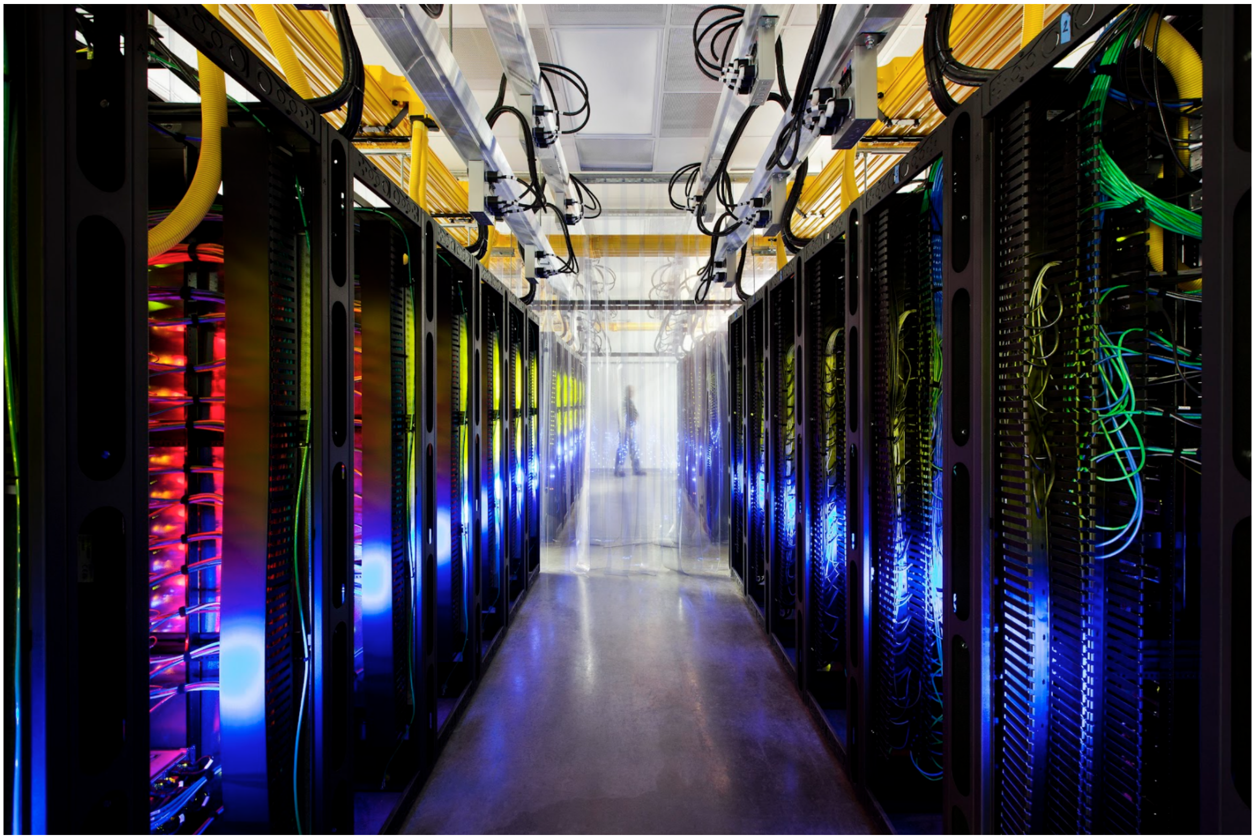
Insights into the U.S. Telecommunications Industry



Introduction **3**
Telecommunications Industry Trends 3
Regulations and Standards Impacting the Telecom Industry **3**
Federal Communications Commission (FCC) 4
Mutually Agreed Norms for Routing Security (MANRS) 4
3rd Generation Partnership Project (3GPP) 4
Federal Risk and Authorization Management Program (FedRAMP) 5
Health Insurance Portability and Accountability Act (HIPAA) 5
Privacy laws 6
Regulatory Themes When Adopting Cloud **6**
Foundational security requirements 6
Enhanced customer control over their data 7
Customer data protection 8
Additional challenges faced by telecom organizations **8**
Legacy systems 8
Management of IoT devices 8
Operational resilience 10
Supply chain risks 10
How telecom companies are addressing these challenges and their regulatory needs **11**
Cloud-native management capabilities for IoT 11
Managing large scale data and analytics for revenue or billing 11
Multi-cloud container strategy 12
Telecommunications network management 13
Conclusion **13**

Disclaimer

This whitepaper applies to Google Cloud products described in the Google Cloud Services Summary. The content contained herein is correct as of June 2022 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

Organizations, especially in the Telecommunications and Technology sector, are looking to accelerate their digital transformation journey towards long-term growth powered by cloud technologies. The demand is for streamlined development, faster innovation, efficient scale, and effective cloud-enabled, data-driven decision making to support prolonged success for both the organization and its customers. As with any transformational technology, the challenge lies in ensuring data is safe, technology risks are managed, and compliance and regulatory requirements are addressed. With this vast amount of change, industry trends emerge, and new regulations are developed. Let's look at what the telecom industry is experiencing and how Google Cloud is helping.

Telecommunications Industry Trends

- With a proven track record of providing cost savings, scalability, transparency, and security, among several other benefits, businesses are moving to the cloud at a faster rate now more than ever. Decision makers are placing cloud infrastructure at the forefront by adopting a **cloud-first approach**, ensuring any new development is natively in a cloud environment.
- Over 50% of surveyed executives expect to increase migration of assets to the cloud[1]. This approach requires refactoring existing applications to be cloud-compatible. In some instances, this would necessitate incorporating cloud-native infrastructure with legacy systems.
- Due to the present-day ubiquitous nature of IoT devices and the rise of newer technologies such as 5G, **edge computing** is becoming increasingly pervasive in delivering low latency and high-speed data transfer solutions to telecommunication clients.
- Telecommunications organizations provide solutions for various highly-regulated industries, including healthcare, retail, and financial services, and by extension, are now looking to be **compliant with a wide variety of industry standards** that apply to these industries, such as Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA), which are discussed in detail below.

Regulations and Standards Impacting the Telecom Industry

For many in telecom, the regulatory landscape is expanding. As the industry broadens and new business lines are added, there is a shifting risk landscape for trust leaders in privacy,

[1] LaBerge, Laura, Clayton O'Toole, Jeremy Schneider, and Kate Smaje. "How COVID-19 has pushed companies over the technology tipping point—and transformed business forever." McKinsey & Company, October 5, 2020. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever.

compliance, risk, and security. Narrowing the focus, let's review some of the top requirements impacting telecom today.

Federal Communications Commission (FCC)

The FCC ensures the reliability and resiliency of telecommunications networks throughout the United States. It regularly publishes advisories, rulings, decisions, and compliance guides to help telecommunications providers and consumers understand the latest changes to the regulatory landscape.

One such compliance guide describes the **Customer Proprietary Network Information (CPNI)** and details the steps required to comply with section 222 of the Communications Act, 47 U.S.C. § 222. What does section 222 state? All telecommunications carriers must complete the annual certification process demonstrating compliance. In particular, it requires carriers to:

- Safeguard CPNI
- Enforce controls for authorized access of CPNI
- Provide guidelines for the use of CPNI for marketing while respecting customer opt-in/opt-out approval
- Require training for employees with regards to the safe handling of CPNI
- Impose notification requirements for the solicitation of customer approval
- Mandate certain recordkeeping requirements

Mutually Agreed Norms for Routing Security (MANRS)

Developed by the non-profit organization Internet Society (ISOC), MANRS has four programs for each type of stakeholder in the **global internet routing system** - Network Operators, Internet Exchange Points, Content Delivery Network Providers and Cloud Providers, and Equipment Vendors. These stakeholders are responsible for ensuring their offerings are robust and secure through a set of mandatory and recommended actions. These actions range from technical requirements, such as protection against route hijacking and spoofing to the promotion of MANRS through training and technical content.

How we help: As a MANRS member, we helped create a specific program focused on cloud and CDN providers working with a number of major service providers. In support of the major focus areas in the MANRS task force, we've already undertaken several measures to protect our network infrastructure from hijacks, such as filtering and coordinating with peer networks, which will make it easier to extend these protections to other networks in the internet.

3rd Generation Partnership Project (3GPP)

3GPP is an organization comprised of members from China (China Communications Standards Association), Europe (European Telecommunications Standards Institute), India (Telecommunications Standards Development Society), Japan (Association of Radio Industries and Businesses, Telecommunication Technology Committee), South Korea (Telecommunications Technology Association), and the U.S. (Alliance for Telecommunications Industry Solutions), with the goal of developing specifications and standards for three technical specification groups - Radio Access Networks, Services & Systems Aspects, and Core Network & Terminals. For example, the organization is responsible for the **3GPP TS 33.501 version**

15.3.1 security architecture and procedures for 5G systems.

How we help: We design our cloud services to deliver better security than many on-premises approaches. We make security a priority in our operations—operations that serve billions of users across the world. For more information on our physical, administrative, and technical controls that we have deployed to help protect your data, please see our security whitepaper.

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a U.S. government program that enables the adoption of cloud products and services while emphasizing the need to maintain stringent security controls over federal information.To provide products and services to government agencies, a telecom provider needs to be **FedRAMP authorized** in accordance with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130, and FedRAMP policy based on NIST standards and guidelines. Providers must go through three phases to achieve authorization, which at a high level include:

1. **Preparation:** An optional (but highly recommended) readiness assessment and pre-authorization.

2. **Authorization:** A full security assessment performed by an accredited Third Party Assessment Organization, and the agency authorization process where a cloud service provider works directly with the Agency sponsor who reviews the cloud service's security package. After completing a security assessment, the head of an Agency (or their designee) can grant an Authority to Operate (ATO). For more information on the authorization process, you can visit the FedRAMP Get Authorized page.

3. **Continuous monitoring:** Depending on the impact the loss of confidentiality, integrity, and availability of data will have, providers are classified at low, medium or high impact levels, which in turn informs the security controls they will need to satisfy.

How we help: For telecom leaders interested in validating Google's FedRAMP status, it is available on the government's website, FedRAMP Marketplace, and on our FedRAMP compliance page.

Health Insurance Portability and Accountability Act (HIPAA)

As industry leaders explore new digital health opportunities that bring additional connectivity and innovation to an adjacent industry, healthcare, the regulatory space requires investigating HIPAA compliance. For organizations that are confirmed covered entities, HIPAA has provisions that address security and privacy - the Security Standards for the Protection of Electronic Protected Health Information (the Security Rule), the Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), and the Breach Notification Rule.

The Security Rule specifies the technical and non-technical safeguards required to protect electronic personal health information (e-PHI) in accordance with the Privacy Rule. The Security Rule dictates that organizations must enforce the confidentiality, integrity, and availability of all e-PHI within their scope, identify threats to e-PHI and protect against them, safeguard against improper disclosure, and ensure the proper handling of e-PHI by the organization's workforce.

The Privacy Rule requires organizations handling, storing, and transmitting sensitive data to enforce safeguards for protecting the privacy of e-PHI. It outlines how organizations may use protected information and the types of disclosures they may make without authorization from the individual. Lastly, the Privacy Rule articulates an individual's rights over their e-PHI, including the right to request a copy of their e-PHI, the right to request transmission of electronic health records to a third party, and the right to request any necessary corrections.

How we help: It is important to note that there is no certification recognized by the U.S. Department of Health and Human Services (HHS) for HIPAA compliance and that complying with HIPAA is a shared responsibility between the customer and Google. Google Cloud supports HIPAA compliance (within the scope of a Business Associate Agreement), but ultimately,customers are responsible for evaluating their own HIPAA compliance. Additional information is available from our HIPAA compliance page.

Privacy laws

While there have been efforts in the past to protect individuals' data in the U.S., such protections were sector-specific and covered particular types of information. For instance, the HIPAA Privacy Rule applies to health information and the Gramm-Leach-Bliley Act is targeted to protecting financial information. It wasn't until the passage of the **California Consumer Privacy Act** (CCPA) in 2018 that lawmakers enforced broader consumer privacy protections.Since CCPA was passed, additional states have been evaluating or passing similar legislation. Furthermore, additional privacy regulations may apply to certain individuals in the U.S., even if other countries instituted them. For additional privacy support, please visit our Privacy Resource Center.

Regulatory Themes When Adopting Cloud

There are several common themes we see across the regulations and industry standards above.

Foundational security requirements

A consistent requirement across all the regulations is to enable safeguards for accessing and properly storing customer data. Enforcing these requirements is typically done through establishing security controls for systems processing, transmitting and storing sensitive information, authentication and authorization mechanisms, encryption standards, network, and perimeter security controls.

How we help: In addition to the security whitepaper mentioned above, Google has produced a number of other whitepapers detailing our security practices, including encryption at rest, encryption in transit, and infrastructure security. Beyond our security measures, we also publish guidance on security best practices, use cases, and blueprints.

Google Cloud's industry-leading security, third-party audits, and certifications help support your compliance. Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Some of the key international standards we are audited against are:

- ISO 27001 (Information Security Management)
- ISO 27017 (Cloud Security)
- ISO 27018 (Cloud Privacy)
- ISO/IEC 27701 (Privacy - Data Processor)
- SOC 2 and SOC 3 reports
- NIST 800-53
- PCI DSS
- CSA Star
- GxP

We also provide resource documents and mappings to frameworks and laws where formal certifications or attestations may not be required or applied. Please visit our compliance resource center for a complete listing of our compliance offerings.

Enhanced customer control over their data

Now more than ever, the appropriate usage of customer data is under heavy scrutiny, with corporations facing fines for failure to do so. To that end, regulations and standards have evolved to grant customers more power regarding how they want their data to be handled once it is within an organization's environment. A recent example of such control enhancements is the rise of opt-in/opt-out features provided to end users, with 47% of organizations viewing consent as a mechanism to build trust with consumers.[2]

How we help: The data you put into Google Cloud services is yours. We do not scan it for advertisements, and we do not sell it to third parties. The Cloud Data Processing Addendum for Google Cloud describes our commitment to protecting your data. That document states that we will not process data for any purpose other than to meet our contractual obligations. If you choose to stop using our services, we provide tools that make it easy for you to take your data with you, without penalty or additional cost. For more information about our commitments for Google Cloud, see our trust principles.

Customer data protection

Combining the elements of security and privacy programs with the ultimate goal of protecting customer data has become apriority for many organizations. Over 50% of PwC's Digital Trust[3] Survey respondents indicated that they have processes in place for the governance, protection, and discovery of customer data, in alignment with privacy regulations such as the California

[2] "2021 Global Privacy Benchmarks Report." TrustArc May 26,2021. https://info.trustarc.com/Web-Resource-2021-05-26-Global-Benchmarking-Report_LP.html

[3] PricewaterhouseCoopers. "Building Digital Trust: Trust in Data." PwC. Accessed June 17, 2022. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/digital-trust-leadership-operations-partnership/trust-in-data.html.

Privacy Rights Act (CPRA).

How we help: Cloud Data Loss Prevention (DLP) helps customers to discover, classify, and de-identify data such as payment card numbers, national identification numbers, protected health information, and other types of personally identifiable information (PII). DLP provides techniques such as pseudonymization, tokenization, bucketing, date-shifting, and more, which can help you de-risk structured and unstructured data.

Additional challenges faced by telecom organizations

Aside from regulations and standards, telecoms are facing other challenges as they strive to keep up with the latest trends in their industry.

Legacy systems

One of the biggest roadblocks for telecommunication companies as they move to modernize their infrastructure is their reliance on legacy systems. A common example is the billing and revenue recognition systems, which historically are built on monolithic architecture with very little room for customization to adapt to the ever-changing needs of customers and the industry.

How we help: Google Cloud has a variety of solutions to assist with infrastructure modernization. With solutions like SAP on Google Cloud, you can maintain business continuity on a secure cloud with advanced reliability, network, and uptime performance. Similarly, Google Cloud VMware Engine allows you to easily lift and shift VMware-based applications to Google Cloud without changes to your apps, tools, or processes.

Management of IoT devices

Due to the nature of IoT devices, and because they often reside on the periphery of an organization's network, they are prime targets for malicious activity. Connecting to the internet exacerbates this fact and increases the size of the attack surface of these devices.

How we help: In our infrastructure security design whitepaper, we discuss the lengths we go to secure our infrastructure, including implementing the zero trust security model. This includes securing communication between the internet and the services that run on Google infrastructure.

The infrastructure consists of many physical machines interconnected over the LAN and WAN. The security of inter-service communication is not dependent on the security of the network. However, we isolate our infrastructure from the internet into a private IP address space. We only expose a subset of the machines directly to external internet traffic so that we can implement additional protections such as defenses against denial of service (DoS) attacks.

Google Front End service

When a service must make itself available on the internet, it can register itself with an infrastructure service called the Google Front End (GFE). The GFE ensures that all TLS connections are terminated with correct certificates and by following best practices such as supporting perfect forward secrecy. The GFE also applies protections against DoS attacks. The GFE then forwards requests for the service by using the RPC security protocol discussed in Access management of end-user data in Google Workspace.

In effect, any internal service that must publish itself externally uses the GFE as a smart reverse-proxy frontend. The GFE provides public IP address hosting of its public DNS name, DoS protection, and TLS termination. GFEs run on the infrastructure like any other service and can scale to match incoming request volumes.

Customer VMs on Google Cloud do not register with GFE. Instead, they register with the Cloud Front End, a special GFE configuration that uses the Compute Engine networking stack. Cloud Front End lets customer VMs access a Google service directly using their public or private IP address. (Private IP addresses are only available when Private Google Access is enabled.)

DoS protection

The scale of our infrastructure enables it to absorb many DoS attacks. To further reduce the risk of DoS impact on services, we have multi-tier, multi-layer DoS protections.

When our fiber-optic backbone delivers an external connection to one of our data centers, the connection passes through several layers of hardware and software load balancers. These load balancers report information about incoming traffic to a central DoS service running on the infrastructure. When the central DoS service detects a DoS attack, the service can configure the load balancers to drop or throttle traffic associated with the attack.

The GFE instances also report information about the requests they are receiving to the central DoS service, including application-layer information that the load balancers don't have access to. The central DoS service can then configure the GFE instances to drop or throttle attack traffic.

User authentication

After DoS protection, the next layer of defense for secure communication comes from the central identity service. End users interact with this service through the Google login page. The service asks for a username and password, and it can also challenge users for additional information based on risk factors. Example risk factors include whether the users have logged in from the same device or from a similar location in the past. After authenticating the user, the identity service issues credentials such as cookies and OAuth tokens that can be used for subsequent calls.

When users sign in, they can use second factors such as OTPs or phishing-resistant security keys such as the Titan Security Key. The Titan Security Key is a physical token that supports the FIDO Universal 2nd Factor (U2F). We helped develop the U2F open standard with the FIDO Alliance. Most web platforms and browsers have adopted this open authentication standard.

Operational resilience

Organizations and regulators are increasingly focused on operational resilience, reflecting an organization’s growing dependancy on complex systems, automation and technology, and third parties. Without a fault-tolerant architecture at the foundation of an organization’s technology stack, a single failure in the environment can have cascading effects on the availability of products and services.

How we help: Google Cloud has a robust, flexible, and cost-effective selection of products and features that customers can use to build or augment the right solution. These include a global network, redundancy, scalability, security and compliance. Customers can use Google Cloud services such as Shared VPC, Google Cloud firewalls, Cloud Deployment Manager, Anthos and Cloud Storage to design and build robust DR patterns that can meet their specific recovery time objectives (RTOs) and recovery point objectives (RPOs).

Additionally, Disaster Recovery Plans (DRP) have always been a priority for enterprises seeking to provide a consistent customer experience regardless of potential risks such as natural disasters, hardware failure, human errors, and cyber crimes.

Google Cloud offers many data archive and backup features across its database and storage solutions, such as Bigtable's regional replication, BigQuery's long term storage, Datastore's managed export service, Cloud SQL's automated backup and recovery, Spanner's export, and Cloud Storage's nearline & coldline.

Supply chain risks

Given the scale and scope of telecommunication companies, they often struggle with the issue of "nested vendors," which arises when they outsource parts of their service delivery or product development to third-party providers. The third-party organizations further outsource certain elements of their work to another third-party organization, which introduces additional risk and becomes increasingly difficult to identify the sources of risks at any given time.

How we help: Google provides its customers with information on subprocessors and outlines Google and customer responsibilities in the Cloud Data Processing Addendum. Additionally, Google requires its subprocessors to sign the Subprocessor Data Processing Agreement which include their responsibilities to the data. For Google Cloud, Google maintains public subprocessor lists for review. The lists are updated when subprocessors are added, modified, or removed, and the lists provide guidance on the functions performed. Customers interested in the list of subprocessors can access the respective list for Google Cloud services and Google Workspace.

How telecom companies are addressing these challenges and their regulatory needs

To combat the risks that come with the changes in this ever evolving industry, telecommunications companies are leveraging cloud environments to deliver the security features required to create secure products and services.

Cloud-native management capabilities for IoT

Multi-access Edge Computing (MEC), an architectural concept developed by European Telecommunications Standards Institute (ETSI), allows for decentralization and pushing out of cloud-computing capabilities and an IT service environment to the edge of the network. Companies achieve this through low latency levels and data processing in the cloud as opposed to the IoT devices making it easier to enforce security requirements in a platform hosted in the cloud environment.

How we help: Part of the Google Distributed Cloud portfolio, Google Distributed Cloud Edge is ideal for running local data processing, low-latency edge compute workloads, modernizing on-premises environments, and deploying private 5G/LTE solutions across a variety of industries.

Google Distributed Cloud Edge is a fully managed product that brings Google Cloud's infrastructure and services closer to where data is being generated and consumed. Google Distributed Cloud Edge empowers communication service providers to run 5G Core, and radio access network (RAN) functions at the edge. It also enables an ecosystem of partners and developers to create enterprise applications to meet mission-critical use cases such as computer vision and Google AI edge inferencing. Google Distributed Cloud Edge builds on our telecommunication solutions and empowers communication service providers to deliver new experiences that leverage 5G and edge.

In addition to network modernization, we are focused on building an edge ecosystem to help communication service providers move beyond connectivity services and monetize the edge. Together, 5G and edge provide a powerful combination to help enterprises continue to digitize their business while leveraging third-party services from our trusted partner ecosystem in their dedicated environment.

Managing large scale data and analytics for revenue or billing

Companies are now leveraging cloud as the core component to their most complex solutions, such as billing and revenue recognition systems. Cloud helps introduce innovations at scale, such as hyper-transactionality, Artificial Intelligence (AI), and Machine Learning (ML) / Reinforcement Learning (RL) at a faster pace, that's more readily possible than in an on-prem environment. Companies also use AI and ML/RL capabilities for data analytics performed on centralized collections of customer data (Data Lakes), to derive meaningful insights into their usage patterns and, in turn, offer targeted products and features to the customers.

How we help: With solutions like BigQuery, customers can democratize insights with a secure and scalable platform with built-in machine learning. BigQuery ML enables data scientists and data analysts to build and operationalize ML models on planet-scale structured or semi-structured data, directly inside BigQuery, using simple SQL—in a fraction of the time. Export BigQuery ML models for online prediction into Vertex AI or your own serving layer. Learn more about the models we currently support.

Customers operating in a multicloud environment may be interested in BigQuery Omni, a flexible, fully managed, multicloud analytics solution that allows you to cost-effectively and securely analyze data across clouds such as AWS and Azure.

Multi-cloud container strategy

Many telecoms have been migrating from legacy code-bases to a microservices-based architecture to realize the benefits of a scalable, flexible, and reliable build. Cloud service providers offer environments conducive to this type of product development. A multi-cloud container strategy inserts resilience into the development process and introduces elements of portability that containerization offers.

How we help: Google is committed to an open cloud that enables our customers to set up the optimal solution, spanning on-premise and multiple clouds, without being locked into a single provider. We offer tools that operate across systems and vendors and allow you to monitor your system from a single place.

Our belief in an open cloud stems from our deep commitment to open source. We believe that open source is the future of public cloud: It's the foundation of IT infrastructure worldwide and has been a part of Google's foundation since day one. Google is the #1 contributor to the Cloud Native Computing Foundation, an open source development community, with 50%+ of code commits. This is reflected in our contributions to projects like Kubernetes, TensorFlow, Go, and many more. We believe customers should use us because they love us, not because they are locked in.

What the solution looks like

With Anthos for Telecom, we‘ve brought our Anthos cloud application platform to the network edge, allowing telecommunications companies to run their applications wherever it makes the most sense. Much like Android provided an open platform for mobile-centric applications, Anthos for Telecom—based on open-source Kubernetes—will provide a similar open platform for network-centric applications.

Anthos provides a single platform for multi-cloud management, allowing you to deploy applications across hybrid and multi-cloud without changing the underlying code. Anthos' full suite of features, including Migration and Configuration Management, enables you to migrate and modernize your VMs to your container and cloud provider of choice in one streamlined motion, without upfront modifications to the original VMs or applications. This means that you don't have to jump through hoops or learn a new language - you can run all your container workloads on one consistent platform. Anthos is a 100% software solution that works on your existing hardware.

Telecommunications network management

5G has shown to be the most open and flexible of all generations of networks thus far. 5Ghas enabled the separation of various hardware and software components that comprise the network, further pushing the core elements into the cloud for easier programming and management. To secure these elements in the cloud, the Cybersecurity & Infrastructure Security Agency (CISA) and the National Security Agency (NSA) have collaborated to create the "Security Guidance for 5G Cloud Infrastructures". This guidance addresses prevention and detection of malicious activity in the 5G cloud, the secure isolation of network resources, the integrity of cloud infrastructure, and secure network and customer data guidelines.

How we help: At Google Cloud, we've written extensively on our security posture, including how we work to secure our infrastructure by building security through progressive layers to deliver true defense in depth. Customers can leverage offerings such as Security Command Center to assist in asset discovery and inventory, threat prevention, and threat detection.

For an enterprise already employing or planning to adopt third-party security solutions, Google Cloud curates a diverse and expanding Security Partner Ecosystem, composed of some of the most respected vendors in cloud security. Customers can take advantage of the security solutions offered by our partners to improve their security posture in areas such as data leakage prevention and endpoint protection.

In addition, many Google Cloud services facilitate the adoption of third-party products by allowing for:

- export of Cloud Audit Logs
- export of Security Command Center alerts and findings
- use of extensible markup language for automated application and enforcement of security policies

A full list of third-party security offerings for the Google Cloud environment is available in the Cloud Marketplace.

Conclusion

With the exponential proliferation of technology to deliver products, services, and payments, comes the need for an underlying infrastructure that can manage billions of transactions across the network with little to no downtime. Telecommunications companies are continuously working on solutions that can provide a platform that offers a seamless experience for consumers, while also working within the boundaries of the ever-changing legislative and industry landscape. Consequently, these companies are looking to partner with organizations whose products are scalable and secure, reliable, fault-tolerant, capable of low-latency delivery, and while meeting their customer and regulatory requirements.

Google has a track record of delivering on every front mentioned above, which is why several major U.S. providers continue to partner with Google as they introduce their latest network and technological advancements to the market. Whether it be operational resilience, disaster recovery capabilities, encryption of data in rest and in motion, or meeting privacy needs, Google is committed to keeping in step with the continuously evolving needs of their customers in the telecommunications industry.