Red River

COMPREHENSIVE SECURITY WITH PRISMA CLOUD

paloalto® NETWORKS

FedRAMP

TABLE OF CONTENTS

Now more than ever, it's important for organizations to have a secure cloud platform. Most modern organizations realize the value in shifting security left in the development cycle — especially as applications are becoming collections of microservices and functions. Developers use a variety of tools to build and deploy cloud native applications, and operationalizing security controls that work seamlessly across these tools remain a challenge. However, Palo Alto has developed a cloud security platform that makes the shift across the entire development lifecycle seamless.

WHAT IS PRISMA CLOUD?

Prisma® Cloud, from Palo Alto, 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 making them, and breaks down security operational silos across the entire application lifecycle. This allows for DevSecOps adoption and enhanced responsiveness to the changing security needs of cloud native architectures.

Prisma Cloud uses machine learning to profile users, workload and app behaviors to prevent advanced threats. It also integrates with developer IDE environments and any CI/CD tool to provide full lifecycle vulnerability management, Infrastructure-as-Code scanning, runtime defense and cloud native firewalling. The main benefits of Prisma Cloud are:

- Comprehensive cloud security
- Consistent security across clouds
- Enables DevSecOps

PRISMA CLOUD PILLARS

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

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

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

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 compliance or configuration management. 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 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 cloud, as well as on-premises environment. Security models include:

Host Security:

- Vulnerability management
- Runtime security
- Compliance management
- Access control

Container Security:

- Vulnerability management
- Runtime security
- Compliance management
- Access control
- Git repository scanning

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 developments. Prisma Cloud detects and prevents network anomalies by enforcing container-level micro segmentation, inspecting traffic flow logs and leveraging advanced cloud native Layer 7 threat protection:

- Network visibility and anomaly detection
- Identity-based micro segmentation
- 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. Prisma Cloud provides:

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

PRISMA CLOUD COMPUTE EDITION

Cloud Native Security Challenges

Traditional security tools and methodologies are not suited to protect the developer-driven, infrastructure agnostic, multi-cloud patterns of cloud native applications. This is because:

- Developers and DevOps teams, vital in building and deploying cloud native applications, often operate outside the view of traditional security. This requires security that integrates with developer-led infrastructure and tooling.

- Organizations are using more compute options than ever, spanning hybrid and multi-cloud deployments as well as using a combination of host virtual machines (VMs), containers, Kubernetes, containers as a service (CaaS) and serverless functions.

- Cloud native environments constantly change at a tremendous scale. Security teams require automation to secure the growing number of ever-changing microservices their organizations use.

Cloud Workload Protection Across Hosts, Containers and Serverless

Prisma Cloud Compute Edition is a self-hosted option delivered via a container image that customers deploy and manage themselves in any environment — whether a public, private or hybrid cloud — including entirely air-gapped environments. The key benefits include:

- **Embrace any cloud native technology you prefer.** Future-proof your infrastructure decisions. Choose the right workload for any given application component and know your security platform has you covered.
- **Prioritize risks contextually in cloud native environments.** Leverage continuous vulnerability intelligence and risk prioritization across your entire cloud native infrastructure and throughout software lifecycle, including real-time connectivity graphs with runtime threat data.
- **Automate security at DevOps speed.** Empower developers and DevOps teams to deploy as quickly as possible to deliver business value to your customers and improve security outcomes.

SUMMARY

Prisma Cloud provides comprehensive visibility, threat detection, and rapid response across your entire public cloud environment, including Amazon Web Services, Microsoft Azure®, and Google Cloud Platform. A unique combination of continuous monitoring, compliance assurance, and security analytics enables security teams to respond more quickly to critical threats by replacing manual investigations with automated reports, threat prioritization, and remediation. With its API-based approach, Prisma Public Cloud delivers superior cloud native security.

Many Prisma Cloud CSPM capabilities are part of a Federal Risk and Authorization Management Program (FedRAMP) Moderate Authorized environment. For more information, visit paloaltonetworks.com/resources/datasheets/prisma-cloud-cspm-in-fedramp.

WHY RED RIVER?

Red River can guide your cloud journey and unleash the many benefits of cloud computing for your business. We offer the full spectrum of cloud services, from procurement to ongoing maintenance and management to application development. As a one-stop-shop to design, build and manage your public, private or hybrid cloud, we'll work to improve your customer experience, workforce efficiency and business agility. We understand the marketplace and how your data can be shared and protected.

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for businesses in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and expertise in security, networking, analytics, collaboration, mobility and cloud solutions.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.