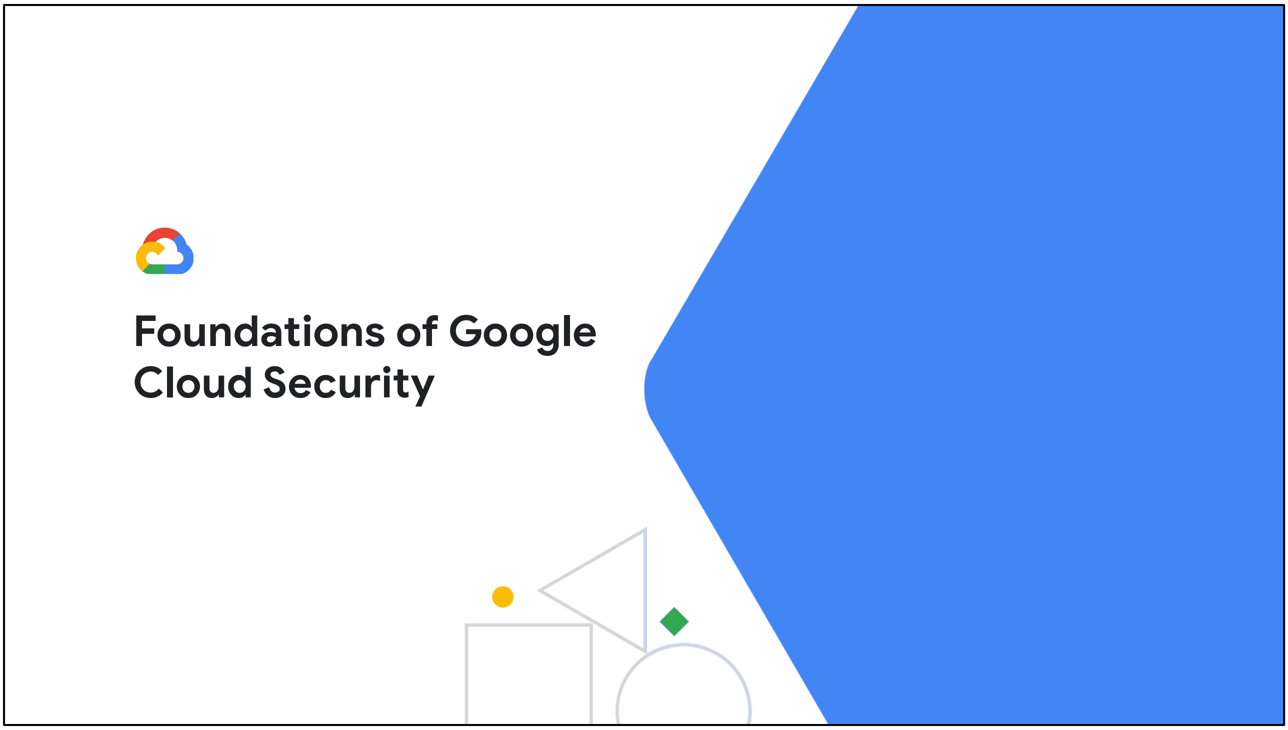
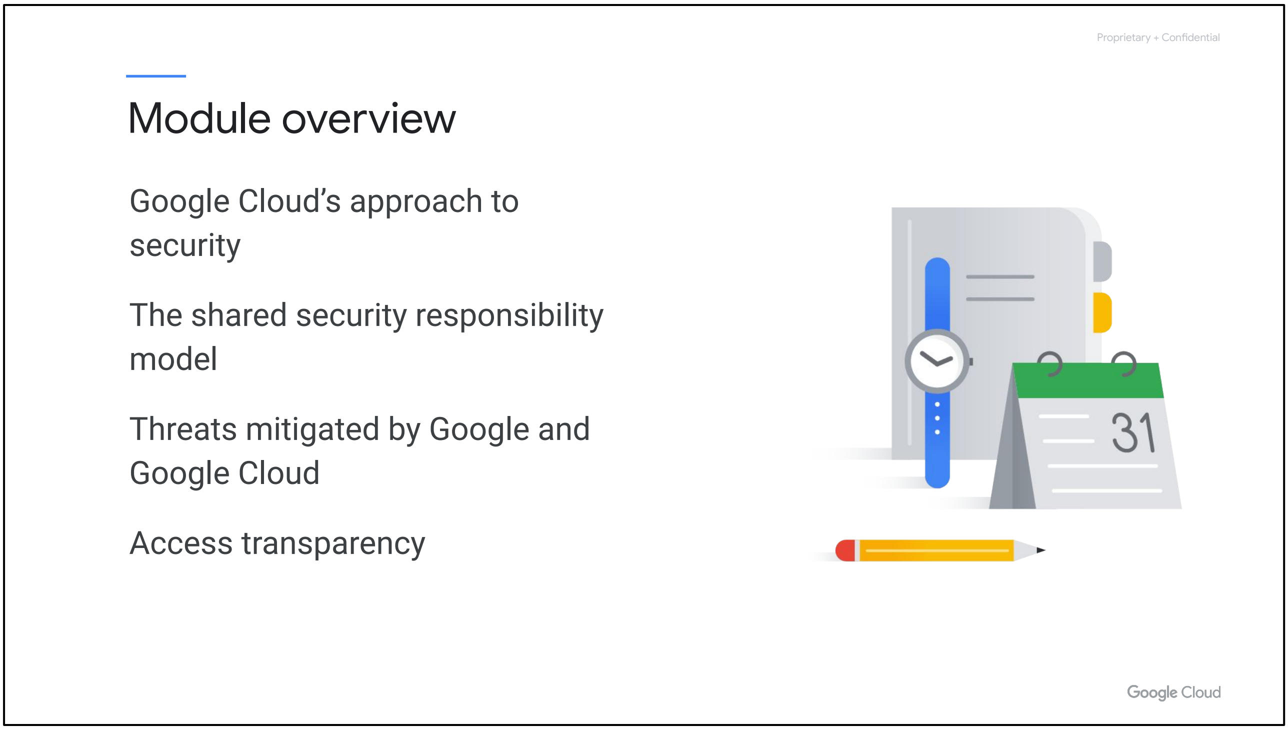


Foundations of Google Cloud Security

Welcome to the Foundations of Google Cloud Security module.



Module overview

Google Cloud's approach to security

The shared security responsibility model

Threats mitigated by Google and Google Cloud

Access transparency

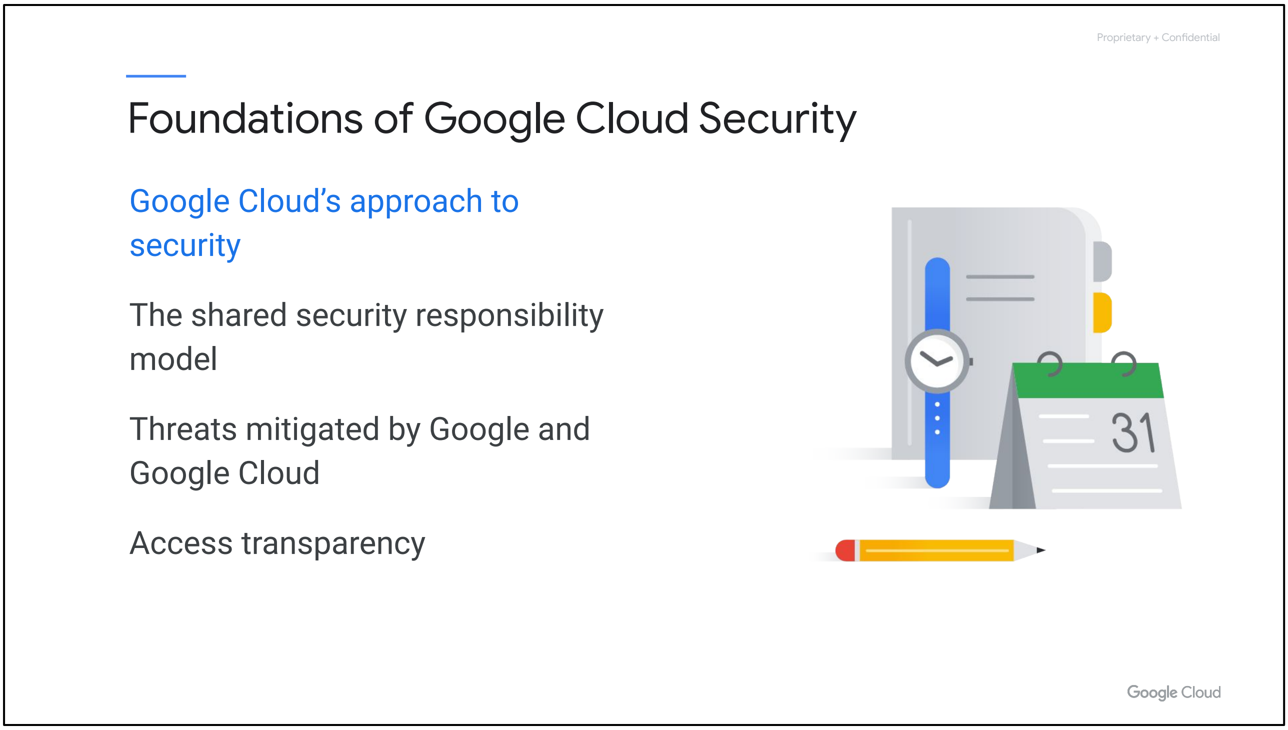
We are glad you are interested in learning more about Google Cloud security. Securing systems are a hot topic and should be a priority for everyone today - and, as you will see, it is definitely a priority here at Google.

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 run on Google's infrastructure in Google Cloud.

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



Foundations of Google Cloud Security

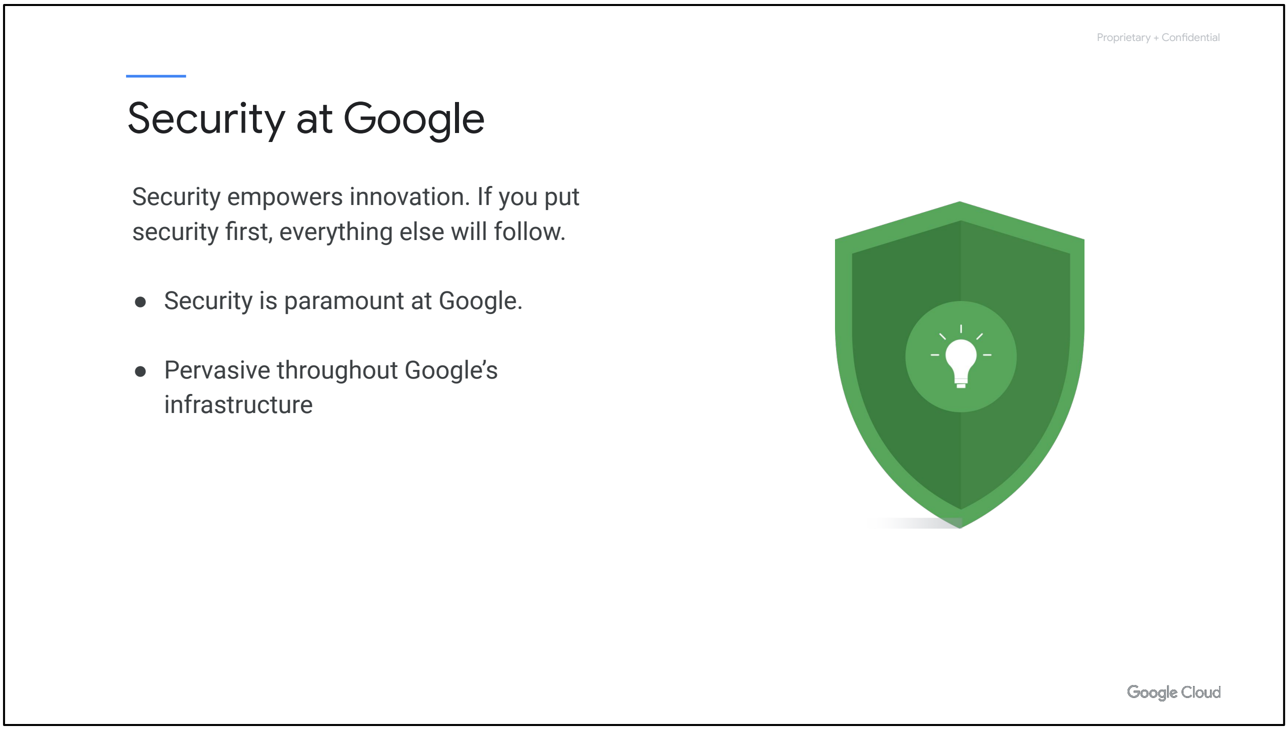
Google Cloud’s approach to security

The shared security responsibility model

Threats mitigated by Google and Google Cloud

Access transparency

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



Proprietary + Confidential

Security at Google

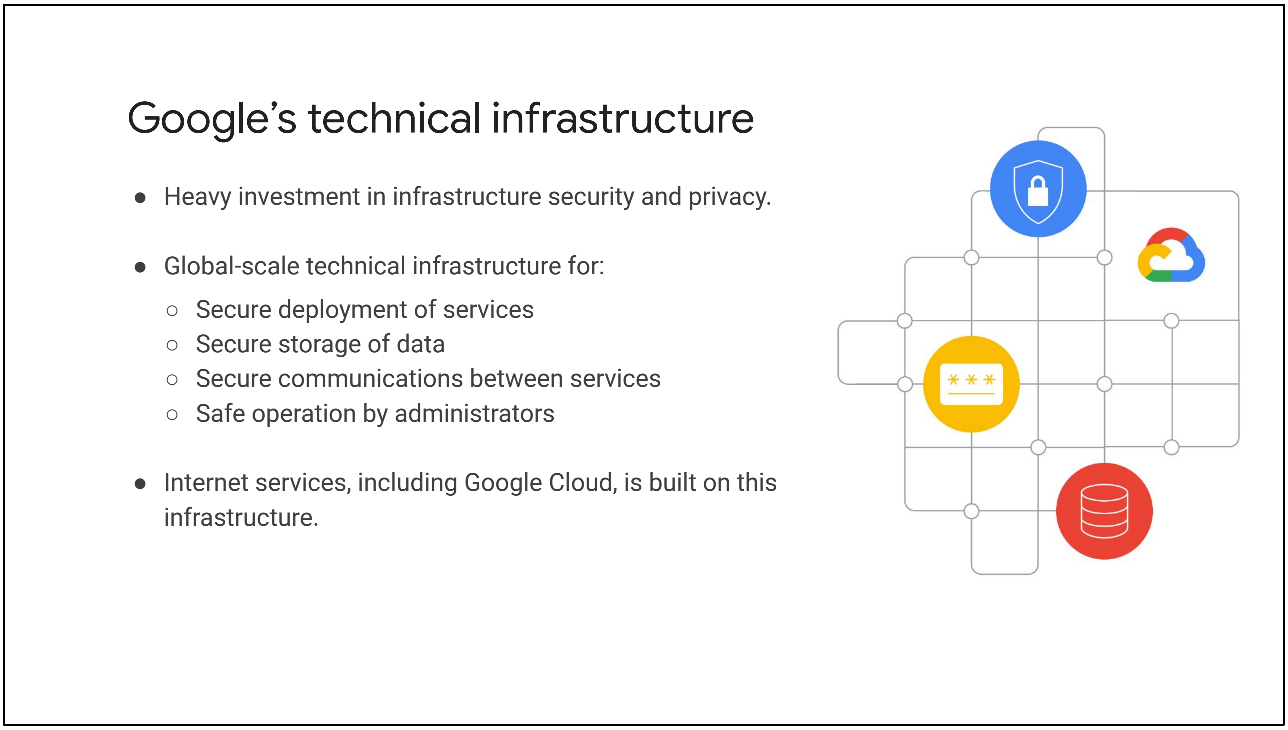
Security empowers innovation. If you put security first, everything else will follow.

- Security is paramount at Google.
- Pervasive throughout Google's infrastructure

Google Cloud

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

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, is built on this infrastructure.

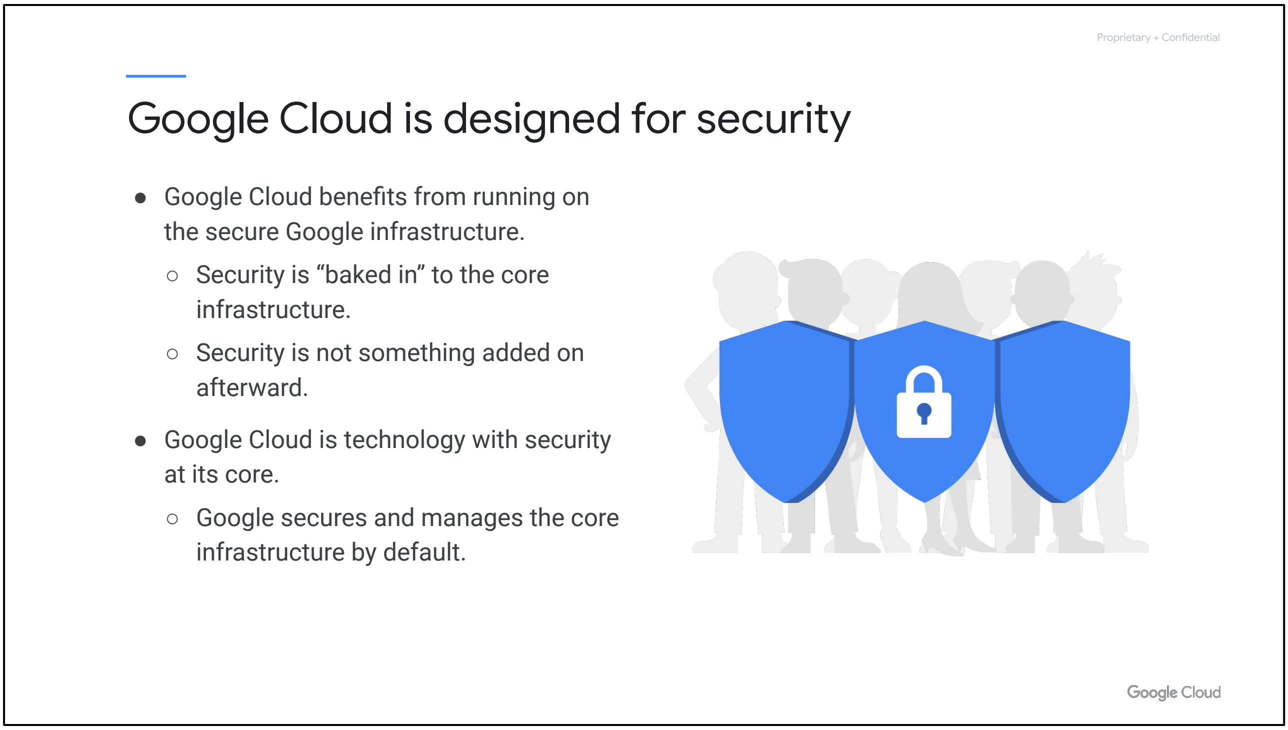
Countless companies and governments have lost data because of security incidents. Just one such breach could cost millions in fines and lost business—and more importantly, the loss of customer trust.

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

Internet services, including Google Cloud, built on this infrastructure.



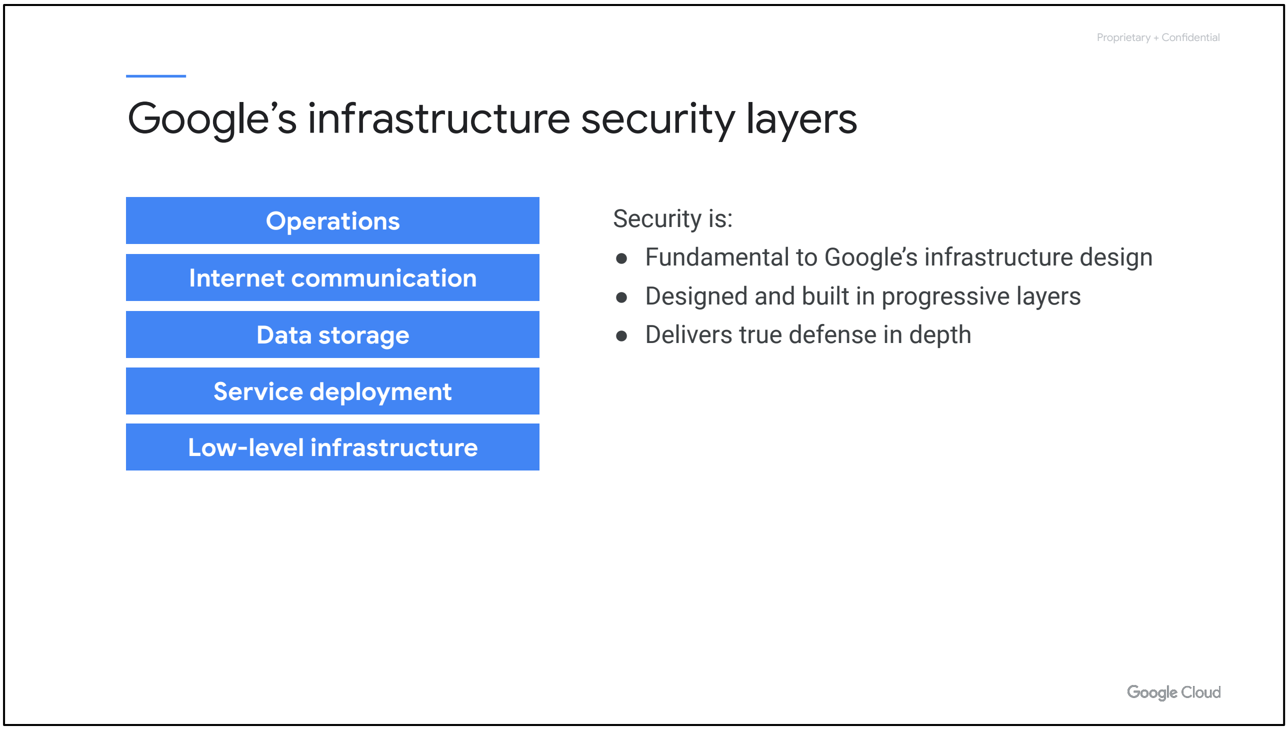
Google Cloud is designed for security

- 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, which highlights how Google Cloud is designed for security from the bottom up.



Google’s infrastructure security layers

Operations

Internet communication

Data storage

Service deployment

Low-level infrastructure

Security is:

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

Google Cloud

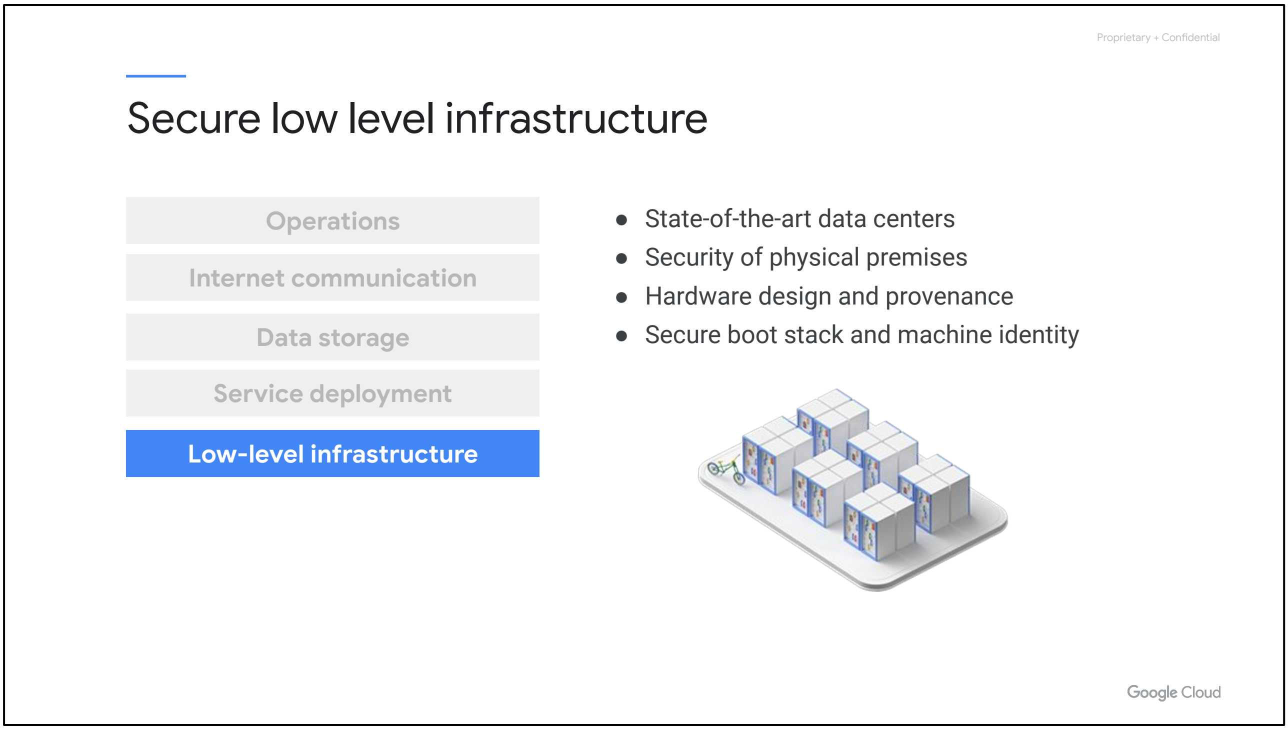
It’s not enough to build something and try to make it secure after the fact.

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 our way up.



Proprietary + Confidential

Secure low level infrastructure

- Operations
- Internet communication
- Data storage
- Service deployment
- **Low-level infrastructure**

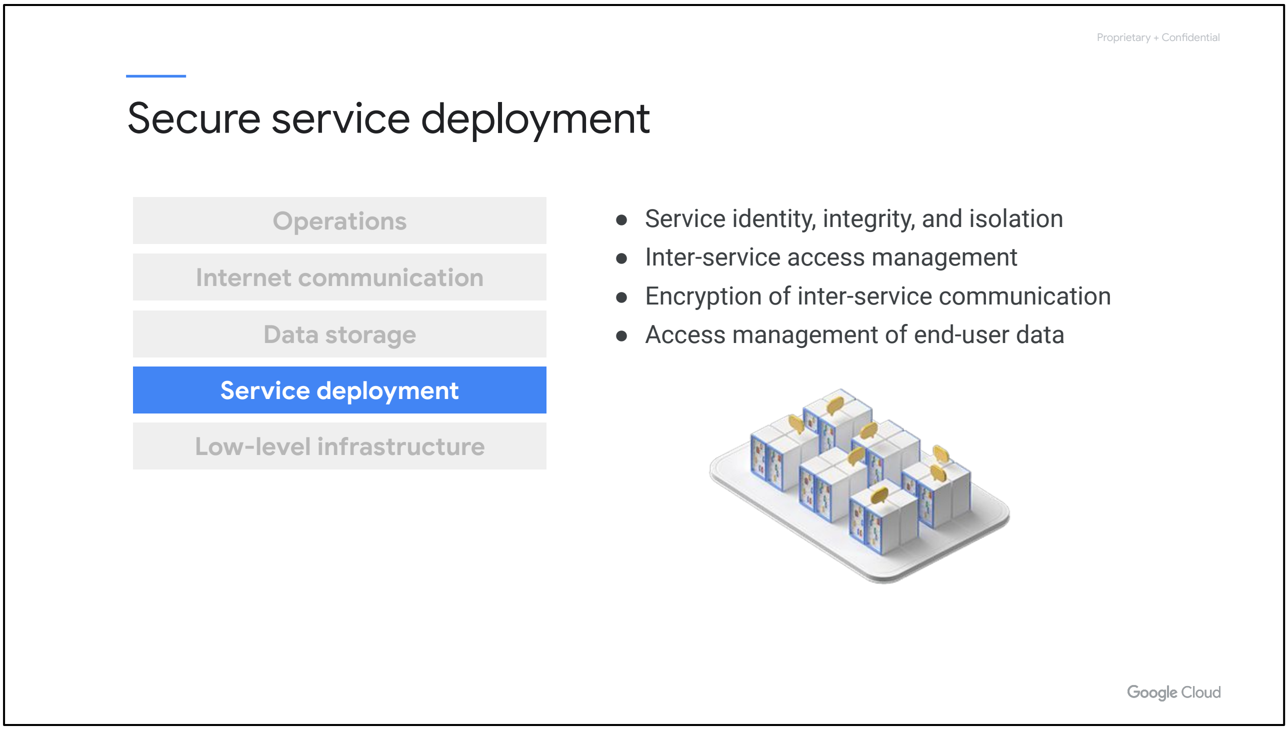
- State-of-the-art data centers
- Security of physical premises
- Hardware design and provenance
- Secure boot stack and machine identity

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

- Operations
- Internet communication
- Data storage
- **Service deployment**
- Low-level infrastructure

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

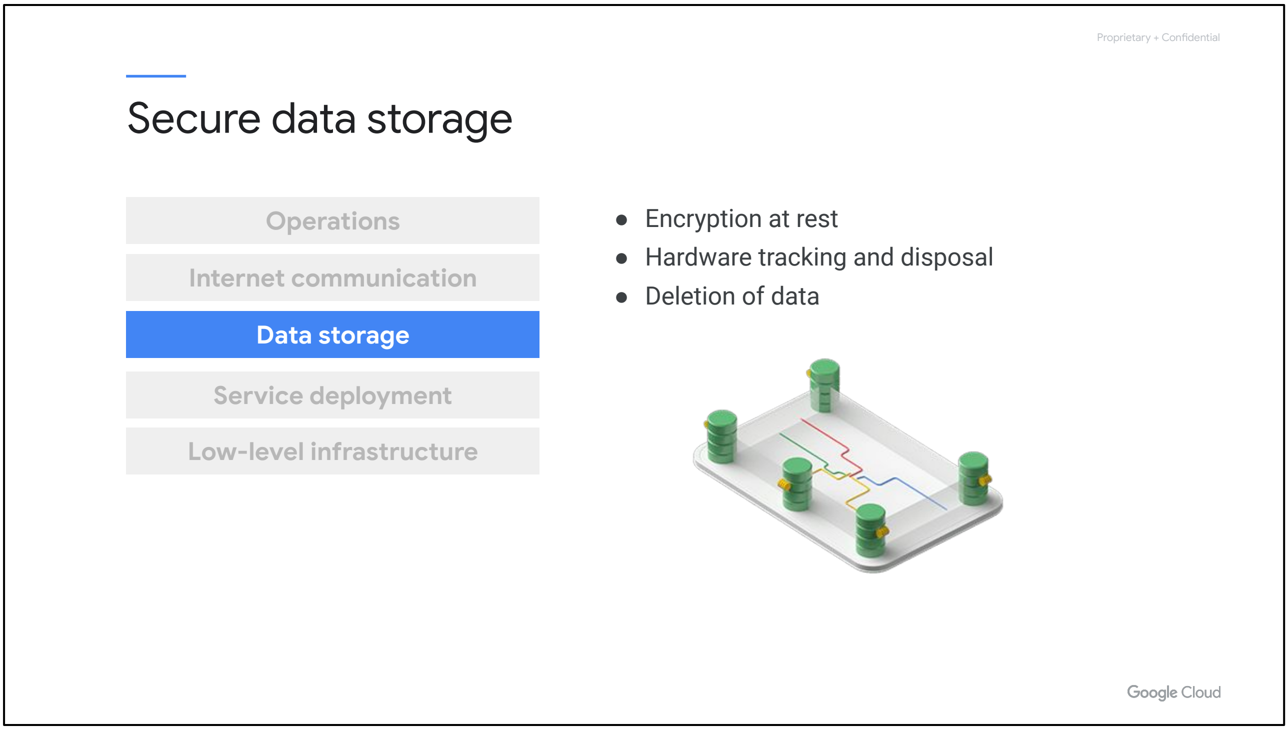
Google Cloud

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.



Proprietary + Confidential

Secure data storage

- Operations
- Internet communication
- **Data storage**
- Service deployment
- Low-level 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:

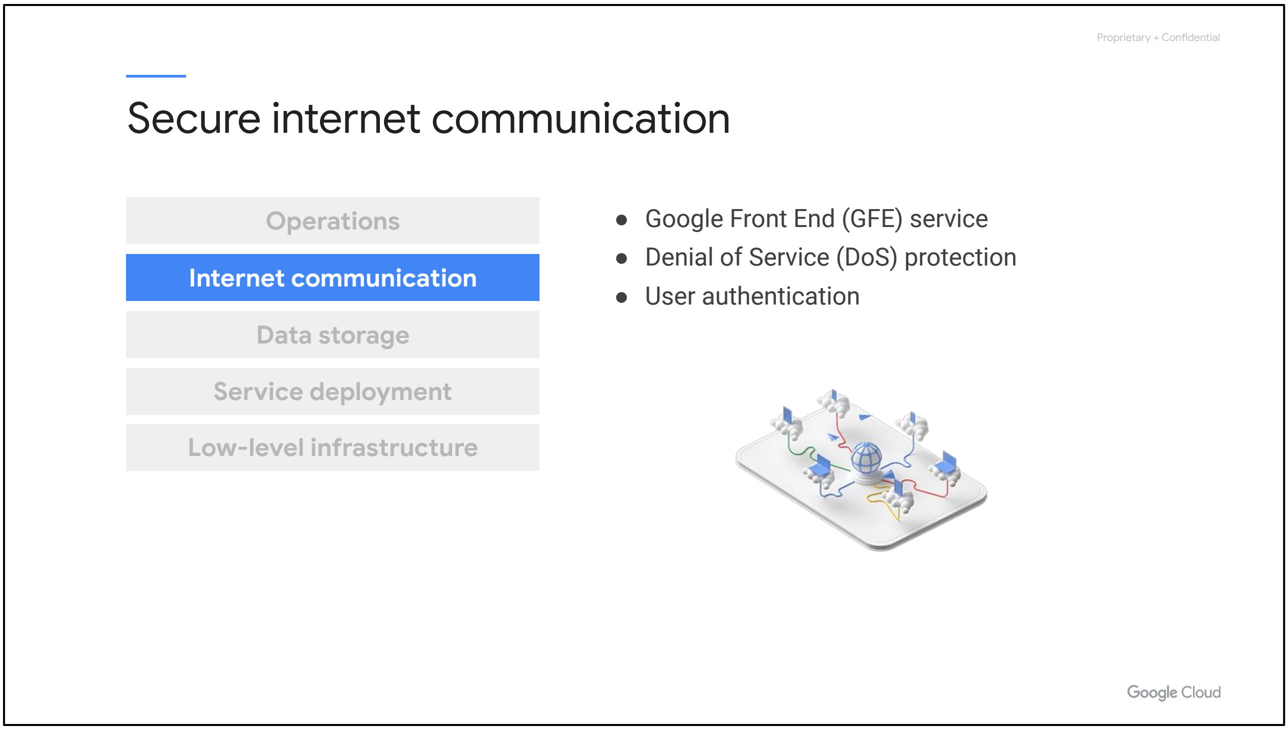
- Customer Managed Encryption keys (CMEKs), where you can manage your own encryption keys with the Google Key Management Service (KMS).
- And Customer Supplied Encryption keys (CSEKs), where you can provide and manage your own keys.

We will cover encryption keys in more detail in a later module.

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.



Proprietary + Confidential

Secure internet communication

- Operations
- **Internet communication**
- Data storage
- Service deployment
- Low-level infrastructure

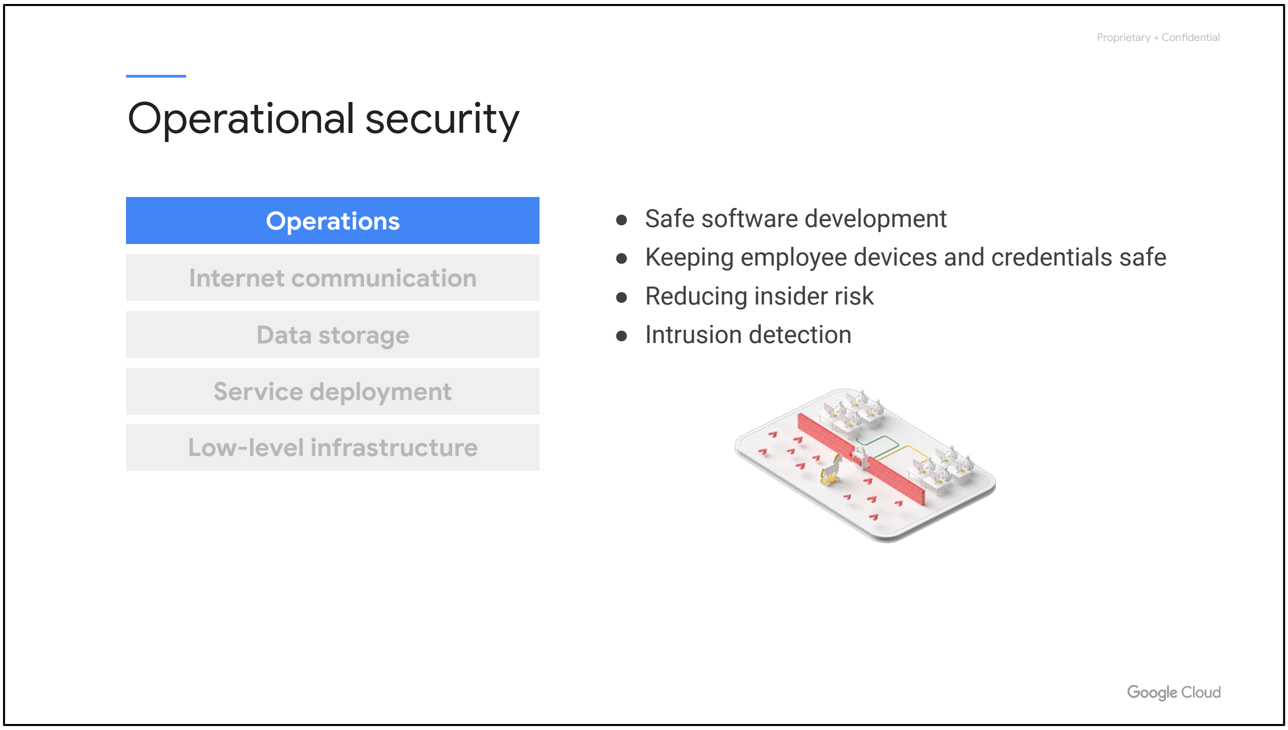
- Google Front End (GFE) service
- Denial of Service (DoS) protection
- User authentication

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, 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, which we'll cover in more detail in a later module.

Google Cloud 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 Cloud Interconnect for highly available, low latency connections.



Operational security

Operations

Internet communication

Data storage

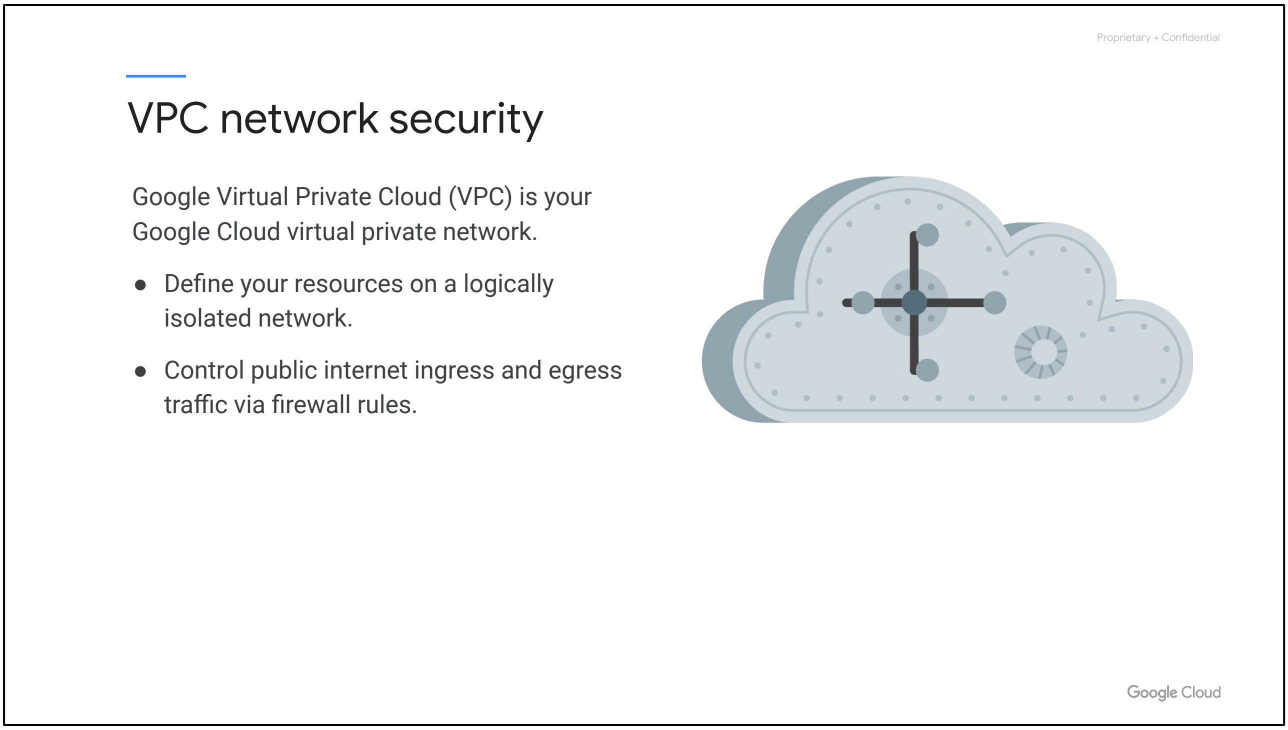
Service deployment

Low-level infrastructure

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

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

Google priorities keeping employees and their devices and credentials safe. Google is keen on reducing insider risk and intrusion detection as well.



VPC network security

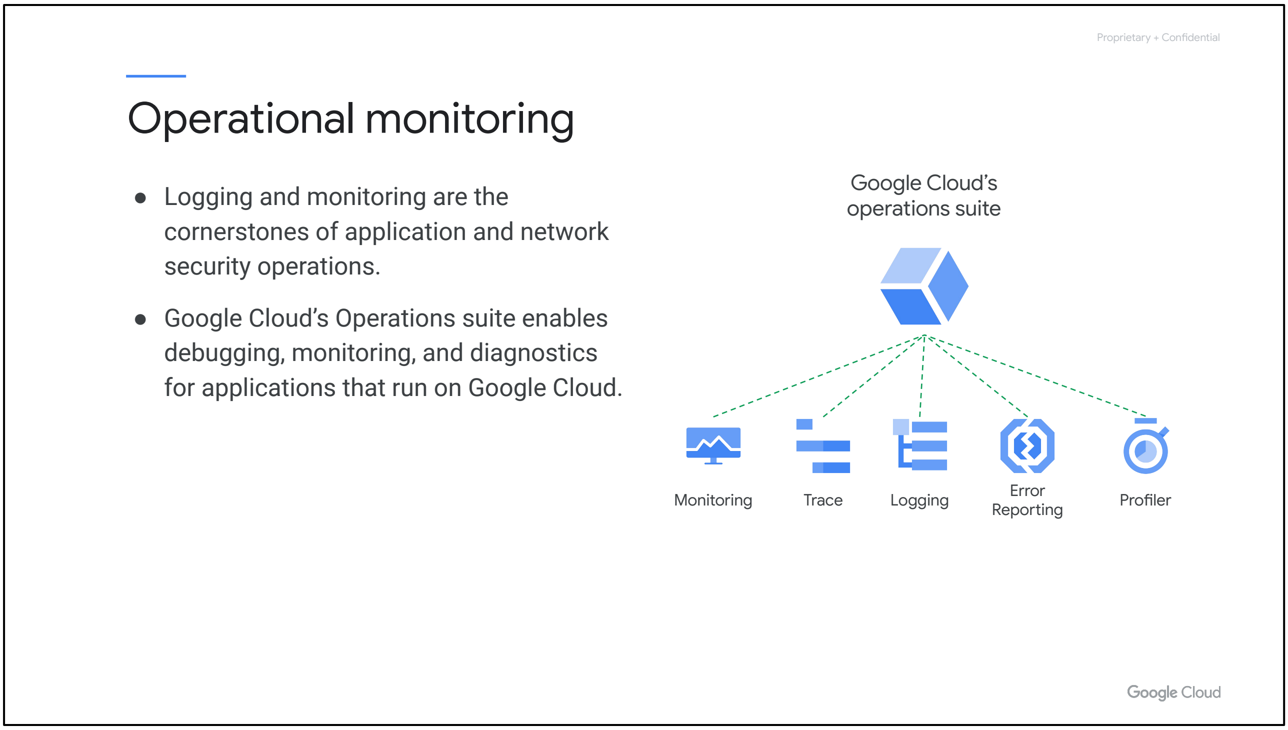
Google Virtual Private Cloud (VPC) is your Google Cloud virtual private network.

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

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 and a many more will be discussed in 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.

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, 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.

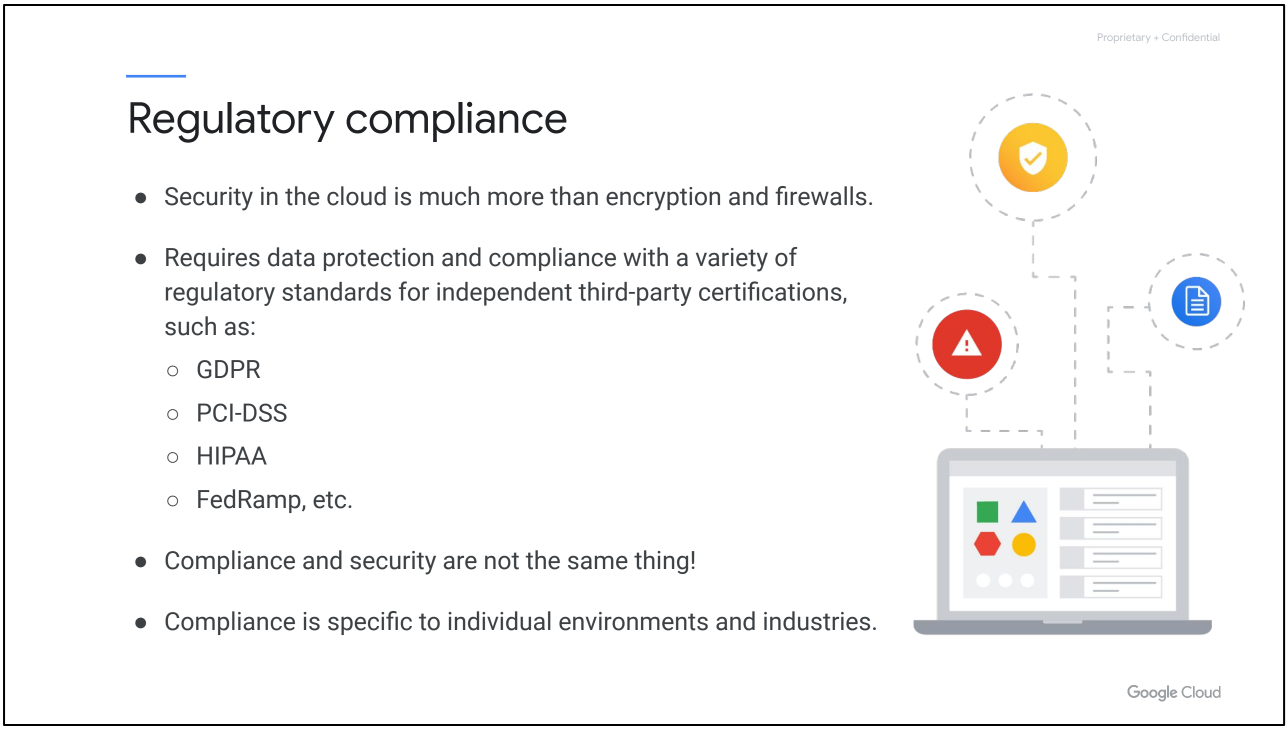
Cloud Logging (formerly Stackdriver Logging) allows you to store, search, analyze, monitor, and trigger alerts on log data and events from Google Cloud. Our API also allows ingestion of any custom log data from any other source.

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 and trace tools help to quickly locate and fix problems in production systems.

Cloud Debugger has been deprecated, but you can still use open source tools like Snapshot Debugger to help you inspect the state of a running cloud system. For more information, see Snapshot Debugger (https://github.com/GoogleCloudPlatform/snapshot-debugger)

Other reporting systems include Security Command Center and Chronicle. We’ll cover the former in more detail in a later module.



Proprietary + Confidential

Regulatory compliance

- Security in the cloud is much more than encryption and firewalls.
- Requires data protection and compliance with a variety of regulatory standards for independent third-party certifications, such as:
  - GDPR
  - PCI-DSS
  - HIPAA
  - FedRamp, etc.
- Compliance and security are not the same thing!
- Compliance is specific to individual environments and industries.

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.

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.

While compliance requirements are a facet of security, they are not one and the same thing. Compliance is very much specific to individual environments and industries. While this will not be covered at length in this course, check out some of the great links in the speaker notes of this module to learn more about Google Cloud's compliance posture.

For Standards, Regulations and Certifications page that Google currently supports, see the link below:

- **Link:** cloud.google.com/security/compliance

You can also download reports from Google Cloud's Compliance Reports Manager from the link below:

- **Link:** cloud.google.com/security/compliance/compliance-reports-manager

Foundations of Google Cloud Security

Google Cloud’s approach to security

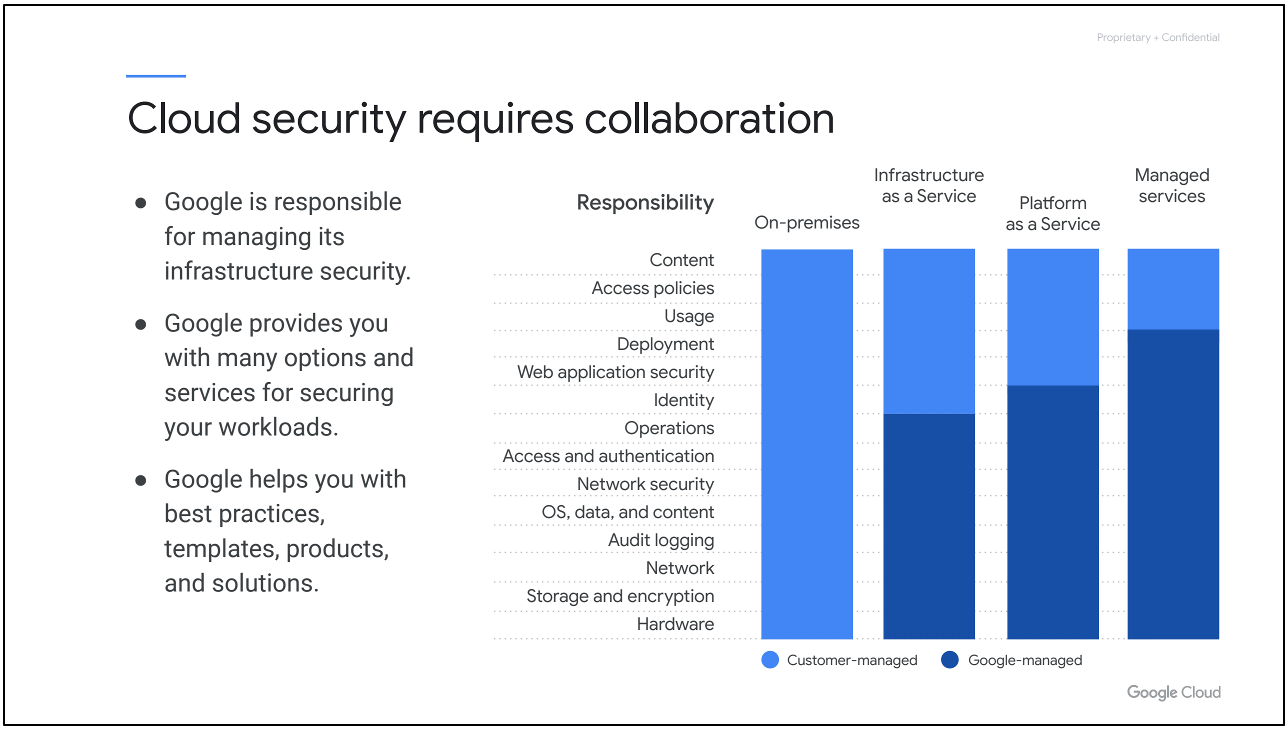
The shared security responsibility model

Threats mitigated by Google and Google Cloud

Access transparency

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.



Proprietary + Confidential

Cloud security requires collaboration

- Google is responsible for managing its infrastructure security.
- Google provides you with many options and services for securing your workloads.
- Google helps you with best practices, templates, products, and solutions.

Google Cloud

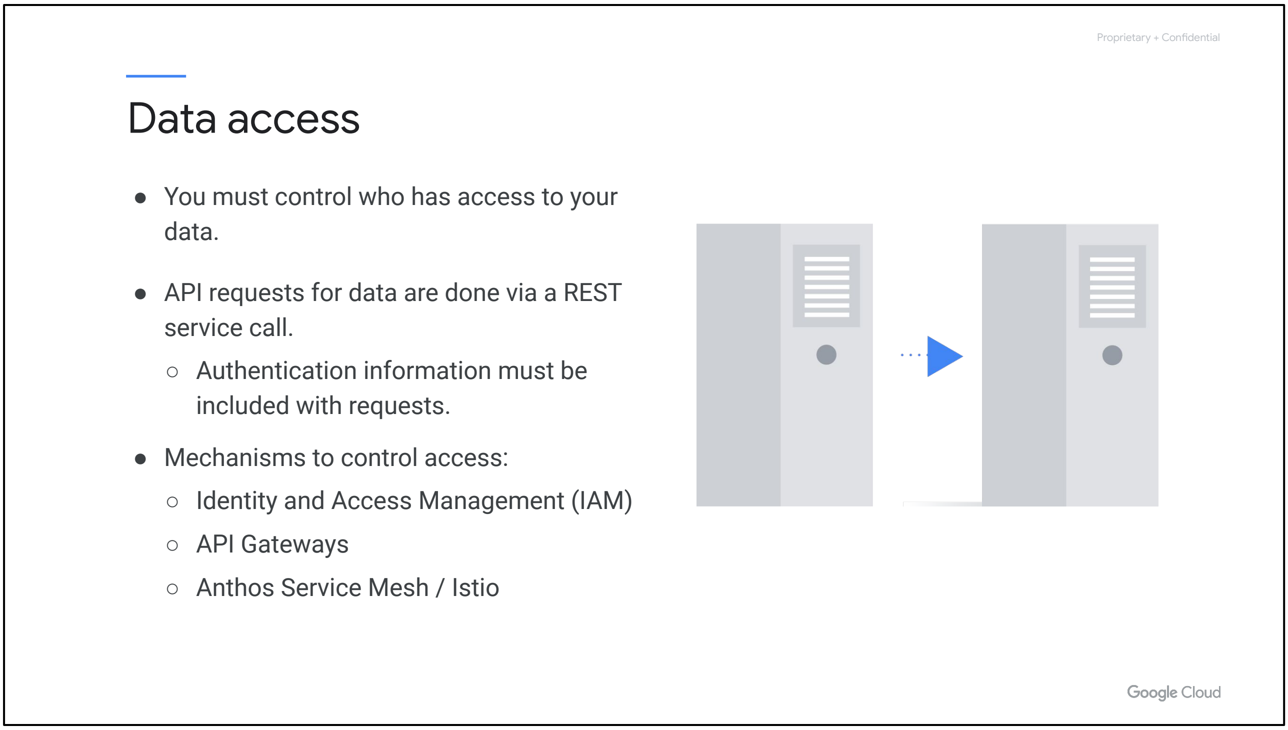
When you build an application with on-premise infrastructure, you are responsible for:

- 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 shared-responsibility model provides you with many options and managed services for securing your workloads. This flexibility is a big reason why businesses are moving to Google Cloud.

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.



Proprietary + Confidential

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.
- Mechanisms to control access:
  - Identity and Access Management (IAM)
  - API Gateways
  - Anthos Service Mesh / Istio

Google Cloud

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.

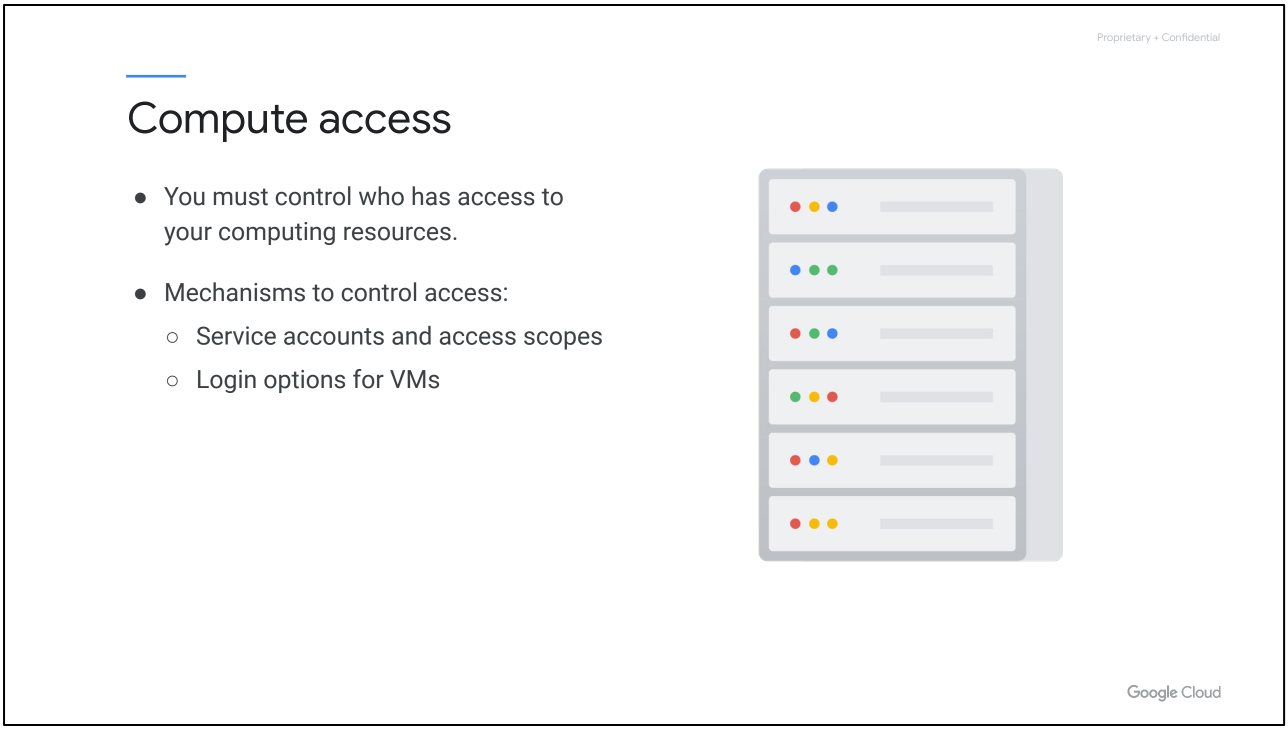
However, in order to protect your data, these controls must be properly configured. We will discuss this in more depth later in the course.

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.

You will be exposed to many services and mechanisms for controlling data throughout the course, but a few examples are:

- **Identity and Access Management (IAM):** allows you to grant granular access to specific Google Cloud resources and helps prevent access to other resources.
- **API Gateways:** allows you to securely transport data between application clients and services.
- **Anthos Service Mesh / Istio:** gives you a control plane to control how microservices communicate and share data with one another.



Compute access

- You must control who has access to your computing resources.
- Mechanisms to control access:
    - Service accounts and access scopes
    - Login options for VMs

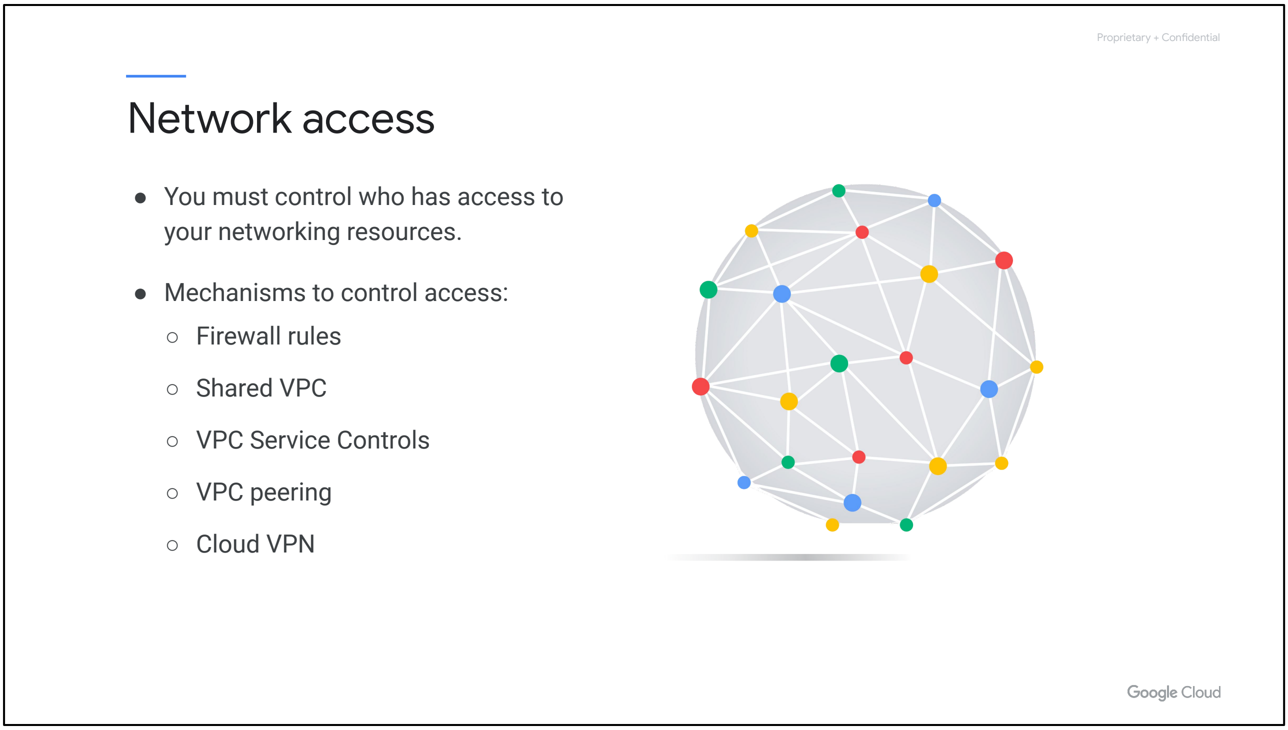
Google Cloud

Another aspect of security responsibilities for customers relates to controlling access to computing resources. Google Cloud provides you with a variety of mechanisms to do this, which we'll cover in more detail in Module 5.

Some examples of this are:

- **Service accounts and access scopes:** allows you to specify permissions and how your computing resources interact with services.
- **Login options for VMs:** allows you to control who and how your computing resources are accessed.

Depending on how a customer works in the cloud, this can involve more or less security responsibility and effort to ensure security compliance. Google helps you by providing best practices, templates, products, and solutions.



Proprietary + Confidential

Network access

- You must control who has access to your networking resources.
- Mechanisms to control access:
  - Firewall rules
  - Shared VPC
  - VPC Service Controls
  - VPC peering
  - Cloud VPN

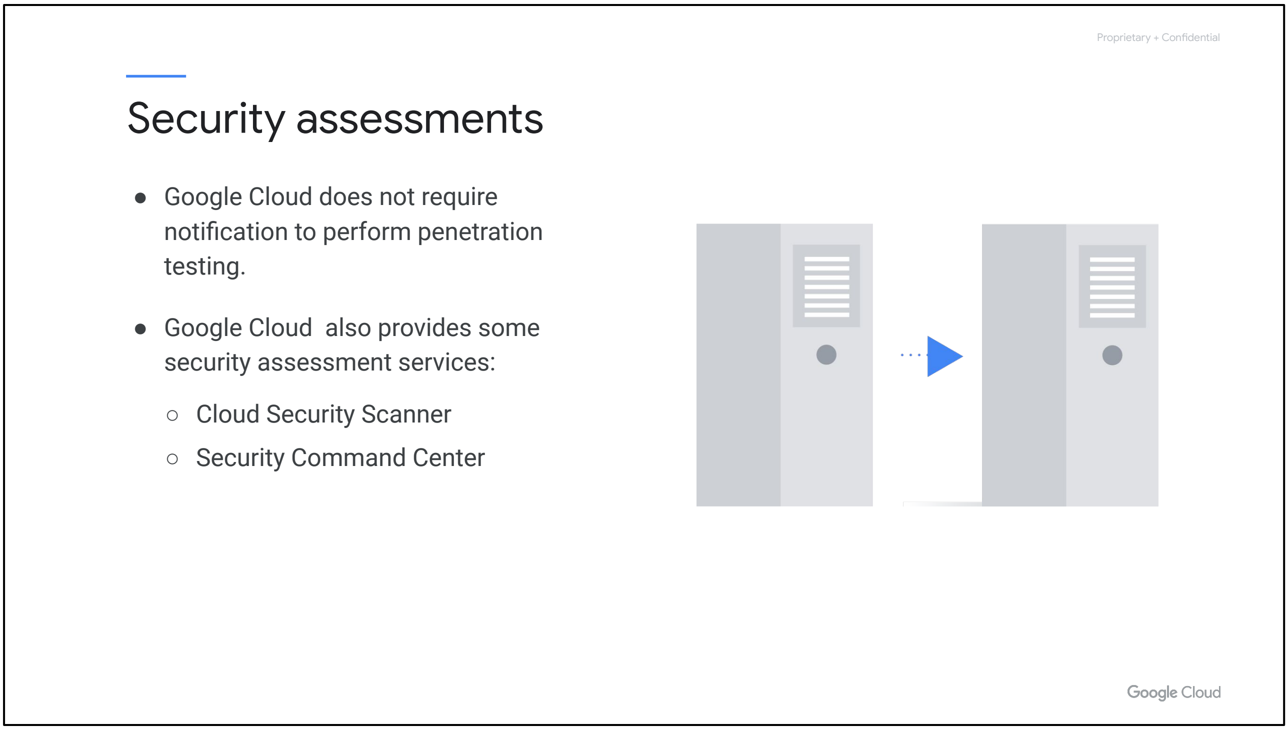
Google Cloud

Finally, another aspect of security responsibilities for customers relates to controlling access to networks. We'll cover the mechanisms Google Cloud provides in more detail in Module 6, but a few examples are:

- **Firewall rules:** allow you to protect VM instances from unapproved connections.
- **Shared VPC**: allows 'centralized network administration' in which a VPC network is defined in a host project and is made available as a centrally shared network for eligible resources in service projects.
- **VPC Service Controls**: enforces a security perimeter with VPC Service Controls to mitigate data exfiltration risks.
- **VPC peering:** enables the resources in your VPCs to communicate across private RFC1918 space, reducing exposure to attack.
- **Cloud VPN:** securely connects your on-premises network to your Cloud VPC network.

The highest trust networks have no direct connectivity to the internet and satisfy strict requirements about when and how they can be used, what sort of traffic can flow into them, and how that traffic is scanned.

Having different VPCs for different workloads can also facilitate location-based access regulatory requirements when combined with VPC service controls.

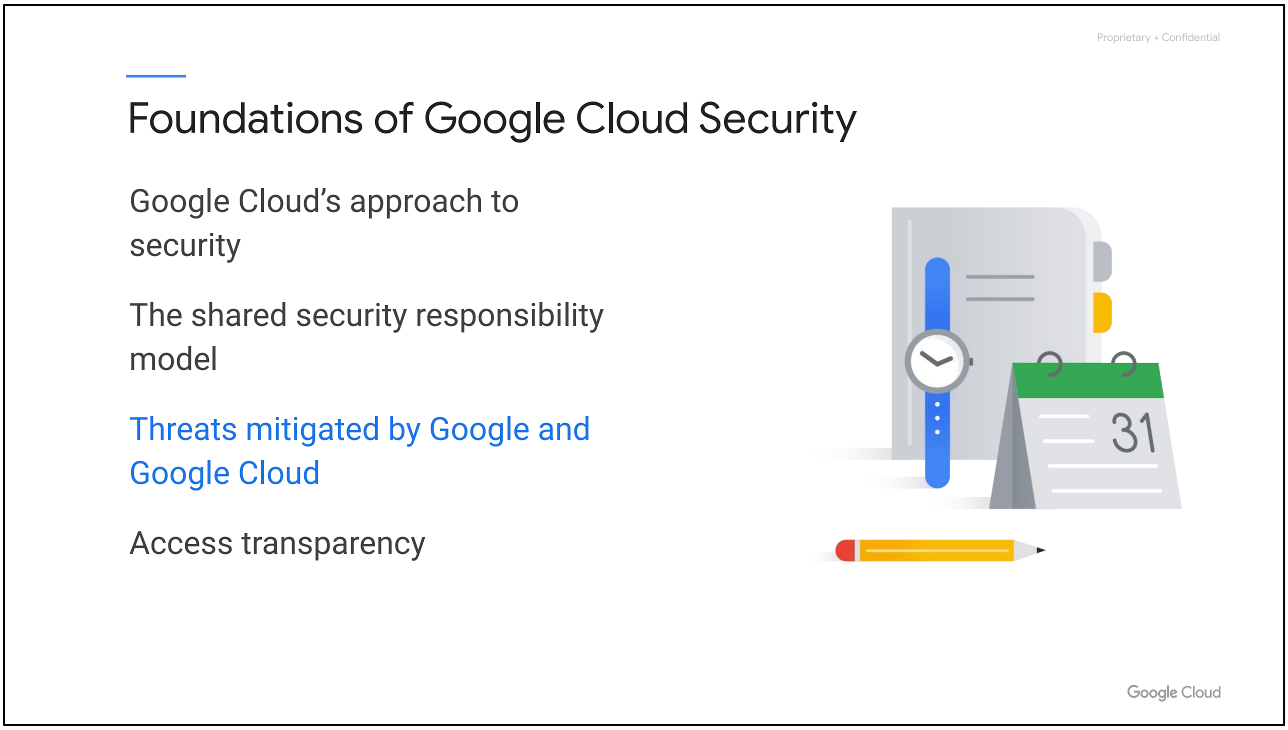


Security assessments

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

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 Security Command Center. We will learn more about these services in more depth later in the course.



Proprietary + Confidential

Foundations of Google Cloud Security

Google Cloud’s approach to security

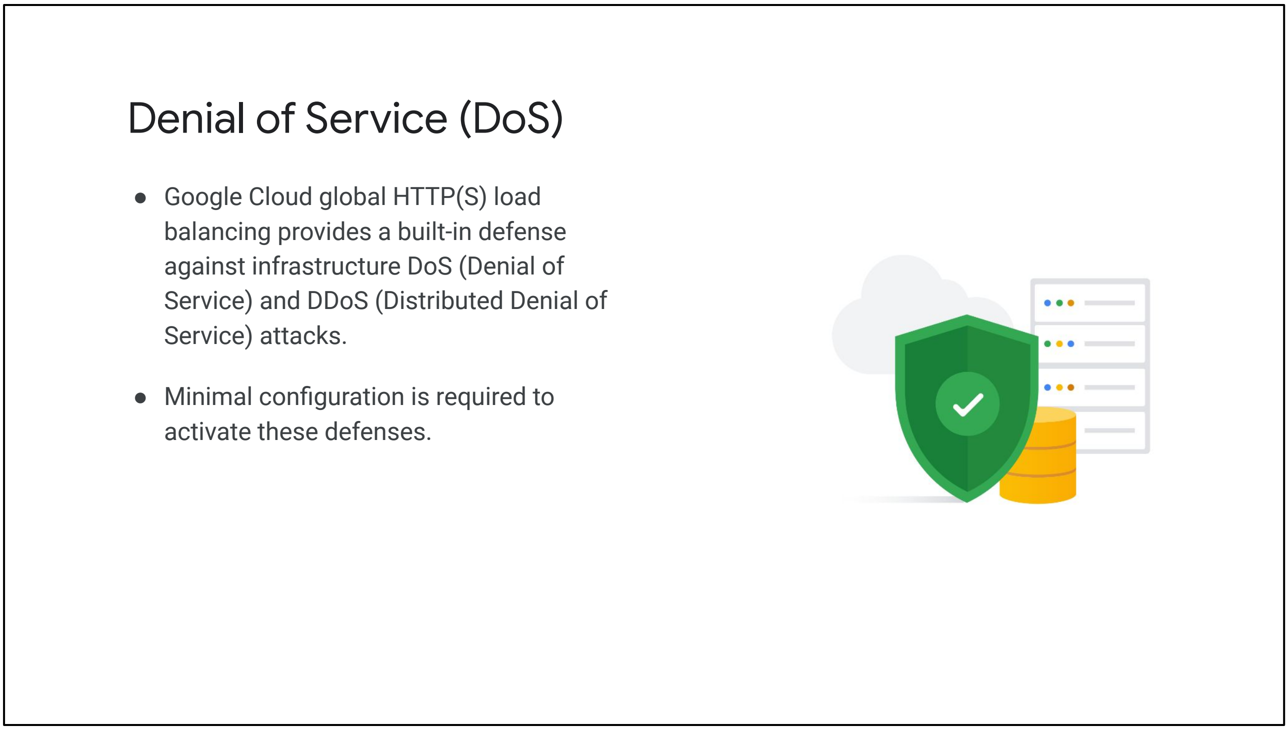
The shared security responsibility model

Threats mitigated by Google and Google Cloud

Access transparency

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.



Denial of Service (DoS)

- Google Cloud global HTTP(S) load balancing provides a built-in defense against infrastructure DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks.
- Minimal configuration is required to activate these defenses.

Some common security threats are DoS and DDoS ….

What is DoS attack? Denial of Service (DoS) attack is a malicious attempt to make a computer or network resource unavailable to its intended users. DoS attacks typically involve flooding the target with so much traffic that it is unable to respond to legitimate requests.

What is DDos attack? In Distributed Denial of Service (DDoS), just like DoS attack, it involves flooding the target so that it is unable to respond to legitimate requests with a difference that the origin of attack is distributed across IP ranges, multiple geo locations, devices and typically originates from a botnet controlled by a third party.

We will handle this in a later module when we will talk about Cloud Armor service.

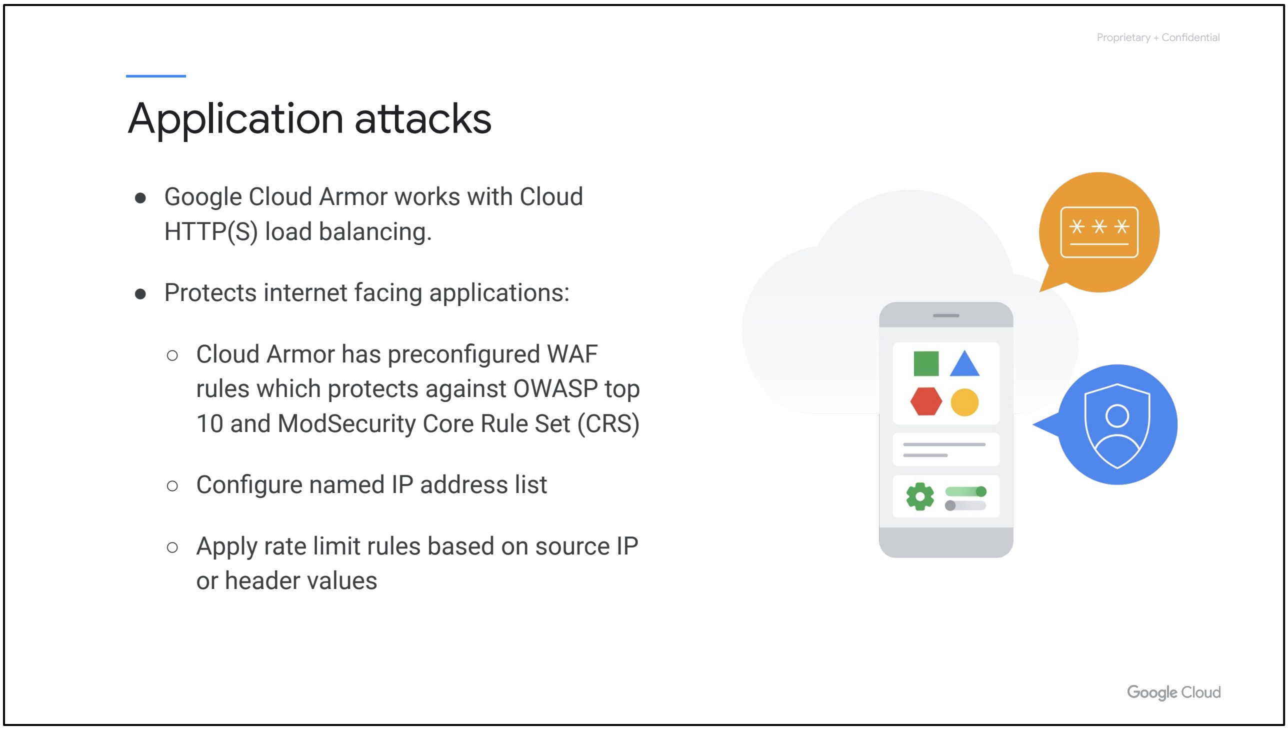
When there is a Denial of Service (or DoS) attack, there is time to isolate it and address it - but Google doesn't stop there.

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 minimal configuration required to activate this DoS defense, when you use Google Cloud Load Balancers to manage your resources!

We will cover DoS attacks and mitigation strategies in more detail later on in this course.



Proprietary + Confidential

Application attacks

- Google Cloud Armor works with Cloud HTTP(S) load balancing.
- Protects internet facing applications:
  - Cloud Armor has preconfigured WAF rules which protects against OWASP top 10 and ModSecurity Core Rule Set (CRS)
  - Configure named IP address list
  - Apply rate limit rules based on source IP or header values

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.

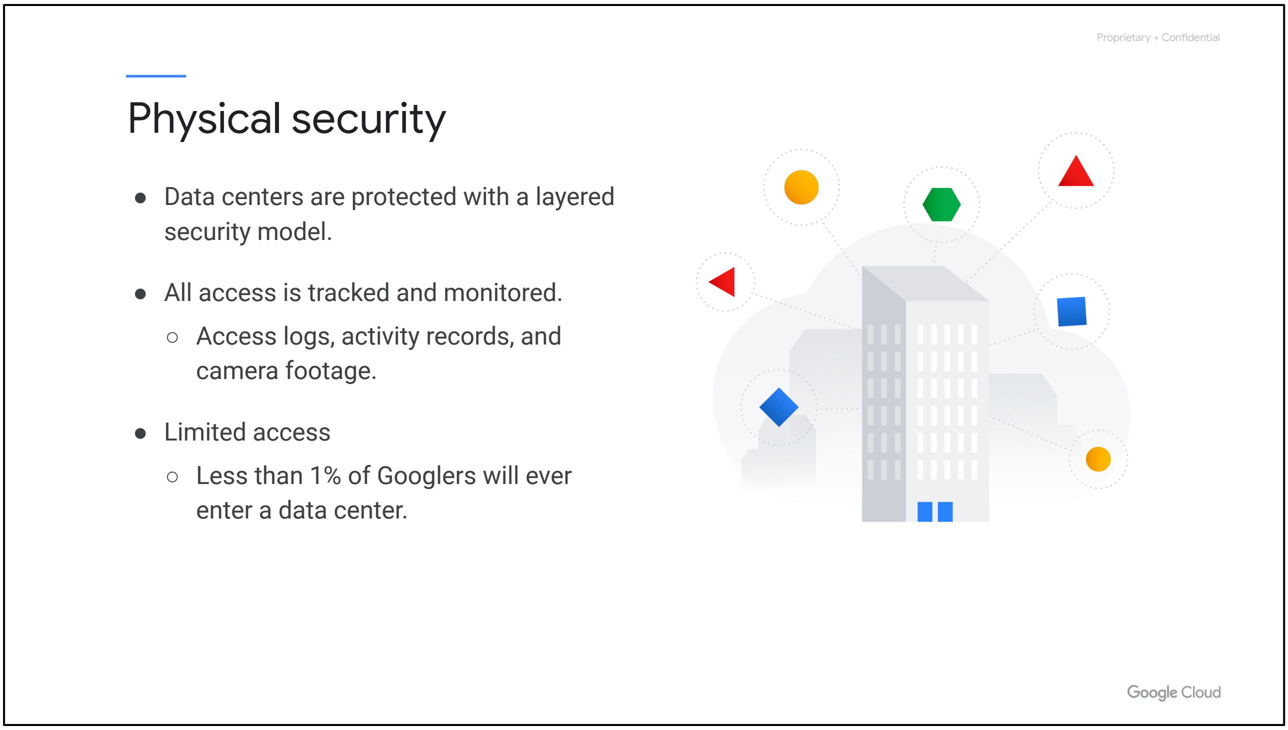
Google Cloud Armor works in conjunction with global HTTP/HTTPS load balancing and enables you to deploy and customize defenses for your internet-facing applications.

It has preconfigured WAF rules and help mitigate the OWASP Top 10 risks. You can manually allowlist or denylist IP addresses or ranges. The named IP address list let you reference IP addresses and IP ranges maintained by third party providers once you subscribe to the Google Cloud Armor Managed Protection Plus service.

You can configure rate based rules to protect the applications from a large volume of requests or volumetric attacks.

We will cover Google Cloud Armor in more detail later on in this course.

Blog link:
cloud.google.com/blog/products/identity-security/cloud-armor-waf-rule-to-help-address-apache-log4j-vulnerability



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

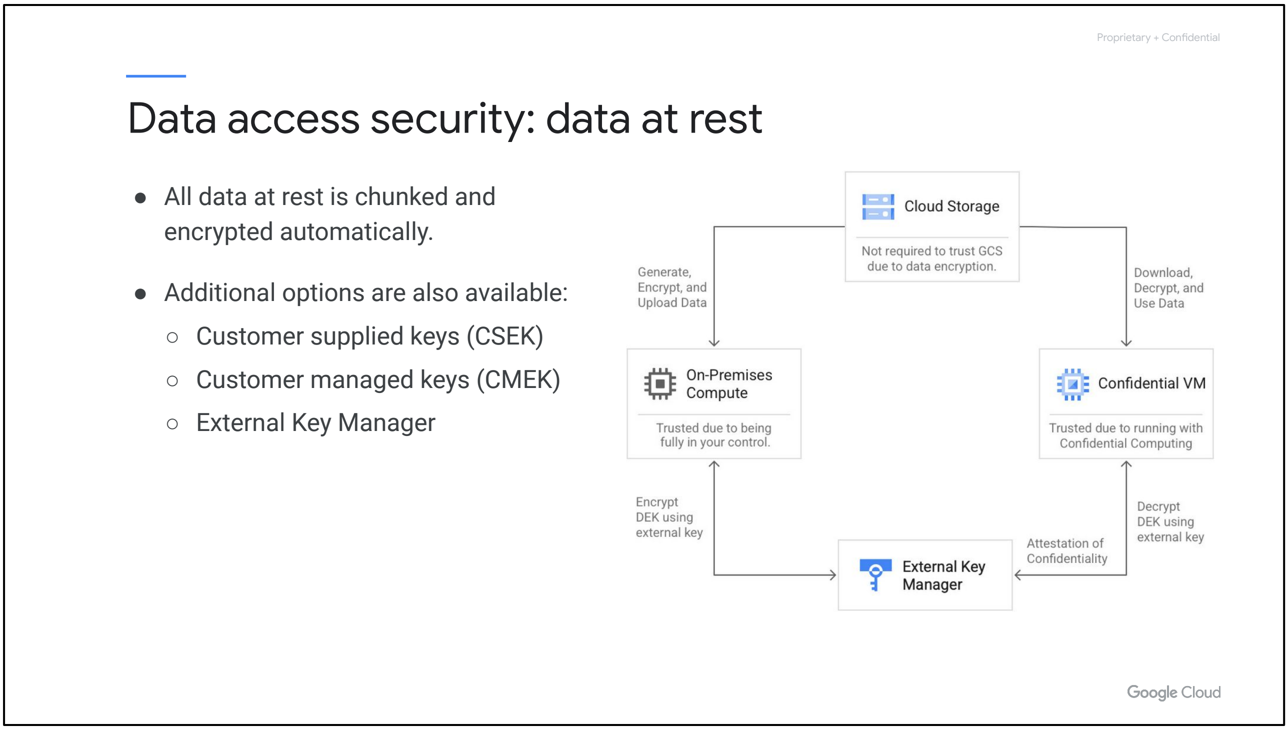
Google's data centers leverage a layered security model and are protected with some of the most advanced physical security controls available today. Some of the controls implemented are:

- 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

For more information on Google's security layers, check out the link in the speaker notes.

- **Link:** google.com/about/datacenters/data-security

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.



Proprietary + Confidential

Data access security: data at rest

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

Cloud Storage

Not required to trust GCS due to data encryption.

Generate, Encrypt, and Upload Data

Download, Decrypt, and Use Data

On-Premises Compute

Trusted due to being fully in your control.

Confidential VM

Trusted due to running with Confidential Computing

Encrypt DEK using external key

Decrypt DEK using external key

Attestation of Confidentiality

External Key Manager

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.

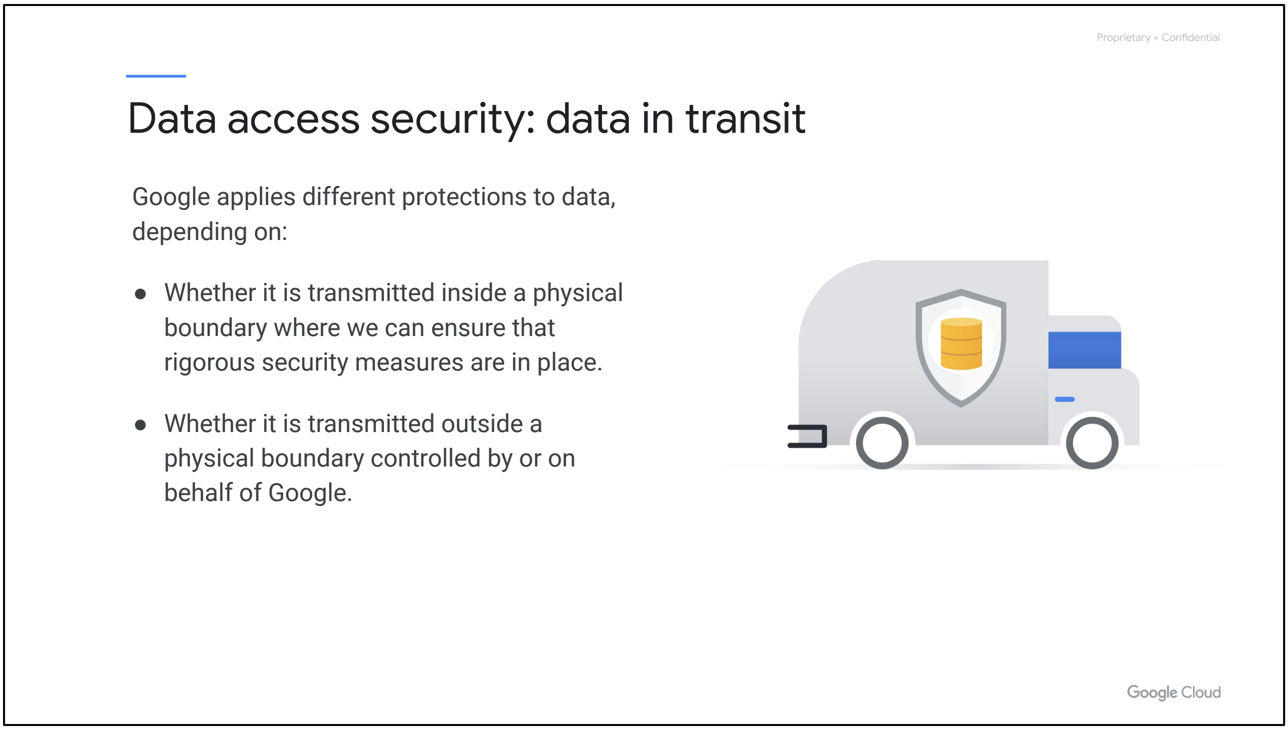
Additional options are also available that allow for customer managed keys and customer supplied keys

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.

You can use solutions such as Cloud External Key Manager (EKM) when encrypting data-at-rest to store and manage keys outside of Google's infrastructure, which the graphic on this slide gives you an example of.

Check out the link for more information on ubiquitous data encryption with Cloud External Key Manager.

- **Link:** cloud.google.com/blog/products/identity-security/ubiquitous-data-encryption-on-google-cloud



Proprietary + Confidential

Data access security: data in transit

Google applies different protections to data, depending on:

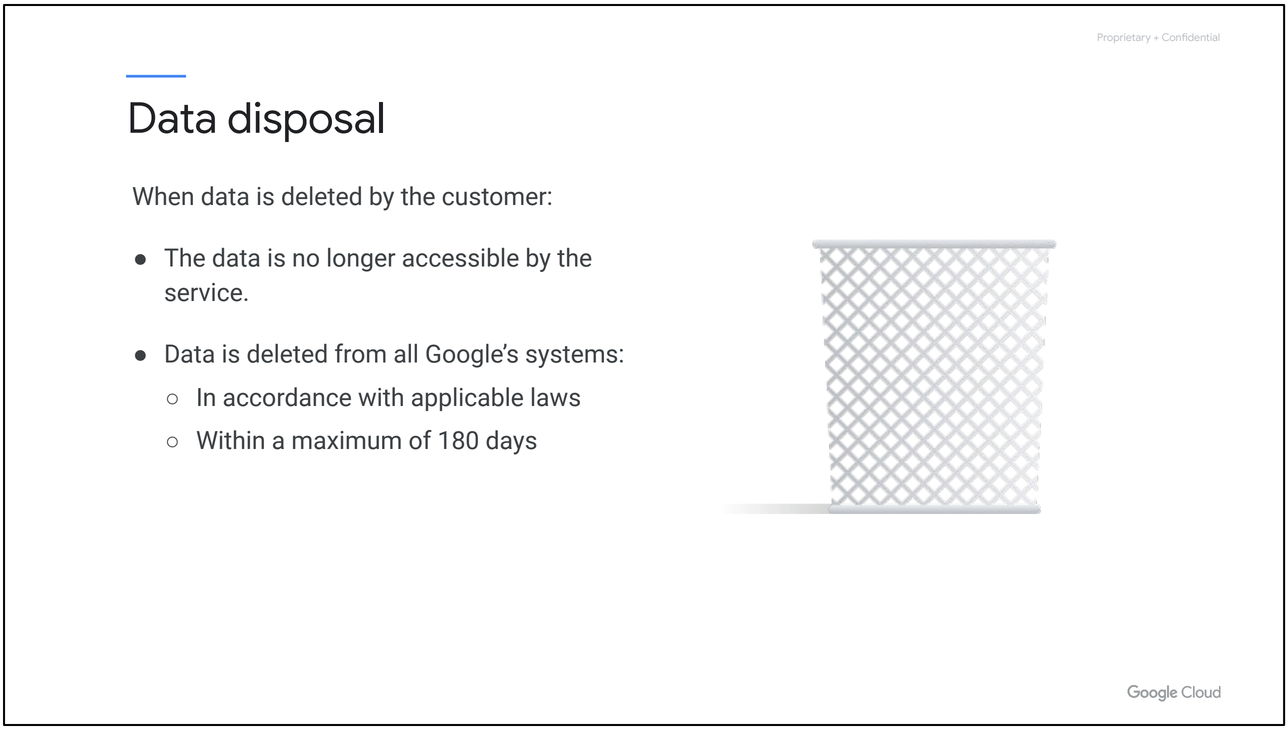
- Whether it is transmitted inside a physical boundary where we can ensure that rigorous security measures are in place.
- Whether it is transmitted outside a physical boundary controlled by or on behalf of Google.

Google Cloud

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.



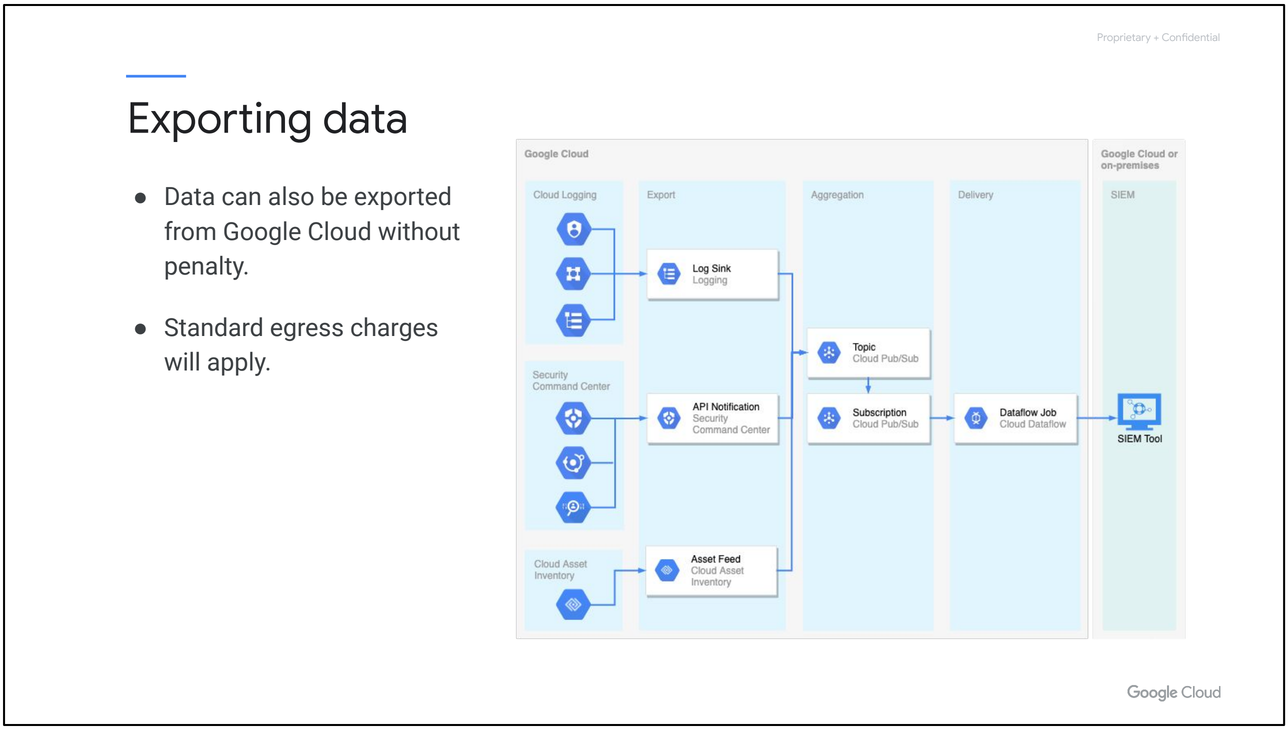
Data disposal

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 then be deleted from all of 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.



Proprietary + Confidential

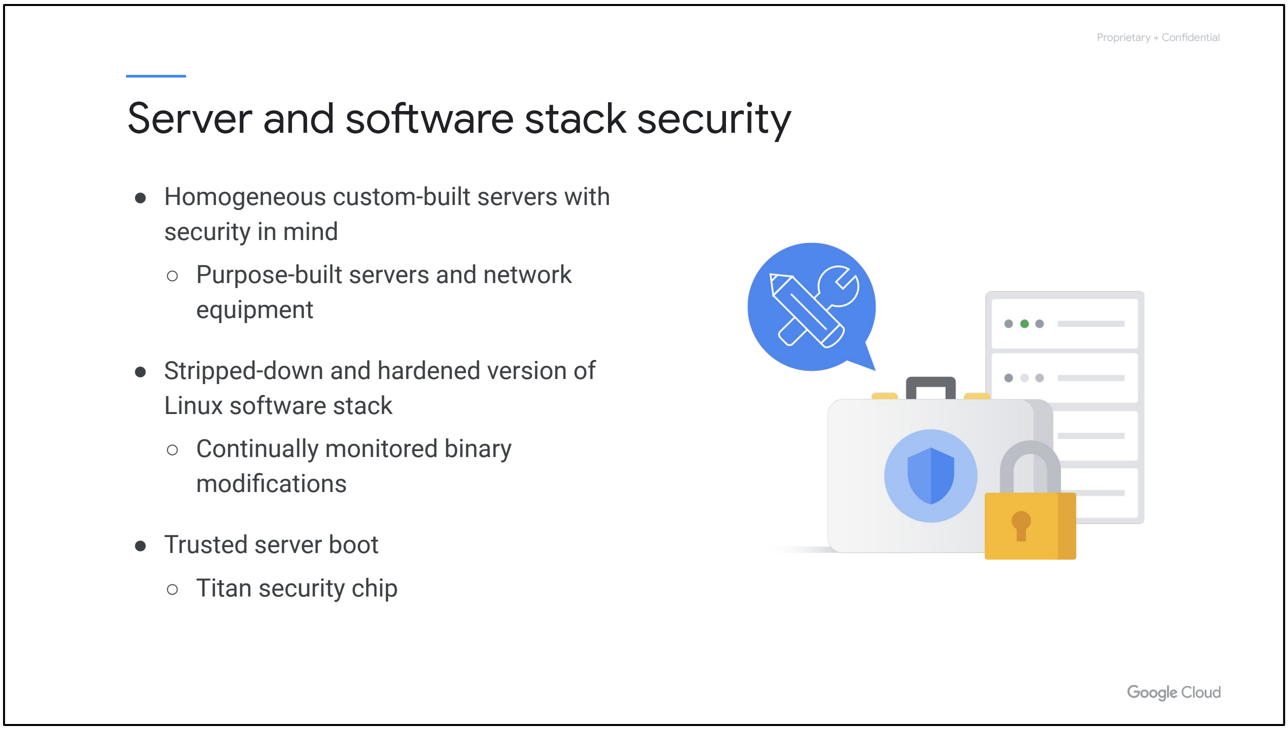
Exporting data

- 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.



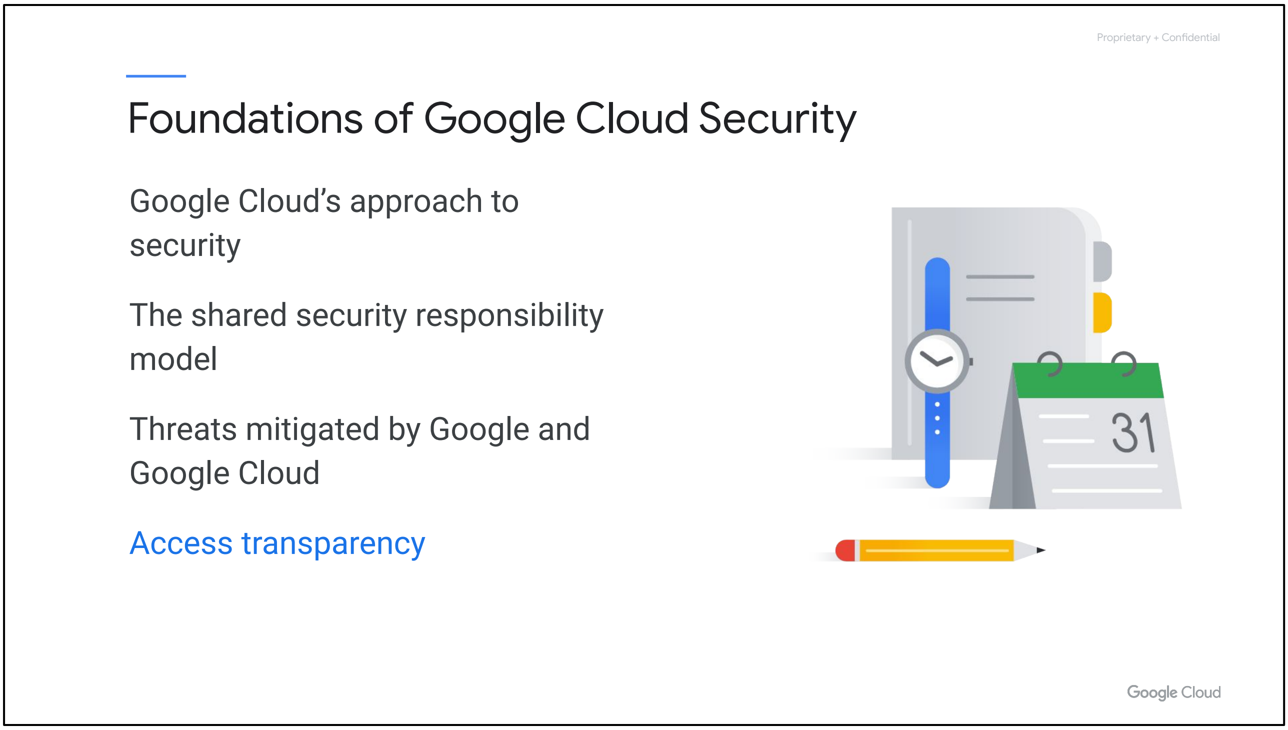
Server and software stack security

- 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 reduce its 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.



Proprietary + Confidential

Foundations of Google Cloud Security

Google Cloud’s approach to security

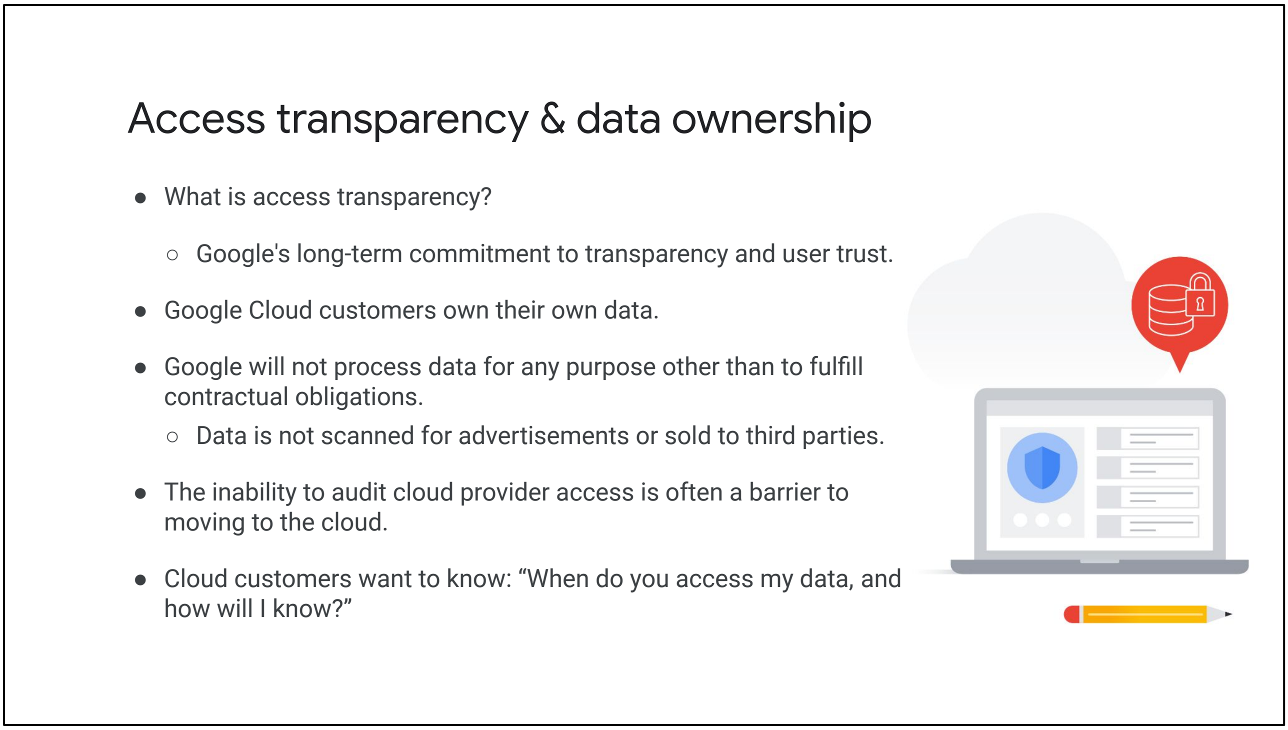
The shared security responsibility model

Threats mitigated by Google and Google Cloud

Access transparency

Google Cloud

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.



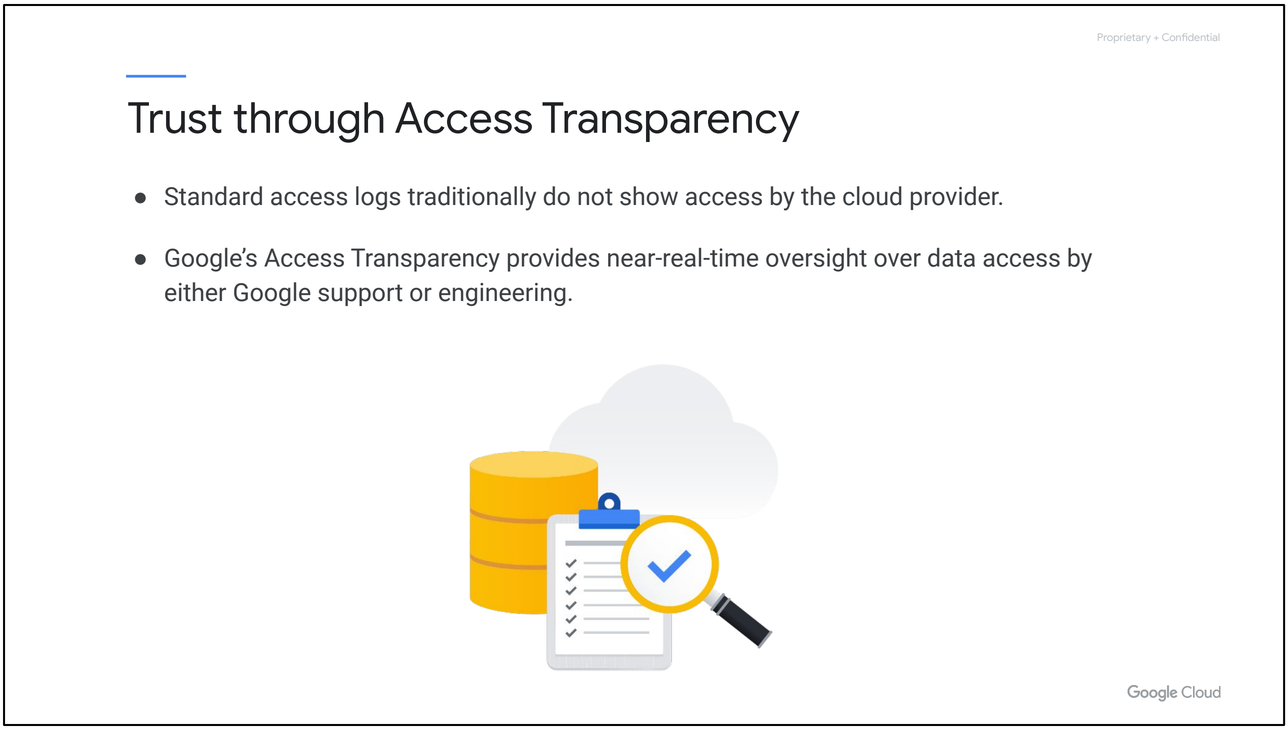
Access transparency & data ownership

- What is access transparency?
  - Google's long-term commitment to transparency and user trust.
- 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?”

So, what is access transparency? At a high level, it is Google's long-term commitment to transparency and user trust.

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.



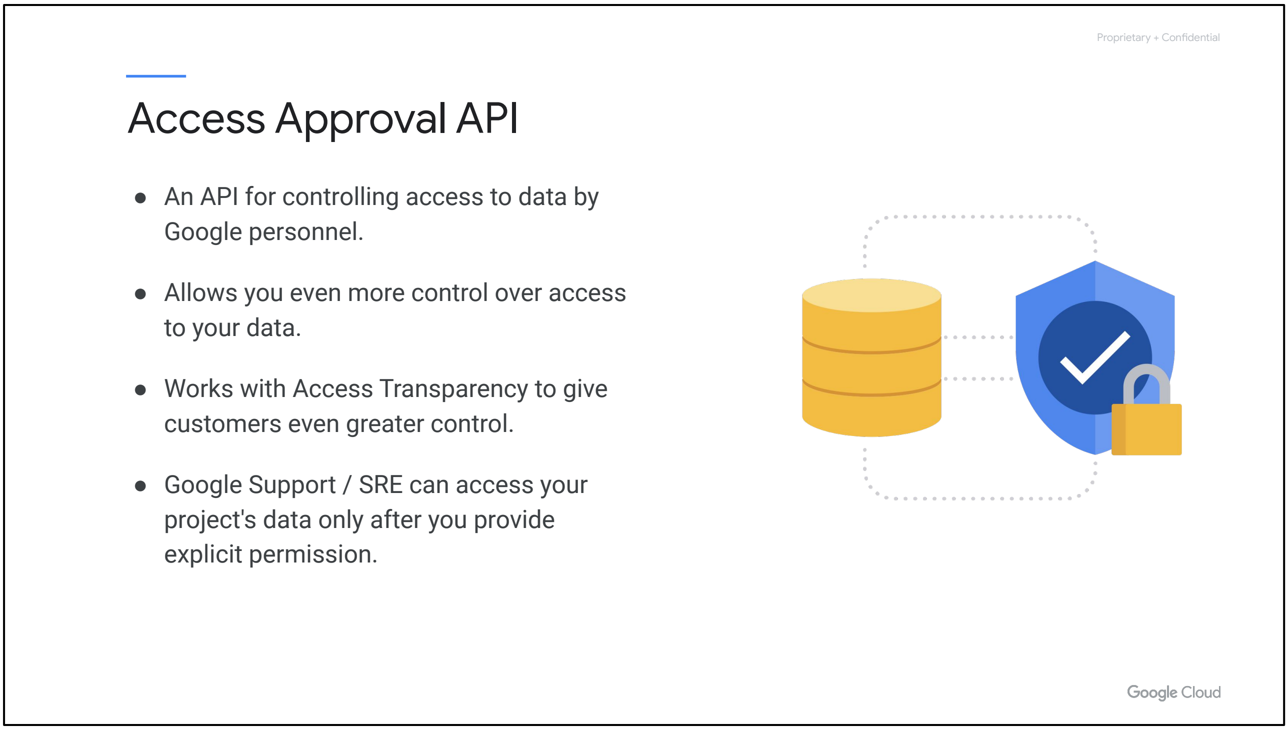
Trust through Access Transparency

- 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.

Google also provides customer trust through access transparency, which come in two flavors:

- **Standard access logs**
  - Traditionally, cloud providers do not provide services or features to illustrate access.
  - 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.

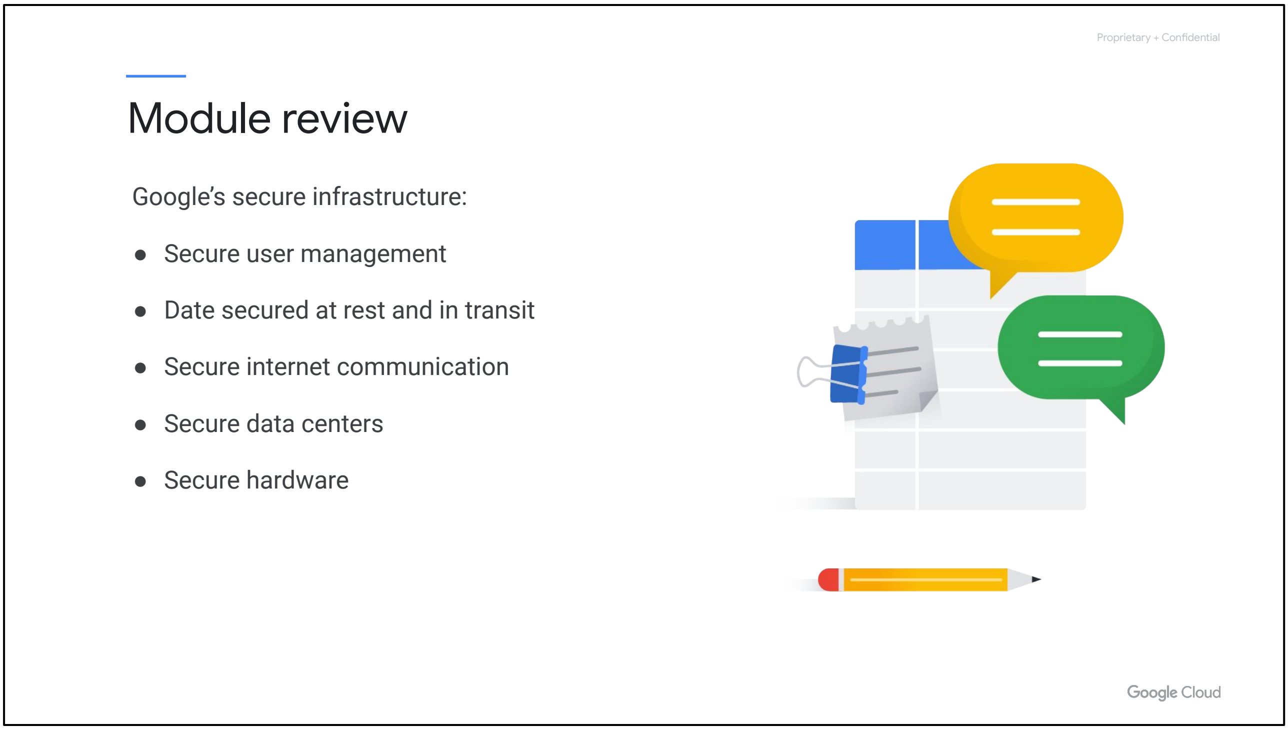


Access Approval API

- An API for controlling access to data by Google personnel.
- Allows you even more control over access to your data.
- Works with Access Transparency to give customers even greater control.
- Google Support / SRE can access your project's data only after you provide explicit permission.

An API for controlling access to data by Google personnel.

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



Module review

Google's secure infrastructure:

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

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.