No.47
June 2021

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/SPONSORED**

Oracle Security for Telecom Operators

Sponsored by Oracle Communications

- The 5G security model is fundamentally different compared to the legacy telco security model. Communications service providers need partners that have in-depth expertise in securing cloud native environments throughout the stack.
- Oracle Communications has critical capabilities and expertise in building, operating and securing telecom network functions, cloud native development environments and public cloud infrastructure.
- The Oracle Communications portfolio offers a critical supply chain alternative to Ericsson, Nokia and Huawei - as well as to Google, AWS, Azure and VMware.

Opportunity and Risk with Telco Transformation

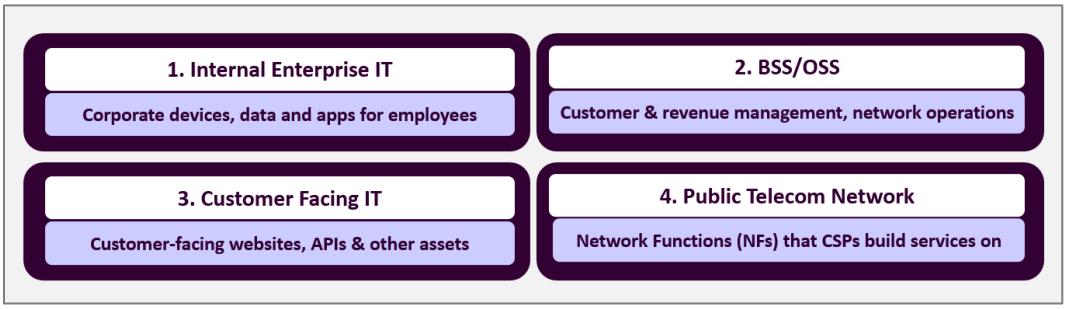
Increased dependence on public cloud providers and cloud native 'cloudification' of their own data centers is driving the digital transformation or 'telco transformation' goals of communications service providers. It's useful to break down the core technology assets of these companies into the four primary domains shown in **Figure 1**. In the case of the enterprise IT domain, the opportunities and risks of cloud migration are much the same as for any organization. That's also largely true of BSS/OSS as these are also IT systems.

Business surveys routinely show cyber security risk as a critical barrier to moving workloads, especially sensitive workloads, into the cloud.

It's when they're evolving their public telecom infrastructure from a model driven by proprietary hardware or Network Functions Virtualization (NFV) to a cloud native 5G Core that communications service providers face unique challenges. These arise from the multi-layered complexity of a telecom networking environment, the challenges of 5G's new Service Based Architecture (SBA), and the specific regulations they face as government-licensed Critical National Infrastructure (CNI) entities.

Business surveys routinely show cyber security risk as a critical barrier to moving workloads – especially sensitive workloads – into the cloud. That's largely because security gaps arising from benign misconfigurations are the single biggest cause of security breaches in the cloud. Advanced tools are available for building, operating and managing clouds securely but communications service providers don't always use them, often because they lack the internal expertise to consistently make best use of them.

Figure 1: The Four Technology Domains of Telco Transformation



Source: HardenStance

The big opportunity with telco transformation lies in embracing the cloud native principles of agile software development and DevOps frameworks; Network Functions (NFs) composed of microservices running in containers with open APIs; and the ability to run these NFs in any public or private cloud that's built according to cloud native principles. This requires major changes in a communications service provider's use of people, technology and processes, which inherently introduces new risk. As they are generally risk-averse, this introduction of new risk has to be very carefully managed.

The amount of risk associated with deploying in a public cloud varies according to the volume and sensitivity of the workloads - whether they're enterprise IT workloads; NFs driving network services for all customers; or NFs dedicated to one service or one customer such as via a 5G network slice. An additional risk assessment is needed where communications service providers build private clouds. That's because they also have to secure the foundational cloud infrastructure they build from the ground-up (and the cloud native development platform if they assemble that themselves as well.) All sectors of industry also face a world-wide shortage of qualified cyber security professionals. It's not just a matter of recruiting and paying for those skills but of retaining them as well.

The Rise – or Fall – of the Untrusted 5G Supplier

Telecom security risk has gained a very high profile due to the U.S. and many allies classifying Chinese vendors as "Untrusted Suppliers" and restricting or excluding them from 5G contracts. But nation states directing domestic telecom vendors to try and melt trojan malware into their code to enable eavesdropping is only the tip of the iceberg in terms of supply chain and other cybersecurity risk the telecom sector faces now.

Communications service providers are among the victims of the recent supply chain attacks triggered by the SolarWinds breach.

As stated by FireEye, a leading Incident Response company, in one of its first blogs following the discovery of the attack, communications service providers are among the victims of the recent supply chain attacks triggered by the SolarWinds breach. It's not as uncommon as it should be to find serious bugs in commercial telecom vendor software either. Just a couple of years ago, the Canadian operator, Telus, found 'Shellshock' – first discovered in 2014 – in a master certified image of a critical NFV platform.

The colossal scale of the SolarWinds attack is giving even greater impetus to government-mandated action on supply chain security. The 'Prague Principles' emerged from a 2019 cyber security conference in the Czech capital attended by government officials from 32 countries, the EU and NATO. The EU incorporated these principles into its 'EU Toolbox on 5G Cyber Security', released in January 2020. Among other things, this specifies that 5G vendors must demonstrate a secure software development process and support open interfaces. The Prague Principles are routinely cited now by other governments including the US and the UK.

The telecom sector routinely suffers everyday enterprise breaches and outages due to ransomware, phishing, DDoS attacks or APIs flaws. It is also vulnerable to attacks exploiting telecom protocols like SS7 and Diameter. Without robust firewall protection, these allow mobile networks to be used to steal from on-line bank accounts or track the location of targeted businessmen, political opponents or spouses. As communications service providers look to exploit and de-risk digital transformation, public cloud providers are becoming critical partners for 5G supplier diversity and cyber security risk mitigation.

- Compare the revenues of any communications service provider and any big cloud provider. Now take, say, 3% of each number to represent their spending on security to gauge how much more the big cloud providers are currently spending. Now consider that not much telecom sector spending goes on cloud security yet, whereas all of a cloud provider's does. Now consider the cumulative amount a cloud provider has spent on cloud security over, say, fifteen years. The unavoidable conclusion is that a cloud provider's investment and know-how in cloud security – combining openly available as well as proprietary security features - dwarfs that of most communications service providers.

- With the exclusion of Chinese vendors from 5G contracts and the momentum behind the Prague Principles, communications service providers must turn to other vendors to mitigate the risk of over-dependence on Ericsson and Nokia. Public cloud providers like Microsoft and Oracle Communications that sell their own 5G NFs are now de facto key players in 5G network supply chain resiliency alongside these telecom vendors.
- As procurement strategy is aligned with new supply chain diversity mandates, it's essential to avoid making the same mistake in procuring public cloud services that has been made with mobile network suppliers. That means embracing a multicloud strategy rather than becoming dependent on just one or two cloud providers.

Communications service providers must turn to other vendors to mitigate the risk of over-dependence on Ericsson and Nokia.

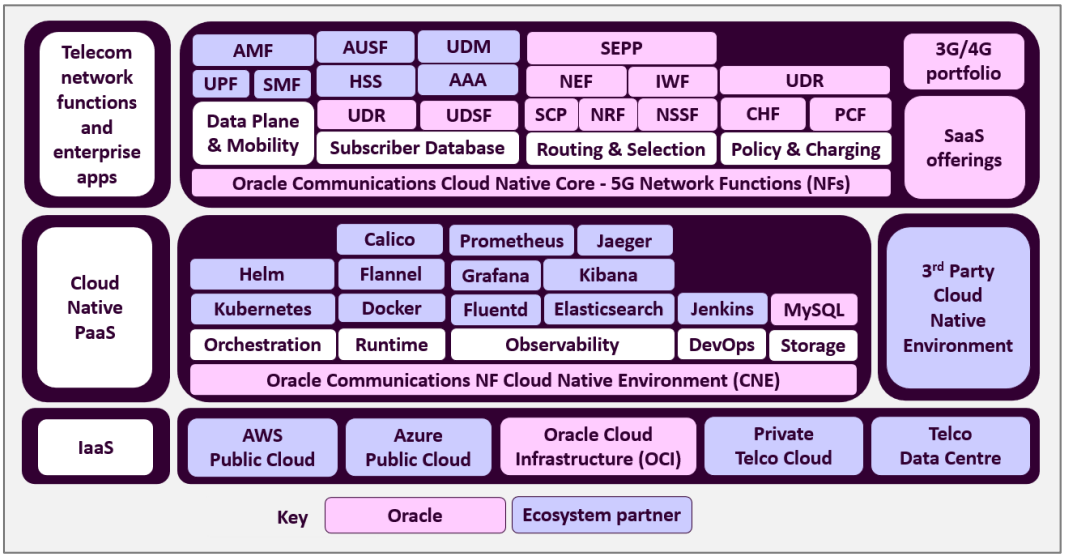
The Oracle Communications Portfolio

This HardenStance Briefing describes Oracle Communications' portfolio for the communications market and how its own internally developed parts of the portfolio are secured by the company's own know-how in cyber security. As depicted in **Figure 2**, the portfolio comprises three main layers:

- **Network Functions:** the top layer consists of a portfolio of cloud native 5G network functions. It also includes 3G and 4G network functions that are available in older virtualized and hardware appliance formats. This part of the portfolio also includes SaaS offerings for both communications service providers and enterprises.
- **Cloud Native Platform as a Service (PaaS)**: the middle layer comprises Cloud Native PaaS platforms such as Oracle's own NF Cloud Native Environment (NF CNE).
- **Infrastructure as a Service (IAAS):** Here the company offers Oracle Cloud Infrastructure (OCI) and supports private telco cloud and other public cloud options.

Consistent with cloud native principles, there is inter-operability between internally developed and third party hardware and software components throughout the stack. Aligned with this portfolio, Oracle Communications participates in several industry associations, standards fora and government advisory councils that are driving telco transformation and telecom security. Among these are the Cloud Native Computing Forum (CNCF) where Oracle serves as a platinum member; the GSM Association's Fraud and Security Group (FASG); 3GPP; the TM Forum; the FCC Communications, Security, Reliability and Interoperability Council (CSRIC); ETSI TC_Cyber; and the IETF.

Figure 2: The Oracle Communications Portfolio



Source: HardenStance/Oracle Communications

Cloud Native Core Solutions for 5G

As detailed on the next page, Oracle Communications has a strong pedigree in control plane solutions for 3G, 4G and fixed line networks going back many years. The company has brought this heritage to bear to assemble an extensive portfolio of cloud native, 3GPP-compliant, NFs for the 5G era. This positions the company as an important alternative to incumbent 5G network vendors. Recent announcements include a customer win with DISH Wireless and multivendor proof of concept (PoC) with Telenor.

As shown in **Figure 3**, the portfolio consists of cloud native 5G NFs for the four domains of data plane and mobility; subscriber database; routing and selection; as well as policy and charging. All the control plane NFs shown in pink have been developed internally. These are supplemented by data plane and mobility NFs like the User Plane Function (UPF), shown in pale blue, which are sourced from third party vendor partners. All of the 5G NF portfolio shown is Generally Available (GA).

While all the 5G NFs featured in the portfolio benefit from Oracle's secure development and secure verification processes, the ones that can make the biggest impact from a scalability, resiliency and security perspective are those that feature in the routing and selection part of the portfolio.

Oracle Communications has combined open source mesh technologies with its mobile network signaling heritage to develop a Service Communication Proxy (SCP) that is 5G-aware.

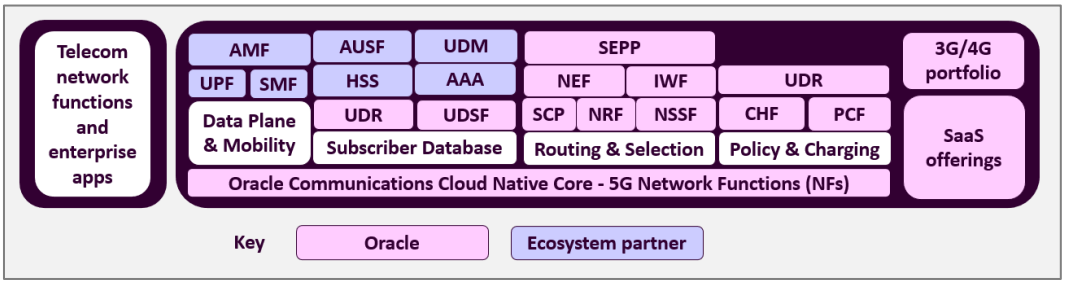
The Service Communication Proxy and Secure Edge Protection Proxy

Perhaps the two most significant in that context are the Service Communications Proxy (SCP) and the Secure Edge Protection Proxy (SEPP). The Service Communication Proxy (SCP) is a new NF specified for 5G by 3GPP. The easiest way to think of the SCP is as the 5G equivalent of a Diameter Routing Agent (DRA), which secures and connects the interaction between NFs in a traditional, centralized 4G network. To achieve similar outcomes in 5G's much flatter Service Based Architecture, where there is a much larger volume of interactions between individual NFs, the SCP needs to leverage relatively new service mesh ideas and technology that are new to mobile networks.

Oracle Communications has combined open source mesh technologies with its mobile network signaling heritage to develop an SCP that is 5G-aware, meaning that it has awareness of the attributes published by other producers as part of their NF profile. It's this which enables it to take optimal load balancing and traffic prioritization decisions within the SBA. Hence it can optimize and simplify signaling and routing as 5G networks scale up as well as out in distributed Multi access Edge Compute (MEC) use cases.

The SEPP protects the HTTP/2 control plane messages between one mobile operator's 5G core and another's, as SS7 and Diameter firewalls protect the 3G and 4G interconnect. Unlike SS7 and Diameter, HTTP/2 is an IT protocol not a telecom protocol. So while it's open to a huge global pool of developers that can help fix flaws in it, many, many more malicious hackers have the skills to exploit HTTP/2 to criminal ends than could ever exploit SS7 and Diameter. Since SEPP is already specified, it's available to operators in advance of them rolling out 5G roaming agreements at scale rather than them having to wait for these security specs to be written retrospectively as in the past.

Figure 3: The Oracle Communications Portfolio of Network Functions



Source: HardenStance/Oracle Communications

Support for 3G/4G and Communications SaaS

While the 5G era marks a key inflection point where the requirements of the telecom sector finally converge with the cloud native requirements of the public cloud, one of Oracle Communications differentiators is the company's supporting portfolio of control plane networking and security products that are critical for 3G, 4G and fixed networks. These are shown as the first of two layers depicted in **Figure 4**. These are all delivered in on-premises as well as NFV-compliant virtualized software formats.

Some of these products also have cloud native releases in roadmap. For example, the Session Border Controller (SBC) already comes in separate appliance and vSBC formats, providing SIP firewalling protection against fraud, DDoS attacks and malware distribution within and between 3G and 4G networks. As communications services providers look to evolve their SBC requirements into 5G with stronger encryption, multifactor authentication and broader Zero Trust principles, as well as STIR/SHAKEN functionality, the Oracle SBC is also being developed as a cloud native NF.

The SBC is just one of three signaling firewalls in the Oracle Communications portfolio. The other two are the Diameter Signaling Router (DSR) - the company's Diameter Routing Agent (DRA) for 3G and 4G networks – and the SS7 firewall functionality which is embedded in the Oracle Communications Eagle Signaling Transfer Point (STP).

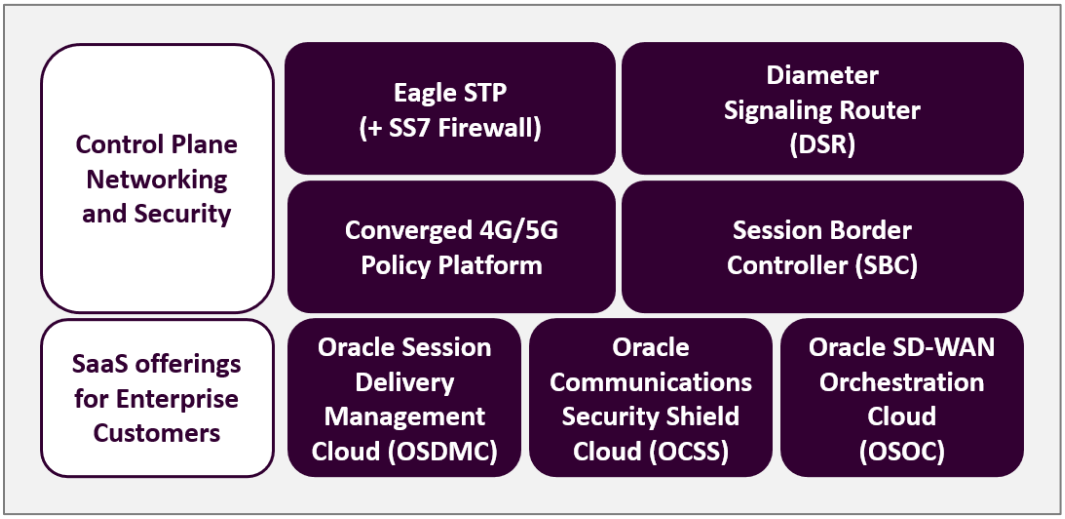
The vulnerabilities in SS7 and Diameter have been known about for years but real-world attacks are mounting now.

Real World SS7 Attacks in Germany, the UK and Israel

The vulnerabilities in SS7 and Diameter have been known about for years but real-world attacks are mounting now. In the last three years, there have been incidents in Germany, the UK and Israel – three of the world's most developed markets - in which several consumers in each market have had money stolen from ordinary bank or cryptocurrency accounts by exploiting SS7 vulnerabilities to manipulate SMS authentication messages.

Exploiting SS7 and Diameter flaws is also among the tools being used to grow the Espionage as a Service market. For a few hundred or a few thousand dollars, more or less anyone nowadays can pay for the location of a target individual's mobile phone to be tracked, including in real time, by accessing mobile networks to manipulate signaling messages. The practice is much more widespread than generally recognized. Signaling firewalls provide the best tools for protecting end users against these threats. Lastly, the Converged Policy Platform is a cloud native microservices based unified policy framework that supports policy functions across 4G and 5G.

Figure 4: A Portfolio of 3G/4G Networking and Enterprise SaaS Products



Source: HardenStance/Oracle Communications

A Variety of SaaS Applications

As shown in the bottom layer of **Figure 4**, three Communications Cloud Service SaaS offerings are available for communications service providers and enterprise customers via OCI, Oracle's IaaS offering. These three SaaS offerings are:

- **Oracle Session Delivery Management Cloud (OSDM):** this enables communications service providers and enterprises to monitor Key Performance Indicators (KPIs) and call traffic details via integration with monitoring solutions.
- **Oracle SD-WAN Orchestration Cloud (OSOC)**: this manages and monitors the lifecycle of an Oracle SD-WAN deployment.
- **Oracle Communications Security Shield Cloud (OCSS)**: this protects against malicious voice traffic and is applicable to a communications service provider's own contact centers or to enterprise customers. This also has potential to be developed as a carrier grade component of a STIR/SHAKEN solution to protect end users from fraudulent and other nuisance calls.

NF CNE and Other Cloud Native PaaS Options

Embracing a cloud native architecture in which application components are broken down into independent microservices instead of building monolithic applications, and embracing agile development and DevOps instead of a traditional waterfall model, has far-reaching impacts on the skills, processes and technologies used throughout a communications service provider's organization.

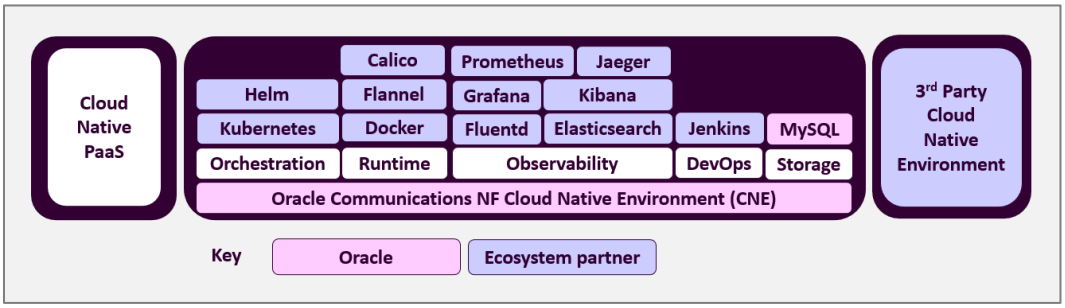
Without proper hardening, even entry-level hackers can obtain API keys, gain full access to a Kubernetes environment in minutes, and potentially shut down the network.

A microservices architecture using Kubernetes-orchestrated containers is the core technology engine for achieving the automation, scalability and faster time to market goals of telco transformation. But securing a cloud native environment to telecom standards requires a lot of expertise. In this so-called 'chaos engineering' environment, it's pieces of code themselves - not Systems Administrators or engineers with keys loaded onto their laptops – that need to be granted specific access rights to resources. Kubernetes has to place each of the resources needed by a given application, including the OS, into separate containers. The containers have to be configured so that they can't see into one another, or you risk cross-pollination of malware across the environment.

Out of the box, Kubernetes allows containers to run as root, meaning they can execute any command and access any resource they like. Without proper hardening, even entry-level hackers can obtain API keys, gain full access to a Kubernetes environment in minutes, and potentially shut down the network. Robust key management and Role Based Access Control (RBAC) enabled with least access privileges is only the tip of the iceberg in terms of what's needed to secure a cloud native development environment.

Also, the array of proprietary tools that communications service providers have built and tweaked in their dev environment over years can't be ported into a cloud native environment. Instead, a variety of cloud native, open source, runtime, observability and DevOps tools must be embraced alongside the Kubernetes orchestration environment.

Figure 5: Oracle NF CNE and Third Party Cloud Native PaaS Options



Source: HardenStance/Oracle Communications

These cloud native tools are well established in enterprise IT circles but they're relatively new to the telecom sector. Adopting them triggers two new operational requirements. One is for all these unfamiliar tools to be integrated into the dev environment and maintained on an ongoing basis; the other is for dev teams to be trained in using them.

As shown in **Figure 5**, and consistent with cloud native principles, Oracle Communications NFs can run in third party cloud native PaaS environments. However they are optimized to run in the company's own cloud native PaaS offering. This is Network Function Cloud Native Environment (NF CNE), a highly integrated, Kubernetes-based, cloud native PaaS solution for the telecom market. Drawing on the work of the Cloud Native Compute Foundation(CNCF), NF CNE leverages open source tools to drive operation and management of 5G NFs with full lifecycle automation in a production and carrier grade environment. NF CNE, along with Oracle Communications 5G NFs, are built according to eight core principles of successful cloud native operations.

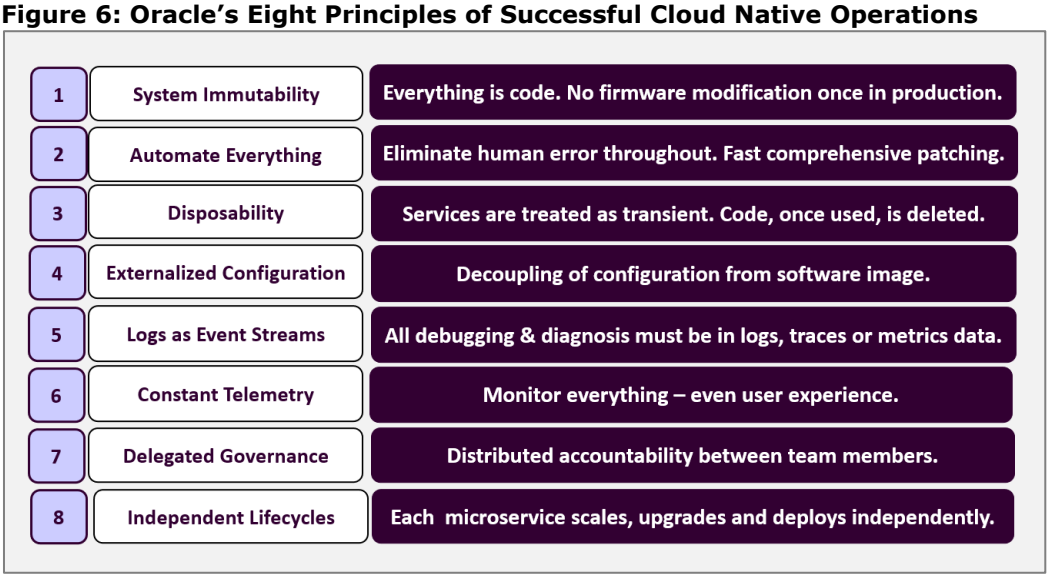
These are depicted in **Figure 6** and described below:

Highly automated patching in a homogeneous cloud environment like NF CNE can substantially improve cyber security posture compared with legacy data centers.

1. **System immutability.** Everything, software and configuration, is code. All changes are made through Continuous Integration/Continuous Development (CI/CD) where they are deployed as immutable artifacts. No manual configurations or customizations are allowed. Any changes not coming though the delivery pipeline can be considered malicious.
2. **Automate everything.** All aspects of build, test, verification, and deployment are automated, including backup, recovery, password/key rotation. Fully automating the DevOps pipeline (including verification and testing) removes potential for human error, allows changes to be applied with confidence, and provides for rapid repair.

   As previously noted, misconfigurations and unpatched systems are the biggest threat vector in the cloud. Communications service providers already see this risk in their relatively heterogenous data center environments. Today, many of them still take up to a month to implement even critical patches, which has resulted in some very high profile data breaches. The nation state-backed 'Soft Cell' attack disclosed in July 2019, and another one by the Hezbollah-linked 'Lebanese Cedar' threat group disclosed in January 2020, both exfiltrated customer data – Call Data Records (CDRs) in the case of 'Soft Cell'. They did this by initially exploiting unpatched servers in communications service provider data centers.

Figure 6: Oracle's Eight Principles of Successful Cloud Native Operations



Source: HardenStance/Oracle Communications

Highly automated patching in a relatively homogeneous cloud environment like NF CNE can substantially improve cyber security posture compared with legacy data centers. It allows patches to be universally deployed within hours of being released rather than days or weeks.

3. **Disposability**. All services are treated as short lived. Instead of focusing on never failing, services are designed to go up and down quickly without service interruption. Code should be disposable - if it's only needed temporarily in run mode, it should be deleted immediately after. Ensuring code doesn't reside permanently in the application any longer than needed reduces the attack surface. Regular 'repaving' of the environment removes failing services and allows new ones to be deployed.
4. **Externalized configuration**. Configurations (including passwords, credentials, location of backing stores, etc) are kept in an external storage system, separate from the software image, and like software, can be treated as a build artifact in a controlled and versioned manner. Versioned configuration enables development and production parity as an artifact and can eliminate costly operational errors.

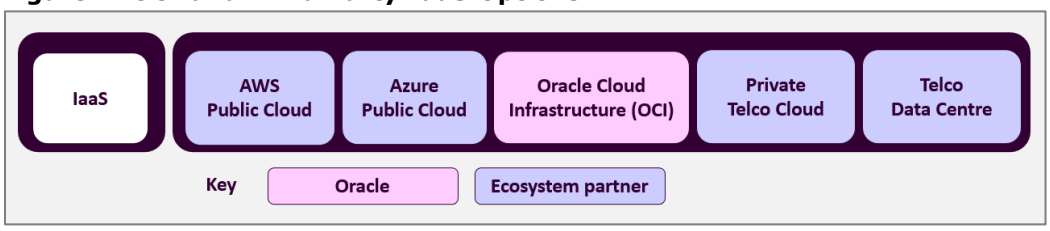
Teams delivering a service can be responsible for operating the service while top level administrators can focus on things like securing resources in your cloud.

5. **Logs as Real-Time Event Streams.** Everything needed to debug or diagnose any functional, operational, or security issue is in logs, traces, or metrics data. These are treated as a real-time stream of time-ordered events and stored in a centralized collector outside the system. Here, better threat monitoring, forensics, and diagnostics can be done through event correlation or analyzing the holistic view.
6. **Constant Telemetry**. This should extend beyond simple monitoring of server load, disk utilisation, memory consumption to cloud metrics that might be specific to an individual application, even to the user experience.
7. **Delegated Governance**. Some shared aspects of the environment are centrally managed, but Administrators can still delegate some tasks. For example, teams delivering a service can be responsible for operating the service while top level administrators can focus on things like securing resources in your cloud.
8. **Independent Lifecycle**. Upgrading, scaling and deploying each microservice independently is critical to other cloud native principles as well as minimizing the amount of change in the system at a given time. Such decoupling also makes other principles like repaving easier and promotes easier isolation of issues.

OCI and Other IaaS Options

As with other layers in the Oracle Communications portfolio, and as shown in **Figure 7**, communications service providers can choose to run their applications in their own private telco cloud, third party public clouds or in Oracle's own Gen 2 Oracle Cloud Infrastructure (OCI). OCI is Oracle's integrated IAAS/PaaS offering, built according to the company's "security-first" design principles. Having first supported Oracle's ERP and database software, OCI supports third party workloads now. Zoom runs their own workloads on it, for example. Oracle's ruggedized Roving Edge device for edge applications, announced earlier this year, fills the last significant gap in its IAAS portfolio. This enables Oracle Communications to compete for communications service provider

Figure 7: OCI and Third Party IaaS Options



Source: HardenStance/Oracle Communications

business against Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure as well as Ericsson, Nokia and Huawei.

The 'seven pillars of a trusted cloud' depicted in **Figure 9** are the design principles that drove Oracle to use security as a differentiator with Gen 2 OCI. These seek to learn from the failings in legacy cloud designs to reduce the risk of cyber attacks getting through - as well as reduce the 'blast radius' of those that do get through.

A critical building block of Gen 2 OCI's security architecture is that it assumes the eventual compromise of some cloud instances. It is therefore designed to completely eliminate the possibility of any attacks spreading between tenant networks and the cloud provider itself, whether they are bare metal or Virtual Machine (VM) instances. It achieves this through the first of the seven principles. This is customer isolation through hardware and software isolation as presented in **Figure 8** below.

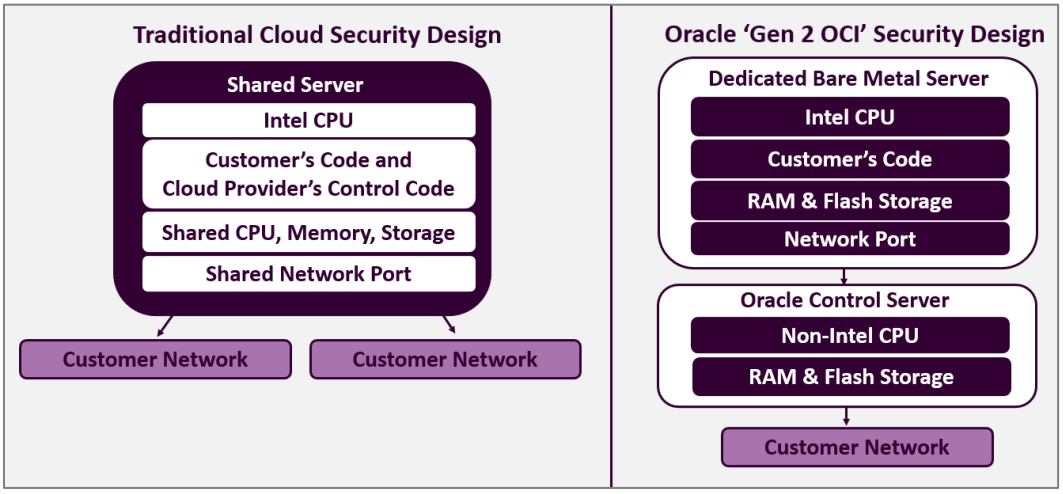
Physical Isolation between Tenant and Cloud Provider

As shown on the left of **Figure 8**, traditional data center security architectures allow the cloud provider and tenant to share the same hardware. That means the cloud provider and the tenant can potentially see one another's data - hence potentially share one another's malware. The Gen 2 OCI design prevents this by enforcing physical isolation between the cloud provider and tenant domains.

Gen 2 OCI Oracle's own control code is physically isolated or air-gapped by being deployed on its own dedicated bare metal server.

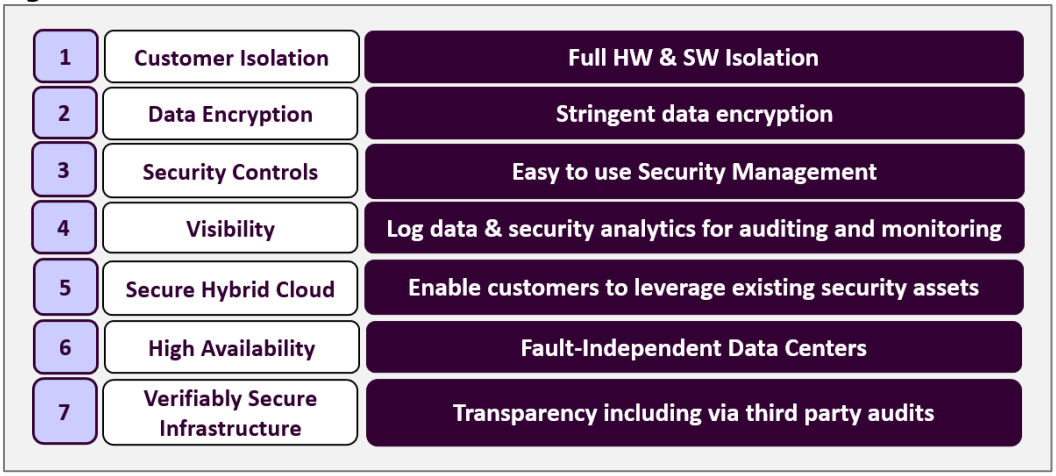
As shown on the right, in Gen 2 OCI Oracle's own control code is physically isolated or air-gapped by being deployed on its own dedicated bare metal server. To ensure any bare metal host is only ever made available to a Gen 2 OCI tenant in pristine condition, it is wiped clean of any software used by the previous tenant. The process leverages a Hardware Root of Trust within the server chassis. This allows OCI to force it to execute a known bootstrap image in a way that's designed to be tamper-proof.

Figure 8: Hardware and Software Isolation in the Gen 2 OCI Architecture



Source: HardenStance/Oracle Communications

Figure 9: Oracle's Seven Pillars of a Trusted Cloud Platform



Source: HardenStance/Oracle Communications

Oracle's second principle of a trusted cloud is that data should always be encrypted at rest and in transit. Whilst the benefits are clear, organizations can nevertheless be tempted to bypass this security control because traditional approaches to encryption in the cloud do tend to impact performance. Gen 2 OCI gets around this via a proprietary approach to automating encryption within the silicon as default. This prevents encryption from being turned off while assuring zero impact on performance.

As of January 2021, OCI had 29 regions or Points of Presence live as well as 6 Interconnect regions live with Microsoft Azure.

Security Controls Must be Easy to Use

Oracle's third pillar of a trusted cloud states that security controls must be effective and easy to use. This refers to tools preventing unauthorized access; allowing operational responsibilities to be segregated; and relieving pressure on tenants to have to master and integrate separate tools. The fourth pillar is customer visibility into their cloud environment via provision of log data and analytics. The fifth – secure hybrid clouds – enables tenants to use their own security controls in the OCI environment, although those tools must necessarily be cloud native.

High availability, complete with scalability and protection from external environmental attacks, is a core feature that all public cloud providers have to compete on. As of January 2021, OCI had 29 regions or Points of Presence (POPs) live as well as 6 Interconnect regions live with Microsoft Azure.

Lastly, the principle of verifiable security highlights the importance of the security of a cloud being independently audited and verified by credible, internationally recognized, certification schemes such as Centre for Internet Security (CIS) certification. At every stage of a product development lifecycle, any Oracle software must also comply with Oracle Software Security Assurance (OSSA). This is the company's methodology for building security into the design, build, testing and maintenance of all software products.

More Information

- Oracle Communications Cloud Native Security Guide
- Oracle Software Security Assurance

About Oracle Communications

Oracle Communications provides integrated communications and cloud solutions for Service Providers and Enterprises to accelerate their digital transformation journey in a communications-driven world from network evolution to digital business to customer experience. Please visit us at www.oracle.com/communications.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum.

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.