Prisma Cloud Compute Edition
At a Glance

PRISMA™

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 delivers a cloud workload protection platform (CWPP) for modern enterprises, providing holistic protection across hosts, containers, and serverless deployments in any cloud, throughout the software lifecycle. Prisma Cloud Compute Edition is cloud native and API-enabled, protecting all your workloads regardless of their underlying compute technology or the cloud in which they run.

Features

Rounding out its holistic protection, Prisma Cloud Compute Edition offers:

- **Vulnerability management**: Enjoy security from development through 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 security**: Integrate security directly into the continuous integration (CI) process to find and fix problems before they ever make it into production.
- **Runtime defense**: Secure your environments at scale with machine learning that automatically creates least-privileged, allow-list-based runtime models for every version of every application.
- **Web application and API security**: Protect against Layer 7 and OWASP Top 10 threats in any public or private cloud.
- **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 VMs, Docker containers, Kubernetes clusters, CaaS, PaaS apps on Pivotal Application Service, and serverless applications. Defenders protect by allow-listing 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 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
At a Glance

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. For more information on the SaaS deployment model, please see Prisma Cloud: At a Glance.

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 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 your security outcomes.

To learn more about Prisma Cloud, visit us online.

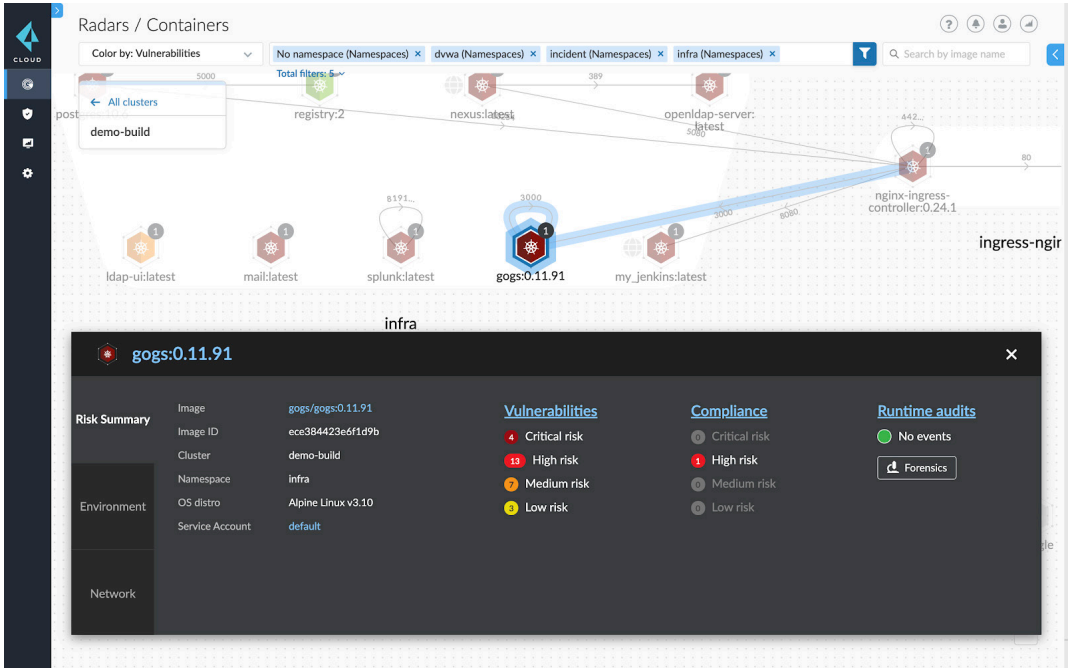

Figure 1: Prisma Cloud Radar and integrated vulnerability, compliance, and runtime details for containers