PRISMA CLOUD
BY PALO ALTO NETWORKS

10 Ways Prisma Cloud Complements Cloud-Native Security

1. Adopt Public Cloud with Confidence

Forget having to glue together disparate cloud-native services on your own in an attempt to gain visibility into your cloud environment. Prisma™ Cloud is a security and compliance service that enables anyone to safely adopt public cloud—no specialized expertise required. By automatically mapping resource configurations against hundreds of built-in security policies, Prisma Cloud can quickly show you where resources are misconfigured and provide recommendations to eliminate vulnerabilities before they can be exploited.

2. Bridge the Visibility Gaps Between Clouds

The vast majority of customers deploy applications across multiple cloud platforms. Although each provider offers its own version of "single-pane-of-glass management", the lack of cross-cloud visibility creates blind spots. Prisma Cloud unifies the three major clouds (GCP™, AWS®, and Azure®) by providing a focused console for complete visibility and seamless management of threats and misconfigurations across distributed, multi-cloud environments. Only Prisma Cloud builds a single source of truth across your cloud environments by correlating identity, network traffic, cloud resource configurations, and data.

3. Simplify Compliance Management

Managing compliance in cloud environments where resources are constantly being added and moving around is incredibly costly and time-consuming for organizations. Prisma Cloud comes prepackaged with the most comprehensive set of supported compliance frameworks across industry standards—including CIS, GDPR, HIPAA, ISO, NIST, SOC 2, and PCI DSS—and supports custom policies for specific needs as well. Ensuring continuous compliance in the public cloud is vastly simplified with Prisma Cloud, which is constantly monitoring the entire environment for policy violations and enables audit-ready reports to be generated in a matter of seconds.

4. Accelerate Alert Prioritization Through Automation

With multiple users making changes in cloud environments, alerts can quickly become overwhelming in number and complexity. Prisma Cloud automatically computes risk scores for every resource based on the severity of business risks, violations, and anomalies. By quickly identifying the riskiest resources, security operations center (SOC) teams can quickly prioritize remediation efforts and easily quantify the cloud environment's overall security posture to leadership with unmatched accuracy.

5. Detect Suspicious and Unauthorized Behavior

Prisma Cloud automatically detects user and entity behavior anomalies across multi-cloud environments. The platform establishes behavior baselines and flags any deviations. For example, a potential access key compromise will be flagged if a user is determined to be using access keys from an unknown location to perform activities that have not been observed in the past. Prisma Cloud integrates with cloud-native services like AWS CloudTrail®, Azure Log Analytics, and GCP Audit Logging to build baseline behavior profiles for each user and alert cloud users of any anomalous behavior caused by compromised credentials or keys.

6. Sharpen Incident Response with Detailed Cloud Forensics

With deep understanding of cloud environments, Prisma Cloud reduces investigation time to seconds. Visualize your cloud environment to quickly pinpoint issues and perform upstream and downstream impact analysis. Prisma Cloud also provides the time-machine-like capability to view activity for any given resource. You can review the history of changes for a resource and better understand the root cause of an incident, past or present. For example, you can run a query to find all databases that were communicating directly via the internet last month. The resulting map will find all such instances as well as highlight the resources that are potentially compromised.

7. Protect Data Throughout the Lifecycle

Storage volumes within public cloud services are an often-over-looked source of security threats and attacks. With Prisma Cloud, you can discover and classify data within containers and buckets; evaluate your exposure based on policy; auto-remediate publicly exposed data; and quarantine malware—so you can be assured that your use of public cloud storage does not expose your company to new security vulnerabilities.

8. Amplify the Value of Existing Investments

Most organizations have already invested in existing technologies to help them manage logging and reporting, security orchestration or threat intelligence feeds to stay up to date on the latest threats. Prisma Cloud natively integrates with Qualys® and Tenable®, further enriching the depth of visibility into the security state of your cloud environment. By directly integrating with common security information and event management (SIEM) systems, such as Splunk®, Prisma Cloud seamlessly fits into existing workflows, eliminating the requirement to learn new processes or add more steps.

9. Remove the Roadblocks to Growth and Change

As organizations build comfort and confidence in the public cloud, environments grow more complex and distributed. This leads to overwhelmed security teams unable to keep pace with the sheer number of resources and alerts to manage. Prisma Cloud eliminates this feeling by helping teams maintain full visibility and granular control over their environments regardless of complexity. Furthermore, because Prisma Cloud is cloud agnostic, it enables seamless transitions between cloud providers as the UI remains the same. This means organizations can choose the best cloud platform for their project without worrying about having to learn a new set of services.

10. Focus on the Business, Not Learning a New Service

Cloud providers continue to deliver new services at a frenetic pace, leaving already time-constrained teams with having to learn how these newly released services fit (or do not fit) into their existing workflows. Prisma Cloud eliminates the need to keep up to date with the latest by making sense of new services for you, ensuring you adopt them safely and correctly. Let Prisma Cloud figure out how to ingest the new API data and provide actionable insight so you can focus on what really matters: running your business.

PRISMA CLOUD
BY PALO ALTO NETWORKS

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

10-ways-prisma-cloud-complements-cloud-native-security-ds-080219