What is cloud security?

11 August 2021

What is cloud security?
What is cloud computing?
Why is cloud security important?
What are some cloud security challenges?
What types of cloud security solutions are available?
How should you approach cloud security?
Why is cloud security important?
What are some cloud security challenges?
What types of cloud security solutions are available?
How should you approach cloud security?

What is cloud security?

Cloud security is a collection of procedures and technology designed to address external and internal threats to business security. Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.

The terms digital transformation and cloud migration have been used regularly in enterprise settings over recent years. While both phrases can mean different things to different organizations, each is driven by a common denominator: the need for change.

As enterprises embrace these concepts and move toward optimizing their operational approach, new challenges arise when balancing productivity levels and security. While more modern technologies help organizations advance capabilities outside the confines of on-premises infrastructure, transitioning primarily to cloud-based environments can have several implications if not done securely.

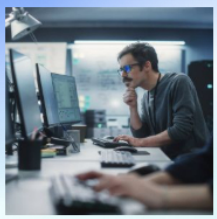
Striking the right balance requires an understanding of how modern-day enterprises can benefit from the use of interconnected cloud technologies while deploying the best cloud security practices.

Report

Cost of a Data Breach Report 2024

Data breach costs have hit a new high. Get essential insights to help your security and IT teams better manage risk and limit potential losses.

Read the report →



Strengthen your security intelligence

Stay ahead of threats with news and insights on security, AI and more, weekly in the Think Newsletter.

Subscribe today →

What is cloud computing?

The "cloud" or more specifically, "cloud computing" refers to the process of accessing resources, software and databases over the internet and outside the confines of local hardware restrictions. This technology gives organizations flexibility when scaling their operations by offloading a portion, or majority, of their infrastructure management to third-party hosting providers.

The most common and widely adopted cloud computing services are:

- **IaaS (Infrastructure-as-a-Service):** Offers a hybrid approach, which allows organizations to manage some of their data and applications on-premises. At the same time, it relies on cloud providers to manage servers, hardware, networking, virtualization and storage needs.
- **PaaS (Platform-as-a-Service):** Gives organizations the ability to streamline their application development and delivery. It does so by providing a custom application framework that automatically manages operating systems, software updates, storage and supporting infrastructure in the cloud.
- **SaaS (Software-as-a-Service):** Provides cloud-based software hosted online and typically available on a subscription basis. Third-party providers manage all potential technical issues, such as data, middleware, servers and storage. This setup helps minimize IT resource expenditures and streamline maintenance and support functions.

Why is cloud security important?

What are some cloud security challenges?

What types of cloud security solutions are available?

How should you approach cloud security?

Mixture of Experts | 23 May, episode 56

Decoding AI: Weekly News Roundup

Join our world-class panel of engineers, researchers, product leaders and more as they cut through the AI noise to bring you the latest in AI news and insights.

Watch the latest podcast episodes →

Why is cloud security important?

In modern-day enterprises, there has been a growing transition to cloud-based environments and IaaS, PaaS or SaaS computing models. The dynamic nature of infrastructure management, especially in scaling applications and services, can bring several challenges to enterprises when adequately resourcing their departments. These as-a-service models give organizations the ability to offload many of the time-consuming, IT-related tasks.

Why is cloud security important?

What are some cloud security challenges?

What types of cloud security solutions are available?

How should you approach cloud security?

As companies continue to migrate to the cloud, understanding the security requirements for keeping data safe has become critical. While third-party cloud computing providers can take on the management of this infrastructure, the responsibility of data asset security and accountability doesn't necessarily shift along with it.

By default, most cloud providers follow best security practices and take active steps to protect the integrity of their servers. However, organizations need to make their own considerations when protecting data, applications and workloads running on the cloud.

Security threats have become more advanced as the digital landscape continues to evolve. These threats explicitly target cloud computing providers due to an organization's overall lack of visibility in data access and movement. Without taking active steps to improve their cloud security, organizations can face significant governance and compliance risks when managing client information, regardless of where it is stored.

Cloud security should be an important topic of discussion regardless of the size of your enterprise. Cloud infrastructure supports nearly all aspects of modern computing in all industries and across multiple verticals.

However, successful cloud adoption depends on putting in place adequate countermeasures to defend against modern-day cyberattacks. Regardless of whether your organization operates in a public, private or hybrid cloud environment, cloud security solutions and best practices are a necessity for maintaining business continuity.

What are some cloud security challenges?

Why is cloud security important?

What are some cloud security challenges?

What types of cloud security solutions are available?

How should you approach cloud security?

Lack of visibility

It's easy to lose track of how your data is accessed and by whom because many cloud services are accessed outside of corporate networks and through third parties.

Multitenancy

Public cloud environments house multiple client infrastructures under the same umbrella. As a result, it's possible that your hosted services can get compromised by malicious attackers as collateral damage when targeting other businesses.

Access management and shadow IT

While enterprises may be able to successfully manage and restrict access points across on-premises systems, administering these same levels of restrictions can be challenging in cloud environments. This can be dangerous for organizations that don't deploy bring-your-own device (BYOD) policies and allow unfiltered access to cloud services from any device or geolocation.

Compliance

Regulatory compliance management is oftentimes a source of confusion for enterprises that use public or hybrid cloud deployments. Overall accountability for data privacy and security still rests with the enterprise, and heavy reliance on third-party solutions to manage this component can lead to costly compliance issues.

Misconfigurations

A substantial portion of breached records can be attributed to misconfigured assets, making the inadvertent insider a key issue for cloud computing environments. Misconfigurations can include leaving default administrative passwords in place, or not creating appropriate privacy settings.

Why is cloud security important?

What are some cloud security challenges?

What types of cloud security solutions are available?

How should you approach cloud security?

What types of cloud security solutions are available?

Identity and access management (IAM)

Identity and access management (IAM) tools and services allow enterprises to deploy policy-driven enforcement protocols for all users attempting to access both on-premises and cloud-based services. The core functionality of IAM is to create digital identities for all users so they can be actively monitored and restricted when necessary during all data interactions.

Data loss prevention (DLP)

Data loss prevention (DLP) services offer a set of tools and services designed to ensure the security of regulated cloud data. DLP solutions use a combination of remediation alerts, data encryption and other preventive measures to protect all stored data, whether at rest or in motion.

Security information and event management (SIEM)

Security information and event management (SIEM) provides a comprehensive security orchestration solution that automates threat monitoring, detection and response in cloud-based environments. SIEM technology uses artificial intelligence (AI)-driven technologies to correlate log data across multiple platforms and digital assets. This gives IT teams the ability to successfully apply their network security protocols, enabling them to quickly react to any potential threats.

Why is cloud security important?

What are some cloud security challenges?

What types of cloud security solutions are available?

How should you approach cloud security?

Business continuity and disaster recovery

Regardless of the preventive measures organizations have in place for their on-premises and cloud-based infrastructures, data breaches and disruptive outages can still occur. Enterprises must be able to quickly react to newly discovered vulnerabilities or significant system outages as soon as possible. Disaster recovery solutions are a staple in cloud security and provide organizations with the tools, services and protocols necessary to expedite the recovery of lost data and resume normal business operations.

How should you approach cloud security?

The way to approach cloud security is different for every organization and can depend on several variables. However, the National Institute of Standards

and Technology (NIST) has made a list of best practices that can be followed to establish a secure and sustainable cloud computing framework.

The NIST has created necessary steps for every organization to self-assess their security preparedness and apply adequate preventive and recovery security measures to their systems. These principles are built on the NIST's five pillars of a cybersecurity framework: Identify, protect, detect, respond and recover.

Another emerging technology in cloud security that supports the execution of NIST's cybersecurity framework is cloud security posture management (CSPM). CSPM solutions are designed to address a common flaw in many cloud environments, misconfigurations.

Cloud infrastructures that remain misconfigured by enterprises or even cloud providers can lead to several vulnerabilities that significantly increase an organization's attack surface. CSPM addresses these issues by helping to organize and deploy the core components of cloud security. These include identity and access management (IAM), regulatory compliance management, traffic monitoring, threat response, risk mitigation and digital asset management.

available?

How should you approach cloud security?

Resources

Report

IBM® X-Force® threat intelligence index 2025

Gain insights to prepare and respond to cyberattacks with greater speed and effectiveness with the IBM X-Force threat intelligence index.

Read the report →

Report

Cybersecurity in the era of generative AI

Learn how to navigate the challenges and tap into the resilience of generative AI in cybersecurity.

Read the report →

Report

IDC MarketScape: Cybersecurity Consulting Services Vendor Assessment 2024

See why IBM has been named a Major Player and gain insights for selecting the Cybersecurity Consulting Services Vendor that best fits your organization's needs.

Read the report →

Report

IBM® X-Force® cloud threat landscape report 2024

Understand the latest threats and strengthen your cloud defenses with the IBM X-Force cloud threat landscape report.

Read the report →

‹ 1 / 2 ›

Related solutions

Cloud security services

Protect your hybrid cloud and

Cloud security solutions

Move confidently to hybrid

IBM Security and Compliance Center

Address unified security,

multicloud environments through continuous visibility, management and remediation.

Explore cloud security services →

multicloud and integrate security into every phase of your cloud journey.

Explore cloud security solutions →

compliance and risk visibility across hybrid multicloud environments.

Explore IBM Security and Compliance Center →

Take the next step

Securely manage infrastructure and resources ahead of advanced threats. Our experts help ensure cloud and platform security, with broader visibility to cloud infrastructure, both now and into the ever-evolving future.

Explore cloud security services → | Explore cloud security solutions →

About IBM
- Overview
- Annual report
- Corporate social responsibility
- Inclusion@IBM
- Financing
- Investor
- Newsroom
- Security, privacy & trust
- Senior leadership
- Careers with IBM

IBM Research
- Website
- Blog
- Publications

Industry
- Automotive
- Banking
- Consumer Goods
- Energy
- Government
- Healthcare
- Insurance
- Life Sciences
- Manufacturing
- Retail
- Telecommunications
- Travel

Partners
- Our strategic partners
- Find a partner
- Become a partner - Partner Plus
- Partner Plus log in

Engage with IBM
- IBM TechXChange Community
- LinkedIn
- X
- Instagram
- YouTube
- Subscription Center
- Participate in user experience research
- Podcasts

United States — English

Contact IBM
Privacy

Terms of use
Accessibility

× Close

Hello! How can we help you?