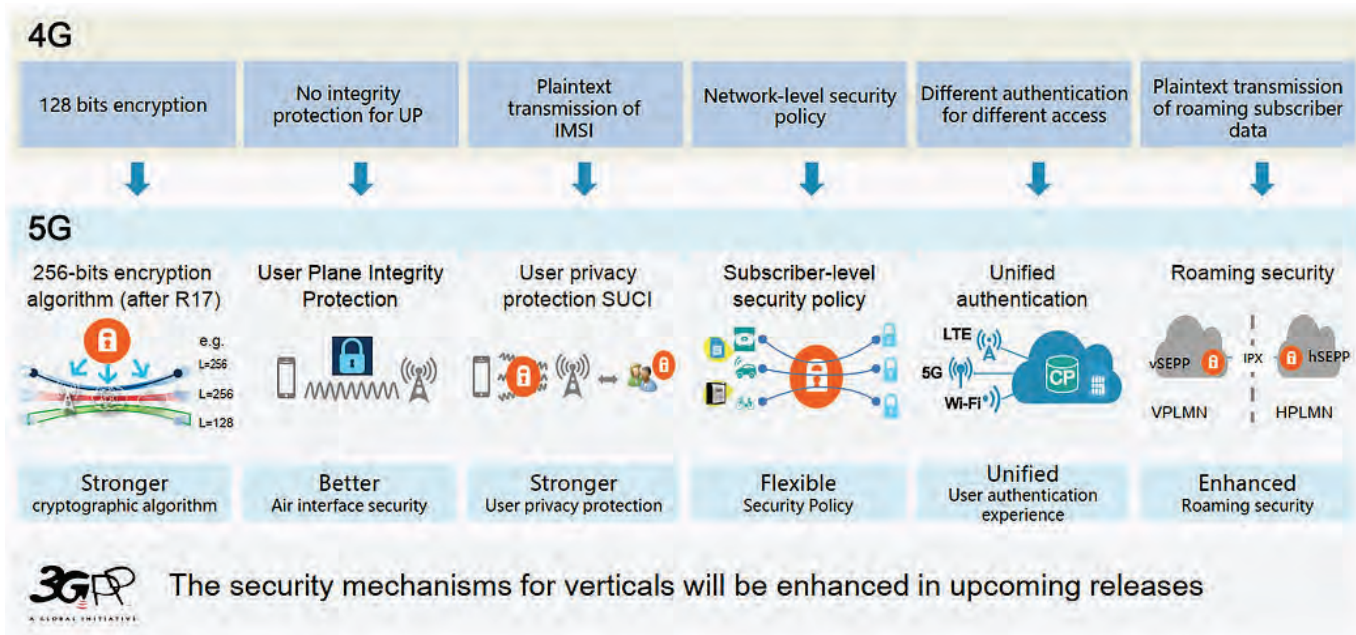

4   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije

CISO Security Mind Map

Nick Kirtley | 19 January 2023 | v1.1

The security mechanisms for verticals will be enhanced in upcoming releases

5G v javnih in zasebnih oblačno zasnovanih omrežjih

Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij   **TelekomSlovenije**

Stanje mobilnih omrežij v svetu: javna in zasebna 4G/5G NSA/SA

249 operators have launched commercial public 5G services, in 97 countries and territories

As of end of February 2023, GSA's data showed:

- **523** operators in **155** countries and territories have been investing in 5G networks in the form of tests, pilots, licence acquisitions, planned and actual deployments
- Of those, **249** operators in **97** countries and territories have launched commercial 3GPP-compatible 5G services (mobile or fixed wireless access), which includes **10** operators that have soft-launched networks
- **115** operators are identified as investing in standalone 5G for public networks (including those evaluating or testing, piloting, planning or deploying as well as those that have launched standalone 5G networks). GSA has catalogued **40** operators as having deployed, launched or soft-launched standalone 5G in public networks

Vir: gsacom.com

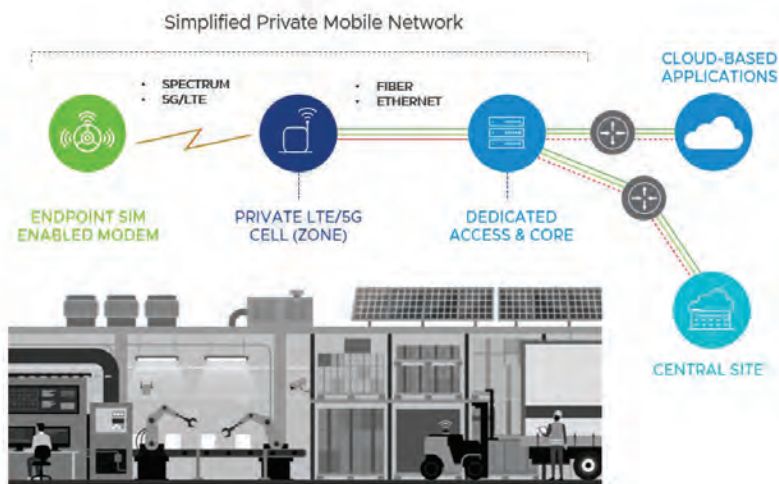Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij   **TelekomSlovenije**

Mobilna zasebna omrežja 4G/5G
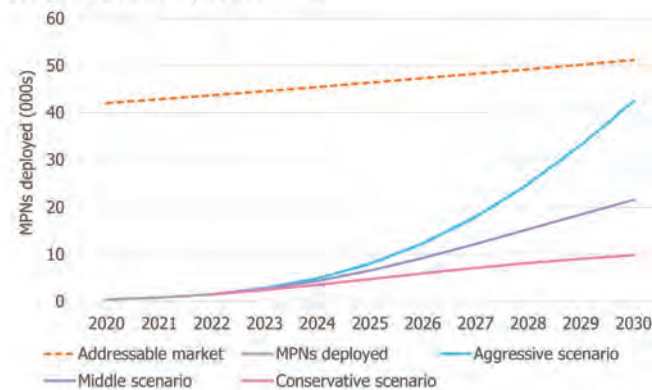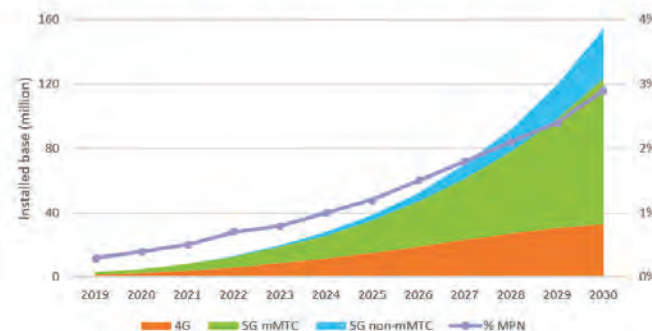
9   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

Podpora in sobivanje 4G, 5G NSA in 5G SA do 2030
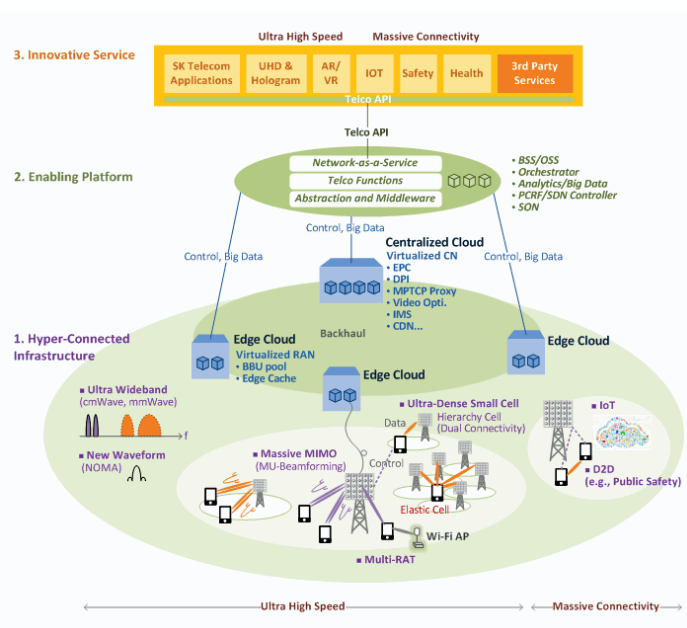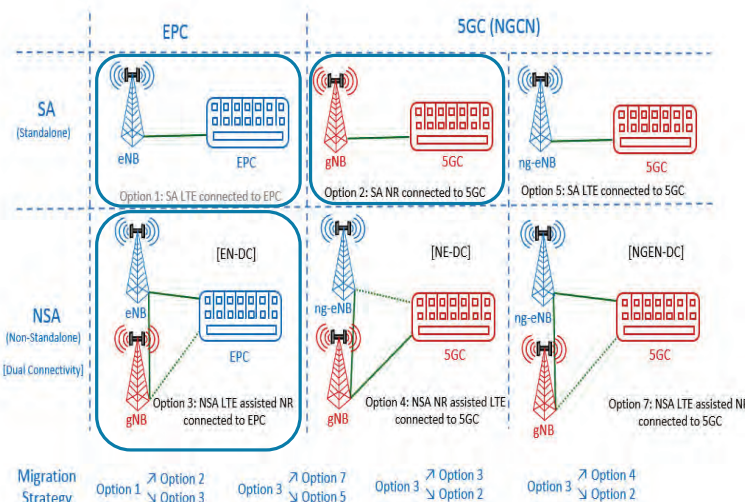
10   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

Oblačno zasnovana 5G omrežja

Izzivi uvajanja 5GC

- Poslovni
- Tehnični
- Regulatorni
- Varnostni

"Cloud-native" trendi

- Cloud Computing
  - Sistem, ki ponuja IT vire na zahtevo (infrastruktura, shranjevanje, baze podatkov, aplikacijske storitve) preko interneta

- Cloud Native
  - Je vzorec SW arhitekture za razvoj aplikacij z uporabo osnovnih principov "cloud computing" kot je skalabilnost, elastičnost in agilnost

Status uvajanja 5GC tehnologije: raziskava 138 operaterjev (TM F)

Status uvajanja 5GC

Nismo še uvedli 5G ne v RAN ne v jedru	32%
Uvedli smo 5G RAN, glede jedra se še odločamo	14%
Uvedli smo 5G RAN, 5G jedro uvedemo v 12-24 mesecih	17%
Uvedli smo 5G RAN, 5G jedro uvedemo v 12 mesecih	18%
5G jedro smo že uvedli	19%

- 150 operaterjev v svetu uvaja 5G SA tehnologijo, kar predstavlja cca 85% industrije (po prihodkih), sicer pa le 25% vseh operaterjev
- Velika večina ostaja na 5G NSA, ki temelji na 4G

Migracijske strategije

Vse 5G NSA funkcije bodo takoj migrirane	16%
Samo nekatere obstoječe 5G NSA funkcije bodo migrirane	30%
Ne bo migracije, 5GC bo deloval vzporedno	24%
Vse storitve planiramo migrirati na 5GC	12%
Migracijske strategije ne bomo odločili, dokler ne vzpostavimo novega 5GC	40%

Glavni razlogi za usmeritev v oblačno zasnovana ("cloud-native") omrežja

What are the main drivers in your organization for the push towards cloud-native networks?
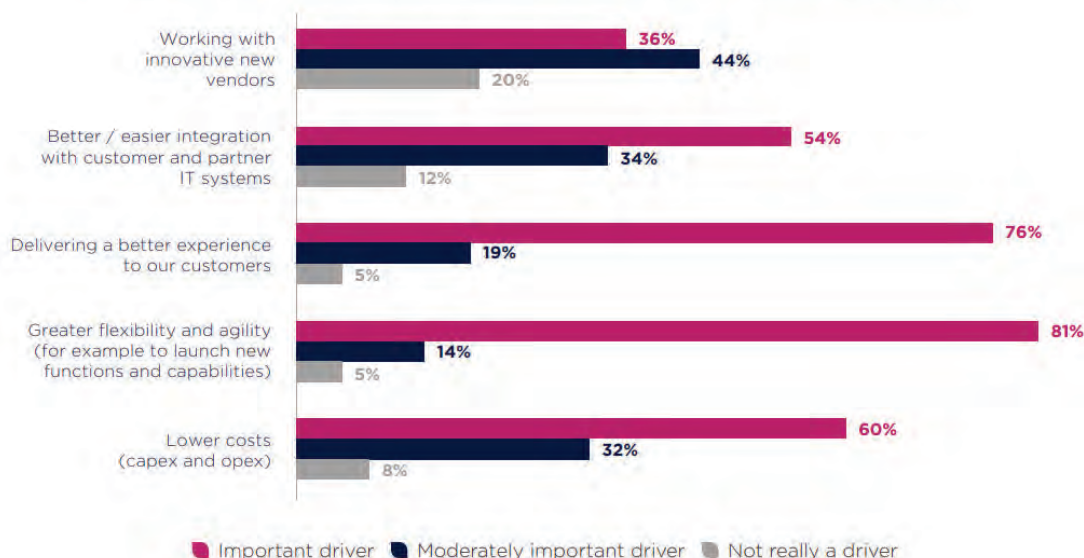
> The main drivers towards cloud-native networks are greater flexibility and agility and delivering a better experience to customers.
>
> inform.tmforum.org

TM Forum, 2022

Glavni izzivi pri uvajanju oblačno zasnovanih ("cloud-native") omrežij

What are the main challenges to adopting cloud-native networks?
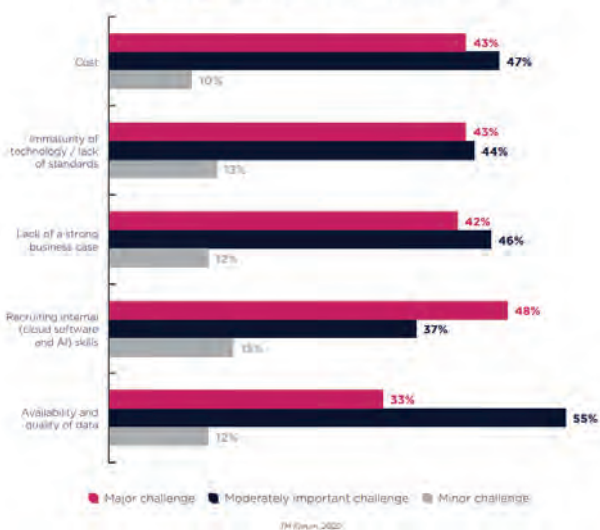
How do you expect to deploy network slicing?
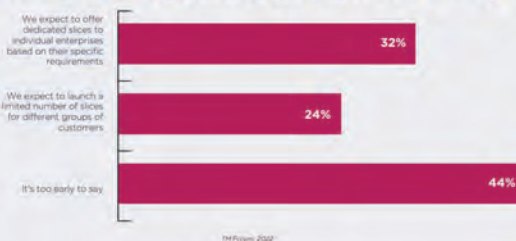
Which vendors / approach do you expect to take to your 5G Core network deployment?
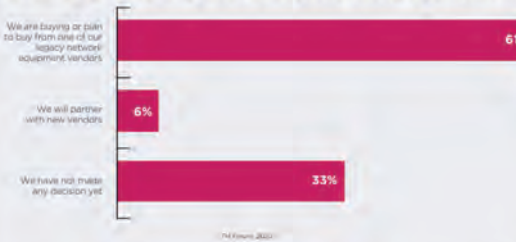
> The 5G Core is implemented as microservices, which allow network resources to be scaled up and down on-demand to suit the needs of individual services or users.

Paleta groženj s katerimi se soočajo 5G omrežja

Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije

Kaj ogroža delovanje 5G omrežij?

Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije

ENISA threat landscape for 5G networks

Zasnova omrežja 5G in ahitektura

- NSA/SA; RAN, CORE; glavne funkcionalnosti; razvoj 3GPP
- Elementi jedrnega omrežja; rezinjenje in izolacija rezin
- Primeri uporabe; model zaupanja
- Varnostna shema; življenjski cikel

Ranljivosti 5G

- Core-SBA: 19 skupin ranljivosti
- Rezinjenje: 7 skupin ranljivosti
- RAN: 13 skupin ranljivosti
- MANO: 7 skupin ranljivosti
- SDN: 7 skupin ranljivosti
- MEC: 10 skupin ranljivosti
- Fizična infrastruktura: 6 skupin ranljivosti
- Ostalo: 35 skupin ranljivosti

Viri in grožnje

- Klasifikacija virov: organizacija, procesi, storitve, povezave, podatki, protokoli
- Zemljevid groženj – SCAS STRIDE model
- Tipi groženj – grožnje – potencialni vpliv – prizadeti viri
- Agenti groženj: kiber-kriminalci, insajderji, države, aktivisti, teroristi, korporacije, nadebudneži

Zaključki in priporočila

- ENISA EU akcijski načrt
- Standardi
- Znanje in izkušnje; ISO 27005

17   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij
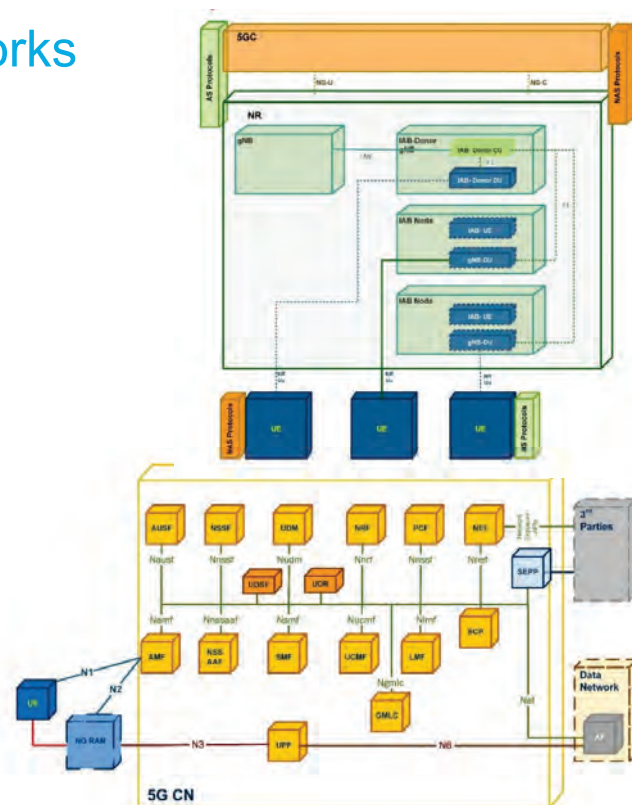
Varnost v 5G standardih
Kontrole v 3GPP varnostnih specifikacijah (5G SA)

TelekomSlovenije

Varnostne specifikacije 3GPP za 5G

Standardizacijske organizacije relevantne za 5G varnost

Varnostna arhitektura in procedure za 5G system

Glavne varnostne funkcije

Ostali varnostni vidiki

Zaključki

The Network Equipment Security Assurance Scheme (NESAS), jointly defined by 3GPP and GSMA, provides an **industry-wide security assurance framework** to facilitate improvements in security levels across the mobile industry

NESAS defines 1) **security requirements and an assessment framework** for *secure product development and product lifecycle processes*; and 2) **security evaluation schemes** for *network equipment,* using 3GPP defined security test cases, i.e. 3GPP SCAS – Security Assurance Specifications

19   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije

Varnostne specifikacije 3GPP za 5G

20   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije
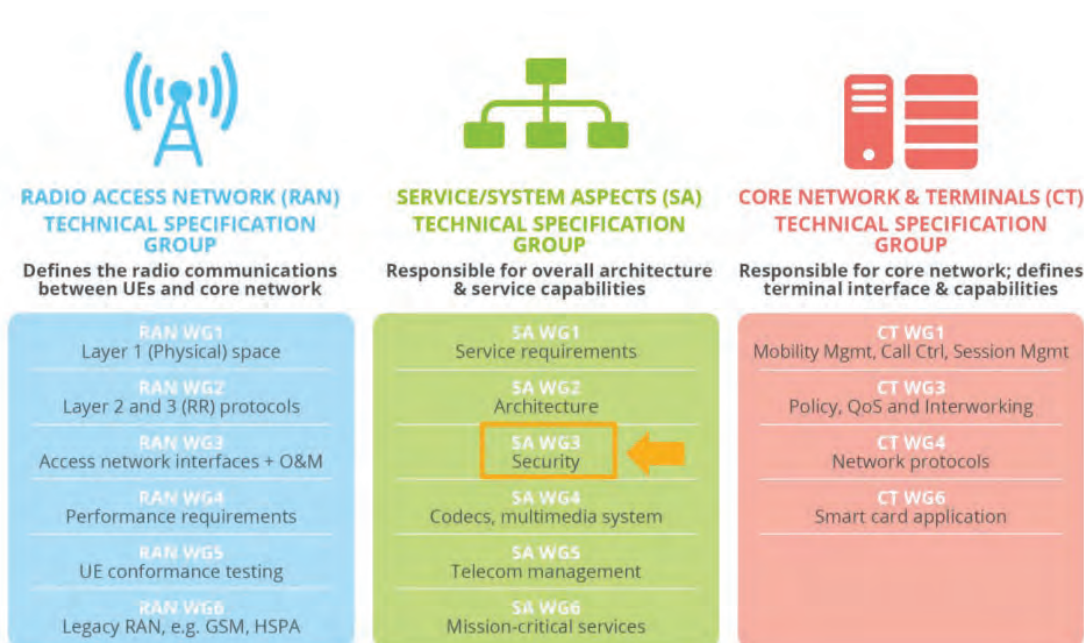
5G varnost v ETSI in ITU-T
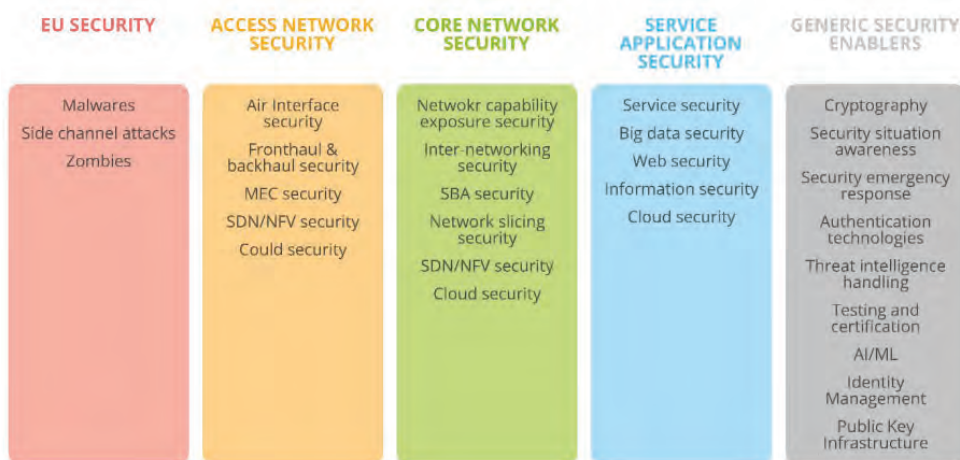
Varnostne specifikacije 3GPP za 5G

Model varnostne arhitekture 3GPP TS 33.501
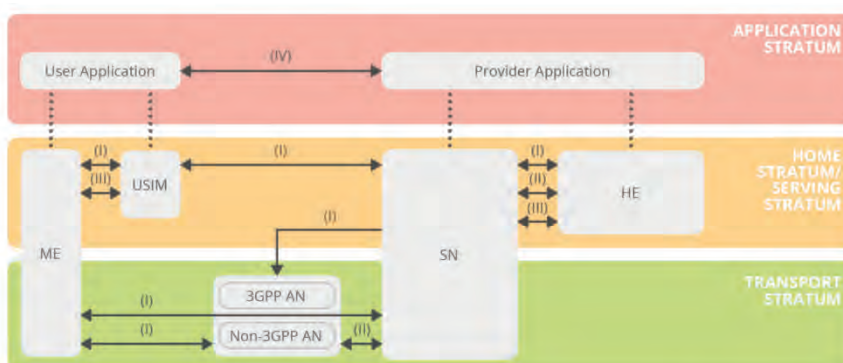
- **Network access security (I)** – security features that enable a user terminal to authenticate and access the network by providing protection on the radio interfaces.
- **Network domain security (II)** - security features that enable network nodes to exchange signalling and user data securely.
- **User domain security (III)** - security features that enable the secure user access to mobile devices.
- **Application domain security (IV)** - security features that enable user and provider domain applications to exchange messages securely. 33.501 specifications do not cover application domain security.
- **Service Based Architecture (SBA) domain security (V)** - a new set of security features that enable network functions of the SBA to communicate securely within serving and other network domains.
- **Visibility and configurability of security (VI)** - security features that enable the user to be informed regarding which security features are in operation or not.

Varnostne specifikacije 3GPP za 5G

- Zasebnost uporabnikov – zaščita identifikacij
- Zaščita uporabniških in signalizacijskih podatkov - zaščita zaupnosti (NEA) in integritete (NIA)
- Zaščita vzpostavitve in konfiguracije gNB
- Zaščita RAN vmesnikov (CU-DU; N2 in N3)
- Zaščita SBA (RESTful preko HTTP/2 TLS, OAuth 2.0) – zaščita na omrežnem transportnem nivoju, avtentikacija, avtorizacija, skrivanje topolgije
- Avtentikacijski okvir – primarna in sekundarna avtentikacija
- Varnost za gostovanje (roaming) – SEPP med operaterji
- Varno shranjevanje – v napravah (UE), v gNB, v 5GC
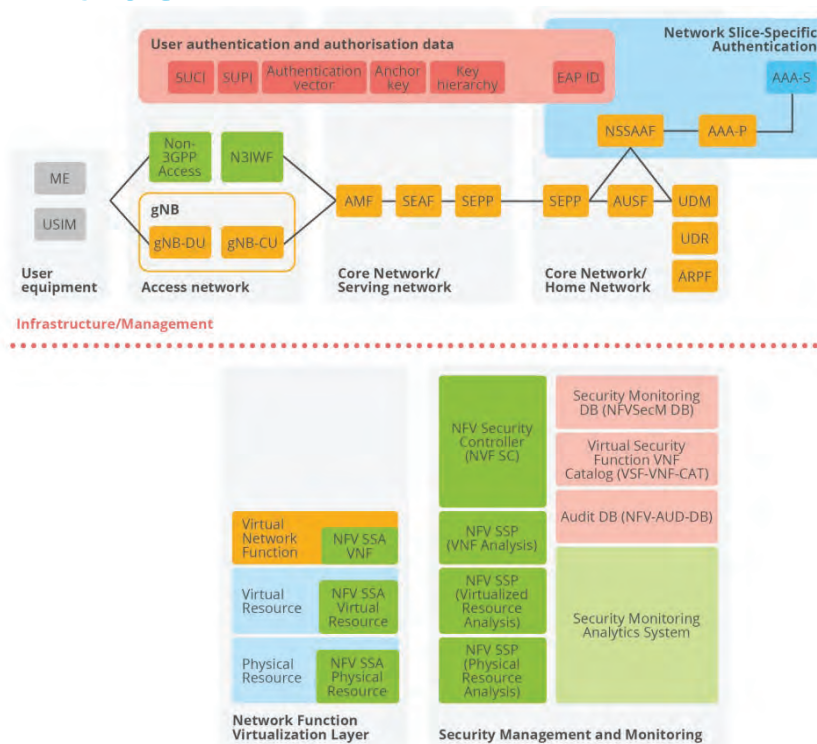
TelekomSlovenije

Ostali varnostni vidiki

- D1: Governance and risk management
- D2: Human resources security
- D3: Security of systems and facilities
- D4: Operations management
- D5: Incident management
- D6: Business continuity management
- D7: Monitoring, auditing and testing
- D8: Threat awareness

TelekomSlovenije

Zaključki - priporočila

UE mora šifrirati SUPI/SUCI in tako mora biti na celi poti preko omrežja (ECIES)

Zaščita podatkov pred prestrezanjem ali spreminjanjem (>128-NEA1& 128-NIA1) UE – omrežje

Varen protocol omrežja-transporta (IPSec ali DTLS) za CIR za oba tipa prometa na RAN vmesnikih

Zaščita SBA vmesnikov med VNF/CNF (zaščita prenosa in vzajemna avtentikacija – TLS1.3, X.509 certifikati; Oauth2.0

Zaščita avtentikacij (prim/sec) z eksternimi omrežji; SEPP, TLS in varno shranjevanje (UICC, HSM)

TelekomSlovenije

NFV varnost v 5G

Izzivi in dobre prakse

TelekomSlovenije

Varnostni okvir 5G NFV

E2E arhitektura
NFV arhitektura
NFV z SDN vlogami
Akterji 5G NFV
Varnostne priložnosti NFV
Glavne NFV tehnologije
Modeli uvajanja NFV
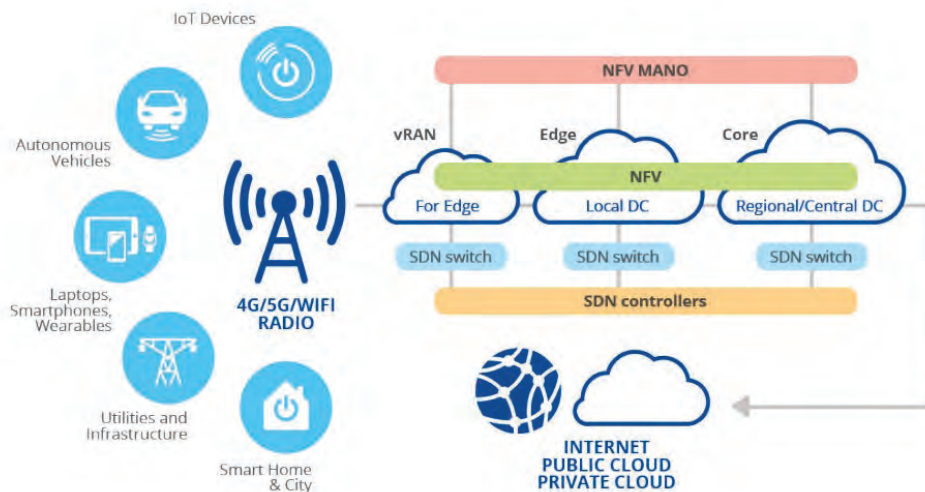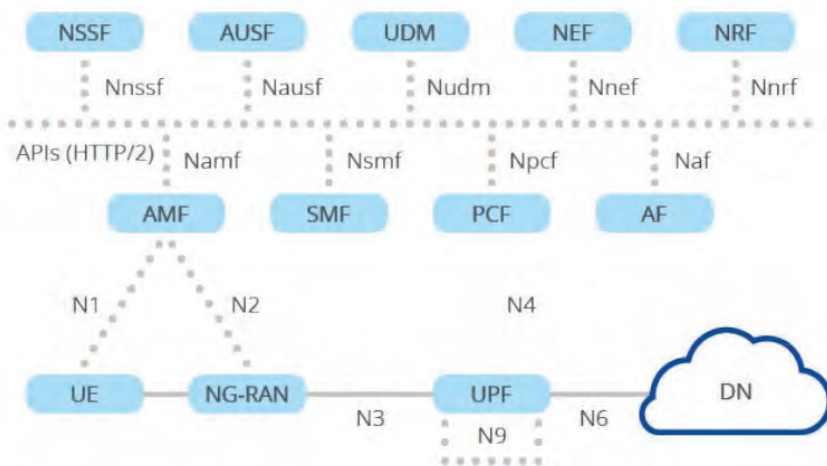
27   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije

Varnostni okvir 5G NFV: SBA

28   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije

Varnostni okvir 5G NFV: varnostne funkcije 5G omrežja
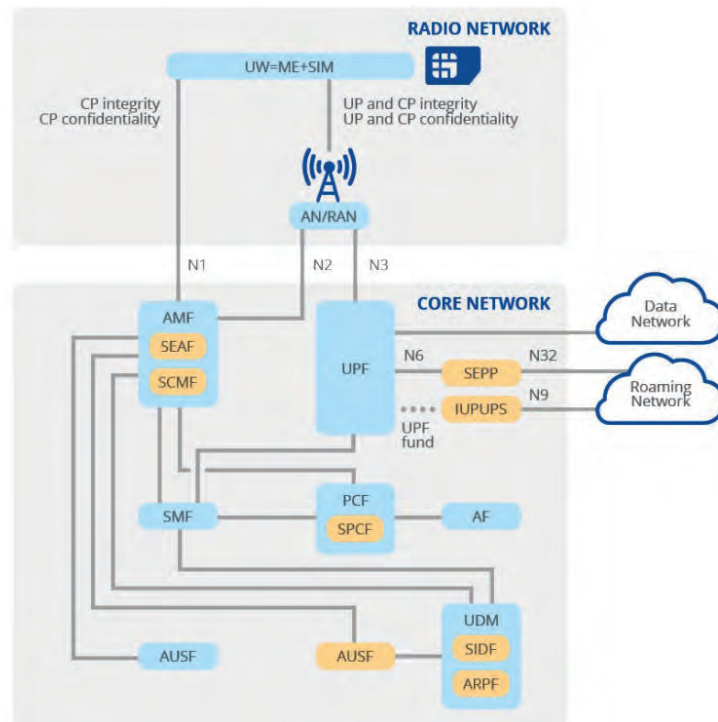
29   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

Varnostni okvir 5G NFV: NFV arhitektura
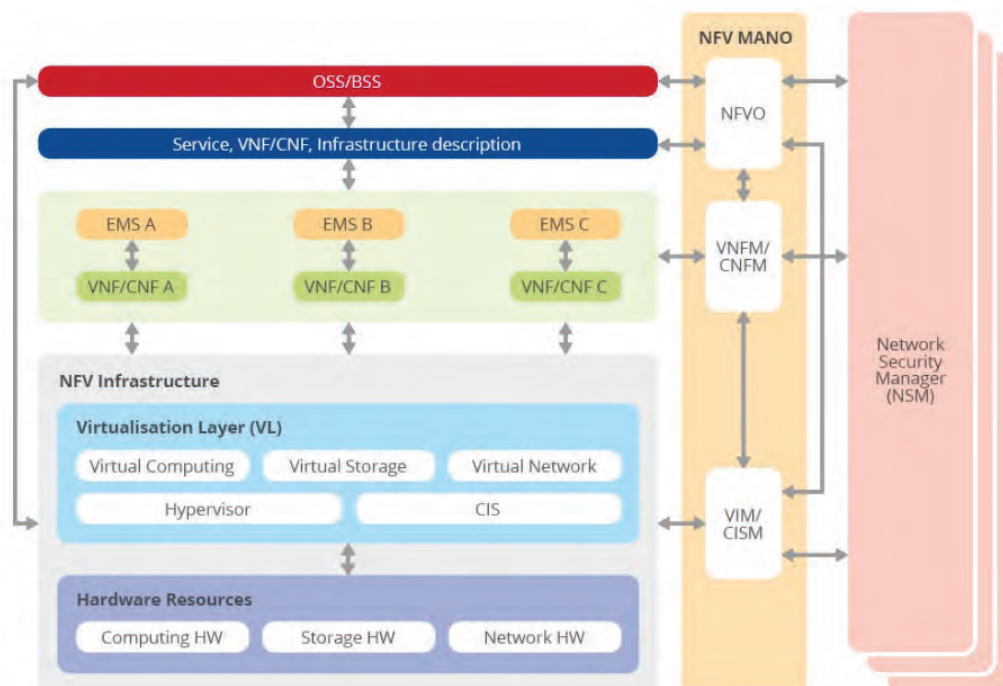
30   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

Varnostni okvir 5G NFV: NFV z SDN vlogami

31   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij
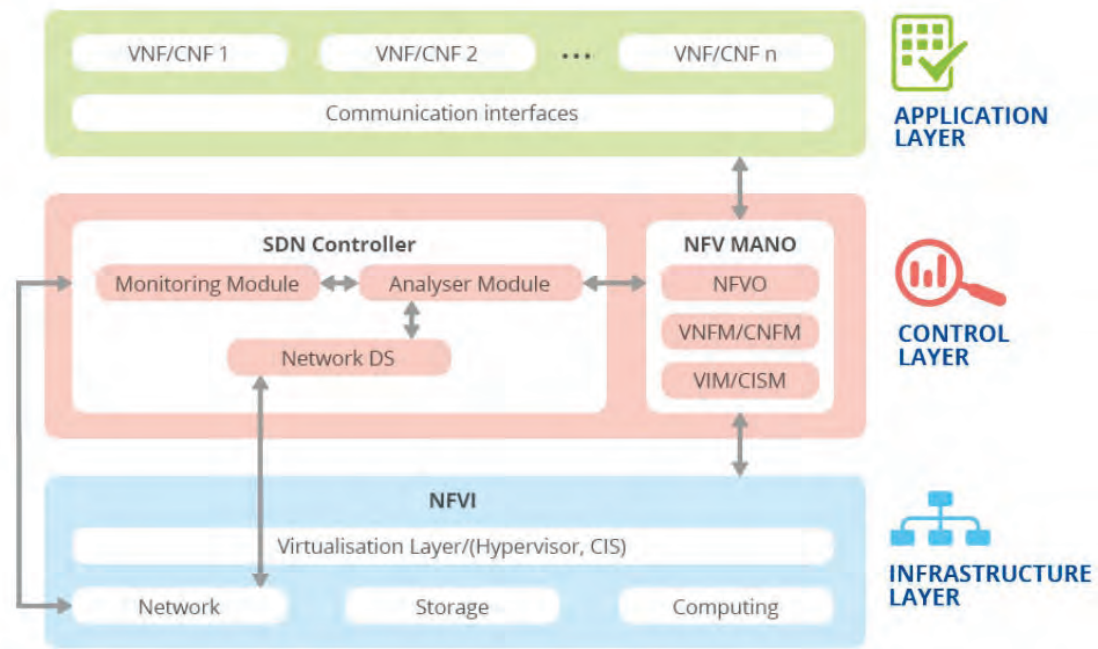
Varnostni okvir 5G NFV: virtualizacija in kontejnerizacija

32   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij
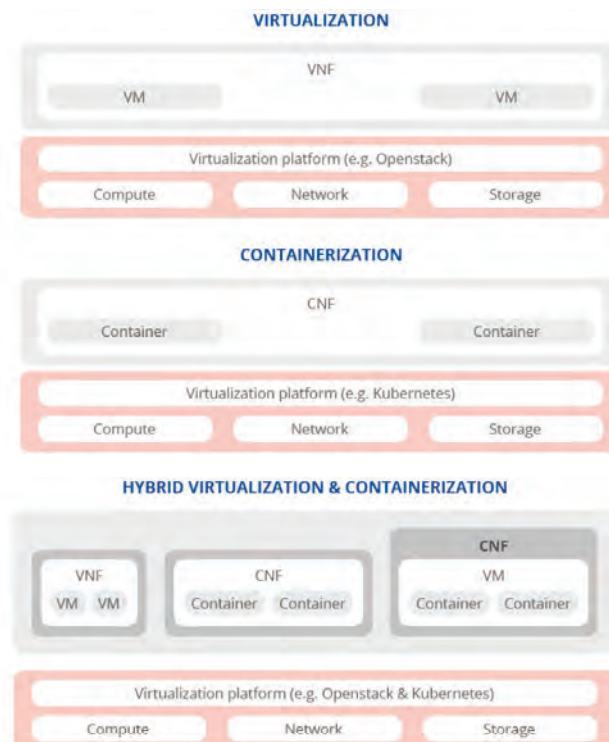
Varnostni okvir 5G NFV: primerjava tehnologij virtualizacije

Feature	Virtual Machines	Containers	Unikernels
Isolation	Strong	Weak	Strong
Image size	Large	Small	Small
Instantiation (boot time)	Slow	Fast	Fast
Memory consumption (resource overhead)	High	Low	Medium
Toolset	Strong	Strong	Weak

VIRTUAL MACHINES

VM	VM
App	App
Bins/Libs	Bins/Libs
OS+Kernel	OS+Kernel

Hypervisor

Hardware

CONTAINERIZATION

Container	Container
App	App
Bins/Libs	Bins/Libs

OS+Kernel

Hardware

UNIKERNELS

VM	VM
App	App
Bins/Libs	Bins/Libs
Kernel	Kernel

Hypervisor

Hardware

33   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije
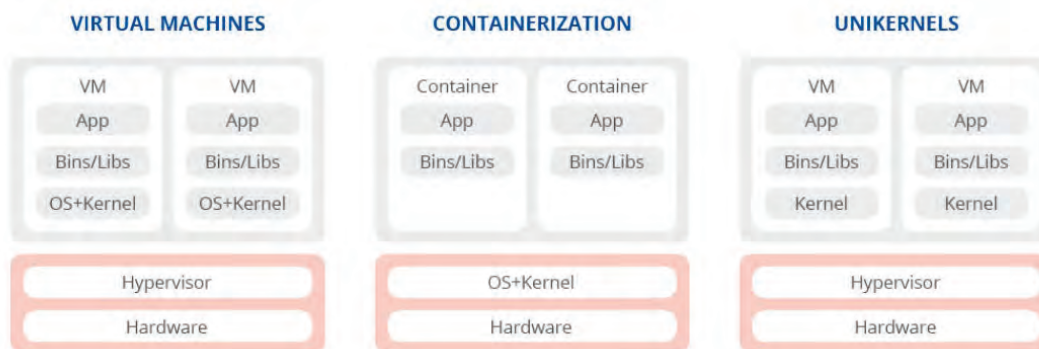
Varnostni okvir 5G NFV: načini uvedbe

SINGLE OPERATOR ENVIRONMENT–PRIVATE CLOUD

VNFs/CNFs/Applications
Hypervisor/CIS
Host OS
Hardware resources (Compute, Storage, Network)

MANO
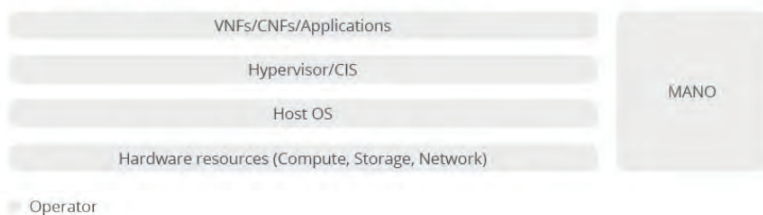
Operator

OPERATOR HOSTING VIRTUAL NETWORK OPERATORS–PRIVATE CLOUD

VNFs/CNFs/Applications
Hypervisor/CIS
Host OS
Hardware resources (Compute, Storage, Network)

MANO

Operator   Virtual Operator(s)
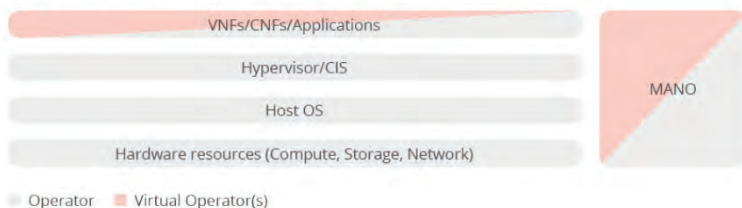
THIRD PARTY HOSTING SCENARIO 1–HYBRID CLOUD

VNFs/CNFs/Applications
Hypervisor/CIS
Host OS
Hardware resources (Compute, Storage, Network)

MANO

Operator   Cloud Provider
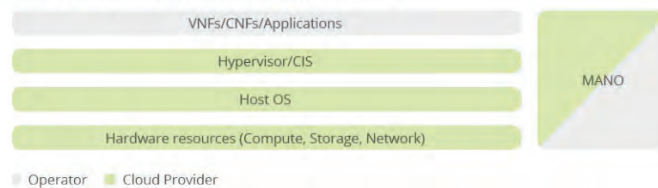
THIRD PARTY HOSTING SCENARIO 2–COMMUNITY CLOUD

VNFs/CNFs/Applications
Hypervisor/CIS
Host OS
Hardware resources (Compute, Storage, Network)

MANO

Cloud Provider   Operator 1   Operator 2
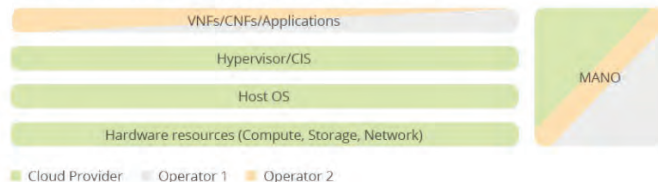
THIRD PARTY HOSTING SCENARIO 3–PUBLIC CLOUD

VNFs/CNFs/Applications
Hypervisor/CIS
Host OS
Hardware resources (Compute, Storage, Network)

MANO

Cloud Provider   Operator(s)   Service provider(s)

34   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij

TelekomSlovenije
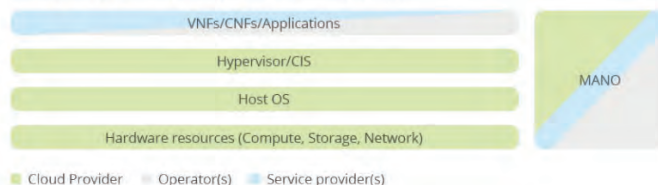
Varnostni okvir 5G NFV: načini uvedbe (primerjava)

Deployment model	Hardware	Virtualisation layer (Host OS, Hypervisor, CIS)	VNFs/Appl ications	MANO	Location	Cloud Type	Suitable for
Single operator environment	Operator	Operator	Operator	Operator	On premise	Private Cloud	Core
Operator hosting virtual network operators	Operator	Operator	Operator, Virtual Operator (s)	Operator, Virtual Operator (s)	On premise	Private Cloud	Core, MEC, RAN
Third party hosting – scenario 1	Cloud Provider	Cloud Provider	Operator	Cloud Provider, Operator	Vendor Locations	Hybrid Cloud	Core, MEC, RAN
Third party hosting – scenario 2	Cloud Provider	Cloud Provider	Operators	Cloud Provider, Operators	Vendor Locations	Community Cloud	MEC, RAN
Third party hosting – scenario 3	Cloud Provider	Cloud Provider	Operators, Service Providers	Cloud Provider, Operators, Service Providers	Vendor Locations	Public Cloud	MEC
Operator hosting third party service providers	Operator	Operator	Operator, Service Providers	Operator, Service Providers	On Premise	Edge Cloud	MEC

35   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij   **Telekom**Slovenije

5G NFV: viri, izzivi, ranljivosti in scenariji napadov

- 34 varnostnih izzivov glede virtualizacije/kontejnerizacije
- 4 varnostni izzivi glede orkestracije in upravljanja (MANO)
- 6 varnostnih izzivov glede administracije in kontrole dostopa
- 4 varnostni izzivi glede mešanja obstoječih in novih tehnologij
- 2 varnostna izziva glede odprtokodnih rešitev in COTS
- 6 varnostnih izzivov glede dobavne verige
- 4 varnostni izzivi glede legalnega prestrezanja

SECURITY CHALLENGES

Virtualization/ Containerization — Orchestration and management — Administration and access control — New and legacy technologies — Adoption of open source/ COTS — Supply chain — Lawful interception (LI)

36   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij   **Telekom**Slovenije

5G NFV: viri, izzivi, ranljivosti in scenariji napadov

TelekomSlovenije

5G NFV: dobre prakse glede varnosti

Kategorizacija varnostnih ukrepov

Varnostne zahteve in ukrepi of the EECC

Ostale relevantne smernice varnostnih utrjevanj

Povezava med kategorijami izzivov, kategorijami ranljivosti, napadi, prizadeti viri in dobre prakse

TelekomSlovenije

5G NFV: dobre prakse glede varnosti

BEST PRACTICES

Organisational
- BP-O1 Secure Physical Environment and Geographical location
- BP-O2 Training and awareness
- BP-O3 Trust model
- BP-O4 SLAs establishment

Policy
- BP-P1 Zero Trust
- BP-P2 Security Assessment of new or changes to existing VNF/CNF Service Templates
- BP-P3 Vulnerability handling & patch management
- BP-P4 Security testing and assurance
- BP-P5 Incident management
- BP-P6 Secure Update Management
- BP-P7 Restriction on installing applications
- BP-P8 Defense in depth
- BP-P9 String password policy
- BP-P10 Secure supply chain
- BP-P11 Resources inventory management system and database
- BP-P12 Apply hardening policies
- BP-P13 Multi-vendors segregation and trust
- BP-P14 Security by design
- BP-P15 Life cycle management
- BP-P16 Software Bill Of Materials (SBM)

Technical
- BP-T1 Security monitoring and filtering
- BP-T2 VNF/CNF Image validation and protection
- BP-T3 Tracking VNF/CNF version changes
- BP-T4 VNF/CNF deployment
- BP-T5 VNF/CNF detection or relocation
- BP-T6 Cryptography
- BP-T7 Hypervisor protection
- BP-T8 Security Management and orchestration
- BP-T9 remote attestation
- BP-T10 Software compliance and integrity preservation
- BP-T11 Security segmentation and isolation between network functions
- BP-T12 Secure boot integrity
- BP-T13 data protection and privacy
- BP-T14 Encrypting VNF/CNF Volume/swap Areas
- BP-T15 Trusted computing technologies
- BP-T16 Hardware security
- BP-T17 Centralized log auditing
- BP-T18 Use and ownership of "root" administration credentials
- BP-T19 VNF/CNF protection
- BP-T20 Local or removal Blade Storage – SAN protection
- BP-T21 Network security
- BP-T22 SDN security management
- BP-T23 MANO access control and management
- BP-T24 VIM/CISM connectivity to Hypervisor/CIS
- BP-T25 Recovery and reinstallation
- BP-T26 Deploying VMs/Containers of differing trust levels
- BP-T27 Orchestration platform security management
- BP-T28 Trusted time source
- BP-T29 Secure 3rd party hosting environments
- BP-T30 Redundancy and backup
- BP-T31 Specific container security controls
- BP-T32 OSS/BSS protection
- BP-T33 LI capabilities
- BP-T34 User plane security
- BP-T35 MEC security

39   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij   **Telekom**Slovenije

Odprti prihodnji varnostni izzivi in zaključki

- Previsoka stopnja centralizacija upravljanja
- Uporaba standardiziranih splošnih strežnikov in pomnilnikov ter odprtokodnih rešitev
- Veliko število partnerjev in dobaviteljev, kompleksne dobavne verige
- SW ranljivosti v NFV okolju
- 5G NFV varnostna arhitektura mora biti decentralizirana – vsaj na jedro in rob
- Vidljivost omrežja
- Hitrejši razvoj varnostnih standardov 5G, certifikacije in izmenjava dobrih praks

40   Varnostni izzivi in dobre prakse upravljanja 5G omrežij na osnovi oblačnih tehnologij   **Telekom**Slovenije

Ključni viri

TM Forum:	5G Core, exploring CSP approaches
TM Forum:	5G Future - Targeting the enterprise
ENISA:	Threat landscape for 5G networks
ENISA:	NFV security in 5G
ENISA:	Securit in 5G specifications
Gigi Sayfan:	Mastering Kubernetes
GSA:	5G public and private networks reports
GSMA:	NESAS
CNCF:	Cloud Native computing Foundation

Oblačno zasnovana zasebna omrežja 5G – tehnološka, operativna in poslovna rešitev za vitka in agilna podjetja

Cloud-based private 5G networks – technological, operational and business solutions for lean and agile companies

Urban Zaletel, Ana Robnik, Robert Zlatanov, Janez Öri

S&T Iskratel

POVZETEK

Današnja sodobna podjetja imajo vse večje zahteve v zvezi s povezljivostjo. Nastajajoče aplikacije in industrijska okolja zahtevajo večjo pasovno širino, predvsem pa izjemno nizko zakasnitev, več spektra in večjo zanesljivost. Z dodeljevanjem namenskega spektra za ta okolja s strani regulatorjev (Nemčija, Norveška, Združeno kraljestvo in druge napredne države) so nastali pogoji za uvajanje zasebnih mobilnih omrežjih v podjetjih, ki so samostojna in razširjajo njihova obstoječa brezžična omrežja za primere uporabe, ki zagotavljajo namenski dostop do omrežja. Oblačno zasnovana omrežja podjetjem omogočajo učinkovito upravljanje in pomagajo pri sprejemanju hitrejših in boljših poslovnih odločitev. Podjetje S&T Iskratel se je pred tremi leti odločilo razviti lastno 5G jedro kot del celovite 5G rešitve, s katero ponuja podjetjem visokokakovostno industrijsko omrežje za njihovo digitalno preobrazbo. Za hitro uvajanje sodobnih primerov uporabe in potreb v zvezi z razširljivostjo je pri snovanju svoje rešitve uporabilo koncept oblačno zasnovanega omrežja, ki omogočaj 5G jedru izkoristiti poln potencial. Uspešno je postavilo 5G jedro tako na javno kot tudi zasebno oblačno infrastrukturo, kar je omogočilo izjemno gibkost in skalabilnost ne le lastnega jedra, ampak celotne 5G rešitve. Z uporabo oblačne infrastrukture se 5G rešitev odlično prilagajajo potrebam in zahtevam strank ter s tem zagotovijo optimalno izkušnjo uporabnikov. Postavitev 5G jedra na oblačni infrastrukturi omogoča tudi učinkovitejše izkoriščanje virov ter večjo varnost in zanesljivost celotnega omrežja. V prispevku bomo naslovili motivacijo prehoda na oblačno nativno arhitekturo in pridobljene izkušnje, ki smo jih pridobili ob razvoju in uvajanju oblačno zasnovanih rešitev. Izpostavili bomo težave in izzive, s katerimi so se soočali inženirji. Nanizali bomo številne pridobljene kompetence, ki jih S&T Iskratel ponuja tudi svojim strankam v obliki profesionalnih storitev.

SUMMARY

Today's modern businesses have increasing connectivity requirements. Emerging applications and industrial environments require greater bandwidth, particularly extremely low latency, more spectrum, and greater reliability. By allocating dedicated spectrum for these environments by regulators (Germany, Norway, the United Kingdom, and other advanced countries), conditions have been created for the introduction of private mobile networks in companies that are independent and extend their existing wireless networks for use cases that provide dedicated network access. Cloud-based networks enable companies to efficiently manage and help make faster and better business decisions. Three years ago, S&T Iskratel decided to develop its own 5G core as part of a comprehensive 5G solution, offering high-quality industrial networks for digital transformation. To quickly introduce modern use cases and scalability requirements, it used the concept of a cloud-based network that enables the 5G core to realize its full potential. It has successfully deployed the 5G core on both public and private cloud infrastructure, enabling exceptional flexibility and scalability not only for its own core but for the entire 5G solution. Using cloud infrastructure, 5G solutions can be tailored to the needs and demands of customers, providing an optimal user experience. Deploying the 5G core on cloud infrastructure also enables more efficient resource utilization, greater security, and reliability of the entire network. In this talk, we will address the motivation for transitioning to a cloud-native architecture and the experiences gained in developing and deploying cloud-based solutions. We will highlight the problems and challenges that engineers faced and list the numerous competences that S&T Iskratel also offers its customers in the form of professional services.

O AVTORJIH

Urban Zaletel je vodja oddelka za razvoj pete generacije mobilnih omrežij v S&T Iskratel. V zadnjih desetih letih je bil v različnih vlogah in pridobljene izkušnje pridoma uporablja pri implementaciji strategije v vseh ekipah podjetja, vključno z marketingom in produktnim vodenjem. Je tudi organizator največje tehnološke konference za Oracle tehnologije (Java, APEX, podatkovne baze, …).

Ana Robnik je svetovalka za raziskave in strateški razvoj, koordinira delo v standardizacijskih organizacijah in sodeluje v raziskovalnih in inovacijskih projektih podjetja Iskratel. Svojo poklicno pot je po univerzitetnem študiju uporabne matematike na Fakulteti za matematiko, fiziko in mehaniko Univerze v Ljubljani in opravljenem magisteriju iz računalništva na Fakulteti za računalništvo Univerze v Ljubljani nadaljevala v razvojno raziskovalni enoti Iskra Kibernetika, nato pa v IT-oddelku Iskratela in do leta 2009 vodila sektor za telemanagement. S prehodom v pisarno tehničnega direktorja je razširila svoje področje delovanja na domene energetike, transporta in javne varnosti in rabo omogočitvenih tehnologij 5G, oblaka, industrijskega IoT in umetne inteligence. Je spodbujevalka STEM poklicev, nominiranka za inženirko leta 2019 in inovatorka leta 2021 v podjetju. Koordinira vertikalo Varnost v Strateškem razvojnem inovacijskem partnerstvu Pametna mesta in skupnosti.

Robert Zlatanov je po zaključeni Srednji elektro in strojni šoli v Kranju, nadaljeval s študijem na Ekonomski fakulteti v Ljubljani na smeri Poslovna informatika ter ga uspešno zaključil z magisterijem na področju Informacijsko-upravljalskih ved. V S&T Iskratelu je že skoraj desetletje odgovoren za produktni marketing za digitalne rešitve v raznih industrijskih vertikalah kot so transport, energetika in javna varnost. Aktivno sodeluje tudi pri korporativnem marketingu, strategiji in produktnem vodenju tako pri komunikacijskih, kot sodobnejših rešitvah v sklopu 5G ekosistema. Kot vodja poslovno-referenčnega centra je pridobljena informacijsko-telekomunikacijska znanja nadgradil tudi z domenskimi znanji zgoraj omenjenih zgoraj sektorjev kritične infrastrukture.

Janez Öri je v S&T Iskratel odgovoren za program Zasebna mobilna omrežja. Na več kot 20-letni profesionalni poti v telekomunikacijski industriji je delal na različnih delovnih mestih, začenši z raziskavami in razvojem v Iskratelu, razvojem tehničnih rešitev na področju IP in širokopasovnih omrežij za stranke v podjetjih Cisco in Iskratel ter vodil skupine za produktno vodenje, razvoj poslovanja in trženje ter strateški razvoj. V zadnjih letih soustvarja strategijo za preoblikovanje iz klasičnega ponudnika telekomunikacijskih produktov in rešitev v ponudnika celovitih digitalnih rešitev za različne vertikalne industrije. Diplomiral je s področja telekomunikacij/elektrotehnike na Fakulteti za elektrotehniko Univerze v Ljubljani.

ABOUT THE AUTHORS

Urban Zaletel is Head of Fifth Generation Mobile Network Development at S&T Iskratel. Over the last ten years, he has served in various roles and applies his experience in strategy implementation in all teams of the company, including marketing and product management. He is also the organizer of the largest technology conference for Oracle technologies (Java, APEX, databases, etc.).

Ana Robnik is a Research and Strategic Development Consultant, coordinates work in standardisation organisations and participates in Iskratel research and innovation projects. After completing her Bachelor's degree in Applied Mathematics at the Faculty of Mathematics, Physics and Mechanics of the University of Ljubljana and her Master's degree in Computer Science at the Faculty of Computer

Science of the University of Ljubljana, she continued her professional career in the Iskra Kibernetika research and development unit and then in the IT department of Iskratel, where she headed the telemanagement sector until 2009. Moving to the CTO's office, she expanded her scope to the domains of energy, transport and public safety, and the use of enabling technologies such as 5G, cloud, industrial IoT and artificial intelligence. She is a promoter of STEM professions, nominated as 2019 Engineer of the Year and 2021 Innovator of the Year in the company. She coordinates the Safety vertical in the Strategic Research & Innovation Partnership) for the Smart Cities and Communities.

After graduating from the High school of Electrical and Mechanical Engineering in Kranj, Robert Zlatanov continued his studies at the Faculty of Economics in Ljubljana in the field of Business Informatics and successfully completed his master's degree in information and management sciences. For almost a decade, he has been responsible for product marketing in S&T Iskratel for digital solutions in various industrial verticals such as transport, energy, and public safety. He also actively participates in corporate marketing, strategy and product management in both communication and modern solutions within the 5G ecosystem. As the head of the business reference centre, he also upgraded the acquired ICT knowledge with the domain knowledge of the above-mentioned critical infrastructure sectors.

Janez Öri is responsible for the Mobile Private Networks programme at S&T Iskratel. During his more than 20-year career in the telecommunications industry, he has worked in various roles, starting with R&D at Iskratel, developing technical solutions in IP and broadband networks for customers at Cisco and Iskratel, and leading teams in product management, business development and marketing, and strategic development. In recent years, he has been co-creating a strategy to transform from a traditional telecommunications product and solutions provider to a provider of end-to-end digital solutions for various vertical industries. He graduated in telecommunications/electrical engineering from the Faculty of Electrical Engineering, University of Ljubljana.

s&t ISKRATEL

Cloud-native 5G private networks

Technological, operational and business solution for lean and agile enterprises
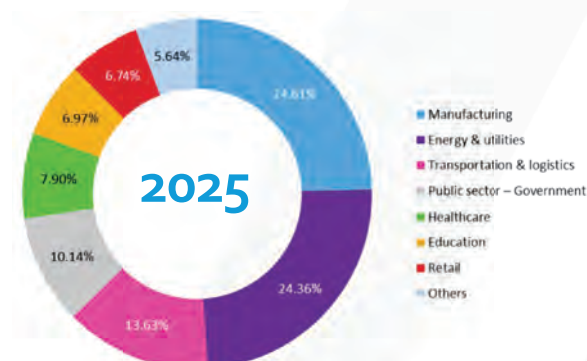
May 2023

Industry Trends

— **Investments in traditional** ICT **slowing down** — „classical" **digitalisation** used to be the main driver

— But **physical industry sectors** projected to have big **growth** in **investments** in ICT

— **Process/cost optimisation** and business agility as the **main value** preposition

99% of enterprises surveyed (by Omdia) **would take additional services**

Private networks highly demanded in:

— Manufacturing
— Energy & Utilities
— Transport & Logistics
— Mission critical communications

- Manufacturing
- Energy & utilities
- Transportation & logistics
- Public sector – Government
- Healthcare
- Education
- Retail
- Others

s&t ISKRATEL

Why & Where *5G Mobile Private Networks*

High Capacity and Low Latency network

Dedicated local private RF spectrum
(indoor and outdoor coverage).

Professional private network for wide area coverage,
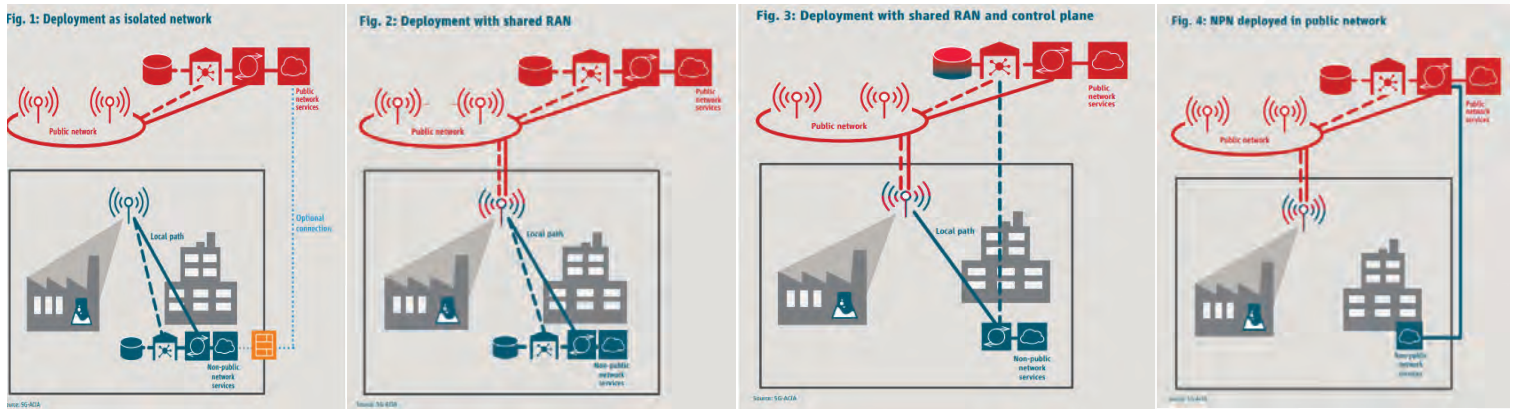reliability and high mobility
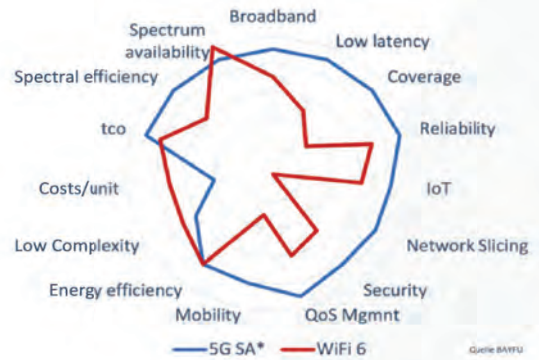
Trustfully and securely integrated on site with
corporate Information (IT) and operational (OT)
networks

Lowest TCO for wide-area
Indoor and Outdoor coverage
(> 20.000 m2)

Implementation scenarios for deploying a private network based on spectrum and RAN ownership

Standalone NPN isolated   NPN with shared RAN   NPN with shared RAN & Core   NPN hosted by public network
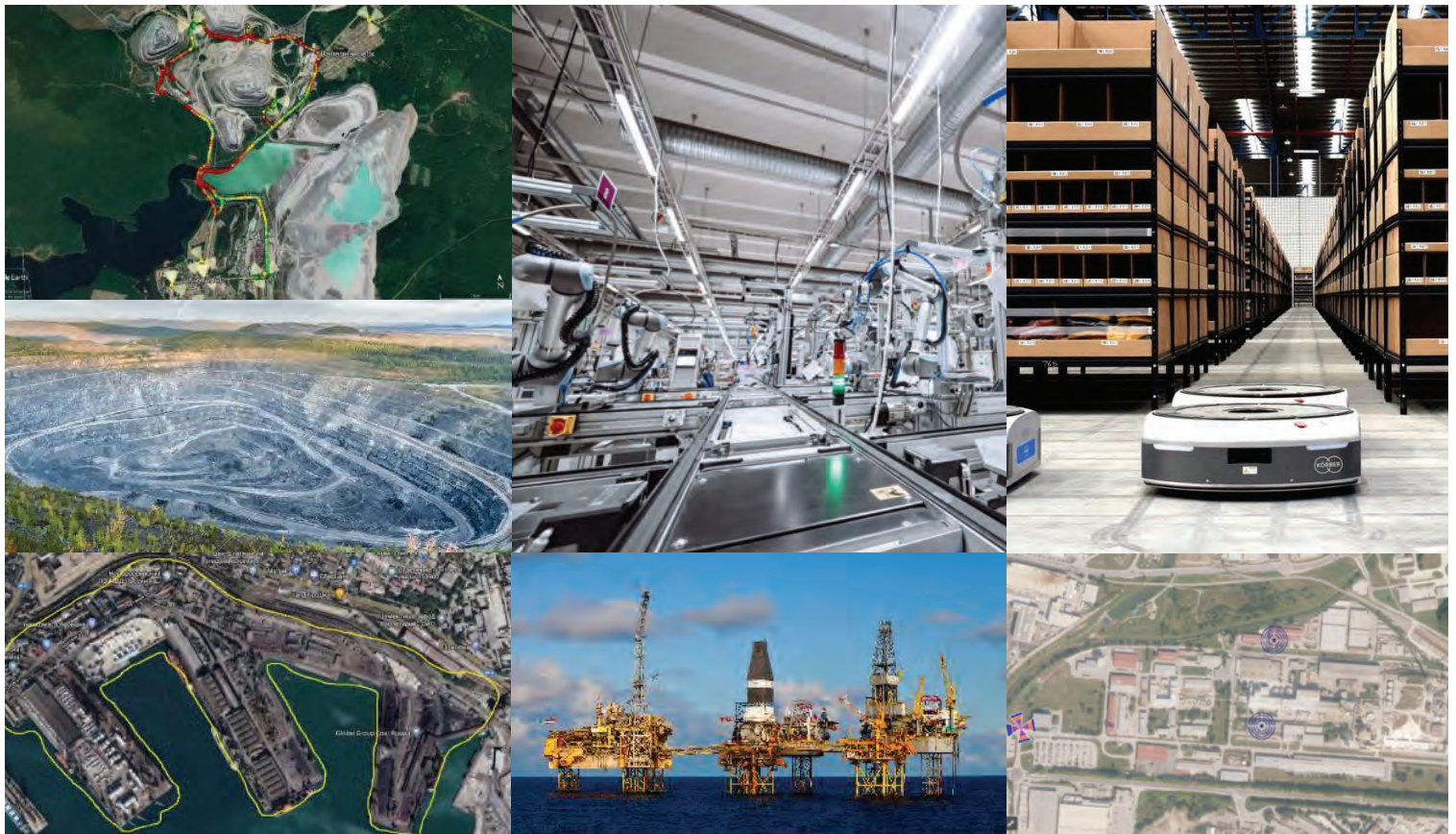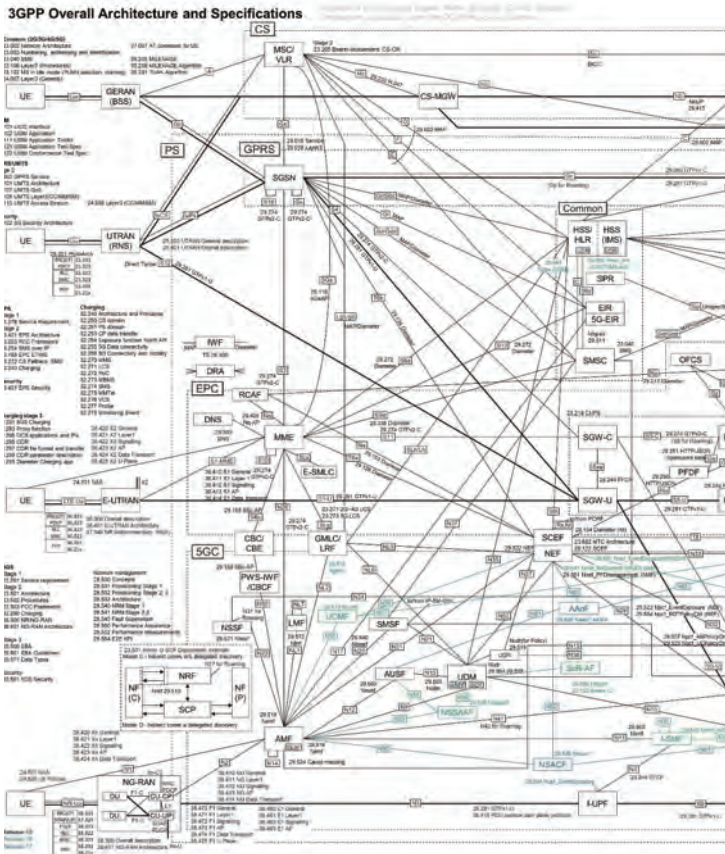
5G MPN Use Cases

Single 5G Network with multiple purpose connectivity

Massive	Broadband	Critical	Industrial

Asset management

FWA/eMBB for IoT

Automotive– C-ITS

Smart grid automation

Mobility & AGVs

Advance automation and control

Smart metering

Fleet management

AV/VR

Traffic safety and control

Collaborative robotics

| Massive	Broadband	Critical	Industrial
• Low-cost device • Small data volume • Extreme coverage	• High data rates • Large data volume • Low latency (best effort)	• High availability • Ultra-Reliable data delivery • Ultra-low latency	• Ethernet protocol • TSN • Clock sync as a service
LTE and 5G	LTE and 5G	5G	5G

s&t ISKRATEL

Cloud Native 5G Core Pillars
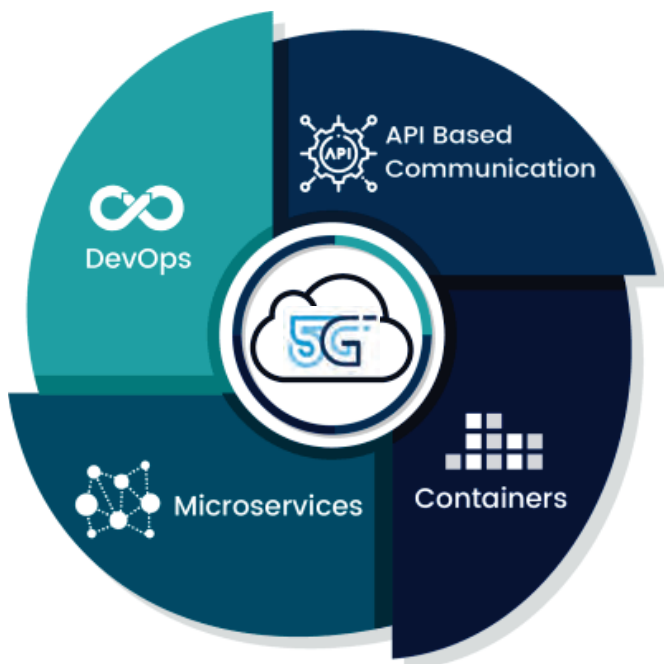
- 5G Service Based Architecture using HTTP/2, enable APIs on all communication paths
- Stateless **microservices**, use stateless containers, context stored in UDSF – „Redis", user data in databases.
- Create **new** microservice only where scalability is expected
- **CNCF toolset** – use only what you intend to use and what sounds great
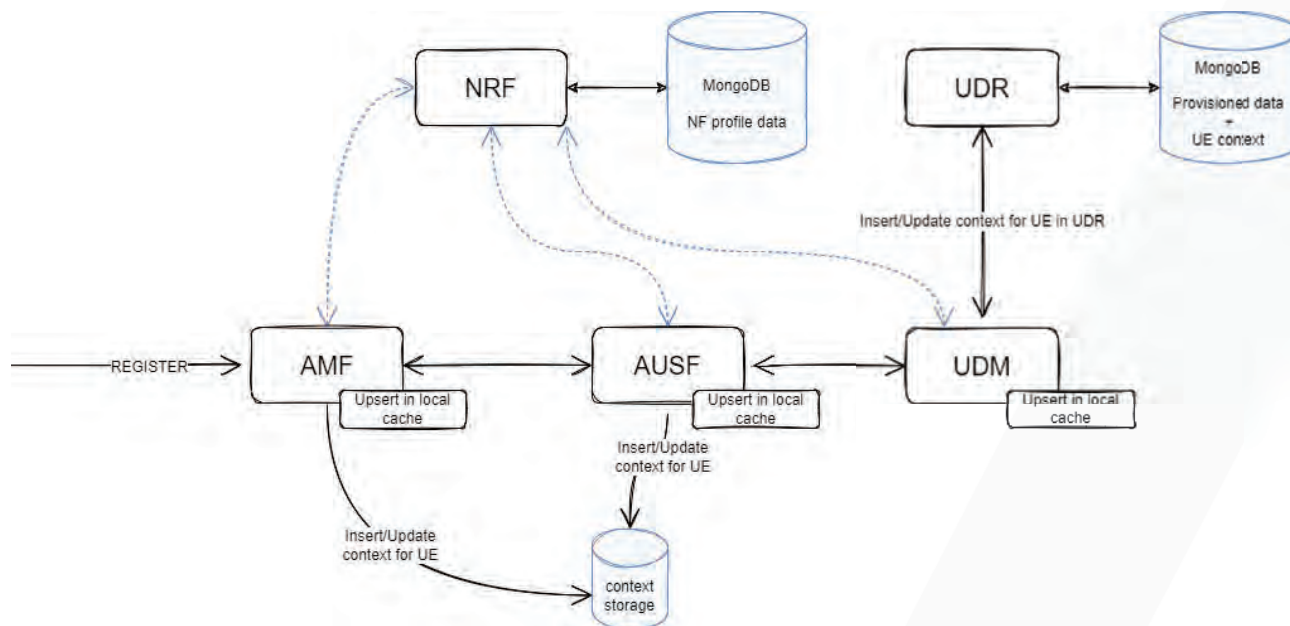- **CI/CD, Automation, Security by design**

DevOps – It's about the people

5G Cloud-native Platform
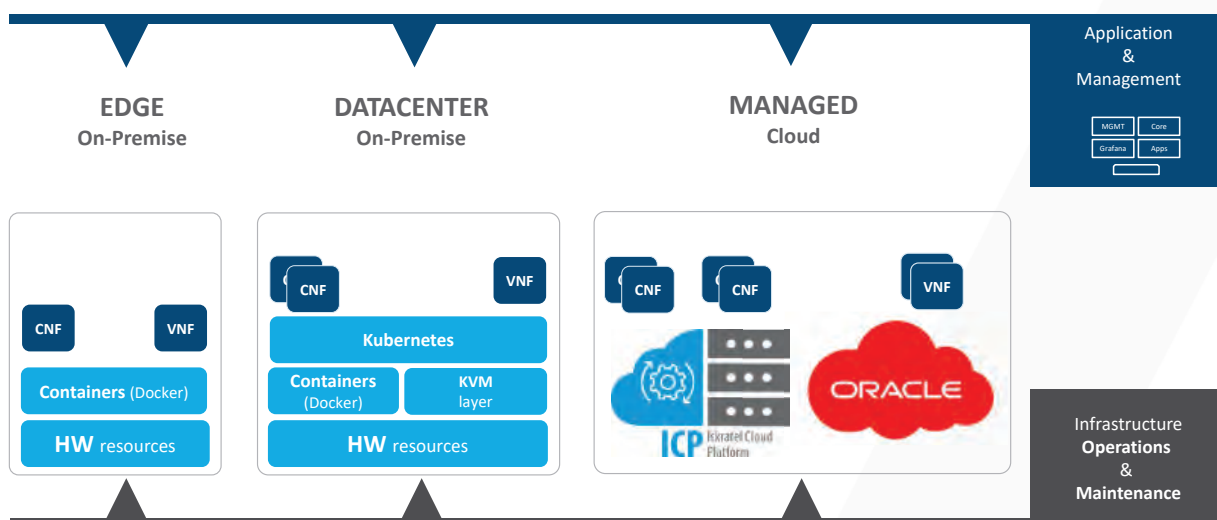
Stateless microservices

CNCF Toolset: Monitoring & Logging

Observability tools ensure that key operation information is easily accessed and understood
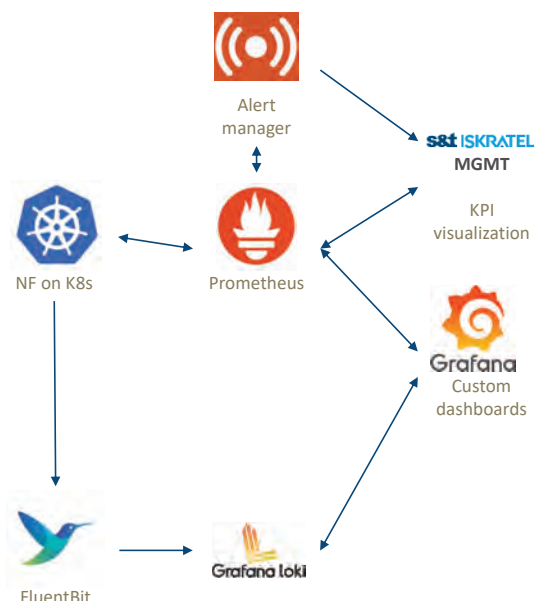
- **Fault Management & Central Metric collection**
  - Metric collection from network functions. Pull over HTTP
  - Time series data identified by metric name and key-value pairs
  - Alert manager

- **Performance management**
  - KPI visualizations of metrics
  - Custom dashboards with Grafana

- **Logging and troubleshooting**
  - Tracing with GrafanaTempo
  - Log collection with FluentD
  - Query with Grafana Loki and visualization in Grafana

CI/CD & Security
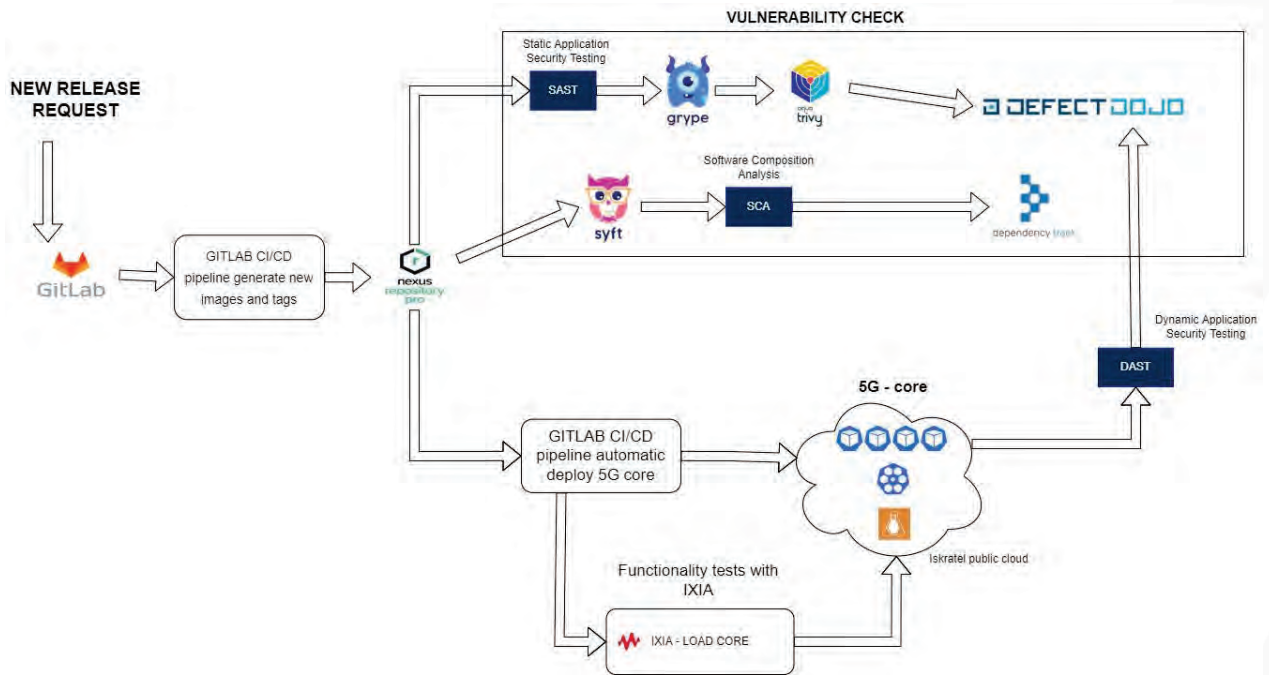
S&T Iskratel 5G Core Network
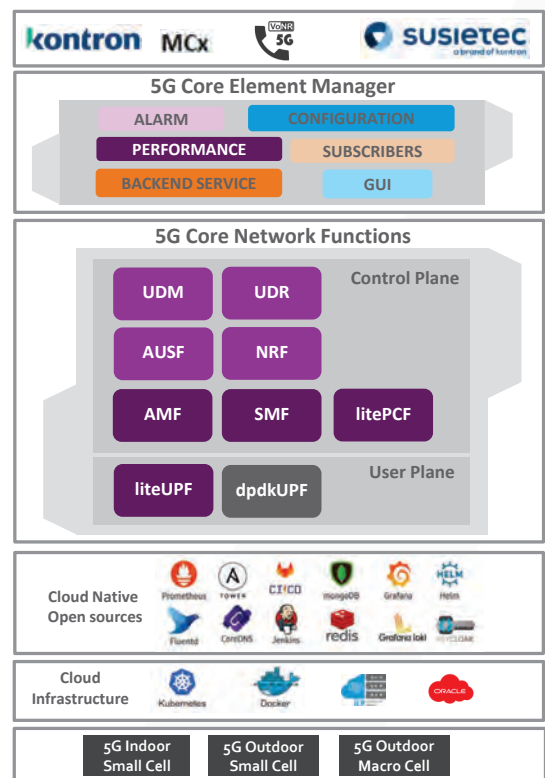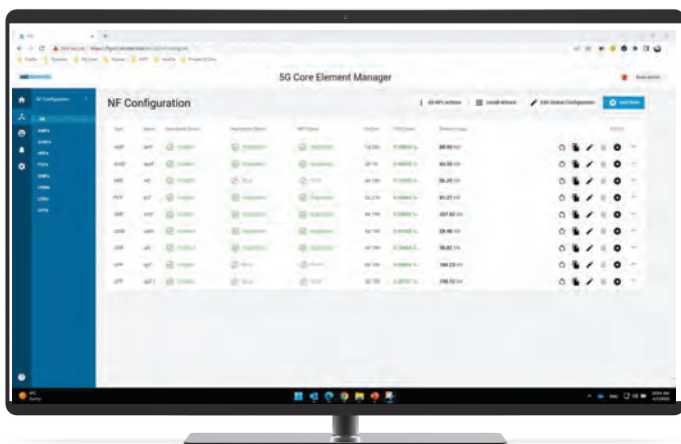
PLUG AND PLAY

s&t ISKRATEL

5G Core in Managed Cloud

All Cloud	Edge Computing	Disaster recovery	On-premise
VPN	VPN	VPN	

CUSTOMER PREMISE

s&t ISKRATEL

15
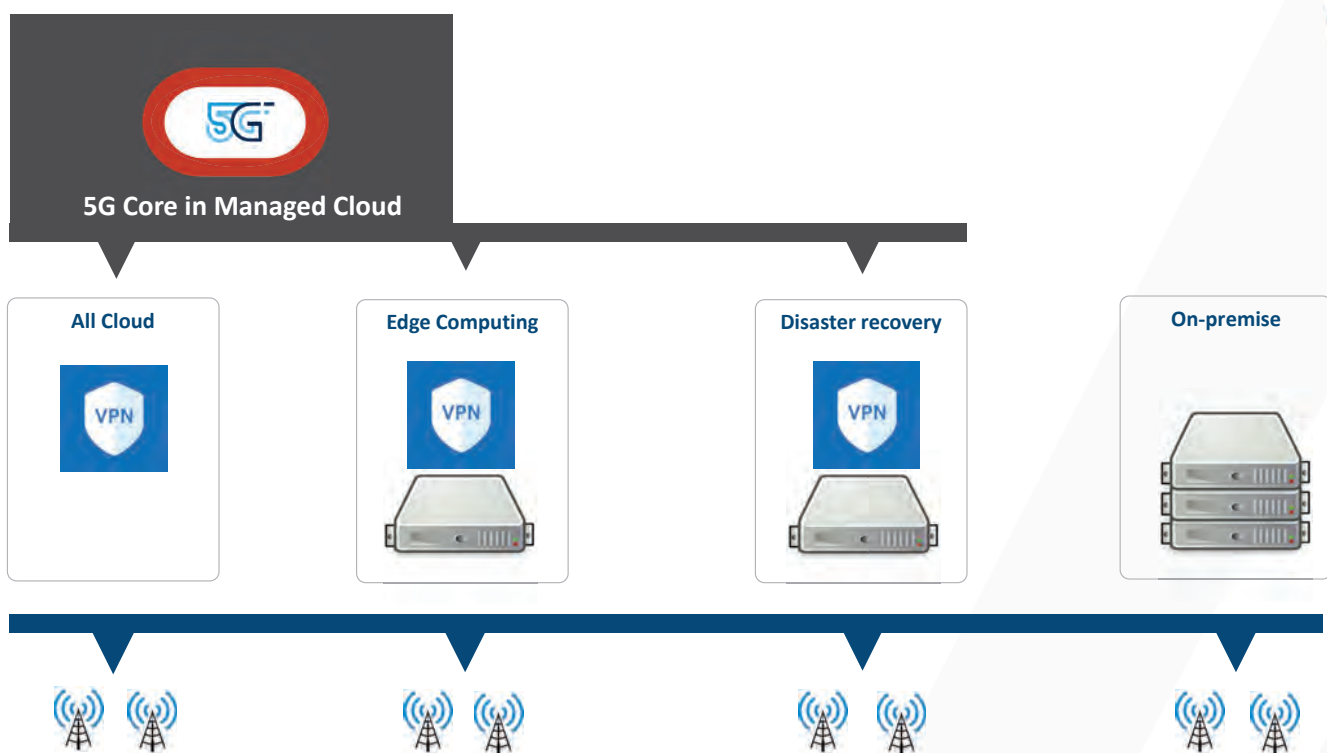
5G Core flavours

ALL-IN-ONE	ON-PREMISE	MANAGED
Ready to use solution, suitable for a work on a workfield:	Highly available solution for mobile private networks:	Plug-and-play solution offering from public cloud:

ALL-IN-ONE
- 5G core
- 5G BBU + RRH (macro / small cell)
- Management
- Applications: xPTT, Voice

ON-PREMISE
- SBA 5G core
- High throughput, high availability
- Applications: xPTT, Voice

MANAGED
- 5G core on OCI
- Automatic provisioning
- Edge capabilities
- Additional applications
- Seamless OCI integration

s&t ISKRATEL   16

Takeaways…

– **Massive cloud native ecosystem – less is more!**
  – S&T Iskratel has done a job for you and is offering it in professional services

– **Security, Automation, CI/CD is essential in Cloud native.**
  – 5G needs to be Cloud-native to be flexible

– **S&T Iskratel is working hard to bring 5G closer to the enterprises**
  – Leverage the knowledge of Cloud native & lower complexity and bring 5G fully managed from the cloud to the customer

s&t ISKRATEL   17

Oblaki v oblaku

Clouds in the cloud

Jure Jerman

Agencija Republike Slovenije za okolje

POVZETEK

Institucije z daljšo tradicijo se težje prilagajajo informacijskim izzivom, saj iz zgodovinskih razlogov s seboj nosijo težak tehnološki nahrbtnik. Na ARSO vidimo oblačne tehnologije kot eno od možnosti, da lovimo vlak napredka, ki sicer grozi, da bo kmalu odpeljal. V predavanju skušam našteti razloge, ki so nas usmerili v področje oblačnih tehnologij. Opisujem pot, ki smo jo prehodili do sedaj in težave, na katere smo naleteli. Navajam perspektive za naprej in razloge za odločitvi za privatni oblak. Uporaba oblačnih tehnologij zahteva tudi spremembe v poslovnih procesih in v načinu organizacije IT služb. V prispevku so opisani trendi s področja uporabe oblačnih tehnologij v drugih evropskih meteoroloških službah.

SUMMARY

Institutions with a longer tradition find it more difficult to adapt to information challenges, because for historical reasons they carry a heavy backpack full of legacy systems. At ARSO, we see cloud technologies as one of the possibilities to catch the train of progress, which otherwise threatens to depart soon. In the lecture, I try to list the reasons that directed us to the field of cloud technologies. I describe the path we have travelled so far; describe the problems we have encountered and outline perspectives for the future. I give the reasons for the decisions for the private cloud. The use of cloud technologies also requires changes in business processes and in the way IT services are organised. I also describe trends of cloud technologies in other European meteorological services.

O AVTORJU

Jure Jerman je diplomiral leta 1994 s področja uporabe nevronskih mrež pri kalibraciji meteorološkega radarja za analizo padavin, kar je bila eno od pionirskih uporab umetne intelegence v meteorologiji. Od leta 1994 dela na Hidro-meteorološkem zavodu Slovenije, danes Agenciji za okolje (ARSO). Ukvarjal se je predvsem z numeričnim meteorološkimi modeli in z zmogljivo IT infrastrukturo potrebno za njihovo izvajanje. Prav numerično modeliranje vremena je področje, ki je v zadnjih desetletjih po zaslugi osnovnih razvoja IT-tehnologije postalo osnovno orodje za analizo in napovedovanje vremena. Z informatiko se ukvarja od časov, ko računalniki na takratnem delovnem mestu še niso bili povezani v internet, več sodelavcev pa si je delilo eno delovno postajo. Bil je priča bliskovitega razvoja IT sistemov in njihovem nekoliko počasnejšem vpeljavanjem v delovne procese. Skupaj s sodelavci je še v prejšnjem tisočletju postavil eno od prvih Linux gruč na področju Slovenije. Danes niha med fascinacijo nad novimi informacijskimi tehnologijami in pesimizmom, ki ga prinaša spoznanje, da tehnološki napredek kot tak še ni garancija za napredek družbe.

ABOUT THE AUTHOR

Jure Jerman graduated in 1994 in the field of usage of neural networks in the calibration of meteorological radar for precipitation analysis, which was one of the pioneering uses of artificial intelligence in meteorology. Since 1994, he has been working for the Hydrometeorological Institute of Slovenia, today the Environmental Agency (ARSO). He mainly dealt with numerical meteorological models and the high-performance IT infrastructure required for their implementation. Numerical weather modelling is a field that has become a basic tool for weather analysis and forecasting in recent decades thanks to the basic developments in IT technology. He has been working with informatics since the days when computers at the workplace were not yet connected to the Internet, and several colleagues shared one workstation. He witnessed the rapid development of IT systems and their somewhat slower introduction into work processes. Together with his colleagues, he set up one of the first Linux clusters in Slovenia in the previous millennium. Today, he oscillates between the fascination with new information technologies and the pessimism brought by the realisation that technological progress as such is not yet a guarantee for the progress of society.

"Oblaki" v oblaku

Kakšna je prihodnost uporabe "oblačnih" tehnologij v državni meteorološki službei

Jure Jerman, Agencija za okolje (ARSO)

Konferenca Vitel, Bled, 29. In 30. 5.2023

Vsebina

- O IT-ju na Uradu za meteorologijo / Agenciji za okolje
- Oblačne priložnosti
- Pogoji za oblačno tranzicijo
- Poskus vzpostavitve hišnega oblaka
- Lekcije do sedaj
- Pogled v prihodnost

IT na Uradu za meteorologijo

- Meteorologija ima svoje specifike:
- V hiši obstaja dolga tradicija uporabe Linux sistemov
  - 1995: prve delovne postaje
  - HPC gruča 1997
- Visoko zmogljivo računalništvo
  - HPC sistemi so bili osnova za tehnološki razvoj in napredek na področju modeliranja (vremena, oceanov, vodostaja rek, onesnaženja zraka).
  - Trenutno 2 gruče, ~ 4000 jeder
  - Uporaba virov na ECMWF, Vega
  - Za doseganje operativnosti potrebni"hišni" (*on premise)* sistemi
- Sorazmerno veliko IT sistemov razvitih v hiši.
- Razširjena uporaba odprtokodnih rešitev.
- Kronično pomanjkanje sistemskih administratorjev.
- Veliko število produktov, slaba končna predstavitev in dostopnost

Problem tehnološkega nahrbtnika

- V Institucijah z daljšo zgodovino prisotno veliko število "legacy" sistemov, ki predstavljajo tehnološki nahrbtnik.
- Ta lahko postane pretežek, preden se institucija sploh zave, da ga nosi s seboj.
- Pomanjkanje sistemskega "top down" pristopa k reševanju problematike.
- Vzdrževanje zastarelih sistemov se zajeda v vire potrebne za razvoj.
  - Bazični sistemi,
  - Primer: nadgradnja relacijske baze Oracle in povezanih aplikacij
- Kako narediti IT sisteme bolj agilne?
- Koliko agilnosti si lahko institucija privošči?

Oblačne priložnosti:

- Visoka razpoložljivost.
- Modularnost informacijskih rešitev
- Samopostrežni princip za devOps-e
- Odmiranje "legacy" sistemov
- Poenotenje podporne infrastrukture

Potrebna je sprememba v koncipiranju IT rešitev

- Prehod iz monolitnih sistemov k servisno orientirani arhitekturi
- Uvajanje podporne infrastrukture:
  - Git okolje: gitLab
  - CI/CD cevovodi
- NFS -> S3
- Sporočilne vrste (Message Queues)
- Načrtovanje informacijskih rešitev

European Weather Cloud (EWC)

- Nekaj pojmov:
  - ECMWF: Evropski center za srednjeročno napovedovanje vremena
  - EUMETSAT: Evropska agencija za uporabo meteoroloških satelitov
  - Oba centra proizvajata stalen tok informacij
- Ideja: državam članicam omogočiti, da informacije obdelujejo bližje viru informacij.
- A s spremembo koncepta pride tudi potreba po spremembi pristopa k načrtovanju IT rešitev.

Ideja o hišnem oblaku

- Okolje za spoznavanje z oblačnimi tehnologijami
- Osnova oblačno tranzicijo.
- Izobraževanje uporabnikov in sistemskih administratorjev
- Konsolidacija podpornih tehnologij.

Koncepiranje ekosistema: Infrastrukturna kopica

- Kubernetes OpenShift (OKD) gruča
- ProxMox cluster (Virtualni strežniki ali LC)
- Reverse Proxy Server
- Ceph gruča

Servisna kopica (npr)

API Gateway:	Gravitee
Identity provider:	Keycloak
Message Queue:	RabbitMQ, Kafka
Objektno skldišče:	CEPH S3
Reverse Proxy:	HAProxy
Real Time Monitoring:	Sentry
Monitoring:	Icinga

Narejeno do sedaj:

- Vzpostavitev CEPH podatkovnega skladišča:
  - 13 strežnikov
  - 1.5 pB diskovnega prostora
  - Heterogena mrežna infrastruktura (10gbE, 40gbE, 56gB Infiniband)
  - S3 pride v paketu.
- Vzpostavitev Kubernetes gruče:
  - 7 strežnikov
  - OKD (OpenShift)
  - Zaradi napačnih odločitev na začetku težave pri administracija
  - Integrirano s CEPH podatkovnim skladiščem

Zaključki

- IT postaja neskončno kompleksen
- "Outsourcing" ni odgovor na vsa težave.
- Redko Kdo je sposoben predvideti optimalno smer razvoja
- Potrebne bodo organizacijsko-strukturne spremembe: administracija velikega števila komponent oblačnega eko-sistema.
- Slab doseg informacij do končnih uporabnikov.
  - V razvoju novo spletišče.
  - API-ji za notranje in zunanje uporabnike
  - Razvoj naprednejših storitev.

Razvoj novih poslovnih modelov z uporabo povezljivih gospodinjskih aparatov

Development of new business models using connected household appliances

Andrej Črepinšek

Hisense Europe

POVZETEK

Prispevek predstavlja nove vidike, ki prihajajo z vpeljavo povezljivih naprav - kaj to pomeni za končne uporabnike, kaj za proizvajalca in s kakšnimi novimi izzivi se proizvajalec srečuje. Pri ustvarjanju konkurenčne prednosti je ključnega pomena vrednost glede na strošek, pri premium izdelkih kvaliteta in ekskluzivnost. V obeh primerih je zelo pomembna uporabniška izkušnja. Za boljše razumevanje, kaj vpliva na dobro izkušnjo strank ter hitro prilagajanje izdelkov trgu, je potrebno naslednje: (1) podatki o uporabnikovih navadah (npr. katera funkcionalnost prinaša največjo dodano vrednost, kako uporabnik aparate uporablja in kdaj) ter izzivih ter kvalitetna analitika na teh podatkih, (2) hitrost vpeljave novih storitev s pomočjo agilnih metodologij, mikrostoritev in okolja DevSecOps, (3) spremljanje in zagotavljanje klvalitete storitev, (4) zagotavljanje varnosti in zaupnosti osebnih podatkov. V prispevku je predstavljena Hisensova zgodba digitalne transformacije skozi celoten življenski cikelj – od razvoja nove naprave, proizvodnje do tehnične podpore.

SUMMARY

The paper presents the new aspects that come with the introduction of connectable devices - what this means for end users, what for the manufacturer and what new challenges the manufacturer faces. When creating a competitive advantage, value relative to cost is key, with premium products quality and exclusivity. In both cases, the user experience is very important. For a better understanding of what affects a good customer experience and rapid adaptation of products to the market, the following is necessary: (1) data on user habits (e.g. which functionality brings the greatest added value, how the user uses the devices and when) and challenges, as well as quality analytics on these data, (2) the speed of introducing new services with the help of agile methodologies, microservices and the DevSecOps environment, (3) monitoring and ensuring the quality of services, (4) ensuring the security and confidentiality of personal data. The paper presents Hisens' story of digital transformation throughout the entire life cycle - from the

development of a new device, production to technical support.

O AVTORJU

Mag. Andrej Črepinšek je od leta 2021 tehnični vodja digitalnih storitev v podjetju Hisense Europe. Pred tem je bil vrsto let tehnični direktor IBM-a za Vzhodno in Srednjo Evropo, kjer je imel priložnost sodelovati s številnimi podjetji v tej regiji ter delati na najbolj inovativnih projektih. Diplomiral je na Univerzi v Ljubljani, Fakulteti za Elektrotehniko in računalništvo, kjer je tudi dokončal magistrski študij. Z digitalnimi transformacijami se ukvarja že vrsto let in je sodeloval pri številnih digitalnih transformacijah podjetij in organizacij kot so Škoda Auto, Sberbank Rusija, e-uprave v Jordaniji, e-zdravja v Republiki Južna Afrika, itd. Od leta 2006 ima najvišji industrijski certifikat za IT arhitekte – Opengroup certified Distinguished Architect.

ABOUT THE AUTHOR

Andrej Črepinšek, MSc., is a Lead Architect and Technical Leader in Hisense Europe. Before this position he was acting many years as a Chief Technology Officer for IBM Central and Eastern Europe where he got a chance to work with several companies in the region and participate in the most innovative projects. He got his bachelor's degree at University in Ljubljana, Faculty for electro engineering and computer science. He has been working on digital transformation for many years and he was engaged on digital transformation projects with several companies and organizations like Škoda Auto, Sberbank Russia, Jordan government, e-health transformation in The Republic of South Africa, etc. He is holding the highest industry certificate for IT Architects since 2006 - Opengroup certified Distinguished Architect.
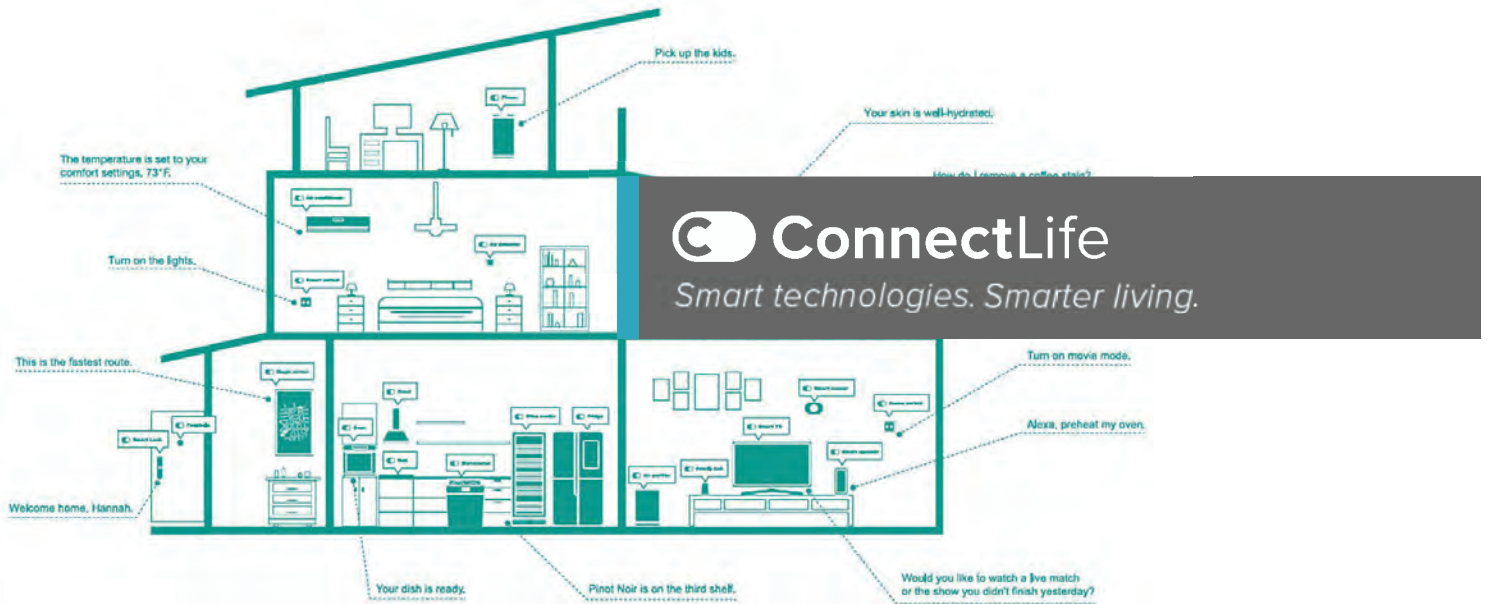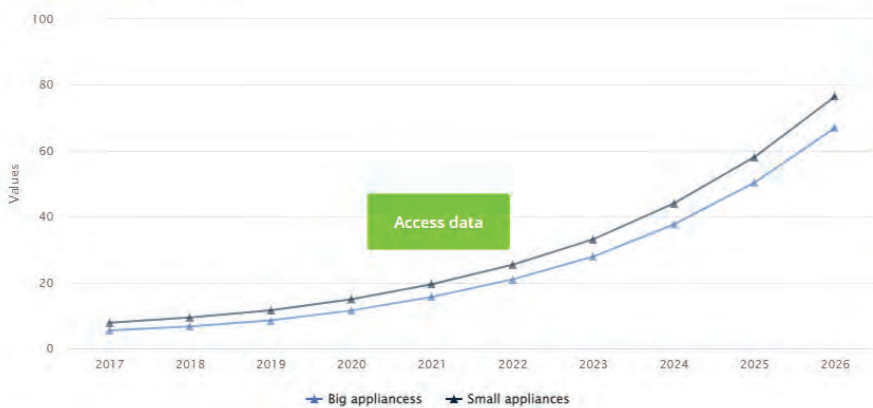
- **Global company with more than 80.000 employees**
- **4 industries**
- **More than 70 years tradition (Gorenje since 1950)**
- **60 countries**
- **3 main manufacturing sites, 4 main R&D centers and 27 business units**
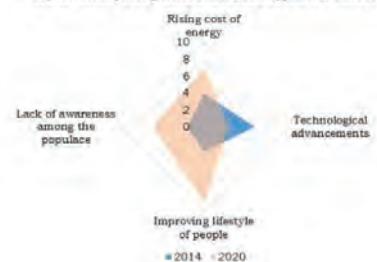- **No. 1 TV producer globally**

2/23

ConnectLife

Connectable Home appliances market

ConnectLife Reference Architecture

INTERNAL INTEGRATION

- PRODUCTION
- SALES/ MARKETING
- AFTERSALES/ SERVICE
- SERVICE CALL CENTER

EXTERNAL INTEGRATION

- SOCIAL LOGIN
- EXTERNAL SERVICES
- EXTERNAL DATA
- CLOUD 2 CLOUD

UI/UX

Mobile · OEM APPs
Web · TV · Voice

INTEGRATION LAYER

API

Registers (User, Appliance, Pairing)

Data & Services Integration

Process Automation (Wizards)

Management

DIGITAL PLATFORM

Data Analytics and AI · Digital services · Digital Content · Connected appliances

APPLIANCES

Connected appliances · ASKO Pro appliances · Non-connected appliances · OEM Appliances

Management

5/23

Connectivity Value

Digital services for End users

Remote technical support

Data / Analytics
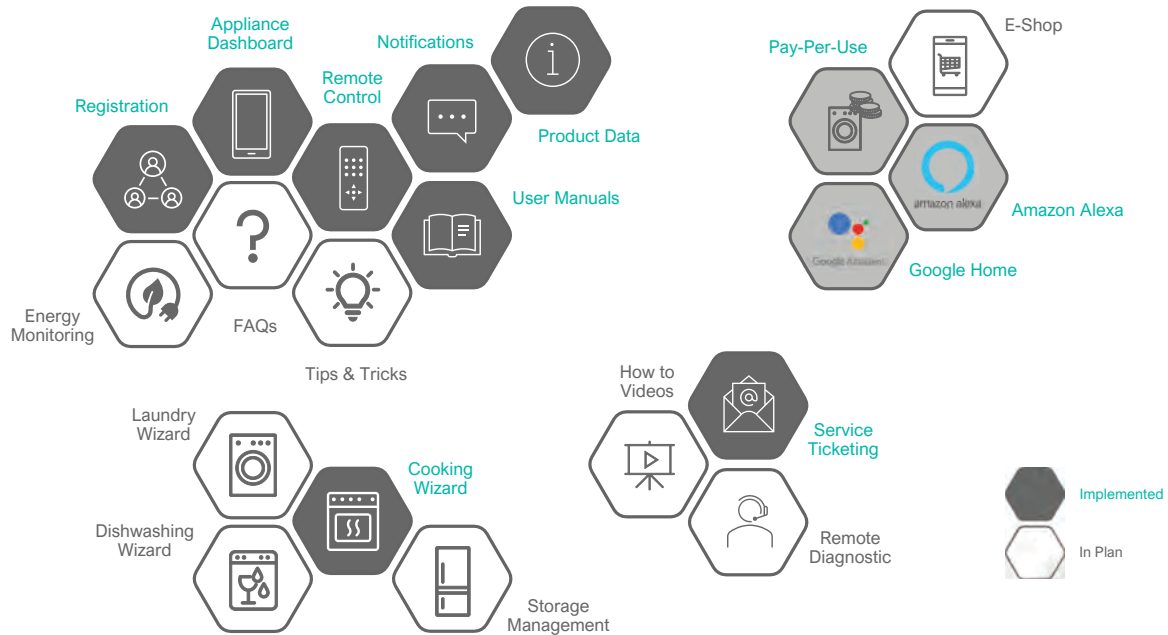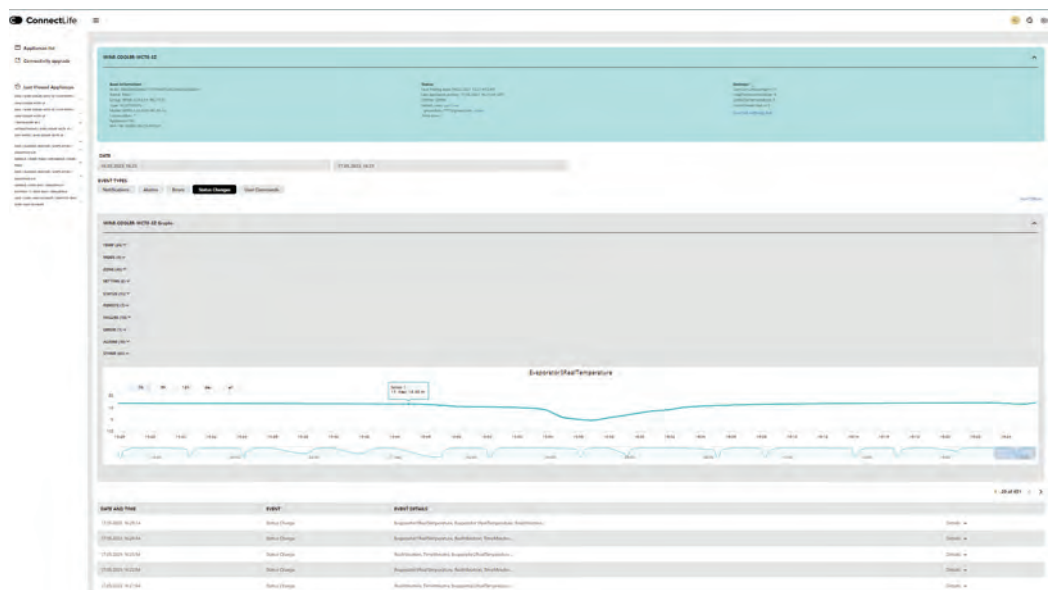
6/23

Overview of Digital Services

After Sales Dashboard

- Dashboard to access appliance data of connected appliances
- Accessible to after sales service team within define access rights
- Web solution, mobile ready
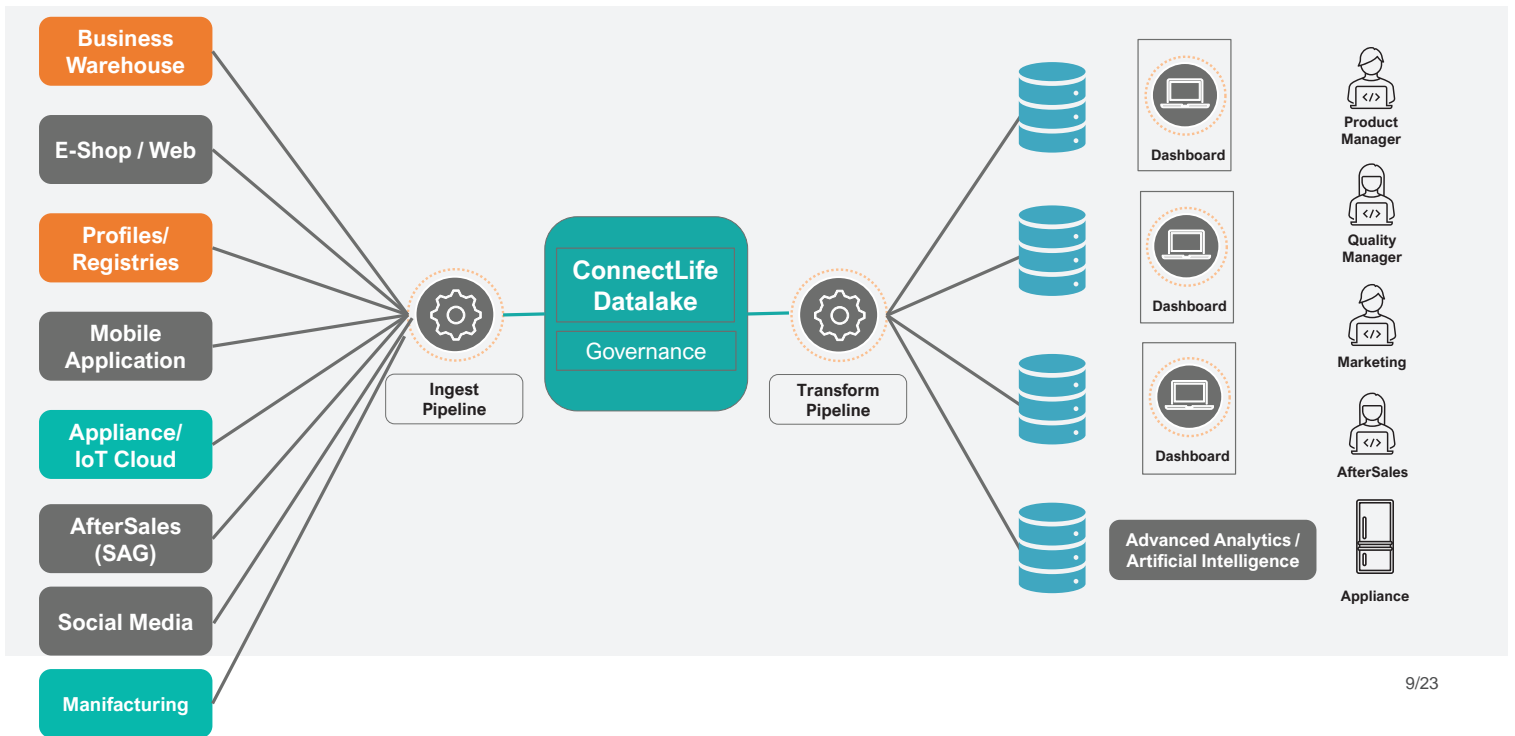- 3 User roles: Admin, Manager and User

Benefits for Hisense

Support on better services intervention results in better performance and increase user experience.

ConnectLife Big Data Platform

9/23

Types of Corporate Data

10/23

ConnectLife Big Data – Phase 1 Dashboard
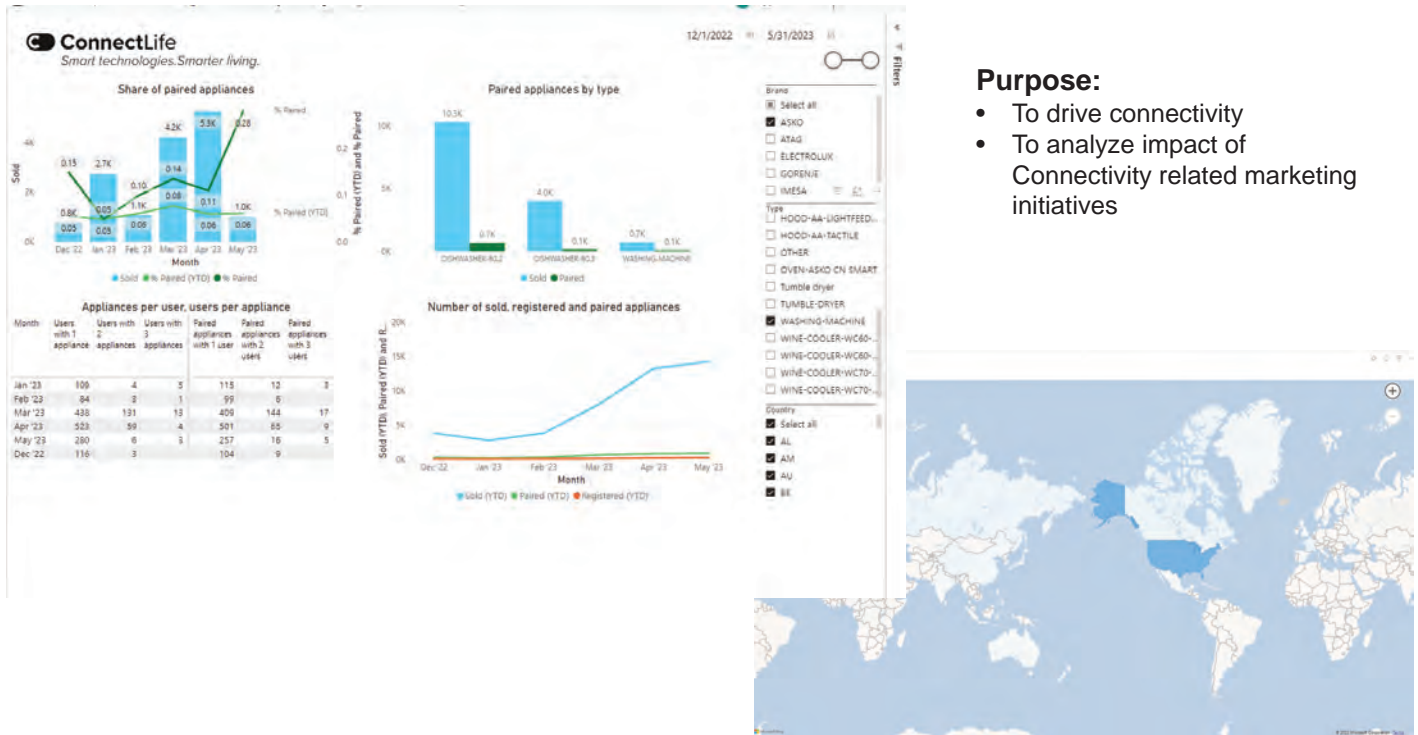
Purpose:
- To drive connectivity
- To analyze impact of Connectivity related marketing initiatives

Summary

Pig with a lipstick is still just a pig

Appliance connectivity is not additional feature, but transformation

Current vs. Strategic value

How to justify investments?

Physical vs. Digital

Shift from Appliance Manufacturing to Services, shift in skills and resources, etc

Where to start?

Quick wins, when to switch from "demo" to "enterprise" solution

12/23

Zavarovalniške storitve v oblaku

Cloud insurance services

Izidor Žontar, Miran Ficko

Zavarovalnica Triglav

POVZETEK

Sodobni časi zahtevajo od infrastrukture in ekip, ki jo upravljajo, hitro prilagodljivost in odziv na nove zahteve in načine dela ter tako spreminjajo tradicionalno vlogo upravljanja infrastrukture. V uporabo vstopajo storitve, ki so izredno kompleksne, tako pri vzpostavitvi, kot tudi pri vzdrževanju. Take storitve zahtevajo strokovnjake s specifičnimi znanji. Tu se izkažejo prednosti oblačnih storitev, saj ponudniki zagotavljajo te storitve in zanje nudijo ustrezno podporo in vzdrževanje. Prav tako oblačna okolja nudijo storitve, ki jih v taki obliki ni možno vzpostaviti v lastnih podatkovnih centrih, kot so recimo specifične storitve iz naslova poslovne inteligence, umetne inteligence in storitve, ki zahtevajo specifično strojno opremo. Po drugi strani pa oblačna okolja prinašajo tudi spremembo procesov upravljanja in dojemanja odgovornosti, ter tako vnašajo nove izzive.

Še pred izbruhom pandemije, ki je dodatno pospešila uporabo oblačnih storitev, smo ugotovili, da moramo ponudbo infrastrukturnih storitev, ki tečejo v lastniških podatkovnih centrih, ustrezno dopolniti s ponudbo oblačnih storitev. Tako smo vzpostavili hibridno okolje, ki ga sestavljajo tako lastniški viri in storitve kot tudi storitve, ki jih nudi Microsoft Azure. Tako okolje omogoča segmentacijo storitev glede na njihovo pomembnost, namembnost in lokacijo uporabe, širitev kapacitet in uporabo specifičnih storitev ter zasnov, ki jih ponujajo oblačna okolja. Arhitekturo čez leta širimo z novimi komponentami in pristopi. Tu bi omenili kontejnerizacijo, ki je eden od temeljev učinkovitega DevOps procesa. Kot finančna institucija s področja zavarovalništva smo še dodatno regulirani, kar pri uporabi oblačnih storitev predstavlja še dodaten izziv.

V prispevku so predstavljeni začetki uporabe oblačnih storitev in hibridnega okolja, prednosti ter izzivi in pasti, ki jih tako okolje prinaša. Opisane so tudi storitve, ki jih uporabljamo, kot so storitve umetne inteligence, poslovne inteligence, DevOps, low/no code, kontejnerizacije in *serverless*. V zaključku je podana implementacija kontejnerizacije z uporabo hibridne rešitve Redhat Openshift.

SUMMARY

Modern times require infrastructure and the teams managing infrastructure to adapt and respond quickly to new demands, changing the traditional role of infrastructure management. Services are coming into use that are extremely complex, both to set up and to maintain. Such services require experts with specific skills. This is where the benefits of cloud services come into play, as cloud providers offer these services and offer the appropriate support and maintenance for them. Cloud environments also offer services that cannot be set up as such in proprietary data centres, such as specific business intelligence services, artificial intelligence services and services that require specific hardware. On the other hand, cloud environments also bring a change in management processes and perceptions of responsibility, thus introducing new challenges.

Even before the pandemic, which has further accelerated the use of cloud services, we realised that we needed to complement the infrastructure services running in proprietary data centres with cloud services. We have therefore created a hybrid environment consisting of both proprietary resources and services as well as services offered by Microsoft Azure. This environment allows for the segmentation of services according to their importance, purpose and location of use, the expansion of capacities and the use of specific services and concepts offered by cloud.

O AVTORJIH

Izidor Žontar (1968, Kranj) se je prvič srečal s področji računalništva in informatike kot štipendist podjetja Iskra Delta. V srednješolskem obdobju na Gimnaziji Kranj in na Fakulteti za računalništvo in informatiko v Ljubljani je s podjetjem aktivno sodeloval kot štipendist in v številnih projektih s področij sistemske programske, kot tudi strojne računalniške opreme. Kasneje se je pridružil Zavarovalnici Triglav in pred desetimi leti prevzel mesto direktorja službe za sistemske storitve informatike. Vodi razvojne ekipe in projekte, od začetne analize in načrtovanja do izvedbe in testiranja ter strateške projekte IT. Žontar je aktiven udeleženec strokovnih konferenc in seminarjev na področju informacijske tehnologije doma in v tujini.

Miran Ficko (1980, Murska Sobota) se je pred dvajsetimi leti zaposlil v Zavarovalnici Triglav kot inženir informatike na delovno mesto JAVA in .NET razvijalca. Z leti je nabiral izkušnje na delovnih mestih kot arhitekt in specialist za integracije. Ukvarjal se je z naprednimi tehnologijami, tehničnim vodenjem projektov, tehničnim skrbništvom različnih platform in rešitev, ter vodenjem oddelka. Zadnja leta se je specializiral za oblačne storitve z uporabo Azure in kontejnerizacijo, zdaj pa deluje kot strokovnjak v službi sistemskih storitev, kjer skrbi za arhitekuro, posamične rešitve, ter vodi projekte z naslova uvajanja novih rešitev in integracije med njimi. Njegov nabor znanj sestavljajo orodja in poznavanje konceptov iz naslova DevOps, programiranje v javi in .net, razni skriptni jeziki, poznavanje podatkovnih baz, Azure oblačnih storitev in Linux. Dobro pozna konternerizacijski platformi AKS in Openshift in različne tehnologije pod okriljem CNCF.

ABOUT THE AUTHORS

Izidor Žontar (1968, Kranj) first encountered the fields of computer science and informatics as a scholarship holder of Iskra Delta. During high school (Gymnasium Kranj) and also at faculty (Faculty of Computer Science and Informatics in Ljubljana) he actively worked with the company as a scholarship holder and in numerous projects in the fields of system software and computer hardware. He later joined Zavarovalnica Triglav (insurance company) and ten years ago took over the position of director of IT system services. He leads development teams and projects, from initial analysis and planning to implementation and testing, as well as strategic IT centralization projects. Žontar is an active participant in professional conferences and seminars in the field of information technology at home and abroad.

Miran Ficko (1980, Murska Sobota) joined Zavarovalnica Triglav as an IT engineer twenty years ago in the role of JAVA and .NET developer. He gained experience in different roles as an architect and integration specialist. He was mainly involved in advanced technologies, technical project management, technical administration of various platforms and solutions, and department management. In recent years he has specialised in cloud services using Azure and containerisation. Today, he works as an expert in the System Services department, where he takes care of architecture, individual solutions, and manages projects related to the deployment of new solutions and providing integration between them. His skillset consists of tools and knowledge of DevOps concepts, java and .net programming, various scripting languages, knowledge of databases, Azure cloud services and Linux. He has good knowledge of the AKS and Openshift containerisation platforms and of the various technologies under the CNCF umbrella.

Zavarovalniške storitve v oblaku

Zavarovalnica Triglav d.d.

Predstavitev podjetja

- Finančna inštitucija
- Skupina – prisotnost v večih državah
- Centralizirana infrastruktura

Strategija IT infrastrukture - sledimo uporabi storitev v oblaku in transformaciji klasičnih podatkovnih centrov v hibridni oblak

- S postopno preobrazbo zagotavljamo učinkovito in zanesljivo delovanje informacijskih rešitev.

- Robustna in visoko razpoložljiva strežniška infrastruktura podpira centralne informacijske storitve.

- Distribuirana strežniška infrastruktura zagotavlja stabilno delovanje podpornih sistemov. Izvaja se preobrazba v konsolidirano informacijsko infrastrukturo (hibridni oblak) za potrebe centralizacije infrastrukture v Skupini Triglav.

- Pri prenovi in obnovi jedrnih informacijskih sistemov (IBM) sledimo migraciji aplikativnih storitev v oblak.
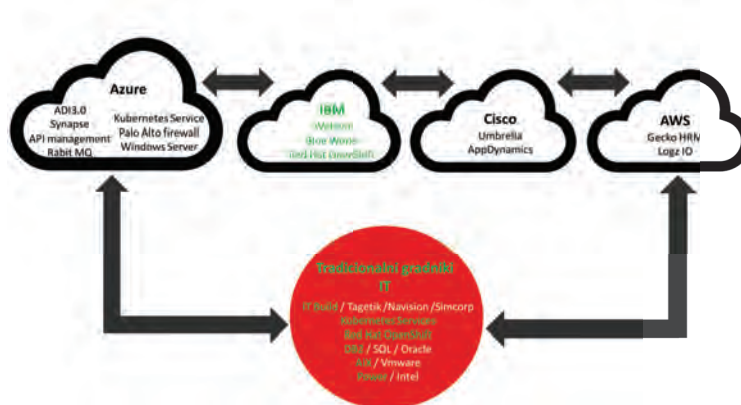
Začetki uporabe oblačnih storitev

Izzivi:

Postavitev in uporaba naprednih storitev

Pokritje povečanih potreb

Cilj:

Dodatna lokacija z dostopom do virov in naprednih storitev – hibridno okolje

Poudarek na dodani vrednosti

Uporaba PaaS in SaaS storitev

Uporaba „infrastruktura kot koda"

Azure oblak

- Celotna linija produktov in s tem lažja integracija

- Eden od vodilnih ponudnikov

- Celovita izkušnja pri integraciji (on-boarding)

Uporaba naprednih oblačnih storitev

- Uporaba PaaS in SaaS

- Power platform (low code/no code)

- Poudarek na kontejnerjih, serverless

- Storitve iz naslova AI, Cognitive

- Storitve poslovne analitike (synapse, power bi)

- DevOps

Kontejnerizacija v hibridnem okolju

- Devops proces

- Fleksibilnost

- Hitrejše prilagajanje

- Izhodni scenariji / izredni dogodki
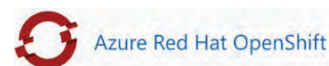
Izzivi oblačnega okolja

- Regulativa, skladnost, …, standardizacija

- Miselnost ljudi

- Povezljivost

- Upravljanje (deljeno upravljanje!, veščine)

- Stroški („Manj je več", SaaS Da/Ne, Rezervacije)

- Varnost (Dostopi, varovanje okolja, …)

- Nadzor (centraliziran monitoring, izziv orodij)

Odprta znanost

Open sicence

Miran Petek

Institut informacijskih znanosti (IZUM)

POVZETEK

Odprta znanost je skupek praks in načel, katerih namen je vsakomur omogočiti dostop do znanstvenih raziskav iz vseh področij znanosti. To je v korist tako znanstveni skupnosti kot tudi razvoju družbe kot celote, saj se lahko pospeši reševanje kompleksnih izzivov današnjega časa v globalno povezanem svetu. Evropski oblak odprte znanosti (EOSC) je praktični odziv Evropske komisije na zahteve odprte znanosti. Portal EOSC bo predstavljal medmrežje odprtih raziskovalnih objav, podatkov, storitev in infrastruktur. Slovenski prispevek v EOSC se bo odražal preko novoustanovljene Slovenske skupnosti odprte znanosti, katere osnovni namen je spodbujanje razvoja odprte znanosti v Sloveniji. Pomembna infrastruktura so digitalni repozitoriji, ki hranijo publikacije, raziskovalne podatke in preostale digitalne objekte po načelih odprtega dostopa. Temu sledi tudi IZUM s svojimi servisi. Digitalni repozitorij dCOBISS in Akademska digitalna knjižnica Slovenije pomembno prispevata k dostopu do informacij in vsebin ter splošni podpori znanja v slovenskem raziskovalnem in izobraževalnem okolju.

SUMMARY

Open Science is a group of practices and principles with the aim of providing access to scientific research from all areas of science to anyone. This contributes to the research community and the development of society as a whole and facilitates the solution of complex challenges of our times in a globally connected world. The European Open Science Cloud (EOSC) is the practical response of the European Commission to the demands of open science. The EOSC Portal is a network of open science publications, data, services and infrastructures. The Slovenian contribution to EOSC will be expressed through the newly established Slovenian Open Science Community, whose main purpose is fostering the development of open science in Slovenia. Digital repositories that store publications, research information and other digital objects following open access principles are an important infrastructure. IZUM and its services also follow this philosophy. The dCOBISS Digital Repository and the Academic Digital Library of Slovenia contribute significantly to the access to information and contents and the general support to knowledge in the Slovenian research and education environment.

O AVTORJU

Miran Petek je zaposlen v IZUM-u od leta 1997 in dela v sektorju za razvoj programske opreme. V zadnjih 15 letih se je ukvarjal s tujimi informacijskimi servisi in upravljanjem dostopa do informacijskih virov, kar vključuje avtoriziran dostop do licenčnih elektronskih virov, iskalnikom Metaiskalnik, konzorcijskimi servisi, aplikacijo COBISS+ in drugimi nalogami s področja odkrivanja informacij. V zadnjih štirih letih je pomagal pri razvoju Akademske digitalne zbirke Slovenija (ADZ) in aplikacije za Digitalni repozitorij COBISS (dCOBISS).

ABOUT THE AUTHOR

Miran Petek has been working at IZUM since 1997 and is part of the software development group. In the last 15 years he has been working on foreign information services and managing access to information resources, which includes authorised access to licensed electronic resources, the Metaiskalnik search engine, consortium services, COBISS+, and other activities in the field of information discovery. Over the last four years he has been helping in the development of the Academic Digital Collection of Slovenia (ADZ) as well as of the application for COBISS Digital Repository (dCOBISS).

Odprta znanost

Miran Petek

Agenda

- Kaj je odprta znanost?
- Evropski oblak odprte znanosti
- Slovenska skupnost odprte znanosti
- Digitalni repozitoriji v Sloveniji v podporo odprti znanosti
- Prispevek IZUM-a k odprti znanosti (dCOBISS in Akademska digitalna zbirka Slovenije – ADZ)

Kaj je odprta znanost?

Odprta znanost (ang. Open Science) je gibanje v znanosti, ki zagovarja transparentnost, odprtost in dostopnost znanstvenih raziskav, podatkov in rezultatov. Namen odprte znanosti je povečati dostopnost do znanja in pospešiti napredek v znanosti tako, da omogoča širšo uporabo, ponovljivost in nadaljnji razvoj znanstvenih spoznanj.

Odprta znanost spodbuja objavo znanstvenih člankov v odprtem dostopu, kar pomeni, da so članki brezplačno dostopni za vse, ki jih želijo prebrati. Poleg tega spodbuja tudi deljenje raziskovalnih podatkov in programske opreme, ki so potrebni za ponovitev znanstvenih poskusov in preverjanje znanstvenih ugotovitev. Odprta znanost tako omogoča večjo transparentnost in preverljivost znanstvenih raziskav.

Odprta znanost ima številne prednosti, med drugim pospešuje znanstveni napredek, izboljšuje kakovost raziskav, povečuje dostopnost do znanja in spodbuja sodelovanje med raziskovalci. V zadnjih letih se je odprta znanost postala vse bolj pomembna in se uveljavlja kot pomembno načelo v znanstveni skupnosti.

ChatGPT: https://openai.com/

© IZUM, SIKOM, Bled, 6. junij 2023   3

Odprta znanost

https://igelsociety.org/

© IZUM, SIKOM, Bled, 6. junij 2023   4

Ključni dokumenti politik odprte znanosti

- Commission communication A new ERA for Research and Innovation, 2020
- Commission recommendation on a European strategy for universities, 2022
- Council conclusions on the New European Research Area, 2020
- Council conclusions on the European Universities initiative - Bridging higher education, research, innovation and society: paving the way for a new dimension in European higher education, 2021
- Council conclusions on research assessment and implementation of Open Science, 2022

Slovenija: zakonodajne določbe o odprti znanosti so usklajene z Obzorjem Evropa

- Zakon o znanstvenoraziskovalni in inovacijski dejavnosti (ZZrID), 2021
- Slovenian Scientific Research and Innovation Strategy 2030, 2022
- Načrt razvoja raziskovalne infrastrukture 2030 (NRRI 2030), 2022

Odprti dostop

- brezplačen (prost) dostop do celotnega besedila publikacij (članki, monografije, konferenčni prispevki …) na založnikovi platformi ali v digitalnem repozitoriju
- avtor vsem uporabnikom dovoli dostop do publikacije, razmnoževanje, uporabo, razširjanje in javni prikaz, kar označi z eno izmed licenc – najpogosteje Creative Commons
- večinoma avtor ohrani materialne avtorske pravice, za razliko od klasičnega modela objavljanja, kjer avtor te pravice prenese na založbo

Plan S (cOAlition S)

About Plan S

Plan S is an initiative for Open Access publishing that was launched in September 2018. The plan is supported by cOAlition S, an international consortium of research funding and performing organisations. Plan S requires that, from 2021, scientific publications that result from research funded by public grants must be published in compliant Open Access journals or platforms.

https://www.coalition-s.org/

Podpisnica tudi Slovenija (Agencija RS za raziskovalno dejavnost)

© IZUM, SIKOM, Bled, 6. junij 2023   7

Modeli odprtega dostopa

- **Diamantni odprti dostop** – objava v digitalnem repozitoriju praviloma za nekomercialne namene, kjer ni stroškov objave za avtorja
- **Zlati odprti dostop** – objava je za avtorja brezplačna ali za plačilo stroška procesiranja (APC) in dovoljenje shranjevanja v repozitorij s takojšnjo objavo
- **Zlati odprti dostop v hibridnih revijah** – objava članka v naročniški reviji ob plačilu stroška procesiranja (APC)
- **Zeleni odprti dostop** – objava članka v naročniški reviji z dovoljenjem shranjevanja v repozitorij (preprint ali postprint), kjer je možen embargo dostopa
- Politike odprtega dostopa za posamezne revije se zbirajo na spletni strani SHERPA/RoMEO -> https://www.sherpa.ac.uk/romeo/

© IZUM, SIKOM, Bled, 6. junij 2023   8

Licence Creative Commons

OPEN ACCESS

Javna domena
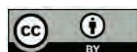
CC BY — Priznanje avtorstva — nekomercialno

Priznanje avtorstva

CC BY-NC-SA — Priznanje avtorstva — nekomercialno – deljenje pod enakimi pogoji
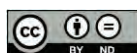
CC BY-ND — Priznanje avtorstva – deljenje pod enakimi pogoji
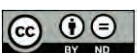
CC BY-NC-ND — Priznanje avtorstva – nekomercialno – brez predelav

CC BY-ND — Priznanje avtorstva – brez predelav

https://creativecommons.si/

9

FAIR in odprti raziskovalni podatki

- Spoštovanje načel FAIR (https://www.go-fair.org/fair-principles/):

    F – Findable – najdljivo (kvalitetni metapodatki – zapisi COBISS)

    A – Accessible – dostopno (platforme za iskanje in odkrivanje informacij – projekt ADZ (COBISS+))

    I – Interoperable – interoperabilno (integracija s preostalimi orodji)

    R – Reusable – ponovno uporabno (obdelava podatkov, HPC)

- Uporaba načrta uporabe podatkov ("Data management plan" (DMP))

- Načelo "Odprto, kolikor gre, zaprto, kolikor je nujno potrebno." ("As open as possible, as closed as necessary" glede dostopa do raziskovalnih podatkov

10

Evropski oblak odprte znanosti

- EOSC – European Open Science Cloud (https://eosc.eu/)
- ustanovljen v letu 2020 na pobudo in s koordinacijo Evropske komisije
- skrbi za ustvarjanje novega znanja in spodbujanje dostopnosti in preglednosti v znanosti (shranjevanje, deljenje, obdelava, analiziranje in ponovna uporaba raziskovalnih podatkov, publikacij, programske opreme …)
- Portal EOSC – enotni dostop do evropskega središča raziskovalnih podatkov, orodij in storitev -> https://eosc-portal.eu/

© IZUM, SIKOM, Bled, 6. junij 2023   11

Slovenska skupnost odprte znanosti

- https://odprtaznanost.si/
- spodbujanje razvoja odprte znanosti v Sloveniji
- vzpostavitev zaupanja vrednega okolja z nemotenim dostopom do raziskovalnih rezultatov in interoperabilnih storitev
- sooblikovanje strateških dokumentov za razvoj odprte znanosti
- sodelovanje pri razvoju in zagotavljanju dolgoročne vzdržnosti nacionalnih raziskovalnih infrastruktur
- usposabljanja in izobraževanja na področju FAIR in odprte znanosti
- …

© IZUM, SIKOM, Bled, 6. junij 2023   12

Digitalni repozitoriji v Sloveniji v podporo odprti znanosti

- Nacionalni portal odprte znanosti -> http://www.openscience.si/
  Digitalna knjižnica Univerze v Mariboru
  Repozitorij Univerze v Ljubljani
  Repozitorij Univerze na Primorskem
  Repozitorij Univerze v Novi Gorici
  Digitalni repozitorij raziskovalnih organizacij Slovenije
  Repozitorij samostojnih visokošolskih in višješolskih izobraževalnih organizacij
  Arhiv družboslovnih podatkov
  VideoLectures.NET
  Digitalna knjižnica Slovenije
  Spletni arhiv NUK
  Digitalna knjižnica Ministrstva za obrambo
  Repozitorij Sci Vie
  CLARIN.SI
  ZRC SAZU

- Digitalni repozitorij COBISS (dCOBISS) – dostop za vse knjižnice v Sloveniji in v mreži COBISS.net

13

dCOBISS in Akademska digitalna zbirka Slovenije – ADZ

Analitika objavljanja v odprtem dostopu (dCOBISS)

Odkrivanje (discovery) vsebin, dostopnih v odprtem dostopu (COBISS+)

14

Digitalni repozitorij COBISS – dCOBISS

- spletna aplikacija IZUM-a za potrebe shranjevanja digitalnih vsebin
- aplikacija je samostojna, vendar integrirana s preostalimi aplikacijami COBISS (COBISS3/Katalogizacija, COBISS+, SICRIS)
- dostopna vsem knjižnicam članicam sistema COBISS.net
- za vnos objave in digitalnih vsebin v repozitorij je potreben bibliografski zapis COBISS (COBISS-ID)
- **aplikacija je namenjena tudi podpori za analitiko odprtega dostopa, ki jo potrebujejo ARRS in raziskovalno-akademske institucije**
- podpora za sinhronizacijo s slovenskimi institucionalnimi univerzitetnimi in raziskovalnimi digitalnimi repozitoriji
- trenutno je v dCOBISS shranjenih skoraj 120.000 objav

© IZUM, SIKOM, Bled, 6. junij 2023   15

Povezljivost dCOBISS z drugimi digitalnimi repozitoriji
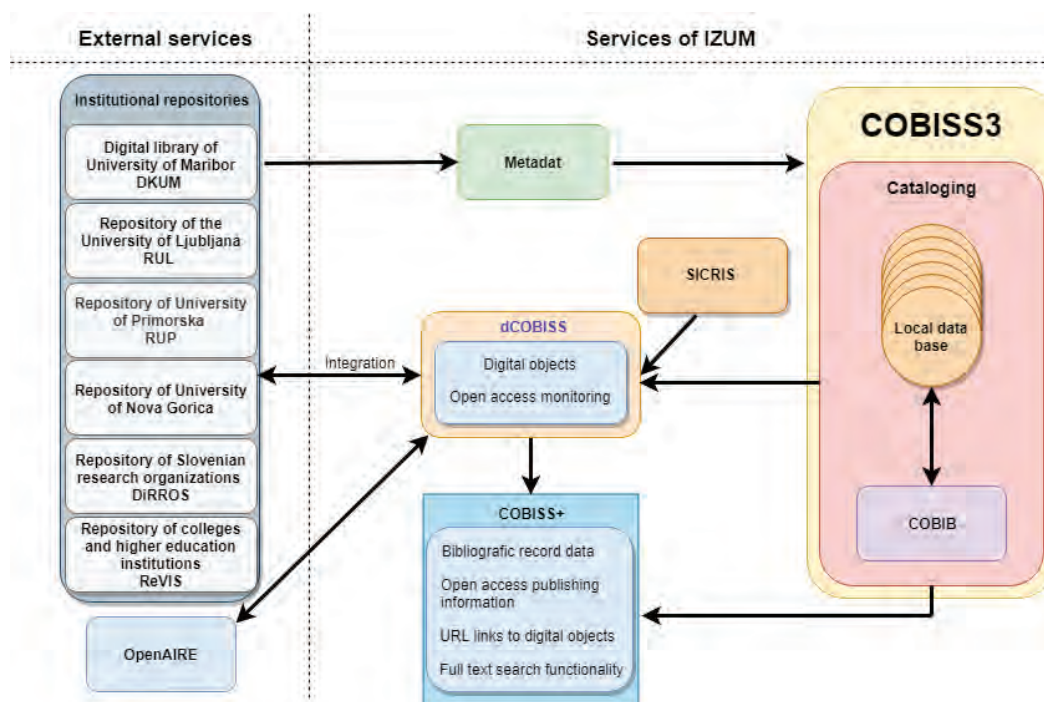
© IZUM, SIKOM, Bled, 6. junij 2023

Kompatibilnost repozitorija dCOBISS z OpenAIRE
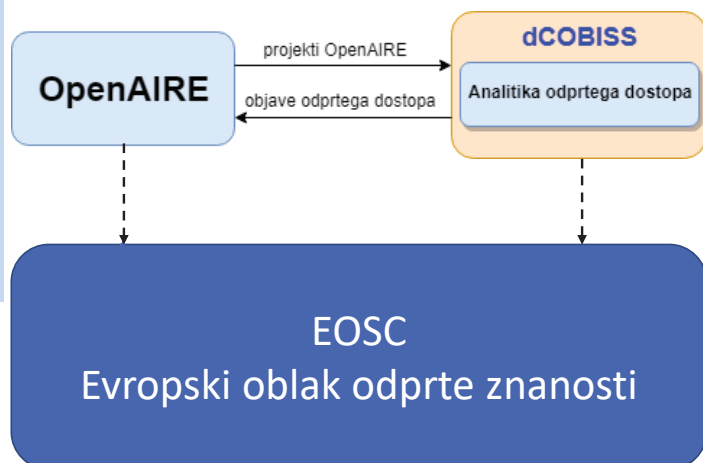
Projekti na platformi OpenAIRE se v dCOBISS uporabljajo za potrebe vnosa objav v odprtem dostopu.

Objave v dCOBISS s podatki o projektih financiranja se prenašajo na platformo OpenAIRE.

V pripravi je integracija z Evropskim oblakom odprte znanosti.

© IZUM, SIKOM, Bled, 6. junij 2023

17

ADZ – Akademska digitalna zbirka Slovenije

https://adz.cobiss.si/

5 portalov na platformi COBISS+
- ADZ – združuje informacije vseh institucij v Sloveniji
- Digitalna knjižnica Univerze v Ljubljani (DiKUL)
- Iskalnik UM:NIK Univerze v Mariboru
- Iskalnik mEga NUK
- Portal Digital : UP Univerze na Primorskem

© IZUM, SIKOM, Bled, 6. junij 2023

18

Odprtodostopne vsebine v ADZ

Odprtodostopne vsebine so dostopne na vseh portalih za kogar koli (avtorizacija ni potrebna) za iskanje in dostop do celotnih besedil.

V ADZ je več kot **200 milijonov** odprtodostopnih zapisov.

Trend naraščanja tovrstnih vsebin

Primer
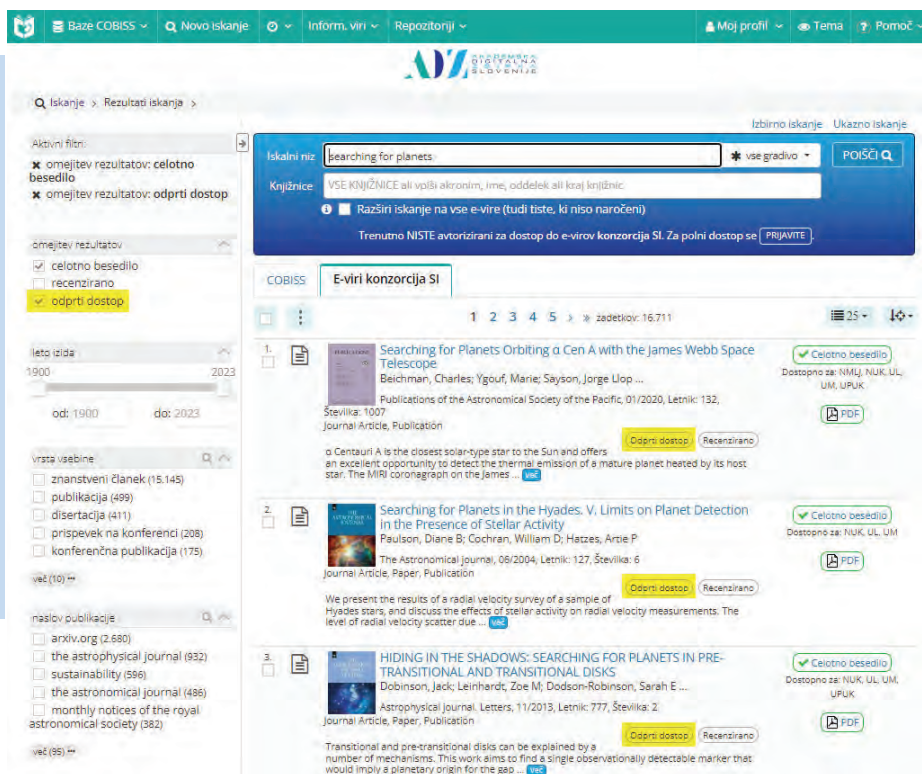
Odprtodostopne revije in e-knjige

Revije: https://adz.izum.si/sfxlcl41/journalsearch

Seznam revij in e-knjig, dostopnih v Sloveniji z informacijami o odprtem dostopu.

Vsaka univerza ima tak seznam, prilagojen njihovemu dostopu.

E-knjige: https://adz.izum.si/sfxlcl41/ebooksearch

© IZUM, SIKOM, Bled, 6. junij 2023

OPEN ACCESS
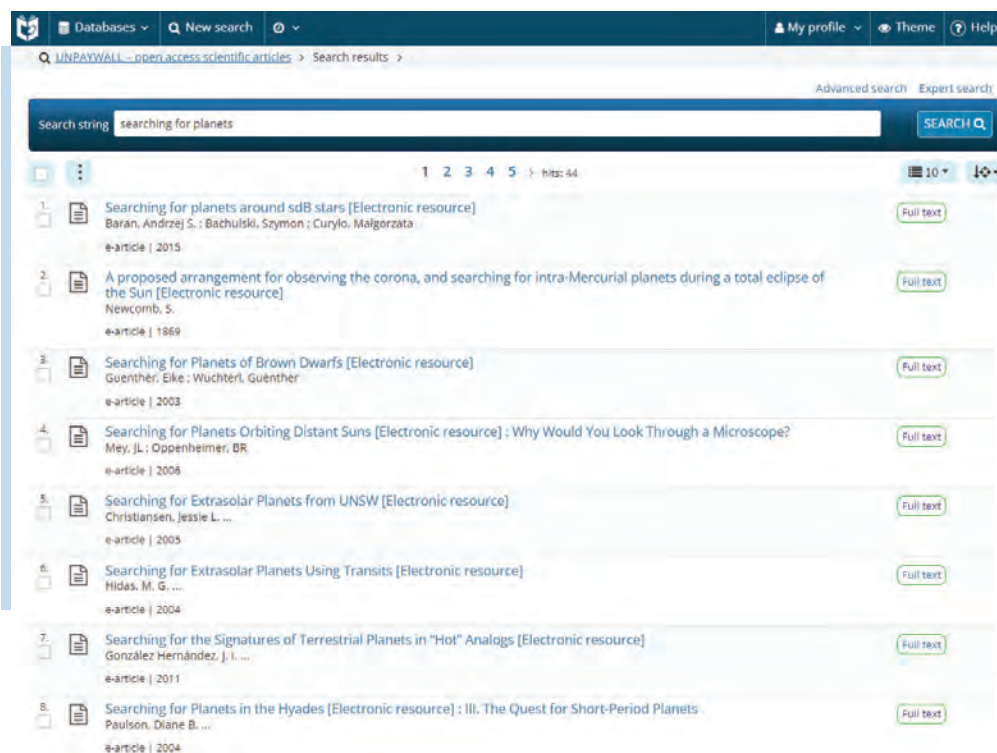
Vključitev servisa Unpaywall: baze podatkov v COBISS+

Baza podatkov je dostopna v COBISS+ vsem uporabnikom COBISS.net.

Dostop do celotnih vsebin več kot **47 milijonov znanstvenih člankov** – servis Unpaywall - https://unpaywall.org/.

Avtorizacija ni potrebna.

Primer   21

Komuniciranje z IZUM-om

- Klicni center: +386 (0)2 25 20 333
- Pon.–pet od 7.30 do 20.00, sob. od 7.30 do 13.00
- E-pošta: podpora@izum.si

f   COBISS - poti do znanja

𝕏   COBISS (@COBISSNET)

▶   COBISS - poti do znanja

in   COBISS / IZUM - Institute of information science Maribor

BLOG   Blog COBISS | Poti Do Znanja

Hvala!
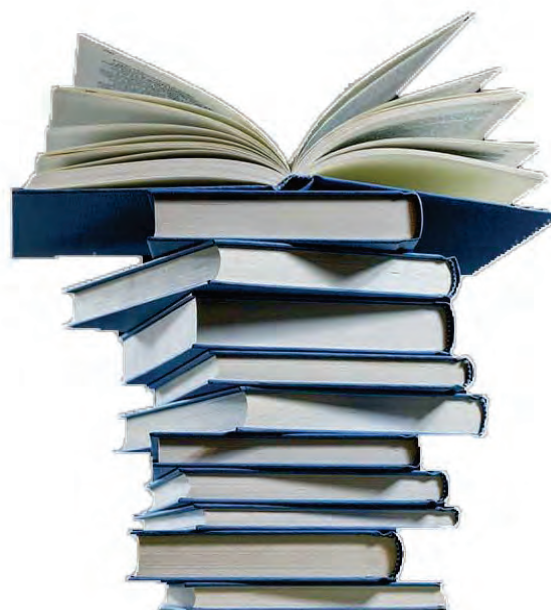
Državni računalniški oblak (DRO)

Slovenian State Cloud (SSC)

Igor Bohinc

Ministrstvo za digitalno preobrazbo, Direktorat za digitalno infrastrukturo

POVZETEK

V prispevku je predstavljeno delovanje Državnega računalniškega oblaka (DRO), ki je v svojem bistvu privatni računalniški oblak državnih organov. Ni tipičen računalniški oblak, ima svoje posebnosti in zahteve. V sedmih letih je preživel več nadgradenj, spremenili smo osnovno namembnost. Na DRO zdaj gostujejo centralizirane storitve za organe državne uprave, storitve za državljane in gospodarstvo ter več kot 400 poslovnih aplikacij državnih organov.

Strojna oprema DRO je stara 7 let in predstavlja tehnologijo iz leta 2015. DRO je v preteklih letih potrdil pravilno odločitev za prehod v zasebni oblak državne uprave, zdaj pa je čas, da ga posodobimo.

SUMMARY

*The paper presents the operation of the State Computer Cloud (DRO), which is essentially a private computer cloud of state bodies. It is not a typical cloud computing; it has its own peculiarities and requirements. Over the course of seven years, it has undergone several upgrades, and we have changed its basic purpose. DRO now hosts centralized services for state administration bodies, services for citizens and the economy, as well as more than 400 business applications of state bodies.*

DRO's hardware is 7 years old and represents technology from 2015. DRO has confirmed the right decision to move to the state government's private cloud over the years, but now is the time to update it.

ABOUT THE AUTHOR

Igor Bohinc has been in the IT industry for more than 20 years. From the beginnings with Novell 3.11, through the maintenance of the server infrastructure of Novell Netware and Windows Server, he slowly moved from a technical profession to the management of projects and systems integration teams. He participated several times as a lecturer at technical conferences (NTK, IJU...). He is currently employed at the Ministry of Digital Transformation as Deputy Director General of the Directorate for Digital Infrastructure.

O AVTORJU

Igor Bohinc je v IT industriji že več kot 20 let. Od začetkov z Novell 3.11, preko vzdrževanja strežniške infrastrukture Novell Netware in Windows Server je počasi prešel iz tehnične stroke do vodenja projektov in ekip sistemske integracije. Večkrat je sodeloval kot predavatelj na tehničnih konferencah (NTK, IJU..). Trenutno je zaposlen na Ministrstvu za digitalno preobrazbo kot namestnik generalnega direktorja Direktorata za digitalno infrastrukturo.

DRO – Državni računalniški oblak

Igor Bohinc
Namestnik generalnega direktorja Direktorata za digitalno infrastrukturo

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DIGITALNO PREOBRAZBO

Direktorat za digitalno infrastrukturo
Davčna ulica 1,
1000 Ljubljana

igor.bohinc@gov.si
http://www.mdp.gov.si

DRO – zakaj?

Stanje 2015 : vsak državni organ živi svoje digitalno življenje po svoje. Vsak zase razvija aplikacije, vsak zase kupuje strežniško opremo, centralnih storitev je bolj malo.

Torej :

- Podatkovne centre državnih organov združimo v DRO

- Virtualizacija je osnova, strojna oprema je bolje izkoriščena

- Konsolidacija verzije programske opreme, skupno licenciranje

- Ena velika, srečna družina informatikov

- DR lokacija, ISO certifikacija

- Skrb za okolje – zelena agenda

DRO ni tipičen oblak

- Storitve se ne plačujejo, uporabljajo jih centralizirani državni organi
- Iaas, Paas?, Saas
- Vpeljan Operations as a Service (OaaS)
- OaaS je razširitev razumevanja IaaS / PaaS
  - nameščanje in konfiguracija poslovnih aplikacij
  - nadzor nad sistemi in aplikacijami
  - tehnična diagnostika
  - administracija podatkovnih skladišč
  - nadgradnja sistemskega in aplikacijskega okolja
  - performančni monitoring
  - informacijska varnost by design

DRO – shema
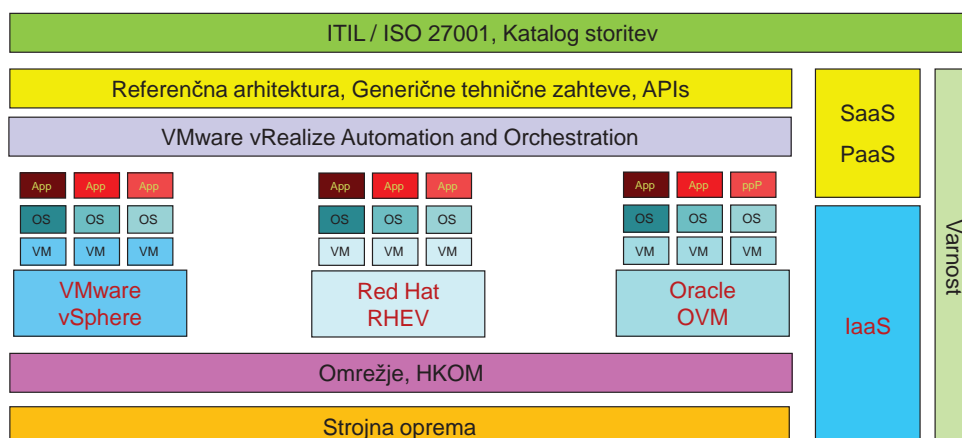
DRO – trenutno stanje

- Strojna oprema
  - 1592 virtualnih strežnikov, 6317 procesorskih jeder
  - 27 TB RAM
  - 8 PB diskovne kapacitete (komaj dovolj po sedmih letih delovanja)
  - Oracle Exadata (1/4 in 1/8)
- Programska oprema
  - Vmware vSphere, vRealize – vOperation & vAutomation
  - RedHat Virtualisation, Oracle LVM (zaradi licenciranja)
  - RHEL, Centos, Oracle Linux, MS Windows Server
- Omrežje
  - 10/25Gb LAN stikala, 32 Gb SAN FC stikala
- Okolje
  - 3 lokacije (2 x Ljubljana, 1 x Maribor – DR lokacija)
  - Električna poraba 460 kW
  - Klimatski sistem 270 kW
  - UPS 2x 500 kVA , diesel agregat 2x 800 kVA

Global Group	Count	CoreCPU	Mem[MB]	Storage[GB]	bckCount	PriceDayCPU[€]	PriceDayRAM[€]	PriceDayOS[€]	PriceDayBACKUP[€]	PriceMonth[€]	PriceYear[€]
Interno	205	686	2.460.584	133.028	94	186,93	452,82	69,33	219,36	39.369	472.422
Drugi organi	463	1464	5.160.872	317.338	295	421,70	963,56	177,37	403,25	86.347	1.036.162
Upravljanje DRO	113	394	1.622.152	45.107	77	97,24	251,89	53,93	28,54	16.385	196.624
HKOM	270	1110	3.142.432	61.738	5	289,84	509,00	48,00	2,81	30.826	369.908
SOC	52	110	440.480	7.283	4	16,36	43,71	5,07	1,41	2.472	29.661
Horizontalne storitve	382	1752	8.163.980	250.863	218	541,60	1.634,39	229,49	216,71	99.396	1.192.749
Microsoft	122	838	6.118.412	492.692	103	259,31	1.234,56	298,77	622,34	114.990	1.379.878
Testne in nerazvrščene	1	2	4.096	44	0	0,63	0,83	0,00	0,00	48	575
VMware infrastruktura	**1592**	**6317**	**26.992.180**	**1.298.888**	**781**	**1.802,29**	**5.067,05**	**875,75**	**1.481,72**	**387.414**	**4.648.971**

4.648.971 € na leto

VMware infrastruktura				
Število strežnikov	1506	1590	6%	
Število vCPU	5911	6313	7%	
RAM [MB]	25467352	26983988	6%	
Diskovni prostor [GB]	1219864	1297883	6%	
Število varnostno kopiranih strežnikov	785	801	2%	

Centralne storitve

- Aktivni imenik
- E-pošta
- Centralni SQL in Oracle
- Spletne strani državnih organov
- eUprava, SPOT
- eJN
- Krpan, eHramba
- ePladenj
- SiPaas, Si-Trust
- Državotvorni registri (CRP, MRVL)
- OPSI
- eCarina, eSociala, eStat, eProstor, Mferac
- Več kot 400 poslovnih aplikacij 44 državnih organov (ministrstev in agencij)

- Krovni dokument GTZ določa DRO arhitekturo, podprte tehnologije in varnostne zahteve. Razvoj aplikacij mora slediti zahtevam v GTZ.
- Dedicirana varnostna ekipa (preverjanje izvorne kode in penetracijski testi

DRO s stališča aplikacij

- DRO ekipe sodelujejo z naročniki pri pripravi tehničnih specifikacij za razvoj aplikacij in nadzoruje pripravo delovnega okolja aplikacije ter postopek nameščanja v produkcijo
- DRO ekipe med delovanjem aplikacij v produkciji nadzirajo delovanje sistemov, nadgrajujejo in vzdržujejo delujoče stanje aplikacije in celega okolja
- Razdelitev odgovornosti : kdo kaj kdaj počne
- Vseh tehnologij ni moč podpreti ali/in uporabljati
- Veliko število razvijalcev in eno oblačno okolje – razvijalci se morajo prilagoditi zahtevam DRO in ne obratno!

DRO zdaj

- DRO je zrel, storitve delujejo
- V načrtih je bil PaaS, kar smo res potrebovali, je bil IaaS, delamo Oaas
- Količina podatkov je presegla vse načrte
- „Legacy" aplikacije povzročajo težave
- SDN ni popolnoma vpeljan

- Centralizacija ni popolnoma zaključena
- Legacy aplikacije, so-odvisnost aplikacij, ne-segmentirana omrežja
- „Tujega nočemo, svojega ne damo"

in v prihodnje…

DRO.next – novi koncepti, nove zahteve

- Nova, dodatna lokacija
- Strojna oprema HCI/DHCI
- Sistemska programska oprema, ki omogoča SDDC
- SDN - v omrežju avtomatiziramo, kar in kolikor lahko
- Xaas – Everything as a Service – DRO nas je naučil, da potrebujemo vse oblike *aaS
- Hibridni računalniški oblak, povezave s podobnimi strukturami v EU
- Vzdrževanje celega sistema z najmanjšim številom administratorjev

- Aplikacije morajo biti razvite v skladu s konceptom „Cloud native application development"
- Varnost je vsebovana od začetka : DevSecOps
- Proces CI/CD, Application lifecycle management -> čimveč avtomatizacije

Kaj smo se doslej naučili

- Dobra ideja, slaba izvedba
- Brez usposobljenih kadrov ne gre
- Brez večletnih zagotovljenih finančnih sredstev ne gre
- Vsega se ne da virtualizirati in/ali centralizirati
- Razvojniki so nevzgojena horda vandalov

NUJNA je podpora vodstva, podpora na čim višjem nivoju

in

česarkoli se lotiš v IT, lahko upaš na 90% uspeh. 10% bo šlo vedno narobe.

Pomen oblačnih storitev za digitalni prehod
Mestne občine Novo mesto

The importance of cloud services for the digital transition of the Novo mesto Municipality

Peter Geršič

Mestna občina Novo mesto

POVZETEK

Mestna občina Novo mesto na različnih področjih uporablja koncepte oblačno zasnovanih omrežij ter storitev, večinoma po principu SaaS. Oblačne storitve tako uporabljamo na nivoju treh stebrov, ki so pomembni tako za razvoj storitev kot tudi za opravljanje osnovnih funkcij lokalne uprave. Ti trije stebri predstavljajo podporo poslovanju, dostopnost informacij ter omogočanje inovativnih storitev. V vseh treh primerih je ključno, da v veliki večini primerov uporabljamo sisteme, ki ne stojijo pri nas, ampak uporabljajo enega od modelov oblačne infrastrukture. Vedno večja pa je zahteva po medsebojnem povezovanju sistemov, kjer stopimo na polje standardizacije ter upravljanja s kontekstom podatkov. Pri tem opozarjamo tudi na nacionalno odsotnost strateškega razvoja oblačne in sorodne infrastrukture na lokalni ravni, kar onemogoča izvedbo hitrih korakov za digitalno tranzicijo tam, kjer je ta najbolj pomembna.

SUMMARY

The municipality of Novo mesto uses the concepts of cloud-based networks and services in various areas, mostly based on the SaaS principle. We use cloud services at the level of three pillars, which are important both for the development of services and for the performance of the basic functions of local administration. These three pillars represent business support, information accessibility and enabling innovative services. In all three cases, the key is that, in the vast majority of cases, we use systems that are not ours, but use one of the cloud infrastructure models. There is an ever-increasing demand for interconnection of systems, where we enter the field of standardization and data context management. We also draw attention to the national absence of strategic development of cloud and related infrastructure at the local level, which makes it impossible to take quick steps for the digital transition where it is most important.

O AVTORJU

Peter Geršič je vodja Razvojno projektne pisarne na Mestni občini Novo mesto in koordinira razvojne projekte in projekte pametnih mest lokalne skupnosti. Njegove kompetence zajemajo sistemsko arhitekturo, vodenje projektov in razvoj rešitev pametnih mest za javni sektor na področju IT, mobilnosti in drugih javnih storitev. Njegove prejšnje izkušnje izhajajo iz obsežnega strokovnega dela na področju digitalnega upravljanja in razvoja sistemov v različnih razvojnih podjetjih kot svetovalec in vodja. Trenutno opravlja tudi naloge direktorja konzorcija ELENA MOBILITY Slovenija.

ABOUT THE AUTHOR

Peter Geršič is head of the Development projects office at Municipality of Novo mesto and is coordinating development and smart city projects of the local community. His competences cover systems architecture, project management and development of smart city solutions for public sector in the field of IT, mobility, and other public services. His previous experience stem from extensive professional work in digital management and systems development at various professional service firms as consultant and manager. At present also serving as the Director of ELENA MOBILITY Slovenia project and consortium.

Pomen oblačnih storitev za digitalni prehod Mestne občine Novo mesto

Izzivi digitalne transformacije v lokalnih skupnostih

Peter Geršič, Mestna občina Novo mesto

Prioritete razvojnih projektov
Digitalni razvoj kot odgovor na sodobne izzive

Demografske spremembe
Demografske spremembe se kažejo na področjih od zaposlovanja do skrbi za starejše...

Mobilnost
Zaradi zelenega prehoda ni dovolj le sprememba energenta, ampak je izziv spreminjanje kulture ter sodobnih rešitev mobilnosti.

Učinkovitost virov
Vprašanje zagotavljanja virov in učinkovito ravnanje z njimi – voda, energija, zelena infrastruktura…

Osnovne točke digitalnega prehoda MO Novo mesto
2020 - 2030

- **Osnovna digitalna infrastruktura** – širokopasovni internet in LoraWan omrežje.
- **Standardizacija sistemov** in prenosa podatkov med njimi (FIWARE).
- **Usmerjenost** v učinkovitost virov.
- **Kontekstualizacija** podatkov.
- **Centralna platforma** zbiranja in upravljanja podatkov – kot cilj združevanja virov in sistemov.
- **Razvoj kompetenc.**
- **Grajenje odpornosti** – potencialna kompleksnost digitalnih sistemov ne sme povečevati ranljivost sistema lokalne samouprave, ampak naj bi gradila odpornost.

Digitalni prehod?
Kaj pomenijo e-government, e-governance za lokalne skupnosti

digitalizacija procesov in IKT podpora poslovanju	e-demokracija e-governance	„Pametna mesta"
sistemi ERP, finančno poslovanje, dokumentni sistemi, e-arhiv…	vključevanje javnosti preko digitalnih orodij – dostopnost, vključenost, opolnomočenje občanov	na večinoma IoT napravah in konceptih temelječi sistemi za upravljanje eko-sistemov urbanih ali podeželskih skupnosti

Mestna občina Novo mesto

Tri vloge digitalnih tehnologij
Kako lahko uporabljamo tehnološke rešitve

Podpora / Enhancement	Dostopnost / Accessibility of information	Omogočanje / Enabling / disruptivna sprememba
Učinkovitejše delovanje, proces, zaradi učinkovitejšega delovanja digitalne tehnologije	„Leveling the field" – omogoča dostop do informacij vsakemu, ni več prepada med npr. različno premožnimi skupinami	Storitev ali produkt brez neke lastnosti digitalne tehnologije ni mogoč (Uber, 100 % kopiranje brez izgube…)

Mestna občina Novo mesto

VARCITIES
Razvoj naravnih in digitalnih rešitev za zdravje ljudi

Future-City Visions

Human Centred

Green Public Spaces

Smart & Resilient

Project duration: Sep 2020 - Feb 2025
Project status: ongoing
Funding: Horizon 2020 EU funding /Project
Partners: 7 pilot cities
Total project budget: 11.000.000 €

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 869505
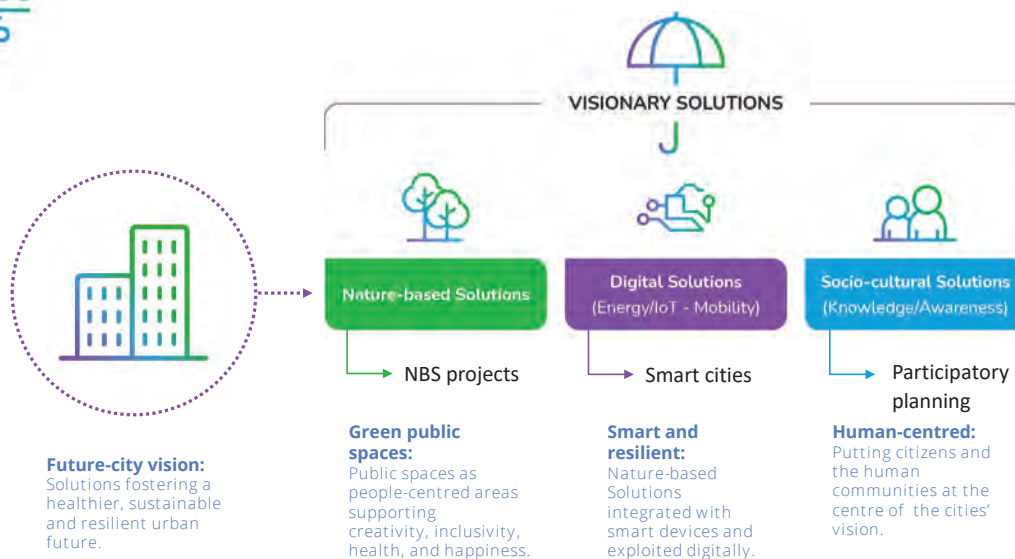
Mestna občina
Novo mesto

VARCITIES
Razvoj naravnih in digitalnih rešitev za zdravje ljudi

VISIONARY SOLUTIONS

Nature-based Solutions

Digital Solutions
(Energy/IoT - Mobility)

Socio-cultural Solutions
(Knowledge/Awareness)

NBS projects

Smart cities

Participatory planning

Future-city vision:
Solutions fostering a healthier, sustainable and resilient urban future.

Green public spaces:
Public spaces as people-centred areas supporting creativity, inclusivity, health, and happiness.

Smart and resilient:
Nature-based Solutions integrated with smart devices and exploited digitally.

Human-centred:
Putting citizens and the human communities at the centre of the cities' vision.

Mestna občina
Novo mesto

VARCITIES
Razvoj naravnih in digitalnih rešitev za zdravje ljudi

VS4
Sensors

Quantitative data on visitor flow / machine vision

Did the visitors used provided flow of experience? How to direct them?

VS5
Wearables

Health & Well-Being Parameters

What type & intensity of movement did we inspire in the visitors?

Mestna občina Novo mesto

NOVO MESTO

SITI**UM** – sistem „mestne kartice"
Razvoj digitalnih storitev za občane

Mestna občina Novo mesto

NOVO MESTO

Digitalna transformacija na lokalni ravni

— **Razvijamo vertikale**, ki so za nas pomembne (promet, okolje, državljani, viri: voda, energija) z razumevanjem naše specifičnosti in uporabo skupnih standardov (FIWARE).

— **Krepimo kompetence** za uporabo novih pristopov.

— **Rešitve širimo s sodelovanjem z drugimi skupnostmi** (sosednjimi, regionalnimi, funkcionalnimi...) in jim prenašamo znanja in sisteme.

— **Proaktivno sodelujemo pri razvoju rešitev na regionalni in nacionalni ravni** (skupni gradniki platform in drugi enotni moduli za podporo digitalizaciji javnega sektorja).

Podporniki
Sponzors

OPERATIVNI CENTER KIBERNETSKE VARNOSTI

VAŠA 360° VARNOST 365 DNI V LETU

360° varnost vam zagotavlja najsodobnejšo kibernetsko zaščito. Zaradi vse večje kompleksnosti kibernetskega okolja in varnostnih groženj brez kibernetske varnosti digitalni razvoj ni več mogoč. Zato naj za vašo varnost in najvišjo stopnjo kibernetske zaščite skrbijo naši visoko certificirani strokovnjaki iz **Operativnega centra kibernetske varnosti**, ki **24 ur na dan in 365 dni v letu** spremljajo in analizirajo varnostne dogodke ter se hitro in učinkovito odzivajo na kibernetske grožnje.

Operativni center kibernetske varnosti je **certificiran po najvišjih mednarodnih standardih**, je **član mednarodnih organizacij s področja kibernetske varnosti** in prejemnik nagrade **za najbolj inovativno varnostno rešitev**, ki jo podeljuje Institut za korporativne varnostne študije v sodelovanju s Slovenskim združenjem korporativne varnosti.

POSLUJTE VARNO. POSLUJTE DIGITALNO.

360°

Telekom Slovenije, d.d., Ljubljana.

TelekomSlovenije
Vedno na boljše.

S&T ISKRATEL

Zasebna mobilna omrežja 5G

Zgradimo vam **visoko zmogljivo**, **varno** in **zanesljivo** zasebno mobilno omrežje 5G, ki vam bo koristilo iz več razlogov:

- Izboljšana povezljivost z občutno višjimi hitrostmi in nižjimi zakasnitvami, saj se industrije zanašajo na prenos podatkov v realnem času;
- Zelo zanesljivo in robustno omrežje zagotavlja nemoteno delovanje, saj namenska infrastruktura povečuje zanesljivost in odpornost kritičnih aplikacij in storitev;
- Varnost in zasebnost občutljivih podatkov si zagotovite z večjim nadzorom nad svojo omrežno infrastrukturo;
- Prilagodljivost omrežja na podlagi posebnih zahtev, kjer zagotovimo optimalno zmogljivost in dodelitev virov za vsak primer uporabe;
- Industrijska avtomatizacija in Internet stvari (IoT) sta zagotovljeni s potrebno pasovno širino in nizko zakasnitvijo za podporo obsežnim uvedbam IoT.

Lastni razvoj ključnega dela omrežja, dolgoletne izkušnje in vodilna telekomunikacijska vloga v regiji so zagotovilo za končni uspeh.

ZAVEZANI SMO H GRADNJI OMREŽIJ, KI SO VARNA, STABILNA IN ZANESLJIVA

VARNOST, BREZ KOMPROMISOV

HUAWEI