Comparing Security Across the Three Main Cloud Providers

○ Get Started

Introduction

Both the speed of innovation and the uniqueness of cloud technology are forcing security teams everywhere to rethink classic security concepts and processes. To keep their cloud environment secure, businesses are implementing new security strategies that address the distributed nature of cloud infrastructure.

Security in the cloud involves policies, procedures, controls and technologies working together to protect your cloud resources, which includes stored data, deployed applications and more. But how do you know which cloud service provider offers the best security services? And what do you do if you're working on improving security for a hybrid or multi-cloud environment?

This ebook provides a security comparison across the three main public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). With insight from leading cloud experts, we also analyze the differences between security in the cloud and on-premises infrastructure, debunk common myths about security, and offer best practices you should take advantage of to ensure your cloud environment is safe.

Cloud security in comparison to on-premises security

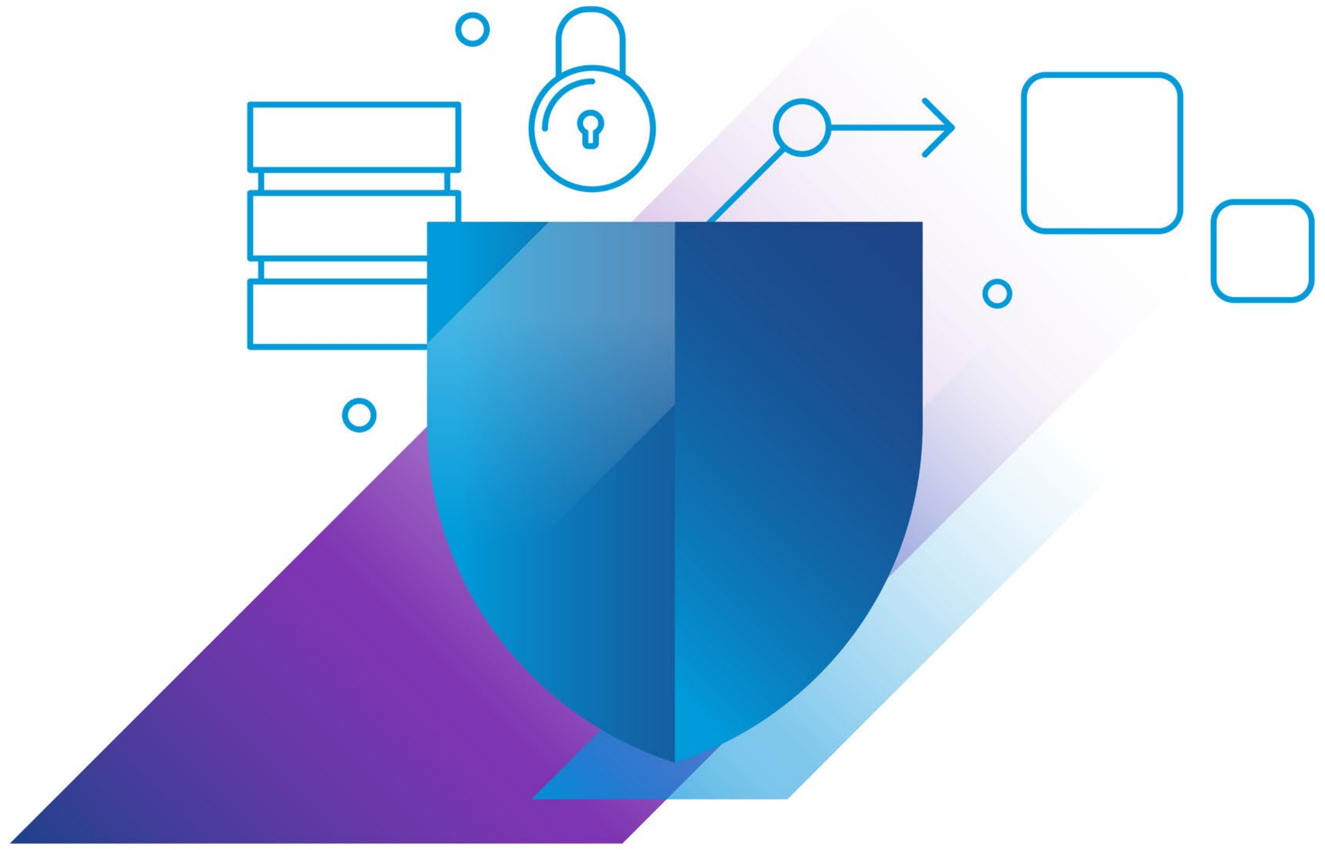
When a business provisions a service from a cloud service provider, at a minimum, it hands over responsibility for the security of the hardware on which that data is stored and applications are run—something that can concern some businesses.

Compared to on-premises infrastructure, there are more attack surfaces in the cloud due to the distributed and dynamic nature of deployments. The on-demand, self-service nature of the cloud can lead to services being provisioned without IT approval or safeguards, which can be problematic if company-wide security best practices haven't been established.

Not only can resources be deployed in the cloud much quicker and easier than in an on-premises environment, there's a much wider choice of resources to deploy, some of which users will inherently be unfamiliar with. This can result in misconfigured applications and misconfigurations in security-sensitive resources, such as security groups, networks, and access policies for databases and object storage.

Unlike in an on-premises environment in which the network is protected by a firewall and IP network rules, an exploited vulnerability in the cloud, such as a misconfiguration, can result in data loss, account hijacking, and advanced persistent threats (APTs), all of which are much harder to detect and eliminate in the cloud than on-premises.

Practically every resource in the cloud can be accessed from a web-based console. Therefore, it's essential users and resources are given the lowest possible access permissions to do their jobs. The wrong credentials in the wrong hands can have far greater implications for security in the cloud than on-premises.



Why things go wrong in the cloud

Cloud security incidents happen every day; some are discovered and resolved quickly, while others may take years to detect. In almost every case, security vulnerabilities can be attributed to poor security practices of the cloud user(s), not the negligence of any given cloud service provider, meaning it's imperative that cloud teams assess their current security posture and implement change to reflect industry best practices.

A number of common Azure misconfiguration issues include the following high/medium risk issues:

- Load balancers are configured to permit clear text communications
- Security updates are missing on Linux and Microsoft operating systems
- Application gateways are configured without a web application firewall
- Azure Active Directory identity protection is disabled
- Azure user access is configured without multifactor authentication
- Azure security groups are configured without rules

Credential theft is another threat facing cloud security. Businesses must work to educate team members with cloud access on basic security best practices to prevent phishing attacks and credential mismanagement.

Myths about cloud security

Due to a lack of understanding about the public cloud's shared responsibility model, some concerns over security vulnerabilities in the public cloud have developed into myths. The following are some of the most common fears we hear from businesses when it comes to cloud security.

The lack of physical control over data makes data insecure

The controls implemented by cloud service providers are more advanced than most on-premises environments, and they consider all potential physical threats when building their data centers—designing, installing and testing top-of-class physical controls to counteract risks. Handing over the reins can be difficult, but cloud service providers exceed expectations over their portion of the shared responsibility model.

If you don't connect to the public cloud, data is less at risk

In today's innovative world, it's impossible for businesses to remain competitive without taking advantage of services operating in the public cloud. Research has shown that teams with poor security posture, who fail to implement security best practices in their everyday operations, are the primary reason for security issues—not where the data is located.

Single-tenant virtual private clouds are more secure than multitenant public clouds

Data stored on single-tenant virtual private clouds and multitenant public clouds has the same level of physical perimeter security. In addition, public clouds use logical content isolation to prevent two sets of devices on the same physical infrastructure from communicating with each other.

Public cloud service providers mine enterprise data

Businesses operating in the public cloud can take advantage of tools such as Azure Monitor Log Analytics, the Google Cloud Operations suite (formerly Stackdriver), and AWS CloudTrail to provide an indisputable audit trail of every activity on the business's public cloud, revealing any attempt to mine data by any source.

Amazon Web Services

Why businesses choose Amazon Web Services

AWS offers 165 cloud services, including 40 unique services that are unavailable anywhere else in the market. In 2018, AWS released 1,957 new features, giving businesses who use the provider an advantage over competitors using other clouds.

In many circumstances, AWS can justifiably claim to be the most flexible and cost-effective option for businesses. The platform offers the widest choice of operating systems, programming languages, and web applications, with convertible discounts available for businesses committing to long-term use. Its infrastructure supports everyone from small businesses to enterprises, and includes public sector and government agencies.

AWS' strengths and weaknesses

AWS offers a huge and growing selection of services, as well as the most comprehensive network of worldwide data centers. Ironically, AWS' strengths and weaknesses are much the same. The wide choice of services and pricing options is great for businesses that have an established cloud strategy and a sense for what options are the best fit for their business needs, while those just starting out might find navigating AWS challenging.

Market rivals Microsoft and Google speak to the breadth of AWS' services portfolio as its major weakness. While the scope of services offered is vast, you might find greater depth with another provider, such as GCP's unsurpassed depth when it comes to using a service such as AI. Customers also speak to AWS' lack of user-friendliness, which can be challenging for new users looking to become proficient in the platform.

What Amazon says about security in AWS

Amazon claims the AWS Cloud has been architected to be the most secure cloud computing environment available. To support these claims, Amazon states the same security hardware and software is used in the development of all its data centers, meaning that the smallest businesses can be assured of the same level of security that's provided to the military, banks and other high-sensitivity organizations.

To keep its 85 security standards and compliance certifications up to date, AWS continually conducts penetration testing on its infrastructure and summarizes the results for businesses to view via the AWS console. Amazon also allows businesses to conduct their own security assessments and penetration testing on core services without prior approval.

For more personalized support, engage with AWS' extensive account management support, either directly through AWS or from the AWS Partner Network. These are in addition to a range of tools that can help prevent and mitigate the consequences of cloud security vulnerabilities.

What users say about security in AWS

From a technical point of view, AWS is equally as secure as Azure and GCP. That being said, because of AWS' wide breadth of security offerings, taking advantage of available security features can be overwhelming for newcomers.

Some users have found AWS' security controls to be complex and awkward. For example, the difference between giving an Amazon Simple Storage Service (S3) bucket full access and read-only access is the choice of one drop-down menu over another, so you can see how easy it is to make a mistake when establishing access permissions. Because almost all security incidents happen due to user error/misconfiguration, the complexity of AWS' security services can have adverse effects for new users who are untrained in how to use the platform.

Microsoft Azure

Why businesses choose Microsoft Azure

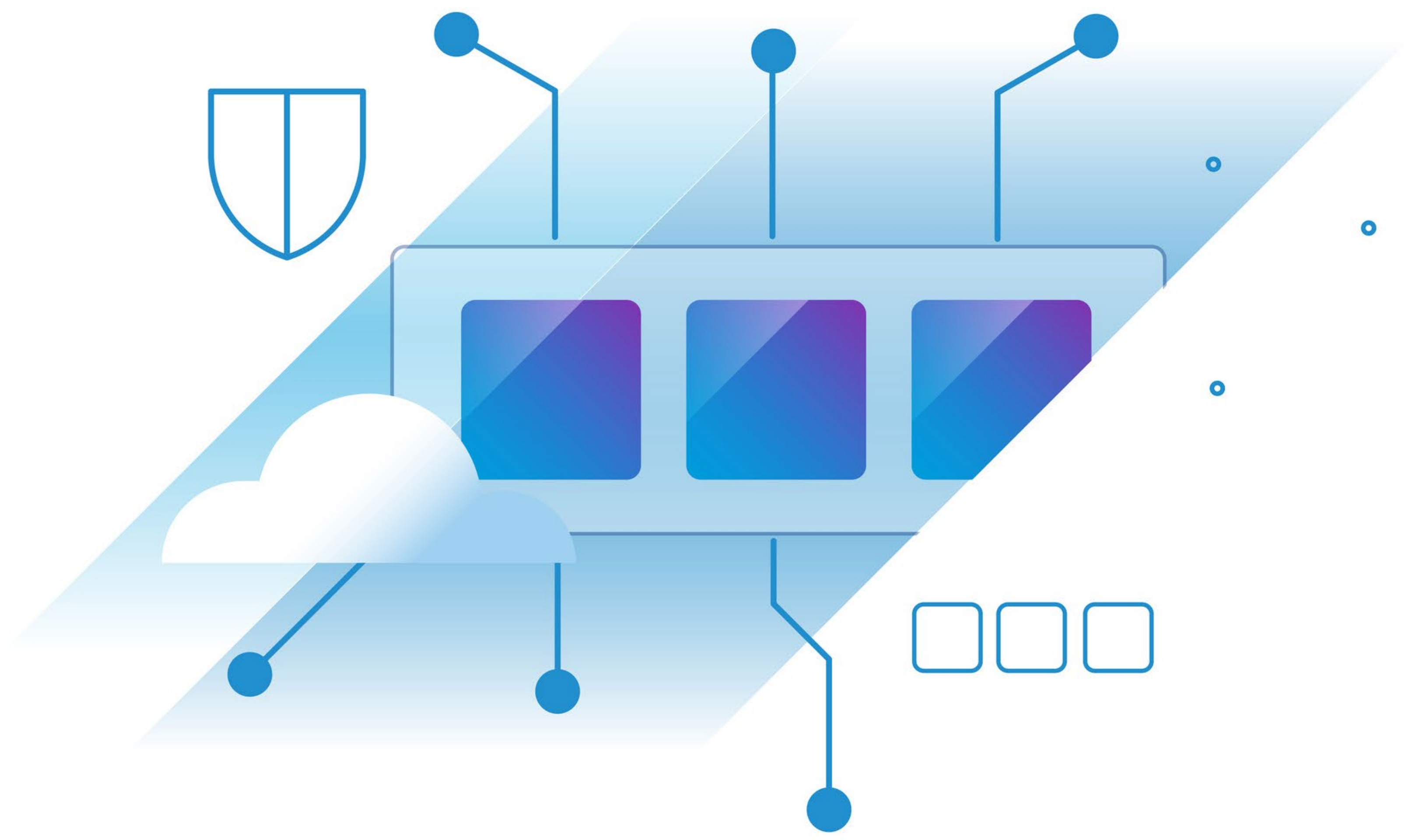
Many businesses choose Azure to leverage their existing knowledge of Microsoft systems, deploy Windows-built apps in the cloud, and take advantage of their existing Microsoft contracts. For organizations already using Microsoft products, such as Office 365, Outlook and SharePoint, the learning curve is quite easy. For businesses looking for easy mobility between on-premises infrastructure and the public cloud, Azure's hybrid capabilities offer a lot of advantages.

As the cloud computing market continues to develop and grow, Microsoft focuses on staying competitive with market rivals by expanding its services portfolio to include next-generation offerings. Currently, Azure is the only cloud service provider to offer blockchain as a service, machine learning bots, and APIs with cognitive capabilities. Azure also offers more than 70 different compliance offerings to ensure customers meet their compliance obligations across regulated industries and markets worldwide.

Azure's strengths and weaknesses

Azure's greatest strength is its compatibility with on-premises infrastructures running Windows Server, Office, and .NET-based applications, making it easier for businesses to migrate to Azure. It also has benefits for Windows users looking to utilize cloud-based backup, site recovery, and disaster recovery services.

While Azure is great for enterprises already deep in the Microsoft stack, Azure's support for other operating systems is quite limiting; it only supports a few versions of Linux, for example. Businesses looking for more robust OS compatibility will find better luck with AWS.



What Microsoft says about security in Azure

Microsoft prides itself on Azure having a defense-in-depth design that offers built-in controls for businesses to secure their infrastructures, apps and data. Microsoft states that all Azure services are designed from the ground up with security in mind and include multiple layers of defense. Key to security in Azure is Microsoft Defender for Cloud (formerly Azure Security Center), a service that provides unified visibility and control across Azure and on-premises infrastructure, and includes machine learning capabilities to provide adaptive threat protection, detection and response. Defender for Cloud also monitors businesses' cloud infrastructure and makes recommendations about how and where security could be improved.

Machine learning, behavioral analytics, and application-based intelligence play a big part in Azure security. Available security tools provide actionable insights in real time about threats to virtual machines (VMs), networks, and service configurations, while Azure Key Vault provides increased control over encryption keys and passwords. Azure also offers an optional service to protect networks against distributed denial-of-service (DDoS) attacks.

What users say about security in Azure

Microsoft claims Azure security offers all of the control and none of the work, but how true is this? While Microsoft provides dozens of tools to enhance security in the cloud, a frequent criticism from customers is that the platform has a steep learning curve. Many users find Azure comparatively harder to use and manage than AWS and GCP. For those willing to take on the educational challenge, they'll be rewarded with Azure's high operational performance, strong hybrid options, and breadth of cloud service offerings.

Google Cloud Platform

Why businesses choose Google Cloud Platform

Although a late arrival in the cloud provider market, Google Cloud Platform offers industry-leading technical expertise. The launch of its production-grade Kubernetes container orchestration system came just at the right time for early adopters of the cloud looking for more efficient ways of using the cloud, and Google's investments in big data and AI makes it a leader in these fields.

Google's customizable VM instances and sustained use discounts make the solution attractive to cost-conscious businesses, while those focused on security know they can rely on the same global infrastructure used to protect Gmail accounts and the Android platform. GCP documentation is written to appeal to new entrants in the world of cloud computing, making enablement services much more accessible than market rivals.

GCP's strengths and weaknesses

Google's attractive pricing model (it was the first provider to bill per second for their services) and robust security offerings are some of its biggest strengths, while investments in new and emerging technologies have been an attractive feature for start-ups and organizations looking for a powerful data and analytics solution.

However, because of its late arrival in the market, GCP's service portfolio doesn't have the same breadth as fellow competitors Amazon and Microsoft, nor a background in serving enterprise. While this has proved advantageous for small businesses that don't have to wade through a massive choice of service offerings and have an easier time accessing enablement materials, some enterprise customers have found GCP's services portfolio unable to support all their needs.

What Google says about security for GCP

Google has been in the data protection space for a few decades and has kept security at the center of everything it builds. Businesses operating in GCP can take advantage of the Security Command Center to gain visibility into assets deployed on the platform and what their current security state is. The Security Command Center helps businesses prevent, detect and respond to security threats, and identifies vulnerabilities so they can be addressed before the misconfigured resources can be exploited.

One of the advantages the Security Command Center has over other cloud service providers' security centers is that it integrates easily with Google's authentication and phishing prevention solutions. It also integrates with a host of third-party security solutions, so businesses can more easily create a custom security solution that matches their individual requirements.

What users say about security in GCP

GCP users find the Security Command Center simple to use with straightforward documentation that helps businesses get started with security right from the beginning.

Cloud security best practices

The following cloud security best practices are just a few examples from industry experts on how you can help reduce the risk of a cloud security incident or mitigate its consequences.

Encrypt data at rest and in transit

Although cloud service providers encrypt data in their data centers, it’s still at risk from theft in transit and when accessed on-premises or on a mobile device. Some businesses are opposed to encrypting all data because it can affect the performance of cloud-based applications. However, encrypting sensitive, personal and business-critical data—and ensuring encryption keys are maintained separately from the encrypted data—is the best way to ensure data is protected in the event of a cloud security incident.

Assign the least privilege levels necessary

With regards to access controls, users and resources should be given only the least privilege levels necessary to get the job done. It’s a best practice to assign the least level of privileges by default and add additional privileges as necessary. It’s also suggested businesses manage privileges in groups, fine-tune privilege levels with policy conditions, and enable logging tools to gain visibility into user activity. A strong password policy should also be enforced and security credentials rotated regularly.

Enable security key multifactor authentication

Multifactor authentication protects accounts from unauthorized access in the event login credentials are leaked to a phisher or obtained by a hacker. However, multifactor authentication tools that use SMS or email may be poor defenses if a user’s mobile device is stolen. A best practice is to enable multifactor authentication that uses hardware security keys. It may be more expensive than SMS or email, but it can make the difference between an account being secured or compromised.

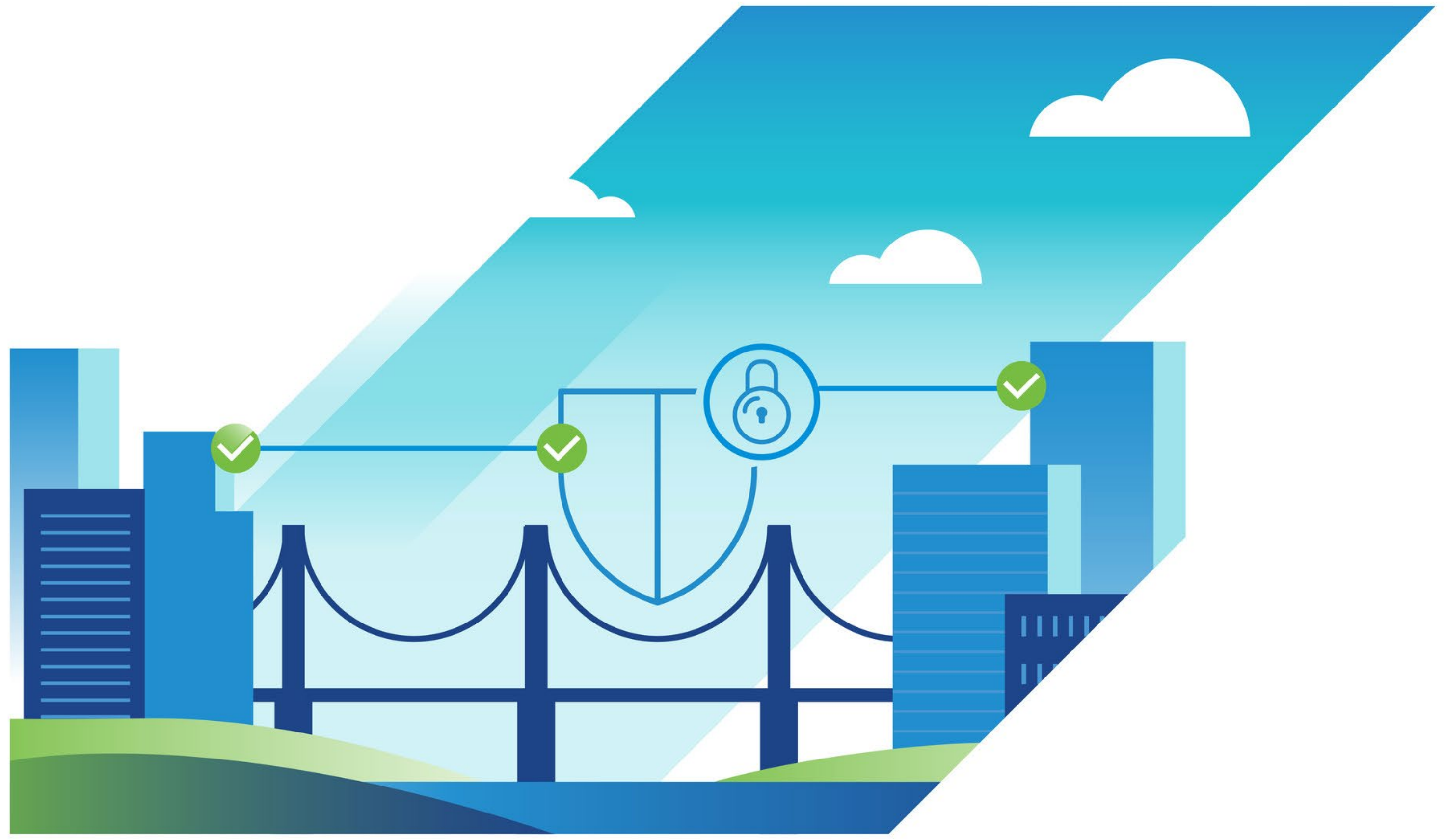
Take advantage of automated cloud governance solutions

Automated cloud governance solutions can be configured to be the eyes and ears of your cloud security. Simply apply your business’s cloud governance policies to the automation solution and the policies are enforced by the solution, preventing users from operating outside the parameters you have defined. Automation is an ideal way to prevent misconfigurations, identify unencrypted data, block APTs, and stop unapproved resources from being launched.

Conclusion

The public cloud has fundamentally changed the way businesses approach IT security. Identifying risk, managing misconfigurations, and remediating vulnerabilities is a real challenge for teams with large volumes of interacting applications spread across multiple clouds.

Because each cloud service provider offers similar industry-leading security services, ownership for your business's security posture is entirely on your team. The uniqueness of cloud will require you to rethink classic security concepts and adopt approaches that match public cloud processes. This includes rethinking security best practices across asset management, compliance and incident response, as well as training and education.



VMware Tanzu Guardrails is an intelligent cloud security solution that helps organizations minimize security risk and proactively mitigate threats across AWS, Azure and GCP. It helps organizations automatically remediate cloud misconfigurations and build security guardrails that help developers innovate across multiple clouds without compromising on agility or security risk.

Get Started Today

See how Tanzu Guardrails can streamline security operations.

LEARN MORE

Join us online: