Module 5

Trust and Security with Google Cloud

Lessons

01 Trust and security in the cloud

02 Google's trusted infrastructure

03 Google Cloud's trust principles and compliance

Welcome to module 5, "Trust and Security with Google Cloud." At Google Cloud, we understand the responsibility that comes with hosting, serving, and safeguarding our customers' valuable data. As organizations increasingly migrate their data and applications to the cloud, it becomes crucial to address the emerging security challenges. Trust and security lie at the heart of our product design and development philosophy.

In this section you'll learn about:

- Fundamental cloud security concepts.
- The business value of Google's multilayered approach to infrastructure security.
- How Google Cloud earns and maintains customer trust in the cloud.

Module 5

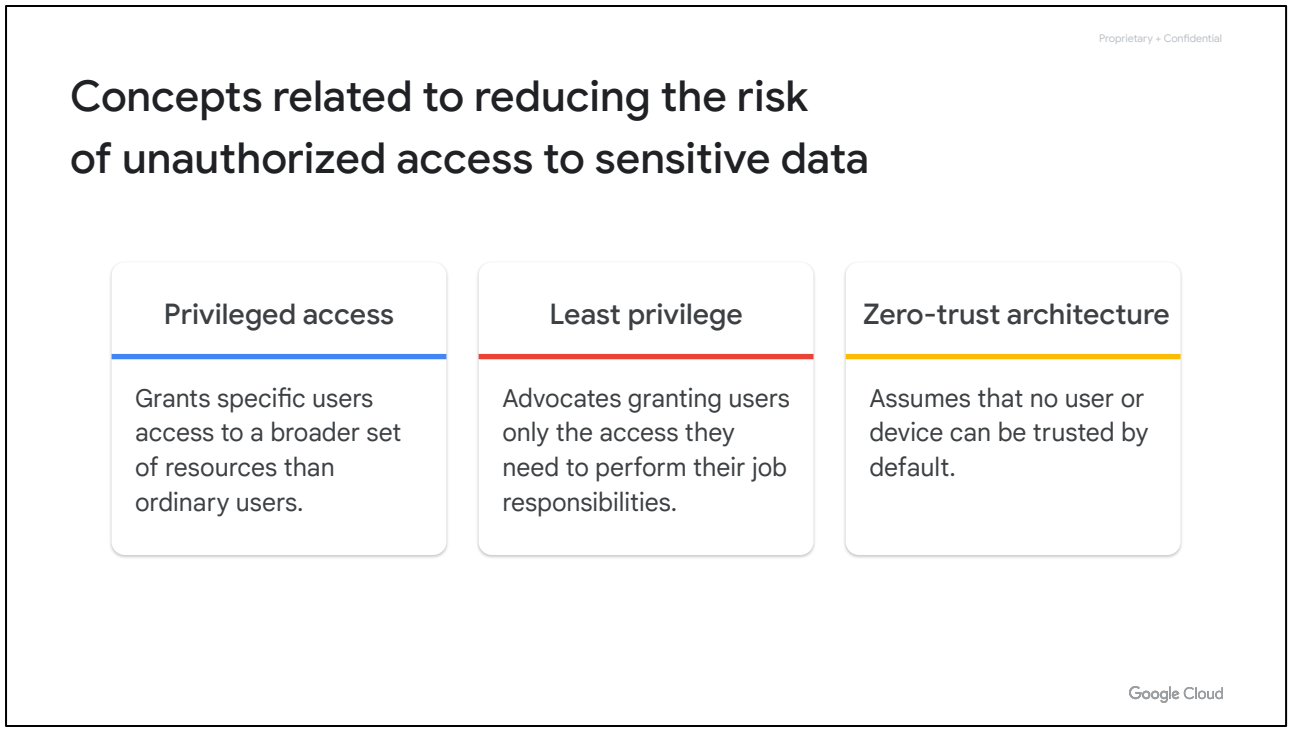
Trust and Security with Google Cloud

Lessons

The rise of cloud computing has transformed the way that organizations store, process, and manage their data. With this increased reliance on the cloud, the need for robust security measures has become essential. Securing data, applications, and infrastructure in the cloud is a complex and ever-evolving challenge. As new threats and vulnerabilities emerge, organizations must stay ahead of the curve and adapt their security strategies to mitigate risks effectively.

Key security terms and concepts

Let’s get started by defining some key security terms and concepts.



The first three concepts relate to reducing the risk of unauthorized access to sensitive data.

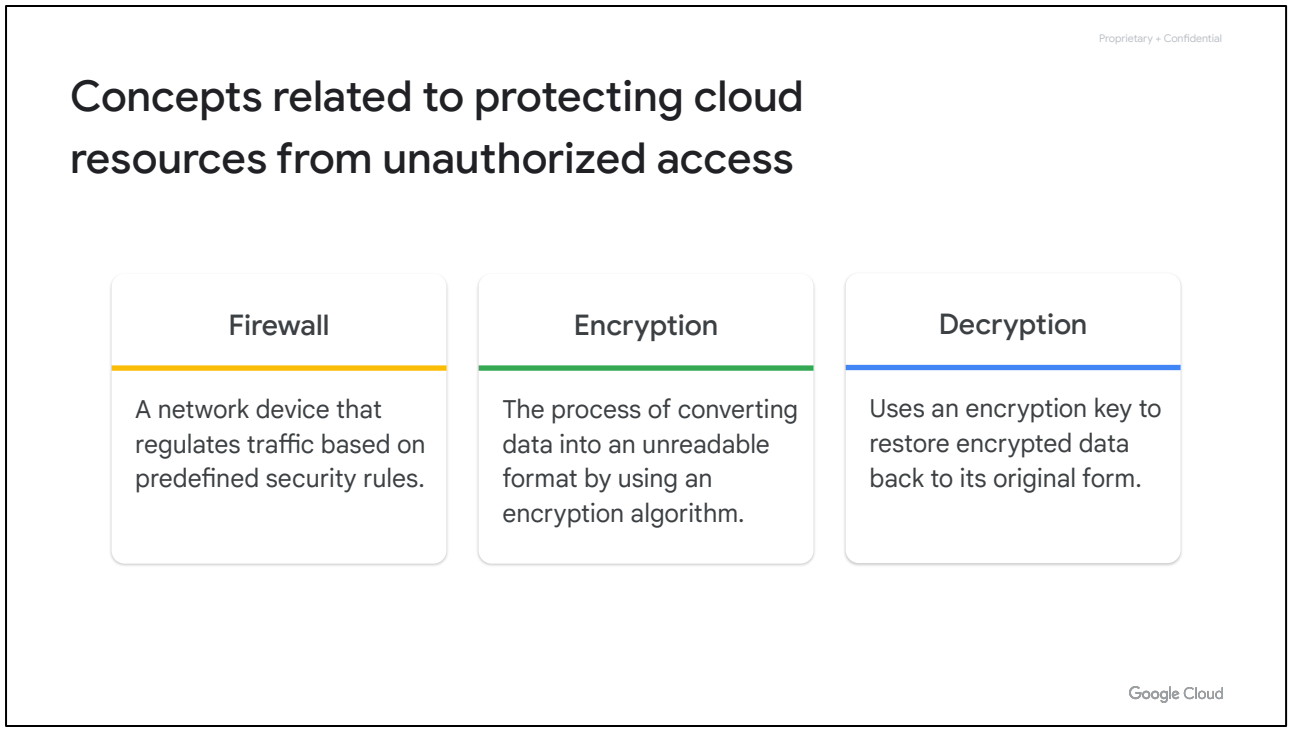
1. The **privileged access** security model grants specific users access to a broader set of resources than ordinary users. For example, a system administrator may have privileged access to perform tasks such as troubleshooting and data restoration. However, the misuse of privileged access can pose risks, so it's essential to manage and monitor such access carefully.

2. The **least privilege** security principle advocates granting users only the access they need to perform their job responsibilities. By providing the minimum required access, organizations can reduce the risk of unauthorized access to sensitive data. For instance, a sales representative might only need access to a customer relationship management (CRM) system without requiring access to other systems like payroll or finance.

3. The **zero-trust architecture** security model assumes that no user or device can be trusted by default. Every user and device must be authenticated and authorized before accessing resources. Zero-trust architecture helps ensure robust security by implementing strict access controls and continuously verifying user identities.

These next three concepts relate to how an organization can protect itself from cyber threats.

1. **Security by default** is a principle that emphasizes integrating security measures into systems and applications from the initial stages of development. By prioritizing security throughout the entire process, organizations can establish a strong security foundation in their cloud environments.
2. **Security posture** refers to the overall security status of a cloud environment. It indicates how well an organization is prepared to defend against cyber attacks by evaluating their security controls, policies, and practices.
3. **Cyber resilience** refers to an organization's ability to withstand and recover quickly from cyber attacks. It involves identifying, assessing, and mitigating risks, responding to incidents effectively, and recovering from disruptions quickly.



Finally, let's explore essential security measures to protect cloud resources from unauthorized access:

1. A **firewall** is a network device that regulates traffic based on predefined security rules. You can think of a firewall like a security guard for a network. It follows certain rules to decide which traffic is allowed to enter or leave a network. These rules help keep unauthorized people or harmful things away from important cloud resources, such as servers, databases, and applications. Following our previous analogy, a security guard checks everyone who wants to enter and only lets in those who have permission. Similarly, a firewall checks the incoming and outgoing traffic in a network and only allows the ones that are safe and authorized.

2. **Encryption** is the process of converting data into an unreadable format by using an encryption algorithm.

3. **Decryption**, however, is the reverse process that uses an encryption key to restore encrypted data back to its original form. Safeguarding the encryption key is crucial, because it holds the secret algorithm necessary for decrypting the data.

Quiz

Question

Which security principle advocates granting users only the access they need to perform their job responsibilities?

A. Security by default
B. Least privilege
C. Zero-trust architecture
D. Privileged access

Which security principle advocates granting users only the access they need to perform their job responsibilities?

A. Security by default
B. Least privilege
C. Zero-trust architecture
D. Privileged access

Quiz

Answer

Which security principle advocates granting users only the access they need to perform their job responsibilities?

A. Security by default

B. Least privilege 

C. Zero-trust architecture

D. Privileged access

The correct answer is B.

A. Security by default
   - Why this is the **incorrect** answer: This principle emphasizes building security into products and systems from the ground up, rather than focusing on user access levels.

B. Least privilege
   - Why this is the **correct** answer: The principle of least privilege limits users' access to only the systems, data, and permissions absolutely necessary for them to carry out their assigned tasks.

C. Zero-trust architecture
   - Why this is the **incorrect** answer: Zero-trust is a security framework that assumes no user or device should be inherently trusted, even inside the network perimeter. While related to least privilege, it's a broader architectural model.

D. Privileged access
   - Why this is the **incorrect** answer: This refers to elevated permissions that allow users or accounts to perform administrative tasks; the principle of least privilege aims to minimize the use of privileged access whenever possible.

Quiz

Question

Which definition best describes a firewall?

A. A security model that assumes no user or device can be trusted by default

B. A set of security measures designed to protect a computer system or network from cyber attacks

C. A software program that encrypts data to make it unreadable to unauthorized users

D. A network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules

Which definition best describes a firewall?

A. A security model that assumes no user or device can be trusted by default
B. A set of security measures designed to protect a computer system or network from cyber attacks
C. A software program that encrypts data to make it unreadable to unauthorized users
D. A network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules

Quiz

Answer

Which definition best describes a firewall?

A. A security model that assumes no user or device can be trusted by default

B. A set of security measures designed to protect a computer system or network from cyber attacks

C. A software program that encrypts data to make it unreadable to unauthorized users

D. A network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules 

The correct answer is D.

A. A security model that assumes no user or device can be trusted by default
   - Why this is the **incorrect** answer: This describes the zero-trust security model, not specifically a firewall.

B. A set of security measures designed to protect a computer system or network from cyber attacks
   - Why this is the **incorrect** answer: This definition is too broad, as it encompasses many security tools and practices beyond just firewalls.

C. A software program that encrypts data to make it unreadable to unauthorized users
   - Why this is the **incorrect** answer: This describes encryption software, which is a security tool but distinct from a firewall's primary function.

D. A network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules
   - Why this is the **correct** answer: A firewall acts as a barrier between a trusted internal network and untrusted external networks (like the internet), analyzing traffic and selectively blocking or allowing it based on configured rules.

Cloud security components

Now let’s shift our focus to explore the components that make up a cloud security model and how they contribute to a robust security posture in today's digital landscape.

Three essential aspects of security

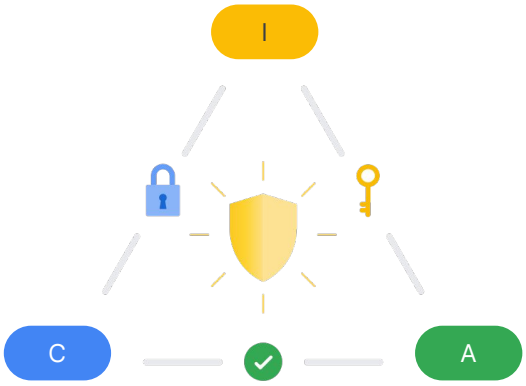
Confidentiality

Integrity

Availability

We'll first explore three essential aspects of security: **Confidentiality**, **Integrity**, and **Availability**. These are **"C" "I" "A"**

The “CIA triad”



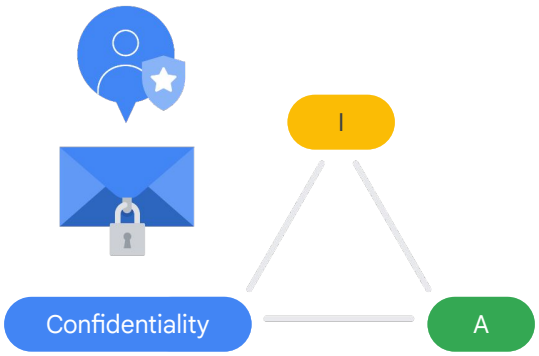
The CIA triad emphasizes:

- The importance of protecting sensitive information.
- Ensuring data accuracy and trustworthiness.
- Maintaining uninterrupted access to resources and services.

These three principles form the foundation of the “CIA Triad”, a widely used model for developing effective security systems.

The CIA triad emphasizes the importance of protecting sensitive information, ensuring data accuracy and trustworthiness, and maintaining uninterrupted access to resources and services. By understanding and implementing measures to address these aspects, organizations can establish a strong security framework to safeguard their digital assets.

Confidentiality

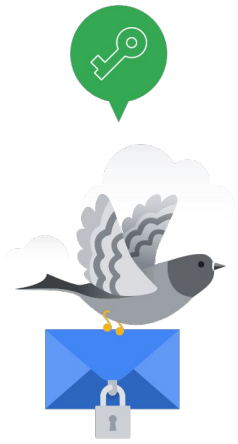


Confidentiality is about keeping important information safe and secret.

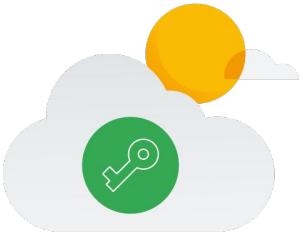
It ensures that only authorized people can access sensitive data, no matter where it's stored or sent.

Confidentiality is about keeping important information safe and secret. It ensures that only authorized people can access sensitive data, no matter where it's stored or sent. Confidentiality is of utmost importance in the cloud, as sensitive information stored and transmitted across cloud environments must be protected from unauthorized access or disclosure.

Confidentiality + encryption



Encryption



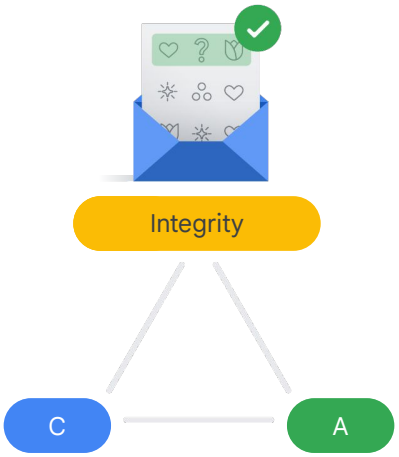
Encryption techniques and encryption keys help ensure that only authorized individuals can access and decrypt sensitive data.

Encryption plays a crucial role in ensuring confidentiality in the cloud. By using encryption techniques and safeguarding encryption keys, organizations can ensure that only authorized individuals can access and decrypt sensitive data, effectively mitigating the risk of data breaches in the cloud.

Integrity

Integrity means keeping data accurate and trustworthy.

It ensures that information doesn't get changed or corrupted, no matter where it's stored or how it's moved around.



Integrity means keeping data accurate and trustworthy. It ensures that information doesn't get changed or corrupted, no matter where it's stored or how it's moved around. You can think of it like making sure a message doesn't get altered during delivery.

Integrity in the cloud involves ensuring the accuracy and trustworthiness of data throughout its lifecycle.

Data integrity controls let organizations verify the authenticity and reliability of their data in the cloud

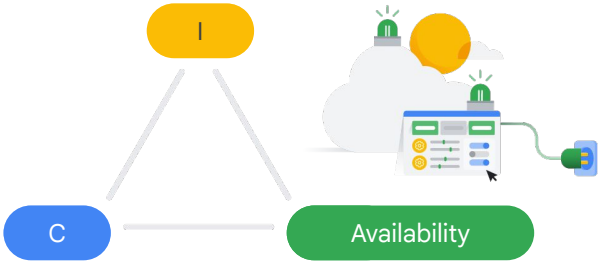
Data integrity controls

Help prevent unauthorized modifications or tampering

Ensure the integrity of critical information stored and processed

Implementing data integrity controls, such as checksums or digital signatures, enables organizations to verify the authenticity and reliability of their data in the cloud. This helps prevent unauthorized modifications or tampering, ensuring the integrity of critical information stored and processed in cloud environments.

Availability



Availability is making sure that cloud systems and services are always accessible and ready for use by the right people when needed.

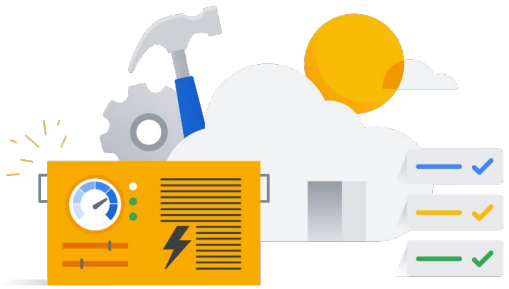
It's like having a reliable electricity supply that never goes out.

Availability is all about making sure that cloud systems and services are always accessible and ready for use by the right people when needed. It's like having a reliable electricity supply that never goes out.

Availability measures can ensure that systems and applications in the cloud remain accessible

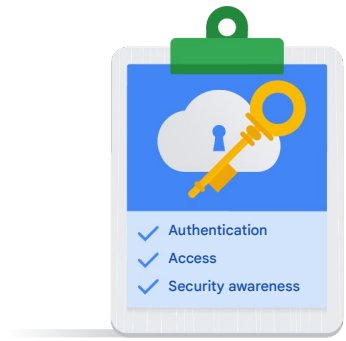
Cloud environments must be designed with:

- Redundancy
- Failover mechanisms
- Disaster recovery plans



Cloud environments must be designed with redundancy, failover mechanisms, and disaster recovery plans to maximize availability and minimize downtime. By implementing these measures, organizations can ensure that their systems and applications in the cloud remain accessible whenever needed, promoting business continuity even in the face of potential disruptions.

Control



Control

The measures and processes implemented to manage and mitigate security risks.

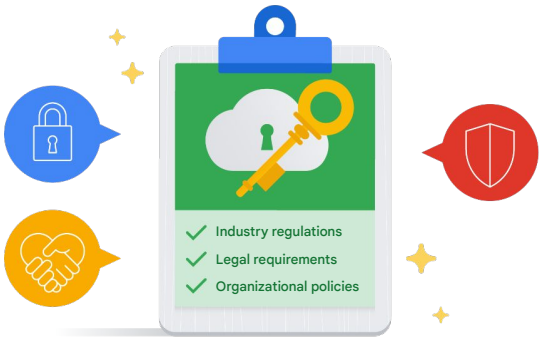
Protect against unauthorized access, misuse, and potential threats.

In addition to the CIA triad, two important cloud security components are control and compliance.

Control refers to the measures and processes implemented to manage and mitigate security risks. It involves establishing policies, procedures, and technical safeguards to protect against unauthorized access, misuse, and potential threats.

Control measures in the cloud include implementing robust authentication mechanisms, access restrictions, and security awareness training. These measures help organizations manage and mitigate security risks associated with cloud-based systems. By ensuring that only authorized individuals have access to sensitive data and systems in the cloud, organizations can reduce the risk of data breaches and unauthorized activities.

Compliance



- Compliance relates to adhering to industry regulations, legal requirements, and organizational policies.
- It involves ensuring that security practices and measures align with established standards and guidelines.
- Cloud providers often offer compliance frameworks and certifications.

Finally, **compliance** relates to adhering to industry regulations, legal requirements, and organizational policies. It involves ensuring that security practices and measures align with established standards and guidelines.

Meeting compliance standards in the cloud demonstrates an organization's commitment to data privacy and security, building trust with stakeholders, and minimizing legal and financial risks.

Cloud providers often offer compliance frameworks and certifications that organizations can leverage to meet their regulatory obligations.

The benefits of integrating a comprehensive cloud security model

Organizations can establish a strong foundation to:

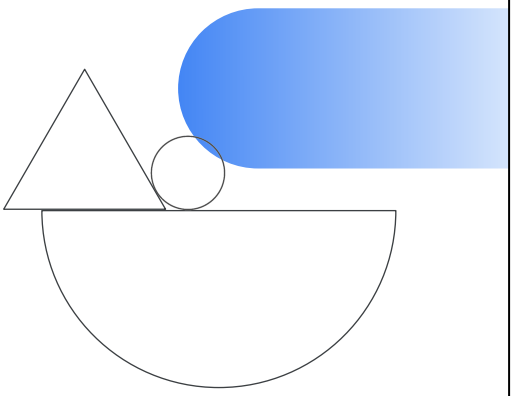
- Protect their data
- Maintain data integrity
- Ensure continuous access to critical resources

By integrating these principles into a comprehensive cloud security model, organizations can establish a strong foundation for protecting their data, maintaining data integrity, and ensuring continuous access to critical resources.

Activity

5 min | Class | Page 24

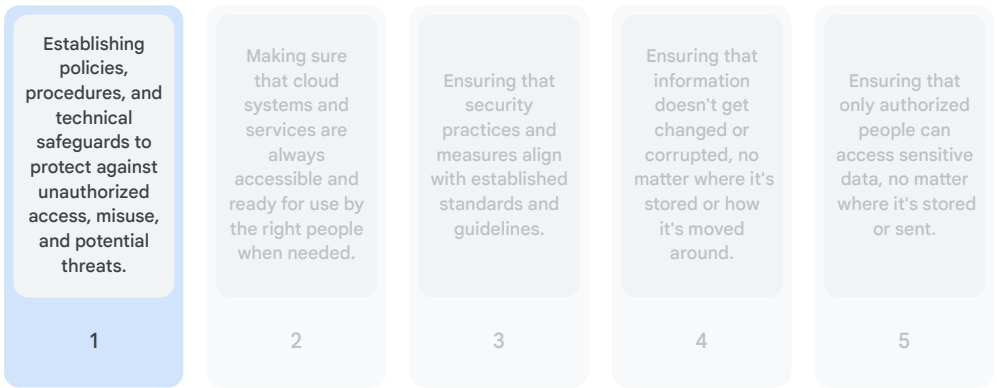
Identify the cloud security concept that matches the description.



Let's put what you've just learned into practice. On the slides that follow, you'll see a list of cloud security concepts. In your workbooks, identify the cloud security concept that matches the description.

Activity

Identify the cloud security concept that matches the description.



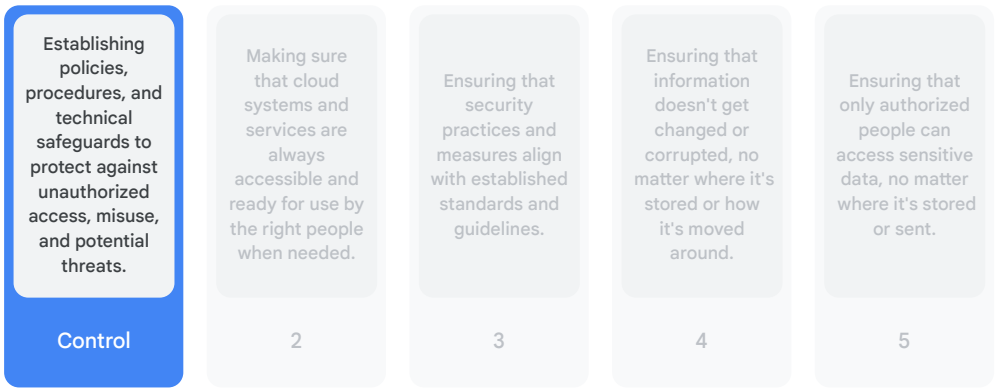
Let’s start with the first column.

What cloud security concept is focused on establishing policies, procedures, and technical safeguards to protect against unauthorized access, misuse, and potential threats?

Options include: Compliance, Integrity, Availability, Control, Confidentiality

Activity

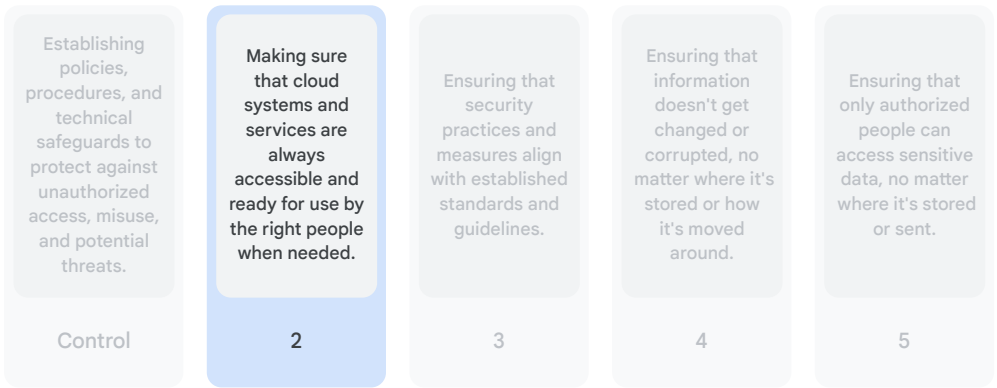
Identify the cloud security concept that matches the description.



The correct answer is **control**. Now let's move on to the second column.

Activity

Identify the cloud security concept that matches the description.

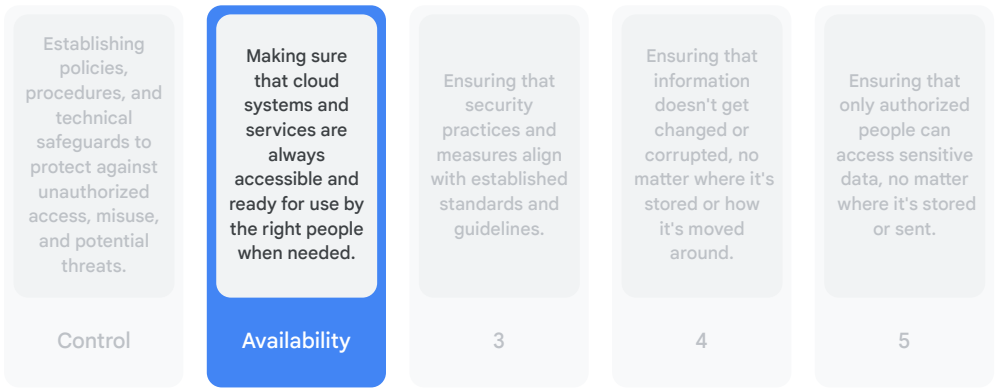


What cloud security concept is focused on making sure that cloud systems and services are always accessible and ready for use by the right people when needed?

Options include: Compliance, Integrity, Availability, Control, Confidentiality

Activity

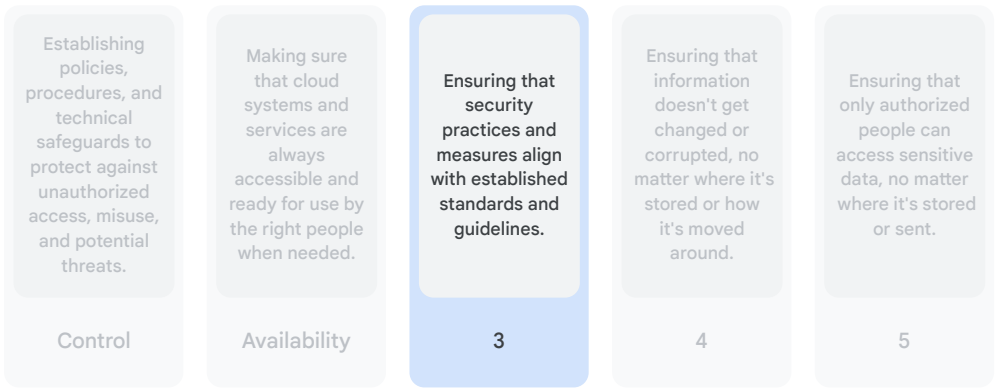
Identify the cloud security concept that matches the description.



The correct answer is **availability**. Now let's move on to the third column.

Activity

Identify the cloud security concept that matches the description.

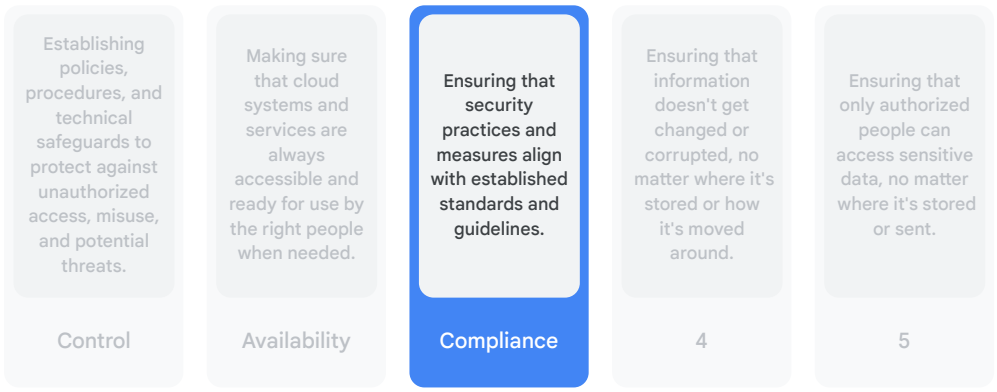


What cloud security concept is focused on ensuring that security practices and measures align with established standards and guidelines?

Options include: Compliance, Integrity, Availability, Control, Confidentiality

Activity

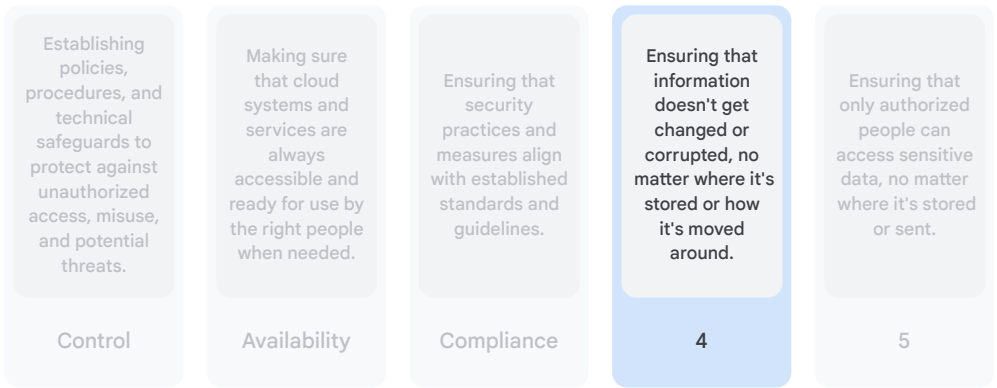
Identify the cloud security concept that matches the description.



The correct answer is **compliance**. Now let's move on to the fourth column.

Activity

Identify the cloud security concept that matches the description.

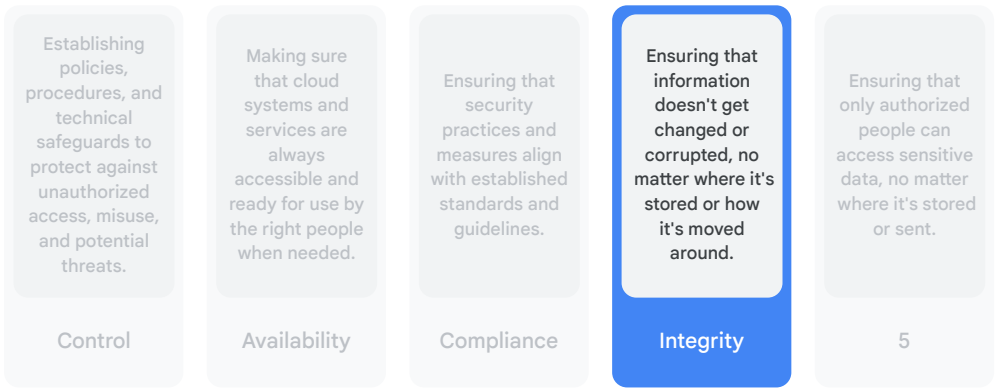


What cloud security concept is focused on ensuring that information doesn't get changed or corrupted, no matter where it's stored or how it's moved around?

Options include: Compliance, Integrity, Availability, Control, Confidentiality

Activity

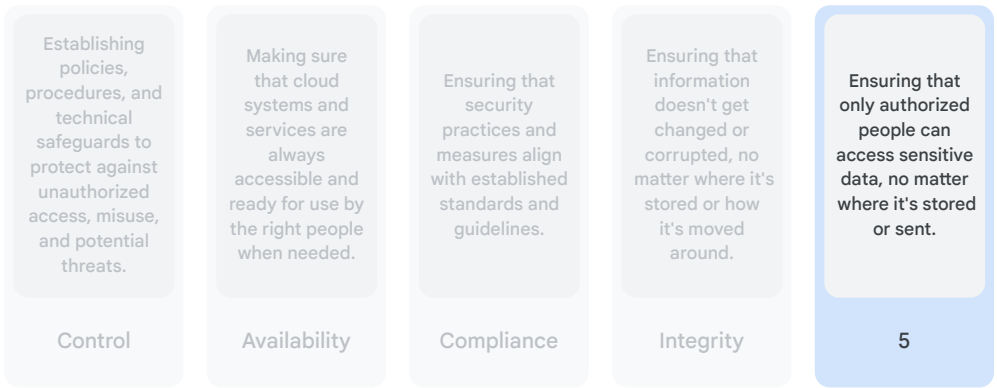
Identify the cloud security concept that matches the description.



The correct answer is **integrity**. Let’s finish up with fifth column.

Activity

Identify the cloud security concept that matches the description.

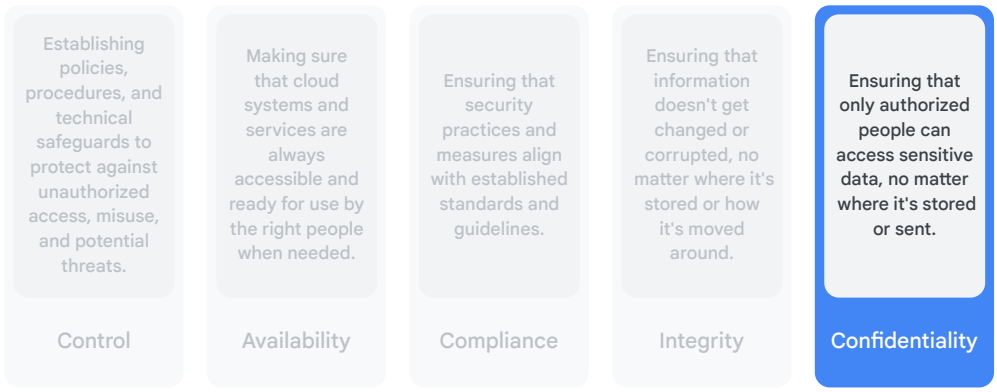


What cloud security concept is focused on ensuring that only authorized people can access sensitive data, no matter where it's stored or sent?

Options include: Compliance, Integrity, Availability, Control, Confidentiality

Activity

Identify the cloud security concept that matches the description.



The correct answer is **confidentiality**.

Cybersecurity threats

New risks have emerged that require enhanced security measures

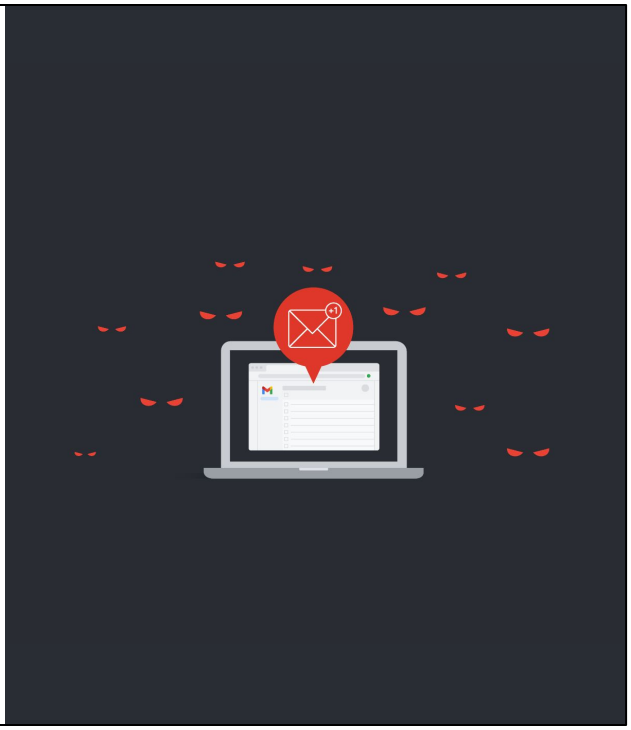
In the past, businesses heavily relied on their own infrastructure and local data centers to manage and protect their digital assets. They had complete control over their hardware, software, and network components, fostering a sense of trust within their premises. However, as organizations now connect digitally with customers, partners, and employees worldwide, new risks and threats have emerged that require enhanced security measures.

Social engineering

Anyone within your organization can be tricked into inadvertently downloading malicious attachments, divulging passwords, or compromising sensitive data.

Phishing attacks

- Collect personal details about you.
- Collect personal details about your employees.
- Collect personal details about your students.



First is deceptive **social engineering**. Imagine that a skilled manipulator is seeking to extract confidential system information from unsuspecting individuals.

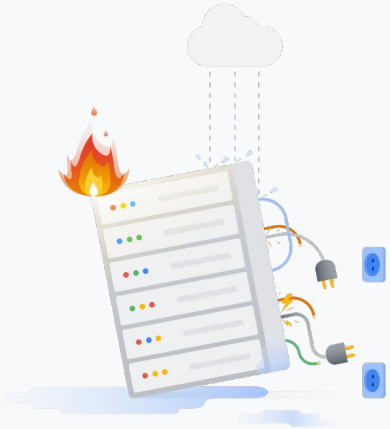
These cybercriminals employ “phishing attacks,” which collect personal details about you, your employees, or your students. They skillfully craft tailored emails and mimic authenticity to deceive their targets.

Therefore, anyone within your organization can be tricked into inadvertently downloading malicious attachments, divulging passwords, or compromising sensitive data.

Physical damage

Organizations are responsible for safeguarding data even in the face of physical adversity.

- Damage to hardware components
- Power disruptions
- Natural disasters: Floods, fires, and earthquakes



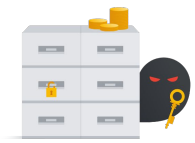
Next is **physical damage**. Whether it be damage to hardware components, power disruptions, or natural disasters such as floods, fires, and earthquakes, organizations are responsible for safeguarding data even in the face of physical adversity.

You can think of this as protecting precious assets amidst nature's unforgiving forces.

Malware, viruses, and ransomware

This malicious software aims to disrupt operations, inflict damage, or gain unauthorized access to computer systems.

Ransomware



Crucial files are held hostage until a considerable ransom is paid.

It's like witnessing the digital equivalent of an extortion scheme.

Another threat is **malware, viruses,** and **ransomware**. These digital adversaries architect chaos within the cyber domain.

Employing malicious software, they aim to disrupt operations, inflict damage, or gain unauthorized access to computer systems. The most insidious of these is ransomware, where crucial files are held hostage until a considerable ransom is paid. It's like witnessing the digital equivalent of a calculated extortion scheme.

Vulnerable third-party systems

Without adequate security measures, third-party systems can transform into potential threats, leaving data security vulnerable.

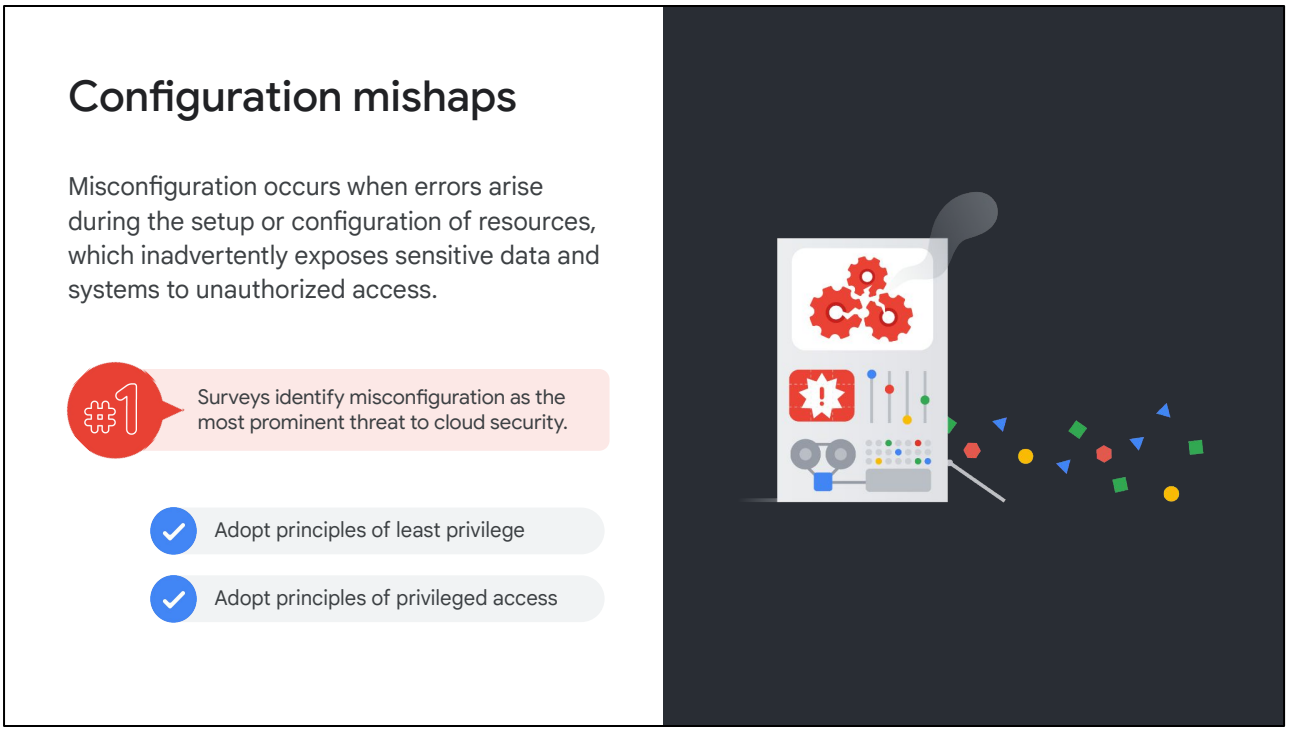
Common functions for third-party systems:

- Finance
- Inventory management
- Account operations

The next cybersecurity threat is **vulnerable third-party systems**. Imagine inviting a trusted ally into your domain, only to discover that they inadvertently compromise your security.

Many organizations rely on third-party systems for essential functions such as finance, inventory management, or account operations. However, without adequate security measures and regular evaluations, these systems can transform into potential threats, leaving data security vulnerable.

It's like using a tool that unwittingly introduces risks to your own treasured possessions.



The final threat is **configuration mishaps**. Even the most seasoned experts make mistakes. Misconfiguration occurs when errors arise during the setup or configuration of resources, which inadvertently exposes sensitive data and systems to unauthorized access.

Surveys consistently identify misconfiguration as the most prominent threat to cloud security.

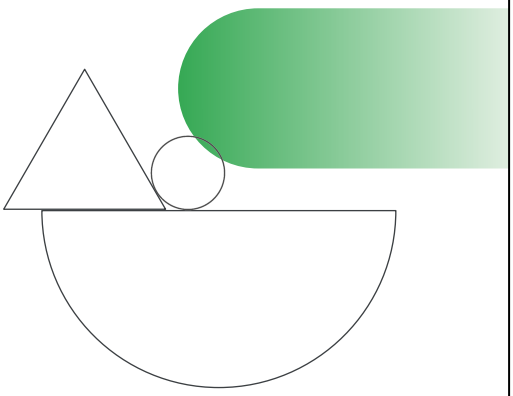
In turn, adopting principles of least privilege and privileged access are imperative, because they allow resource access only when explicitly required and authorized. This is like granting access only to those who have earned your trust.

As technology continues to advance at an astonishing pace, organizations must invest in the right expertise to assess, develop, implement, and maintain robust data security plans.

Activity

5 min | Class | Page 25

Read the case studies that follow and then pinpoint the specific cybersecurity threat that's present in each scenario.

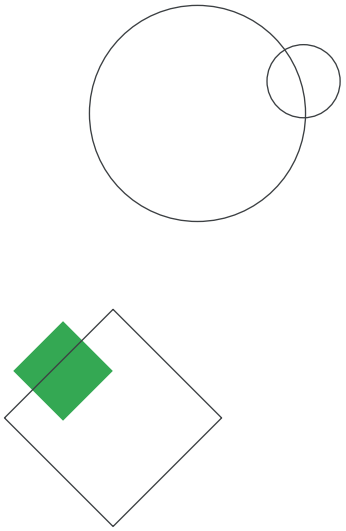


This is an exercise that requires some individual thinking. Let's practice recalling and identifying some common cybersecurity threats—phishing, physical damage, malware or virus attack, ransomware, unsecured third party systems, and misconfiguration—using case studies.

Example 1

An employee finds an old USB memory stick in his home and connects it to his work computer. Soon after, the device begins acting erratically, with many of his files being corrupted or deleted.

What type of cybersecurity threat are they facing?

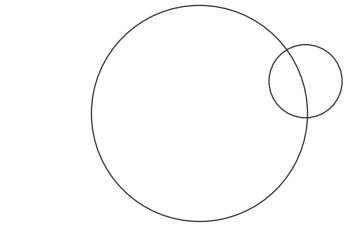


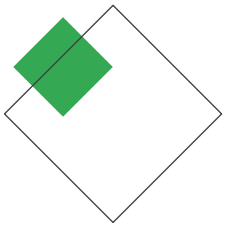
Example 1: An employee finds an old USB memory stick in his home and connects it to his work computer. Soon after the device begins acting erratically, with many of his files being corrupted or deleted. What type of cybersecurity threat are they facing?

Example 1

An employee finds an old USB memory stick in his home and connects it to his work computer. Soon after, the device begins acting erratically, with many of his files being corrupted or deleted.

Answer: A malware or virus attack



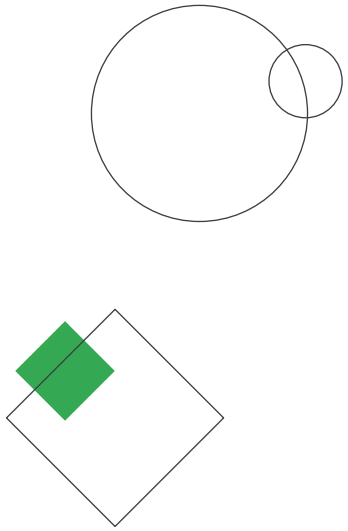


Answer: A malware or virus attack

Example 2

A colleague is searching for an application online. They find the software on an unfamiliar website, download, and run it. Their files then become locked and unusable, with an accompanying message demanding a payout to release the information.

What type of cybersecurity threat are they facing?

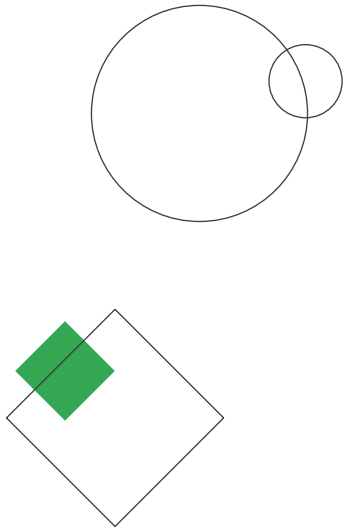


Example 2: A colleague is searching for an application online. They find the software on an unfamiliar website, download, and run it. Their files then become locked and unusable, with an accompanying message demanding a payout to release the information. What type of cybersecurity threat are they facing?

Example 2

A colleague is searching for an application online. They find the software on an unfamiliar website, download, and run it. Their files then become locked and unusable, with an accompanying message demanding a payout to release the information.

Answer: A ransomware attack

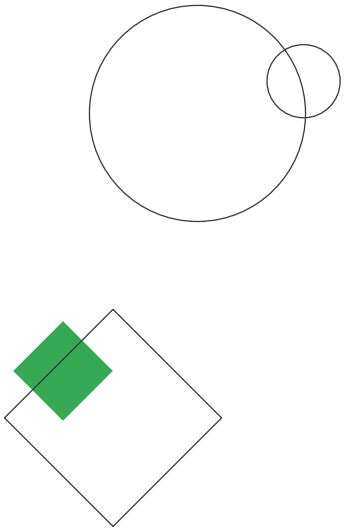


Answer: A ransomware attack

Example 3

Your organization begins using an external system to manage its HR department and employees' personal details. A few months later, these employee details begin to appear online. Your organization's IT teams search and confirm that the data breach was not internal, and your security remains uncompromised.

What type of cybersecurity threat are they facing?

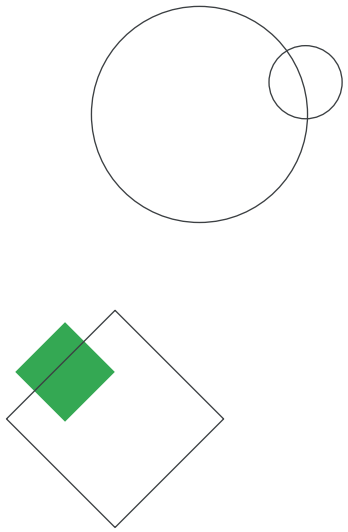


Example 3: Your organization begins using an external system to manage its HR department and employees' personal details. A few months later, these employee details begin to appear online. Your organization's IT teams search and confirm the data breach was not internal, and your security remains uncompromised. What type of cybersecurity threat are they facing?

Example 3

Your organization begins using an external system to manage its HR department and employees' personal details. A few months later, these employee details begin to appear online. Your organization's IT teams search and confirm that the data breach was not internal, and your security remains uncompromised.

Answer: Unsecured third-party systems

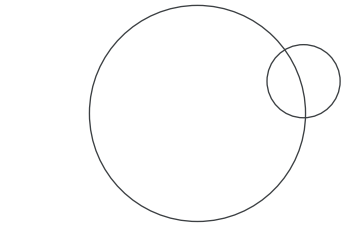


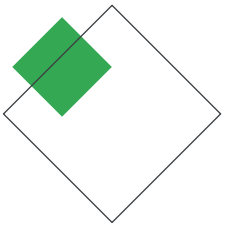
Answer: (Threats arising from) Unsecured third-party systems

Example 4

You receive an email from an unfamiliar address, claiming to be from a colleague. It says she has urgent work for you, and needs you to reply with a mobile number so that she can brief you.

What type of cybersecurity threat are you facing?



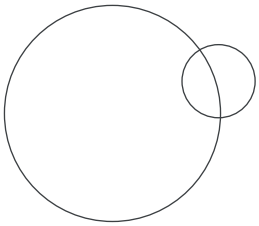


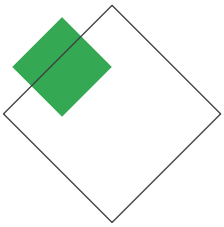
Example 4: You receive an email from an unfamiliar address, claiming to be from a colleague. It says she has urgent work for you, and needs you to reply with a mobile number so she can brief you. What type of cybersecurity threat are you facing?

Example 4

You receive an email from an unfamiliar address, claiming to be from a colleague. It says she has urgent work for you, and needs you to reply with a mobile number so that she can brief you.

Answer: A phishing attack (constant criminal attack)





Answer: A phishing attack (constant criminal attack)

Module 5

Trust and Security with Google Cloud

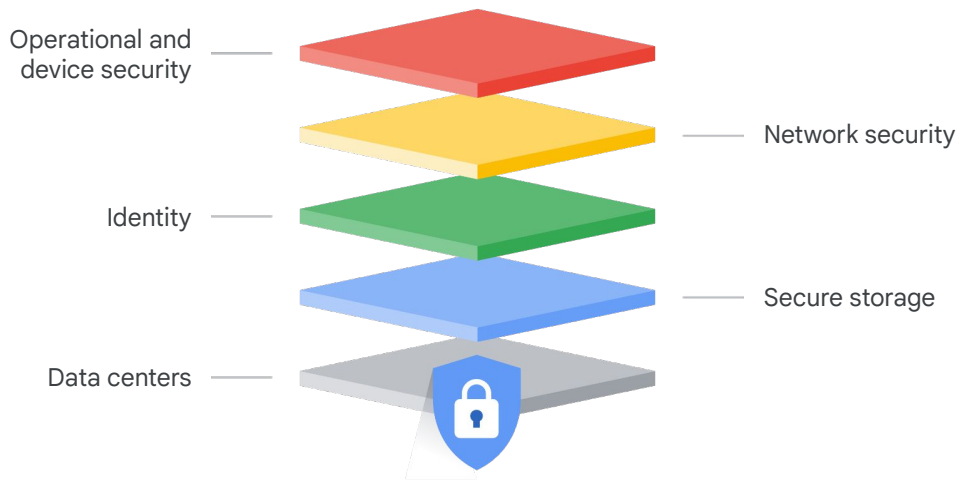
Lessons

01 Trust and security in the cloud

02 Google's trusted infrastructure

03 Google Cloud's trust principles and compliance

Google's multilayered security strategy



At Google Cloud, we believe in going beyond reliance on a single technology for security.

Our multilayered strategy builds progressive security layers, combining global data centers, secure storage on purpose-built servers, identity management, network security, and operational and device security. This approach provides true defense-in-depth.

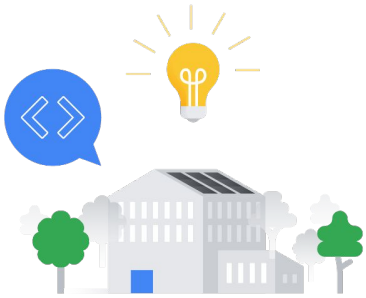
In this section of the course, you'll learn about how:

1. Google designs and builds its own data centers by using purpose-built servers, networking, and custom security hardware and software,
2. The role that encryption plays in securing an organization's data and the ways that it can protect data exposed to risks in different states,
3. The differences between authentication, authorization, and auditing,
4. The benefits of using two-step verification and Identity and Access Management, or IAM,
5. How an organization can protect against network attacks by using Google products, and
6. Security operations in the cloud and its related business benefits.

Data centers

Data centers are more than just facilities filled with computers. They're the backbone of round-the-clock operations for Google's services, including Search, Gmail, and YouTube. Moreover, they play a crucial role in storing and processing data for all the services provided on Google Cloud.

Google operates over 30 state-of-the-art data centers worldwide



- Purpose-built servers
- Advanced networking solutions
- Custom security hardware and software

At present, Google operates over 30 state-of-the-art data centers worldwide, with some still under construction. These advanced facilities are meticulously designed to deliver exceptional reliability, top-notch security, and outstanding efficiency, and they ensure that Google's services are always available when you need them. But it doesn't stop there. Google is committed to minimizing the environmental impact of data centers. By using cutting-edge technologies and renewable energy sources, we strive to reduce our ecological footprint.

Google designs and builds its own data centers includes using purpose-built servers, advanced networking solutions, and custom security hardware and software.

Zero-trust architecture

Our custom hardware and software are purpose-built with features such as:

- Tamper-evident hardware
- Secure boot
- Hardware-based encryption

One of the greatest advantages of Google's data centers is the implementation of a **zero-trust architecture**, which ensures enhanced security at every level.

Our custom hardware and software are purpose-built with features like tamper-evident hardware, secure boot, and hardware-based encryption, which establish a strong security posture within the data center environment.

Physical security

Robust access control measures

Security by default

Biometric authentication in place

Designed with security in mind

Physical security is paramount as well, with robust access control measures and biometric authentication in place. By adopting the principle of least privilege, only authorized personnel have access to the data centers, which minimizes the risk of physical breaches and maintains a privileged access framework.

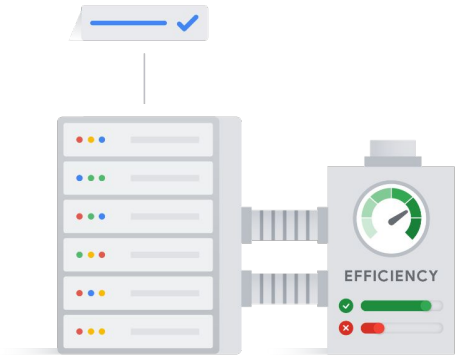
Furthermore, our data centers embody the concept of security by default. From the moment you step into a Google data center, you can trust that every aspect has been designed and implemented with your security in mind.

Cyber resilience

Our data centers are equipped to withstand and recover from potential security incidents, and ensure the continuity and integrity of data.

With cyber resilience as a core principle, our data centers are equipped to withstand and recover from potential security incidents, and ensure the continuity and integrity of your data.

Efficiency

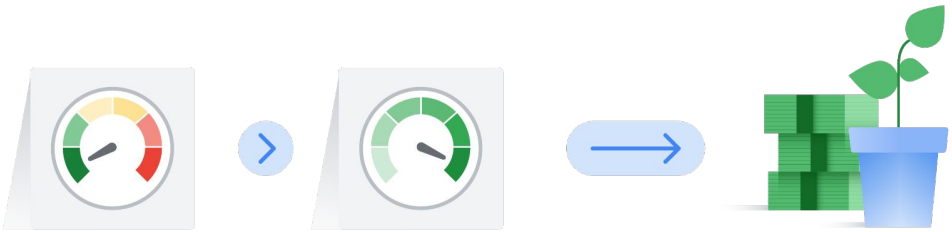


Purpose-built servers are optimized for specific tasks, which:

- Reduces energy consumption
- Cuts down on operating costs
- Saves resources and the environment

Efficiency is another important aspect of our data center design. Purpose-built servers are optimized for specific tasks, which allows them to perform at great speed and with exceptional efficiency. This reduces energy consumption, cuts down on operating costs, and saves resources and the environment.

We measure efficiency success through the Power Usage Effectiveness (PUE) score



Min. PUE

Max. efficiency

Cost savings and reduced carbon footprint

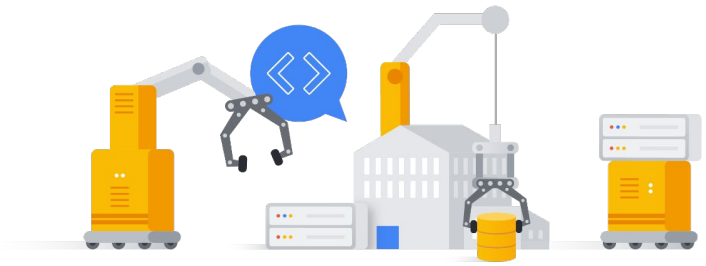
In fact, we measure our success through the Power Usage Effectiveness (PUE) score. By continually striving for the lowest PUE scores, we ensure maximum efficiency in our data centers, leading to significant cost savings and a reduced carbon footprint.

For instance, our data center in Hamina, Finland, stands out as one of the most advanced and efficient facilities in our fleet. Its innovative cooling system, which uses sea water from the Bay of Finland, sets a new standard for energy efficiency worldwide.

Scalability

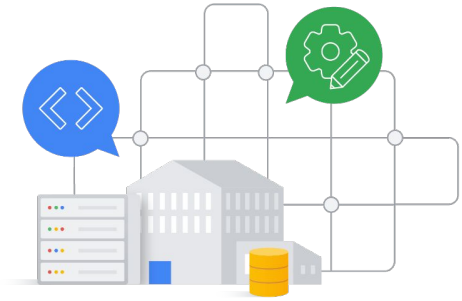
Google data centers can quickly and seamlessly accommodate new hardware and servers.

This allows Google to handle massive data volumes and traffic without any disruptions to services.



Scalability is another benefit. Our data centers can quickly and seamlessly accommodate new hardware and servers, which allows us to scale up computing resources on demand. This flexibility is critical for Google to handle massive data volumes and traffic without any disruptions to services.

Customization



Managing our own servers and network provides us with unparalleled customization capabilities. This allows us to:

- Deliver unique services and capabilities
- Give access to exclusive features and innovations

Furthermore, managing our own servers and network provides us with unparalleled **customization** capabilities. This level of flexibility empowers us to deliver unique services and capabilities that are not available from other providers, giving you access to exclusive features and innovations.

Although designing and building data centers requires significant upfront investment, the long-term benefits are substantial. By optimizing resources for efficiency and scalability, Google can significantly reduce energy consumption and operating **costs**, which results in remarkable savings over time.

Quiz

Question

What metric does Google Cloud use to measure the efficiency of its data centers to achieve cost savings and a reduced carbon footprint?

A. Power Usage Effectiveness (PUE)

B. Data Center Infrastructure Efficiency (DCIE)

C. Total Cost of Ownership (TCO)

D. Energy Efficiency Ratio (EER)

What metric does Google Cloud use to measure the efficiency of its data centers to achieve cost savings and a reduced carbon footprint?

A. Power Usage Effectiveness (PUE)
B. Data Center Infrastructure Efficiency (DCIE)
C. Total Cost of Ownership (TCO)
D. Energy Efficiency Ratio (EER)

Quiz

Answer

What metric does Google Cloud use to measure the efficiency of its data centers to achieve cost savings and a reduced carbon footprint?

A. Power Usage Effectiveness (PUE)

B. Data Center Infrastructure Efficiency (DCIE)

C. Total Cost of Ownership (TCO)

D. Energy Efficiency Ratio (EER)

The correct answer is A.

A. Power Usage Effectiveness (PUE)
- Why this is the **correct** answer: PUE is the industry-standard metric Google Cloud uses to measure data center efficiency, calculating the ratio of total power used by the data center to the power directly delivered to computing equipment.

B. Accounting
- Why this is the **incorrect** answer: DCIE is the reciprocal of PUE (1/PUE), expressing efficiency as a percentage. Both are used, but PUE is the more common term.

C. Auditing
- Why this is the **incorrect** answer: TCO is a broader financial metric that includes costs beyond just energy consumption, making it less focused on pure energy efficiency.

D. Authentication
- Why this is the **incorrect** answer: EER is often used to measure the efficiency of cooling systems specifically, rather than the efficiency of an entire data center as PUE does.

Secure storage

Encryption transforms data into an unreadable format using special algorithms

Encryption protects your data from:

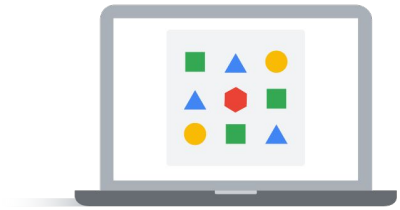
- Unauthorized access
- Loss
- Damage

Previously, you learned that encryption is like a secret code that transforms data into an unreadable format using special algorithms. This process ensures that only those with the right key or password can make sense of the data. It's like using a secret language to protect your information.

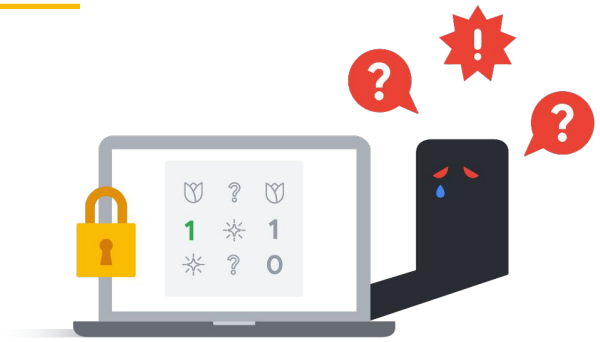
By encrypting your data, you can protect it from various risks, such as unauthorized access, loss, or damage. Imagine your data is locked away in a safe. Without the right key, no one can steal, tamper with, or even understand the information inside.

Let's take a closer look at how encryption protects your data in different states.

Encryption protects data at rest



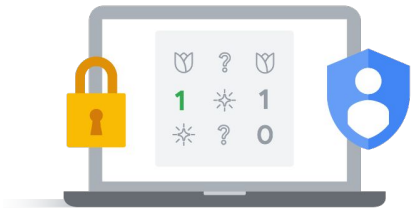
When data is at rest, it's stored on physical devices like computers or servers.



Even if someone gains physical access to the device, they won't be able to decipher the data without the encryption key.

When **data is at rest**, it's stored on physical devices like computers or servers. By encrypting data at rest, even if someone gains physical access to the device, they won't be able to decipher the data without the encryption key.

Google Cloud automatically encrypts all customer content at rest



It's free.

It's built in.

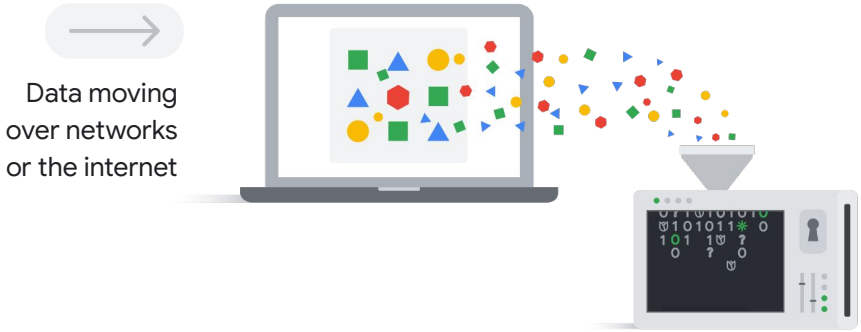
Cloud Key Management Service

A service to encrypt keys yourself

At Google Cloud, we automatically encrypt all customer content at rest, without any effort required from you. It's a free and built-in feature that adds an extra layer of protection to your valuable data.

And if you prefer to manage your encryption keys yourself, you can use our Cloud Key Management Service (Cloud KMS) for added control.

Encryption protects data in transit



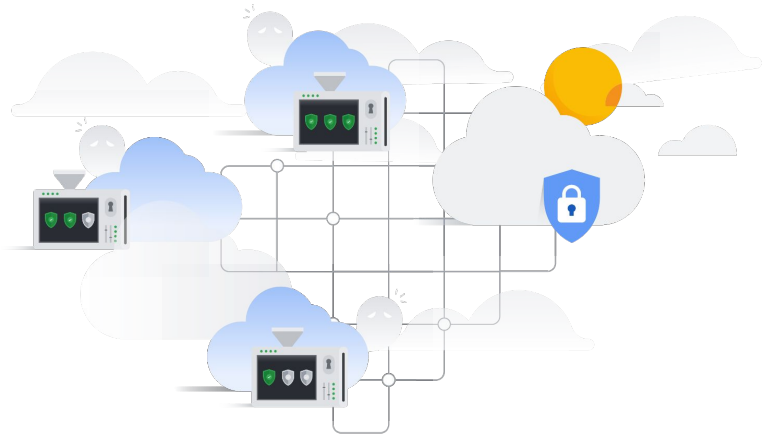
Encryption shields data from interception by cybercriminals or unauthorized parties.

When **data is in transit**, it's moving over networks or the internet. Encryption plays a crucial role here by shielding your data from interception by cybercriminals or unauthorized parties. It's like sending your information in a locked box that only the intended recipient can open.

Data is encrypted and authenticated at multiple network layers

Google employs robust security measures to ensure:

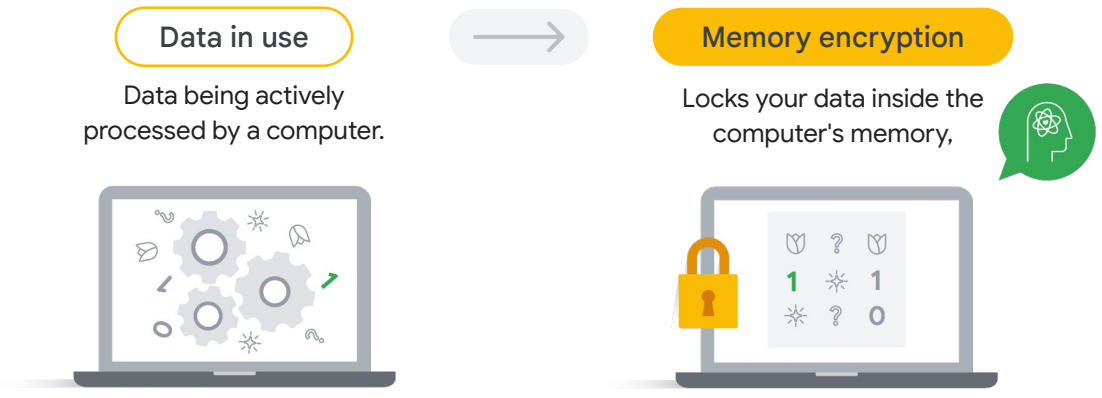
- Authenticity
- Integrity
- Privacy



At Google Cloud, we employ robust security measures to ensure the authenticity, integrity, and privacy of your data during transit.

We encrypt and authenticate data at multiple network layers, especially when it travels outside the physical boundaries we control. This way, your information remains safe and secure as it journeys through the digital world.

Encryption protects data in use



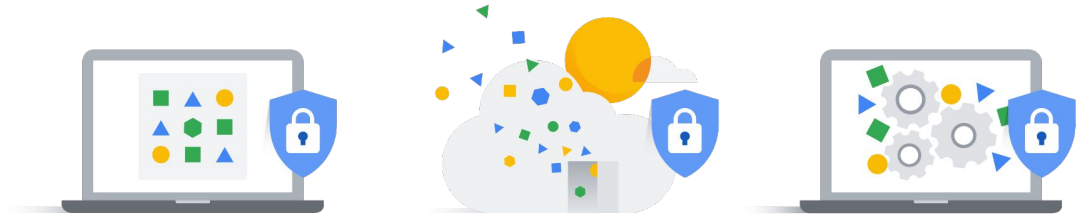
Data in use refers to data being actively processed by a computer. Encrypting data in use adds another layer of protection, especially against unauthorized users who might physically access the computer.

We use a technique called memory encryption, which locks your data inside the computer's memory, making it nearly impossible for unauthorized users to gain access to it.

Advanced Encryption Standard (AES)

AES is a powerful encryption algorithm trusted by governments and businesses worldwide.

Encryption helps ensure confidentiality and protection at every data stage.



Data at rest | Data traveling | Data in use

When it comes to encryption algorithms, the **Advanced Encryption Standard (AES)** takes center stage. AES is a powerful encryption algorithm trusted by governments and businesses worldwide. It's like having a top-secret encryption method that keeps your data safe from prying eyes.

So, whether your data is resting, traveling, or actively in use, encryption acts as your loyal guardian, because it ensures its confidentiality and protection. At Google Cloud, we take encryption seriously to provide you with a secure storage solution you can trust.

Identity

The three A's of cloud identity management

Authentication

Authorization

Auditing

Used to:

- Ensure secure access
- Manage user privileges
- Monitor resource usage

Often referred to as the three A's, **authentication**, **authorization**, and **auditing** are important aspects of cloud identity management used to ensure secure access, manage user privileges, and monitor resource usage.

Authentication

Authentication verifies the identity of users or systems that seek access through unique credentials.

Let's begin with the first A: **authentication**. It serves as the gatekeeper, because it verifies the identity of users or systems that seek access.

Authentication involves presenting unique credentials, such as passwords, physical tokens, or biometric data like fingerprints or voice recognition. Think of it as presenting your identification card before entering a restricted area. By validating the credentials provided, the server confirms that you are who you claim to be.

Authentication

Two-step verification (2SV)

Two-factor authentication

Multi-factor authentication

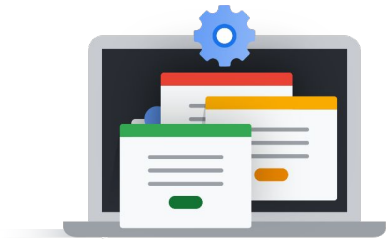
With 2SV enabled, users need to provide two different pieces of information to log in.

Two-step verification, which you may also hear being referred to as two-factor authentication or multi-factor authentication, is a security feature that adds an extra layer of protection to cloud-based systems.

With 2SV enabled, users need to provide two different pieces of information to log in. For example, it could be a combination of a password and a code sent to their phone through text message, voice call, or an app like Google Authenticator. This powerful feature makes unauthorized access more difficult, even if someone manages to obtain your password.

Authorization

Authorization determines what a user is allowed to do within the system.



Admin

Create and remove user accounts

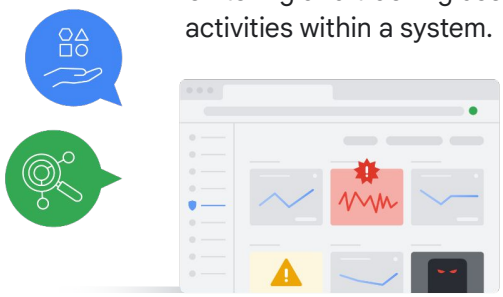
Standard user

View a list of users

The second A is **authorization**. After a user's identity is authenticated, authorization steps in to determine what that user or system is allowed to do within the system. Think of it as the access control mechanism. Different permissions are assigned to individuals or groups based on their roles, responsibilities, and organizational hierarchy.

For example, a system administrator might have the authority to create and remove user accounts, whereas a standard user might only be able to view a list of other users. This fine-grained control ensures that each user has the appropriate level of access to perform their tasks while preventing unauthorized actions.

Auditing (or accounting)



Auditing plays a critical role in monitoring and tracking user activities within a system.

It provides a comprehensive record of actions taken on a system, which is helpful during:

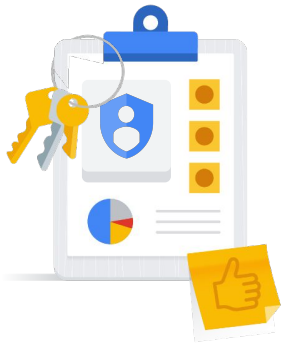
- Security incident investigations
- Compliance tracking
- System performance evaluation

The third A, **auditing** (sometimes referred to as *accounting*), plays a critical role in monitoring and tracking user activities within a system.

By collecting and analyzing logs of user activity, system events, and other data, auditing helps organizations detect anomalies, security breaches, and policy violations. It provides a comprehensive record of actions taken on a system or resource, which proves invaluable during security incident investigations, compliance tracking, and system performance evaluation.

Just like the surveillance cameras in a shopping mall, auditing keeps a watchful eye on activities happening within your system.

Use Identity and Access Management (IAM) for granular access control



Identity and Access Management (IAM)

- Create and manage user accounts.
- Assign roles to users.
- Grant and revoke permissions to resources.
- Audit user activity.
- Monitor your security position.

To provide granular control over who has access to Google Cloud resources and what they can do with those resources, organizations can use **Identity and Access Management (IAM)**. With IAM, you can create and manage user accounts, assign roles to users, grant and revoke permissions to resources, audit user activity, and monitor your security position. It provides a centralized and efficient approach to managing access control within your Google Cloud environment.

Imagine IAM as your organization's security headquarters, equipped with robust tools to manage and safeguard your digital assets. By integrating IAM into your Google Cloud security strategy, you can ensure fine-grained access control, enhanced visibility, and centralized resource management. This empowers you to protect your organization's sensitive data and resources effectively.

Quiz

Question

Which aspect of cloud identity management verifies the identity of users or systems?

A. Authorization
B. Accounting
C. Auditing
D. Authentication

Which aspect of cloud identity management verifies the identity of users or systems?

A. Authorization
B. Accounting
C. Auditing
D. Authentication

Quiz

Answer

Which aspect of cloud identity management verifies the identity of users or systems?

A. Authorization

B. Accounting

C. Auditing

D. Authentication 

The correct answer is D.

A. Authorization
   - Why this is the **incorrect** answer: Authorization focuses on determining what an authenticated user or system is allowed to do or access within a system.

B. Accounting
   - Why this is the **incorrect** answer: Accounting refers to tracking and recording resource usage by users or systems, often for billing or monitoring purposes.

C. Auditing
   - Why this is the **incorrect** answer: Auditing involves reviewing logs and system records to ensure security policies are followed, detect anomalies, and investigate potential security incidents.

D. Authentication
   - Why this is the **correct** answer: Authentication is the process of verifying the identity of a user or system attempting to access a resource. This typically involves confirming factors like usernames, passwords, biometric data, or security tokens.

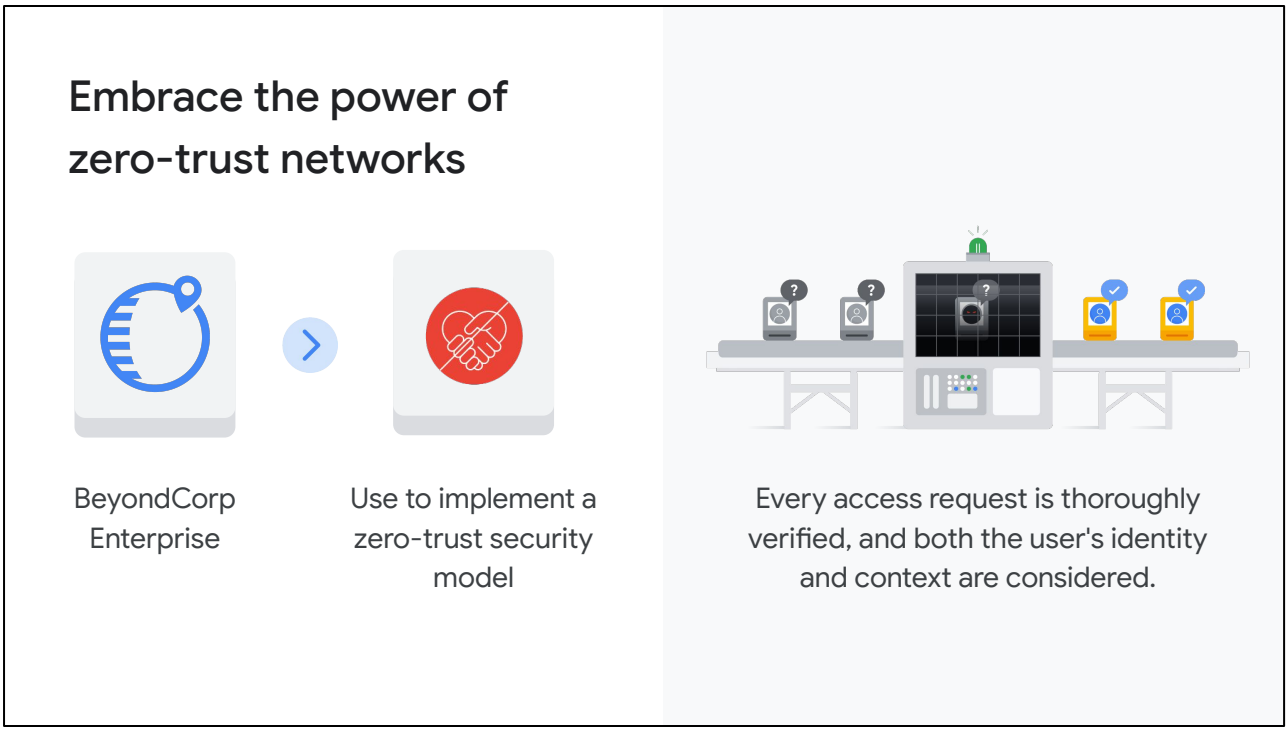
Network security

Strategies to secure your organization's network

- Embrace the power of zero-trust networks.
- Secure your connections to on-premises and multi-cloud environments.
- Protect your perimeter with Google Cloud's powerful tools.
- Stay ahead with a web application firewall.
- Automate infrastructure provisioning for enhanced security.

When you expand your network to include cloud environments, security considerations take on a whole new dimension. Unlike traditional on-premises setups with clear perimeters, the cloud brings new possibilities and challenges.

Let's explore some strategies to secure your organization's network and ensure the safety of your valuable data and workloads in Google Cloud.



Embrace the power of zero trust networks.

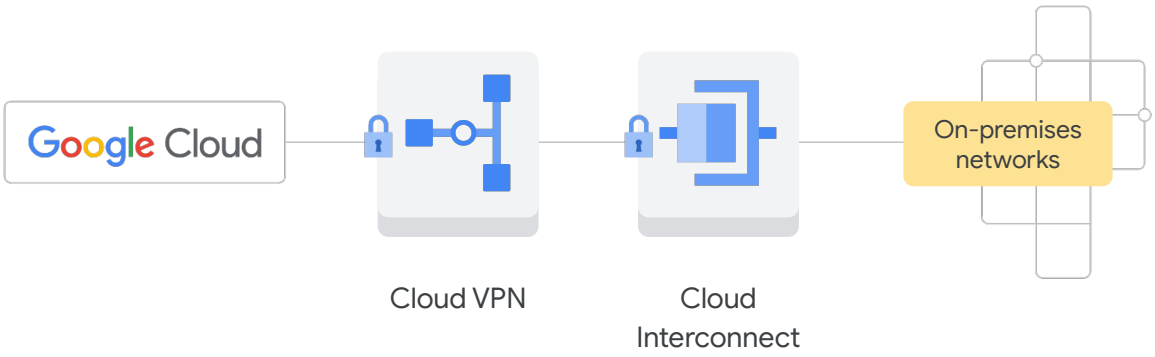
In the world of security, trust shouldn't be given freely. With Google Cloud's BeyondCorp Enterprise, you can implement a zero trust security model.

It means that every access request is thoroughly verified, and both the user's identity and context are considered. This way, you maintain strict control over who can access your network and resources, both inside and outside your organization.

Secure your connections to on-premises and multi-cloud environments

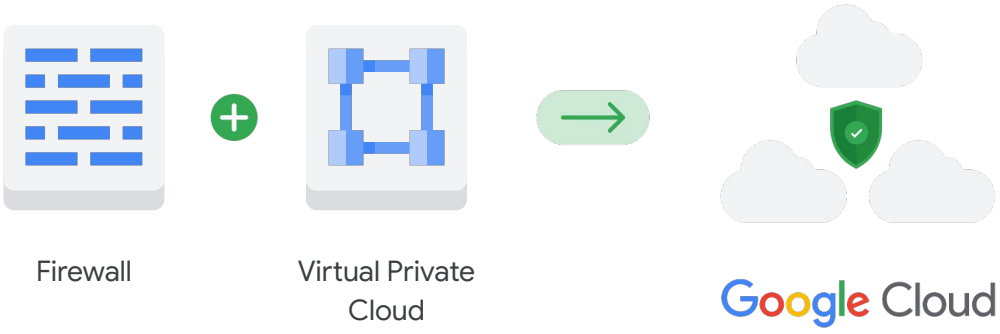
Many organizations have a mix of cloud and on-premises workloads, or they use multiple cloud providers for resiliency. Ensuring secure connectivity across these environments is crucial.

Google Cloud provides private access methods



Google Cloud provides private access methods through services like Cloud VPN and Cloud Interconnect, which let you establish secure connections between your on-premises networks and Google Cloud resources.

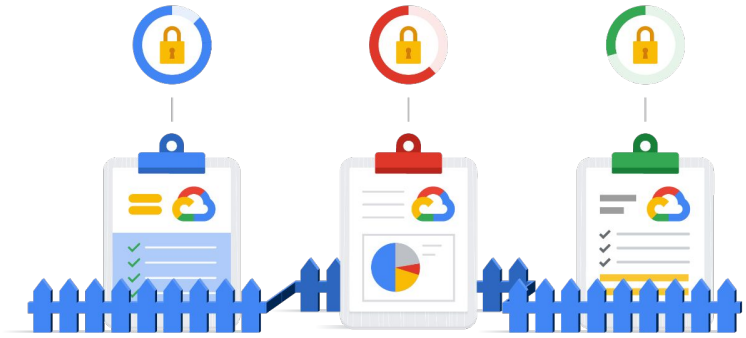
Protect your perimeter with Google Cloud's powerful tools



Protect your perimeter with Google Cloud's powerful tools.

Google Cloud offers various methods to help secure your perimeter, including firewalls and Virtual Private Cloud (VPC) Service Controls, which help you divide your cloud into different sections and keep them secure.

Shared VPC



A shared VPC is like having a large fence that separates each Google Cloud Project so they can work independently and safely.

You can also utilize Shared VPC, which is like having a large fence that separates each Google Cloud Project, so they can work independently and safely.

With these tools, you can keep your cloud environment protected and give different teams their own space to work in.

Stay ahead with a web application firewall

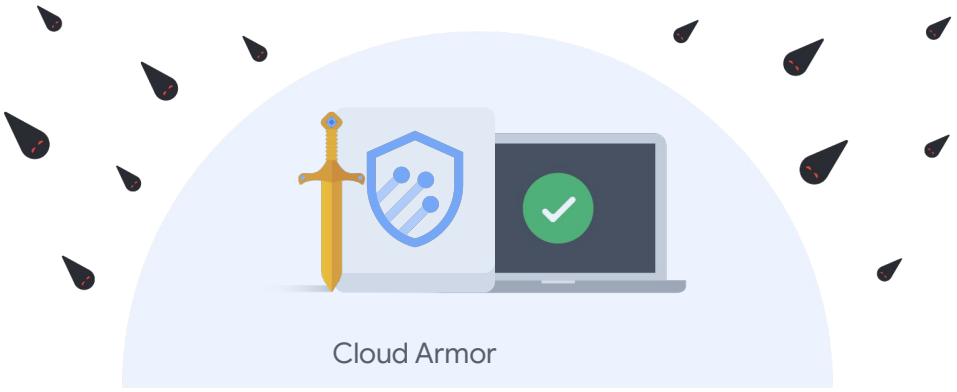
External web applications and services are often targeted by cyber threats, including DDoS attacks.

A cyber attack that floods a target with more traffic than it can handle, causing a denial of service to legitimate users.

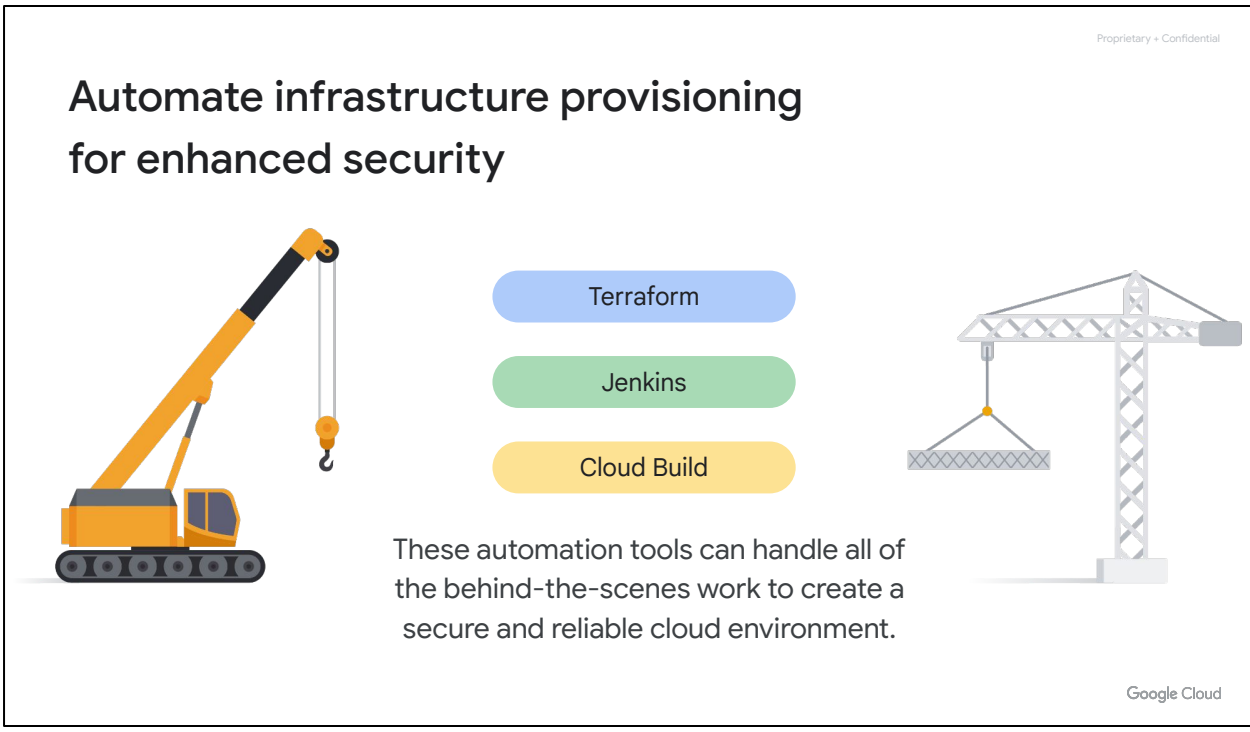
Stay ahead with a web application firewall.

External web applications and services are often targeted by cyber threats, including DDoS attacks. DDoS, which stands for distributed denial-of-service, is a cyber attack that uses multiple compromised computer systems to flood a target with more traffic than it can handle, which causes a denial of service to legitimate users.

Google Cloud Armor provides robust DDoS protection



Google Cloud Armor comes to the rescue by providing robust DDoS protection. It's like a force field that stops harmful attacks and keeps your website or application safe from things that could make it stop working properly.

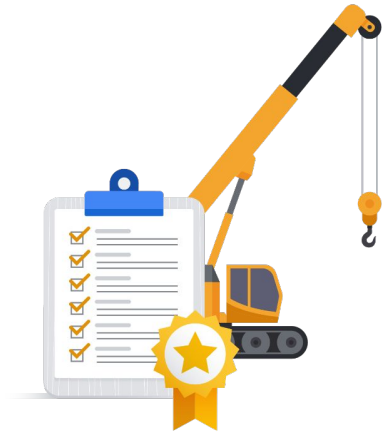


Automate infrastructure provisioning for enhanced security.

By adopting automation tools, you can create immutable infrastructure, which means that it can't be changed after provisioning. Think of infrastructure provisioning tools as your personal assistants for setting up and maintaining your cloud environment.

When you use tools like Terraform, Jenkins, and Cloud Build, they handle all the behind-the-scenes work to create a secure and reliable cloud environment. It's like having a team of efficient workers who build and organize everything you need to run your environment smoothly.

There are benefits to using automation tools to enhance security

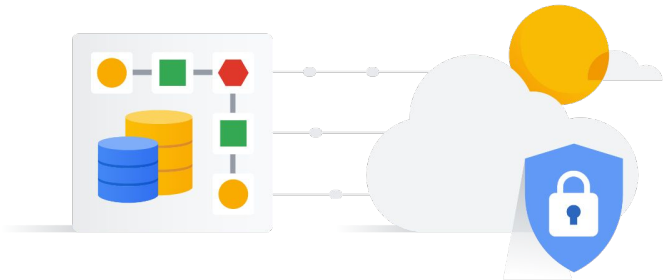


- Your cloud environment becomes like a well-designed workspace.
- When the environment is set up, it stays that way.
- There are no unexpected changes or disruptions.
- Tools can quickly identify and fix issues.

With these tools, your cloud environment becomes like a well-designed workspace where everything has its place and functions perfectly. And the best part is, when it's set up, it stays that way. No unexpected changes or disruptions. If anything does go wrong, these tools are there to quickly identify and fix any issue and ensure that your cloud environment keeps running smoothly.

Security operations

SecOps → Security operations



SecOps is all about protecting your organization's data and systems in the cloud.

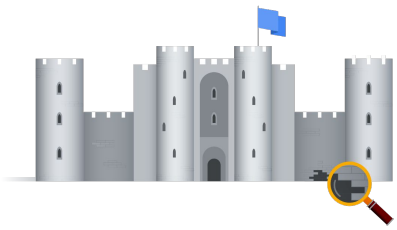
It helps reduce the risk of:

- Data breaches
- System outages
- Other security incidents

SecOps—short for Security Operations—is all about protecting your organization's data and systems in the cloud. It involves a combination of processes and technologies that help reduce the risk of data breaches, system outages, and other security incidents.

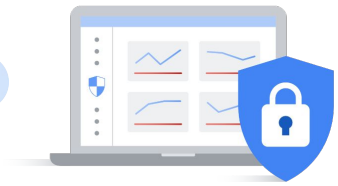
Think of it as your secret weapon for keeping your valuable data safe. Let's explore some of the essential activities involved in SecOps.

Vulnerability management



The process of identifying and fixing security vulnerabilities in cloud infrastructure and applications.

Security Command Center (SCC)

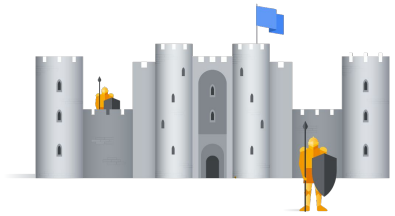


Provides a centralized view of your security posture.

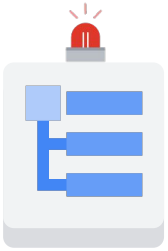
Vulnerability management is the process of identifying and fixing security vulnerabilities in cloud infrastructure and applications. It's like regularly checking your castle walls for weak spots.

Google Cloud's Security Command Center (SCC) provides a centralized view of your security posture. It helps to identify and fix vulnerabilities, and it ensures that your infrastructure remains solid and protected.

Log management



It's like having a watchful eye on your castle grounds, looking out for any suspicious activity.



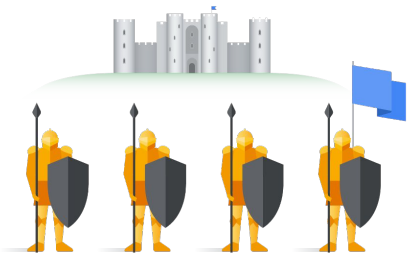
Cloud Logging

A service to collect and analyze security logs from your entire Google Cloud environment.

Another crucial activity is **log management**. It's like having a watchful eye on your castle grounds, looking out for any suspicious activity.

Google Cloud offers Cloud Logging, a service to collect and analyze security logs from your entire Google Cloud environment. It helps you detect and respond to any signs of trouble and ensures that you anticipate any potential threats.

Incident response



It's like having a team of knights ready to defend your castle at a moment's notice.

Google Cloud has expert incident responders across various domains.

Of course, being prepared for security incidents is equally important. This is where **incident response** comes in.

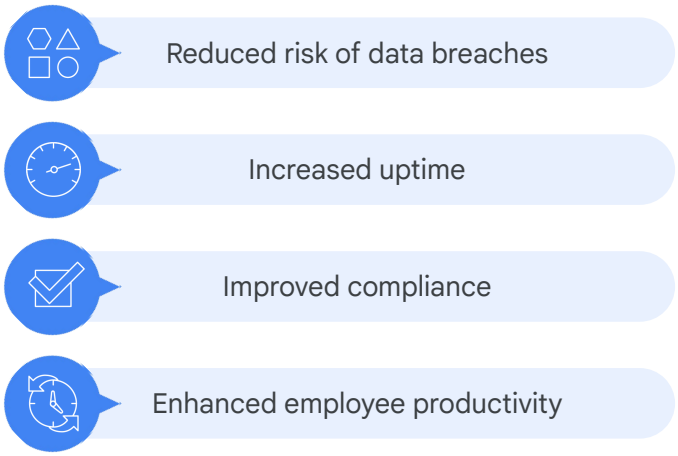
Imagine having a team of knights ready to defend your castle at a moment's notice. Google Cloud has expert incident responders across various domains, who are equipped with the knowledge and tools to tackle any security incident swiftly and effectively.

It's important to educate employees on best practices

Security awareness training helps prevent incidents by raising awareness and empowering employees to protect themselves and the organization.

Another crucial aspect of SecOps is educating your employees on security best practices. Just like teaching everyone in the castle to be vigilant and lock the gates, security awareness training helps prevent incidents by raising awareness and empowering employees to protect themselves and the organization.

SecOps benefits



Now, you might be wondering, why should your organization implement SecOps? Well, here are the benefits:

- **Reduced risk of data breaches:** SecOps helps identify and fix vulnerabilities, which significantly reduces the risk of data breaches.
- **Increased uptime:** A swift and effective incident response minimizes the impact of outages on your business operations, which ensures smoother and uninterrupted services.
- **Improved compliance:** SecOps helps with meeting security regulations, such as the General Data Protection Regulation (GDPR), and keeps your organization in good standing.
- **Enhanced employee productivity:** By educating employees on security best practices, SecOps minimizes the risk of human error and promotes a more secure and productive work environment.

Discussion

Cloud security operations

- Why is SecOps important for organizations?
- What are some of the challenges that organizations face when implementing SecOps?
- How does Google Cloud help organizations implement SecOps practices?

Let's pause for a quick discussion around the benefits of running compute workloads in the cloud.

- Why is SecOps important for organizations that use Google Cloud?
- How does Google Cloud help organizations implement SecOps practices?
- What are some of the challenges that organizations face when implementing SecOps?

Module 5

Trust and Security with Google Cloud

Lessons

Privacy plays a critical role in earning and maintaining trust and transparency

At Google, we know that privacy plays a critical role in earning and maintaining trust.

Customers need to be sure that their data and applications are safe and secure, and so Google Cloud has a strong set of trust principles and compliance programs in place, which are designed to protect customer data and meet the needs of a wide range of customers, from small businesses to large enterprises.

In this final section of the course, you learn about:

- Google's seven trust principles.
- Data residency and data sovereignty options with Google Cloud.
- And how the Google Cloud compliance resource center and Compliance Reports Manager support industry and regional compliance needs.

The Google Cloud trust principles and Transparency Reports

The Google Cloud trust principles

Google Cloud's trust principles are designed to empower you and ensure that the security and control of your business data is not compromised.

At Google, we believe in transparency and want you to have complete confidence in our services. Google Cloud's trust principles are designed to empower you and ensure that the security and control of your business data is not compromised.

Let's explore these principles.

The Google Cloud trust principles

1. You own your data, not Google.
2. Google does not sell customer data to third parties.
3. Google Cloud does not use customer data for advertising.
4. All customer data is encrypted by default.
5. We guard against insider access to your data.
6. We never give any government entity "backdoor" access.
7. Our privacy practices are audited against international standards.

Google Cloud

1: You own your data, not Google. We prioritize your control and let you access, export, delete, and manage data permissions within Google Cloud.

The Google Cloud trust principles

1. You own your data, not Google.
2. Google does not sell customer data to third parties.
3. Google Cloud does not use customer data for advertising.
4. All customer data is encrypted by default.
5. We guard against insider access to your data.
6. We never give any government entity "backdoor" access.
7. Our privacy practices are audited against international standards.

Google Cloud

2: Google does not sell customer data to third parties. We safeguard your data from being used for Google's marketing or advertising purposes.

The Google Cloud trust principles

1. You own your data, not Google.
2. Google does not sell customer data to third parties.
3. Google Cloud does not use customer data for advertising.
4. All customer data is encrypted by default.
5. We guard against insider access to your data.
6. We never give any government entity "backdoor" access.
7. Our privacy practices are audited against international standards.

Google Cloud

3: Google Cloud does not use customer data for advertising. Your data remains confidential, because Google Cloud ensures that it's never utilized to target ads.

The Google Cloud trust principles

1. You own your data, not Google.
2. Google does not sell customer data to third parties.
3. Google Cloud does not use customer data for advertising.
4. All customer data is encrypted by default.
5. We guard against insider access to your data.
6. We never give any government entity "backdoor" access.
7. Our privacy practices are audited against international standards.

Google Cloud

4: All customer data is encrypted by default. Your data is protected with robust encryption, because Google Cloud safeguards it even in the unlikely event of unauthorized access.

The Google Cloud trust principles

1. You own your data, not Google.
2. Google does not sell customer data to third parties.
3. Google Cloud does not use customer data for advertising.
4. All customer data is encrypted by default.
5. We guard against insider access to your data.
6. We never give any government entity "backdoor" access.
7. Our privacy practices are audited against international standards.

Google Cloud

5: We guard against insider access to your data. We implement stringent security measures to prevent unauthorized employee access to customer data.

The Google Cloud trust principles

1. You own your data, not Google.
2. Google does not sell customer data to third parties.
3. Google Cloud does not use customer data for advertising.
4. All customer data is encrypted by default.
5. We guard against insider access to your data.
6. We never give any government entity "backdoor" access.
7. Our privacy practices are audited against international standards.

Google Cloud

6: We never give any government entity "backdoor" access. Your data remains secure, and no government entity can access it without proper authorization.

The Google Cloud trust principles

1. You own your data, not Google.
2. Google does not sell customer data to third parties.
3. Google Cloud does not use customer data for advertising.
4. All customer data is encrypted by default.
5. We guard against insider access to your data.
6. We never give any government entity "backdoor" access.
7. Our privacy practices are audited against international standards.

Google Cloud

And **7: Our privacy practices are audited against international standards**. We undergo regular audits to ensure compliance with rigorous privacy standards.

Reports to stay informed and maintain trust in Google Cloud services

Transparency Reports and **Independent Audits Transparency** are a core element of our commitment to trust. We provide valuable insights and accountability through our transparency reports, which shed light on government and corporate actions that affect privacy, security, and access to information.

These reports let you stay informed and maintain trust in our services.

Google Cloud undergoes independent, third-party audits and certifications

This verification process ensures that our data protection practices align with our commitments and industry standards.

Participation in initiatives like the **EU Cloud Code of Conduct** reinforces our dedication to accountability, compliance support, and robust data protection principles.

Additionally, Google Cloud undergoes independent, third-party audits and certifications. This verification process ensures that our data protection practices align with our commitments and industry standards.

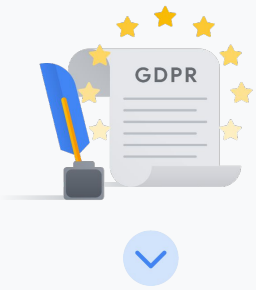
Our participation in initiatives like the **EU Cloud Code of Conduct** further reinforces our dedication to accountability, compliance support, and robust data protection principles.

Data residency and data sovereignty

When it comes to storing data and keeping it secure, **data sovereignty** and **data residency** are two important concepts to understand.

Data sovereignty

The legal concept that data is subject to the laws and regulations of the country where it resides.



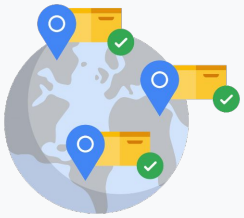
The **General Data Protection Regulation** in the European Union requires companies to comply with data protection laws when processing or storing the personal data of EU citizens, regardless of their location.

Data sovereignty refers to the legal concept that data is subject to the laws and regulations of the country where it resides.

For example, the General Data Protection Regulation (GDPR) in the European Union requires companies to comply with data protection laws when processing or storing the personal data of EU citizens, regardless of their location. This ensures that individuals have control over their personal data and its usage.

Data residency

The physical location where data is stored or processed.



Some countries mandate that the personal data of its citizens must be stored on servers within the country.

This ensures that data remains within the jurisdiction of local laws.

In contrast, **data residency** refers to the physical location where data is stored or processed. Some countries or regions have laws or regulations that require data to be stored within their borders.

For instance, some countries mandate that the personal data of its citizens must be stored on servers within the country. This ensures that data remains within the jurisdiction of local laws.

Google Cloud addresses data residency requirements by letting you choose where your data resides

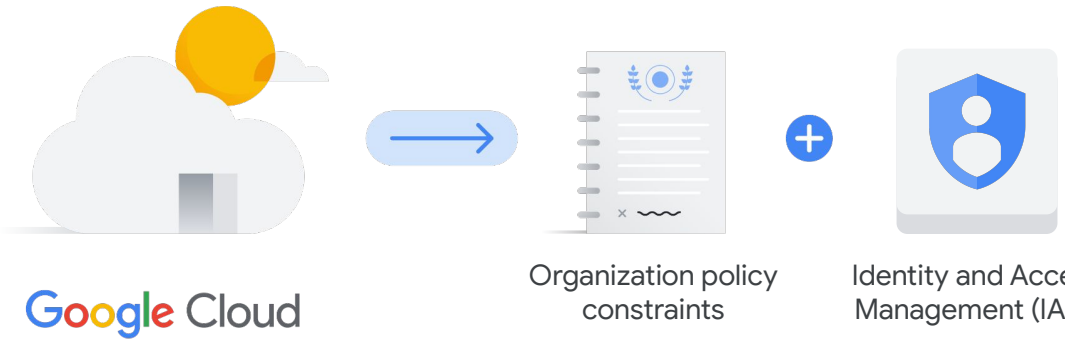
Within the European Union, you can select regions located in various countries like the UK, Belgium, Germany, Finland, Switzerland, and the Netherlands.

Now, let's explore how Google Cloud addresses data residency requirements. We offer a range of options to control the physical location of your data through regions.

Each region consists of one or more data centers, which lets you choose where your data resides. For example, within the European Union, you can select regions located in various countries like the UK, Belgium, Germany, Finland, Switzerland, and the Netherlands.

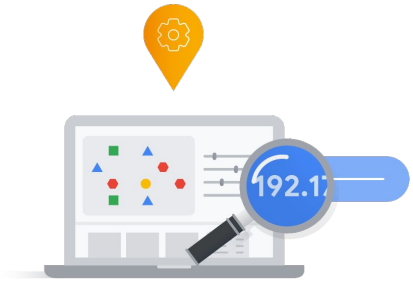
By configuring your resources in specific regions, Google ensures that your data is stored only within the selected region, as stated in our Service Specific Terms.

Organization policy constraints and IAM can help prevent accidental data storage in the wrong region



Additionally, Google Cloud provides organization policy constraints, coupled with IAM configuration, to prevent accidental data storage in the wrong region. These controls offer peace of mind and reinforce your data residency requirements.

VPC Service Controls and Google Cloud Armor



VPC Service Controls

Restrict network access to data based on defined perimeters and limit user access through IP address filtering.

Cloud Armor

Restrict traffic locations for your external load balancer by adding an extra layer of protection.

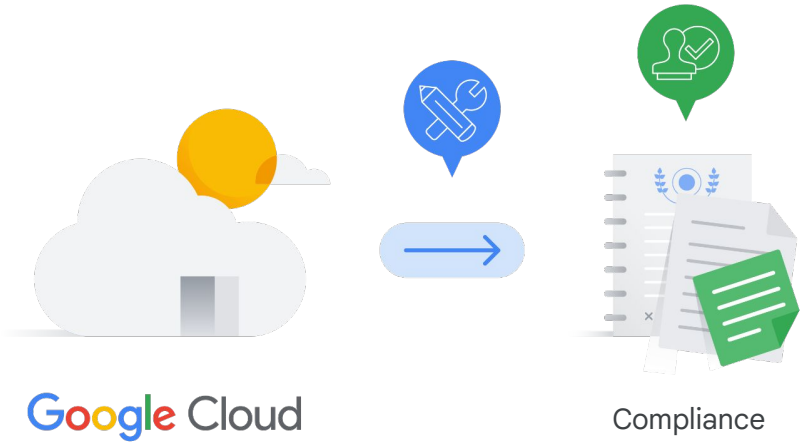
Furthermore, Google Cloud offers features like VPC Service Controls, which let you restrict network access to data based on defined perimeters. You can limit user access through IP address filtering, even if they have authorization.

Google Cloud Armor lets you restrict traffic locations for your external load balancer by adding an extra layer of protection.

By using these capabilities, organizations can adhere to data residency and data sovereignty requirements, ensure compliance, and maintain control over their valuable data within the Google Cloud ecosystem.

Industry and regional compliance

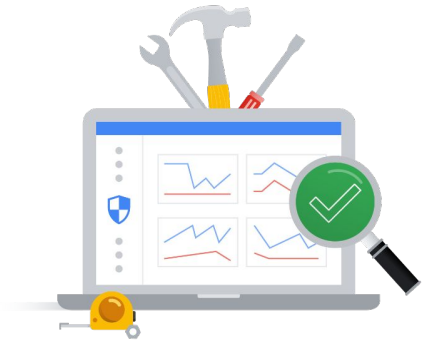
It's essential to protect workloads and ensure compliance



As organizations migrate to the cloud, it becomes essential to protect sensitive workloads while ensuring compliance with diverse regulatory requirements and guidelines.

Compliance is a critical aspect of the cloud journey, because not meeting regulatory obligations can have far-reaching consequences.

Resources and tools to help achieve compliance



Compliance resource center

- Provides detailed information on the certifications and compliance standards we satisfy.
- Offers valuable documentation on regional and sector-specific regulations.
- Equips you with the necessary insights and documentation to align your compliance efforts with HIPAA requirements.
- Provides guidance on meeting regulations in the financial sector like PCI DSS.

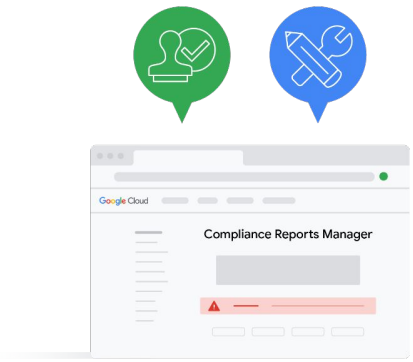
To assist you in achieving compliance, Google Cloud offers robust resources and tools tailored to support your specific needs.

First, let's explore the Google Cloud **compliance resource center**. This comprehensive hub provides detailed information on the certifications and compliance standards we satisfy.
You can find mappings of our security, privacy, and compliance controls to global standards. This transparency lets you validate our adherence to industry-leading practices.

The resource center also offers valuable documentation on regional and sector-specific regulations, and empowers you to navigate complex compliance landscapes.
Imagine you're a healthcare organization subject to HIPAA regulations, which protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

The resource center equips you with the necessary insights and documentation to align your compliance efforts with HIPAA requirements.
Similarly, if you operate within the financial sector, you'll find guidance on meeting regulations like PCI DSS, which stands for Payment Card Industry Data Security Standard.
Google Cloud's compliance resource center is your go-to source for actionable information and support.

Resources and tools to help achieve compliance



Compliance Reports Manager

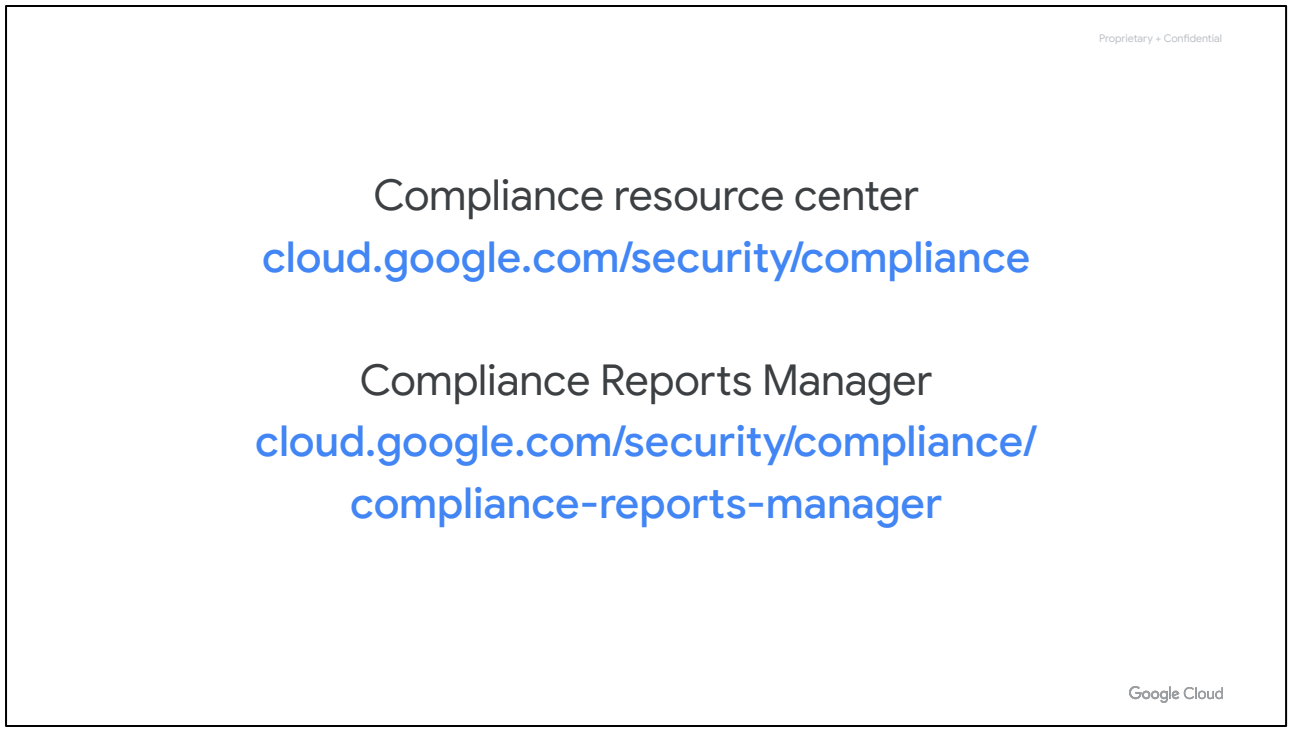
- Offers easy, on-demand access to critical compliance resources at no extra cost.
- Lets you discover Google's latest ISO/IEC certificates, SOC reports, and self-assessments.

In addition to the resource center, we provide the **Compliance Reports Manager**, a powerful tool at your disposal.

This intuitive platform offers easy, on-demand access to critical compliance resources at no extra cost. Within the Compliance Reports Manager, you'll discover our latest ISO/IEC certificates, SOC reports, and self-assessments. These resources provide evidence of our adherence to rigorous compliance standards and help streamline your own reporting and compliance efforts.

Imagine you're an enterprise seeking ISO/IEC 27001 certification. The Compliance Reports Manager lets you access the necessary documentation efficiently, and it saves you time and effort in the certification process.

With this tool, we aim to simplify your compliance journey and empower you to meet your regulatory obligations effectively.



By using the Google Cloud **compliance resource center** and the **Compliance Reports Manager**, you can navigate the complex realm of industry and regional compliance with confidence. Our dedicated teams of engineers and compliance experts work hand in hand with you to address your specific regulatory needs. Together, we create an integrated controls and governance framework, while we ensure a robust compliance posture.

You can visit the compliance resource center at **cloud.google.com/security/compliance** and explore the Compliance Reports Manager at **cloud.google.com/security/compliance/compliance-reports-manager**.

Discussion

Collecting customer data in your organization

Organizations are constantly collecting, storing, and using customer data to improve their products and services. However, this data also needs to be protected from unauthorized access and use.

- How can your organization strike a balance between respecting customer data privacy and leveraging data to drive innovation?
- How can your organization effectively navigate challenges in managing data storage and complying with local regulations while maintaining global operations?

Let's pause for a quick discussion around collection of data within your organization.

Organizations are constantly collecting, storing, and using customer data to improve their products and services. However, this data also needs to be protected from unauthorized access and use.

- How can your organization strike a balance between respecting customer data privacy and leveraging data to drive innovation?
- How can your organization effectively navigate challenges in managing data storage and complying with local regulations while maintaining global operations?

Quiz

Question

Which is the responsibility of the cloud provider in a cloud security model?

A. Setting access policies for the customer's data
B. Maintaining the customer's infrastructure
C. Configuring the customer's applications
D. Managing the customer's user access

Which is the responsibility of the cloud provider in a cloud security model?

A. Setting access policies for the customer's data
B. Maintaining the customer's infrastructure
C. Configuring the customer's applications
D. Managing the customer's user access

Quiz

Answer

Which is the responsibility of the cloud provider in a cloud security model?

A. Setting access policies for the customer's data

B. Maintaining the customer's infrastructure 

C. Configuring the customer's applications

D. Managing the customer's user access

The correct answer is B.

A. Setting access policies for the customer's data
   - Why this is the **incorrect** answer: Customers retain control over who can access their data and define these policies through Identity and Access Management (IAM) tools.

B. Maintaining the customer's infrastructure
   - Why this is the **correct** answer: Depending on the cloud service model (especially IaaS), the cloud provider handles aspects like physical security of data centers, the health of servers and network equipment, and aspects of virtualization security.

C. Configuring the customer's applications
   - Why this is the **incorrect** answer: Customers are generally responsible for the secure configuration of their own applications. This includes applying security patches, choosing appropriate settings, and hardening their applications to reduce vulnerabilities.

D. Managing the customer's user access
   - Why this is the **incorrect** answer: While cloud providers provide IAM tools, organizations must create their own users, assign roles and permissions, and ensure authentication practices align with their security policies.

Quiz

Question

Which cybersecurity threat occurs when errors arise during the setup of resources, inadvertently exposing sensitive data and systems to unauthorized access?

A. Phishing
B. Virus
C. Malware
D. Configuration mishaps

Which cybersecurity threat occurs when errors arise during the setup of resources, inadvertently exposing sensitive data and systems to unauthorized access?

A. Phishing
B. Virus
C. Malware
D. Configuration mishaps

Quiz

Answer

Which cybersecurity threat occurs when errors arise during the setup of resources, inadvertently exposing sensitive data and systems to unauthorized access?

A. Phishing

B. Virus

C. Malware

D. Configuration mishaps 

The correct answer is D.

A. Phishing
   - Why this is the **incorrect** answer: Phishing is a social engineering attack where attackers use deception to trick users into giving up sensitive information or clicking on malicious links. It might exploit a misconfiguration, but isn't the error itself.

B. Virus
   - Why this is the **incorrect** answer: A virus is a type of malware (see below) that spreads by attaching itself to files and programs. While it can take advantage of a poorly configured system, it doesn't describe the core problem of setup errors.

C. Malware
   - Why this is the **incorrect** answer: This is a broader category of malicious software that includes viruses, ransomware, spyware, etc. Malware may exploit configuration errors, but the misconfiguration itself is the initial vulnerability.

D. Configuration mishaps
   - Why this is the **correct** answer: This is the best description of the security threat related to setup errors. It means incorrect or insecure configuration of cloud resources, applications, or systems can lead to accidental exposure of data or create entry points for malicious actors.

Quiz

Question

What Google Cloud product provides robust protection from harmful distributed denial-of-service (DDoS) attacks?

A. Google Cloud Armor
B. Cloud Load Balancing
C. IAM
D. Cloud Monitoring

What Google Cloud product provides robust protection from harmful distributed denial-of-service (DDoS) attacks?

A. Google Cloud Armor
B. Cloud Load Balancing
C. IAM
D. Cloud Monitoring

Quiz

Answer

What Google Cloud product provides robust protection from harmful distributed denial-of-service (DDoS) attacks?

A. Google Cloud Armor

B. Cloud Load Balancing

C. IAM

D. Cloud Monitoring

Say: The correct answer is A.

A. Google Cloud Armor
- Why this is the **correct** answer: Google Cloud Armor is specifically designed to defend against DDoS attacks. It works by filtering out malicious traffic at the edge of Google's network, protecting your applications and infrastructure from being overwhelmed.

B. Cloud Load Balancing
- Why this is the **incorrect** answer: Cloud Load Balancing distributes traffic across multiple instances of your application, improving scalability and performance. While it has some load management features, it isn't a primary DDoS defense tool.

C. IAM
- Why this is the **incorrect** answer: IAM focuses on controlling user and service account access to Google Cloud resources. It's vital for security but doesn't directly mitigate DDoS attacks.

D. Cloud Monitoring
- Why this is the **incorrect** answer: Cloud Monitoring helps you observe metrics, logs, and traces from your cloud applications and infrastructure. While useful for detecting attacks, it doesn't provide active protection against them.