paloalto NETWORKS

PRISMA™
BY PALO ALTO NETWORKS

Benefits

Prisma Cloud enables you to:

- Visualize every connected resource across your Azure environment.
- Maintain continuous compliance and easily generate reports across your Azure environment.
- Protect Azure applications and workloads across VMs and container services.
- Use anomaly detection capabilities to root out account compromises, insider threats, and anomalies in both network and application behavior.
- Investigate current threats or past incidents and quickly determine root cause.
- Get contextual alerts to help your team prioritize issues and respond more quickly.
- Integrate seamlessly with native Azure services, including Azure Policy and Azure DevOps.
- Utilize RQL to uncover new security and compliance risks as well as seek out incidents using threat hunting queries.
- Take advantage of AutoFocus™, the industry's most advanced contextual threat intelligence feed, to detect and prevent critical attacks.

Protect Microsoft Azure Environments with Prisma Cloud

Simplified Security Across the Lifecycle

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. Its integrated approach enables SecOps and DevOps teams to stay agile, collaborate effectively, and securely accelerate cloud native application development and deployment.

Complete Security for Microsoft Azure

Prisma Cloud provides full lifecycle security for any cloud native workload or application running on Microsoft Azure®. Prisma Cloud protects applications and the underlying compute by integrating security into Azure DevOps and Azure Container Registry (ACR) while protecting running workloads and apps. Whether you're running Azure Kubernetes Service, container instances, virtual machines, or Azure Red Hat OpenShift, Prisma Cloud has you covered. Beyond securing Azure compute, Prisma Cloud continuously monitors your environment's security posture and enforces governance guardrails on Azure services and users.

Key Features and Benefits to Secure Azure

Unmatched Visibility

Visualize your entire Azure environment, down to every component. Prisma Cloud dynamically discovers cloud resources and applications by continuously correlating configuration, user activity, and network traffic data.

Simplified Cloud Compliance

Prisma Cloud includes more than 550 built-in policies, providing coverage for various standards—such as CIS, GDPR, NIST, SOC 2, and PCI DSS, among others—as well as frameworks like MITRE ATT&CK®. You can customize any policy to suit your business needs. Prisma Cloud continuously monitors for policy violations across all resources and supports one-click reports for simplified audits of your Azure environment.

Full Lifecycle Security

Stay secure from development to production with unmatched vulnerability detection through native and third-party integrations, offering prevention at every stage of the application lifecycle. Detect and prevent security issues in container and machine images as well as infrastructure as code (IaC) templates. Prisma Cloud integrates with Azure DevOps and other tools along the development lifecycle to detect and address vulnerabilities before they make it to production.

Threat Detection

Prisma Cloud automatically detects anomalies in user and network behavior across your entire Azure environment, establishing behavior baselines and flagging any deviations. For example, a potential access key compromise will be flagged if a user is determined to be using access keys from two locations at similar times.

Incident Investigation

Prisma Cloud reduces investigation time to seconds. You can quickly pinpoint issues, perform upstream and downstream impact analysis, and review the history of changes to a resource to better understand the root cause of an incident. For example, you can run a query to find all databases that were exposed to and communicating directly with machines on the internet last month. The resulting map will find all such instances and highlight resources that may be compromised.

Integration with Azure Policy

Prisma Cloud integrates with Azure Policy to provide centralized visibility into security and compliance risks across your entire Azure environment. With this, your security teams can quickly gather data, identify threats, and take action before business damage or loss occurs.

Developing a Cloud Threat Defense Roadmap for Microsoft Azure

Prisma Cloud enables you to develop a cloud threat defense program across your entire Azure environment, from inception to maturity, with the following capabilities:

- **Compliance assurance:** Mapping cloud resource configurations to compliance frameworks, such as CIS, GDPR, PCI DSS, and HIPAA, can be extremely time-consuming. Using prepackaged policies, Prisma Cloud enables continuous monitoring, auto-remediation, and one-click reporting, simplifying the process of staying compliant.
- **Security governance:** Incomplete visibility and imprecise control over changes in dynamic public clouds can make security governance difficult. Prisma Cloud enables architecture validation by establishing policy guardrails to continually detect and auto-remediate risks across resource configurations, network architecture, and user activities. You can finally support DevOps agility without compromising on security.
- **SOC enablement:** Identify vulnerabilities, detect threats, investigate current or past incidents, and remediate those issues across your entire Azure environment in minutes. Prisma Cloud supports a broad set of integrations with ticketing systems; security information and event management (SIEM) solutions; and security orchestration, automation, and response (SOAR) tools such as Cortex™ XSOAR, making it fit seamlessly into day-to-day SOC operations.

Visit us online to learn more about how Palo Alto Networks secures Microsoft Azure environments.