Google Cloud Whitepaper
May 2019

Financial services compliance overview

Google Cloud

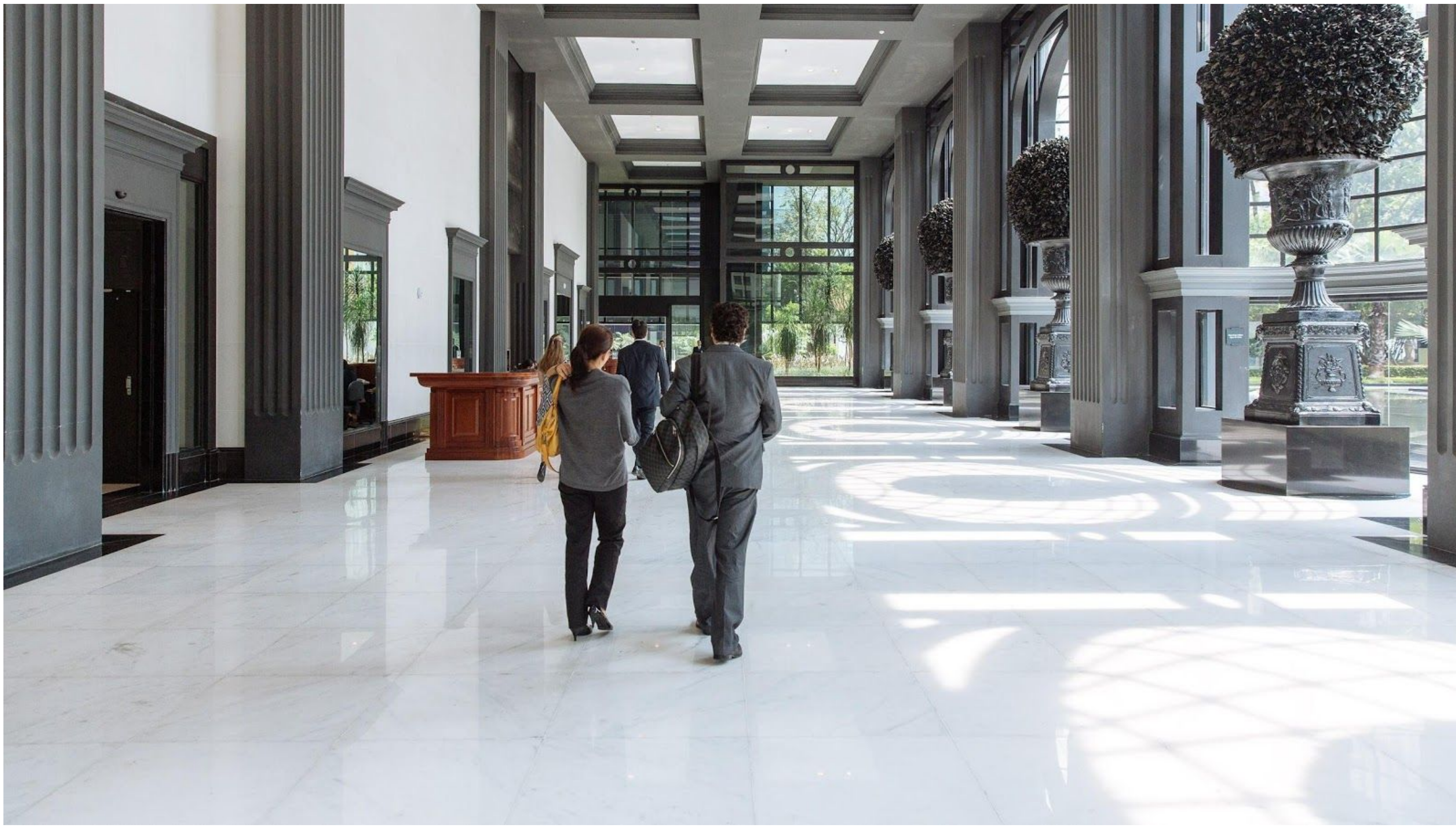
Introduction

The use of cloud services has become mainstream for organizations of every type and size across the globe. Cost savings, enhanced collaboration, business agility, artificial intelligence, and advanced data analytics are key benefits that can be realized through cloud adoption. Organizations migrating their workloads to the cloud can take advantage of Google's security capabilities and products. At Google Cloud, protecting the security and privacy of our customers' information is a top priority, and we have a team of more than 850 security professionals dedicated to this effort. We are committed to helping our customers with their compliance journey by providing robust security and privacy protections.

This whitepaper provides an overview of data security and privacy compliance in the cloud for financial services (FS) organizations and describes how Google Cloud is best suited to help organizations meet their regulatory requirements. We also address some common misconceptions about the cloud and answer frequently asked questions.

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of May 2019 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.



Financial services security and regulatory landscape

Organizations operating in the heavily regulated FS industry understand that the high-value information they process, transmit, and store is a constant target for adversaries to exploit. Over the past ten years, financial institutions (FIs) have faced mounting pressures from customer demands and new competition to improve internal operations for cost savings. These drivers of change have led to greater innovation through the use of new technologies and data-driven processes.

Underpinning the above challenges is the need to create a more robust defense and information security posture against the rise of cybercrimes and threats. While data protection and privacy have always been a priority for FIs, market and economic conditions have led to a growing number of regulations and security assurances required by financial services regulators. Given the complexity of the regulatory landscape, FIs (while early adopters of private clouds) were initially slow to migrate to the public cloud. The primary inhibitors commonly cited were security, compliance, and privacy. Nevertheless, adoption of public cloud services has gradually increased over the past few years, as FIs have realized the business and security benefits of making the shift.

As the global regulatory compliance landscape evolves, FIs have turned to cloud service providers (CSPs) as a means of risk mitigation and for the benefits of an infrastructure that can provide high availability along with data integrity, portability, and confidentiality. For their part, financial regulators have sought deeper understanding of the cloud and have begun establishing standards and guidance around the use of cloud computing. Regulators including the Federal Financial Institutions Examination Council in the United States, the European Banking Authority in the European Union, and the Monetary Authority of Singapore have all issued guidance for firms outsourcing to cloud services.

As cloud technologies continue to evolve, we expect regulators to further refine their guidance. They are likely to consider advancements in cloud technology, including how modern distributed networks such as Google Cloud operate (read Freedom of data movement in the cloud era for more information). The refined guidance is likely to center around security and privacy, with a principle-based approach enabling FIs to develop tailored and adaptable approaches to regulatory compliance and risk management that enhance security without stifling innovation and competition. At Google Cloud, we're engaged in an ongoing dialogue with regulators across the globe to help them understand the functionality and benefits of Google Cloud. We also work with regulators to ensure we understand the letter and spirit of the regulations they enforce, which enables us to continue building compliant cloud technologies.

Business case for financial services cloud adoption

FIs can realize many benefits by adopting cloud services, including cost reductions, information management efficiencies, and insights from data analytics.

Technology cost reduction

To offset the rising costs of doing business, FIs are seeking to reduce waste within their operations and improve utilization of IT, enabling them to more effectively compete and meet customer experience demand. Google Cloud enables FIs to meet these challenges through our preemptible virtual machines (VMs), sustained-use discounts, per-second billing, and committed-use discounts. We invite you to visit Google Cloud Pricing to learn more.

Information management efficiencies

Organizations face a continual challenge when it comes to managing their most critical data. With the emergence of various cloud technologies such as those offered by Google Cloud, FIs are evolving the way in which they approach this challenge.

Managers responsible for organizations' data protection technology decisions are moving beyond the silo approach in which information is heavily replicated across locations and storage sites with no central oversight. This typically involved backing up servers, adding email archiving, setting up disaster recovery, purchasing compliance-monitoring systems, and adding more offices requiring their own systems and infrastructure. This approach is not sufficiently scalable, and the disparate information silos create inefficiencies in the information management process.

Managers are now viewing their data landscapes through the lens of information management. By leveraging Google Cloud products, FIs can implement a flexible and scalable information technology model. Through this model they can instantly add or remove information management services as the need arises, without having to conduct technical or internal training or investing heavily in new infrastructure to take advantage of the latest technologies.

Centralized visibility and control is a core component of information management. Managers can use Cloud Deployment Manager to quickly build a comprehensive picture of when and how cloud resources and data are being used. This level of visibility simplifies the journey to comply with regulations about privacy, confidentiality, and retention. Data archiving and backup is another component of information management, and Google Cloud offers a variety of tools and resources for this. We invite you to visit Cloud SQL, Cloud Spanner, and Archival Cloud Storage to learn more.

As the following figure demonstrates, FIs that leverage Google Cloud for their information management needs can achieve increased operational efficiency, reduced costs, and increased revenue.

Benefits of leveraging the cloud for information management

Increased operational efficiency

- Centrally manage customer data across the organization
- Establish a single source of truth to improve data accuracy
- Eliminate duplicate activities in the middle and back office, and free resources to work on other revenue-generating and value-add activities

Reduced costs

- Eliminate the need for business units to collect data the risk, regulatory, and compliance functions have already gathered
- Reduce duplication of data between risk, regulatory, compliance, and customer intelligence systems
- Avoid wasted marketing expenses by carefully targeting marketing campaigns based on an improved understanding of customer needs and preferences

Increased revenue

- Customize products based on enhanced knowledge of each customer’s risk profile and risk appetite
- Identify new customer segments and potential new products through better understanding of customer patterns, preferences, and behaviors
- Enable a more complete view of the customer to pursue cross-sell and up-sell opportunities

Data analytics

Today's FIs deploy analytics and data-driven capabilities to increase growth and profitability, lower costs and improve efficiencies, drive digital transformation, and support risk and regulatory compliance priorities — all while supporting and driving the business strategy and priorities. Cloud technology further expands the analytical capabilities elastically upon demand, increasing analytical processing power quickly and efficiently. At Google Cloud, we know the power of big data. Our suite of services, including BigQuery, Cloud Dataflow, and Cloud Dataproc, is changing how customers analyze and use data.

Challenges to cloud adoption and Google's response

Data security and privacy

FIs increasingly expect a simple, fast-to-deploy, "always-on" IT service to meet business needs, and are prudently adopting cloud services to solve this challenge. Despite this gradual move to the public cloud, FIs must still contend with the growing number and sophistication of security threats and regulatory requirements. FIs must know what and how sensitive data is processed in all formats — whether it's in databases, exported data sheets, or stored in the cloud. Controlling and auditing access to sensitive data must also be monitored. Google Cloud's access and attestation logs can help FIs accomplish these objectives.

We offer a variety of security and privacy products to help organizations meet their policy requirements and protect their critical assets. These options cover the spectrum of security functions, including identity and access management (IAM), network security, endpoint security, data security, application security, and security monitoring. The following tables list some of our most popular Google Cloud Platform (GCP) and G Suite offerings.

Google Cloud Platform

Function	Offering	Description
Governance	Asset Tracking	Accurate, real-time global location data for fleets, assets, and devices
	Cloud Console	GCP's integrated management console
	Cloud Console Mobile App	Manage GCP services from your Android or iOS device
	Cloud Deployment Manager	Manage cloud resources with simple templates
	Cloud Endpoints	Develop, deploy, and manage APIs on any Google Cloud backend
	Cloud Healthcare API	Standards-based APIs powering actionable healthcare insights for security and compliance-focused environments
	Cloud Shell	Manage infrastructure and applications from the command line in any browser

Function	Offering	Description
Governance (continued)	Stackdriver	Monitoring and management for services, containers, applications, and infrastructure
	Stackdriver Monitoring	Provides visibility into the performance, uptime, and overall health of applications running on GCP and AWS
Identity & Access Management	Cloud IAM	Fine-grained identity and access management
	Cloud Identity	Easily manage user identities, devices, and applications from one console
	Cloud Identity-Aware Proxy	Use identity to guard access
	Cloud Resource Manager	Hierarchically manage resources on GCP
	Security Keys	Prevent phishing with security keys
Data Security	Cloud Data Loss Prevention API	Discover and redact sensitive data
	Cloud Hardware Security Module (HSM)	Protect your cryptographic keys in a fully managed cloud-hosted HSM service
	Cloud Key Management Service (KMS)	Manage encryption keys on GCP
	Encryption at Rest	Encryption at rest by default
Network Security	Application Layer Transport Security	Mutual authentication and transport encryption system
	Cloud Load Balancing	High-performance, scalable load balancing
	Encryption in Transit	Default TLS encryption provided to protect data in transit between customers and Google infrastructure
	Virtual Private Cloud (VPC)	Manage networking functionality for your Cloud Platform resources
	VPC Service Controls	Define secure access zones for sensitive data in GCP services
Infrastructure Security	Binary Authorization	Deploy only trusted containers on Kubernetes Engine
	Container Security	Secure your container environment on GCP
	Shielded VMs	Hardened virtual machines on GCP
Endpoint Security	Chrome Browser	Protection at every layer of the product, from malware and phishing protection to state-of-the-art sandboxing and network security

Function	Offering	Description
Endpoint Security (continued)	Chrome OS	Protect Chrome devices with enterprise-grade security
	Safe Browsing API	Protect devices by showing warnings to users across Google products
Application Security	Cloud Security Scanner	Automatically scan your App Engine apps
Security Monitoring & Operations	Access Transparency	Expand visibility over your cloud provider through near-real-time logs
	Cloud Security Command Center	A comprehensive security and data risk platform for GCP
	Stackdriver Logging	Store, search, analyze, monitor, and alert on log data

G Suite

Function	Offering	Description
Governance	G Suite Device Management	Mobile device management solution
Identity & Access Management	G Suite Doc Controls	Set file-sharing permissions for organizations
Data Security	G Suite DLP Mail	Scan your email traffic using data loss prevention (DLP) rules
	G Suite DLP Drive	Scan and protect Drive files using DLP rules

For more information on our products and services that help customers meet their policy, regulatory, and business objectives, refer to our Security Products page.

Regulatory compliance

Financial institutions seeking to adopt cloud solutions can utilize a CSP to support them in their compliance journey. Existing and new regulations place significant emphasis on FIs knowing how their data is being processed, who has access to customer data, and when security breaches occur.

Google Cloud continues to make significant investments in security, privacy, and compliance to support our customers in meeting their current and emerging regulatory compliance and risk management obligations. Our approach to supporting this effort include collaborating with our customers to understand and address their specific regulatory obligations, delineating responsibilities, conducting internal and independent audits, and delivering the necessary transparency. We also provide our customers with information about our internal risk and compliance programs, domain best practices, along with easy access to documentation. These enable our customers in documenting a complete, integrated controls and governance framework.

Our commitments to you about your data

Your data is critical to your business, and you take great care to keep it safe and under your control. We want you to feel confident that taking advantage of G Suite and Google Cloud Platform doesn’t require you to compromise on security or control of your business’s data.

At Google Cloud, we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data in the cloud.

When you use Google Cloud, you can:

1. **Know that your security comes first in everything we do.**

   We promptly notify you if we detect a breach of security that compromises your data.
2. **Control what happens to your data.**

   We process customer data according to your instructions. You can access it or take it out at any time.
3. **Know that customer data is not used for advertising.**
   You own your data. Google Cloud does not process your data for advertising purposes.
4. **Know where Google stores your data and rely on it being available when you need it.**

   We publish the locations of our Google data centers; they are highly available, resilient, and secure.
5. **Depend on Google’s independently verified security practices.**

   Our adherence to recognized international security and privacy standards is certified and validated by independent auditors — wherever your data is located in Google Cloud.

6. **Trust that we never give any government entity "backdoor" access to your data or to our servers storing your data.**

   We reject government requests that are invalid, and we publish a transparency report for government requests.

Please refer here for more details on our Trust Principles. Also see our data processing terms for Google Cloud Platform and G Suite for further details.

Operational resiliency

The significance of IT operational resiliency in the FS industry has been constantly increasing. FS regulators are imposing fines on FIs that experience interruptions in services which impact customers. Additionally, regulators are seeking to identify and eliminate sources of systemic risk from the high degree of technology that FIs depend on to operate and grow their business, leading to increased efforts to satisfy regulatory compliance.

FIs must be proactive to ensure IT operational resilience in an environment susceptible to technical failures, software glitches, cyber attack, human error, and natural disasters. Any of these factors have the potential to cripple an enterprise. The best way to avoid unanticipated downtime is to add redundancy. This means backing up important databases and architecting a replication solution, which can result in high costs. FIs are turning to cloud solutions to strengthen their resilience and meet stringent internal downtime requirements in a cost-effective manner. Similar to building resiliency, organizations are also leveraging the cloud for cost-effective disaster recovery (DR) plans that meet recovery time objectives and recovery point objectives. Cloud-based DR solutions provide the means to store log data and historical data needed to meet compliance regulations. They also provide the means for application recovery and server failover. Organizations are moving to the cloud to enhance their DR and IT resilience, and it is clear why. In fact, the market size for disaster recovery as a service is expected to grow at an estimated 45.9% CAGR, reaching more than $11 billion in 2021, as a result of organizations moving to cloud-based disaster recovery.[1]

FIs are turning to cloud solutions to strengthen their resilience and meet stringent internal downtime requirements in a cost-effective manner.

[1] Disaster Recovery as a Service Market by Service Type - Global Forecast to 2021, (n.d.). Retrieved April 4, 2019, from https://www.geminare.com/2015/06/marketsandmarkets-disaster-recovery-service-market-service-type-global-forecast-2021/ MarketsAndMarkets

The SLAs for Google Cloud's service offerings meet system availability requirements for organizations across various industries. We have data centers geographically distributed to minimize the effects of disruptions caused by local and regional incidents. Application and network architecture are designed for maximum reliability and uptime. We utilize robust software failover within our cloud computing platform to minimize the impact of unlikely hardware disruptions. All systems within the Google infrastructure that support Google Cloud services are redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation. Data is replicated multiple times across active servers so, in the case of a machine failure, data will still be accessible through another system. For more information, refer to our GCP SLAs and G Suite SLA.

Furthermore, we have a business continuity program for our data centers and production operations to account for major disasters such as earthquakes or other incidents like public health crises. This program is designed to enable continued delivery of our services to our customers. Our DR program enables continuous and automated disaster readiness, response, and recovery of our business, systems, and data. We conduct DR testing on a regular basis to provide a coordinated venue for infrastructure and application teams to test communication plans, failover scenarios, operational transition, and other emergency responses. All teams that participate in the DR exercise develop testing plans and contribute to postmortems that document the results, lessons learned, and remediation plans (if applicable).

We have data centers geographically distributed to minimize the effects of disruptions caused by local and regional incidents. Application and network architecture are designed for maximum reliability and uptime.

Data portability and migration

Porting data and migrating from one system to another can be a daunting task. The cloud provides an opportunity to address this challenge. Instead of taking weeks to install hardware from multiple vendors in a data center, cloud customers can launch everything from a common platform. And, because this process all happens through software, it is easier for customers to view the technology they have created and the types of activities and data it uses. As a result, FIs can build a consistent set of compliance processes across business units and functions.

Google Cloud's focus on data portability and migration helps FIs that have concerns about moving entire workloads to the cloud. FIs with significant legacy infrastructure and data footprints express apprehension that cloud migration projects are overly complex. The overall architecture of Google Cloud makes cloud migration easier. Our customers can start by using individual service capabilities — such as the machine learning application programming interfaces (APIs), or BigQuery — and then transition additional workloads to the cloud over time. To further ease legacy integration, containerization is now an effective way to move legacy workloads to the cloud because it enables organizations to package software and dependencies in executable units (containers) and port those directly to the cloud. We provide Kubernetes Engine for deploying containerized applications. The main value of containerization is not just migration, but also the encapsulation of security and network connectivity that can be managed by a central team. This process can run as a customer-managed container deployment on Google Compute Engine or as a Google-managed deployment on Google Kubernetes Engine. Additionally, for FIs migrating to G Suite, Google's CloudMigrator, CloudMigrator Go, and Managed Migration help them transfer email, calendars, contacts, and files from enterprise sources to G Suite. These tools and services have been used to migrate over 7.1 million users across 81 countries worldwide.

Google Cloud's focus on data portability and migration helps FIs that have concerns about moving entire workloads to the cloud.

Dispelling cloud adoption misconceptions

The move to cloud is a transformative experience for organizations — and a means of embracing progressive and modern technology. Still, concerns over data control and information security have led to some misconceptions about what it means to use services provided by a CSP. We are working with our customers to address the root of their concerns.

Common misconception #1: *Lost sense of control*

A common regulatory requirement that hasn't changed with the usage of cloud computing is for FIs to abide by the same standards of outsourcing which require them to know what data is being transmitted or stored. These regulatory obligations also include FIs setting the controls to secure their data and knowing the steps to recover data in case of disaster for business continuity. At Google Cloud, we process our customers' data according to their instructions. Our customers can access their data when they want or take it out at any time. We provide a host of services to enable them to control the information they upload as well as logging and monitoring reports to support audit requirements.

We have built a global infrastructure that is geared toward serving customers in a low-latency, high-performance manner with a high degree of security.

Common misconception #2: *Cloud suffers from more breaches*

The risk of a data breach in the cloud is multiplying, with breaches becoming costlier and happening more frequently, according to a 2016 Ponemon study. This does not mean that cloud computing is less secure than on-premises deployments. Instead, it highlights the need for FIs to perform proper due diligence for CSPs that can provide secure services and platforms to handle the increased emphasis on data security.

Google Cloud's infrastructure is designed, built, and operated with security at our core. We protect our customers' data and intellectual property by monitoring data health, detecting anomalous behaviors, and proactively preventing security incidents utilizing machine intelligence. We regularly undergo independent verification of security, privacy, and compliance controls to ensure we comply with stringent global data protection standards.

Common misconception #3:
The cloud service provider is responsible for its customers' compliance

As regulations evolve with the invention of new technologies, FIs and CSPs should help shape policies that govern, but do not stifle innovation. FIs should also recognize the advantages of cloud technology solutions to create a proactive and automated approach to compliance.

It is imperative that organizations understand the types of services they are consuming, as there are significant implications around security and compliance. FIs may need to adapt their security and compliance strategies to account for the cloud services being delivered. Each cloud delivery model brings varying levels of management responsibilities that are spread across various business units including IT, Privacy, Compliance, Security, Risk Management, and Legal. It is important to understand also that while CSPs may assume certain responsibilities contractually with FIs, the FIs remain at all times responsible for their own legal and regulatory compliance obligations.

Frequently asked questions

How are FIs using the cloud?

FIs have already been migrating functions like customer relationship management (CRM), human resources (HR), and financial accounting to the cloud. A trend is emerging where FIs are migrating core business functions such as data analytics to the cloud. Risk analytics applications that are used to calculate metrics like cost of trade, current value, and yields on securities are being implemented on cloud-based platforms such as GCP. Big data analytics to generate customer insights to help FIs focus on services that align with customer needs is being performed using cloud services such as Google's BigQuery. Another emerging trend is the use of cloud-based machine learning to improve compliance management, deliver a better customer experience, and detect and prevent fraud.

How are responsibilities shared between Google Cloud and its customers?

Google Cloud and its customers share responsibilities for managing the IT environment, including those related to security and compliance. Shared responsibility enables our customers to allocate resources more effectively by reducing the amount of effort needed to provision and support their IT environment. Our Shared Responsibility Model does not remove the accountability and risk from customers using our services, but it does help relieve the burden as we manage and control system components and physical control of facilities. It also shifts a portion of the cost of security and compliance onto Google Cloud and

away from customers. Note that customers are ultimately responsible for ensuring their own compliance with applicable laws and regulations.

Our role in the Shared Responsibility Model includes providing services on a highly secure and controlled platform and offering a wide array of features that customers can tailor to their needs. For GCP services such as BigQuery, Google App Engine, Google Compute Engine, and Google Cloud Storage, we define and document roles and responsibilities in a shared responsibility matrix, developed with Payment Card Industry Data Security Standard (PCI DSS) requirements in mind. For G Suite offerings such as Gmail and Drive, we are responsible for the majority of the management functions. To see an example of how we document shared compliance responsibilities with our customers, please visit GCP: Customer Responsibility Matrix.

How does Google Cloud prevent unauthorized access to its customers' data by other tenants?

To prevent unauthorized access by other tenants sharing the same physical server, we logically isolate our customers' data. We also have a variety of isolation and sandboxing techniques for protecting a service from other services running on the same machine. These techniques include normal Linux user separation, language and kernel-based sandboxes, and hardware virtualization. Furthermore, we perform encryption at the application layer, which allows our infrastructure to isolate itself from potential threats at the lower levels of storage such as malicious disk firmware.

How does Google Cloud prevent unauthorized access to its customers' data by external threats?

To prevent unauthorized access to our customers' data from external threat actors, we employ a defense-in-depth approach starting with state-of-the-art physical security at our data centers. We have also designed our entire infrastructure stack for security, using cryptographic signatures to ensure no unauthorized changes can be made without detection. This starts from low-level components, such as the BIOS, and includes all key components of the boot process, such as the bootloader, kernel, and the base operating system. All of these are controlled, built, and hardened by us. In short, we develop and deploy physical and virtual infrastructure using rigorous security practices. In addition, our operations teams detect and respond to threats to the infrastructure from insiders and external actors, 24/7/365.

How do Google Cloud customers gain visibility and access to their own audit and security logs?

Google Cloud maintains two audit logs: Admin Activity and Data Access. Google Cloud services write audit log entries to these logs to help its customers answer the questions of "who did what, where, and when?" within the Google Cloud services being used. Admin Activity logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, the logs record when VM instances and App Engine applications are created and when permissions are changed. Data Access audit logs record API calls that create, modify, or read user-provided data. In summary, we provide our customers the tools they need to manage their organization's information at all times so they have extensive control and visibility over system and application security settings. Visit our Cloud Audit Logging page to learn more.

Conclusion

As FIs increasingly adopt cloud services and reap the myriad benefits of this transformational change, they also need to ensure that they are meeting their regulatory compliance and risk management obligations. For this reason, Google Cloud technologies and services are designed with compliance in mind, while recognizing that we must enable our customers, including the FIs, to keep pace with drivers of change in their highly competitive and regulated business environments.

In taking advantage of Google Cloud products, FIs can have the confidence that comes with the transparency we provide to our customers with respect to how their information is processed, transmitted, and safeguarded by Google Cloud. In addition, adopting Google Cloud service means working with a team that is committed to upholding the responsibilities we share with our customers with respect to data security and privacy.

At Google Cloud, we work continuously to ensure our customers are well positioned to meet their regulatory and compliance requirements. We also engage with them, through means such as this whitepaper, to help them understand our approach to compliance and risk management, so they can, in turn, build and maintain trust with their stakeholders.

To learn more about our products, or to contact us, please visit cloud.google.com.