Prisma Cloud
At a Glance

Comprehensive Cloud Native Security. Full Lifecycle. For Any Cloud.

Prisma™ Cloud is the industry's most 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 platform offers an integrated approach that enables security operations and DevOps teams to collaborate effectively and accelerate secure cloud native application development.

Prisma Cloud protects and integrates with cloud native architectures and toolkits to ensure complete security coverage while breaking security operational silos across the entire application lifecycle. Fundamentally, it enables DevSecOps adoption and enhanced responsiveness to the changing security needs of cloud native architectures.

Prisma Cloud Pillars

Cloud Security Posture Management (CSPM)

Effective cloud security requires complete visibility into every deployed resource along with absolute confidence in their configuration and compliance status. Prisma Cloud takes a unique approach to CSPM, going beyond mere compliance or configuration management. Vulnerability intelligence from more than 30 sources provides immediate risk clarity while controls across the development pipeline prevent insecure configurations from ever reaching production in the first place. Prisma Cloud provides:

- Visibility, compliance, and governance
  - » Cloud asset inventory
  - » Configuration assessment (runtime)
  - » Compliance monitoring and reporting
  - » Infrastructure-as-code (IaC) configuration scans (IDE, SCM, and CI/CD)
- Threat detection
  - » User and entity behavior analytics (UEBA)
  - » API-based network traffic visibility, analytics, and anomaly detection
  - » Automated investigation and response

- Data security (AWS® support only)
  - » Data classification
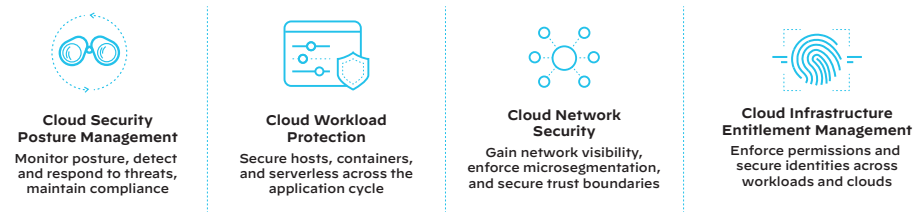 - » Malware scanning
  - » Data governance

Cloud Security Posture Management
Monitor posture, detect and respond to threats, maintain compliance

Cloud Workload Protection
Secure hosts, containers, and serverless across the application cycle

Cloud Network Security
Gain network visibility, enforce microsegmentation, and secure trust boundaries

Cloud Infrastructure Entitlement Management
Enforce permissions and secure identities across workloads and clouds

Figure 1: Prisma Cloud pillars

Cloud Workload Protection

The cloud native landscape is constantly evolving. New platforms and technologies allow organizations to deploy more rapidly and at greater scale than ever. Prisma Cloud delivers full lifecycle protection across public and private clouds as well as on-premises environments. You can easily integrate security into the leading continuous integration/continuous delivery (CI/CD) workflows, registries, and running stacks. Security modules include:

- Host Security
  - » Vulnerability management
  - » Runtime security
  - » Compliance management
  - » Access control
- Container Security
  - » Vulnerability management
  - » Runtime security
  - » Compliance management
  - » Access control
  - » Git repository scanning

Prisma Cloud
At a Glance

- Serverless Security
  - » Vulnerability management
  - » Runtime security
  - » Compliance management
  - » Access control
- Web Application and API Security
  - » OWASP Top 10 protection
  - » API protection

Cloud Network Security

Network protection must be adapted for cloud native environments while still enforcing consistent policies across hybrid environments. Prisma Cloud detects and prevents network anomalies by enforcing container-level microsegmentation, inspecting traffic flow logs, and leveraging advanced cloud native Layer 7 threat prevention:

- Network visibility and anomaly detection
- Identity-based microsegmentation
- Cloud native firewalling

Cloud Infrastructure Entitlement Management

Traditional manual methods for determining least-privileged access make it difficult for security teams to keep up with the growing number of entitlements across cloud services. Prisma Cloud continuously detects and automatically remediates identity and access risks across infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) offerings. It discovers all human and machine identities across cloud environments, and then analyzes entitlements, roles, and policies. Prisma Cloud provides:

- Permissions visibility
- IAM governance
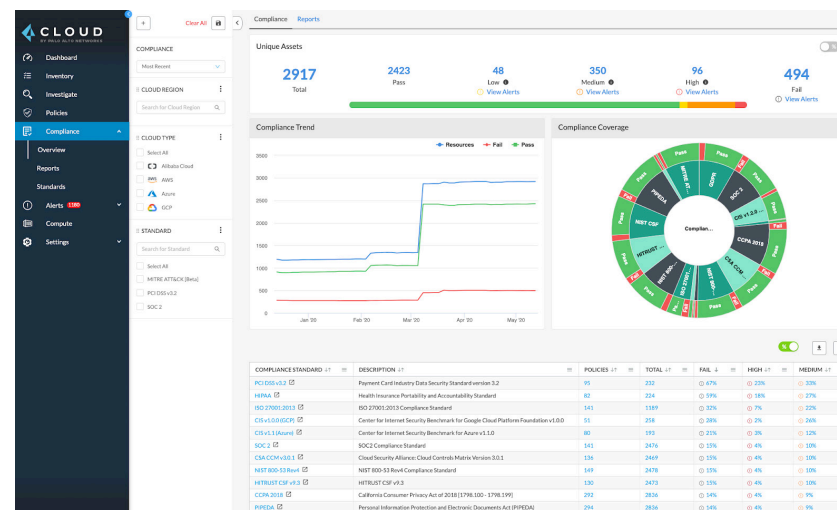- Automated response
- User and entity behavior analytics (UEBA)

Figure 2: Prisma Cloud dashboard

"When we looked at Prisma Cloud, it just wasn't just the tool or the capabilities that they have today, it was the roadmap that they have, the vision that they have. And that makes a huge difference—because this is a journey."

—Experian

Read the full case study

About Prisma Cloud

Prisma Cloud is a comprehensive cloud native security platform 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.