Protecting Your 5G Revenue Stream in the Cloud

Google Cloud

Communications service providers (CSPs), like any other business in every other industry, are increasingly transitioning their operations to the cloud to gain advantages in speed, cost and scale, and to expand their reach to customers and business partners alike.

CSPs who are deploying 5G network capabilities have even more reason to embrace cloud solutions — 3GPP 5G network standards are designed based on a cloud native architecture, ensuring the degree of efficiency, distribution, redundancy, availability, scalability and automation that will be needed to support the burgeoning volumes and the diversity of network services requiring guaranteed levels of service. As network functions and supporting operational systems move to the cloud, CSPs benefit from valuable complementary capabilities delivered by public cloud infrastructure providers, including security, orchestration and analytics.

As a CSP's operational boundaries increasingly blur between on-premise systems, in private clouds and in the public cloud, fundamental IT principles remain unchanged. Foremost among those is data security. In the face of intensifying data protection and privacy regulations that mandate personal data privacy and impose several penalties when data is breached, CSPs must evaluate, select and operate every facet of their networks and operating systems by placing the security of their customer data at the forefront of their

By 2024, most enterprises aspire to have $8 out of every $10 for IT hosting go toward the cloud, including private cloud, infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Achieving that aspiration will require significant effort from both enterprises and technology providers.[1]

---

[1] "Cloud-migration opportunity: Business value grows, but missteps abound," McKinsey & Company, October 2021.

MATRIXX® SOFTWARE

requirements. And in an increasingly competitive market, CSPs need to maintain their customers' trust more than ever by ensuring that the privacy of their data is equally as important as regulatory compliance.

MATRIXX and Google Cloud offer a joint solution for CSPs — a carrier-grade real-time 5G monetization platform deployed securely in the public cloud. MATRIXX, with Google Cloud's support, recently validated the operation of MATRIXX Digital Commerce Platform in a Google Cloud environment with confidential computing enabled, demonstrating production-ready, real-time performance of monetization algorithms with charging data encrypted in process. This project showed that data security for the Google Cloud Platform (GCP) public cloud can be delivered without any core changes to the MATRIXX monetization solution, providing hardware-based in-memory encryption while maintaining the throughput and scalability required for a Tier 1 real-time application. Finally, MATRIXX established that a CSP using Google Cloud Confidential Computing can deliver the audits and controls required by its regulator to demonstrate the security of private data within their monetization processes.

Data protection and privacy laws are numerous and varied around the world, often with separate disparate requirements at local and regional levels. In the United States, for example, there are various federal laws with specific data protection in different sectors (like health care and financial services) and state-level laws that seek to protect consumer data (and specify penalties when that privacy is violated) across the board for companies in all sectors. The same is true in the EU, with broad requirements such as the General Data Protection Regulation (GDPR) supplemented by country-specific privacy laws. As businesses adopt cloud operations, they face a growing need to comply with and demonstrate compliance to the most stringent regulations where their customers are, where their operations are and where their data resides or transits.

What MATRIXX Validated

No MATRIXX application changes required ✓	Encryption of private data in use ✓	Achieved regulatory compliance ✓

5G Real-Time Charging in the Cloud

5G represents perhaps the most significant change in telecommunications network architectures in decades. With this next wave of network investment, CSPs once again are challenged to generate returns on that investment. And this, at a time when CSP revenues continue to come under pressure from old and new competitors alike. Developed market CSP growth rates have slowed and converged on 1% CAGR, while aggregate investment in 5G will surpass US$130 billion by 2025.[2] The path to generating a return on that investment is not immediately clear. To achieve a meaningful ROI, CSPs are evolving their commercial models to focus on platform and network-as-a-service (NaaS) based propositions that will drive new revenue streams at higher margins than their traditional minutes and megabytes-driven business models. Existing IT infrastructure was not built, nor is not agile enough, to absorb and support this fundamental shift. So, while 5G is initially a network evolution, it drives transformation across all IT infrastructure and business support systems.

[2] Gartner Forecast: Communications Service Provider Operational Technology, Worldwide, 2019-2025, 2Q21 Update, published 24 June 2021 by Michael Porowski, Jouni Forsman. G00751152

With this wave of investment, CSPs have no choice but to do things differently than they have in the past. Fortunately, the 5G standards have been designed to help them do just that. The 5G converged charging system (CCS), for example, is newly defined to provide a unified service that sits between the network and the business to provide real-time monetization capabilities for complex services, including numerous simultaneous sessions by the same connected device. Other significant capabilities delivered by 5G networks will initiate a wave of innovative consumer and business services alike that require extreme bandwidth, ultra-low latency, a massive number of connections and, across all these capabilities, guarantee service levels.

With a 5G platform for delivering new connectivity-based services, coupled with a charging function that can assign value to those services in real-time, the stage is set for a wave of CSP innovation. However, CSPs must innovate to overcome the revenue and ROI pressures they have experienced in previous network generations.

MATRIXX Digital Commerce Platform (DCP) is more than a 3GPP-compliant 5G converged charging system. It is an agile platform for real-time monetization that supports the rapid rollout of limitless new services and offers. In a single, centralized DCP monetization platform, CSPs can expand offers to consumers, enterprises, wholesale customers and third parties in a B2B2X marketplace. They can apply the broadest set of monetization levers to measure and assign charges to the user, based on units of value beyond traditional minutes, messages, and megabytes, such as concurrent users, application load/utilization, usage within a time or geographical window and much more. And MATRIXX DCP supports charging for the unique network characteristics of 5G itself, such as for edge applications, mobile edge computing resources, network slices and charges for the orchestration functions as well, for example, the creation and decommissioning of slices and multi-access edge computing (MEC) resources.

With the increased complexity of 5G ecosystems, the growing number of services and the increased load, MATRIXX DCP delivers unsurpassed, carrier-grade throughput and latency with its real-time monetization platform.

MATRIXX DCP is designed for deployment in any CSP cloud environment, whether it is in a private cloud, hybrid cloud or public cloud. MATRIXX CSP customers are embracing the move of DCP to the cloud to address several requirements:

- To achieve agility and reduce costs, CSP's enterprise customers demand more agile and cost-effective solutions themselves in their pursuit of reducing their communications spend which has always been the largest line item in the IT budgets.
- To facilitate an integrated ecosystem of partners in the cloud and deliver on their B2B2X strategies.
- To incorporate edge deployments, as enabled by 5G network architectural advancements, taking advantage of the investments already made by the public cloud providers.

Furthermore, in the face of data security requirements, DCP must be deployed on infrastructure that facilitates the security and encryption of customer data in the revenue stream while at rest, in transit and in process, in whichever on-premise or cloud environment is chosen.

That's where Google Confidential Computing comes in.

The Criticality of Cloud Security

As a global provider of consumer and business services, Google Cloud builds, maintains and continually enhances and expands its cloud infrastructure. It makes this infrastructure available to other businesses who can take advantage of its scale, performance and reliability. As cloud technology evolves and security regulations expand, maintaining compliance becomes more complicated. Google Cloud makes it easy for CSPs to understand the guidelines and requirements by region and to generate compliance reports for the applicable regulatory bodies. Key compliance subjects include:

• Data sovereignty
• Data audit logs
• Data accessibility

Google Cloud Confidential Computing enables a focus on secure data accessibility. With confidential computing, a CSP's customer data is hosted on Google managed infrastructure and the data itself is encrypted to protect it from being accessed by anyone outside authorized CSP users and processes.

Gartner analysis indicates that confidential computing today is in the early innovation state, and will reach full maturity in 5-10 years. However, Google's global clients, driven by intensifying regulatory environments, are rapidly moving through confidential computing proof of concepts into full production, giving all indications that the adoption cycle to maturity will be shorter.

> **"Confidential computing may mitigate one of the major barriers to cloud adoption for highly regulated businesses or any organization concerned about unauthorized third-party access to data in use in the public cloud."** [3]
> **— Gartner, July 2021**

Google Cloud is a co-founder and member of the Confidential Computing Consortium[4] and partners with silicon vendors to expand the marketplace of highly secure confidential computing solutions for on-premise and cloud applications.

By expanding Google Cloud Confidential Computing to support Google Kubernetes Engine and Google Datapoc for secure analytics, Google Cloud further enhances the usability of this platform, supporting the deployment of the same application and containers without modification to meet new compliance requirements with minimal performance impact.

Google Confidential Computing Delivers Global Privacy Requirements

Security has been a core attribute of the Google Cloud since inception, with innovations from the zero-trust network[5] to encrypted-by-default behavior for all apps and services that Google Cloud offers. As cloud adoption grows, enterprises increasingly rely on their provider to deliver not only core security but also to enrich that security with their own policies and preferences. This is a key differentiator in GCP; with the Security Command Center[6] and the ability to onboard third-party security solutions into an environment, a CSP can extend, customize and optimize its security fit-for-purpose.

---

[3] Gartner G00747396 Hype Cycle for Computer Infrastructure, by Tony Harvey, July 2021.
[4] https://confidentialcomputing.io/members/
[5] https://cloud.google.com/beyondcorp
[6] https://cloud.google.com/security-command-center

Google Cloud Confidential Computing extends security boundaries to users who have access to the physical servers as well as to other processes running on shared hardware. Along with hardware-based encryption, Google Cloud Confidential Computing provides audit reports to validate the integrity of the AMD secure processor firmware and to enable Google Cloud organizational policies that ensure usage of the confidential environments to address compliance concerns and enforce processes to run only on confidential virtual machines (VMs).

Google is committed to providing cloud infrastructure that delivers reliability, performance, scalability and security. As the cloud market evolves, confidential computing will reach mainstream adoption in the next few years. By introducing confidential computing technology from the outset, and providing the tools for transparency, Google Cloud Confidential Computing enables businesses to expand in the cloud with confidence and the flexibility of deploying secure environments on anything from full VMs to Kubernetes workloads.

When CSPs deploy VMs, containers and apps on GCP, they are incorporating Google Cloud infrastructure within their trust boundary. Keeping their cloud workloads protected end to end typically is the most complicated step to implement, and Google Cloud Confidential Computing simplifies the encryption of sensitive data during processing.

Data at Rest, in Transit and in Use

Data at Rest
Google Cloud transparently encrypts data at rest by default.[7] A CSP can augment the default GCP encryption with customer-managed keys, generated and controlled by GCP or customer-supplied keys created outside of Google Cloud and then incorporated inside the Cloud environment.

Data in Transit
Google Cloud transparently encrypts traffic in transit within the CSP's virtual private cloud (VPC).[8] Customers can extend Google Cloud's default encryption by implementing their own encryption, either integrated into the platform, like SSL offloading on load balancers, or isolated from the platform, such as customer-provided SSL certificates, external certificate authority, etc.

Data in Use
Google Cloud Confidential Computing brings the third pillar of security to a CSP's operations, encrypting data in use, during storage in memory and during processing.[9] Confidential computing achieves this by utilizing third-party CPU chips from providers like AMD's Epyc[10] chips. A randomly generated key is stored within the chipset and configured to uniquely encrypt per VM in isolation from every other VM on the machine and from the hypervisor. This encryption key cannot be exported or accessed by Google Cloud. Data encryption and decryption are handled transparently to the guest OS; therefore, no application changes are needed to take advantage of the increased security and isolation of data in use. This is a key feature of confidential computing and a significant advantage to software vendors like MATRIXX and joint CSP customers.

---

[7] https://cloud.google.com/security/encryption/default-encryption#:~:text=Google%20using%20the%20Advanced%20 Encryption,to%202015%20that%20 use%20AES128
[8] https://cloud.google.com/security/encryption-in-transit
[9] https://cloud.google.com/compute/confidential-vm/pricing
[10] https://www.amd.com/en/products/epyc

How Google Cloud Confidential Computing Works

When deploying in the Google Cloud, CSPs can rely on Google Cloud Confidential VMs to encrypt their most sensitive data while it's being processed. When MATRIXX DCP is deployed in Google Cloud with confidential computing, its subscriber data, account balances, network events and charges/revenue streams are encrypted in use *without making any code changes to the application or compromising on performance*. With DCP and Google Cloud Confidential Computing, a CSP can immediately support business scenarios that previously had been next to possible, including collaborating with a growing number of partners to develop, launch and deliver innovative offers while preserving the confidentiality of their customers' private data.

Google Cloud Confidential Computing encrypts data in use/in process via Secure Encrypted Virtualization (SEV). This encryption incorporates a dedicated on-die memory controller that uses AES to encrypt data when it is written to DRAM and decrypts it when it is needed. Each VM has its own unique key which lasts for the duration of the VM.

Data in Use Encrypted via SEV[11]
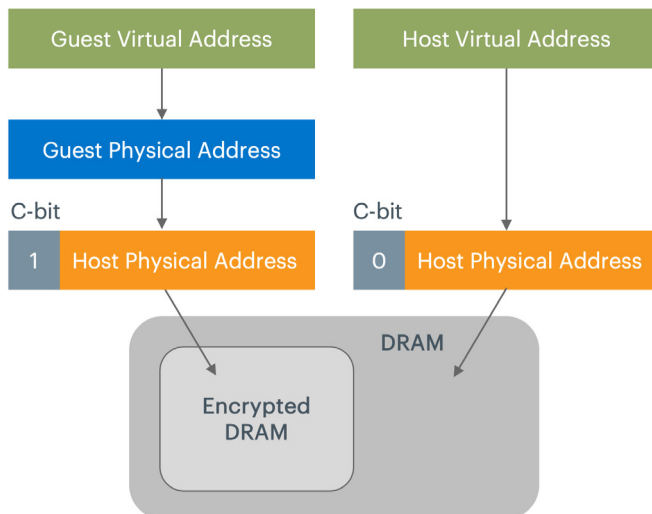
With SEV, the hypervisor and guest are fully isolated from each other. This is due to the nature of access to the encrypted DRAM, which is only decryptable via the virtual machine and on the hypervisor. Since the encryption applies to memory, the machine operates as a regular virtual instance. CPU and network utilization metrics are monitored as normal, but monitoring memory utilization requires an agent installed inside the instance (as is the case with most Google Cloud Compute Engine instances).

As the encryption and decryption are transparent to the guest OS, most workloads can be run inside the VM, benefit from the security isolation and do not require application or code changes. By deploying SEV in this manner, this enables nested hypervisors like Docker or containerd to run inside the VM protected by SEV as normal. This is how GKE Confidential Computing nodes provide transparent encryption for data in use/in process to supplement encryption for data at rest and for in transit with Anthos Service Mesh, Cilium (which can enable transparent encryption with IPsec) or Istio.

[11] https://developer.amd.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf

Additionally, as part of the VM tear-down process, the memory is cleared of the previous instance cache. If a new VM spins up and subsequently tries to access the same memory page, it will just receive garbled data that has been decrypted with the wrong key.

By incorporating SEV encryption, along with services like binary authorization, the assured workload[12] makes it easy for a CSP to become and remain confidentiality compliant in the cloud.

MATRIXX DCP Validation with Google Cloud Confidential Computing

In the first half of 2021, the operation of MATRIXX DCP was validated in a cloud environment with confidential computing enabled, demonstrating production-ready, real-time performance of monetization algorithms with charging data encrypted in process. This certification was conducted at the request of a Tier 1 mobile operator in Europe and validated the goals of Google Cloud Confidential Computing:

- Confidential computing can be enabled for MATRIXX DCP operations *without any changes* to the core application
- Regulator *private data compliance* of MATRIXX DCP running in a GCP environment can deliver the required audits and controls MATRIXX DCP *performs in a secure cloud environment* with the throughput and latency required for the real-time operations of a Tier 1 operator

The MATRIXX engineering, product management and strategic alliances teams were supported by both the GCP Strategic Partnership team and the GCP ISV Center of Excellence. GCP provided the program management and infrastructure required for the duration of the certification process, and dedicated support to answer questions and troubleshoot during the setup and execution of the tests. The project delivered on all the goals, allowing the CSP to advance its requirements to demonstrate and certify its public cloud operations to the local regulator.

MATRIXX DCP Configuration

MATRIXX uses a real-world production environment for all infrastructure validations to simulate the requirements of a CSP's advanced consumer and enterprise operations. For the Google Cloud Confidential Computing validation, a DCP environment was used with one million subscribers, each with five active offers and price plans. Each account or wallet had 15 independent balances to maintain and update during the charging process, with balances spanning multiple charging and billing periods.

The simulated load on MATRIXX DCP simulated a combination of 4G and 5G network traffic, and 20% of the overall processing load simulated API calls that represented interactions between the CRM/BSS and DCP.
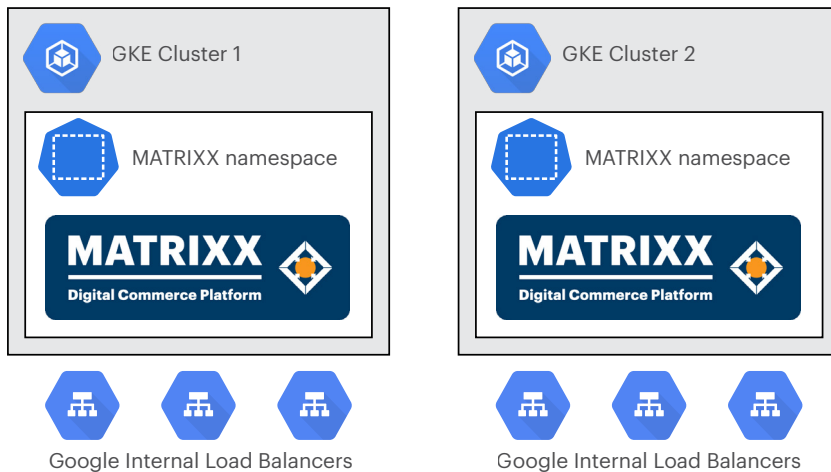
---

[12] https://cloud.google.com/assured-workloads

MATRIXX Pricing Configuration Used in the Validation
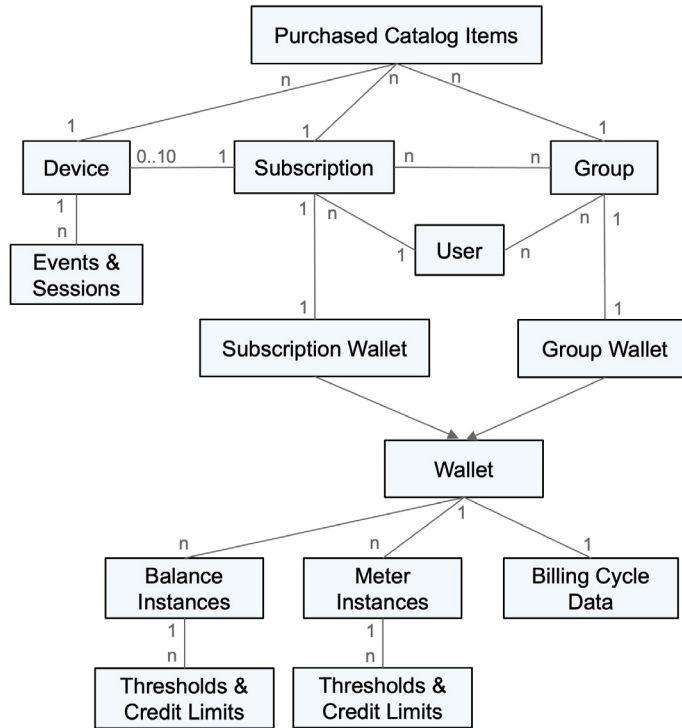
GCP GKE Infrastructure Configuration

The GCP validation environment consisted of two GKE clusters.

Google Internal Load Balancers

Google Internal Load Balancers

The GCP environment was:

- GKE running on the Google Public Cloud
- K8s 1.19-9-gke. 1900
- Container runtime: docker 19.3.15
- CNI: GKE native CNI
- Node OS: container-optimized OS from Google, kernel version 5.4.109+
- GKE cluster 1: 8 worker nodes
- GKE cluster 2: 6 worker nodes
- Node type: n2d-custom-96-266240, 96 vCPU, 255 GB RAM
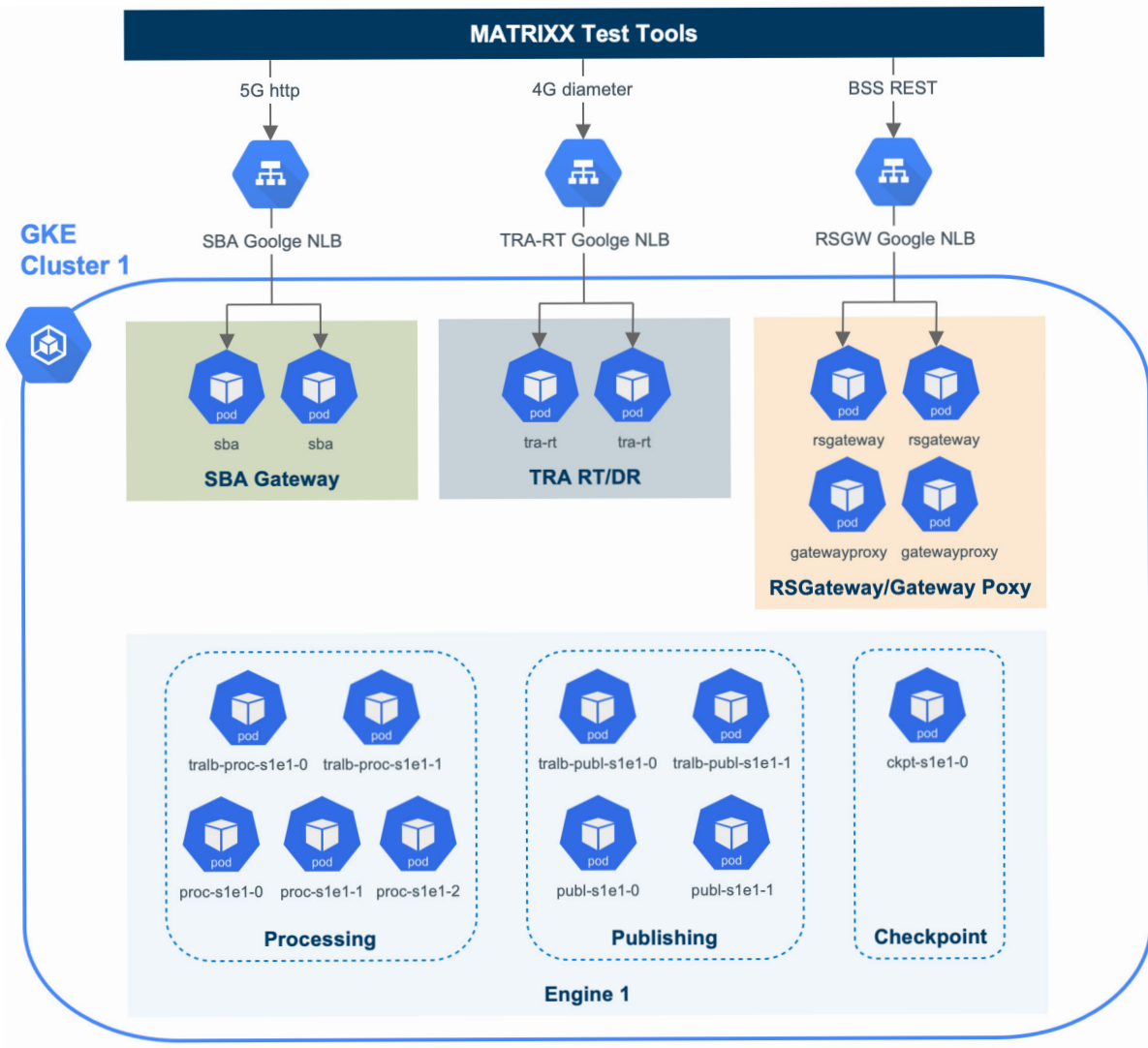
MATRIXX + Google Cloud Deliver Secure Tier 1 Monetization

MATRIXX DCP deployed in the Google Cloud Platform with confidential computing is an unmatched solution for 5G monetization in a highly secure environment that protects consumer and enterprise data at the highest levels. MATRIXX DCP leads the market in deploying converged charging and monetization capabilities on the Google Cloud Platform with confidential computing features enabled, ensuring that customer data and revenue streams are encrypted while being processed.
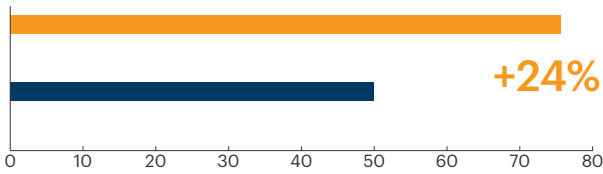
What MATRIXX Validated

No MATRIXX application changes required ✓	Encryption of private data in use ✓	Achieved regulatory compliance ✓

Outperformers Reveal the Winning Recipe for Cloud Adoption[13]

Characteristics of outperformers, % of respondents (n = 443)

█ Outperformers ■ Others

+24%

0 10 20 30 40 50 60 70 80

Develop comprehensive/security compliance

Outperformers in the path to cloud migration involved their CxOs in establishing comprehensive security and compliance plans 24% more than others.

This paper was authored by MATRIXX Software.

MATRIXX Software is the global leader in 5G monetization for the communications industry. Serving many of the world's largest operator groups, regional carriers, and emerging digital service providers, MATRIXX delivers a cloud native digital commerce solution that enables unmatched commercial and operational agility. Unifying IT and networks, MATRIXX delivers a network-grade converged charging system (CCS) enabling efficient hyper-scaling of infrastructure to support consumer services, wholesale and enterprise marketplaces. Through its relentless commitment to product excellence and customer success, MATRIXX empowers businesses to harness network assets and business agility to succeed at web scale.

Google Cloud accelerates organizations' ability to digitally transform their business with the best infrastructure, platform, industry solutions and expertise. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology — all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems.

---

[13] "Cloud-migration opportunity: Business value grows, but missteps abound," McKinsey & Company, October 2021.