TechTarget | SearchCloud Security

E-guide

PRO+ Content

Guide to Cloud Security Management and Best Practices

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

In this e-guide:

This cloud security guide explains the challenges facing enterprises today, best practices for securing and managing SaaS, IaaS and PaaS, and comparisons of cloud-native security tools.

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

Guide to cloud security management and best practices

Sandra Gittlen, *Editor at Large, SearchCloudSecurity*

Organizations of all sizes have adopted cloud strategies to varying degrees. While beneficial in many ways, the cloud also has its risks, which organizations should fully assess before placing assets there. In this comprehensive guide, complete with links to more information, we lay out the challenges in securing the cloud environment as well as how to develop best practices for managing cloud security.

Why is cloud security important?

Far too often, organizations place their trust in cloud providers to ensure a secure environment. Unfortunately, that approach has numerous problems -- namely that cloud providers don't always know the risk associated with a customer's systems and data. They don't have visibility into other components in the customer's ecosystem and the security requirements of those components. Failing to take ownership of cloud security is a serious downfall that could lead organizations to suffer data loss, system breaches and devastating attacks.

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

The Cloud Security Alliance shared the most common cloud security challenges to give organizations a sense of the massive attack surface cloud computing presents. In addition to the potential for data breaches and lack of visibility, the following are some of the most egregious problems the alliance found:

- misconfigurations and inadequate change controls;
- lack of cloud security architecture and strategy;
- insufficient identity, credential, access and key management;
- account hijacking;
- insecure interfaces and APIs; and
- abuse and nefarious use of cloud services.

The fallout from cloud attacks is often exponential, and the blast radius of attacks continues to expand. For example, "an attack on a single user's credentials reaches far beyond the targeted victim, often affecting the entire organization and its customers," wrote Dave Shackleford, principal consultant at Voodoo Security. Recent attacks also illustrate an immaturity of organizations' ability to defend their cloud environments, he added.

Image on the next page

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

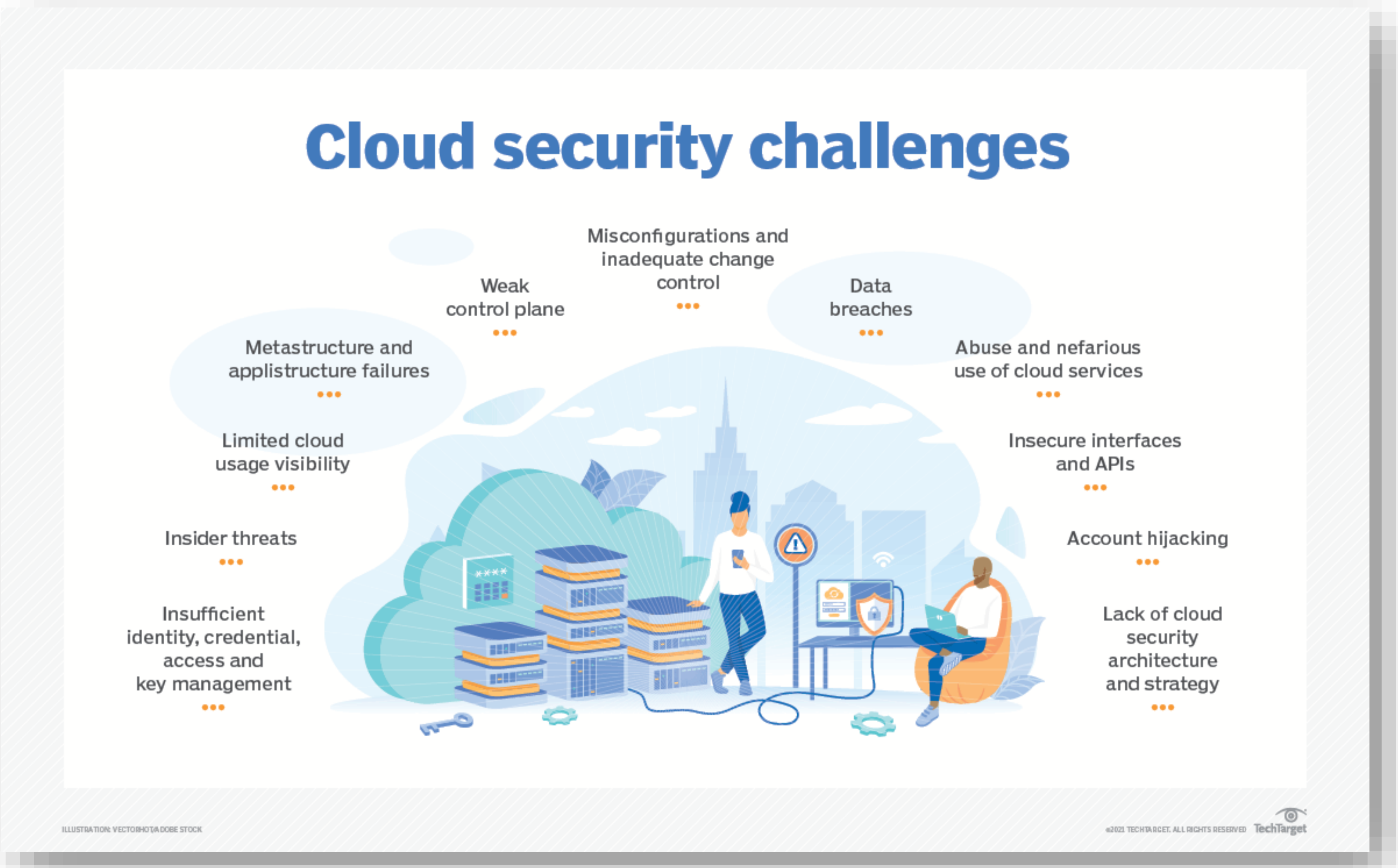
Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17



Cloud security challenges

Misconfigurations and inadequate change control

Weak control plane

Data breaches

Metastructure and applistructure failures

Abuse and nefarious use of cloud services

Limited cloud usage visibility

Insecure interfaces and APIs

Insider threats

Account hijacking

Insufficient identity, credential, access and key management

Lack of cloud security architecture and strategy

ILLUSTRATION: VECTORHOT/ADOBE STOCK

©2021 TECHTARGET. ALL RIGHTS RESERVED TechTarget

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

The type of cloud environment an organization selects must be well-considered because private, public and hybrid options each have pros and cons. For instance, a public cloud strategy can lighten the load on an organization's IT team since they don't have to manage systems in-house. A public cloud provider might not be as particular as the organization about security, however, which could leave gaps in the organization's protection.

With a private cloud environment, an organization might gain more control over security, but cloud costs will likely rise as a result. And while a hybrid approach -- part public, part private -- might seem like the perfect compromise, it presents challenges too, including policy enforcement across environments.

Best practices for cloud security

Once an organization has committed to a cloud environment for data, applications, platforms and infrastructure, the next task is 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 that can be sent and stored there, access controls and more.

While developing a cloud security policy can be done using many approaches, including adapting an existing infosec policy or using a software package, independent IT consultant and auditor Paul Kirvan created a cloud security policy template that walks organizations through policy creation.

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

How you address cloud security is also dependent on the type of cloud service an organization needs: 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. Instead, organizations need to look at a roster of guidelines and apply the ones that best fit the service being adopted. Ed Moyle, software security principal at Adaptive Biotechnologies, laid out the following best practices to protect SaaS-based applications:

- vet and oversee potential providers;
- deploy enhanced authentication, such as multifactor authentication (MFA), where possible;
- encrypt data in motion and at rest in the cloud; and
- utilize manual and automatic methods to discover and inventory cloud assets.

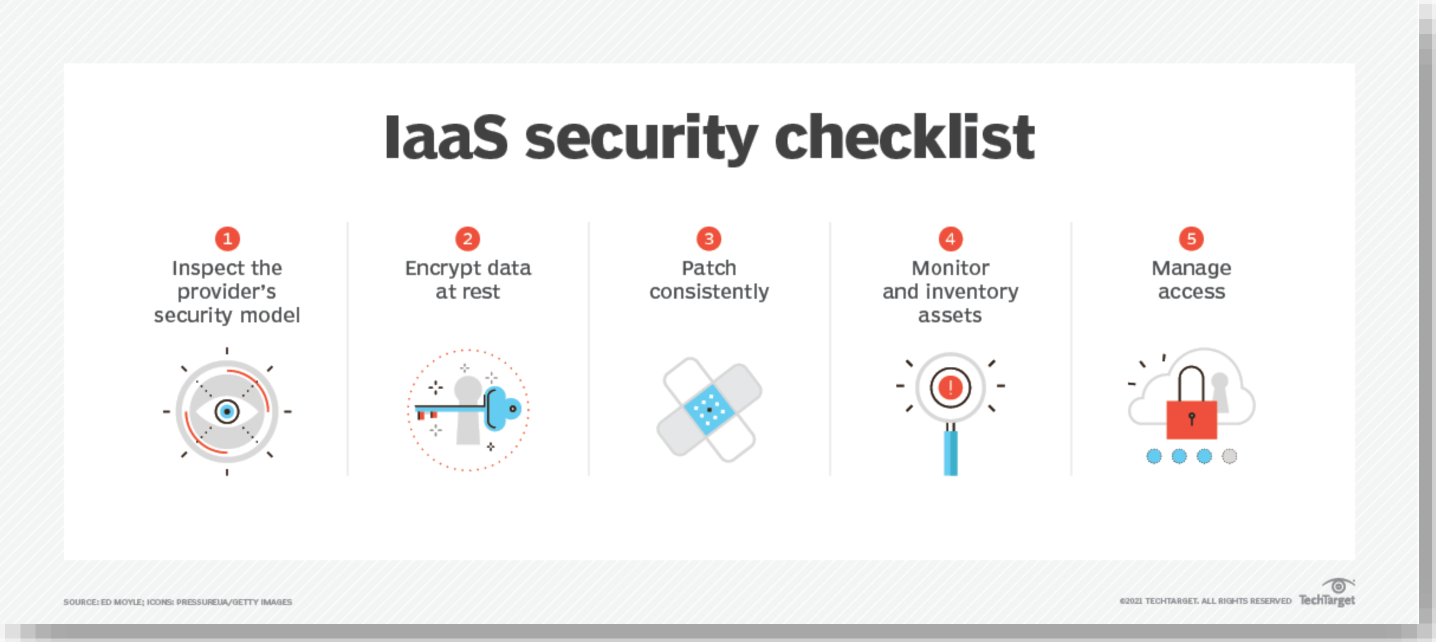
SaaS also requires a corporate culture where IT and security teams work together to secure a cloud-based business application.

IaaS security best practices

Like SaaS, IaaS requires organizations to consider how to encrypt data at rest and inventory cloud assets, but securing infrastructure in the cloud requires even more attention to security. Organizations need to develop an IaaS security checklist to ensure consistent patching and access management. IaaS has many access layers to be

Guide to cloud security management and best practices p. 2
Why is cloud security important? p. 2
Best practices for cloud security p. 5
Who is responsible for cloud security? p. 8
Cloud security management strategies p. 12
Cloud security tools p.13
Further reading p. 17

managed, including access to the IaaS console and specific features such as backup and recovery.



IaaS security checklist

1 Inspect the provider's security model

2 Encrypt data at rest

3 Patch consistently

4 Monitor and inventory assets

5 Manage access

SOURCE: ED MOYLE; ICONS: PRESSUREUA/GETTY IMAGES

©2021 TECHTARGET. ALL RIGHTS RESERVED TechTarget

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 up to the provider. For example, enterprises should engage in threat modeling and the deconstruction of an

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

application design, which will help identify vulnerabilities and mitigate them, according to Moyle.

Another key best practice for PaaS users is to carefully plan out portability so the organization isn't bound to one provider. One way to do this is to use common programming languages -- such as C#, Python and Java -- that are supported across providers.

Who is responsible for cloud security?

While traditional enterprise security teams can take on some cloud security duties, protecting cloud data and other assets requires a specific skillset.

Organizations should create a cloud IAM team dedicated to certain aspects of cloud security, such as access, authentication and authorization. Shackleford recommended that the cloud IAM team, which could tackle single sign-on and federation, should be started with existing internal groups because they have a deep understanding of the business and its goals.

A dedicated IaaS team might also address cloud security automation in four key areas:

- container configuration;
- infrastructure as code;
- asset tagging; and
- vulnerability scanning.

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

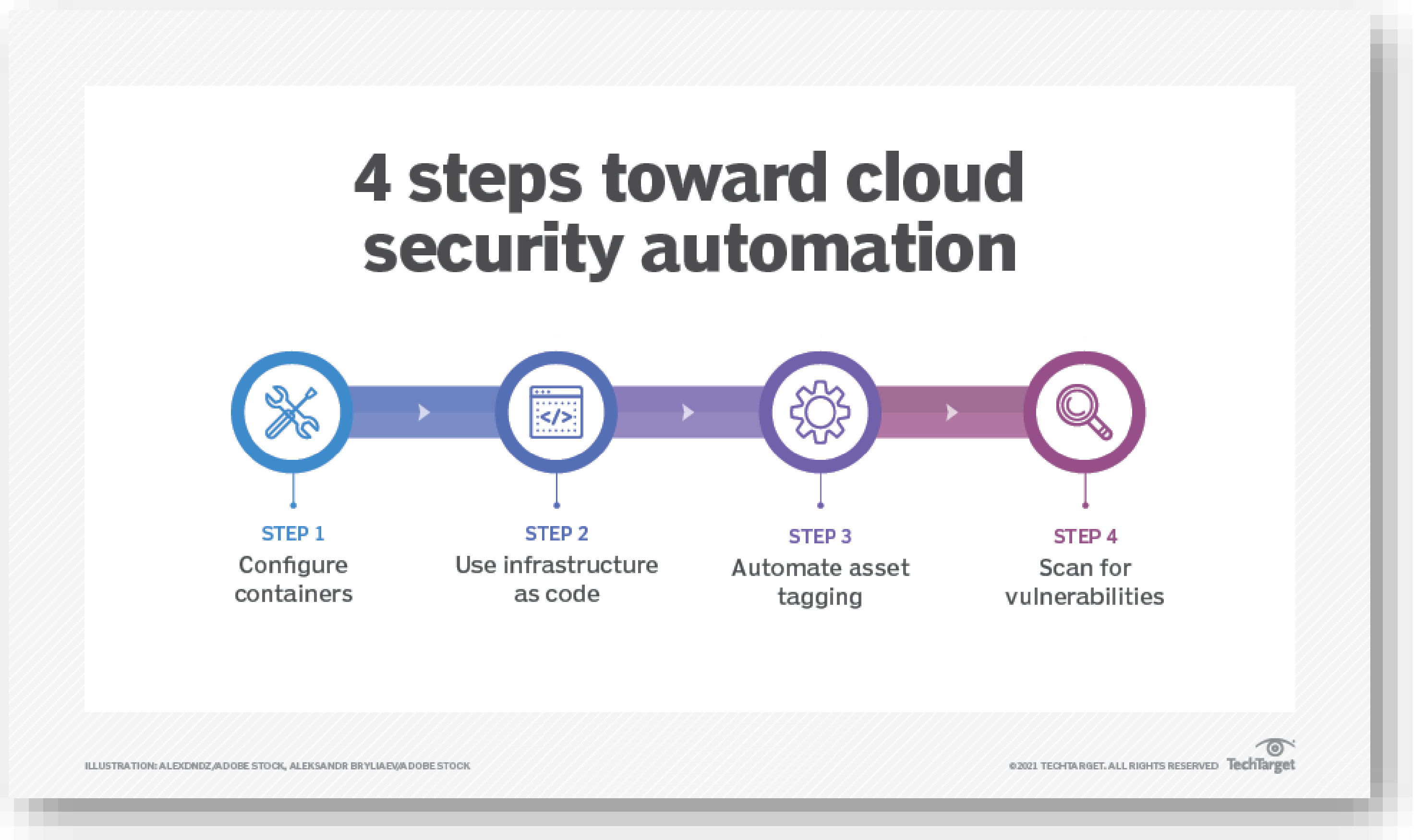
Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

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



4 steps toward cloud security automation

STEP 1
Configure containers

STEP 2
Use infrastructure as code

STEP 3
Automate asset tagging

STEP 4
Scan for vulnerabilities

ILLUSTRATION: ALEXDNDZ/ADOBE STOCK, ALEKSANDR BRYLIAEV/ADOBE STOCK

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

These special-purpose teams follow cloud compliance standards closely, making sure cloud service providers are up on the latest industry requirements. Read about the top cloud security standards bodies and their areas of compliance oversight.

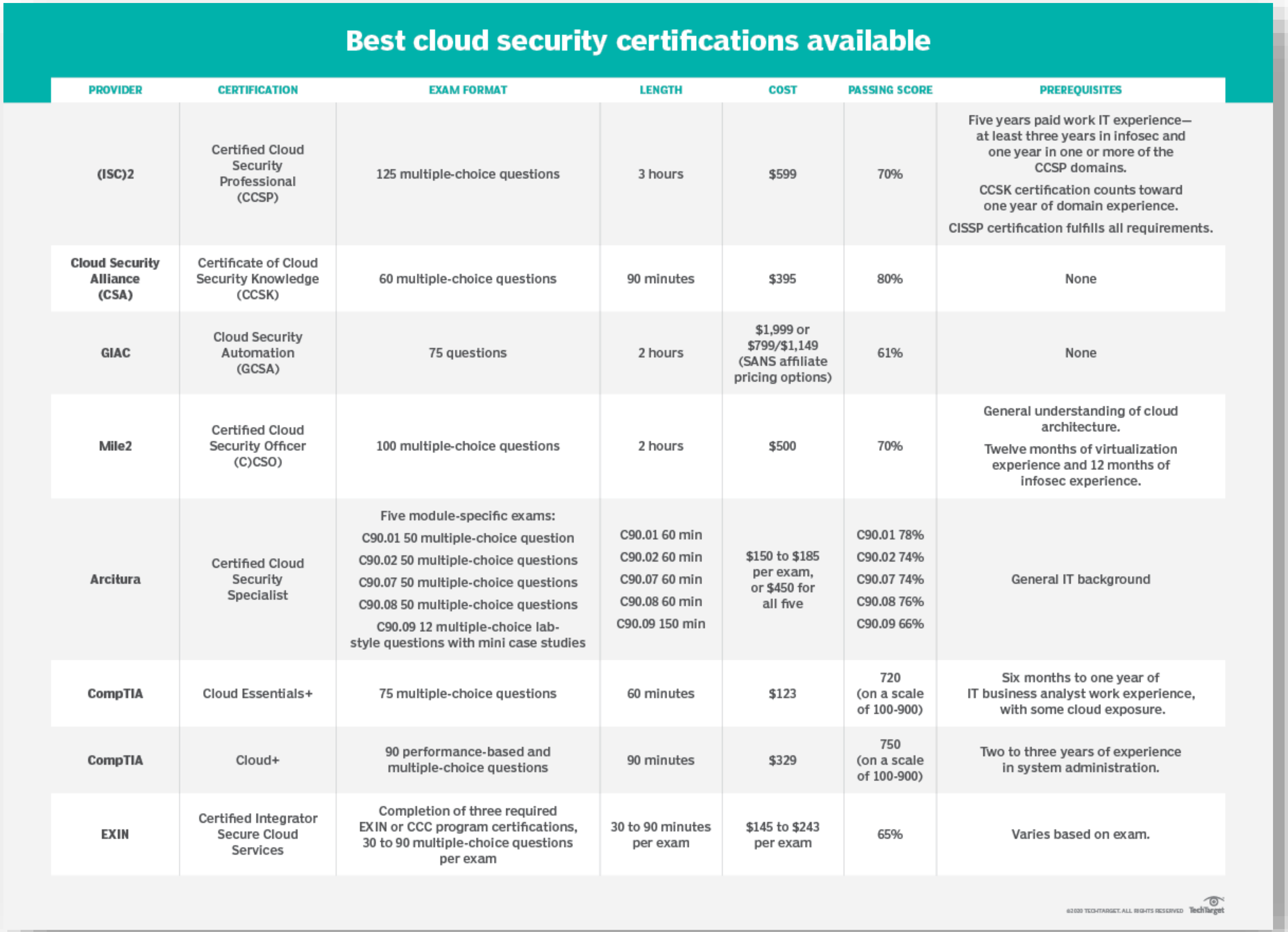
Cloud security training has improved in recent years, and targeted certifications can demonstrate a professional's cloud security chops. For instance, (ISC)^2 has a Certified Cloud Security Professional (CCSP) certification, and the Cloud Security Alliance offers a Certificate of Cloud Security Knowledge. CompTIA, Arcitura and Exin also have programs, as do vendors such as Amazon, Google and Microsoft.

Cloud security-savvy professionals can test their bona fides with these CCSP exam questions.

↘ Image on the next page

In this e-guide

- Guide to cloud security management and best practices p. 2
- Why is cloud security important? p. 2
- Best practices for cloud security p. 5
- Who is responsible for cloud security? p. 8
- Cloud security management strategies p. 12
- Cloud security tools p.13
- Further reading p. 17



Best cloud security certifications available

PROVIDER	CERTIFICATION	EXAM FORMAT	LENGTH	COST	PASSING SCORE	PREREQUISITES
(ISC)2	Certified Cloud Security Professional (CCSP)	125 multiple-choice questions	3 hours	$599	70%	Five years paid work IT experience—at least three years in infosec and one year in one or more of the CCSP domains. CCSK certification counts toward one year of domain experience. CISSP certification fulfills all requirements.
Cloud Security Alliance (CSA)	Certificate of Cloud Security Knowledge (CCSK)	60 multiple-choice questions	90 minutes	$395	80%	None
GIAC	Cloud Security Automation (GCSA)	75 questions	2 hours	$1,999 or $799/$1,149 (SANS affiliate pricing options)	61%	None
Mile2	Certified Cloud Security Officer (C)CSO)	100 multiple-choice questions	2 hours	$500	70%	General understanding of cloud architecture. Twelve months of virtualization experience and 12 months of infosec experience.
Arcitura	Certified Cloud Security Specialist	Five module-specific exams: C90.01 50 multiple-choice question C90.02 50 multiple-choice questions C90.07 50 multiple-choice questions C90.08 50 multiple-choice questions C90.09 12 multiple-choice lab-style questions with mini case studies	C90.01 60 min C90.02 60 min C90.07 60 min C90.08 60 min C90.09 150 min	$150 to $185 per exam, or $450 for all five	C90.01 78% C90.02 74% C90.07 74% C90.08 76% C90.09 66%	General IT background
CompTIA	Cloud Essentials+	75 multiple-choice questions	60 minutes	$123	720 (on a scale of 100-900)	Six months to one year of IT business analyst work experience, with some cloud exposure.
CompTIA	Cloud+	90 performance-based and multiple-choice questions	90 minutes	$329	750 (on a scale of 100-900)	Two to three years of experience in system administration.
EXIN	Certified Integrator Secure Cloud Services	Completion of three required EXIN or CCC program certifications, 30 to 90 multiple-choice questions per exam	30 to 90 minutes per exam	$145 to $243 per exam	65%	Varies based on exam.

In this e-guide

Guide to cloud security management and best practices p. 2
Why is cloud security important? p. 2
Best practices for cloud security p. 5
Who is responsible for cloud security? p. 8
Cloud security management strategies p. 12
Cloud security tools p.13
Further reading p. 17

Cloud security management strategies

Rarely do organizations have a single cloud environment -- more likely they have multiple ones that 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.

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.

Cloud security teams need to test their cloud environments regularly. Nemertes Research Founder and President Johna Till Johnson encouraged companies to tap into specialized tools that enable organizations to run hostile tests against their environments. These tools help shore up the cloud environment. She also suggested performing live-fire training -- where cloud environments are made deliberately insecure -- so security professionals can learn how to combat threats and discover weaknesses and gaps in the environment and their skills in real time.

Testing also is essential for the shared responsibility model where in-house and provider security teams together assume the role of protecting assets in the cloud.

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

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 to support investigations. 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, and logs and other event data) but also mitigate any issues based on what is discovered.

One of the most significant types of attacks security teams must ward off through better cloud security management is cloud account hijacking, in which hackers compromise a subscription or other type of cloud account to engage in malicious activities. The following three key strategies can protect an organization from such an incident:

- use MFA;
- segregate duties; and
- trust but verify account access.

Cloud security tools

Many enterprise tools try to extend security to the cloud, but cloud-native tools can provide more seamless and comprehensive protection for cloud assets.

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

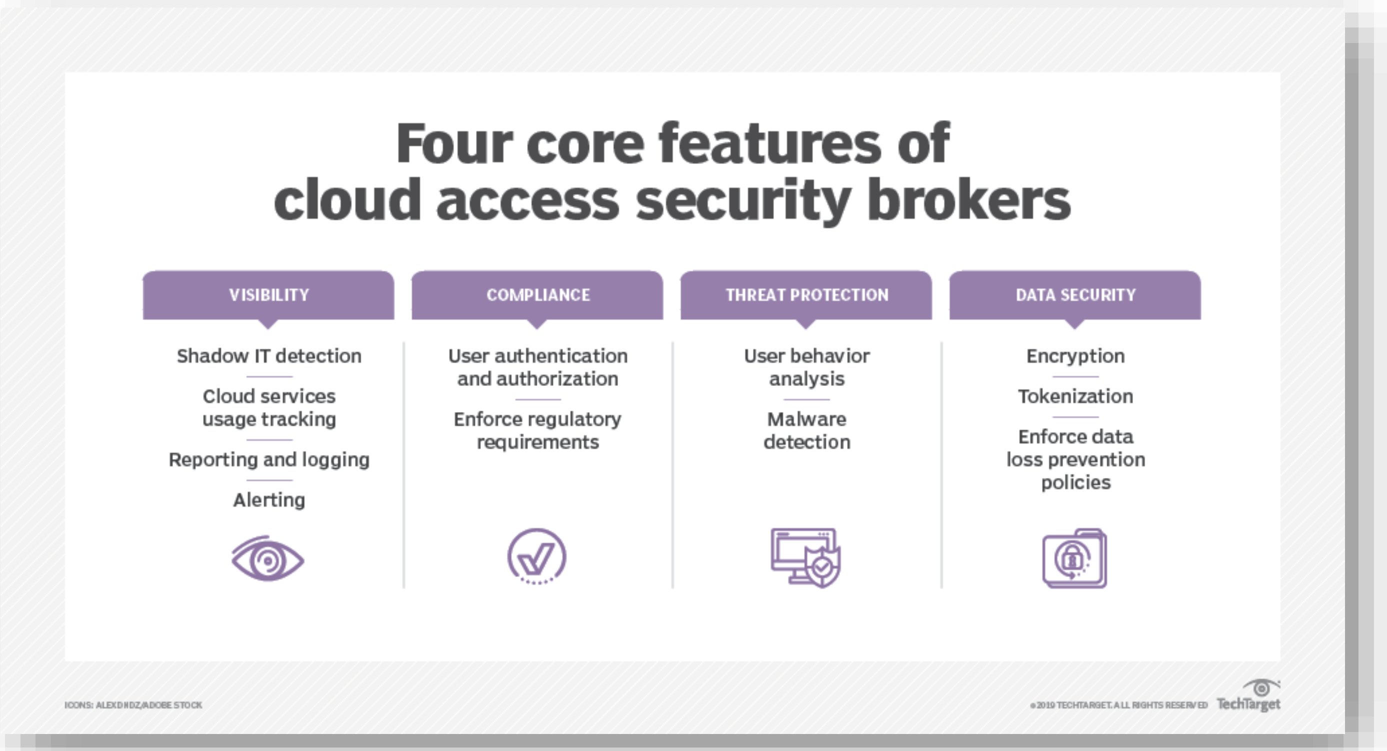
Cloud security tools p.13

Further reading p. 17

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. Purchasing a CASB requires careful consideration, and to help, Kevin Tolly, founder of The Tolly Group, shared some CASB buying tips and vendor comparisons.



Four core features of cloud access security brokers

VISIBILITY
- Shadow IT detection
- Cloud services usage tracking
- Reporting and logging
- Alerting

COMPLIANCE
- User authentication and authorization
- Enforce regulatory requirements

THREAT PROTECTION
- User behavior analysis
- Malware detection

DATA SECURITY
- Encryption
- Tokenization
- Enforce data loss prevention policies

ICONS: ALEXDNDZ/ADOBE STOCK

©2019 TECHTARGET. ALL RIGHTS RESERVED TechTarget

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

For multi-cloud deployments, Moyle offered tips for evaluating CASB tools.

Cloud security posture management tools

Cloud security posture management tools (CSPM) enable companies to perform continuous compliance monitoring, prevent configuration drift, set limits on permittable configurations or behavior in the cloud, and support SOC 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 -- according to SearchSecurity Associate Site Editor Katie Donegan.

Zscaler, Orca Security and Trend Micro are some of the vendors offering CSPM tools.

Cloud workload protection platforms

A cloud workload protection platform (CWPP) unifies management across multiple cloud providers, packages controls together with workloads and ensures controls are designed to be cloud-native.

CWPPs have the following benefits:

- reduced complexity;
- consistency; and
- portability.

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

Microsoft, Amazon, Palo Alto Networks and Capsule8 are among the vendors with CWPP offerings.

Further reading

In this e-guide

Guide to cloud security management and best practices p. 2

Why is cloud security important? p. 2

Best practices for cloud security p. 5

Who is responsible for cloud security? p. 8

Cloud security management strategies p. 12

Cloud security tools p.13

Further reading p. 17

About SearchCloudSecurity

Part of the TechTarget family of websites that covers a wide range of business technology topics, SearchCloudSecurity is a trusted source for emerging and recurring infosec advice. Our award-winning technical tips, news and feature content is designed for all levels of expertise -- from security novice to chief information security officer (CISO).

Our editorial team and pool of IT professionals craft expert articles for enterprise security professionals and business technology buyers that cover a wide variety of topics, from data security and risk management to threat detection and compliance, to cloud security and security certifications.

In addition, we offer free infosec training courses in our Security Schools. Our courses, led by renowned experts, cover today's need-to-know topics. These lessons will arm you with the foundational and tactical knowledge needed to keep your organization secure and compliant. Check out our CISSP Security School to access CISSP training materials and practice exam questions to help you prep for the exam of this gold-standard certification.

For further reading visit us at www.SearchCloudSecurity.com