PRISMA CLOUD | paloalto NETWORKS

Cloud Security Posture Management

Monitor posture, detect and respond to threats, and maintain compliance

Prisma® Cloud reduces complexity and secures resources across hybrid and multi-cloud environments. Trusted by more than 1,800 leading organizations worldwide, our comprehensive cloud native security platform (CNSP) has monitored more than 1.5 billion cloud assets, ingested more than 500 billion terabytes of flow logs, and processed 5 billion audit logs. Prisma Cloud eliminates blind spots and detects threats that other tools miss, giving users complete visibility, continuous threat detection, and automated response.

Comprehensive Security Posture Management for a Multi-Cloud Reality

Effective cloud security requires complete visibility into every deployed resource as well as absolute confidence in their configuration and compliance status. As enterprises further adopt cloud native methodologies and gain the flexibility of multi-cloud architectures, stitching together security data from disparate legacy tools becomes a considerable obstacle. DevOps and security teams need a single, integrated solution like Prisma Cloud.

The platform takes a unique approach to cloud security posture management (CSPM), going beyond mere compliance or configuration management. Vulnerability intelligence from more than 30 data sources provides immediate clarity on critical security issues while controls across the development pipeline prevent insecure configurations from ever reaching production.

Prisma Cloud CSPM Modules

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.

Amazon EFS	aws	24	0	24	0	24	0	0%
AWS Secrets Manager	aws	7	7	0	0	0	0	100%
Amazon EKS	aws	1	0	1	0	1	0	0%
Amazon SQS	aws	5	0	5	0	5	0	0%
Amazon S3	aws	66	0	66	66	0	0	0%
Azure Virtual Network	Azure	120	87	33	18	15	0	73%
Azure Network Watcher	Azure	31	31	0	0	0	0	100%
Azure Resource Manager	Azure	9	7	2	0	0	2	78%
Azure Policy	Azure	3	3	0	0	0	0	100%
Azure SQL Database	Azure	2	0	2	2	0	0	0%
Azure Compute	Azure	31	17	14	5	9	0	55%
Azure Storage	Azure	13	0	13	1	12	0	0%
Azure App Service	Azure	1	1	0	0	0	0	100%
Azure Security Center	Azure	2	0	2	0	2	0	0%
Google Resource Manager	Google	114	91	23	12	11	0	80%

Figure 1: Asset inventory

Compliance Monitoring and Reporting

Prisma Cloud continuously monitors cloud compliance posture and supports one-click reporting from a single console. More than 15 compliance frameworks are included out of the box, and you can build additional custom frameworks.

Figure 2: Compliance dashboard

Infrastructure-as-Code (IaC) Scanning

Prisma Cloud enables users to scan IaC templates for vulnerabilities and build cloud-agnostic policies for the build and runtime development phases.

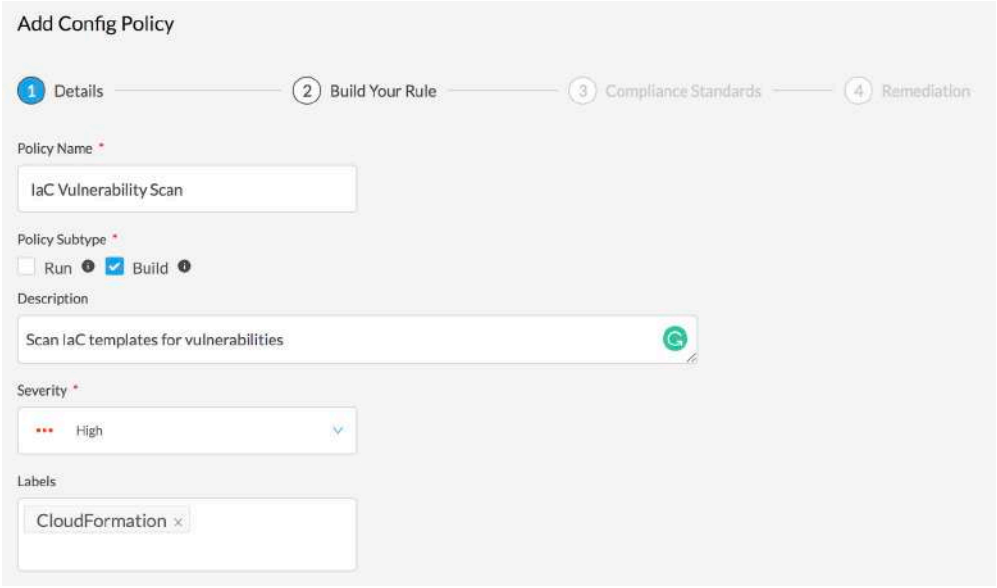

Figure 3: Custom IaC policy creation

Threat Detection

User and Entity Behavior Analytics (UEBA)

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

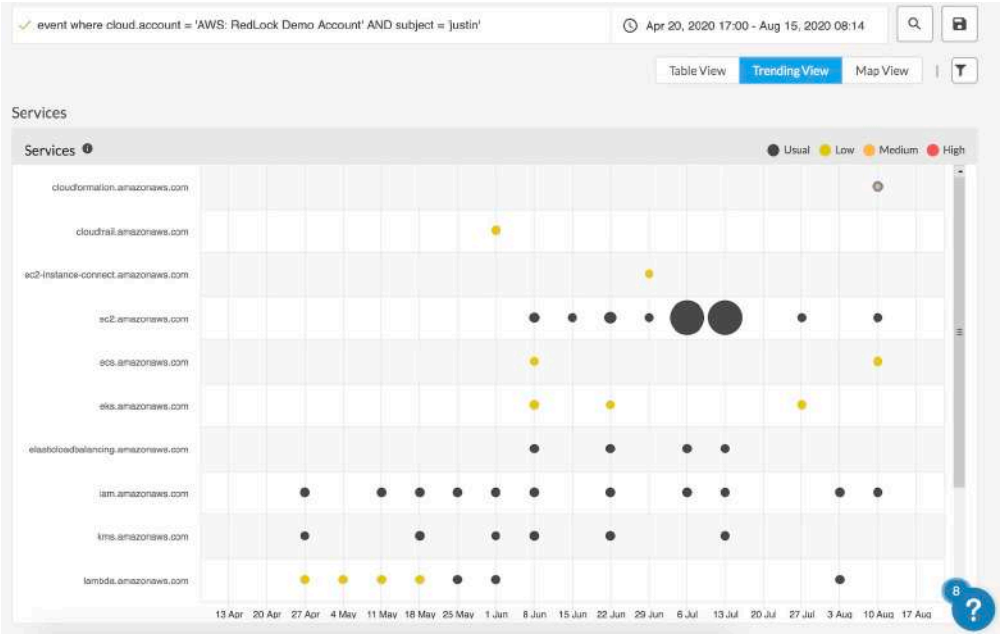

Figure 4: Anomalous activity tracker

Network Anomaly Detection

Prisma Cloud monitors cloud environments for unusual network behavior and can detect unusual server port or protocol activity, including port scan and port sweep activities that probe a server or host for open ports.

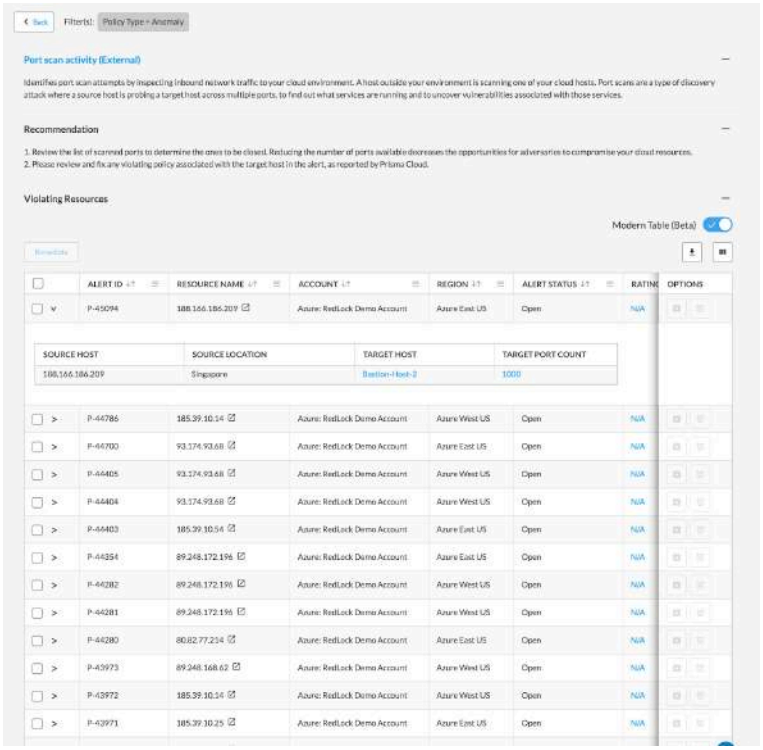

Figure 5: Port scan activity detail

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.

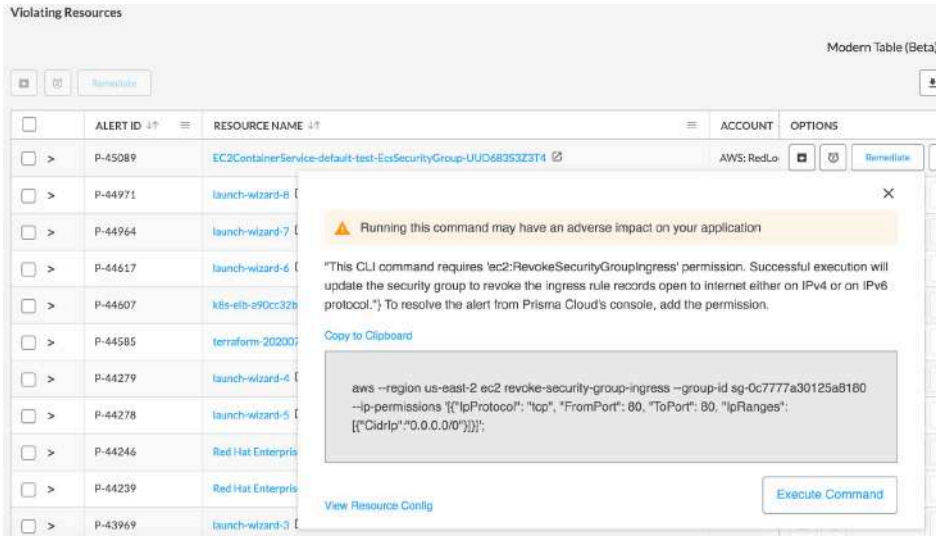

Figure 6: Automated investigation detail

Data Security

Data Visibility and Classification

Prisma Cloud provides complete visibility into all Amazon Web Services Simple Storage Service (AWS® S3) buckets and objects, including contents by region, owner, and exposure level. You can fine-tune data identifiers—such as driver's license, Social Security number, credit card number, or other patterns—to identify and monitor sensitive content.

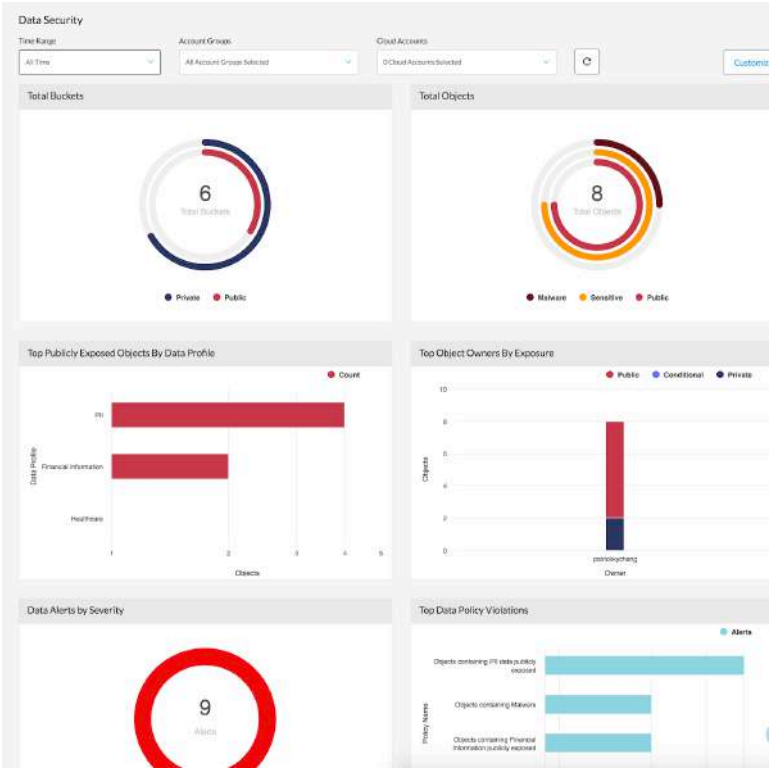

Figure 7: S3 Data Security dashboard

Data Governance

Prisma Cloud includes specific data policies to quickly determine your risk profile based on data classification and exposure/file types. Enable or disable data compliance assessment profiles (e.g., PCI, GDPR, SOC 2, and HIPAA) based on needs and generate audit-ready reports with a single click.

Malware Detection

Prisma Cloud helps users identify and protect against known and unknown file-based threats that have infiltrated S3 buckets, leveraging the WildFire® malware prevention service to flag any objects that contain malware.

Alerting and Remediation

Prisma Cloud automatically generates alerts for each object based on data classification, data exposure, and file types. Analysts can take action on alerts to quickly remediate exposure, tag individual DevOps teams for violations, and delete any objects that contain malware.

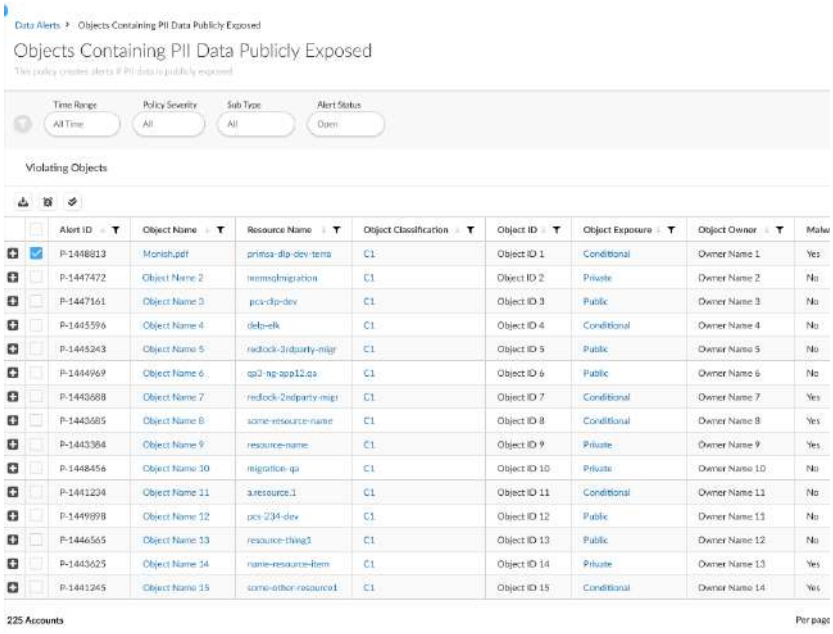

Figure 8: Object scan results for PII

"As a leader, I sleep better at night knowing I have a tool that does continuous monitoring for me. My teams are very plugged into it, and we have folks that look at Prisma Cloud every day. It has transformed the way we maintain compliance and visibility."

—John Hluboky, Vice President of Information Security, Veradigm Health

Read the full case study

About Prisma Cloud

Prisma® Cloud is a comprehensive cloud native security platform (CNSP) with the industry's 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. The integrated approach eliminates the security constraints around cloud native architectures—rather than masking them—and breaks down security operational silos across the entire application lifecycle, allowing DevSecOps adoption and enhanced responsiveness to the changing security needs of cloud native architectures.

To learn more, visit us online or watch a demo now.

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