

Cloud Security

What is cloud security?

- Cloud security refers
 - to the cybersecurity policies,
 - best practices, controls, and technologies used to secure applications, data, and infrastructure in cloud environments.
- In particular, cloud security works
 - to provide storage and network protection against internal and external threats,
 - access management,
 - data governance and compliance, and
 - disaster recovery.

- Cloud computing has
 - become the technology of choice for companies looking to gain the agility and flexibility needed to accelerate innovation and meet the expectations of today's modern consumers.
- But migrating to more dynamic cloud environments requires
 - new approaches to security to ensure that data remains secure across online infrastructure, applications, and platforms.

How does cloud security work?

- Cloud security mainly focuses on
 - how to implement policies, processes, and technologies together so they ensure data protection, support regulatory compliance, and
 - provide control over privacy, access, and authentication for users and devices.

How does cloud security work?

- Cloud service providers (CSPs) typically follow
 - a shared responsibility model, which means implementing cloud computing security is both the responsibility of the cloud provider and you—the customer.
 - Think of it as a responsibility framework that defines which security tasks belong to the cloud provider and which are the duty of the customer.
 - Understanding where your provider's security responsibilities end and yours begin is critical for building a resilient cloud security strategy


How does cloud security work?

- Broadly speaking,
 - the CSP is always responsible for the cloud and its core infrastructure,
 - while the customer is expected to secure anything that runs “in” the cloud,
 - such as network controls, identity and access management, data, and applications.
 - Shared responsibility models vary depending on the service provider and the cloud computing service model you use—the more the provider manages, the more they can protect.

Guide to the shared responsibility model

■ USER'S RESPONSIBILITY ■ SERVICE PROVIDER'S RESPONSIBILITY



 EXAMPLES		APPLICATIONS	MIDDLEWARE	VIRTUALIZATION	DATA	O/S	NETWORKING	RUNTIME	SERVERS	STORAGE
SaaS	Dropbox, Salesforce CRM, Zoom, Microsoft 365, Google Workspace	■	■	■	■	■	■	■	■	■
PaaS	Microsoft Azure App Service, AWS Elastic Beanstalk, Google Kubernetes Engine, Red Hat OpenShift	■	■	■	■	■	■	■	■	■
IaaS	Microsoft Azure, Amazon Web Services (AWS), Google Compute Engine (GCE)	■	■	■	■	■	■	■	■	■

Here's a look at how this typically works:

Cloud computing service model	Your responsibility	CSP responsibility
Infrastructure as a service (IaaS)	You secure your data, applications, virtual network controls, operating system, and user access.	The cloud provider secures compute, storage, and physical network, including all patching and configuration.
Platform as a service (PaaS)	You secure your data, user access, and applications.	The cloud provider secures compute, storage, physical network, virtual network controls, and operating system.
Software as a service (SaaS)	You are responsible for securing your data and user access.	The cloud provider secures compute, storage, physical network, virtual network controls, operating system, applications, and middleware.

Cloud security risks and challenges

- Cloud suffers from similar security risks that you might encounter in traditional environments, such as insider threats, data breaches and data loss, phishing, malware, DDoS attacks, and vulnerable APIs.
- However, most organizations will likely face specific cloud security challenges, including:
 - Lack of visibility
 - Misconfigurations
 - Access management
 - Dynamic workloads
 - Compliance

Lack of visibility

- Cloud-based resources run on infrastructure that is located outside your corporate network and owned by a third party.
- As a result, traditional network visibility tools are not suitable for cloud environments, making it difficult for you to gain oversight into all your cloud assets, how they are being accessed, and who has access to them.

Misconfigurations

- Misconfigured cloud security settings are one of the leading causes of data breaches in cloud environments.
- Cloud-based services are made to enable easy access and data sharing, but many organizations may not have a full understanding of how to secure cloud infrastructure.
- This can lead to misconfigurations, such as leaving default passwords in place, failing to activate data encryption, or mismanaging permission controls.

Access management

- Cloud deployments can be accessed directly using the public internet, which enables convenient access from any location or device.
- At the same time, it also means that attackers can more easily gain authorized resources with compromised credentials or improper access control.

Dynamic workloads

- Cloud resources can be provisioned and dynamically scaled up or down based on your workload needs.
- However, many legacy security tools are unable to enforce policies in flexible environments with constantly changing and ephemeral workloads that can be added or removed in a matter of seconds.

Compliance

- The cloud adds another layer of regulatory and internal compliance requirements that you can violate even if you don't experience a security breach.
- Managing compliance in the cloud is an overwhelming and continuous process.
- Unlike an on-premises data center
 - where you have complete control over your data and
 - how it is accessed, it is much harder for companies to consistently identify all cloud assets and controls,
 - map them to relevant requirements, and properly document everything.

Types of cloud security solutions

- Cloud security is constantly evolving and adapting as new security threats emerge.
- As a result, many different types of cloud security solutions are available on the market today, and the list below is by no means exhaustive.
 - Identity and access management (IAM)
 - Data loss prevention (DLP)
 - Security information and event management (SIEM)
 - Public key infrastructure (PKI)

Identity and access management (IAM)

- IAM services and tools allow administrators
 - to centrally manage and control who has access to specific cloud-based and on-premises resources.
- IAM can enable you
 - to actively monitor and restrict how users interact with services,
 - allowing you to enforce your policies across your entire organization

Data loss prevention (DLP)

- DLP can help you
 - gain visibility into the data you store and
 - process by providing capabilities to automatically discover, classify, and de-identify regulated cloud data

Security information and event management (SIEM)

- SIEM solutions
 - combine security information and security event management to offer automated monitoring, detection, and incident response to threats in your cloud environments.
 - Using AI and ML technologies,
 - SIEM tools allow you to examine and analyze log data generated across your applications and network devices—
 - and act quickly if a potential threat is detected.

Public key infrastructure (PKI)

- PKI is the framework
 - used to manage secure, encrypted information exchange using digital certificates.
- PKI solutions typically provide
 - authentication services for applications and
 - verify that data remains uncompromised and confidential through transport.
- Cloud-based PKI services allow organizations
 - to manage and deploy digital certificates used for user, device, and service authentication.