White Paper: **December 2022**

Building a Successful Cloud Infrastructure Security and Compliance Practice

Table of contents

Executive summary

Cloud security truly is a team sport that requires strong collaboration between security, IT and line of business teams. The dynamic nature of cloud is forcing information security teams to rethink how they operate and partner with other groups to address emerging security and compliance challenges their organizations face.

This white paper provides guidance for various leaders driving toward the shared goal of building secure and compliant cloud infrastructure to accelerate their company's digital transformation:

- Understand why it's critical to switch to a security model focused on enabling developers with best practices while building guardrails.
- Explore the roles of the cloud security architect and other stakeholders critical to a cloud security and compliance organization.
- Learn about different steps in the cloud security and compliance maturity model and key performance indicators (KPIs) for measuring success in each phase.

What is cloud security?

Cloud security (or cloud infrastructure security) is a set of company policies and processes implemented to protect data and infrastructure resources in public clouds. A mature cloud security program ensures that a company's cloud accounts and services are configured correctly to encrypt data, prevent unauthorized access to resources, and maintain regulatory compliance—all without slowing down innovation.

Over the years, accidental misconfigurations of cloud services have led to a number of security breaches, resulting in massive data exposures, financial losses and erosion of brand value for companies. Gartner predicts that through 2025, 99 percent of cloud security failures will be the customer's fault and 90 percent of the organizations that fail to control public cloud use will inappropriately share sensitive data.[1]

While misconfigurations might seem benign at first, hacker groups around the world are known to use sophisticated tools that expose and exploit such common misconfigurations. They begin by exploiting these initial attack vectors and then move laterally, gaining access to the broader infrastructure that hosts corporate and customer data. Recent data breaches across the industry have all resulted from seemingly small misconfigurations.

1. Gartner, Inc. "Is the Cloud Secure?" Kasey Panetta. October 10, 2019.

To get deeper insight into the types of misconfigurations that exist in cloud environments, we looked at a sample data set of 6.9 million misconfigurations across a large number of cloud accounts. Among the common high-risk violations, we found typical mistakes such as unencrypted data volumes, unsecured network port settings, and lack of multifactor authentication requirements. These misconfigurations can easily be corrected with simple changes in service parameters, but managing the volume of issues at scale makes cloud security harder for organizations.

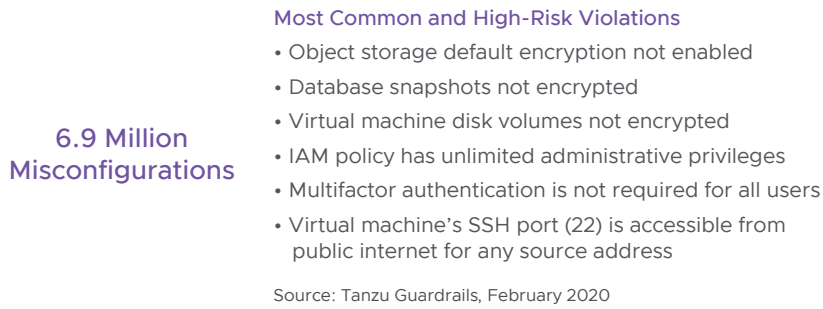

Figure 1: Common cloud misconfigurations.

Organizations need to rethink how security operates

To get a better understanding of cloud security challenges, you need to first understand how cloud computing impacts security teams, processes and the technologies they use today.

Challenge 1: Security change management cannot handle the speed of cloud
Cloud computing has made DevOps real for companies. Developers building applications in the cloud commit hundreds of code changes every week. The traditional change management approach of meeting once a month (or at any other regular interval) to review the security impact of new updates and changes to the golden images doesn't work in cloud.

Solution: Shift in security mindset from blocking teams to building guardrails
To help the business move fast and stay secure, security needs a shift in mindset. Rather than limit developers to a certain set of services and templates they're allowed to use, cloud security teams need to think about how they can enable developers with best practices for using different cloud services. The best security teams today think like developers. They share code examples of correct usage and build security guardrails to ensure someone accidentally doesn't make a mistake.

Challenge 2: Lack of skilled staff and appropriate guidelines for security teams
Even though IT teams and developers have been embracing DevOps techniques and building applications in cloud for years, these technologies are relatively new for most security teams. Finding engineers who are skilled in both security and cloud is a tough challenge for many companies.

Solution: Train internal teams and leverage cloud security standards
Although there is no easy solution to this problem, organizations can start by identifying internal personnel skilled in DevOps and train them in cloud security. These individuals can gradually help raise the overall security awareness among developer teams. To help organizations get off the blocks quickly, different cloud providers and public sector groups publish cloud-specific best practices and security controls for maintaining compliance with industry regulations.

Challenge 3: Traditional security approaches don't protect resources in the cloud
Cloud environments are extremely dynamic. The lifecycle of resources in cloud is often short-lived. Network parameters such as IP addresses and network ports are no longer reliable for identifying resources in cloud. Solutions that rely on these resource identities are no longer useful for security teams. Perimeter firewalls that have served security teams for years in the data center no longer work in cloud.

Solution: Use a security posture management solution built for cloud
Unlike the traditional security solutions, cloud security posture management solutions leverage cloud APIs and event logs to provide visibility into service configuration risks in the cloud. Many of these solutions provide out-of-the-box implementation of security controls recommended by different cloud providers and industry standards, such as the Center for Internet Security (CIS), NIST, GDPR and HIPAA. While selecting the right cloud security solution, security teams should compare how different solutions model configuration risk factoring in service dependencies, verify the speed at which they detect changes in cloud, and provide integrations to enable all security stakeholders.

Building a cloud security organization

Security of applications and data in the cloud is a shared responsibility across multiple entities. Cloud providers ensure the responsibility of the cloud infrastructure, which includes the physical hardware and virtualization layer running different infrastructure-as-a-service (IaaS) solutions. The customers using the cloud services are responsible for security of the guest operating system, applications, virtual firewalls and configurations that control access and safety of customer accounts and data in the cloud.

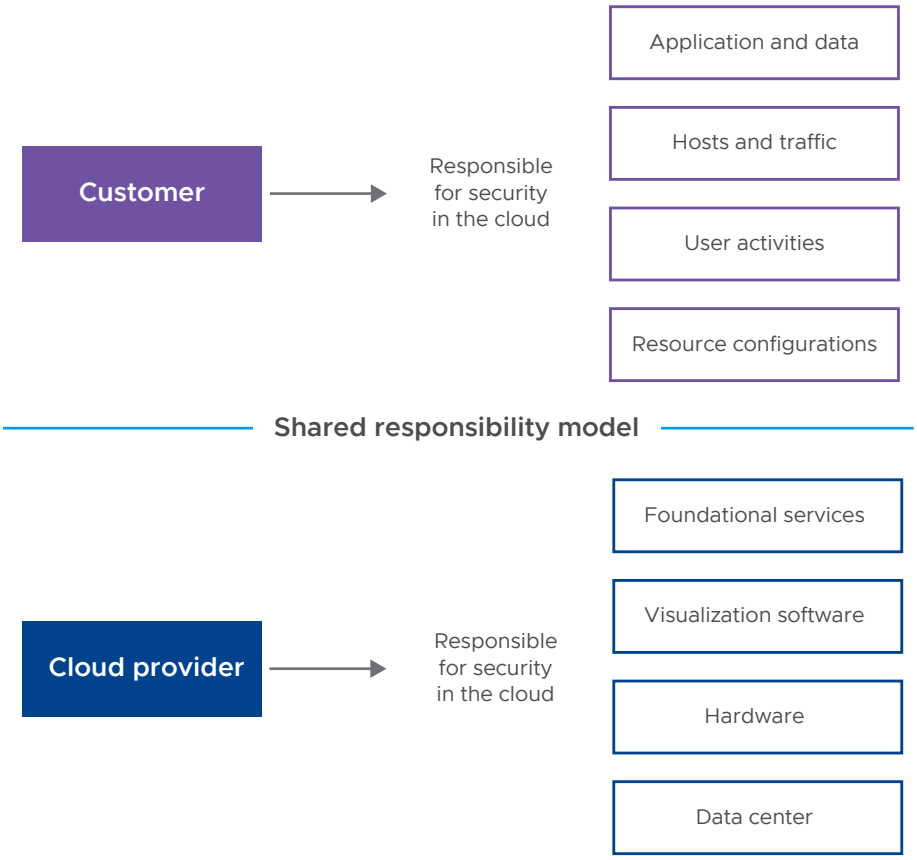

Figure 2: Division of security responsibilities.

Over the years, cloud providers have done a good job of explaining to customers where the demarcation of responsibilities lie and how these vary with the introduction of newer platform-as-a-service (PaaS) and software-as-a-service (SaaS) offerings. However, within the customer organizations, there isn't much clarity around who should be accountable for their share of security responsibilities.

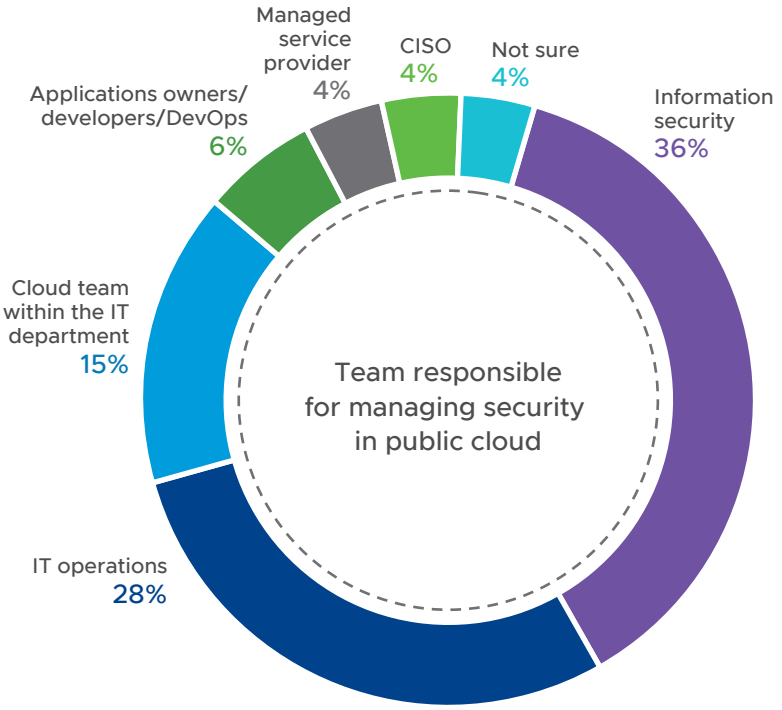

Figure 3: Teams who are responsible for cloud security at different companies.

In most organizations, cloud adoption began at a grassroots level, distributed across multiple teams with developers managing security of applications. As businesses saw the early value, a critical mass of services and data started migrating to the cloud. With mass cloud adoption came an increasing number of security breaches, operational missteps and financial surprises. Today, to ensure success in the public cloud, many organizations build a cloud center of excellence to deliver a coordinated approach of driving best practices for cloud operations, security and financial management.

Know your cloud security architect and stakeholder teams

The key security champion in a cloud center of excellence is the cloud security architect, a person extremely skilled in security and cloud technologies. The primary goal of the security architect is to design security and compliance standards, and scale them in a way that helps the organization meet its business and security needs simultaneously.

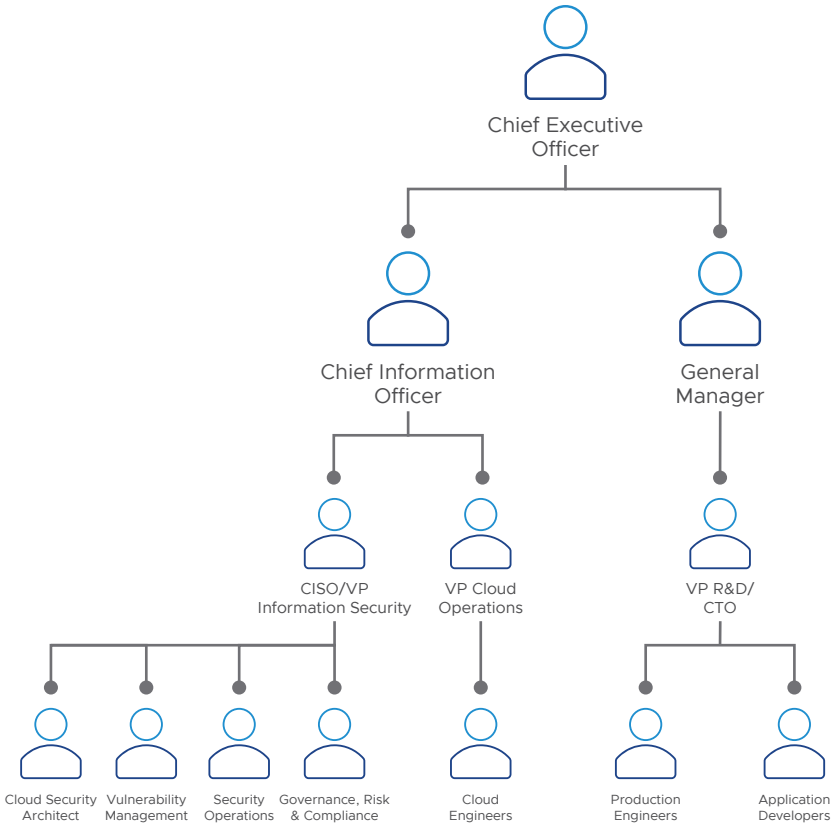

Figure 4: Sample security organization in a large company.

In a larger organization, reporting to the CIO or CISO is the information security department, which can have distinct teams such as security operations, vulnerability management, and governance, risk and compliance. Each one of these teams has specific requirements that the developer teams must address to ensure security and compliance of the infrastructure they build in the cloud. They all need easy access and visibility into the cloud accounts to monitor security risks. A key responsibility for the security architect is to provide security and compliance solutions that enable different information security teams to perform their responsibilities and coordinate efficiently.

Department	Specialized function	Examples of security responsibilities
Information security	Cloud security architect	Designs security standards for building applications in the cloud
	Vulnerability management	Reduces risks due to misconfiguration vulnerabilities in the cloud
	Security operations	Monitors threats to detect and respond to suspicious activities in the cloud
	Governance, risk and compliance	Collaborates with auditors to help the business meet regulatory compliance in the cloud
IT	Cloud operations	Enables security teams to get visibility and monitor company cloud accounts
Line of business	Cloud security architect	Runs applications at scale in production and helps ensure application reliability (including security)
	Vulnerability management	Adopts security and compliance best practices while building applications in the cloud

Table 1: Breakdown of security responsibilities by department.

To begin, the security architect works with IT operations to ensure that the company cloud accounts are configured correctly to give various security functions appropriate roles to monitor and secure cloud resources.

In parallel, the security architect works with developer teams to build standards that establish security and compliance requirements, and are prescriptive and easy for developers to implement. Together, the architect, developers and operations teams find ways to automate processes and ensure that information security controls are implemented in a way that minimizes risk without restricting service access or affecting application reliability.

Organizations that are smaller in size often do not have the resources, nor the need, to dedicate specialized personnel to different roles in information security. No matter the organization's size, the leaders building the cloud security organization must identify the individuals that, together, perform the role of the security architect, and the information security and IT operations teams.

Cloud security and compliance maturity model

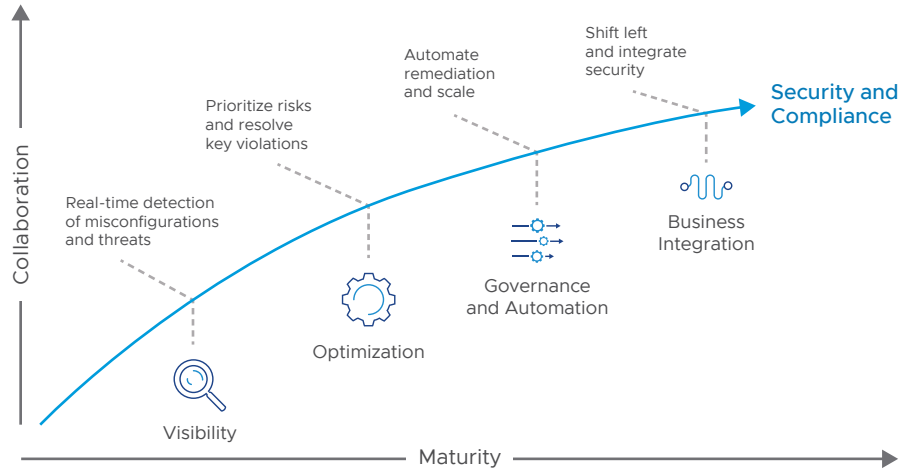

Figure 5: How to mitigate cloud security and compliance risks.

Phase 1: Get visibility into cloud accounts and security vulnerabilities

As the age old saying goes, "You can't protect what you can't see." The first step in assessing the state of cloud security is to get access to all accounts across all clouds. This initial step is a requirement for several other functions within the cloud center of excellence that also need visibility into cloud accounts to help the business better manage costs and ensure operational efficiency across environments.

Building a coordinated approach for managing access and collecting inventory data across clouds and teams is critical. Besides the benefits of maintaining a common source of truth and not duplicating the efforts across teams, organizations don't want their finance, security and IT teams competing for inventory access and making the same API calls that cloud providers throttle, and their developers need, to access cloud resources.

The cloud operations teams migrating shadow IT accounts or standardizing the creation of new accounts under the organization's master account hierarchy can help security teams get appropriate roles in each cloud account to monitor resources and cloud activity.

During this process, it's a good time to implement the following security best practices for your cloud accounts:

- Enable log collection and event alerting by default in each cloud account.
- Federate cloud user identities to an existing identity source that only allows access to corporate email IDs.
- Restrict third-party access to critical applications through appropriate roles, and maintain least-privileged access for all internal users and resources with identity and access management (IAM) roles.

KPIs organizations should track to measure success in Phase 1

- Security violations by cloud provider, accounts and service types
- Failed security controls
- Mean time to detect security and compliance violations

Once the security teams have appropriate access to cloud accounts, they can assess the security and compliance posture of these environments with the help of a number of cloud native services or other solutions that offer multi-cloud support. These solutions can provide out-of-the box assessment on security risks based on security controls recommended by cloud providers or regulatory bodies.

At the time of a first assessment, it's not uncommon for most teams to get flooded with security violations as they uncover issues that were missed across projects. Across accounts, security teams should ensure that they have a real-time view into security events and configuration changes. Limiting visibility based on the polling interval of a security solution can be dangerous. When a criminal can exploit a vulnerability and break into an account within minutes, security cannot wait for hours to find out that something bad has happened.

Once the baseline visibility and monitoring capabilities for all cloud accounts are established, the security architect must ensure that different teams get easy access to these insights for their activities. This can be done by giving them all access to the security posture management solution or building integrations that forward insights into their specialized solutions.

Phase 2: Optimize security controls based on organizational requirements

The results of an initial security or compliance assessment are often overwhelming for security teams. With thousands of newly detected violations based on hundreds of rules, security teams need to identify an optimized set of controls that are critical for their business and minimize false positives. The goal is to have meaningful conversations with developers and guide them to resolve critical violations that have the biggest impact on the organization's overall security posture.

To optimize efforts, teams should target controls based on application or business requirements. Customers often start by protecting critical data, assets and production cloud accounts. Ensure that the security controls for cloud services where the data lives are enabled. Identify servers that are publicly exposed and change port configurations where public access is not needed.

These are just a few examples of security controls. Every security team should build their list of specific controls based on their organizational context.

For example, at a digital marketing company, the architect for cloud security started by protecting Amazon Simple Storage Service (S3) against the accidental misconfigurations, especially the dreaded open S3 bucket. They had seen headline after headline of breaches caused by open S3 buckets, from the data breach that exposed thousands of job applicants to the data of almost 200 million voters leaked online by a GOP analytics firm. By focusing on S3 to start, the security architect allowed teams time to focus on a handful of best practices and integrate them into their own workflows. The result? No open S3 buckets that weren't intended to be that way. And once the teams had mitigated any S3 risks, they were ready to move onto the next critical service: IAM.

KPIs for measuring impact of security and compliance controls

- Critical security controls
- High-risk violations
- Resolved violations
- Compliance with security controls

While service-specific controls offer one way to build standards, many organizations focus on compliance frameworks to define their control strategy. Depending on the data that your organization handles, you may need to focus on controls required by regulators in your industry.

Irrespective of the approach you choose, the trick is to start with a small set of controls, work with developers to resolve violations specific to those controls, and then gradually add additional controls over time. No matter what controls a security team selects, there will always be a few teams and application environments where these controls will not be valid. To build trust and drive adoption of security standards across application teams, security must allow for exceptions and alternatives to their policies. This might seem counterintuitive, but the intent is to not ignore risk, but to avoid bombarding developers with alerts that aren't relevant to their application or to enforce policies that are difficult to implement. In these cases, security teams should find alternative ways to ensure security and meet application and team needs.

Being selective with security controls is just one component of a security optimization strategy. To help maximize the impact, the controls must be paired with detection techniques focused on prioritizing issues with the highest risk. When sorting through similar violations, vulnerability management teams should inspect context holistically and prioritize the most critical ones to drive progress. For example, all virtual machines with an administrative policy could pose risk to security. However, focusing first on the virtual machine that sits in a production account and has a public IP with a remote desktop port open to the internet is more important.

While cloud misconfigurations do not have standardized risk scores, vulnerability management teams must identify an approach to quantify risk and prioritize vulnerabilities. To help narrow down focus, security operations teams should also monitor anomalies and guide vulnerability management efforts to harden parts of cloud where they observe suspicious activities.

By themselves, security teams can only help identify vulnerabilities. For validating risk and resolving violations, they lean heavily on developer teams. To help developers drive improvements, security teams must ensure that they communicate violations clearly in a language that developers understand and be prescriptive in how to fix them. For example, rather than sending a vague alert that says the IAM password policy needs to be corrected, they should be specific about password requirements and the password parameter name that needs to be updated. A prescriptive approach will help developers fix violations quickly and build trust in their security team.

KPIs for measuring effectiveness of automating response to security violations

- Mean time to response
- Security guardrails
- Security controls with automated actions
- Resolved violation trends

Phase 3: Improve governance by automating actions

Bad actors today rely extensively on automation and can target new cloud vulnerabilities quickly, sometimes in just under a minute. While the attacks are getting more frequent and sophisticated, the information security teams defending them are struggling with the slow pace of remediation in their organizations. Security personnel in most companies are heavily outnumbered by their peers building the applications. The ratio of information security to developers in many organizations is as low as 1:100. Under immense pressure from stakeholders to ensure security, information security teams must rely on automated remediation to scale.

Initially, most security teams resist auto-remediation. They worry that without reviewing configuration context, automation might break the app. The key to automation for security teams is to segment security actions into ones that can be fully automated and those that need human intervention.

The idea behind fully automated actions or guardrails is that there are some security policies and configuration standards that apply universally to all cloud teams. Good examples of guardrails for developers include policies that deny accidental changes to baseline security monitoring controls or those that require boundary permissions for IAM users and roles. While guardrails are non-disruptive, security teams must communicate these to developers before implementation. This helps ensure that developers are not surprised by new policies, understand why they exist, and help security teams to implement them.

A typical workflow to remediate service-specific vulnerabilities starts with the vulnerability management team sending a report or alert on a security violation to the developers of the application. Developers then validate the veracity of the report based on application context and agree on remediation steps that are safe in that environment. While a certain amount of developer intervention is critical for making such changes, the security teams can still enable developers to operate productively by automating notifications, giving examples of code changes to resolve policy violations, as well as sharing scripted actions that can be automated locally to speed up remediation.

Phase 4: Integrate security proactively in the application deployment process

The last phase in the security maturity model is to integrate security proactively in the application deployment process. It's critical to detect security violations as early as possible, otherwise you risk notifying a developer of an issue after they've already moved on to something new. Switching context to analyze violations in a piece of code that was deployed a few weeks back can be extremely time consuming. In many cases, remediation might require disruptive changes, resulting in workarounds and accumulation of technical debt.

KPIs to measure the impact of a continuous security verification model over time

- Security violations per deployment
- Security policies built into the CI/CD pipeline
- Resolved violations compared to exceptions per deployment
- Security violations in production accounts

To counter these issues, the most mature organizations adopt a continuous security model, where the goal is to build security checks right into the continuous integration/continuous delivery (CI/CD) pipeline. Besides the static code analysis, this involves continuous monitoring for risks such as host vulnerabilities or misconfigurations at the time of resource deployment. In case a violation is detected, a remediation workflow automatically kicks in to remediate the violation or trigger a notification to the developer, requesting them to fix the issue or provide justification for an exception. This ensures that the violation is resolved before the application hits production, resulting in a delivery model that's secure by design. This approach also establishes a continuous feedback loop for security teams to refine their policies over time and for developers to adopt best practices.

Besides continuous verification, many teams also leverage resource templates that are already hardened and certified by security teams. These templates should be defined as code because it makes it easier for developers to start with a baseline and then modify design and resource configurations based on application needs. Starting with standardized templates improves productivity and reduces the probability of developers making a security mistake. Once the application is deployed in production, the environment should be continuously monitored for configuration drift.

A continuous security approach improves developer productivity and helps companies and their customers build confidence in the security of new releases.

Conclusion

With multiple stakeholder teams collaborating to ensure success of a cloud security and compliance program, it's critical that each one of them has clarity about their roles and is enabled with real-time security insights necessary to perform their duties. Initially, most security teams get overwhelmed with the scale of resources they need to protect and the number of security and compliance controls they need to implement. To progress, they should focus on prioritizing a small set of security and compliance standards, work iteratively with developers to operationalize them, and get some quick wins under their belts.

In hindsight, most cloud security breaches could have been prevented with simple measures, such as a single change in a configuration setting. However, the volume of cloud misconfiguration vulnerabilities makes it difficult to resolve issues at scale. To scale and reduce risk, information security teams need to find ways to embrace automation and proactively verify security earlier in the application deployment process.

Learn more about how VMware Tanzu Guardrails can help you with your cloud security and compliance practice.

Item No: 1703106aq-wp-bldg-scsfl-cld-infra-sec-cmplnce-uslet 12/22