PRISMA CLOUD
BY PALO ALTO NETWORKS

At a Glance: 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 play vital roles in building and deploying cloud-native applications, often operating outside the view of traditional security teams and technologies. This requires security that integrates with developer-led infrastructure and tooling.
- Organizations are using more compute options than ever. These options span multi- and hybrid-cloud deployments, and use a combination of host virtual machines, containers, Kubernetes®, containers as a service (CaaS), and serverless functions.
- Cloud-native environments constantly change at tremendous scale. Security teams require automation to secure the growing number of ever-changing microservices their organizations use.

Holistic Protection Across Hosts, Containers, and Serverless

Prisma™ Cloud Compute edition is the leading cloud-native security platform, providing holistic protection across hosts, containers, and serverless deployments in any cloud, throughout the software lifecycle. Prisma Cloud Compute edition itself is cloud-native and API-enabled, protecting all your workloads regardless of their underlying compute technology or the cloud in which they run.

Vulnerability management: Enjoy security from development to production with unmatched vulnerability detection, understanding, and prevention at every stage of the application lifecycle.

Compliance: Easily implement and maintain compliance for Docker, Kubernetes, and Linux CIS Benchmarks as well as external compliance regimes and custom requirements, including the industry's first compliance checks for the Istio® service mesh.

CI/CD integration: Integrate security directly into the continuous integration (CI) process to find and fix problems before they ever make it into production.

Runtime defense: Protect your environments at scale with machine learning that automatically creates least-privileged, whitelist-based runtime models for every version of every application.

Cloud-native firewalls: Take advantage of core layer 4 and web application firewalling, purpose-built for cloud-native applications.

Access control: Establish and monitor access control measures for cloud workloads and cloud-native applications across underlying hosts, Docker, and Kubernetes while integrating with identity and access management (IAM) and secrets management tools, along with other core technologies.

How It Works

Prisma Cloud Compute edition provides flexible deployment options to protect your workloads and applications wherever you choose to deploy them. Defenders—agents deployed within your environments—protect standalone virtual machines, Docker containers, Kubernetes clusters, CaaS, PaaS apps on Pivotal Application Service, and serverless applications. Defenders protect by whitelisting application behavior and preventing anomalous actions from occurring. Defense-in -depth combines core cloud-native firewalling with runtime defense to protect east-west traffic flows and leverage machine learning for known application behavior.

Prisma Cloud Compute edition provides vulnerability management and compliance for the full software lifecycle by integrating with any CI process, Docker registry, code repository, or any production environment to continuously monitor risk with powerful risk factors and prioritization. Enterprise-grade access control capabilities govern all cloud resources across compute infrastructure, secrets, Kubernetes audits, and IAM tooling.

Prisma Cloud Compute edition is a self-hosted option delivered via a container image that customers deploy and manage themselves in any environment—whether public, private, or hybrid cloud—including entirely air-gapped environments. For more information on the SaaS deployment model, please reference the Prisma Cloud At-a-Glance.

Learn More

To learn more about Prisma Cloud, visit the Palo Alto Networks website or download the Prisma Cloud At-a-Glance.

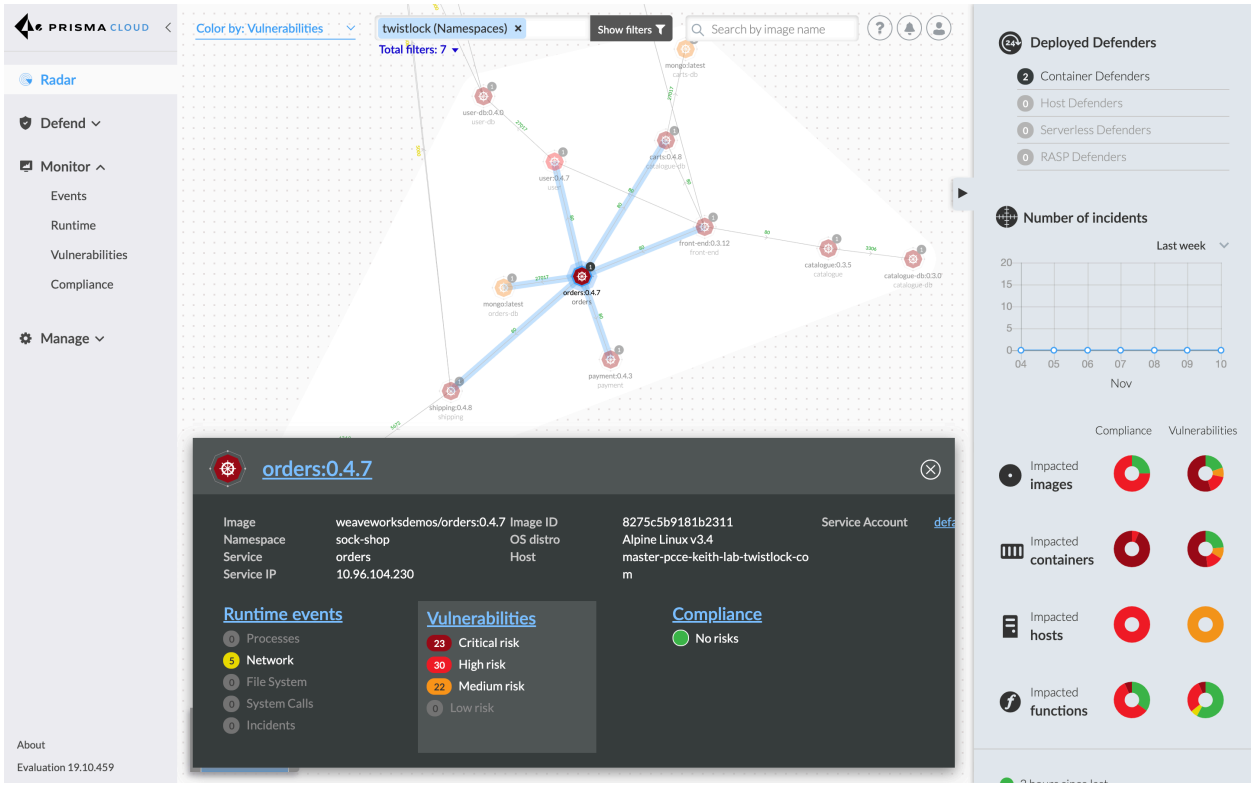

Figure 1: Customer operated-architecture in Compute edition

Key Benefits

- **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 the software lifecycle, including realtime 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 customers, and improve your security outcomes.