What is Cloud Security?

Cloud security defined, explained, and explored

What is Cloud Security?

Cloud security defined, explained, and explored

?

Cloud security defined, explained, and explored



Share

Cloud security defined

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

**Get web, cloud, and data security in a single service with Forcepoint Cloud Security Gateway**

[**Learn How**](https://www.forcepoint.com/product/cloud-security-gateway)

Why is cloud security important?

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

Cloud security offers many benefits, including:

**Centralized security**: Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with [**shadow IT**](https://www.forcepoint.com/cyber-edu/shadow-it) or [**BYOD**](https://www.forcepoint.com/cyber-edu/bring-your-own-device-byod). Managing these entities centrally enhances traffic analysis and [**web filtering**](https://www.forcepoint.com/product/url-filtering), streamlines the monitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.

**Reduced costs**: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.

**Reduced Administration**: When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.

**Reliability**: Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

More and more organizations are realizing the many business benefits of moving their systems to the cloud. Cloud computing allows organizations to operate at scale, reduce technology costs and use agile systems that give them the competitive edge. However, it is essential that organizations have complete confidence in their cloud computing security and that all data, systems and applications are protected from data theft, leakage, corruption and deletion.

All cloud models are susceptible to threats. IT departments are naturally cautious about moving mission-critical systems to the cloud and it is essential the right security provisions are in place, whether you are running a native cloud, hybrid or on-premise environment. Cloud security offers all the functionality of traditional IT security, and allows businesses to harness the many advantages of cloud computing while remaining secure and also ensure that data privacy and compliance requirements are met.

Secure Data in the Cloud

Cloud data security becomes increasingly important as we move our devices, data centers, business processes, and more to the cloud. Ensuring quality cloud data security is achieved through comprehensive security policies, an organizational culture of security, and cloud security solutions.

Selecting the right cloud security solution for your business is imperative if you want to get the best from the cloud and ensure your organization is protected from unauthorized access, data breaches and other threats. [**Forcepoint Cloud Access Security Broker (CASB)**](https://www.forcepoint.com/product/casb-cloud-access-security-broker) is a complete cloud security solution that protects cloud apps and cloud data, prevents compromised accounts and allows you to set security policies on a per-device basis.