Why Prisma Cloud?

- One-click compliance reporting for easy auditing of all major regulatory frameworks.
- Detection for all threats across all AWS accounts. Enforcement with role-based access control (RBAC) and 600+ machine learning (ML)–powered policy controls built specifically for AWS.
- AWS multi-account automation for auto-registration and auto-remediation with Control Tower.
- Data security that scans and detects AWS Simple Cloud Storage (S3) misconfigurations and personally identifiable information (PII) or sensitive data exposure.

Product overview

Prisma® Cloud is a comprehensive, cloud-native security platform (CNSP) with broad security and compliance coverage. It applies across the development lifecycle for applications, data, and the entire cloud-native technology stack. Prisma Cloud offers a comprehensive view of your security posture across your Amazon Web Services (AWS) accounts. Help secure, manage, and scale AWS workloads, containers, and hosts with centralized access and permissions control, compliance, and behavior and resource governance. It also includes Control Tower support for multi-account AWS.

Product features

Cloud native security
Pre-integrated solution that ingests all major AWS application programming interface (APIs) with centralized policy management and native security visibility.

Comprehensive security
- Monitor security posture, detect and respond to threats, and enforce compliance with more than 600 pre-built AWS policies.
- Protect virtual machines (VMs), Amazon Machine Images (AMIs), containers, Kubernetes, and container platforms, serverless functions, and infrastructure-as-code (IaC) templates.
- Secure cloud networks and enforce micro-segmentation.
- Enforce permissions and secure cloud access identities.

Full lifecycle security
Embedded protection across build, deploy, and run phases.
How it works

Prisma Cloud for AWS 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 integrating operational silos across the entire application lifecycle. This allows for development, security, and operations (DevSecOps) adoption and enhanced responsiveness to changing cloud-security needs.

Differentiators

- Collect, aggregate, normalize, and correlate data from various AWS services across accounts.
- Integrate vulnerability and infrastructure-as-code (IaC) scanning across various software and development tools.
- Embed security checks into continuous delivery (CD) workflows and registries to prevent insecure deployments.
- Isolate AWS organizational units, workloads, and apps to receive specific security requirements.
- Ingest GuardDuty and Inspector insights to enable security operations center (SOC) investigation and remediation workflows.
- Scale, experiment, and innovate more quickly across AWS with trusted Palo Alto Networks support.
What our customers are saying

“Prisma Cloud has helped strengthen the relationship between DevOps and InfoSec to unite the two teams.” — Jacob Bornemann, Sr. Security Engineer, Pokémon

Data Points

- 70% of Fortune 100s use Prisma Cloud
- 1.8B+ Resources monitored
- 1M+ Workloads secured
- ~5B Weekly audit logs processed

Additional Resources

- Prisma Cloud AWS datasheet
- Prisma Cloud 2.0
- How Palo Alto Networks and AWS Work Together

Solution available in AWS Marketplace