The Six Key Requirements of Multicloud Security

paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

Table of Contents

The Key to Cloud Security: Consistency

Cloud security threats and risks come in many forms. They range from malware to configuration errors to weak access controls and beyond.

And although these threats are fundamentally different, their ability to materialize inside your environment boils down to one key issue – the lack of consistency. With regards to how your cloud environments are configured and how your workloads are deployed, the less consistency you have, the easier it is for security risks to creep into your cloud and remain under your radar.

Achieving Consistency in Multicloud Environments

Achieving consistency within cloud environments is relatively easy when you're dealing with a single cloud. You have only one set of cloud services, one IAM framework, and one networking configuration to manage.

But when you shift to a multicloud architecture, the challenge of maintaining consistent configurations grows exponentially. The issue is not just that you have a broader attack surface due to running more cloud services, but also that there are significant differences in the way the tools work – even if the differences are not obvious at first glance.

For example, although all cloud providers offer IAM frameworks for defining access controls, each vendor's framework relies on different concepts and configurations. As a result, setting up consistent access control rules can become difficult.

As if to heighten the challenge, each cloud vendor maintains its own shared responsibility model that defines which security tasks fall to customers and which fall to them. Though shared responsibility concepts vary only slightly across cloud platforms, it's easy to miss nuanced differences – and if you happen to overlook something, you could end up with a security strategy with gaps and inconsistencies.

Six Steps Toward Consistent Multicloud Security

The good news is, you can achieve consistent security across multicloud environments with the right approach.

In this eBook, we've laid out actionable guidance to help you optimize multicloud consistency and security. By breaking down best practices and security requirements into six basic categories, your cloud admin and DevSecOps teams can conquer the deep challenges of multicloud security.

Step 1: Visibility and Security Posture Management

The first step toward securing a multicloud environment is to maintain visibility into all cloud services and workloads. With this visibility, you can define and enforce policies that establish a strong security posture – meaning a strong readiness to prevent, identify, and react to threats.

But each cloud platform provides security and visibility tools that work only on its platform, and here's where the challenge of multicloud visibility begins. As organizations add more clouds to their mix of hosting platforms, they add more proprietary tools – none of which integrate with the others. Nor do they use the same language and data taxonomy.

The solution to non-integration is to leverage a unified cloud security platform from a third-party vendor to achieve visibility across your multicloud environment and to normalize monitoring data into a single, easy-to-analyze language. Unified cloud security platforms monitor and audit security data across all your clouds and workloads to provide a centralized, simplified overview of what's happening inside your environment. They can also identify configuration oversights and mistakes that could weaken your cloud security posture.

When you have across-the-board visibility, it's much easier to identify and correct inconsistencies that lead to poor security postures, regardless of how many clouds or workloads you need to protect.

Step 2: Compliance and Governance

Ensuring that your cloud configurations comply with regulatory compliance rules, as well as internal governance requirements established by your organization, is also difficult in multicloud environments. Compliance auditing tools offered by each cloud vendor work exclusively with the vendor's cloud, which is problematic.

Additionally, the auditing tools cloud vendors offer are limited in functionality. They may provide basic configuration scans that align with popular regulatory frameworks, like GDPR and PCI DSS, but they typically don't provide feedback or offer best-practices guidance to help businesses conform with complex compliance rules. The vendors leave it to users to make complicated compliance decisions. And users are charged with the onerous task of compiling their own audit-ready compliance reports, as the compliance tools provided by cloud vendors are incapable of generating audit-ready reports.

But with a unified cloud security platform, you can monitor your compliance posture across all your clouds through a single dashboard. You can generate audit-ready compliance reports to demonstrate compliance and identify gaps. And, because unified cloud security platforms such as Prisma Cloud support dozens of compliance frameworks and user-defined compliance controls, you can track your compliance posture based on any set of rules that apply to your industry or enterprise.

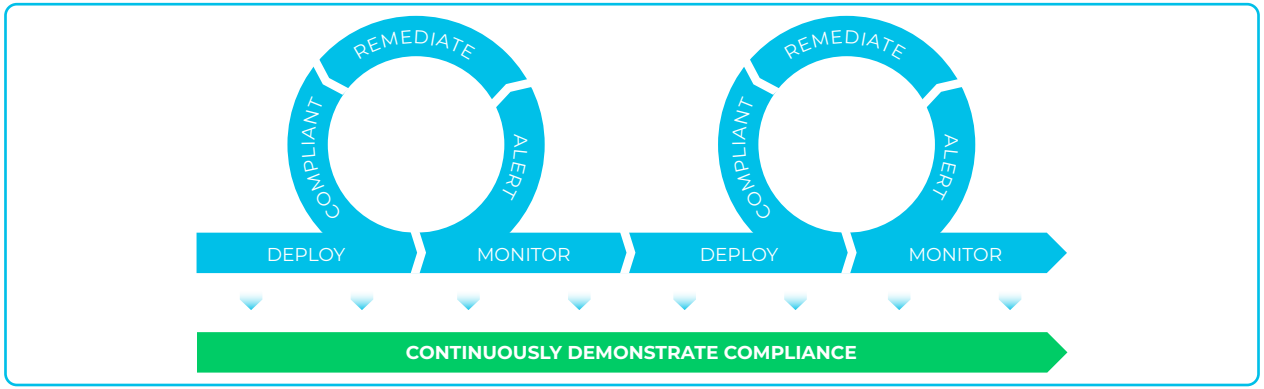


Figure 1: Simplify compliance with continuous monitoring

Step 3: Threat Detection

Security threats in the cloud could emerge from a variety of sources. They could involve external attackers who compromise weak access credentials. They could result from zero-day vulnerabilities that, if left unchecked, could enable exploits against workloads. Threats could even involve insider threat actors taking advantage of overly permissive access controls to move data laterally through the cloud.

Due to the varied nature of these threats, there is no simple or singular means of detecting them. This is especially difficult in multicloud environments where you need to monitor cloud security threats against large sets of services and across many configurations.

What you can do, though, is deploy threat detection tools that assess a broad selection of data points – ranging from logs and API requests to network traffic patterns to configuration files and more – to detect anomalies revealing the first signs of attack. By using machine learning to parse large volumes of data in real time, cloud threat detection platforms are able to identify even the most sophisticated threats, no matter how many different cloud platforms or services you need to protect.

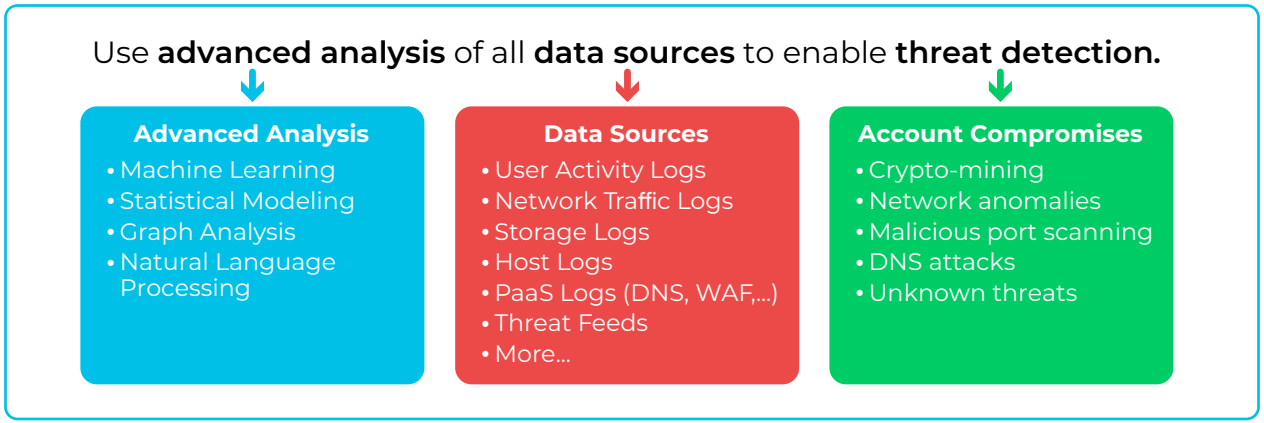


Figure 2: Correlate threat intelligence from multiple sources

Step 4: Data Security

Data stored in the cloud is subject to three main risks. The first is lack of visibility into where sensitive data is stored and which types of protections it requires. Especially in multicloud environments where data sprawls across a variety of databases, object storage services, data lakes, and so on, it's easy to lose track of where sensitive information lies or accidentally upload private data to the wrong storage location.

The second risk involves oversights or mistakes when defining access controls for cloud data. If you accidentally configure a cloud object storage bucket to be accessible from anywhere on the internet, for example, you expose sensitive data inside that security bucket to access by malicious parties.

The third risk to cloud data is malware that may be hidden inside stored data. Organizations need to be able to scan their data to detect malware, and cloud providers don't offer that ability. They'll let you upload whichever data you want to object storage – a VM file system or any other kind of storage resource – without scanning it to ensure it's malware-free.

To protect against each of these risks, you need a cloud-native application protection platform (CNAPP) that can discover and classify sensitive data automatically, as well as ensure the proper access control rules are in place for sensitive data. Given that attempting to track sensitive information by hand isn't feasible – particularly in a large-scale multicloud environment where data may be stored in a variety of locations – the ability to automate data discovery and protection lays the foundation for a comprehensive, consistent approach to cloud data security.

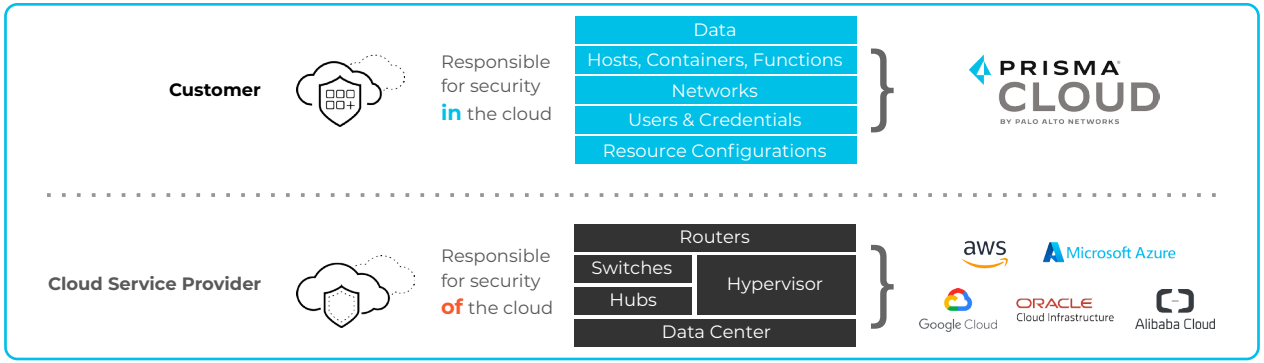
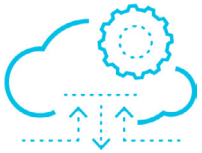


Figure 3: Continuously monitor cloud storage for threats



Step 5: IAM Security

All cloud providers offer Identity and Access Management (IAM) frameworks that allow users to define access control rules to manage permissions for cloud services and resources. Improper IAM settings create a large attack surface that threat actors can use to move laterally within cloud environments. To prevent this risk when using IAM frameworks in a multicloud context, security teams face a number of challenges, including:

- **Varying IAM frameworks:** Although all IAM frameworks perform the same basic function, each cloud's IAM implementation differs. The way you define and manage policies varies across frameworks, as does the way you define and manage identities for both human and machine users. As a result, it's initially difficult to define the proper policies for each cloud. It's also difficult to audit your policies across all clouds to detect configuration risks.
- **Lack of visibility:** Cloud providers don't offer much help with ensuring that IAM rules are properly configured. They won't alert you to configuration oversights, for example, or help you prevent configuration drift (which causes changes in IAM policies over time that lead to inconsistencies even when configurations were initially uniform).
- **Applying rules consistently:** Once you've defined your IAM policies, you need to apply them uniformly across all clouds. Without complete application, you'll have inconsistent access control configurations. Complete and error-free application of IAM policies are especially challenging to achieve for those deploying them manually.
- **Scale:** Finally, the sheer scale of IAM configurations can make them difficult to manage. A modern cloud environment may include thousands of identities, especially considering that both human and machine users require unique identifies and permissions configurations. With so many configurations and configuration variables to manage across multiple clouds, the risk of oversights is steep.

You could try to manage these risks by manually creating IAM policies and periodically reviewing them by hand. That approach, though, takes enormous time and places you in a poor position to detect IAM configuration risks in real time.

A better strategy is to deploy unified cloud security tools that can continuously monitor your IAM configurations. Such tools alert you instantly when they detect overly permissive IAM configurations, such as a lack of encryption, and then suggest remediations to improve your security posture. They can also alert you to unexpected changes in IAM policies so that you can stay on top of configuration drift.

Step 5: IAM Security (continued) – IAM Attacks Formula

1. Attacker compromises cloud instance
2. Identifies and scrapes credentials
3. Escalates to the Cloud Platform
4. Gathers an inventory of cloud resources

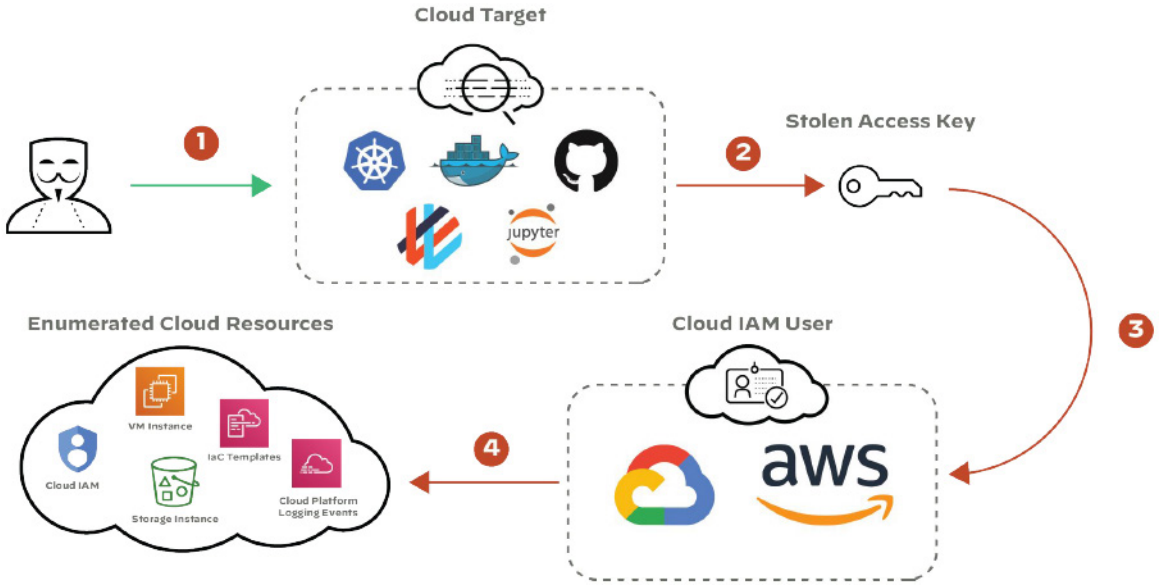


Figure 4: How attackers exploit IAM misconfigurations

Step 6: Shift-Left Security

Sometimes cloud security flaws are introduced early in the application lifecycle – even when the application hasn't been deployed. Developers might build applications using open source software with venerabilities, for example. Or attackers could compromise your continuous integration/continuous delivery (CI/CD) software to inject malware into your code. Perhaps developers used infrastructure-as-code (IaC) templates to rapidly configure and deploy cloud infrastructure, but the templates contained configuration errors that then created security flaws within the cloud environments.

In addition to building security risks into cloud environments, flaws that originate in the application lifecycle burden developers with extra work. They may also delay application releases. When developers have to spend time resolving cloud misconfigurations and vulnerabilities in productions, they have less time to build software.

The key to preventing these challenges is to shift security "left," which means to extend security monitoring and controls into your software development pipeline. By detecting risks and vulnerabilities within software while it's under development, you can mitigate threats before they're deployed into production and can be exploited. In addition, shifting cloud security left helps you to address risks with less time and effort because it's faster and easier to address security problems when you detect them prior to application deployment. Updating risky source code is simpler than redeploying a vulnerable application.

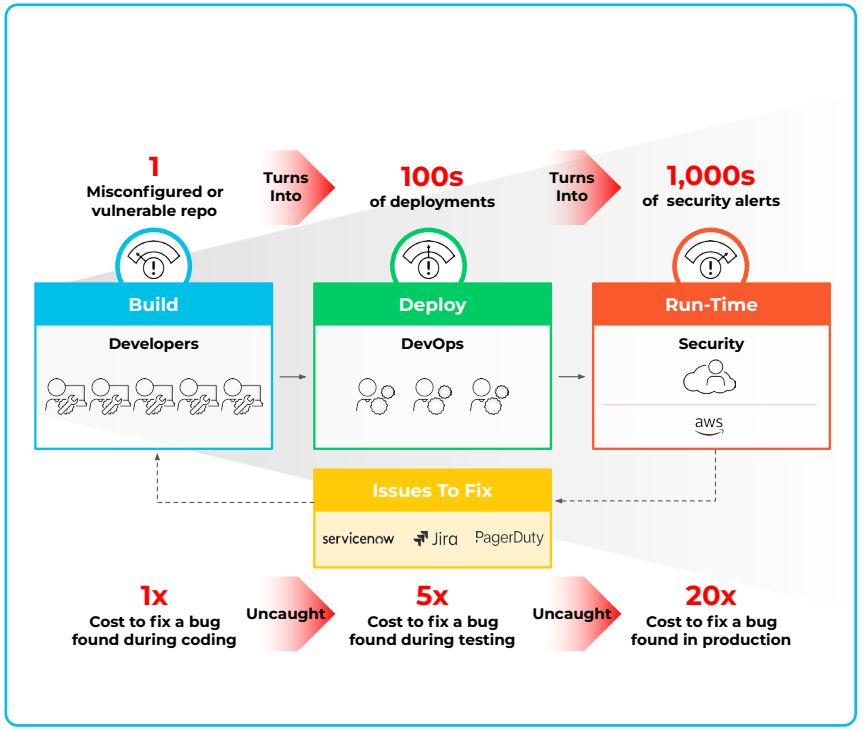


Figure 5: Early detection reduces risk and lowers cost

Conclusion: Achieve Consistent Coverage for Multicloud with CNAPP

There's no denying that maintaining cloud security visibility and consistency is more difficult when you operate on more than one cloud. But with a unified cloud security platform that lets you monitor, audit, and validate all your configurations across all your clouds, you can establish a strong cloud security posture, regardless of your cloud mix.

With a CNAPP, you can embrace DevSecOps practices to secure your entire application development pipeline, not just your production cloud environment. From your source code, to your dev/staging environment to your production environment, CNAPPs automatically detect risks, even if you use multiple clouds to build and/or host your software.

Prisma Cloud from Palo Alto Networks is a CNAPP designed to secure your applications from code to cloud across multicloud environments. The platform delivers continuous visibility and threat prevention throughout the application lifecycle, including zero day threats. With code-to-cloud coverage that encompasses code, infrastructure, workloads, data, networks, web applications, and API security, Prisma Cloud is the only platform that addresses your security needs at every step in your cloud journey. With over 8 billion cloud assets secured, you can trust Prisma Cloud to protect your cloud at any scale. Prisma Cloud enables security and DevOps teams to effectively collaborate to accelerate secure cloud native application development and deployment.

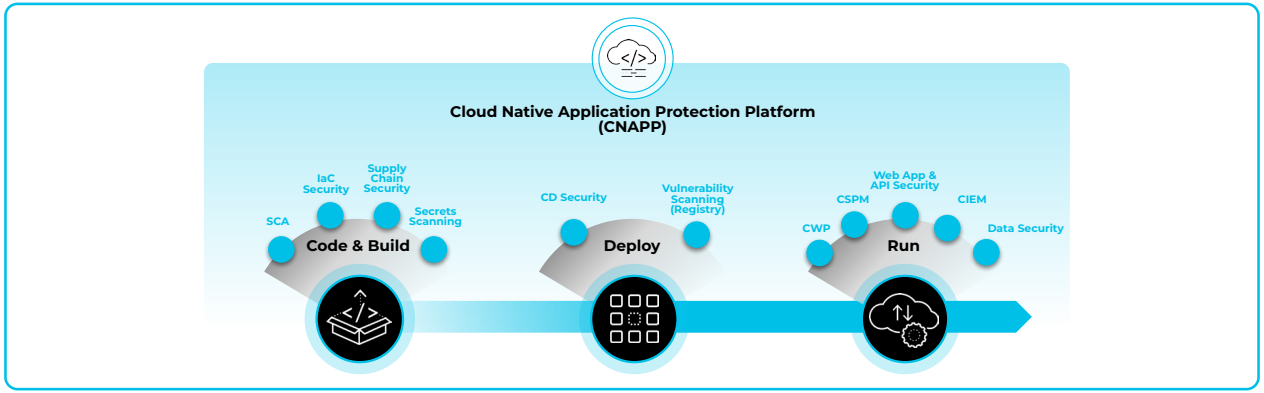


Figure 6: Prisma Cloud: Secure from Code to Cloud

[Learn more by requesting a free trial of Prisma Cloud.]

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

prisma_eb_6-key-requirements-multi-cloud-security_090522