What is cloud security management? A strategic guide

June 2024

In this guide:

Organizations of all sizes make use of cloud computing in some fashion, enabling them to work in more efficient ways without taking on the burden of fully managing applications and infrastructure. This comprehensive guide to cloud security examines the challenges of securing data and workloads. You'll find information about the strategies, tools and best practices that can address the many and evolving threats that cloud users confront. Throughout this guide, links point to articles that delve into particular facets of cloud security, from how to safely use public, hybrid and multi-cloud environments to ongoing security management and the products and services that can help.

In this guide:

What is cloud security management? A strategic guide

PHIL SWEENEY, INDUSTRY EDITOR

Organizations of all sizes make use of cloud computing in some fashion, enabling them to work in more efficient ways without taking on the burden of fully managing applications and infrastructure.

Use of cloud services continues to expand, with some estimates putting global spending in excess of $600 billion annually. And while those investments enable new and productive ways for businesses to interact with customers, suppliers, employees and partners, concerns about the security of those cloud environments are daunting. Surveys of IT staff and executives continue to show that costs and security are the top challenges organizations face in managing their use of cloud services.

This comprehensive guide to cloud security examines the challenges of securing data and workloads. You'll find information about the strategies, tools and best practices that can address the many and evolving threats that cloud users confront. Throughout this guide, links point to articles that delve into particular facets of cloud security, from the big strategic questions about how to safely use public, hybrid and multi-cloud environments to the finer points of ongoing security management and the products and services that can assist in those efforts.

In this guide:

While beneficial in many ways, cloud computing has its risks -- risks that cloud customers must learn to manage.

WHAT IS CLOUD SECURITY MANAGEMENT?

Cloud security management is a complementary combination of strategies, tools and practices that aims to help a business host workloads and data in a cloud efficiently and safely. This complicated endeavor to limit exposure to threats and vulnerabilities requires action on multiple fronts, including the following:

- Authentication and authorization. User management techniques, such as identity and access management (IAM), are essential to ensuring that only authorized users and devices access cloud workloads and data.
- Data security. Encryption is a crucial tool in guarding valuable business data against theft, loss and other unauthorized access.
- Suitable cloud architectures. Workloads are better protected from harm when they run on properly configured cloud architectures.
- Monitoring and reporting. Tools that continuously observe activities and events and provide real-time security alerts are essential for maintaining cloud security.

In this guide:

WHY IS SECURITY MANAGEMENT IN THE CLOUD IMPORTANT?

Failing to take ownership of cloud security is a serious blunder that could lead organizations to suffer data loss, system breaches and devastating attacks. In addition to the potential harm done to its customers and reputation, a business that's been breached can expect to incur costs on average of $4 million to $5 million, according to a 2023 study by IBM and the Ponemon Institute.

Perhaps naively, many organizations approach cloud computing with the notion that the business can offload the problems and responsibilities of everyday computing. While this might be true with respect to facilities maintenance and capital expenditures, a cloud customer still bears considerable responsibility for data compliance and security.

In fact, organizations that engage cloud services must reckon with numerous security challenges, owing to the enormous attack surface the cloud presents. In addition to data breaches, the following are some of the most pressing problems in managing cloud security:

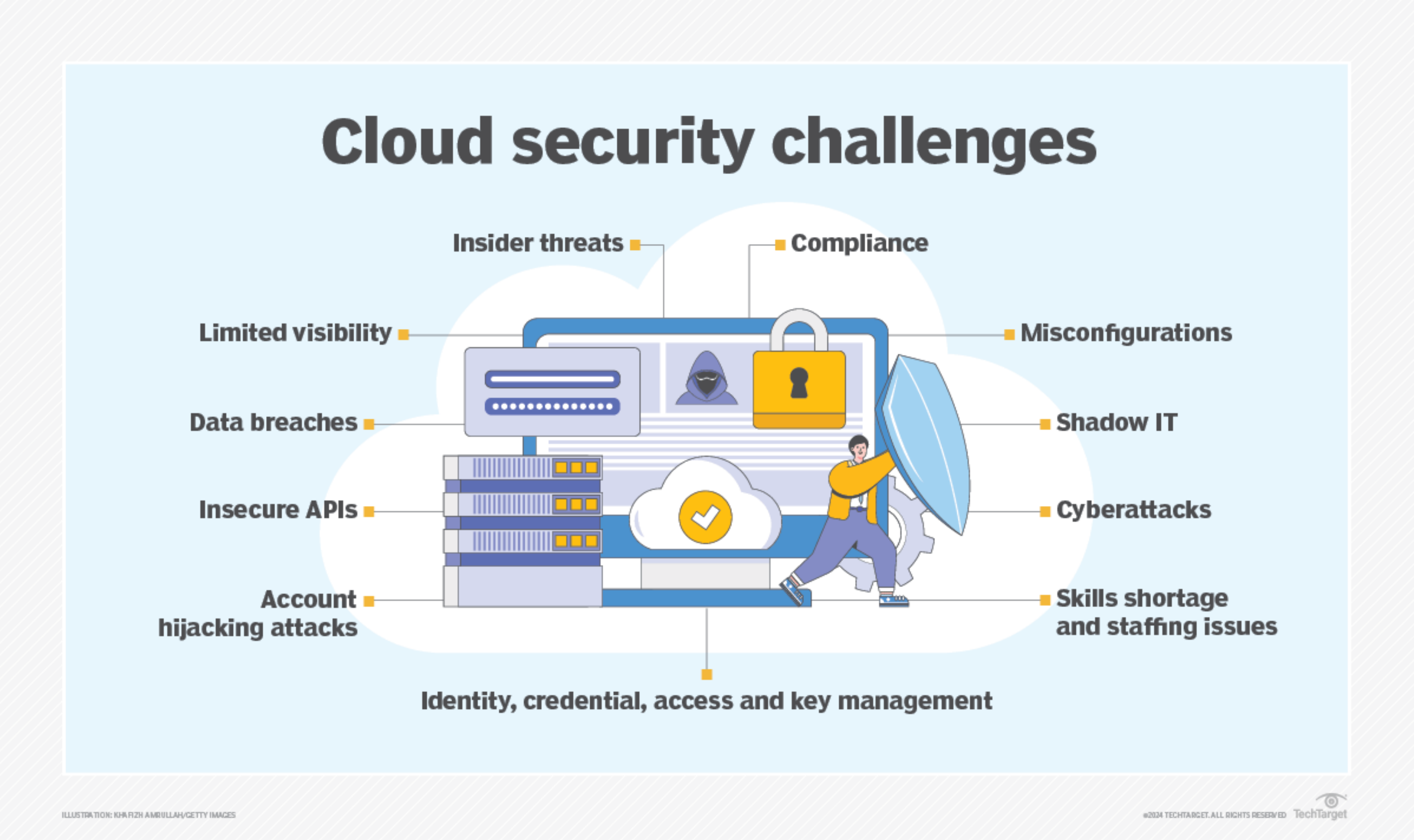
- Misconfigured cloud environments.
- Poorly secured APIs.
- Loose control over access and credentials.
- Insider threats.
- Account hijacking.
- Shadow IT.

The type of cloud environment an organization selects also affects security management and therefore must be carefully considered. Private, public and hybrid options each have advantages and drawbacks. With a public cloud strategy, a customer gains access to a service provider's cybersecurity tools and expertise, which will almost always be more extensive than what that business could muster on its own. Offloading some of those management duties comes with a tradeoff, however. It's the service provider -- not the customer -- that makes important cybersecurity decisions. And because the provider's underlying technologies are abstracted, a business will have little visibility into the resources on which its workloads run.

With a private cloud environment, an organization has full control of and visibility into its security picture; doing so, however, means accepting greater costs and complexity. And while a hybrid approach -- part public, part private -- might seem like the perfect compromise, it presents challenges, too, including policy enforcement across environments.

Companies must bear in mind that an attack on a single user's credentials can affect the entire organization. The fallout from cloud attacks is often exponential, and the blast radius of attacks continues to expand.

In this guide:



Cloud security challenges

Insider threats
Compliance
Limited visibility
Misconfigurations
Data breaches
Shadow IT
Insecure APIs
Cyberattacks
Account hijacking attacks
Skills shortage and staffing issues
Identity, credential, access and key management

ILLUSTRATION: KHAFIZH AMRULLAH/GETTY IMAGES

WHAT ARE THE BENEFITS OF CLOUD SECURITY MANAGEMENT?

Protecting cloud workloads and data is a demanding task. Still, when carefully implemented and managed, cloud security efforts give an organization the chance to fend off malicious actions. Not every threat can be stopped, but a business and a cloud provider working in concert can put formidable obstacles between valuable data and those who seek to take it.

Effective cloud security delivers advantages over a do-it-yourself approach to on-premises IT security, including the following benefits:

- **Better tools.** Cloud service providers offer comprehensive security tools that can scan, analyze, report and alert on potential security threats with a high degree of effectiveness. This alleviates the need for users to install and operate their own security applications or tools in the cloud.
- **Security services.** Service providers typically offer cloud encryption and other services, such as data loss prevention (DLP), that are designed to protect business data at rest and in flight. Data backups, recovery, disaster recovery and other services can further protect vital business data from harm.
- **Lower security costs.** Businesses can often lower security costs and improve security effectiveness when using the sophisticated security tools and services supplied through cloud providers. These offerings are typically updated more frequently and tested more comprehensively than security tools deployed in local data centers.

WHAT ARE THE CHALLENGES OF CLOUD SECURITY MANAGEMENT?

The cloud model requires users to come to terms with its inherent complexity. Cloud management is a difficult and ongoing task. From a security perspective, the challenges include the following:

- **Shared responsibility.** Cloud computing operates on a shared responsibility model, but there are often misunderstandings about which responsibilities fall to the service provider and which belong to the customer. When there's confusion, the likelihood increases that something important will be missed. That creates critical gaps in security management.
- **Limited visibility.** If you can't see it, you can't manage it. It's an old axiom that perfectly suits cloud security efforts. A business that migrates its applications and data to cloud environments confronts a complicated situation in which control is decentralized. Different business teams and divisions, for example, might each make decisions about how they use cloud services. Without a means of discovering, tracking and reporting on the assets present in the cloud, an in-house security team might not even know what it is supposed to be managing.
- **Compliance challenges.** A business is obligated to know where its cloud data is located and how it is being used. When a cloud provider obscures this information -- or a user does not bother to access this information -- the business could experience a costly breach in regulatory compliance. It's important to understand the tools and visibility offered by a provider and to know how that information helps a business meet its compliance requirements.

In this guide:

- **Limited control.** While they can assert considerable control over user authorization and authentication, public cloud customers typically have little control over the underlying cloud infrastructure, which is owned by the service provider. This can lead to security concerns in how data is accessed and shared.
- **Cloud differences.** As businesses explore hybrid and multi-cloud environments, they will find any number of differences in tools, services, configurations and capabilities. For instance, multi-cloud security poses some specific challenges. These differences could result in a business having an inconsistent or incomplete security posture. Consultations with the providers can help address this heterogeneity.

WHO IS RESPONSIBLE FOR CLOUD SECURITY?

Security in cloud computing relies on the shared responsibility model, which places certain responsibilities on the cloud service provider and other responsibilities on the cloud customer. At a high level, this model stipulates that the service provider bears responsibility for security *of* its cloud, while the cloud customer is responsible for security *in* the cloud. It might seem like a fine distinction, but it's a vital one to understand:

- A cloud provider ensures that its infrastructure and services operate in a secure manner. Its servers and networks, for example, must be set up and configured securely.

- A cloud user takes steps to deploy the security features necessary to securely operate VMs and workloads while carefully controlling access to that cloud environment.

As an example, suppose a cloud provider offers IAM services to help customers manage user access to workloads and data. A customer that chooses to forego those services effectively opens access to workloads and data to anyone. The business has neglected its duty to maintain cloud security and, in the process, likely violated compliance and other regulatory obligations. In this scenario, the cloud customer -- not the service provider -- would bear responsibility for any data loss.

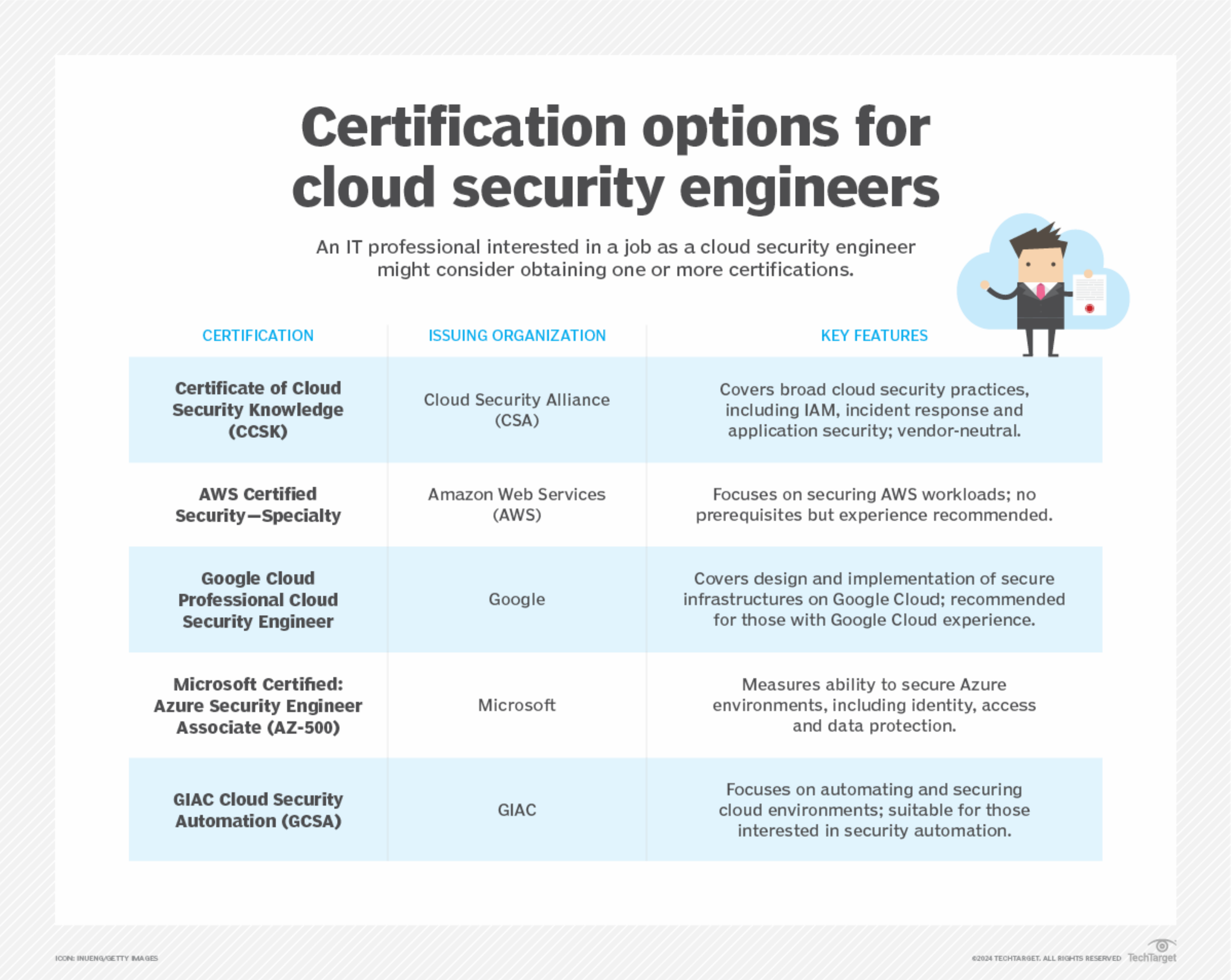
While traditional enterprise security teams can take on some cloud security duties, specific expertise is needed to ensure the ongoing and effective protection of cloud data and workloads. For example, a skilled cloud security engineer will have knowledge about cloud platforms, programming languages, security tools and other relevant topics.

An in-house security team might address cloud security automation in four key areas:

- Container, VM and serverless computing configurations.
- Infrastructure as code and other automated infrastructure composition techniques.
- Asset tagging and other cloud inventory management tactics.
- Vulnerability scanning.

Setting and managing IaaS controls and processes in these areas enables smooth and consistent deployments, proper auditing and reporting, and policy application and enforcement.

These special-purpose teams should follow cloud compliance standards closely, making sure service providers are current on the latest industry requirements. Various professional and technical organizations address compliance standards, offering recommendations and guidance for successful cloud implementation.



Certification options for cloud security engineers

An IT professional interested in a job as a cloud security engineer might consider obtaining one or more certifications.

CERTIFICATION	ISSUING ORGANIZATION	KEY FEATURES
Certificate of Cloud Security Knowledge (CCSK)	Cloud Security Alliance (CSA)	Covers broad cloud security practices, including IAM, incident response and application security; vendor-neutral.
AWS Certified Security—Specialty	Amazon Web Services (AWS)	Focuses on securing AWS workloads; no prerequisites but experience recommended.
Google Cloud Professional Cloud Security Engineer	Google	Covers design and implementation of secure infrastructures on Google Cloud; recommended for those with Google Cloud experience.
Microsoft Certified: Azure Security Engineer Associate (AZ-500)	Microsoft	Measures ability to secure Azure environments, including identity, access and data protection.
GIAC Cloud Security Automation (GCSA)	GIAC	Focuses on automating and securing cloud environments; suitable for those interested in security automation.

ICON: INUENG/GETTY IMAGES

In this guide:

Cloud security training continues to improve, and certifications can demonstrate professional training. The ISC2 Certified Cloud Security Professional program, for example, tests a cybersecurity professional's technical skills in securing cloud applications and infrastructure. Another popular certification is the Certificate of Cloud Security Knowledge from the Cloud Security Alliance. Test takers must show expertise in data encryption, identity access, incident response and other essential aspects of cloud security. Cybersecurity training is also available from GIAC, Arcitura, SANS Institute and other groups.

BUILDING A CLOUD SECURITY POLICY

Any organization that commits to cloud computing will want to create a cloud security policy. The policy should address critical considerations, such as how employees can interact with the cloud, the types of data the organization will allow in the cloud, access controls for a cloud environment and more.

To design a cloud security policy, consider these starting points:

- Add cloud elements into an existing cybersecurity policy.
- Evaluate and select software from vendors that can produce policies quickly.
- Review cloud security standards for frameworks and content that can be built into the policy.

When a policy is not in place, a company could be at greater risk of security breaches and data loss. A business without relevant policies might also face penalties for noncompliance.

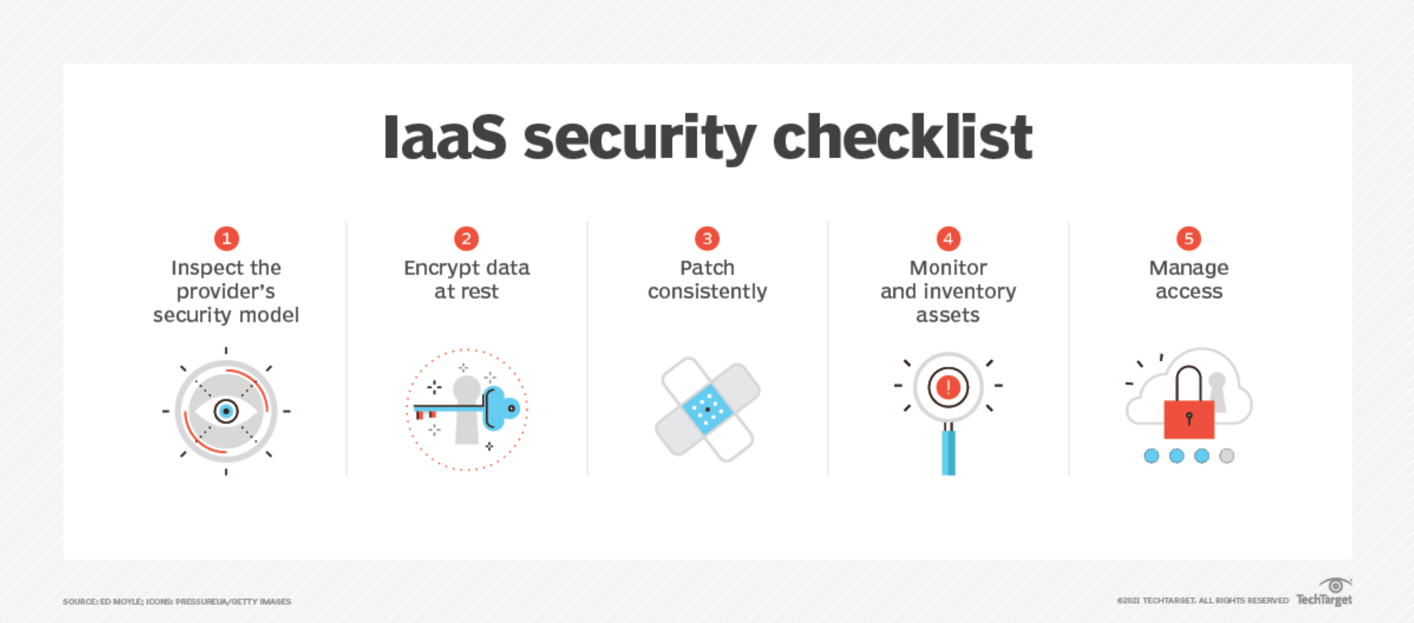
How you organize cloud security policies will also depend on the type of cloud service being used: SaaS, IaaS or PaaS.

SaaS security best practices. SaaS is not a monolithic service and shouldn't be treated as such when it comes to security. Organizations should review the best practices to protect SaaS-based applications and apply the ones that best fit the service being adopted. Experts advise customers to inventory cloud assets, as this clarifies exactly which applications are in use; to deploy enhanced authentication, such as multifactor authentication, where possible; and to encrypt data in motion and at rest.

IaaS security best practices. Like SaaS, IaaS requires organizations to consider how to encrypt data and inventory cloud assets, but securing infrastructure in the cloud requires even more attention. IaaS gives users extensive access to the provider's resources and services, which can be composed as desired to create an operating environment suitable for hosting a business workload and data. Organizations need to develop an IaaS security checklist. This begins with

In this guide:

understanding a specific cloud provider's security practices, ensuring consistent patching and managing access.



SOURCE: ED MOYLE; ICONS: PRESSUREUA/GETTY IMAGES

PaaS security best practices. PaaS security guidelines recommend that organizations be deeply involved in the protection of their platform services and not leave the details to the provider. For example, enterprises should engage in threat modeling and the deconstruction of an application design, which will help identify vulnerabilities and mitigate them. The PaaS provider will offer security tooling and capabilities, but it's up to PaaS users to employ those features. Another key best practice for PaaS users is to carefully plan out portability so the organization isn't bound to one provider. For example, software development PaaS users might choose to work with common programming languages -- such as C#, Python and Java -- that are widely supported.

CLOUD SECURITY MANAGEMENT STRATEGIES

Rarely do organizations have a single cloud environment. It's more likely that they have multiple ones to address various data, application, platform and infrastructure needs. Managing disparate cloud services can be challenging, so organizations need a sound strategy that protects corporate assets while maintaining compliance and managing costs.

To prevent or rein in sprawl, organizations should centralize the procurement, deployment and management of their multi-cloud environments. Doing so can ensure an organization's security policies and compliance requirements are applied and enforced. Centralizing also is critical for organizations to be able to collaborate and communicate in a uniform way about threats and mitigation strategies. Emerging FinOps practices can help establish collaborative cross-discipline teams tasked with managing cloud use, security and spending.

Cloud security teams need to test their cloud environments regularly. Testing is essential for the shared responsibility model, where in-house and provider security teams together assume the role of protecting assets in the cloud. Cloud penetration testing is a useful way to test the shared responsibility model and the security of a cloud environment overall.

Some organizations in highly regulated or high-risk industries might want to employ forensics techniques in their cloud environment. Automation should be top of mind for this goal so that organizations can not only inspect and analyze information in the cloud for court proceedings (e.g., network packets, workload memory, workload disk volumes, logs and other event data) but also mitigate any problems that are discovered.

One of the most significant types of attacks security teams must ward off through better cloud security management is account hijacking, in which hackers compromise a subscription or other type of cloud account to engage in malicious activity. To protect against account hijacking, security teams should take three crucial steps: require multifactor authentication; segregate duties; and trust but verify account access.

One often overlooked aspect of cloud security testing and security management is information sharing. Although there are many tools and practices that can help to find and fix security problems, answers to the following questions can easily be lost or ignored unless documented and shared across the cloud management team:

- What happened?
- Why did it happen?
- What was the root cause?
- What was the remediation?
- What were the results?
- How should policy, practices and processes be adjusted?

Information sharing enables the entire cloud management team to benefit and learn from problems or incidents that affect cloud security.

IMPLEMENTING CLOUD SECURITY MANAGEMENT

Approaches to implementing and managing cloud security are as varied as the tools and businesses that use cloud computing. Still, several guiding principles can be applied to implementation:

- **Understand the business drivers and goals.** Cloud security -- and its proper management -- is there for a purpose, which is to serve the business and facilitate business interests. Any implementation of cloud security management should be in response to business needs. A highly regulated business, for example, will make compliance a primary goal of its security efforts.
- **Understand the threats.** From malware to intrusion to disasters, it's vital to understand where the attacks will come from and how those attacks put the business -- and its goals -- at risk. Perform regular security audits on cloud-based workloads, data and services. By properly identifying the threats it faces,

an organization will find it easier to build new policies and processes as well as to select tools suitable for the task.

- **Select and implement tools.** A business has plenty of tools, platforms and services available to help manage cloud security. One size does not fit all, and each product has specific strengths and tradeoffs. Knowing the business goals and intended practices, however, makes the job of finding and validating cloud security management tools considerably easier. This could still require some adjustments to principles and practices, but the underlying ideas should be consistent.
- **Encrypt data and monitor.** Data should ideally be encrypted at rest and in flight. User and workload access should adopt a zero-trust model and other highly restricted postures. Monitor network traffic and watch for intrusion. Scan for malicious activity, such as unauthorized data access. Oversee end users and devices.
- **Report.** Use the alerting and reporting features of cloud security systems to deliver timely security reports to cloud workload stakeholders and business leaders. Recognize the threats (e.g., an unpatched OS) and take proactive action to mitigate those risks.
- **Reevaluate.** Threats and business needs are always changing, and so should cloud security. To address new and emerging threats, a business will likely need a team effort involving business, technology and legal leadership from across the organization.

Other strategies an organization might consider include adoption of cloud infrastructure entitlement management, a discipline that aims to more rigorously track who has access to cloud infrastructure, and cloud vulnerability management, an emerging tactic to provide continuous remediation of detected vulnerabilities.

Not surprisingly, security vendors are attempting to incorporate AI into their products. Experts predict AI will be helpful in the following areas, among others:

- Detection and remediation of misconfigurations.
- User behavior analysis.
- Threat detection and response.

The prospect of AI being used offensively is a growing concern. In fact, 38% of respondents in a 2024 survey of infosec professionals by Palo Alto Networks ranked AI-powered attacks as one of their leading cloud security worries.

A CLOUD SECURITY CHECKLIST

To determine the effectiveness of cloud security practices, an organization will need to be methodical about checking its defenses. It's not enough to simply implement security; these measures require ongoing assessment and adjustment.

A business should take the time to develop a cloud security assessment process. Through this process, IT teams will learn about potential risks they did not know they faced. Plus, they'll be able to learn the answers to important questions, such as the following:

- **How extensive is our attack surface?** A business cannot mount an adequate defense against cloud threats until it determines exactly how many cloud services and applications are in use.
- **Which assets are most at risk?** An assessment can identify where insufficiently secured images and workloads are being created.
- **Are IAM practices effective?** Organizations that carefully examine their access policies typically find they have been overly generous with granting of permissions. By limiting access, you limit risks.
- **Is the architecture properly designed?** Service providers can help their customers design cloud environments that stand a better chance of withstanding an attack.
- **Do we know when there's a problem?** Tools that monitor and log cloud security incidents can be useful, but these tools need to be checked to verify that they are paying attention to the right things.
- **What about compliance?** Routine assessments will give an organization the chance to see how well it is meeting its compliance responsibilities.

In addition to uncovering potentially unpleasant surprises, ongoing security assessments will reinforce the absolutely essential idea that the cloud security task is never fully accomplished.

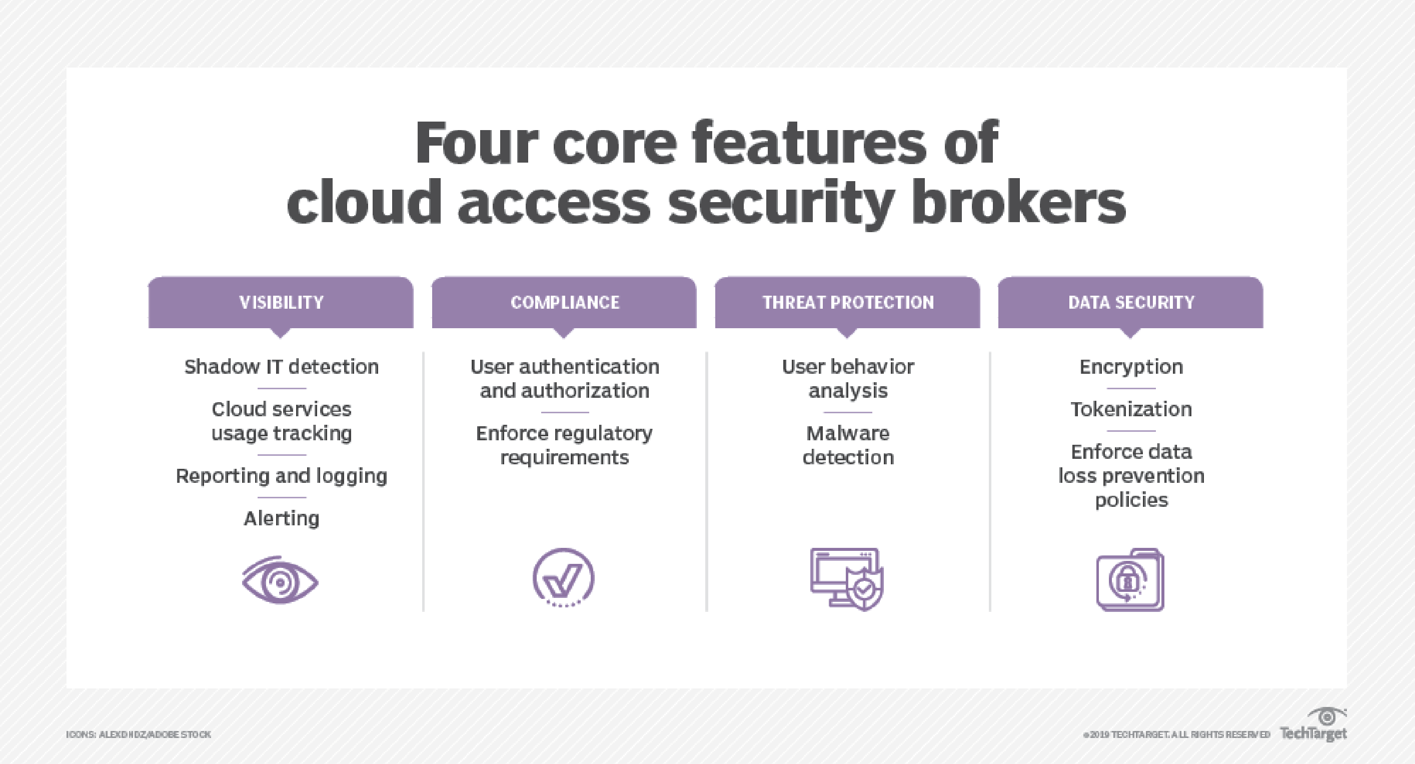
CLOUD SECURITY TOOLS

Some security tools used on-premises can be extended to protect cloud workloads, but tools and tactics designed specifically for cloud computing will provide more seamless and comprehensive protection. Here are some common product categories:

Cloud access security brokers. Cloud access security brokers (CASBs) serve as a security policy enforcement gateway to ensure users' actions are authorized and compliant with company policies. They have four main characteristics: visibility, compliance, threat protection and data security.

CASBs also have business-critical use cases, such as cloud application usage tracking and user behavior analytics.

In this guide:



Four core features of cloud access security brokers

VISIBILITY	COMPLIANCE	THREAT PROTECTION	DATA SECURITY
Shadow IT detection	User authentication and authorization	User behavior analysis	Encryption
Cloud services usage tracking	Enforce regulatory requirements	Malware detection	Tokenization
Reporting and logging			Enforce data loss prevention policies
Alerting			

ICONS: ALEXDNDZ/ADOBE STOCK

©2019 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Cloud security posture management tools. Cloud security posture management (CSPM) tools enable companies to perform continuous compliance monitoring, prevent configuration drift, set limits on permittable configurations or behavior in the cloud and support security operations center investigations.

Organizations can use CSPM tools to uniformly apply cloud security best practices to increasingly complex systems, such as hybrid, multi-cloud and container environments.

Cloud workload protection platforms. A cloud workload protection platform (CWPP) can safeguard workloads regardless of whether they run on a physical server, on a virtual server, as a serverless function or in a container. A CWPP tool should enhance security through several key capabilities, including the following functions:

- Tracking workloads on premises and in one or more cloud environments.
- Monitoring workload configurations.
- Scanning for malware.

Cloud-native application protection platform. One of the stresses of cloud security management is the abundance of security tools on the market. Vendors in the cloud-native application protection platform (CNAPP) category seek to address this by bundling capabilities from several tools into a single product. These tools are designed to integrate multiple security functions, including monitoring, response, analysis and optimization, thereby reducing the number of standalone products a team would need to select, adopt and manage.

CLOUD SECURITY MANAGEMENT VENDORS

There are countless vendors and products available for cloud security management. Each product, platform or service focuses on unique specialties or use cases; might offer some overlap in CASB, CSPM, CNAPP or CWPP areas; and carries its own unique tradeoffs for enterprise users. As with most enterprise tools, it's worth evaluating a number of offerings and investing in proof-of-concept projects to identify and validate preferred products before making a commitment.

Examples of **CASB** vendors and tools include the following:

- Avast Secure Internet Gateway.
- Cato SASE Cloud.
- Citrix Secure Workspace Access.
- Citrix Workspace Essentials.
- Forcepoint One.
- Fortinet FortiCASB.
- Microsoft Defender for Cloud.
- Netskope.
- Oracle CASB Cloud Service.
- Proofpoint Cloud App Security Broker.
- SonicWall Cloud App Security.
- Symantec CloudSOC CASB.
- Symantec Cloud Secure Web Gateway.
- Trend Micro Cloud App Security.

Examples of **CSPM** vendors and tools include the following:

- Check Point CloudGuard.
- CrowdStrike Falcon Cloud Security.
- Cyscale.
- Lacework Polygraph Data Platform.
- Microsoft Defender for Cloud.
- Orca Security.
- Palo Alto Networks Prisma Cloud.
- Rapid7 InsightCloudSec.
- Sonrai Security.
- Sysdig Secure.
- Tenable Cloud Security.
- Trend Micro Cloud One Conformity.
- Zscaler Posture Control.

Examples of **CWPP** vendors and tools include the following:

- AWS Control Tower.
- AWS GuardDuty.
- Check Point CloudGuard Network Security (IaaS).
- CrowdStrike Falcon Cloud Security.
- Google Cloud Security.
- Illumio Core.
- Microsoft Defender for Cloud.
- Orca Security.
- Palo Alto Networks Prisma Cloud.

- PingSafe.
- SentinelOne Singularity Cloud.
- Sophos Cloud Workload Protection.
- Trend Micro Deep Security.
- VMware Carbon Black Workload.

Editor's note: *The lists above have been assembled from varied research sources and are meant to provide examples only; they are not intended to represent all available products in a given area. Readers are advised to perform their own research and make product selections based on their own needs, research and testing results.*

Phil Sweeney is an industry editor and writer focused on information security topics.

Stephen J. Bigelow, senior technology editor at TechTarget, has more than 20 years of technical writing experience in the technology industry.

▼ **CONTINUED READING**

- **How AI is transforming cloud security, according to experts**
- **Cloud vulnerabilities that can cripple your environment**
- **Best cloud security certifications for IT pros**