Prisma Cloud for Cloud Security Posture Management

Gain Visibility and Secure the Cloud Infrastructure

Prisma Cloud reduces complexity and secures resources across hybrid and multicloud environments. Trusted by more than 2,000 leading organizations worldwide, our comprehensive cloud-native application protection platform (CNAPP) secures over four billion cloud resources and analyzes more than one trillion events daily. Prisma Cloud eliminates blind spots and detects threats that other tools miss, giving users complete visibility, continuous threat detection, and automated response.

Why CSPM?

Effective cloud security requires complete visibility into every deployed resource and absolute confidence in its configuration and compliance status. As enterprises continue to adopt cloud-native methodologies and gain the flexibility of multicloud architectures, stitching together security data from disparate legacy tools becomes a considerable obstacle. A single, integrated solution, like Prisma Cloud, can help security teams maintain a strong security and compliance posture across multicloud environments.

Prisma Cloud takes a unique approach to cloud security posture management (CSPM), delivering best-of-breed CSPM capabilities integrated into a comprehensive CNAPP. The CSPM capabilities alone detect misconfigurations and threats, helping organizations improve their security and compliance posture. When coupled with additional modules, Prisma Cloud correlates CSPM findings with vulnerabilities, identity risks, data risks, and more to identify chains of issues that pose the greatest threat to your cloud environments.

This datasheet covers what to expect from the CSPM capabilities of Prisma Cloud, whether they are consumed alone or paired with additional modules.

Prisma Cloud for CSPM

Visibility, Compliance, and Governance

Cloud Asset Inventory

Prisma Cloud delivers comprehensive visibility and control over the security posture of every deployed resource. While some solutions simply aggregate asset data, Prisma Cloud analyzes and normalizes disparate data sources to provide unmatched risk clarity.

Continuous Visibility for Asset and Configuration State Tracking

Unlike some CSPM tools that provide point-in-time snapshots of cloud states, Prisma Cloud provides real-time and historical visibility across assets and configurations. The platform collects audit event logs, allowing security admins to see what configuration changes happened and when.

Detect Misconfigurations

To identify misconfigurations across cloud infrastructure, you can view the cloud configuration. Prisma Cloud offers more than 1,500 misconfiguration checks out of the box. Prisma Cloud also has a customizable policy model, enabling security teams to create additional configuration checks that meet their personal requirements.

Compliance Monitoring and Reporting

Prisma Cloud continuously monitors cloud compliance posture and supports one-click reporting from a single console. More than 75 compliance frameworks are included out of the box, and you can build additional custom frameworks.

Network Flow Visibility

Prisma Cloud processes over 1 trillion cloud events each day, including network flows. By ingesting flow data from AWS CloudWatch, Azure Network Watcher, and Google Stackdriver Logging, security teams can see network communications entering, leaving, and moving across clouds. Prisma Cloud also incorporates threat intelligence, helping you identify traffic coming from the known malicious IP addresses on the internet.

Effective Network Exposure

Network security groups, access control lists (ACLs), and firewall rules are often misconfigured or allow excessive traffic. However, a single misconfiguration does indicate true network exposure. Instead of generating excessive alerts against network security group misconfigurations, Prisma Cloud analyzes relationships between all network configurations across AWS, Azure, and GCP deployments to determine which assets are publicly exposed. The platform also provides a graph to visualize network exposures, including a hop-by-hop analysis of network paths.

Cloud Investigation and Queries

Use a flexible query model to ask questions about your cloud deployments, regardless of the complexity of your environments. Prisma Cloud enables security teams to explore assets, events, network configurations, and traffic. The platform provides output in table and graph views, helping you understand your cloud estate and get the context you need to make informed security decisions.

Remediation

Addressing misconfigurations can be a complex task for some organizations because they may lack the sufficient context to communicate remediation steps with the teams responsible for cloud assets. That's why Prisma Cloud provides step-by-step remediation instructions for misconfigurations and compliance violations. Using native integrations with external ticketing systems (e.g., Jira, ServiceNow, PagerDuty), security teams can send risk and remediation context to the teams who are responsible for misconfigurations. In many cases, Prisma Cloud can enforce automated remediation to fix the misconfiguration with minimal human intervention.

Threat Detection

User and Entity Behavior Analytics (UEBA)

Prisma Cloud analyzes millions of audit events and then uses machine learning (ML) to detect anomalous activities that could signal account compromises, insider threats, stolen access keys, and other potentially malicious user activities.

Network Anomaly and Threat Detection

Prisma Cloud monitors network behavior and uses ML and advanced threat feeds to detect network anomalies and threats. With Prisma Cloud, you can detect port scan and port sweep activities that probe a server or host for open ports as well as threats hiding in Domain Name System (DNS) traffic, such as domain generation algorithm (DGA), and cryptomining activity.

Automated Investigation and Response

Prisma Cloud provides automated remediation, detailed forensics, and correlation capabilities. Insights combined from workloads, networks, user activity, data, and configurations accelerate incident investigation and response.

Extending Beyond CSPM

Prisma Cloud provides value that standalone CSPM tools cannot. The platform integrates best-of-breed CSPM capabilities into a single-vendor CNAPP, providing additional value beyond standalone CSPM products. Below is what Prisma Cloud can do for your organization when bundled with other modules.

Correlate Findings to Prioritize and Understand Critical Risks

A misconfiguration by itself does not always represent application risk. The overall risk requires correlation of a broad set of information beyond what standalone CSPM tools observe. Prisma Cloud analyzes misconfigurations, vulnerabilities, public exposures, excessive permissions, exposed secrets, sensitive data, incidents, and more to identify interrelated issues that present critical risks. By finding interconnected issues, Prisma Cloud identifies potential attack paths that adversaries can use to target applications.

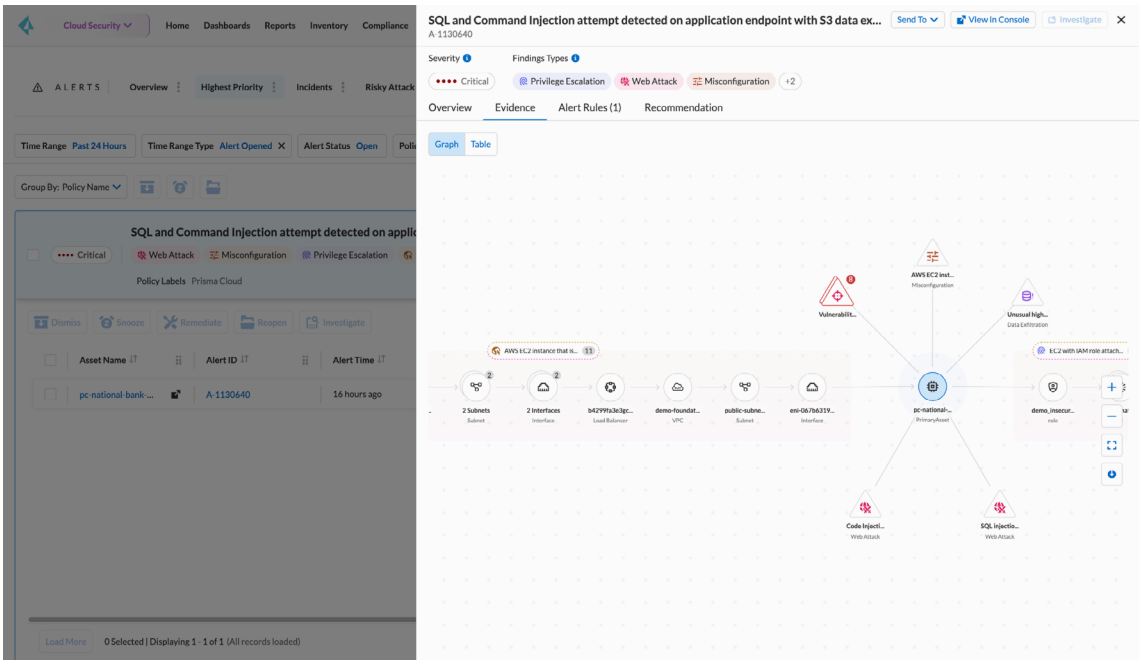

Figure 1: Prisma Cloud illustrates attack paths using a graph

Visualize Attack Paths to Accelerate Investigations

Understand complex attack paths and isolate the root cause of issues. The Infinity Graph in Prisma Cloud visualizes interconnected risks, helping security teams understand how several configuration mistakes form attack paths. Prisma Cloud also provides application context to help identify business logic and the person or team responsible for the application. By contextualizing investigation workflows, security teams can get the information they need to take remediation action.

Remediate Risk Efficiently

Fix issues to break attack paths and potentially prevent future mistakes. Prisma Cloud provides several different options to address risks such as opening tickets with application owners, automatically remediating misconfigurations, or sending pull requests to developers. Security professionals can communicate risk context and remediation steps to help reduce any developer friction.

"Prisma Cloud has definitely enabled me to centralize and automate reporting and alert management, and take on this huge task by myself, thereby freeing up a lot of time for me to do other critical work."

– Jacob Bornemann,
Senior Security Engineer,
The Pokémon Company International, Inc.

Read the full case study.

About Prisma Cloud

Prisma® Cloud is the industry's most comprehensive cloud-native application protection platform (CNAPP) with the broadest security and compliance coverage—for applications, data, and the entire cloud-native technology stack—throughout the development lifecycle and across hybrid and multi-cloud environments. Our integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate secure cloud-native application development.

To learn more, visit us online and request a demo.

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