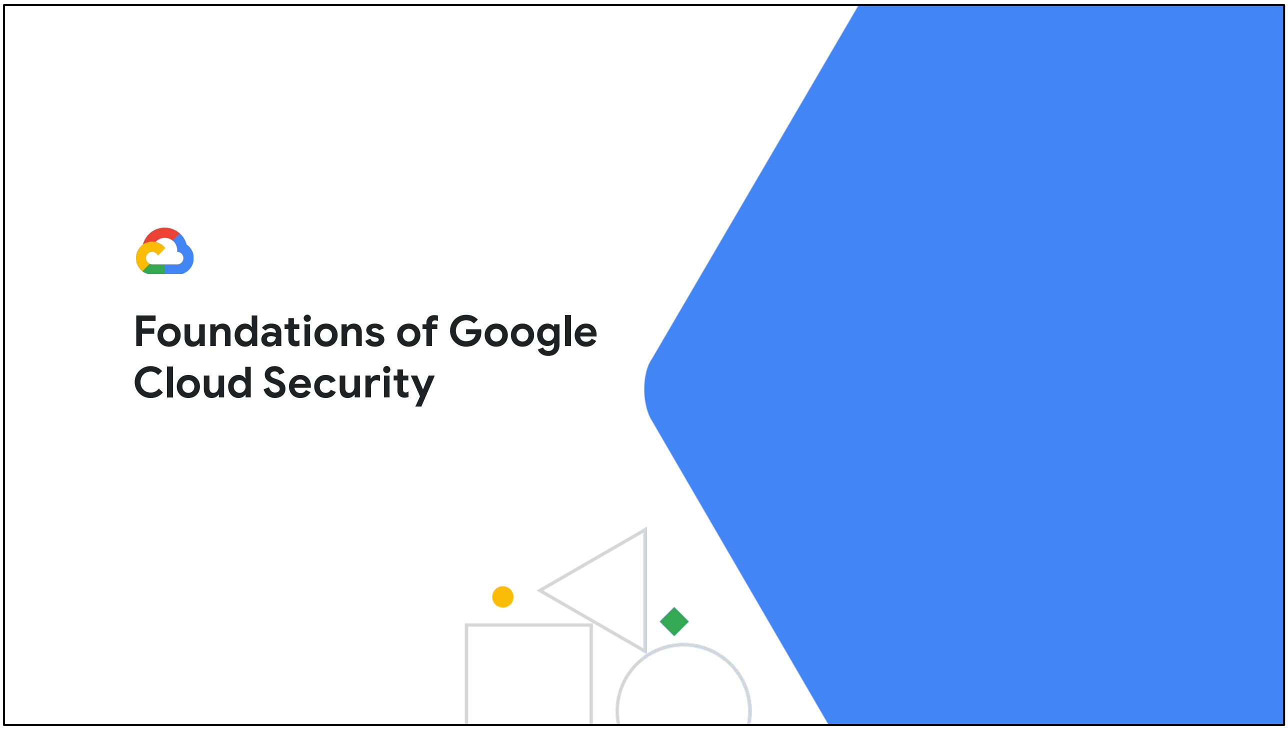
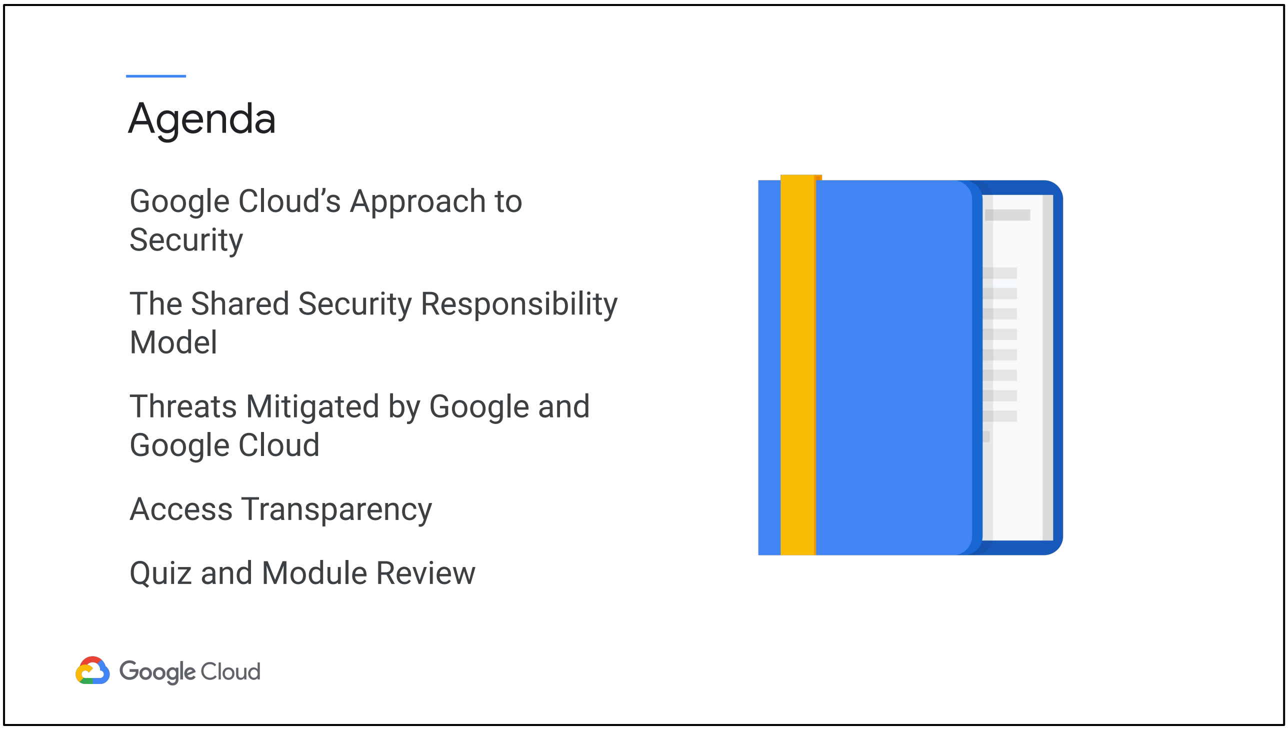


Foundations of Google Cloud Security

Welcome to the Foundations of Google Cloud Security module.



Agenda

Google Cloud's Approach to Security

The Shared Security Responsibility Model

Threats Mitigated by Google and Google Cloud

Access Transparency

Quiz and Module Review

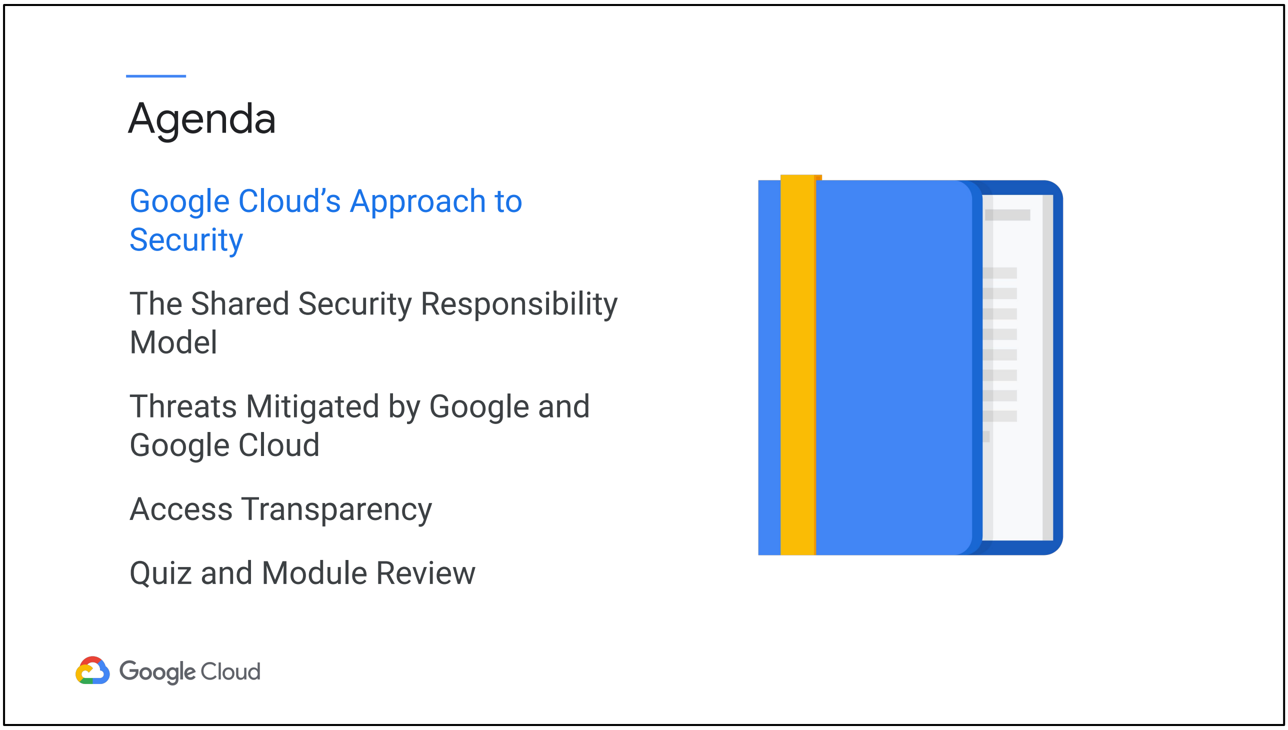
We are glad you are interested in learning more about Google Cloud security. Securing systems is a hot topic and should be a priority for everyone today - and, as you will see, it is definitely a priority here at Google.

In this module, we will introduce you to Google Cloud's approach to security.

We will also discuss the shared security responsibility model, which is a collaborative effort between Google and its users.

Next, we will outline several threats that are mitigated for you when your systems are run on Google's infrastructure in Google Cloud.

And, finally, we will end with a section on access transparency.



Agenda

Google Cloud's Approach to Security

The Shared Security Responsibility Model

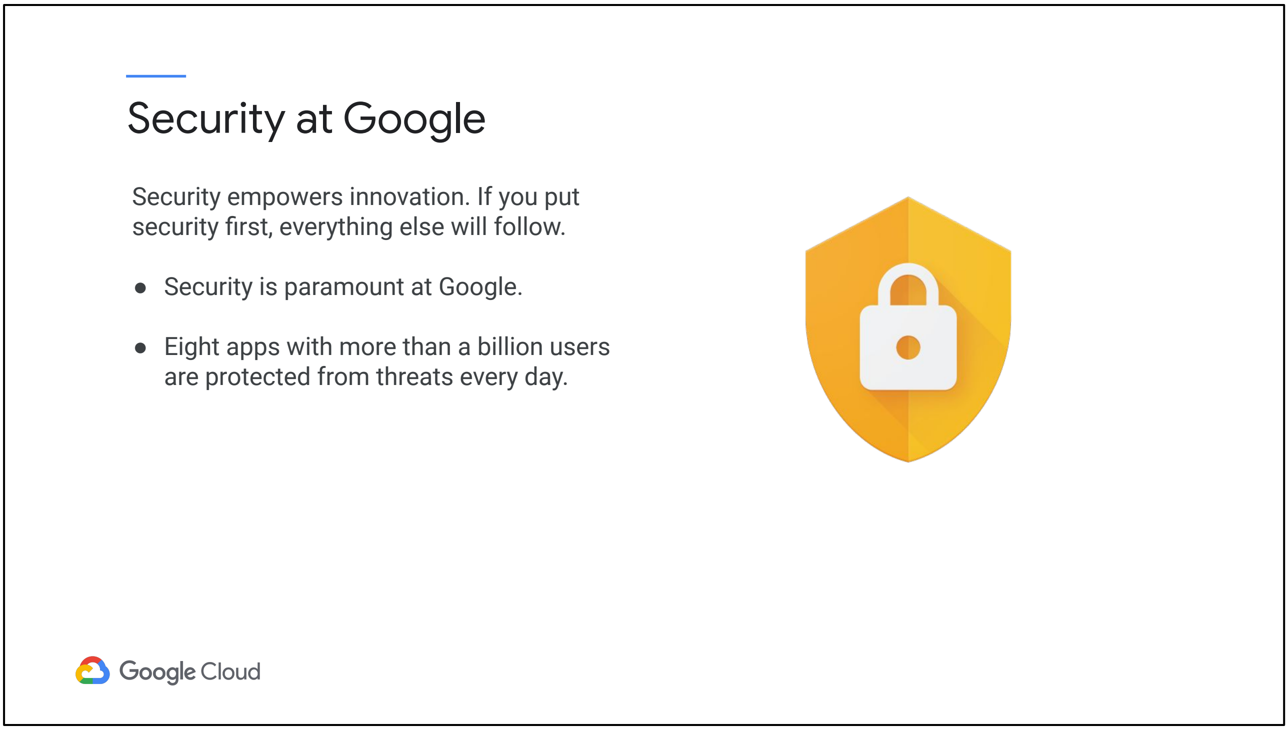
Threats Mitigated by Google and Google Cloud

Access Transparency

Quiz and Module Review

Google Cloud

OK, let's get started with an outline of Google Cloud's approach to security...



Security at Google

Security empowers innovation. If you put security first, everything else will follow.

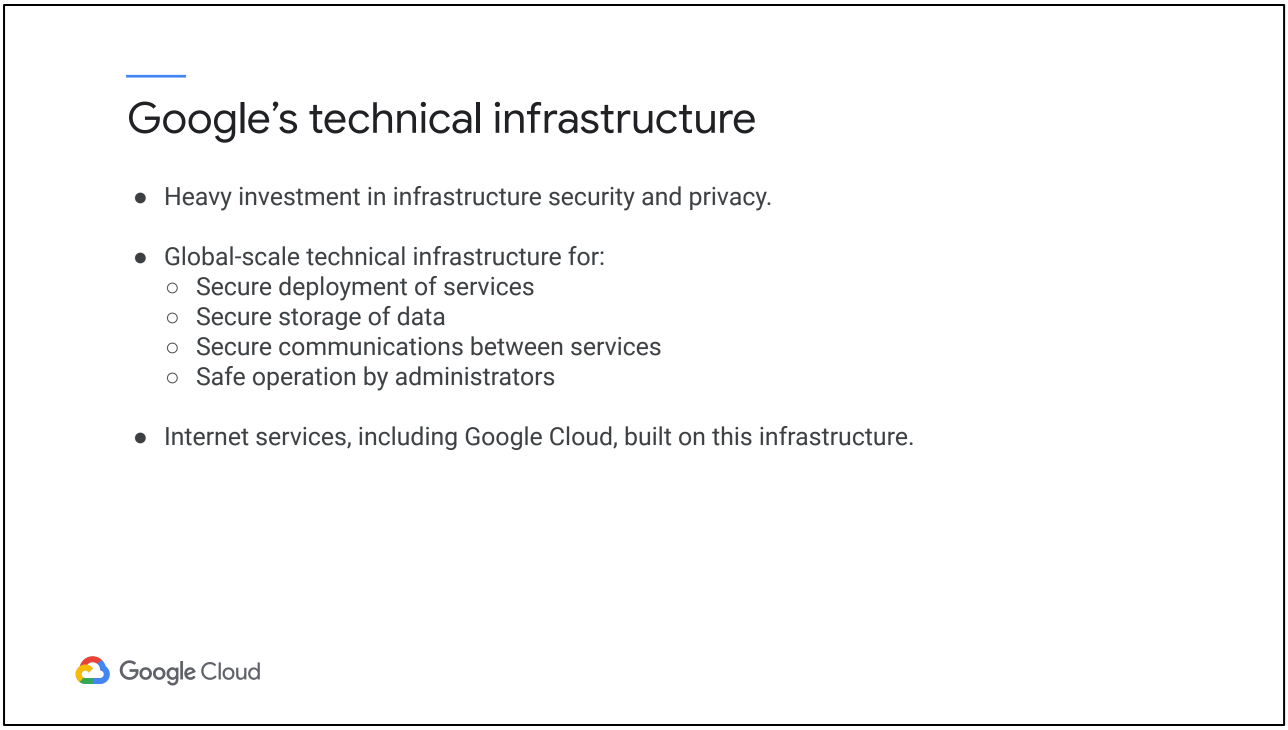
- Security is paramount at Google.
- Eight apps with more than a billion users are protected from threats every day.

Google Cloud

At Google, we believe security empowers innovation. We've been operating securely in the cloud for over 20 years!

Google has eight services with more than a billion users, and Google Cloud connects to more than a billion IPs every day. This means security is always on the minds of Google's employees.

Designing for security is pervasive throughout the infrastructure that Google Cloud and Google services run on. Security is always paramount!



Google’s technical infrastructure

- Heavy investment in infrastructure security and privacy.
- Global-scale technical infrastructure for:
  - Secure deployment of services
  - Secure storage of data
  - Secure communications between services
  - Safe operation by administrators
- Internet services, including Google Cloud, built on this infrastructure.

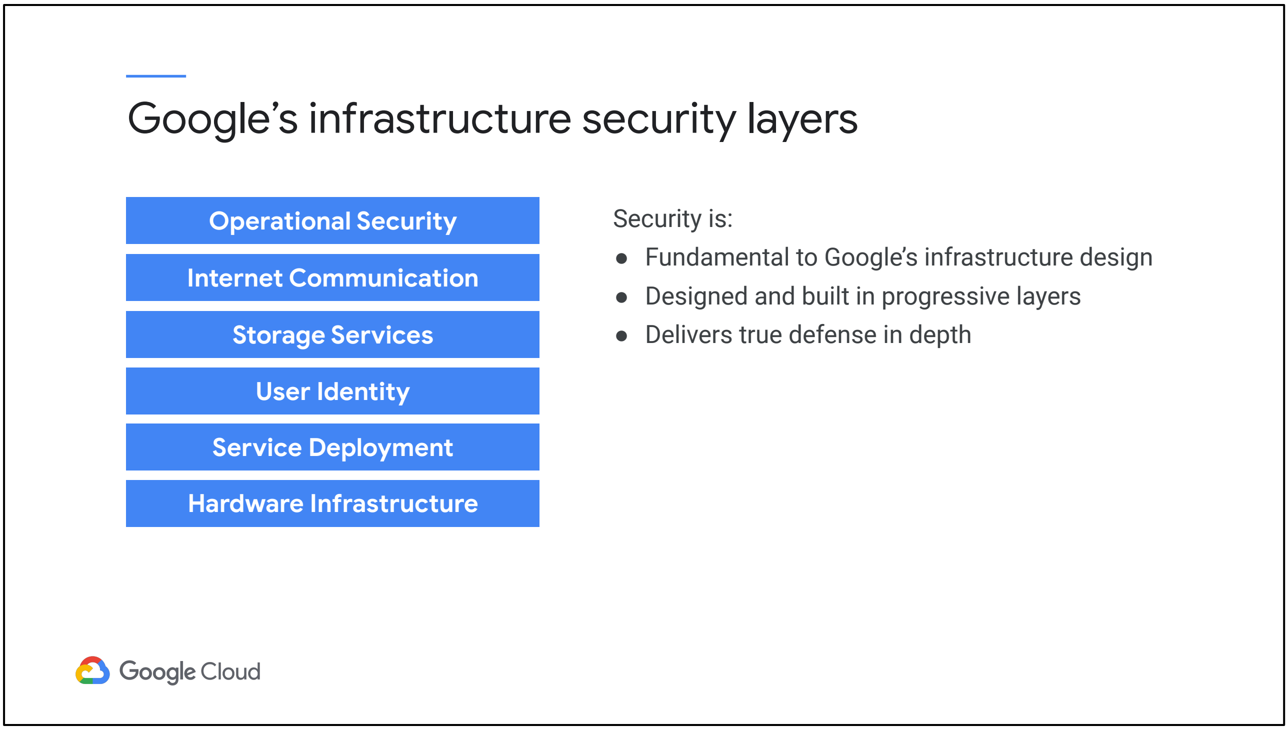
Google Cloud

Countless companies and governments have lost data because of security incidents. Just one such breach could cost millions in fines and lost business—and more importantly, the loss of customer trust.

As a result, security is increasingly becoming a high priority for CEOs and Boards of Directors.

Unfortunately, many organizations do not have access to the resources needed to implement state-of-the-art security controls and techniques. Google has invested heavily in its technical infrastructure and has hundreds of dedicated engineers to provide a secure and robust platform. Deploying your systems on Google Cloud allows you to leverage that same infrastructure and can help you secure your services and data through the entire information processing lifecycle, including:

- Secure deployment of services
- Secure storage of data
- Secure communications between services
- Safe operation by administrators



Google’s infrastructure security layers

- Operational Security
- Internet Communication
- Storage Services
- User Identity
- Service Deployment
- Hardware Infrastructure

Security is:

- Fundamental to Google’s infrastructure design
- Designed and built in progressive layers
- Delivers true defense in depth

Google Cloud

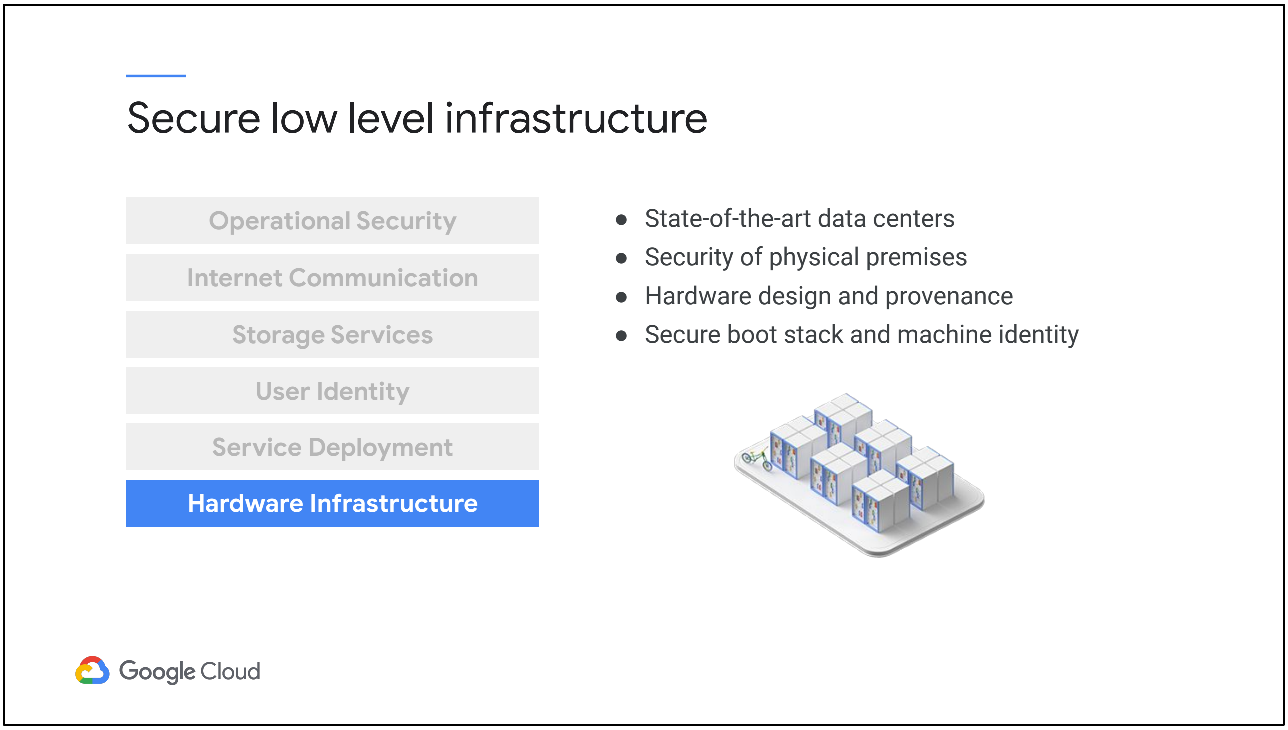
It’s not enough to build something and try to make it secure after the fact.

Security should be fundamental to all designs, not bolted on to an old paradigm.

That’s why we build security through progressive layers that are integrated from the ground up.

Google Cloud delivers true defense in depth, meaning our cloud infrastructure doesn’t rely on any one technology to make it secure.

Let’s talk about a few of our security layers, starting at the bottom and working up.



Secure low level infrastructure

Operational Security

Internet Communication

Storage Services

User Identity

Service Deployment

Hardware Infrastructure

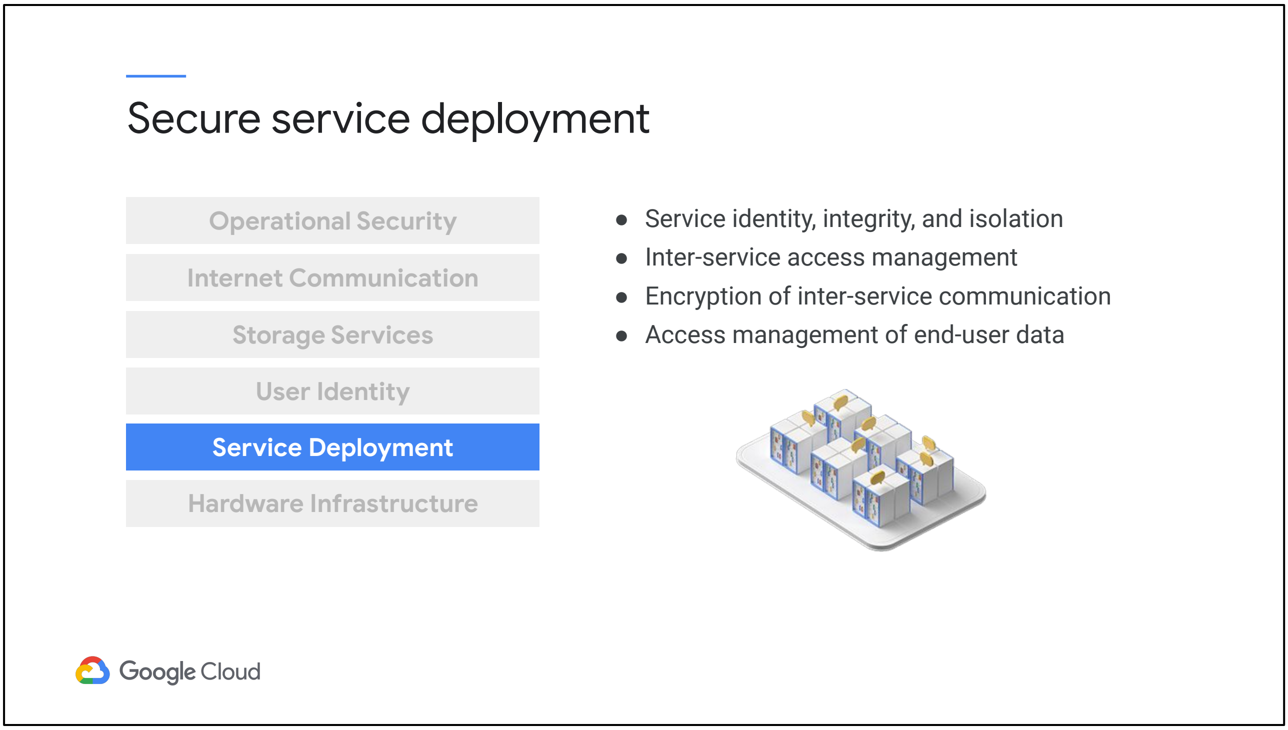
- State-of-the-art data centers
- Security of physical premises
- Hardware design and provenance
- Secure boot stack and machine identity

Google Cloud

Google designs and builds its own data centers, which incorporate multiple layers of physical security protections. Access to these data centers is limited to only a very small fraction of Google employees.

Both the server boards and the networking equipment in Google data centers are custom-designed by Google. Google also designs custom integrated circuits, including a hardware security chip called Titan that's currently being deployed on both servers and peripherals.

Google server machines use cryptographic signatures to make sure they are only booting the correct software.



Secure service deployment

- Operational Security
- Internet Communication
- Storage Services
- User Identity
- **Service Deployment**
- Hardware Infrastructure

- Service identity, integrity, and isolation
- Inter-service access management
- Encryption of inter-service communication
- Access management of end-user data

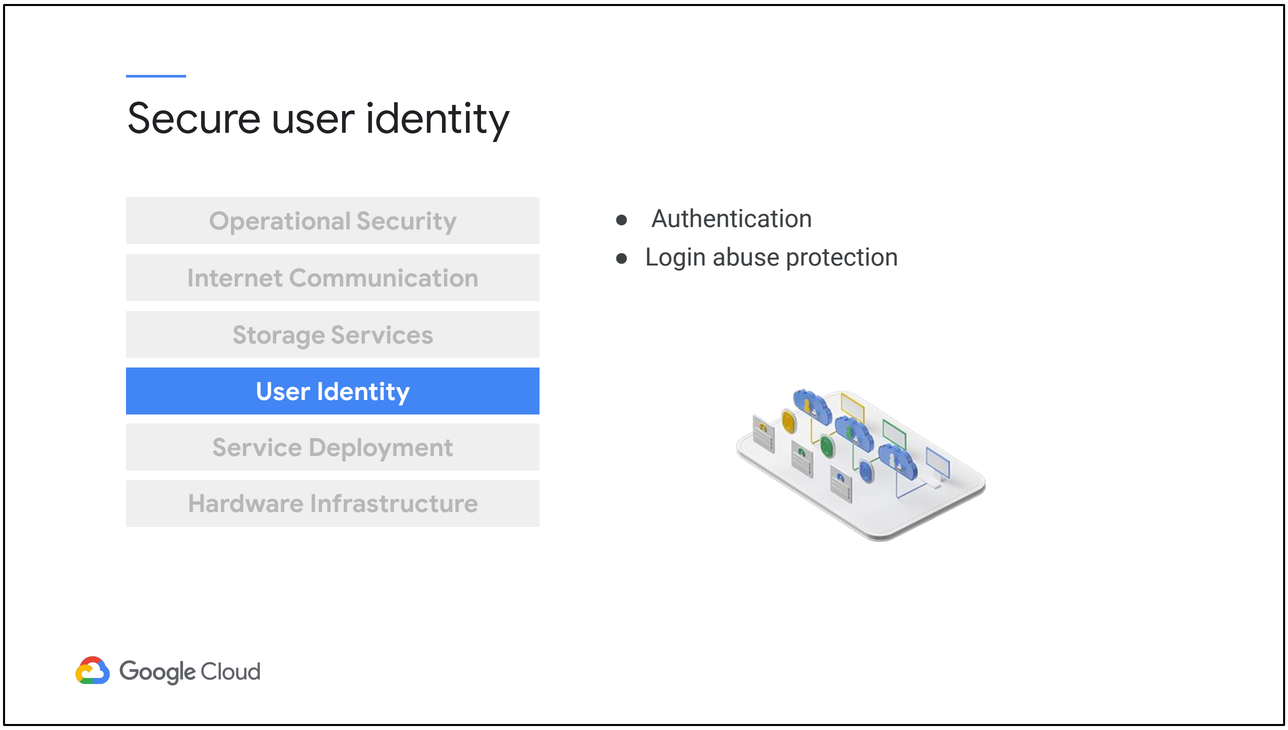
Google Cloud

Google's infrastructure provides cryptographic privacy and integrity for remote procedure call ("RPC") data on the network, which is how Google's services communicate with each other. The infrastructure automatically encrypts RPC traffic in transit between data centers.

To help ensure that code is secure as possible, Google stores its source code centrally and requires two-party review of new code.

Google also gives its developers libraries that keeps them from introducing certain classes of security bugs.

Externally, Google also runs a bug bounty program where we pay anyone who is able to discover and inform us of bugs in our infrastructure or applications.



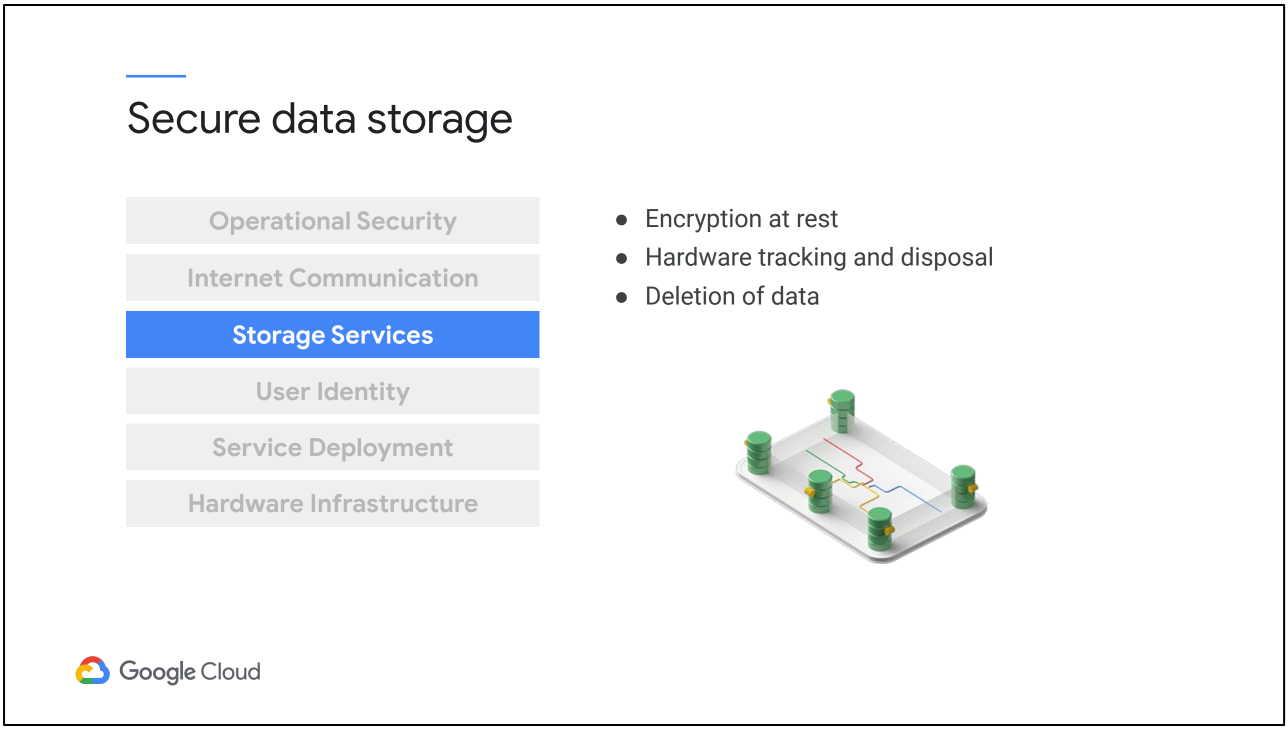
Secure user identity

- Operational Security
- Internet Communication
- Storage Services
- **User Identity**
- Service Deployment
- Hardware Infrastructure

- Authentication
- Login abuse protection

Google’s central identity service, which usually manifests to end users as the Google login page, goes beyond asking for a simple username and password. It also intelligently challenges users for additional information based on risk factors such as whether they have logged in from the same device or a similar location in the past. Users can also use second factors when signing in, including devices based on the Universal 2nd Factor (U2F) open standard.

To guard against phishing attacks, all Google employee accounts, including mine, require the use of U2F compatible security keys.



Secure data storage

- Operational Security
- Internet Communication
- **Storage Services**
- User Identity
- Service Deployment
- Hardware Infrastructure

- Encryption at rest
- Hardware tracking and disposal
- Deletion of data

Google Cloud

In Google Cloud, all data is encrypted at rest by default - without any need for you to configure or enable anything.

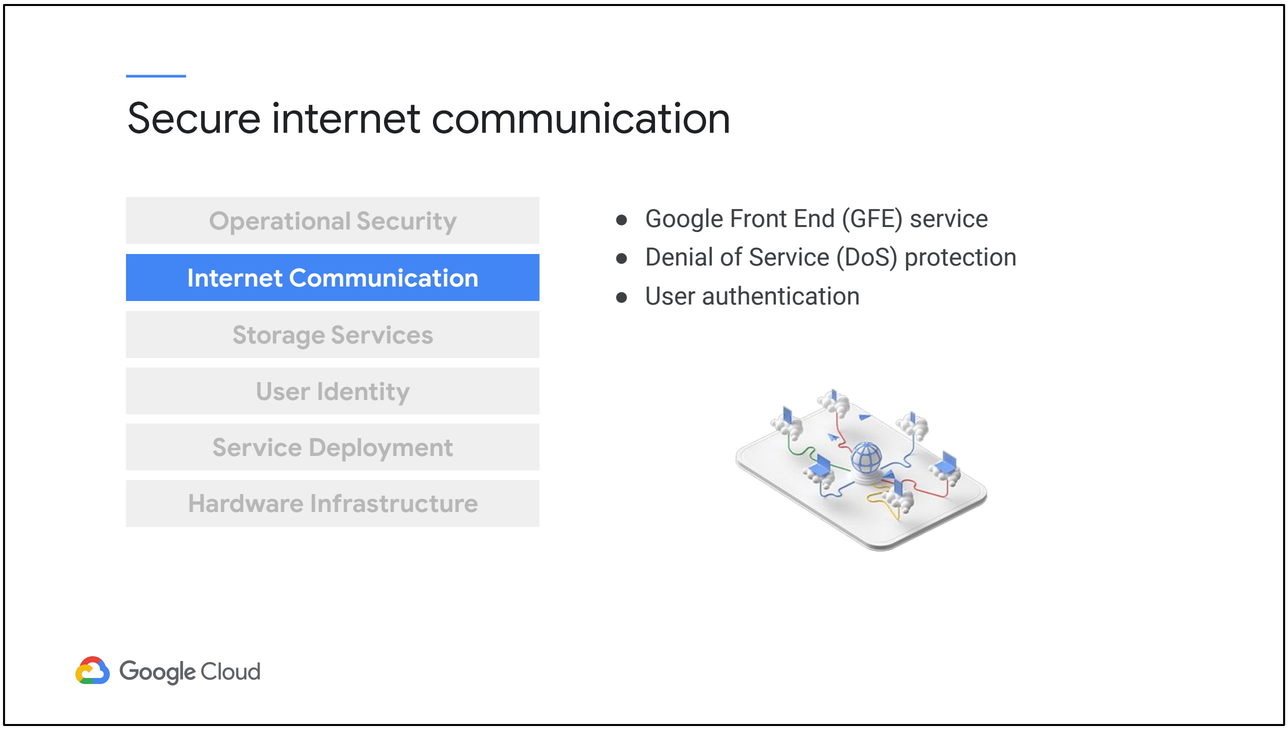
This default encryption leverages Google-managed encryption keys, but also supports:

- Customer Managed Encryption keys, where you can manage your own encryption keys with the Google Key Management Service (KMS)
- And Customer Supplied Encryption keys, where you can provide and manage your own keys.

Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization.

When a hard drive is retired, the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi-stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility.

Additionally, if customers delete their own data, we commit to deleting it from our systems within 180 days.



Secure internet communication

- Operational Security
- **Internet Communication**
- Storage Services
- User Identity
- Service Deployment
- Hardware Infrastructure

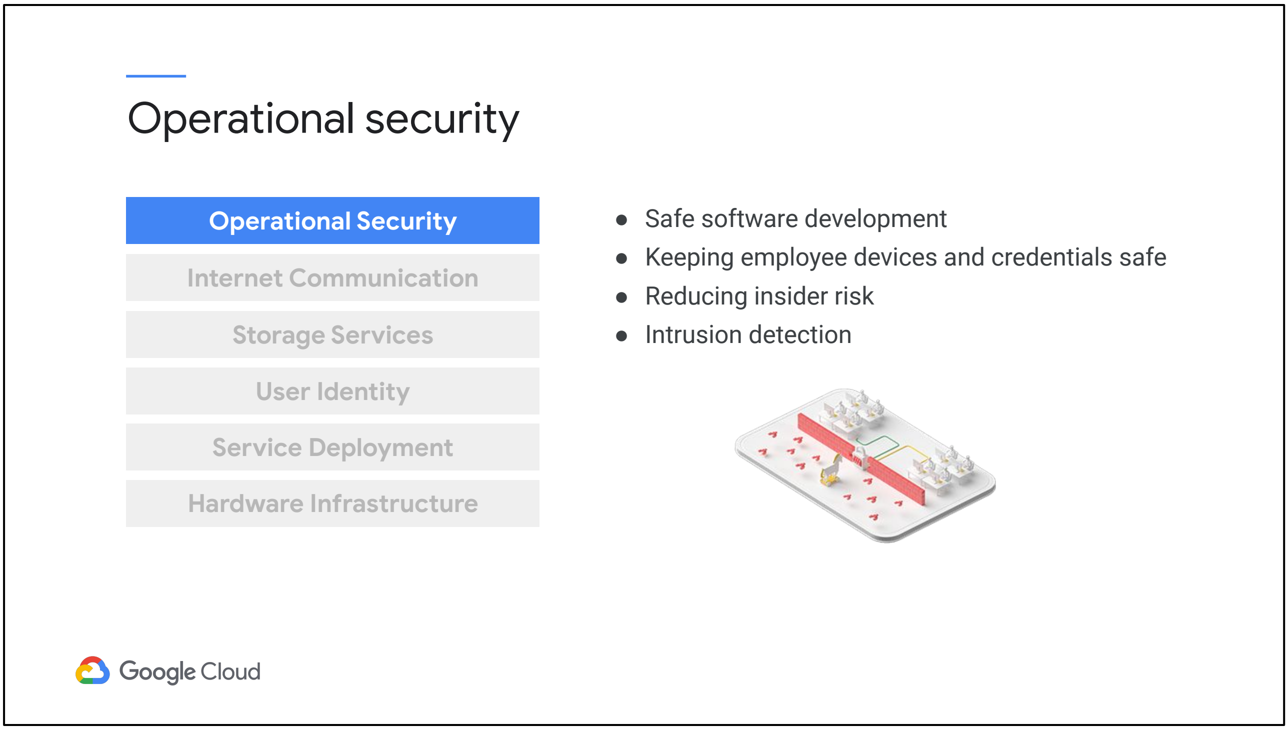
- Google Front End (GFE) service
- Denial of Service (DoS) protection
- User authentication

Google Cloud

Google services that want to make themselves available on the Internet register themselves with an infrastructure service called the Google Front End (GFE). GFE checks incoming network connections for correct certificates, best practices, supports strong encryption, and adds protection against Denial of Service attacks.

The sheer scale of its infrastructure enables Google to simply absorb many Denial of Service attacks. Even behind the GFEs, Google also has multi-tier, multi-layer Denial of Service protections that further reduce the risk of any DoS impact. Cloud customers can take advantage of this extra protection by using the Google Cloud Load Balancer

The Cloud Platform also offers customers additional transport encryption options for connecting on-premises resources to the cloud. These options are Cloud VPN for establishing IPSec connections, and Direct Interconnect.



Operational security

- Operational Security
- Internet Communication
- Storage Services
- User Identity
- Service Deployment
- Hardware Infrastructure

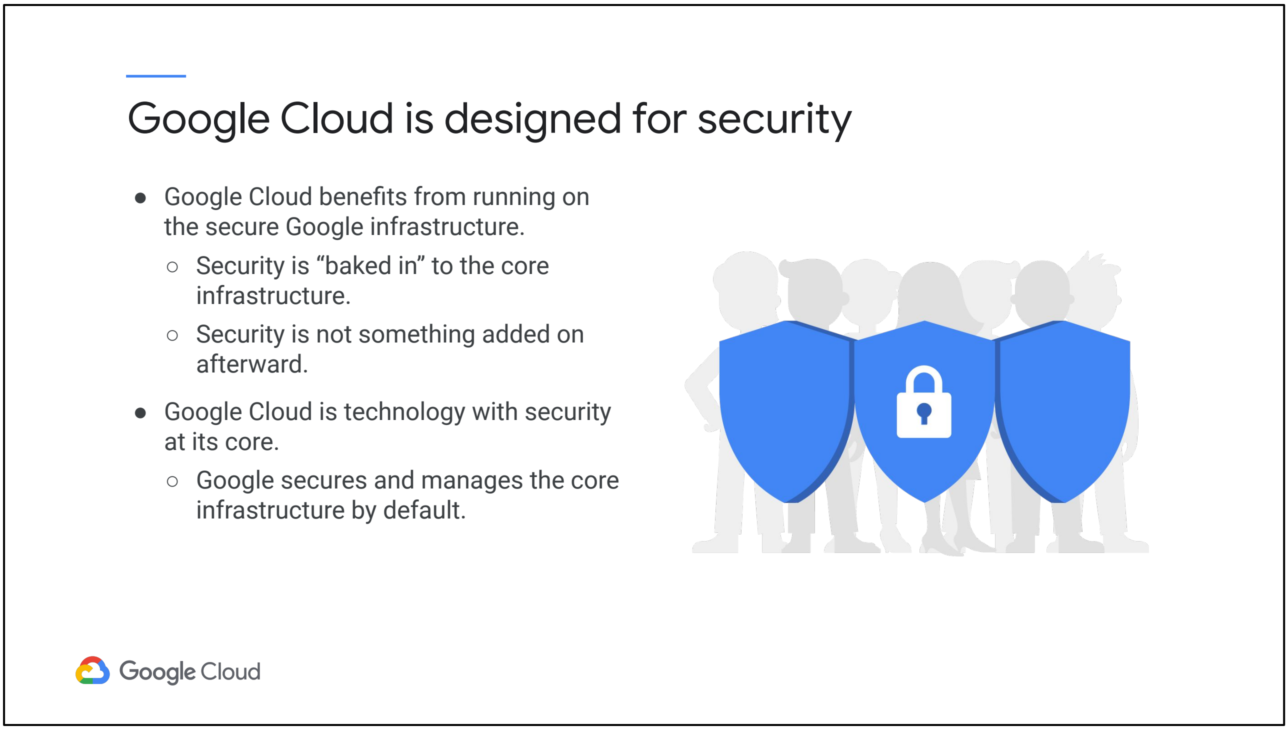
- Safe software development
- Keeping employee devices and credentials safe
- Reducing insider risk
- Intrusion detection

Google Cloud

Google has created security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and in company-wide events to raise awareness.

Before they join our staff, Google will verify an individual's education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, Google may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position.

All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers.



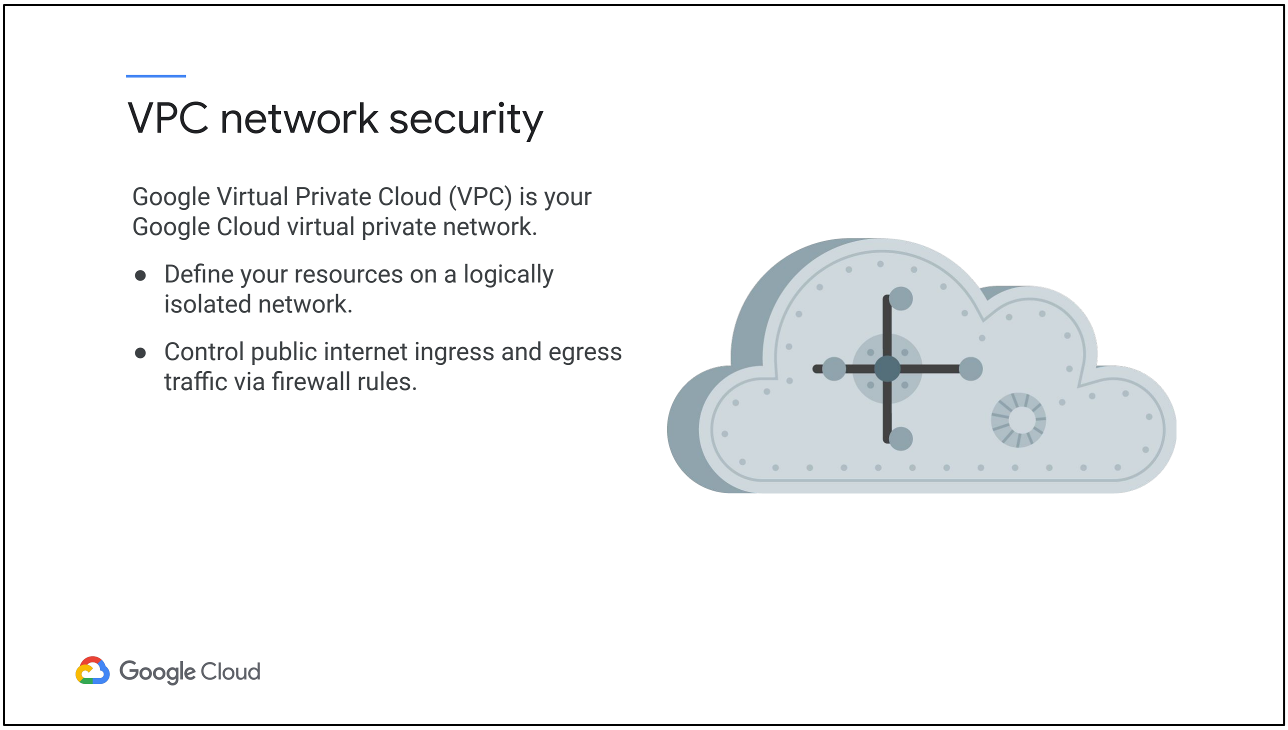
Google Cloud is designed for security

- Google Cloud benefits from running on the secure Google infrastructure.
  - Security is “baked in” to the core infrastructure.
  - Security is not something added on afterward.
- Google Cloud is technology with security at its core.
  - Google secures and manages the core infrastructure by default.

Google Cloud

Now you have a feeling for the high level of security implemented and “baked into” Google’s Infrastructure.

Google Cloud benefits from running on top of all of this secure Google infrastructure. So as you can see, Google Cloud is designed for security.



VPC network security

Google Virtual Private Cloud (VPC) is your Google Cloud virtual private network.

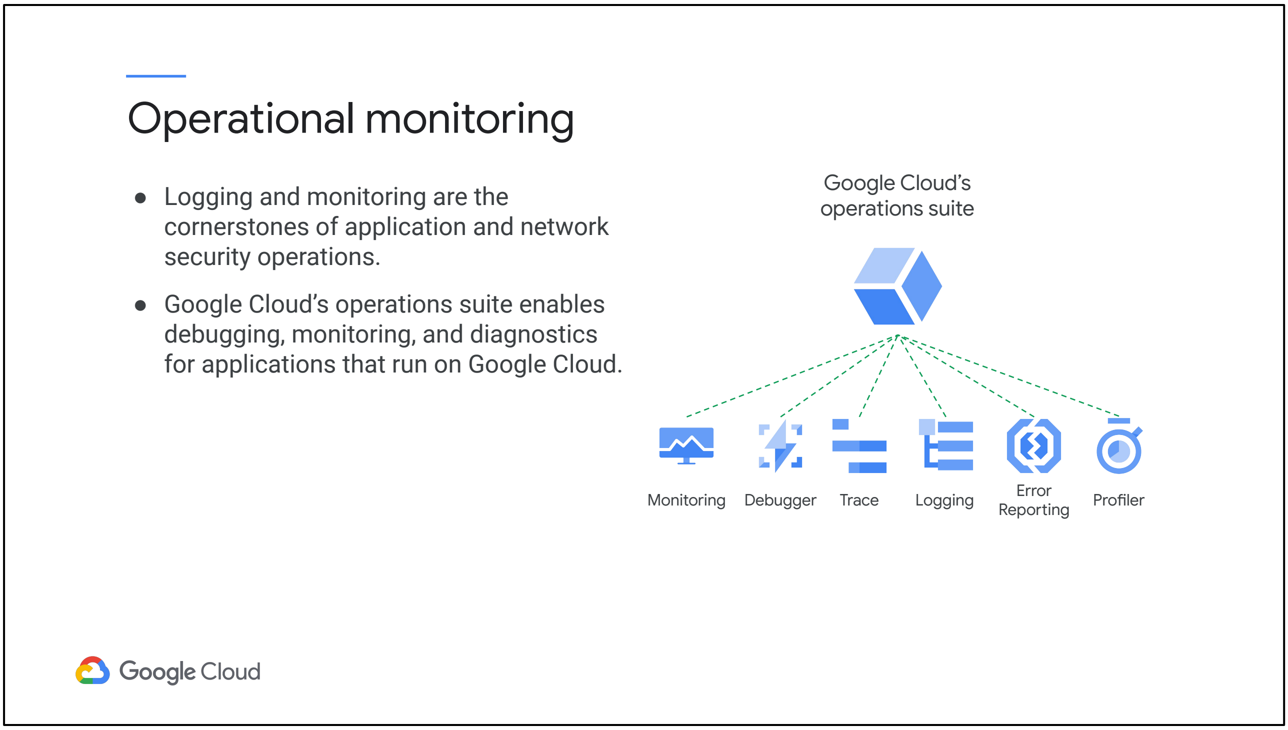
- Define your resources on a logically isolated network.
- Control public internet ingress and egress traffic via firewall rules.

Google Cloud

In addition to the security provided by the Google infrastructure, there are a few Google Cloud specific items that help provide security at the cloud resource level.

Google Virtual Private Cloud or VPC networking provides the ability to logically isolate networks when you define your resources.

You can also control all network ingress and egress traffic to any resource on these networks via firewall rules. These concepts will be discussed in much more detail in a later module.



Operational monitoring

- Logging and monitoring are the cornerstones of application and network security operations.
- Google Cloud's operations suite enables debugging, monitoring, and diagnostics for applications that run on Google Cloud.

Google Cloud's operations suite

Monitoring

Debugger

Trace

Logging

Error Reporting

Profiler

Google Cloud

Logging and monitoring are the cornerstones of application and network security operations.

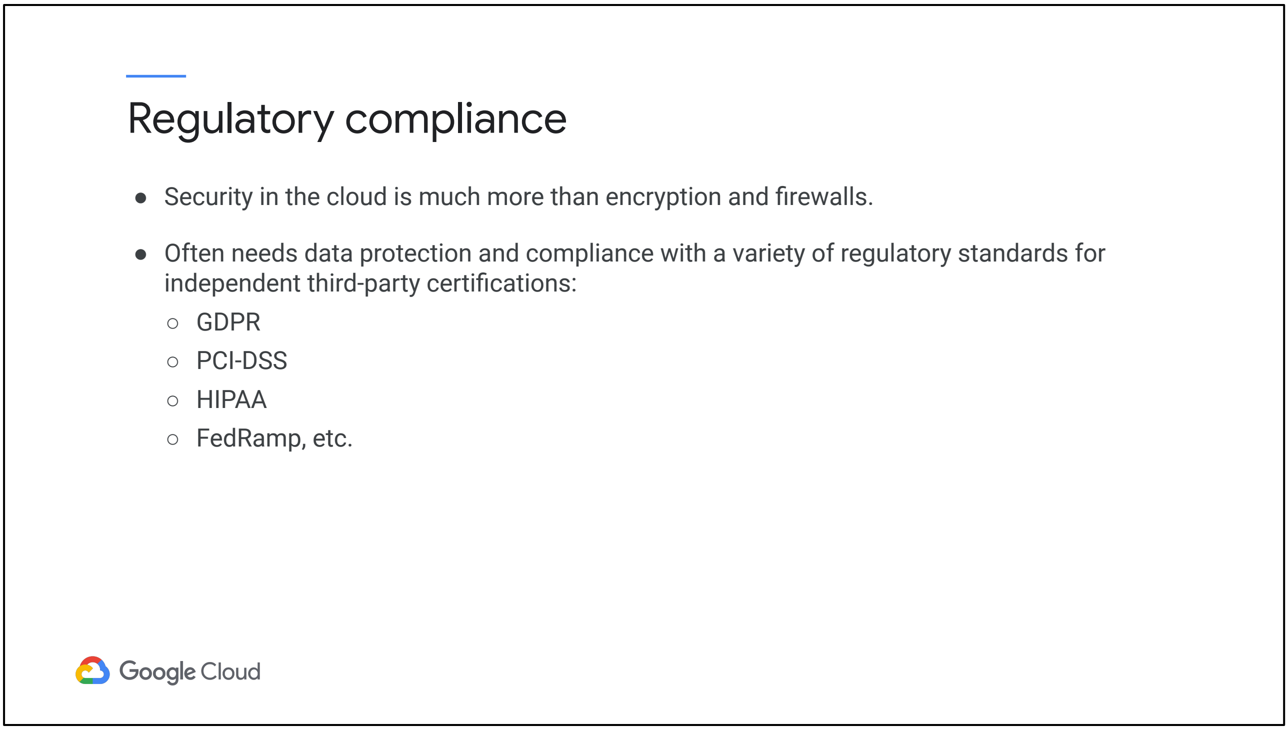
Monitoring and logging enables application analysis, network forensics, access patterns, performance profiling, and more.

Without monitoring it is very difficult to know exactly what is happening or when incidents occur. Monitoring and logging are also needed to help identify security or operational risks to your organization.

Google Cloud's operations suite (formerly Stackdriver) enables debugging, monitoring, and diagnostics for applications and provides a centralized place to manage and analyze operational resources. This helps you increase application reliability when running in the cloud.

Cloud Logging (formerly Stackdriver Logging) allows you to store, search, analyze, monitor, and trigger alerts on log data and events from Google Cloud. Our API also allows ingestion of any custom log data from any other source.

Cloud Logging is a fully managed service that performs at scale and can ingest application and system log data from thousands of VMs. Even better, you can analyze all that log data in real time. Combined with the powerful visualization tools, Cloud Logging helps identify trends and prevent issues before they happen. The error reporting, trace tools and debugger help to quickly locate and fix problems in production systems.



Regulatory compliance

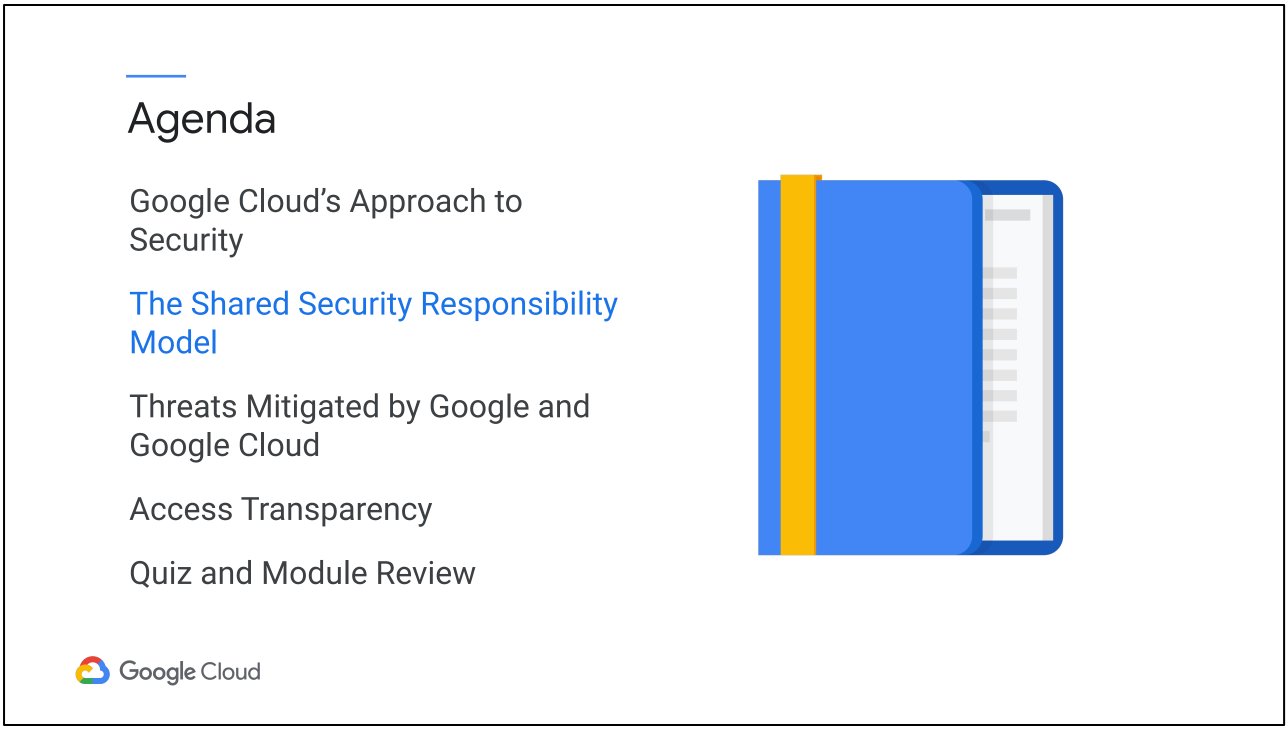
- Security in the cloud is much more than encryption and firewalls.
- Often needs data protection and compliance with a variety of regulatory standards for independent third-party certifications:
  - GDPR
  - PCI-DSS
  - HIPAA
  - FedRamp, etc.

Google Cloud

Another facet of security today is the need to ensure regulatory compliance, which involves much more than just making use of encryption and firewalls - you also need data protection and compliance with a variety of regulatory standards. Our products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn your trust. We are constantly working to expand our coverage.

Visit the Standards, Regulations and Certifications page listed in the Resources for this module for more information on the certifications Google currently supports.

As you have seen, Google Cloud provides many security controls automatically. When implementing systems correctly on Google Cloud, leveraging these aspects can reduce the IT Security resources required, and help drastically reduce the total cost of ownership.



Agenda

Google Cloud's Approach to Security

The Shared Security Responsibility Model

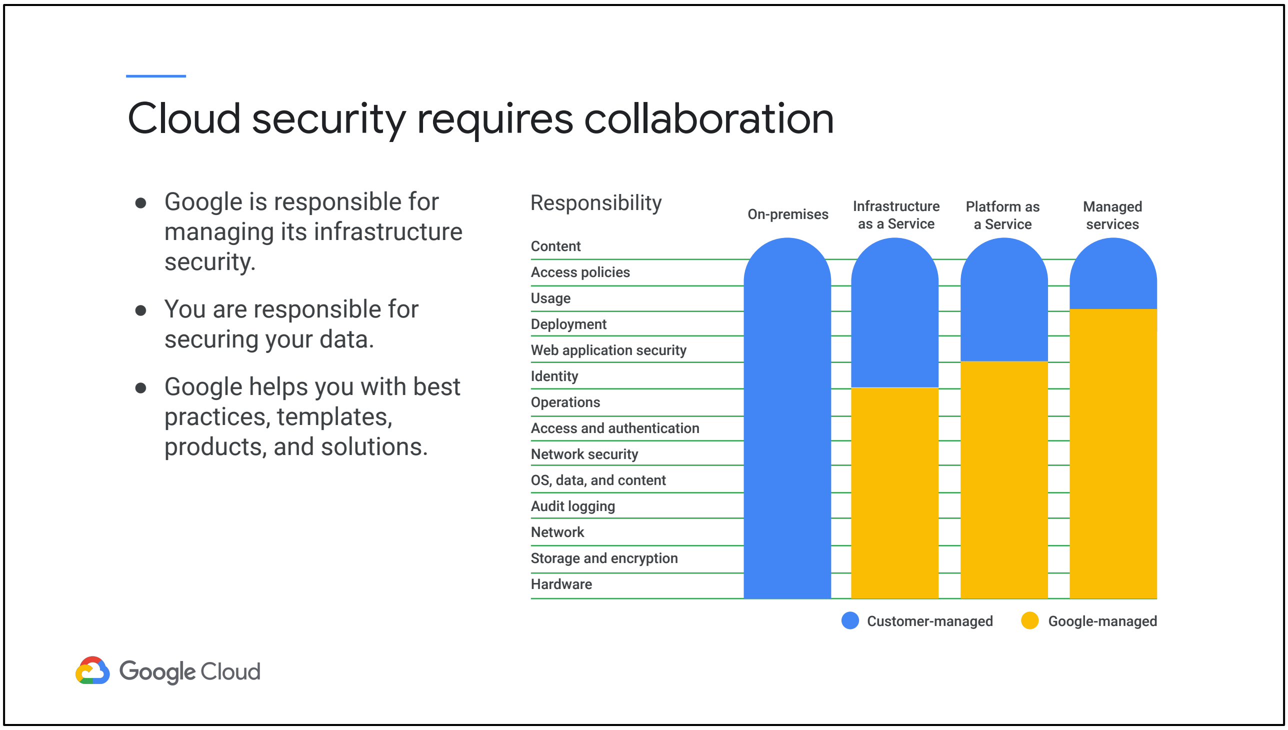
Threats Mitigated by Google and Google Cloud

Access Transparency

Quiz and Module Review

Google Cloud

Security on Google Cloud is a shared responsibility between Google and the customer. Depending on the service being used, the division of responsibilities will vary. You will learn more about that in this lesson.



Cloud security requires collaboration

- Google is responsible for managing its infrastructure security.
- You are responsible for securing your data.
- Google helps you with best practices, templates, products, and solutions.

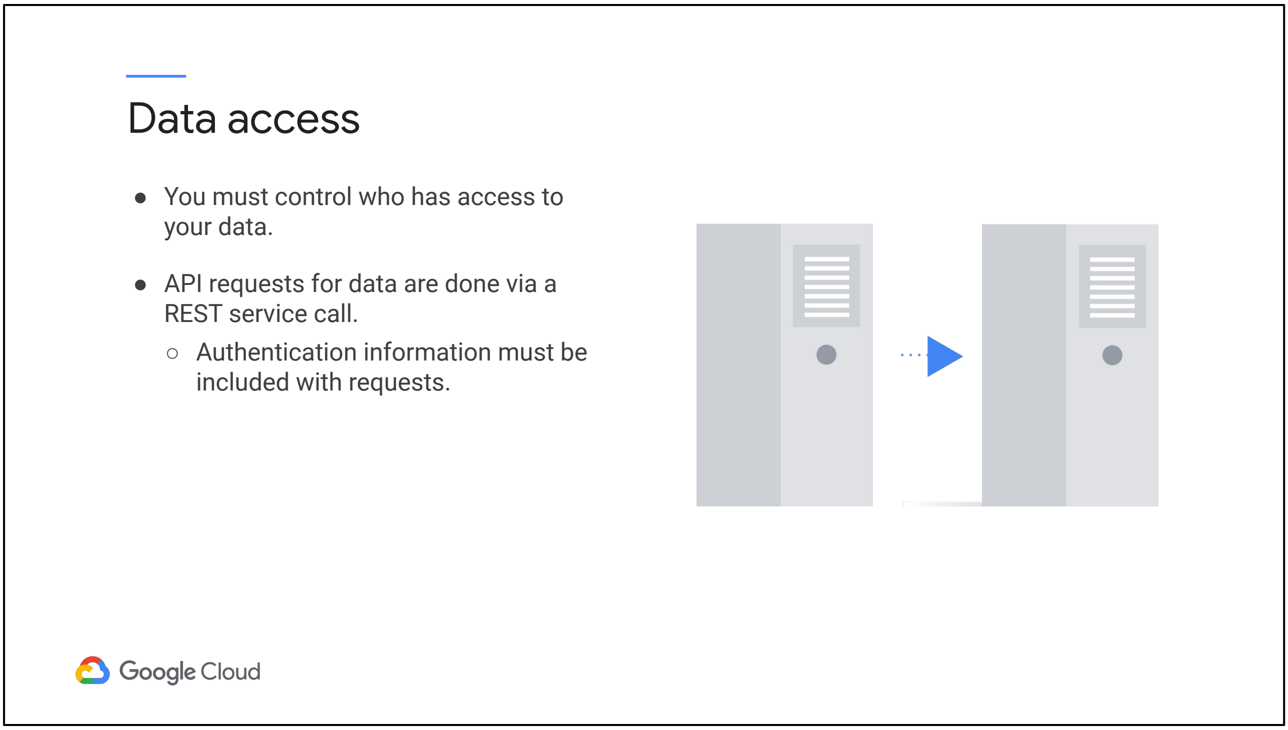
Google Cloud

When you build an application with on-premise infrastructure, you're responsible for:

- The physical security of the hardware and the premises in which it is housed
- The encryption of the data on disk
- The integrity of your network, and
- The security of the content stored in your applications

When you move an application to Google Cloud, Google handles many of the lower layers of the overall security stack. Because of its scale, Google can deliver a higher level of security at these layers than most of its customers could afford to do on their own.

The upper layers of the security stack remain the customer's responsibility. Google provides tools, such as Identity and Access Management (IAM) to help customers implement the policies they choose at these layers.



Data access

- You must control who has access to your data.
- API requests for data are done via a REST service call.
  - Authentication information must be included with requests.

One aspect of security which is almost always the responsibility of the customer is data access. This simply means you are the one who controls who has access to your data.

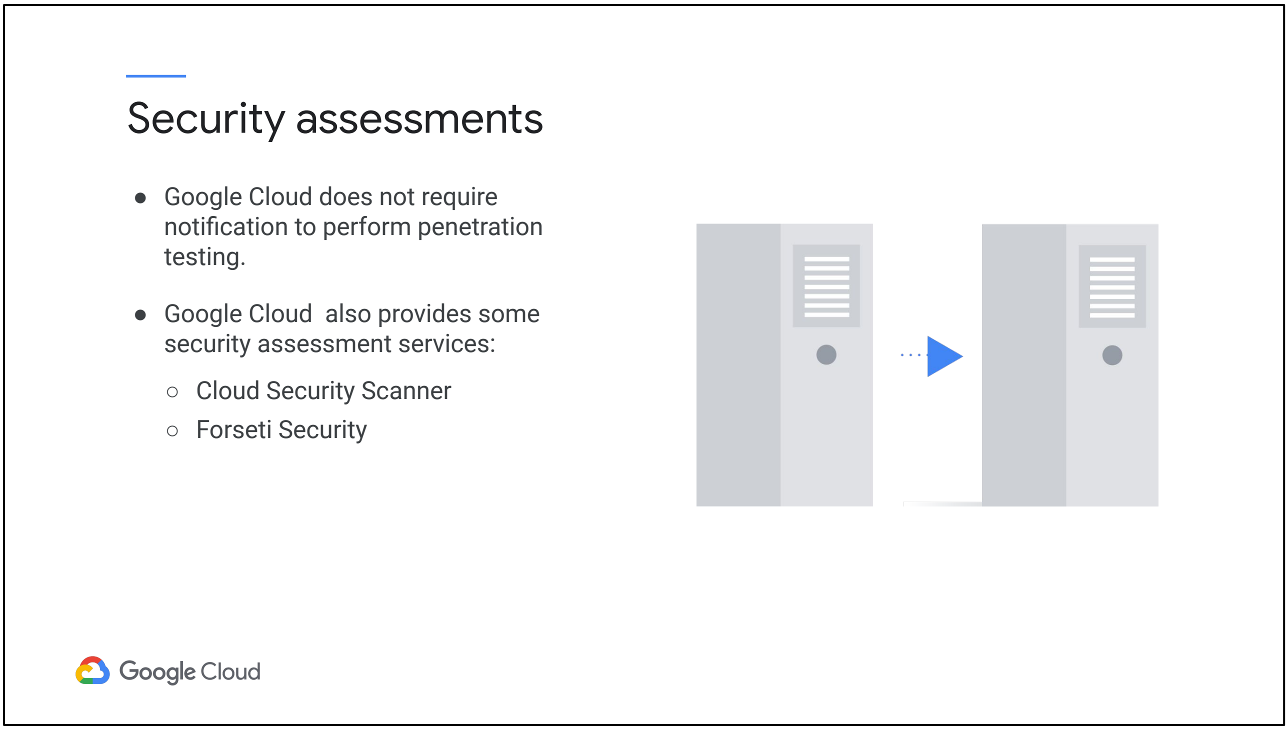
Google Cloud provides mechanisms to help implement these access controls including:

- Cloud Identity and Access Management
- Access Control Lists, and
- Firewall rules

However, in order to protect your data, these must be properly configured. We will discuss this in more depth later in the course.

When calling a Google API to retrieve data, API requests are done via a REST service call. Authentication information must be included with requests.

It is very common for legal or regulatory requirements to require a vulnerability assessment or penetration test against your cloud resources. For example, PCI-DSS security requirements will require this to be done.



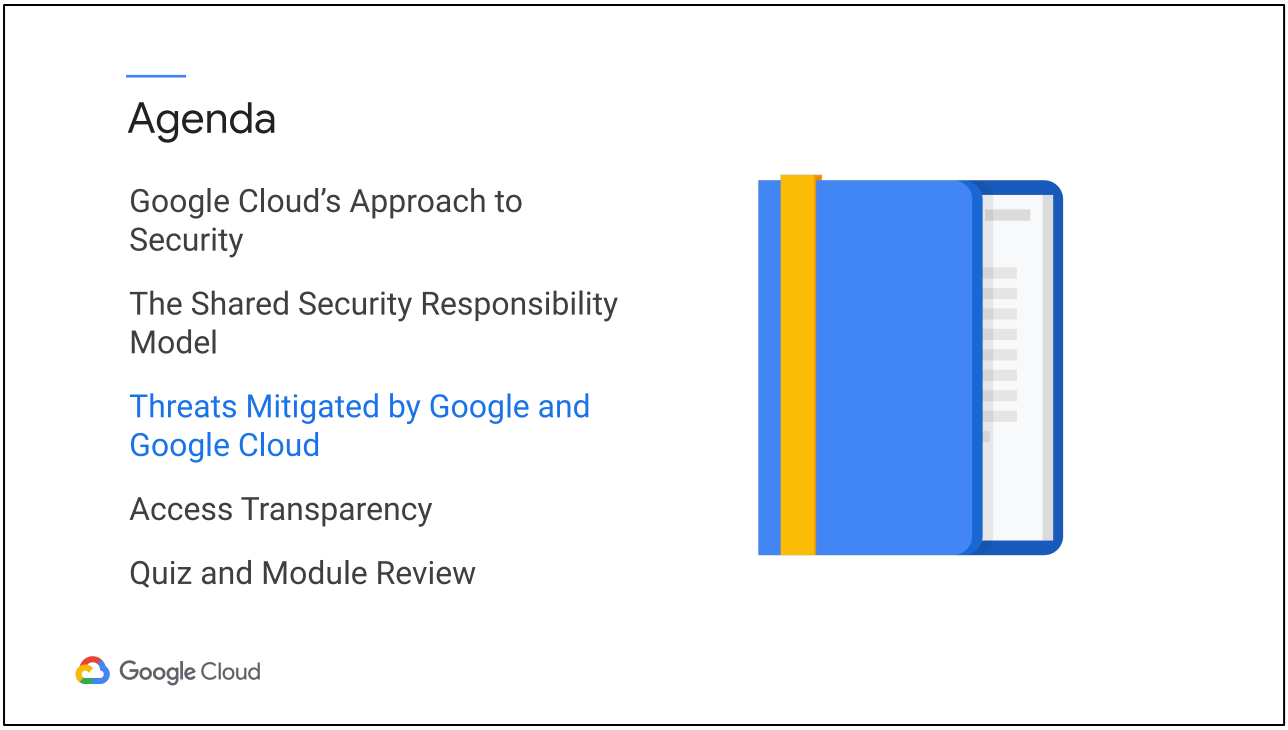
Security assessments

- Google Cloud does not require notification to perform penetration testing.
- Google Cloud also provides some security assessment services:
  - Cloud Security Scanner
  - Forseti Security

Google Cloud

Google Cloud does not require prior notification to perform penetration testing, but please note that you must abide by the Google Cloud Acceptable Use Policy and the Terms of Service when conducting your testing.

Google Cloud also provides some security assessment services to help perform these assessments: Cloud Security Scanner and Forseti Security. We will be investigating these services in more depth later in the course.



Agenda

Google Cloud's Approach to Security

The Shared Security Responsibility Model

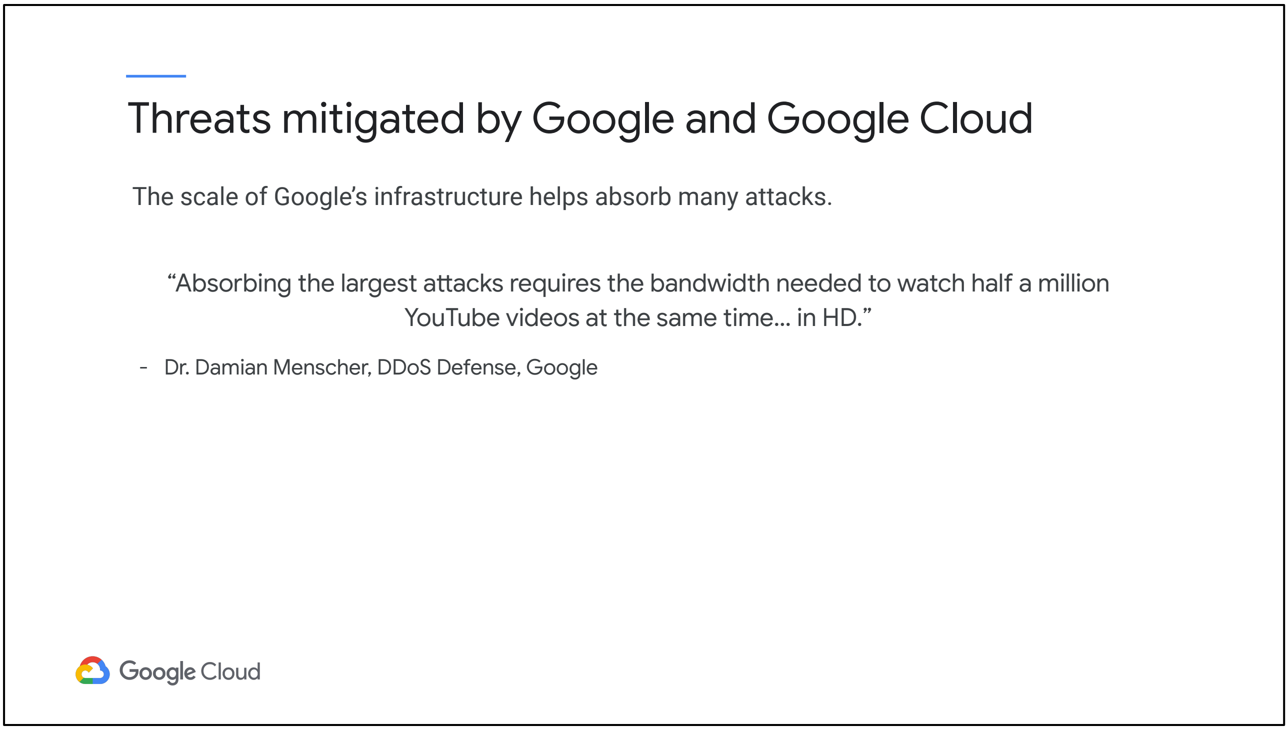
Threats Mitigated by Google and Google Cloud

Access Transparency

Quiz and Module Review

Google Cloud

Deploying systems on Google Cloud offers many benefits derived from the security of Google's underlying infrastructure. This means many of the threats your systems and applications face are automatically mitigated simply by using Google's infrastructure.



Threats mitigated by Google and Google Cloud

The scale of Google's infrastructure helps absorb many attacks.

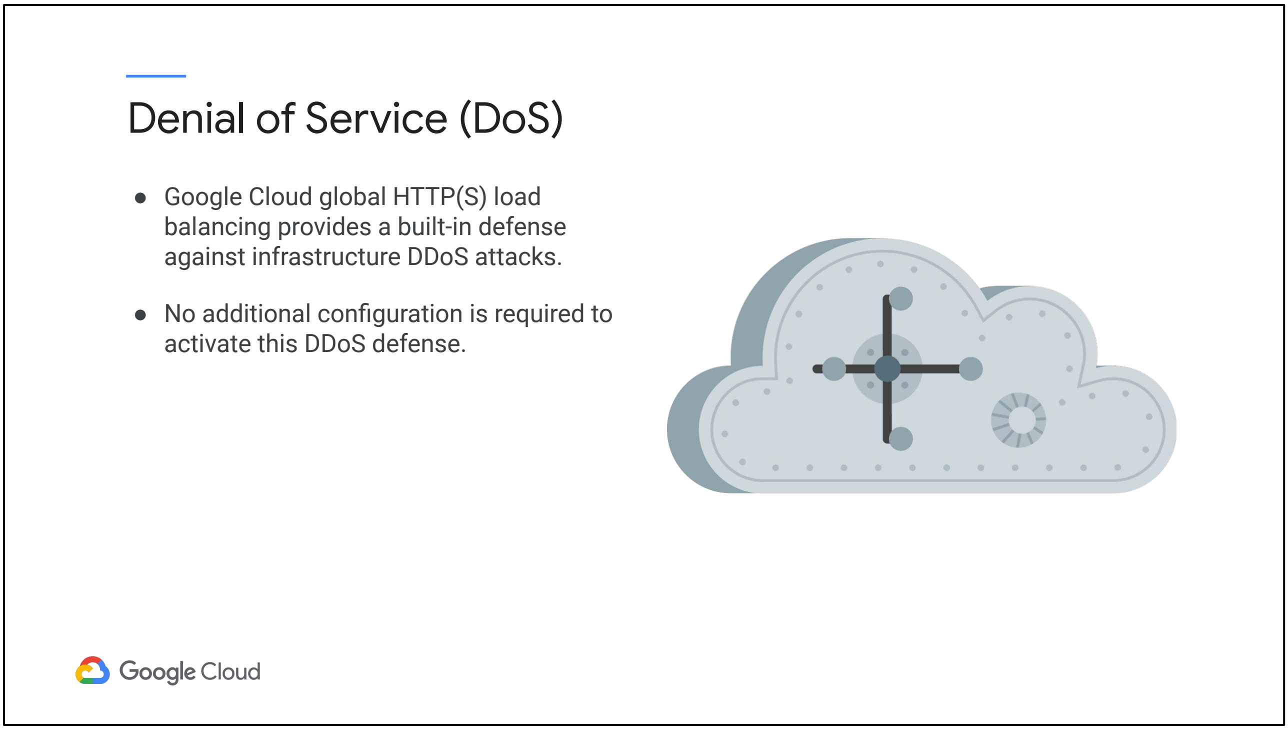
> "Absorbing the largest attacks requires the bandwidth needed to watch half a million YouTube videos at the same time... in HD."

- Dr. Damian Menscher, DDoS Defense, Google

Google Cloud

Protecting from large internet attacks can be very difficult and require a huge amount of resources. According to Dr. Damian Menscher, "Absorbing the largest attacks requires the bandwidth needed to watch half a million YouTube videos at the same time... in HD."

As a Google cloud customer, you are protected by default from many kinds of attack because the scale of our infrastructure enables us to simply absorb them.

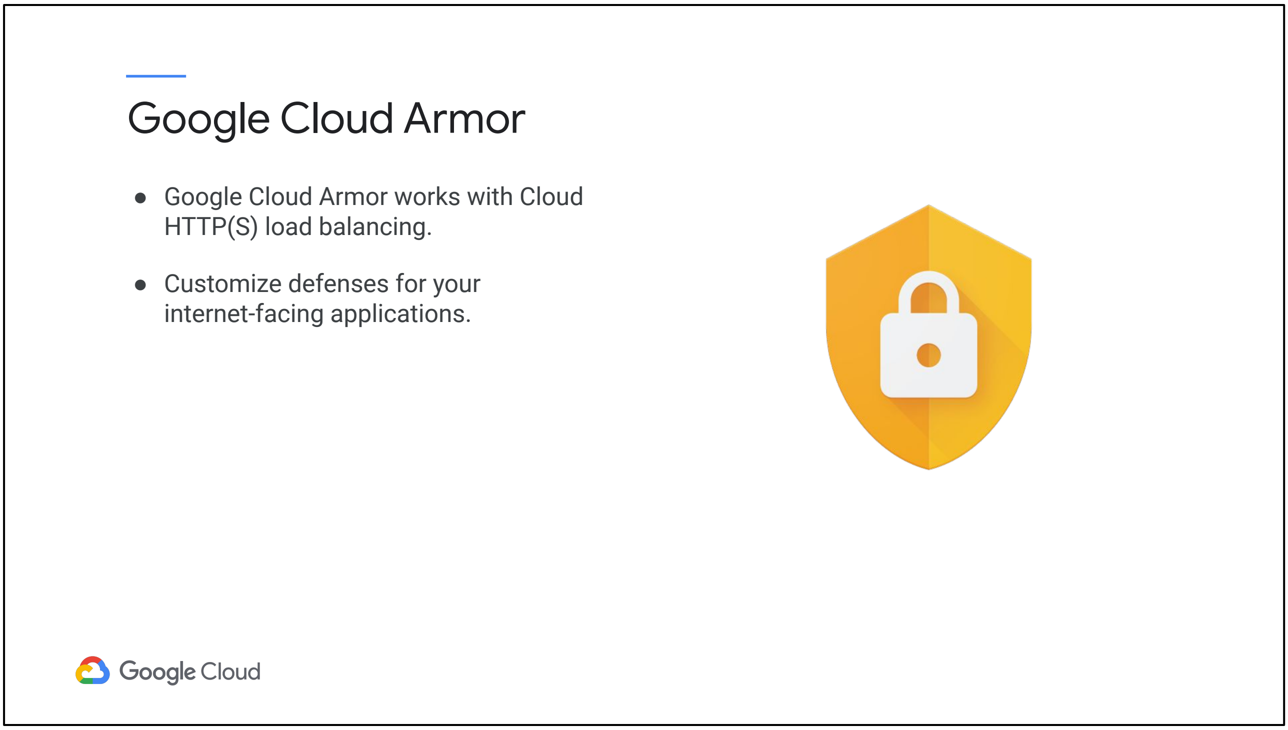


Denial of Service (DoS)

- Google Cloud global HTTP(S) load balancing provides a built-in defense against infrastructure DDoS attacks.
- No additional configuration is required to activate this DDoS defense.

Google Cloud

When there is a DoS attack, there is time to isolate it and address it - but Google doesn't stop there. In Google Cloud, customers also benefit directly from our central DoS mitigation service that provides additional multi-tier, multi-layer protection. Our DoS mitigation service further reduces the risk to services running behind our Google front end by detecting when an attack is taking place and configuring load balancers to drop or throttle traffic associated with the attack. The best news is there is no additional configuration required to activate this DoS defense, when you use Google Cloud Load Balancers to manage your resources!

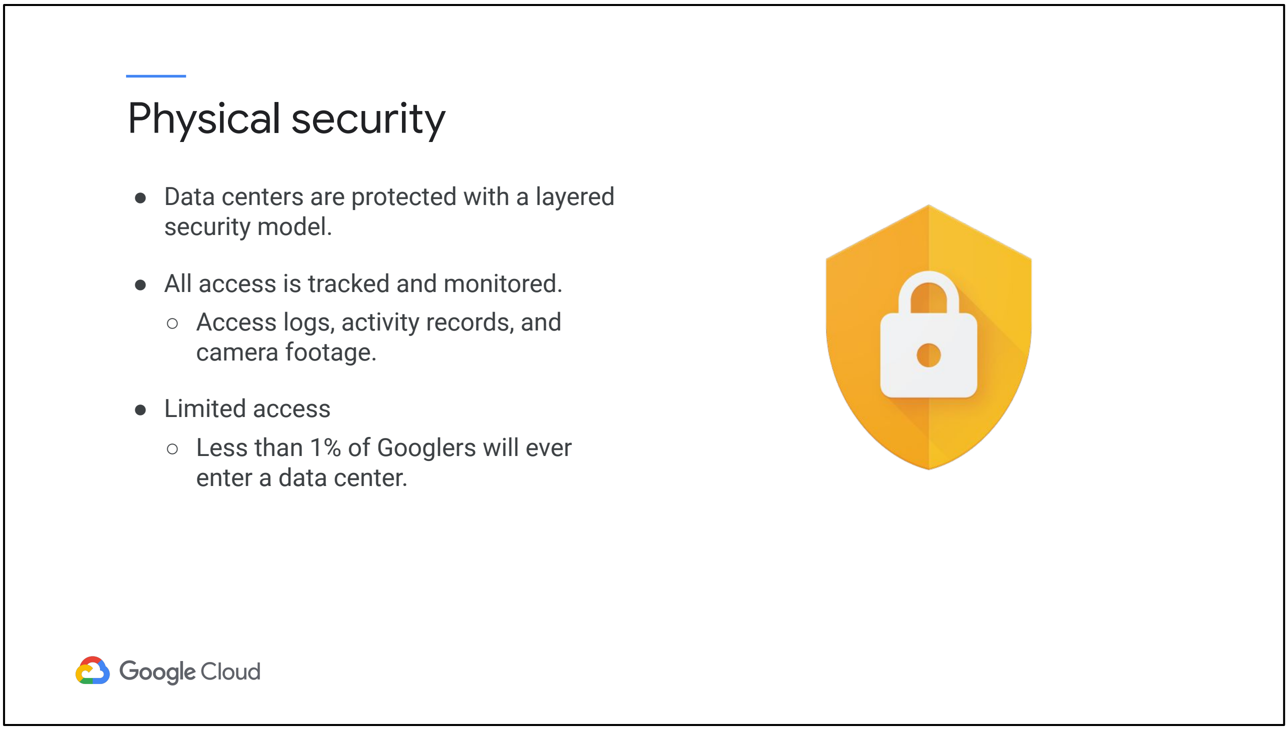


Google Cloud Armor

- Google Cloud Armor works with Cloud HTTP(S) load balancing.
- Customize defenses for your internet-facing applications.

Google Cloud

For additional features, such as IPv4 and IPv6 allowlisting or blocklisting and defense against application-aware attacks such as cross-site scripting and SQL injection, Google Cloud offers Google Cloud Armor. Google Cloud Armor works in conjunction with global HTTP/HTTPS load balancing and enables you to deploy and customize defenses for your internet-facing applications. It’s based on the same technologies and global infrastructure that we use to protect Google services like Search, Gmail and YouTube.



Physical security

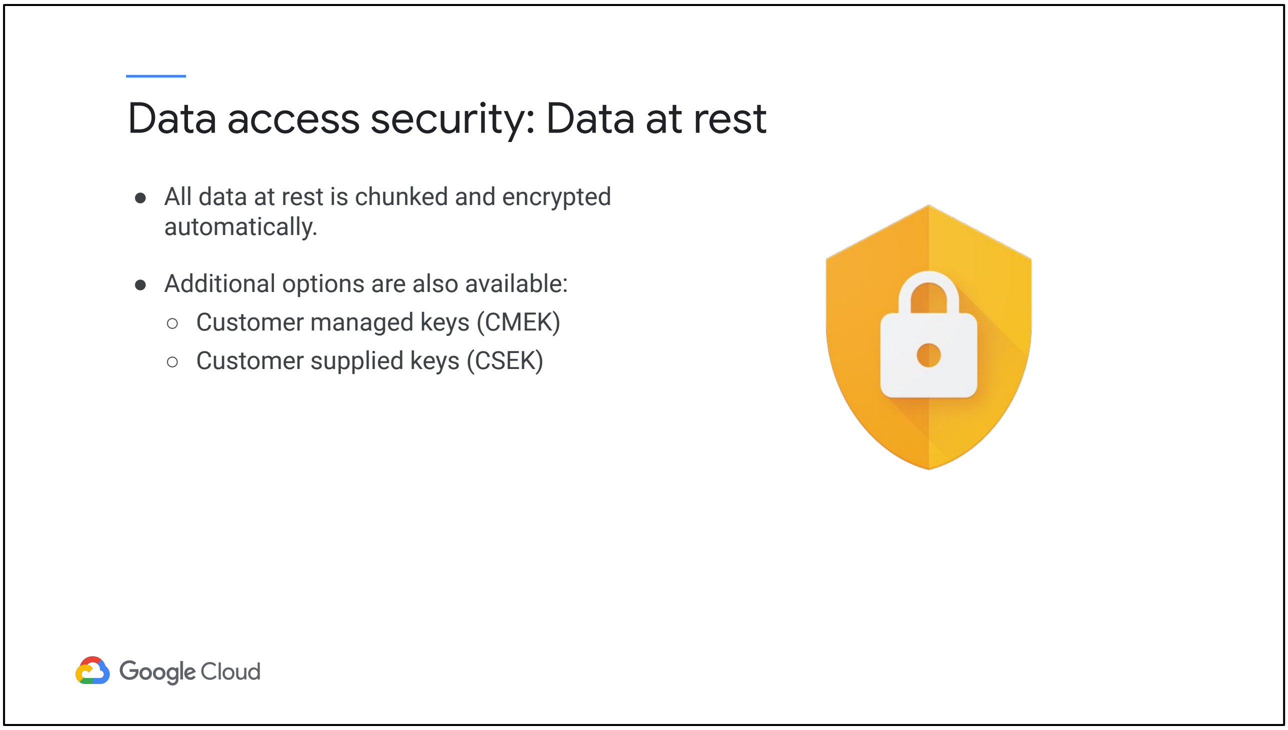
- Data centers are protected with a layered security model.
- All access is tracked and monitored.
  - Access logs, activity records, and camera footage.
- Limited access
  - Less than 1% of Googlers will ever enter a data center.

Google Cloud

Google's data centers leverage a layered security model and are protected with some of the most advanced physical security controls available today. Some of the controls implemented are:

- Custom designed electronic access cards, biometrics and metal detectors
- Vehicle access barriers
- Perimeter fencing and security patrols
- Laser beam intrusion detection on data center floors
- Interior and exterior cameras to detect and track intruders

Additionally all access is tracked and monitored and limited to only those with a direct need to have access. Less than 1% of Googlers will ever set foot in a data center.



Data access security: Data at rest

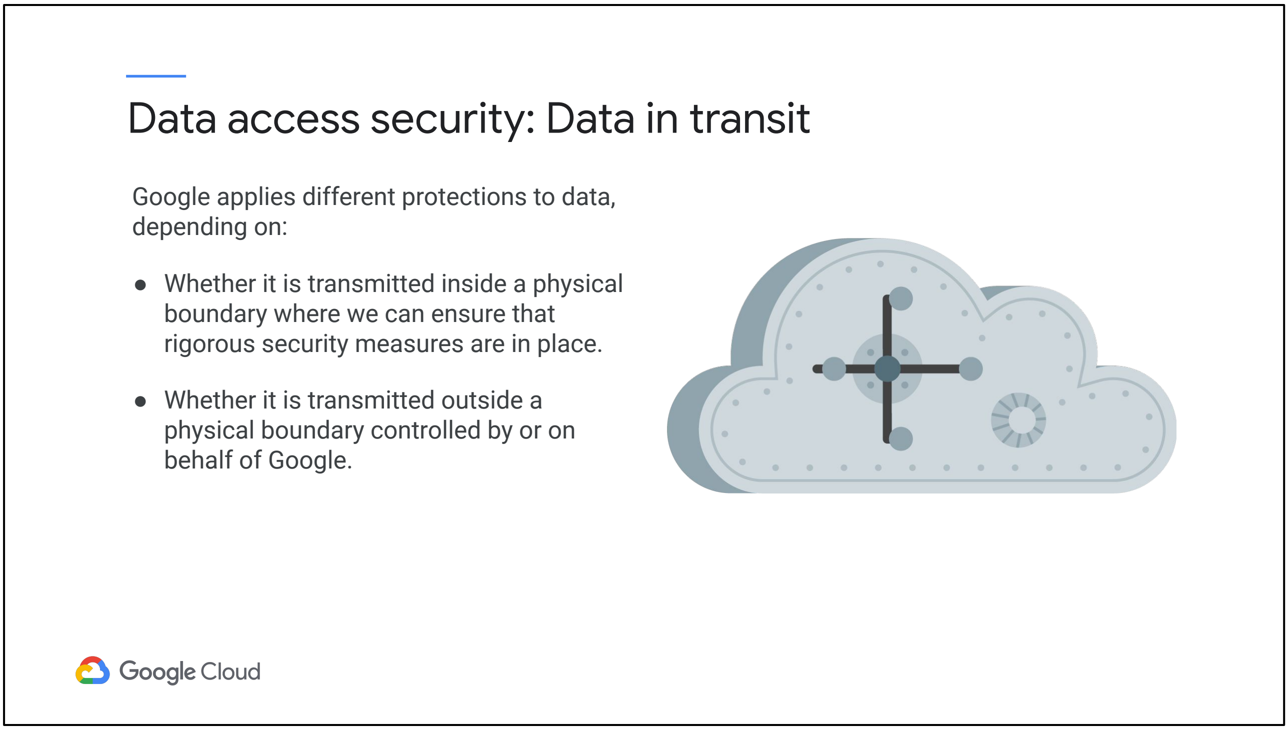
- All data at rest is chunked and encrypted automatically.
- Additional options are also available:
  - Customer managed keys (CMEK)
  - Customer supplied keys (CSEK)

Google Cloud

All data stored at rest in Google Cloud is chunked and encrypted automatically.

All data stored at rest in Google Cloud is automatically split into chunks, and each chunk is encrypted with a unique data encryption key. These data encryption keys are then encrypted with (or sometimes called "wrapped" by) key encryption keys to provide another level of protection. There is nothing for the customer to configure for this to happen.

Additional options are also available that allow for Customer managed keys and Customer supplied keys. These can sometimes be required by legal, regulatory, or organizational requirements. The details of these options will be discussed in further detail later in this course.



Data access security: Data in transit

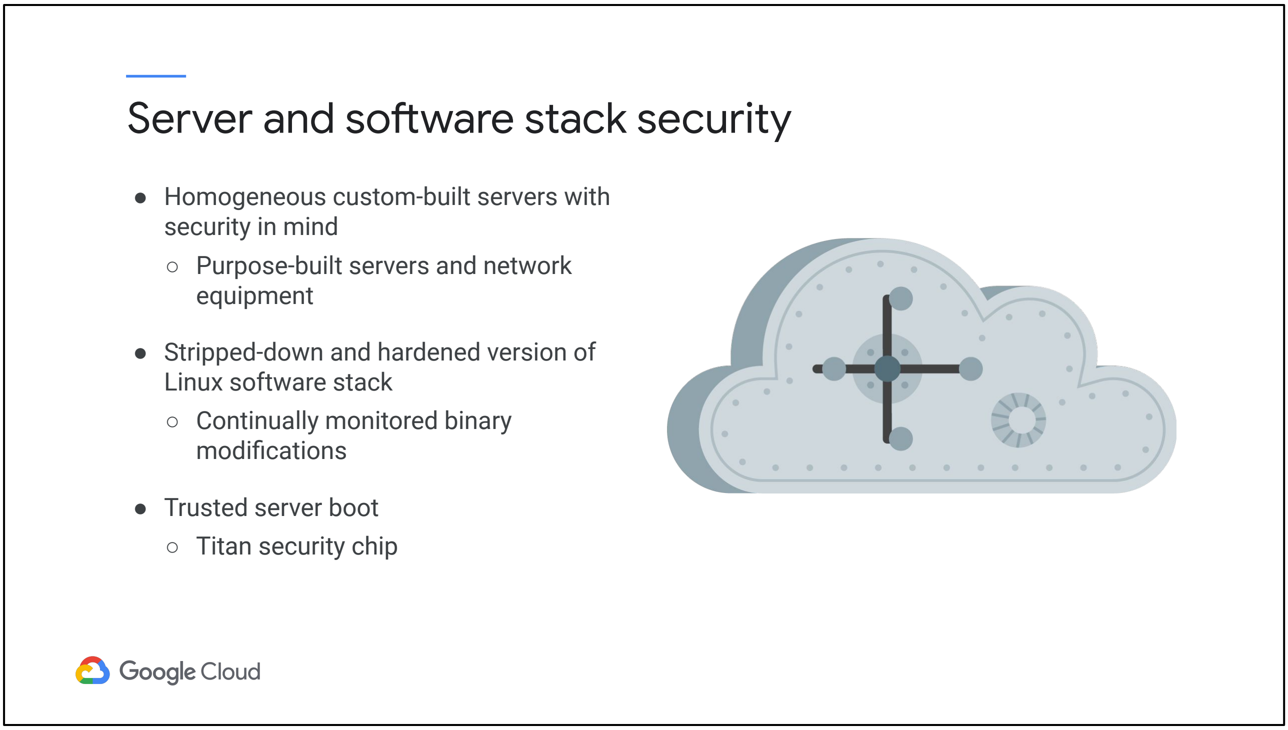
Google applies different protections to data, depending on:

- Whether it is transmitted inside a physical boundary where we can ensure that rigorous security measures are in place.
- Whether it is transmitted outside a physical boundary controlled by or on behalf of Google.

Google applies different protections to data in transit, depending on whether that data is transmitted inside a physical boundary where we can ensure that rigorous security measures are in place, or whether it is transmitted outside a physical boundary controlled by or on behalf of Google.

Data in transit within our physical boundaries is generally authenticated, but may not be encrypted by default. You can choose which additional security measures to apply based on your threat model.

All data is automatically encrypted and authenticated when transmitted outside a physical boundary controlled by or on behalf of Google.



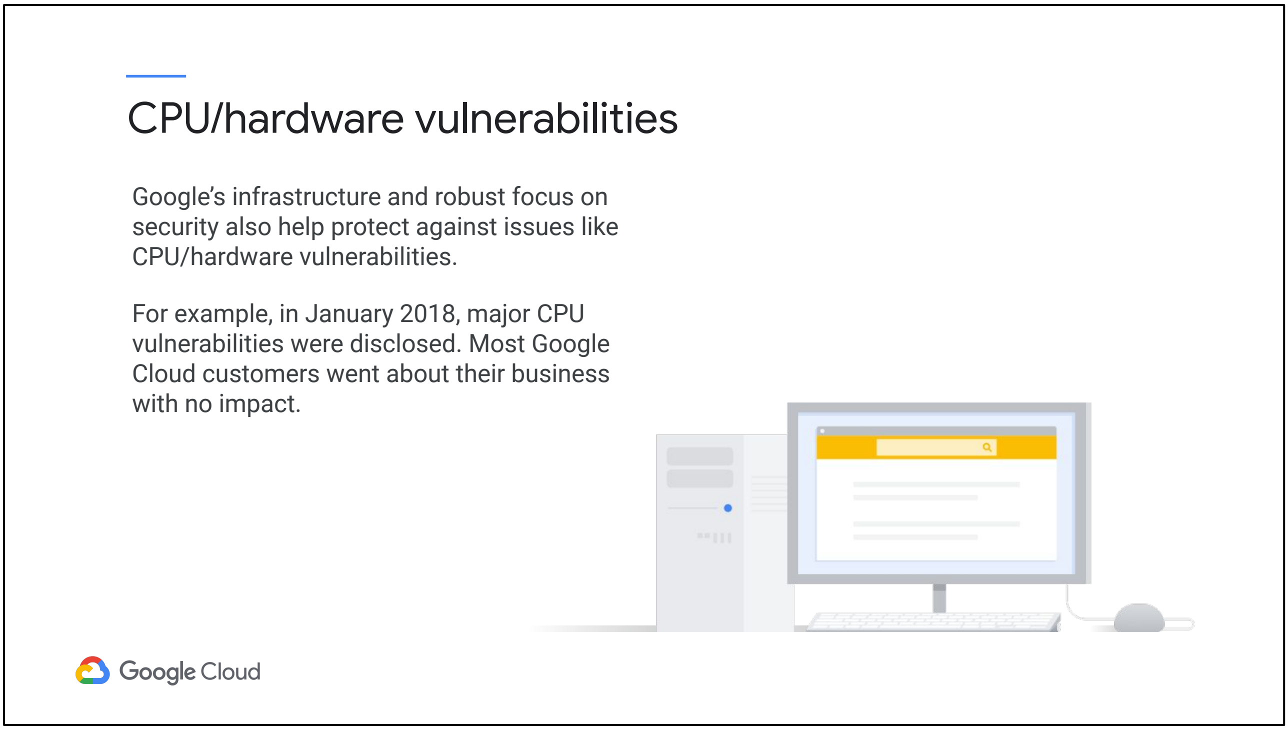
Server and software stack security

- Homogeneous custom-built servers with security in mind
  - Purpose-built servers and network equipment
- Stripped-down and hardened version of Linux software stack
  - Continually monitored binary modifications
- Trusted server boot
  - Titan security chip

Google leverages all purpose-built servers and network equipment to help reduces the security footprint.

All servers running in Google Cloud are homogeneous custom-built servers designed with security in mind. Google servers don’t include unnecessary components such as video cards, chipsets, or peripheral connectors, and leverage the Titan security chip mentioned earlier for trusted server boot process.

All Linux stacks are stripped-down and hardened versions and are continually monitored for binary modifications.



CPU/hardware vulnerabilities

Google's infrastructure and robust focus on security also help protect against issues like CPU/hardware vulnerabilities.

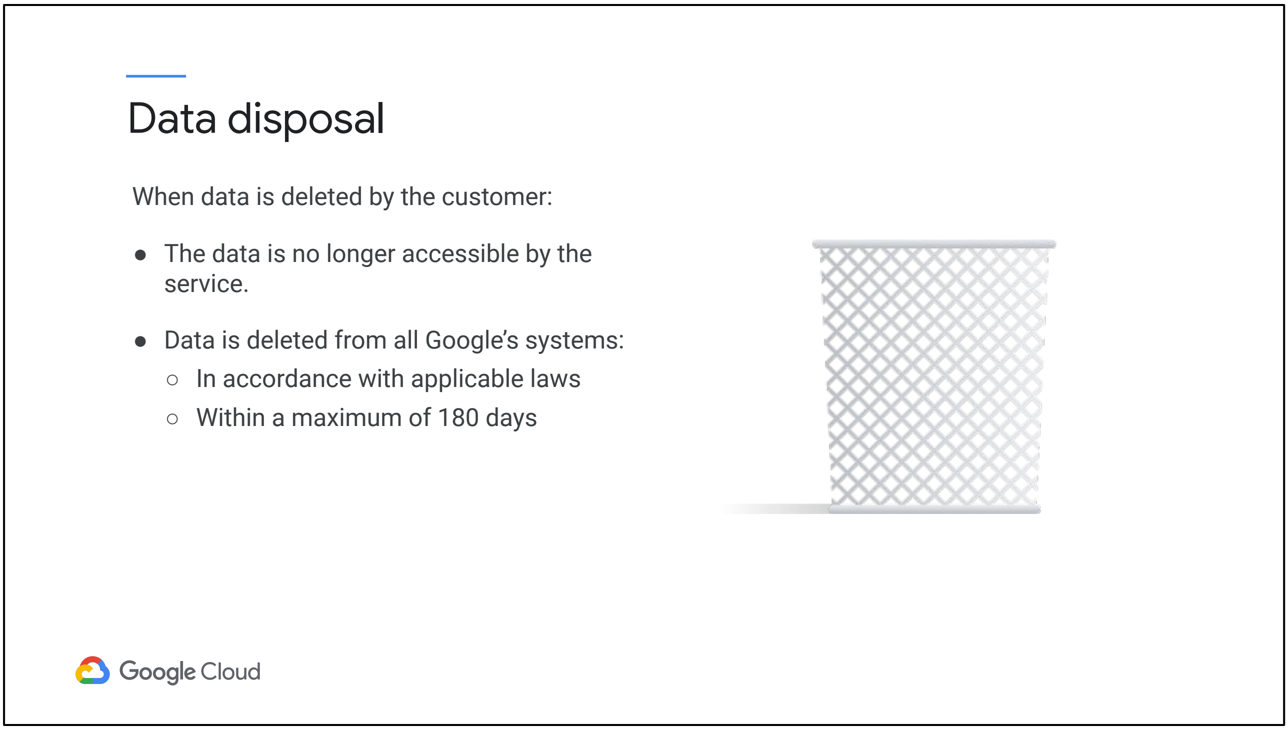
For example, in January 2018, major CPU vulnerabilities were disclosed. Most Google Cloud customers went about their business with no impact.

Google Cloud

Google's infrastructure and robust focus on security also helps protect against things like CPU/hardware vulnerabilities.

For example, consider the CPU vulnerabilities that were disclosed in January 2018. These were major discoveries; in fact, they rocked the tech industry. Despite that, for the most part, Google Cloud customers could go about their business, as usual.

In fact, we got calls from customers asking if we had updated our systems to protect against the vulnerabilities, because they experienced no impact!



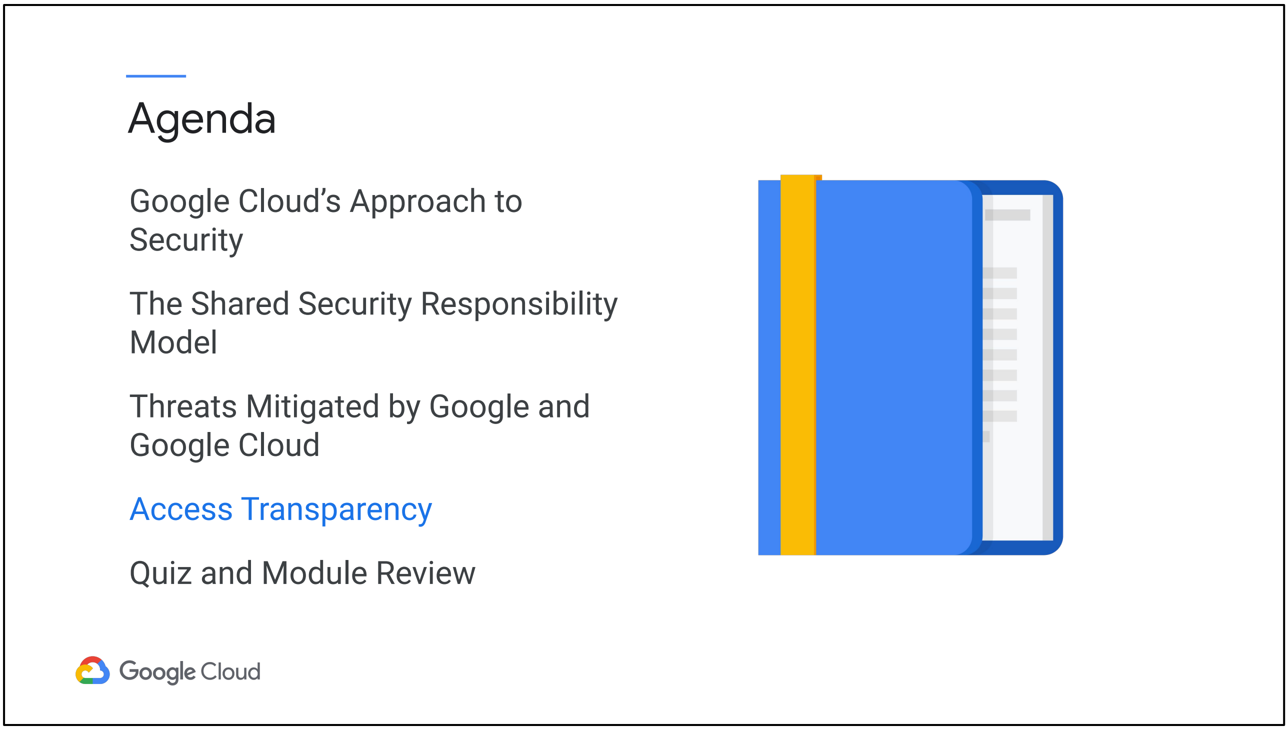
Data disposal

When data is deleted by the customer:

- The data is no longer accessible by the service.
- Data is deleted from all Google's systems:
  - In accordance with applicable laws
  - Within a maximum of 180 days

When data is deleted by the customer, that data becomes inaccessible by the Google Cloud service and cannot be recovered by the customer. The data may still remain on physical storage devices for a period of time.

All relevant data will be then be deleted from all Google's systems and devices in accordance with applicable laws. This deletion will occur as soon as reasonably possible and within a maximum period of 180 days.



Agenda

Google Cloud’s Approach to Security

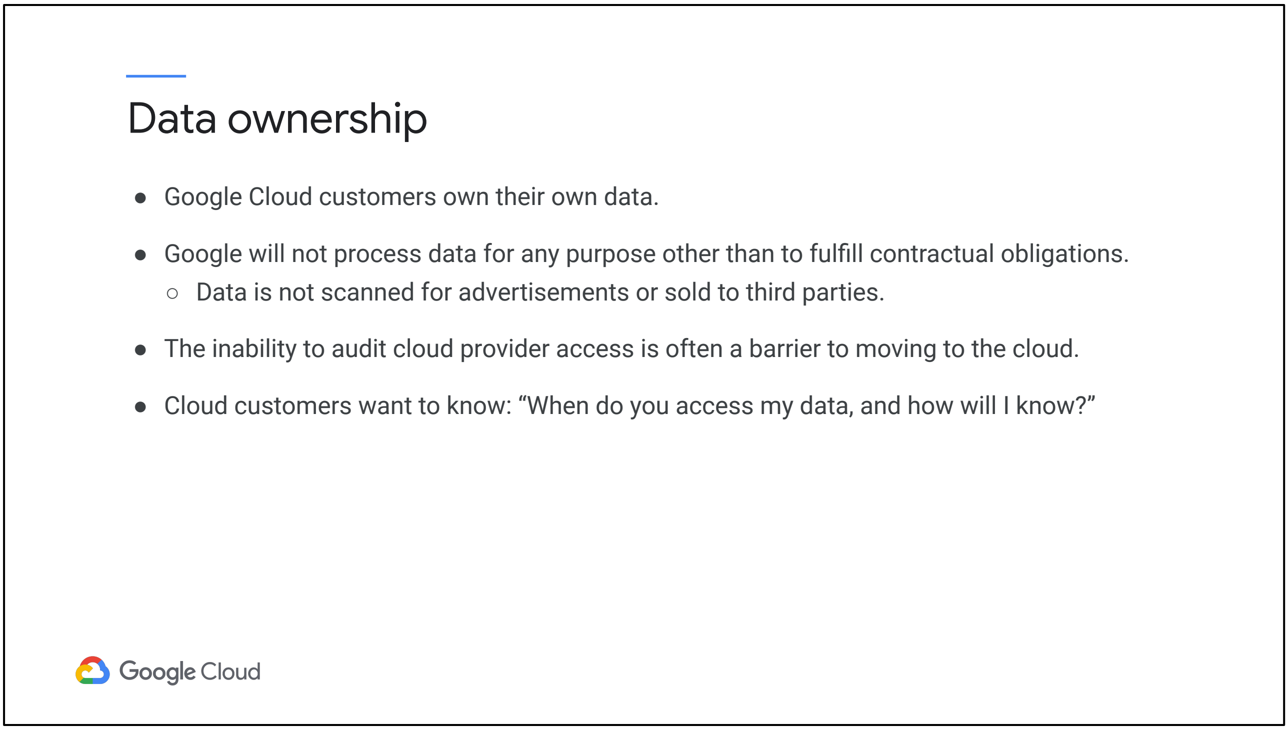
The Shared Security Responsibility Model

Threats Mitigated by Google and Google Cloud

Access Transparency

Quiz and Module Review

When moving systems to the cloud, a common concern is access transparency and knowing exactly what is happening to your data. At Google, we try to expand your visibility into how your data is handled when in the cloud.



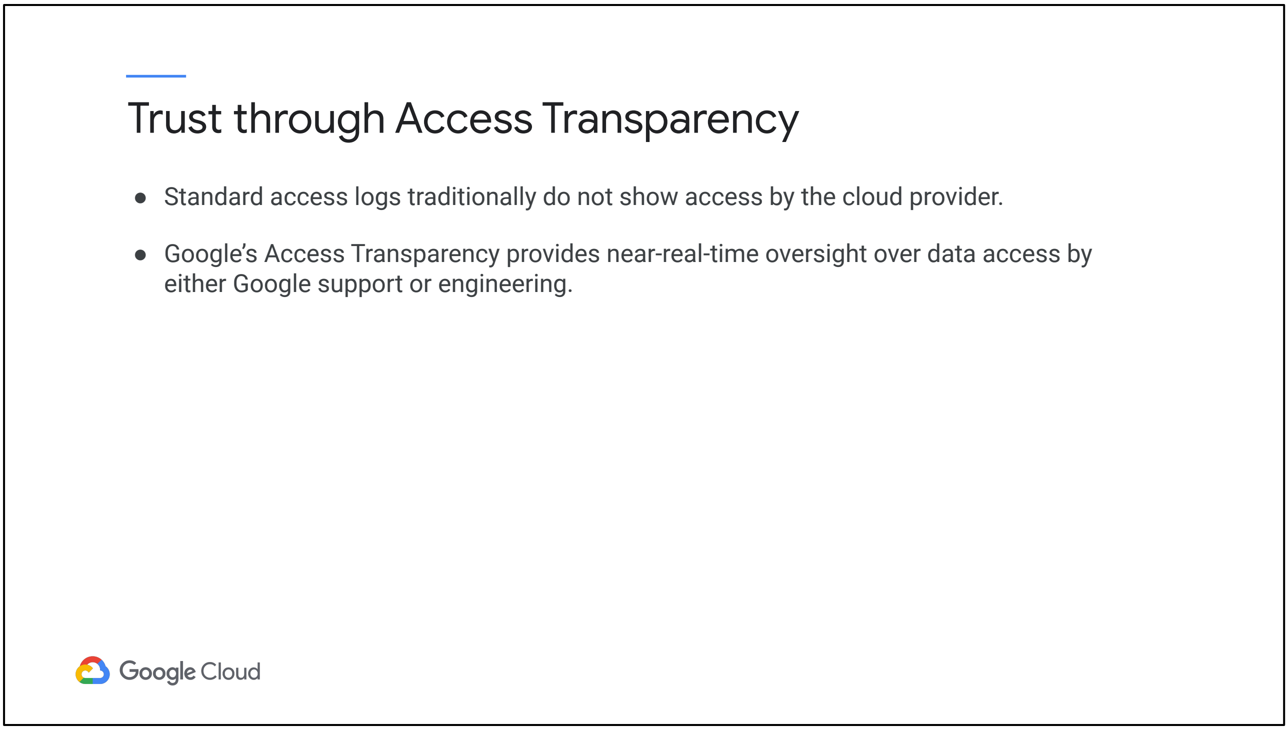
Data ownership

- Google Cloud customers own their own data.
- Google will not process data for any purpose other than to fulfill contractual obligations.
  - Data is not scanned for advertisements or sold to third parties.
- The inability to audit cloud provider access is often a barrier to moving to the cloud.
- Cloud customers want to know: “When do you access my data, and how will I know?”

Google Cloud

Google Cloud customers own their data, not Google. The data that customers put into our systems is theirs, and we do not scan it for advertisements nor do we sell it to third parties.

We offer our customers a detailed data processing amendment that describes our commitment to protecting customer data. It states that Google will not process data for any purpose other than to fulfill our contractual obligations.

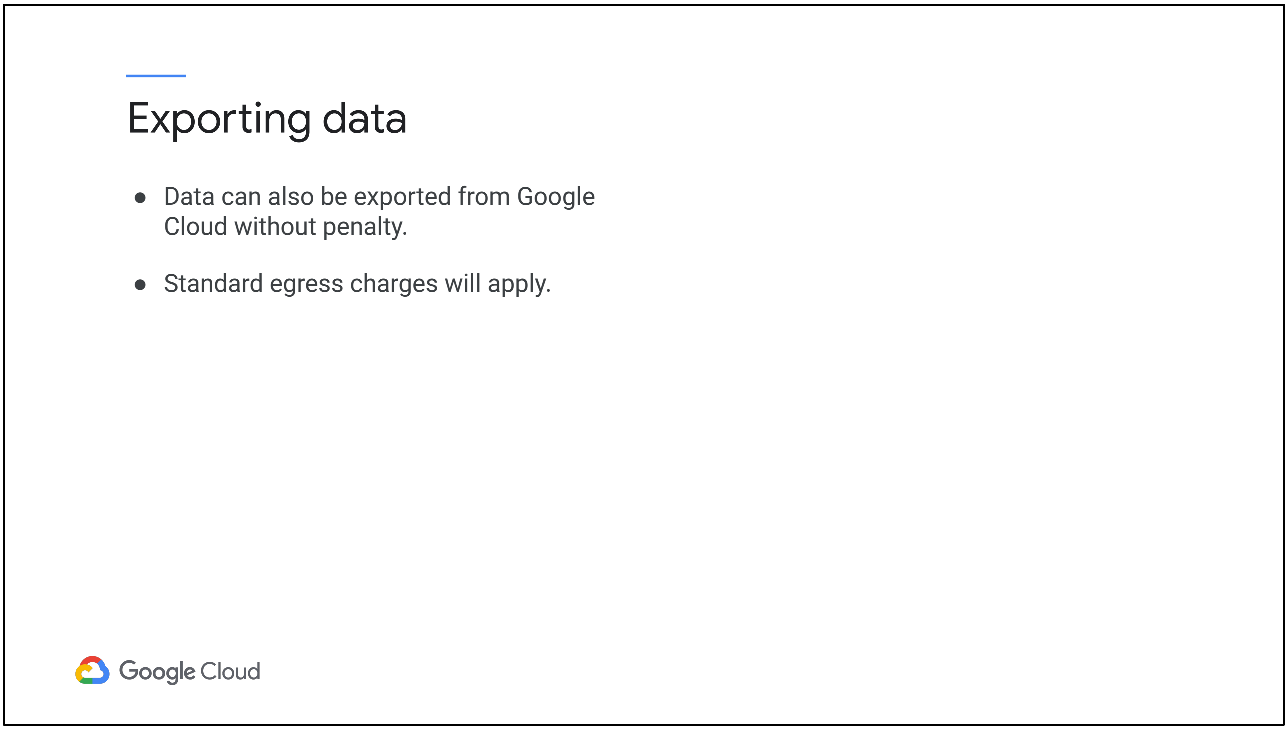


Trust through Access Transparency

- Standard access logs traditionally do not show access by the cloud provider.
- Google's Access Transparency provides near-real-time oversight over data access by either Google support or engineering.

Standard access logs traditional do not show access by the cloud provider. In Google Cloud, Cloud Audit Logs provide visibility into the actions of your own administrators. However, this audit trail typically stops once your cloud provider's support or engineering team is engaged. For example, if you opened a ticket with Google Support that would require data access, that access would not have been reflected in an audit log.

Google's Access Transparency product provides near-real-time oversight over data accesses by either Google support or engineering. But rest assured, at Google Cloud, we do not access customer data for any reason other than those necessary to fulfill our contractual obligations to you. Google also performs regular audits of access by administrators as a check on the effectiveness of our controls.

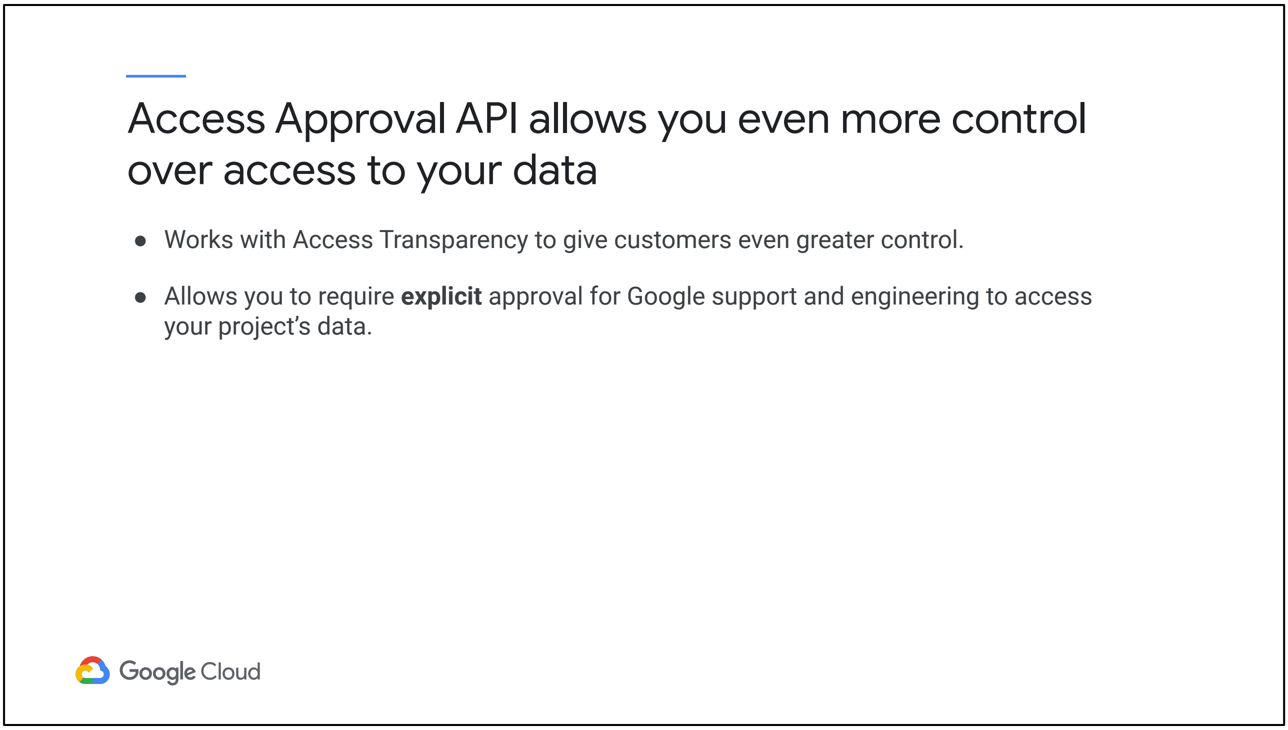


Exporting data

- Data can also be exported from Google Cloud without penalty.
- Standard egress charges will apply.

Google Cloud

What if you want to stop using Google Cloud? The ability to export data from the cloud can be a security concern. Data can be exported from Google Cloud without penalty, but you will need to pay the standard egress charges. This makes it easy for our customers to take their data with them if they choose to stop using Google Cloud.

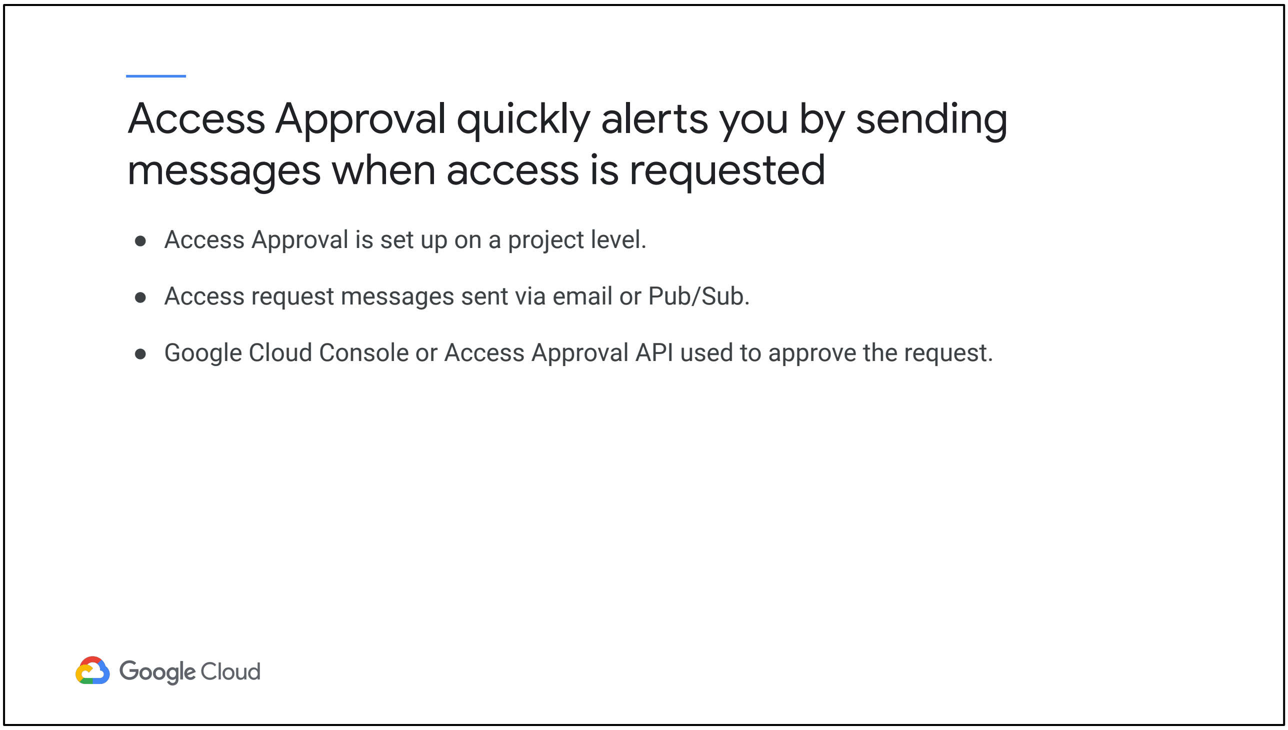


Access Approval API allows you even more control over access to your data

- Works with Access Transparency to give customers even greater control.
- Allows you to require **explicit** approval for Google support and engineering to access your project's data.

Google Cloud

Using Access Approval together with Access Transparency, means explicit consent is needed before Google support or Google engineers can access your project's data.



Access Approval quickly alerts you by sending messages when access is requested

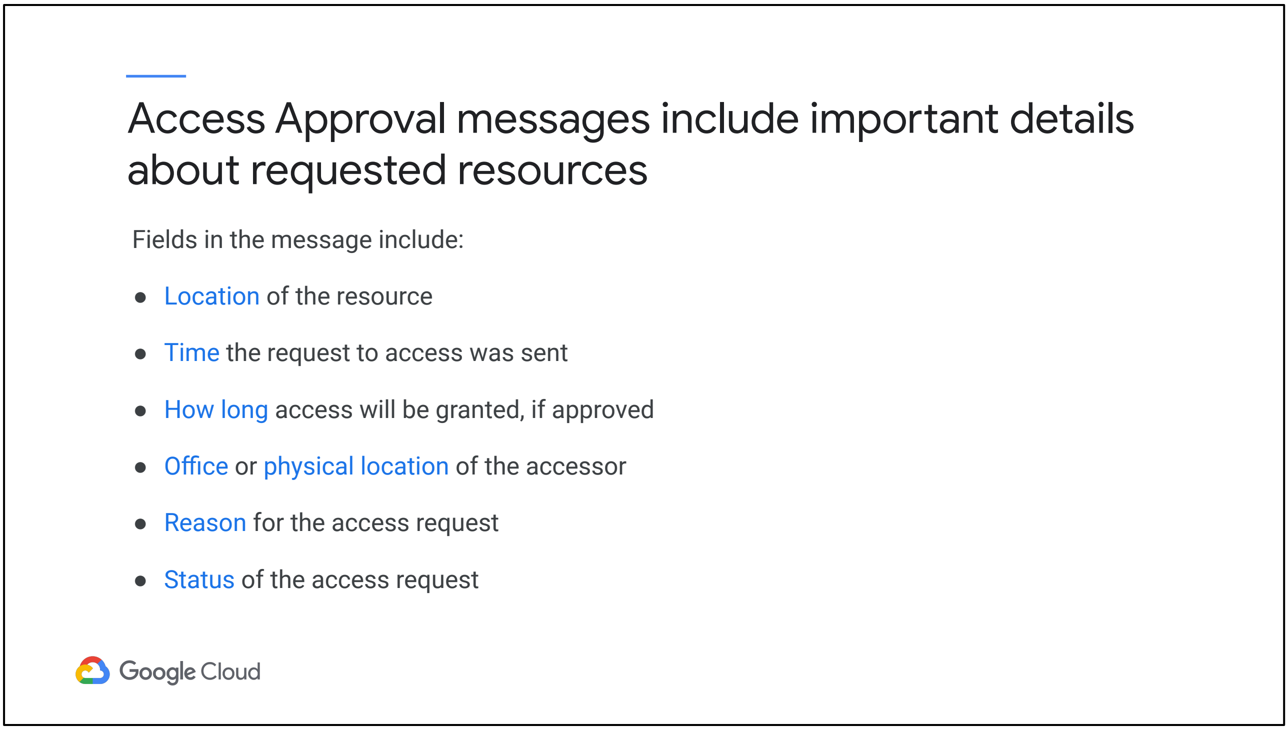
- Access Approval is set up on a project level.
- Access request messages sent via email or Pub/Sub.
- Google Cloud Console or Access Approval API used to approve the request.

Google Cloud

Access Approval is set up on a project level and uses the **Access Approval Config Editor IAM role.**

Access Approval works by sending you an email or Pub/Sub message with an access request.

Using the information sent within the message, you can use either the Google Cloud Console or the Access Approval API to approve the request.



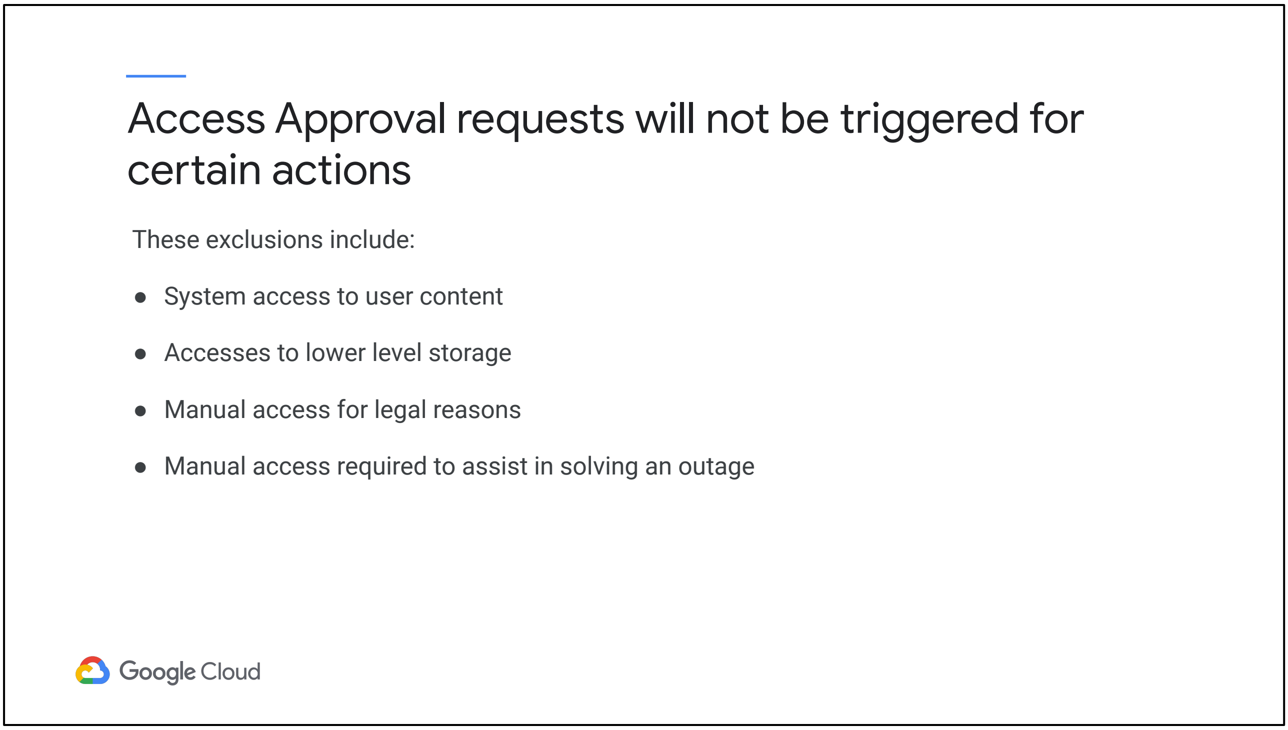
Access Approval messages include important details about requested resources

Fields in the message include:

- Location of the resource
- Time the request to access was sent
- How long access will be granted, if approved
- Office or physical location of the accessor
- Reason for the access request
- Status of the access request

Access may be requested at the level of a resource or at the level of a specific project.

Approving any access request also grants approval to any child of that resource.



Access Approval requests will not be triggered for certain actions

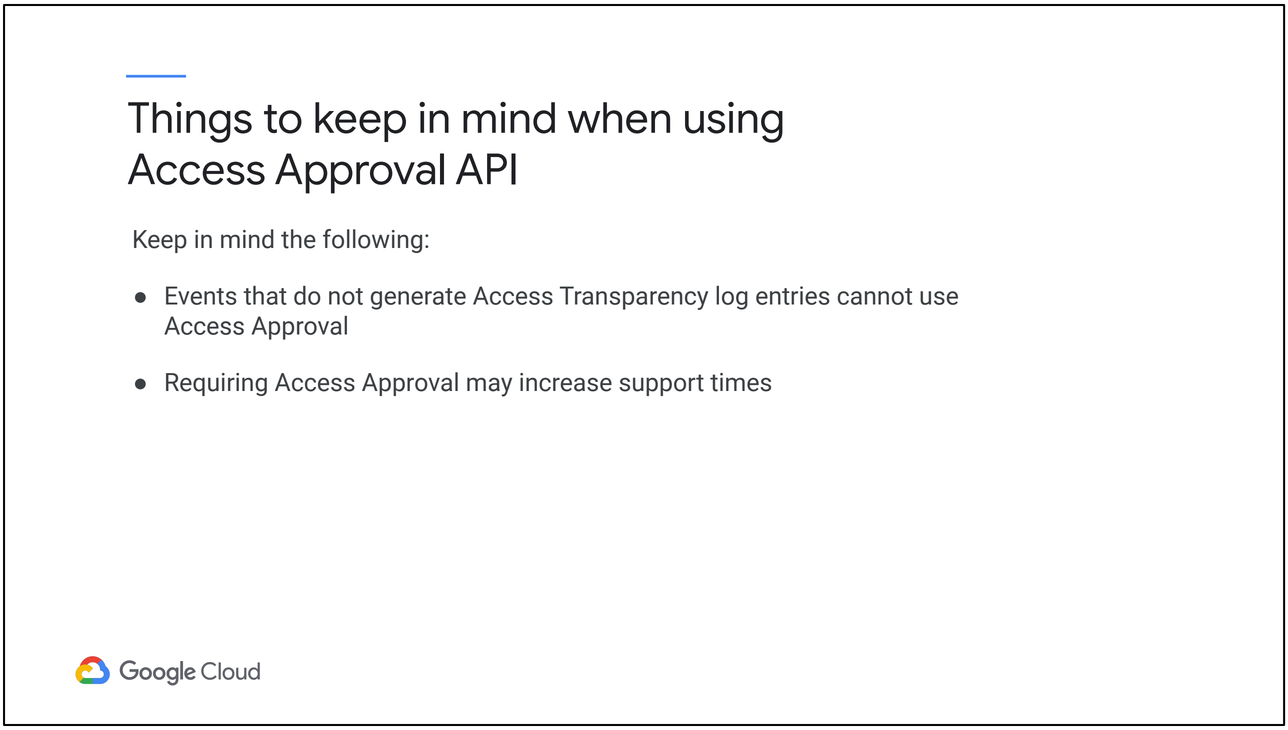
These exclusions include:

- System access to user content
- Accesses to lower level storage
- Manual access for legal reasons
- Manual access required to assist in solving an outage

Google Cloud

System access is covered by another authorization process, and is out of scope for Access Approval API. Access to lower level storage is also out of scope for Access Approval, although it will generate an Access Transparency log entry.

If Google requires access to comply with legal requirements, this access will bypass the Access Approval processes. If Google requires access to assist in resolving an outage, these accesses will also bypass Access Approval.



Things to keep in mind when using Access Approval API

Keep in mind the following:

- Events that do not generate Access Transparency log entries cannot use Access Approval
- Requiring Access Approval may increase support times

Events that do not generate an entry in the Access Transparency log will also not generate an Access Approval request. Requiring Access Approval may increase support times, which may mean Google will not be able to meet SLAs for your chosen products.

Agenda

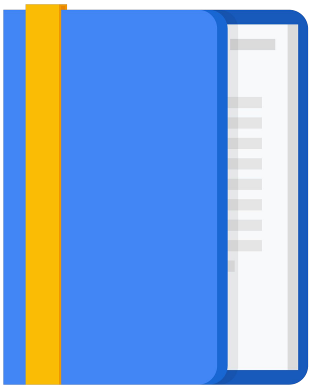
Google Cloud’s Approach to Security

The Shared Security Responsibility Model

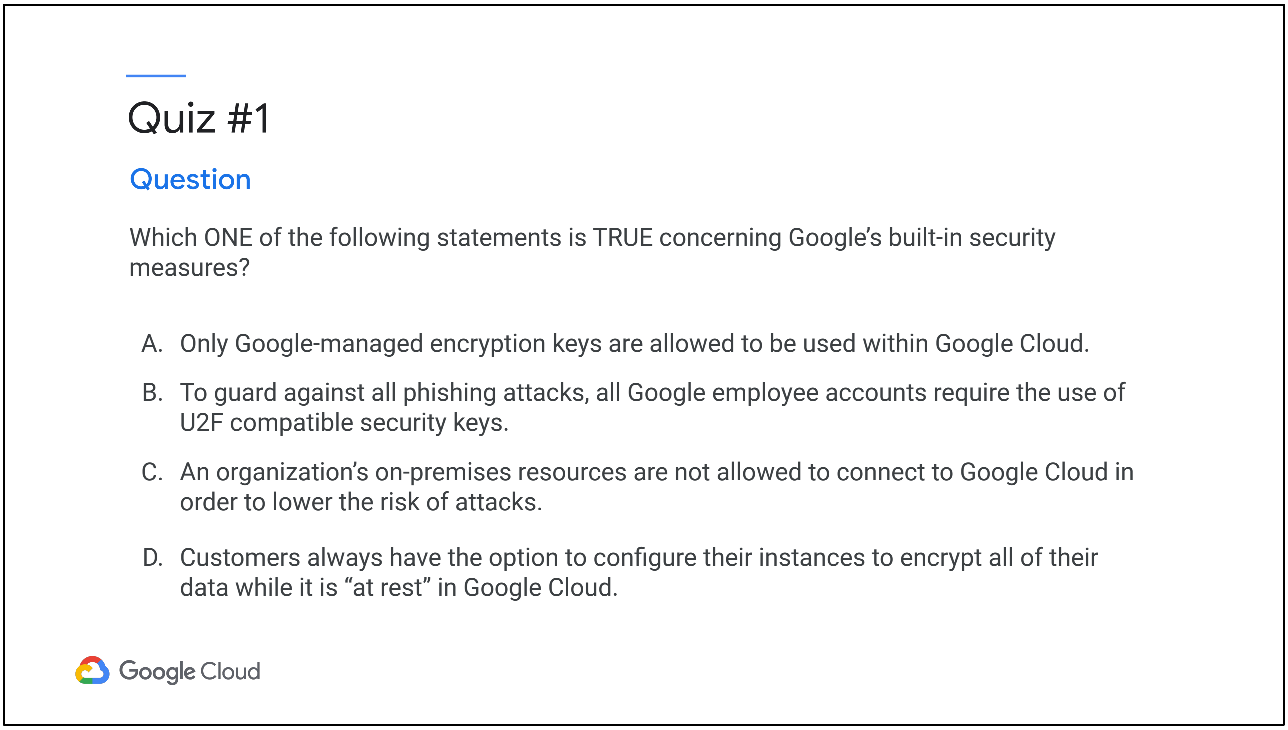
Threats Mitigated by Google and Google Cloud

Access Transparency

Quiz and Module Review



Google Cloud



Quiz #1

Question

Which ONE of the following statements is TRUE concerning Google's built-in security measures?

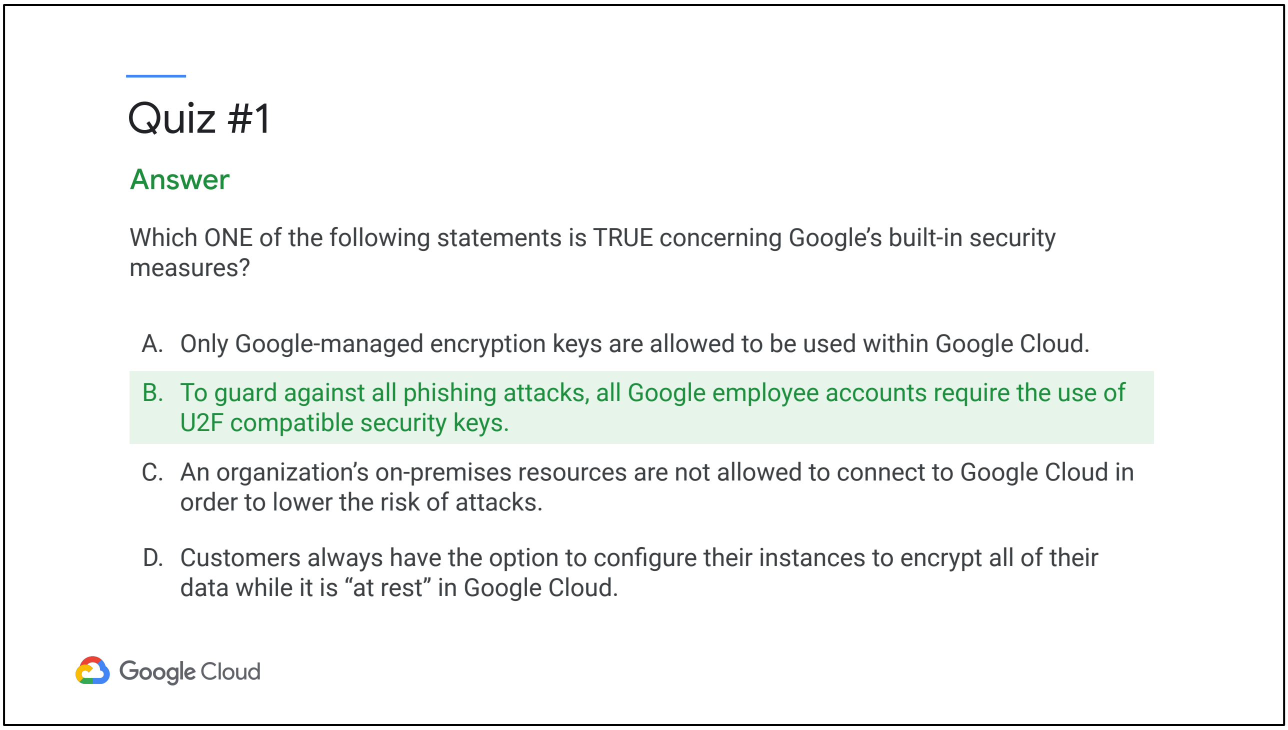
A. Only Google-managed encryption keys are allowed to be used within Google Cloud.

B. To guard against all phishing attacks, all Google employee accounts require the use of U2F compatible security keys.

C. An organization's on-premises resources are not allowed to connect to Google Cloud in order to lower the risk of attacks.

D. Customers always have the option to configure their instances to encrypt all of their data while it is "at rest" in Google Cloud.

Google Cloud



Quiz #1

Answer

Which ONE of the following statements is TRUE concerning Google’s built-in security measures?

A. Only Google-managed encryption keys are allowed to be used within Google Cloud.

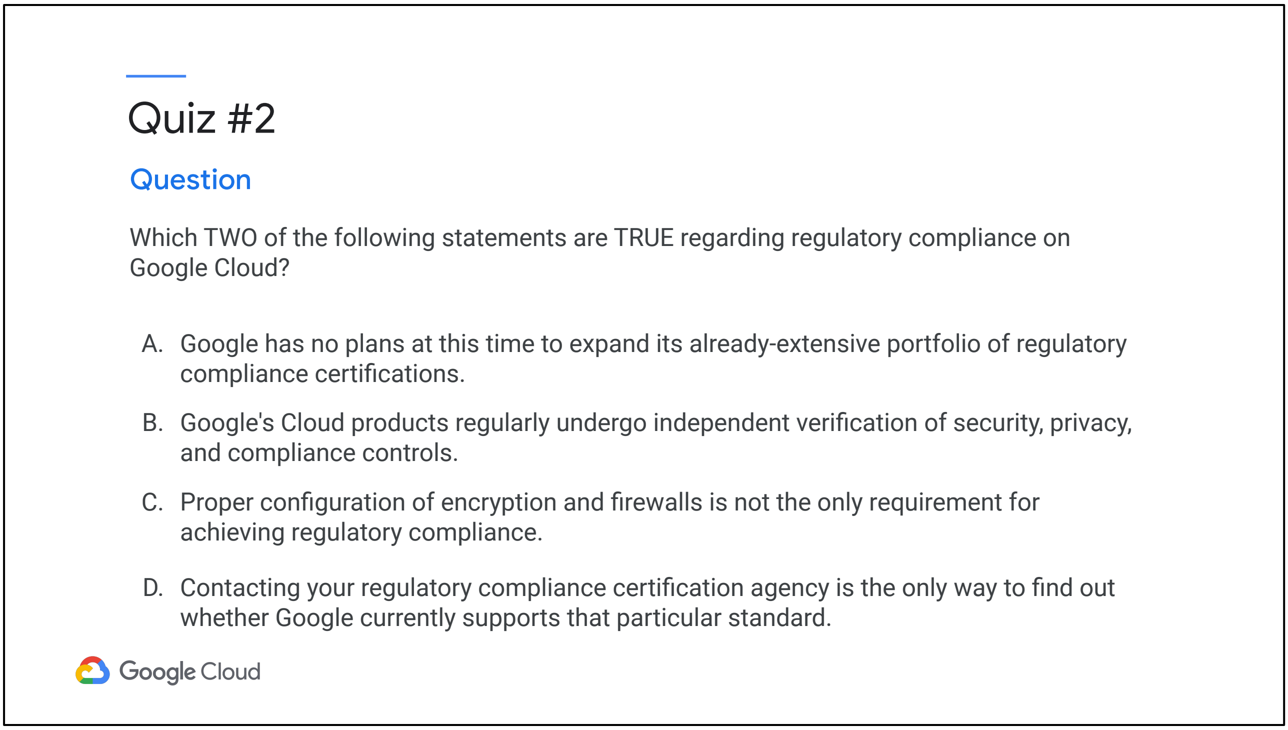
B. To guard against all phishing attacks, all Google employee accounts require the use of U2F compatible security keys.

C. An organization’s on-premises resources are not allowed to connect to Google Cloud in order to lower the risk of attacks.

D. Customers always have the option to configure their instances to encrypt all of their data while it is “at rest” in Google Cloud.

Google Cloud

B. Earlier you learned in the lecture that all Google employee accounts require the use of U2F compatible security keys.



Quiz #2

Question

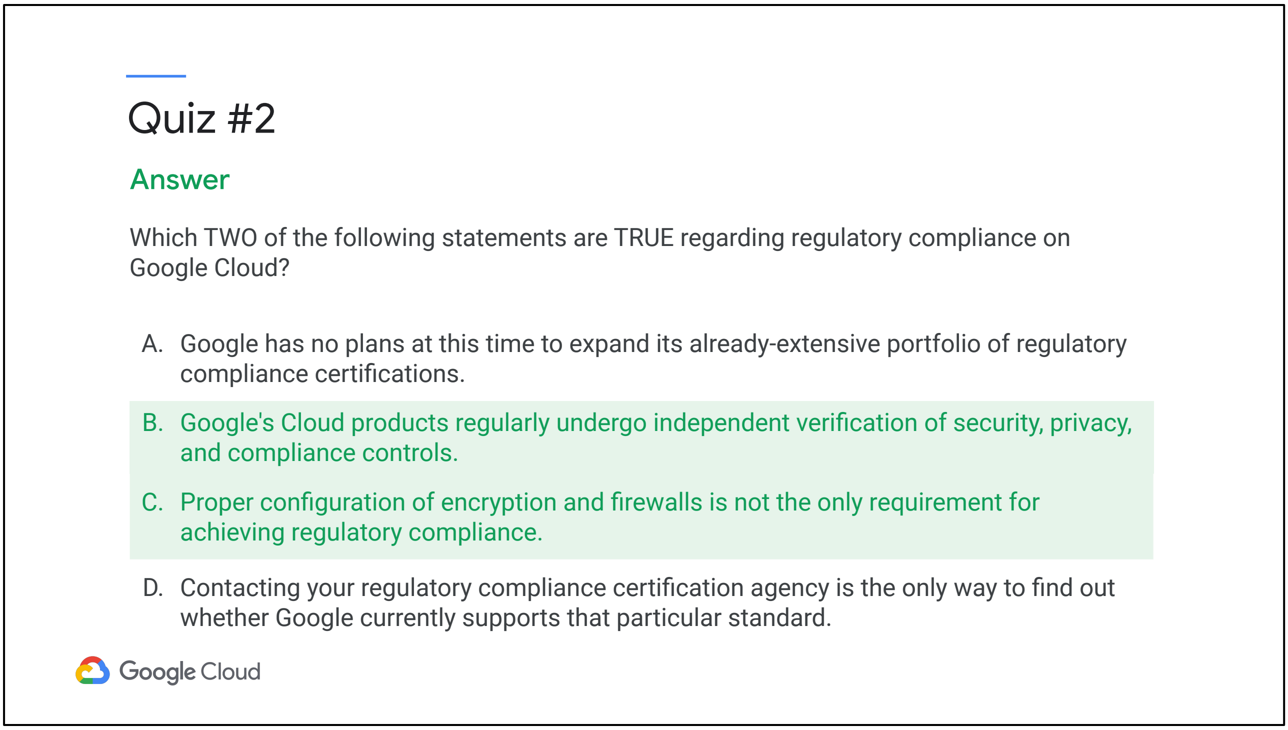
Which TWO of the following statements are TRUE regarding regulatory compliance on Google Cloud?

A. Google has no plans at this time to expand its already-extensive portfolio of regulatory compliance certifications.

B. Google's Cloud products regularly undergo independent verification of security, privacy, and compliance controls.

C. Proper configuration of encryption and firewalls is not the only requirement for achieving regulatory compliance.

D. Contacting your regulatory compliance certification agency is the only way to find out whether Google currently supports that particular standard.



Quiz #2

Answer

Which TWO of the following statements are TRUE regarding regulatory compliance on Google Cloud?

A. Google has no plans at this time to expand its already-extensive portfolio of regulatory compliance certifications.

B. Google's Cloud products regularly undergo independent verification of security, privacy, and compliance controls.

C. Proper configuration of encryption and firewalls is not the only requirement for achieving regulatory compliance.

D. Contacting your regulatory compliance certification agency is the only way to find out whether Google currently supports that particular standard.

Google Cloud

B. Google works to achieve certifications against global standards so we can earn your trust.
C. You also need data protection that is in compliance with the regulatory standards you wish to meet.

Quiz #3

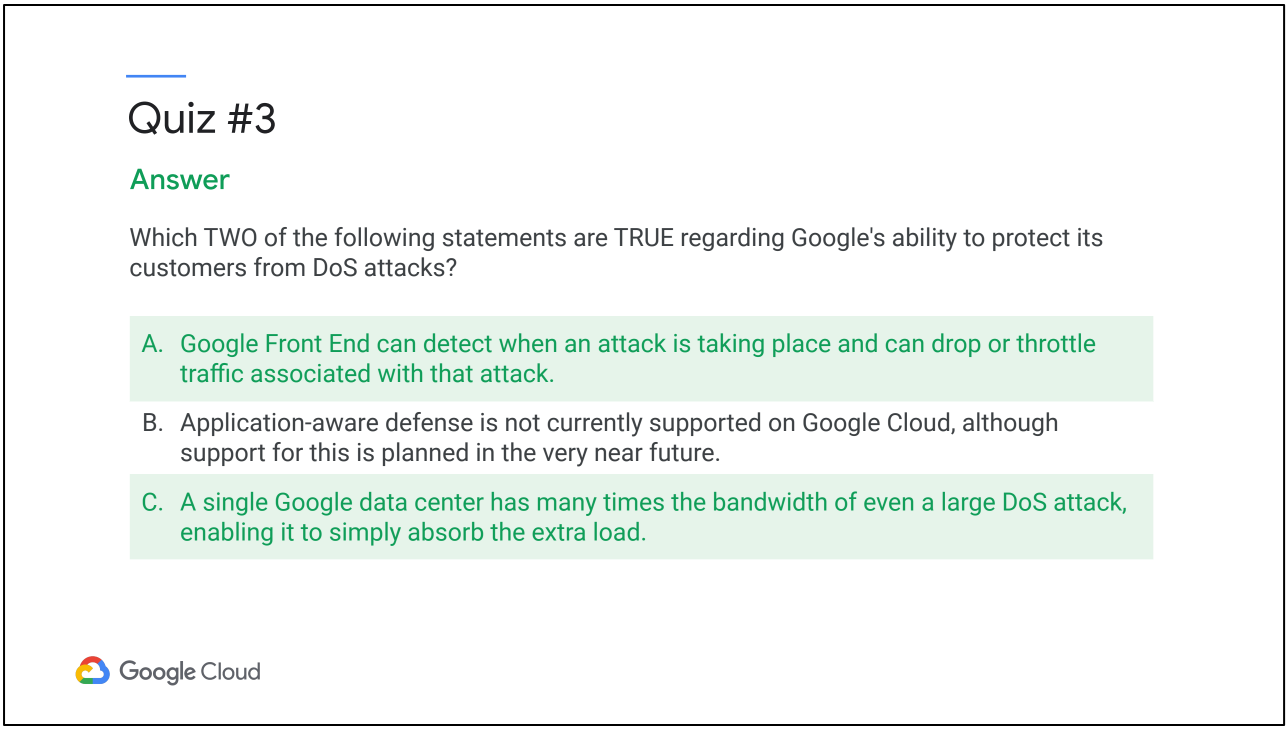
Question

Which TWO of the following statements are TRUE regarding Google's ability to protect its customers from DoS attacks?

A. Google Front End can detect when an attack is taking place and can drop or throttle traffic associated with that attack.

B. Application-aware defense is not currently supported on Google Cloud, although support for this is planned in the very near future.

C. A single Google data center has many times the bandwidth of even a large DoS attack, enabling it to simply absorb the extra load.



Quiz #3

Answer

Which TWO of the following statements are TRUE regarding Google's ability to protect its customers from DoS attacks?

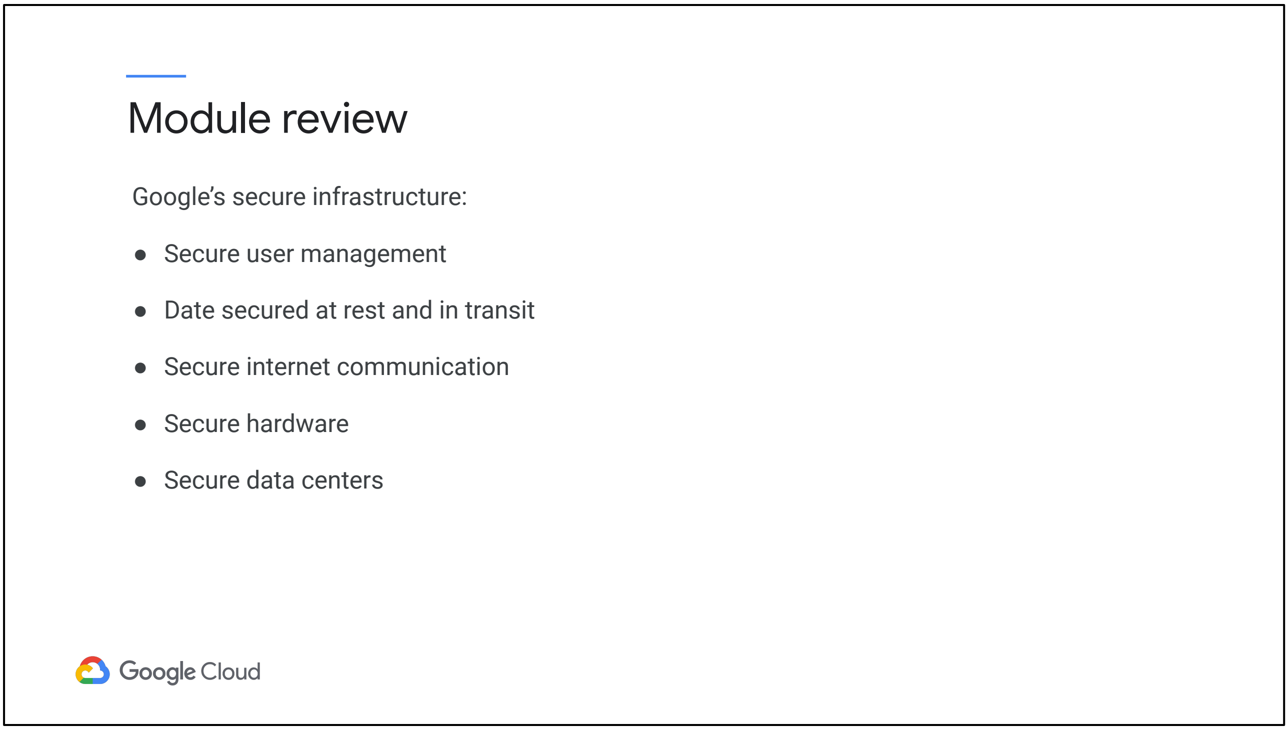
A. Google Front End can detect when an attack is taking place and can drop or throttle traffic associated with that attack.

B. Application-aware defense is not currently supported on Google Cloud, although support for this is planned in the very near future.

C. A single Google data center has many times the bandwidth of even a large DoS attack, enabling it to simply absorb the extra load.

Google Cloud

A. Further, when you use Google load balancers, this protection kicks in automatically, without the need for further configuration.
C. A large attack can be around 1 Tb per second, but a typical Google data center has a bandwidth capacity of around 1300 Tb per second.



Module review

Google's secure infrastructure:

- Secure user management
- Date secured at rest and in transit
- Secure internet communication
- Secure hardware
- Secure data centers

To summarize, in this module we learned more about the fundamentals of security in Google Cloud, including how security is built into the infrastructure at its core.

Security starts at Google with secure user management, and includes data that is secured both at rest and in transit, as well as secure internet communication over Google's own network, via the Google front end.

Google's state of the art data centers complete this circle of trust and security, by making use of custom, Google-designed hardware to help reduce the risk of hardware exploits.

Google Cloud