Prisma Cloud on Amazon Web Services

Prisma Cloud Simplifies Cloud Threat Defense on AWS

Cloud computing adoption is outpacing cybersecurity defenses. The absence of a physical network boundary to the internet, risk of accidental exposure by inexperienced users, decentralized visibility, and the dynamic nature of the cloud increase the attack surface by orders of magnitude. Although security point products may be able to address individual challenges, they are unable to provide holistic protection in an environment where resources are constantly changing, such as Amazon Web Services.

Benefits of Prisma Cloud on AWS

- Visualize every connected resource across your AWS environment.
- Maintain continuous compliance and easily generate reports across your AWS environment.
- Enable secure DevOps by setting guardrails with realtime monitoring for threats, such as risky configurations, sensitive user activities, network intrusions, and host vulnerabilities.
- Use anomaly detection capabilities to root out account compromises and insider threats.
- Investigate current threats or past incidents and quickly determine root causes.
- Get contextual alerts to help your team prioritize issues and respond quickly.
- Integrate seamlessly with Amazon GuardDuty.

Prisma™ Cloud is a security and compliance service that dynamically discovers cloud resource changes and continuously correlates raw, siloed data sources, including user activity, resource configurations, network traffic, threat intelligence, and vulnerability feeds, to provide a complete view of cloud risk. Through an innovative, machine learning-driven approach, Prisma Cloud enables organizations to quickly prioritize risks, maintain agile development, and effectively fulfill their obligations in the shared responsibility model.

Key Features and Benefits to Secure AWS Unmatched Visibility

Visualize your entire AWS® environment, down to every component. Prisma Cloud dynamically discovers cloud resources and applications by continuously correlating configuration, user activity, and network traffic data. Combining this comprehensive understanding of the AWS environment with data from external sources, such as threat intelligence feeds and vulnerability scanners, Prisma Cloud delivers complete context for each risk.

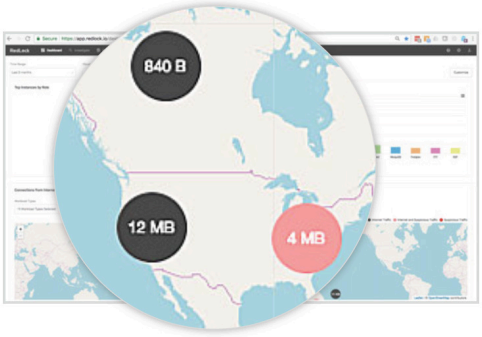

Figure 1: Complete environment visibility

Simplified Cloud Compliance

Prisma Cloud includes pre-built policies that adhere to industry-standard best practices, such as those put forth by CIS, GDPR, NIST, SOC 2, and PCI. You can also create custom policies based on your organization's specific needs. Prisma Cloud continuously monitors for policy violations across all connected resources and supports one-click reports for simplified audits of your AWS environment.

Figure 2: Continuous compliance monitoring

Policy Guardrails

Prisma Cloud lets you set guardrails for DevOps to maintain agile development without compromising on security. This enables you to detect threats, such as risky configurations, sensitive user activities, network intrusions, and host vulnerabilities. Prisma Cloud automatically ranks risk scores for every resource, based on the severity of business risks, violations, and anomalies, helping SecOps quickly identify the riskiest resources and prioritize remediation efforts accordingly.

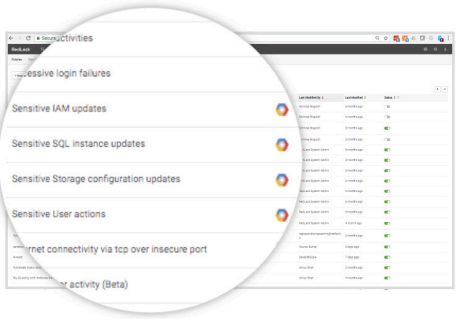

Figure 3: Automatic risk triage

Threat Detection

Prisma Cloud automatically detects anomalies in user and other behavior across your entire AWS environment, establishing behavior baselines and flagging any deviations. For example, a potential access key compromise will be flagged if a user is determined to be using access keys from two locations at similar times that are geographically impossible.

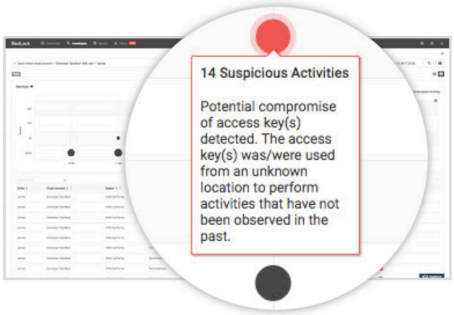

Figure 4: Automatic anomaly detection

Incident Investigation

With deep understanding of the AWS environment, Prisma Cloud reduces investigation time to seconds. You can quickly pinpoint issues, perform upstream and downstream impact analysis, and review the history of changes to a resource to better understand the root cause of an incident. 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 and highlight the resources that are potentially compromised. figure 5, many resources are communicating with known malicious IP addresses.

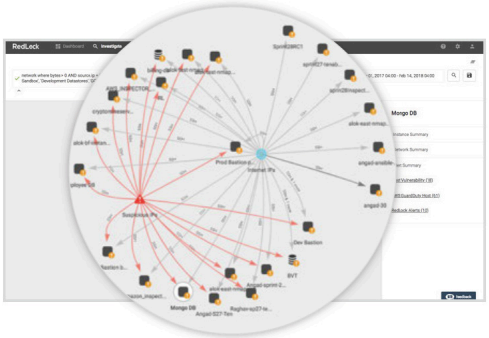

Figure 5: Fast, easy investigation

Contextual Alerting and Adaptive Response

Prisma Cloud enables your teams to quickly respond to issues based on contextual alerts. These alerts, triggered based on a patent-pending risk scoring methodology, provide context on all risk factors associated with a resource, making it simple to prioritize the most important issues. You can send alerts, orchestrate policy, or perform auto-remediation. You can even route alerts to tools such as Slack®, Splunk®, and our own Cortex™ XSOAR to remediate issues. In the case of a risky database, Prisma Cloud will generate a contextual alert with information on risk factors to enable automated response.

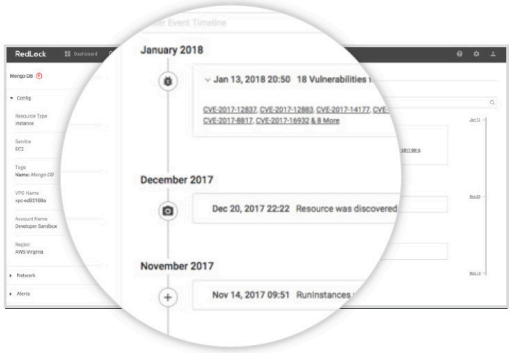

Figure 6: Contextual alerts

Integration with Amazon GuardDuty

The contextual, machine learning-powered security and compliance controls of Prisma Cloud natively integrate with Amazon GuardDuty® to continuously monitor for malicious or unauthorized behaviors across your entire AWS environment. This lets you detect activities such as unusual API calls or potentially unauthorized deployments that indicate possible account compromises, including potentially compromised instances or reconnaissance by attackers.

Developing a Cloud Threat Defense Roadmap for AWS

Prisma Cloud enables you to develop a cloud threat defense program across your entire AWS environment, from inception to maturity, with the following capabilities:

- **Compliance assurance:** Mapping cloud resource configurations to compliance frameworks, such as CIS Benchmarks, GDPR, PCI DSS, and HIPAA, can be extremely time-consuming. Using prepackaged policies, Prisma Cloud enables continuous monitoring, auto-remediation, and one-click reporting, simplifying the process of staying compliant.
- **Security governance:** Incomplete visibility and imprecise control over changes in dynamic public cloud computing environments can make security governance difficult. Prisma Cloud enables architecture validation by establishing policy guardrails to detect and auto-remediate risks across resource configurations, network architecture, and user activities. With Prisma Cloud, you can finally support DevOps agility without compromising on security.
- **SOC enablement:** Security operations teams are inundated with alerts that provide little context on the issues, which makes it hard to triage issues in a timely manner. Prisma Cloud makes it possible to identify vulnerabilities, detect threats, investigate current or past incidents, and remediate issues across your entire AWS environment in minutes.

Table 1: Cloud Threat Defense Maturity Model

Stage 1: Adopt	Stage 2: Expand	Stage 3: Scale
Cloud Footprint: • Dozens of workloads • Few cloud accounts	**Cloud Footprint:** • Hundreds of workloads • Many cloud accounts	**Cloud Footprint:** • Multiple cloud providers • Thousands of workloads • Dozens of cloud accounts
Objectives: • Compliance assurance • Security governance	**Objectives:** • Central visibility • Threat detection • Vulnerability management **+ Stage 1 objectives**	**Objectives:** • Auto-remediation • Incident investigation **+ Stage 2 objectives**

Prisma Cloud Security Suite

Prisma Cloud provides comprehensive visibility, threat detection, and rapid response across your entire AWS environment. A unique combination of continuous monitoring, compliance assurance, and security analytics enables security teams to respond more quickly to the most critical threats by replacing manual investigations with automated reports, threat prioritization, and remediation. With its API-based approach, Prisma Cloud delivers superior cloud native security.

paloalto 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