Cloud Workload Protection

Secure hosts, containers, and serverless across the application cycle

Secure hosts, containers, Kubernetes®, and serverless functions across the application lifecycle. Combine runtime protection with vulnerability management and compliance. Prisma™ Cloud secures any cloud native workload across build, deploy, and run.

Ranked #1 in Cloud Workload Security on IT Central Station	Ranked #1 in Container Security on IT Central Station	Trusted by 40+ of the Fortune 100
Secures workloads across hybrid and multi-cloud environments	Secures Linux and Windows containers running on Kubernetes or any other container platform	Protects leading organizations, helping secure 1,800+ customers globally

Unified Protection for Any Cloud Native Architecture

Today's enterprises use a combination of virtual machines (VMs), containers and Kubernetes, platform as a service (PaaS) offerings, and serverless functions to power their cloud workloads and cloud native applications. That's why Prisma Cloud delivers a unified agent framework to secure all these workloads and architectures.

Security Integrated Across the Application Lifecycle

Prisma Cloud integrates cloud workload protection platform (CWPP) capabilities across the application lifecycle. This enables enterprises to integrate vulnerability management and compliance as part of continuous integration (CI) processes and continuous delivery (CD) workflows; continuously monitor container registries and serverless repositories; and prioritize risk at runtime across hosts, containers and images, and serverless functions.

Modules

Host Security

Prisma Cloud Host Security protects Linux and Windows® hosts running on public or private clouds, delivering powerful capabilities:

- **Vulnerability management**: Continuously monitor hosts for vulnerabilities, combined with powerful risk prioritization with top 10 vulnerability lists.
- **Compliance**: Monitor and enforce pre-built security policy compliance checks with the Linux CIS Benchmark and Windows configuration checks, or implement custom compliance checks.
- **Runtime security**: Automatically profile workload behavior to alert on or prevent anomalous and malicious activity. Integrated protection includes file and directory read/write changes, host log inspection, and custom runtime rules language.
- **Network visibility**: View all the network communications of hosts in real time.
- **Access control**: Establish and monitor access control measures for cloud workloads.
- **Amazon Machine Image (AMI) scanning**: Scan AMIs for vulnerabilities before VMs are deployed on Amazon Web Services (AWS®).

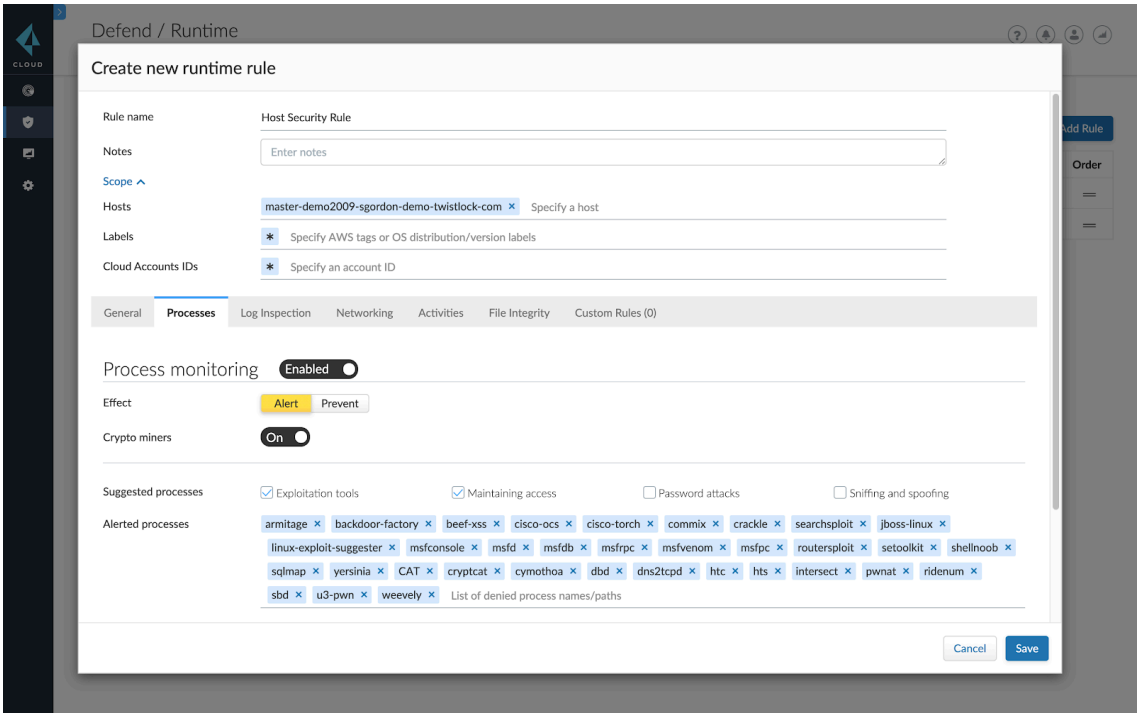

Figure 1: Host Security module

Container Security

Prisma Cloud Container Security secures containers and Kubernetes running on public or private clouds, offering:

- **Vulnerability management**: View accurate insights into vulnerabilities for images and containers. Vulnerability top 10 lists provide risk prioritization across all known CVEs and are supported with remediation guidance and per-layer image analysis.
- **Compliance checks**: Leverage more than 400 compliance checks, including CIS Benchmarks for Docker®, Kubernetes, Linux, Windows configurations, and Istio®. Pre-built, customizable frameworks support PCI DSS, HIPAA, GDPR, and NIST SP 800-190.
- **Runtime security**: Protect running applications by automating runtime policy creation across process, network, and file system sensors, ensuring security scales with your applications. Powerful custom runtime rules add to the security of your containerized applications.
- **Network visibility**: View all the network communications of containers and Kubernetes in real time.
- **Access control**: Establish and monitor access control measures for 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.
- **CI/CD security**: Integrate security as part of CI/CD workflows. Set granular vulnerability thresholds to alert on or block vulnerable images, or alert on or enforce compliance policies.

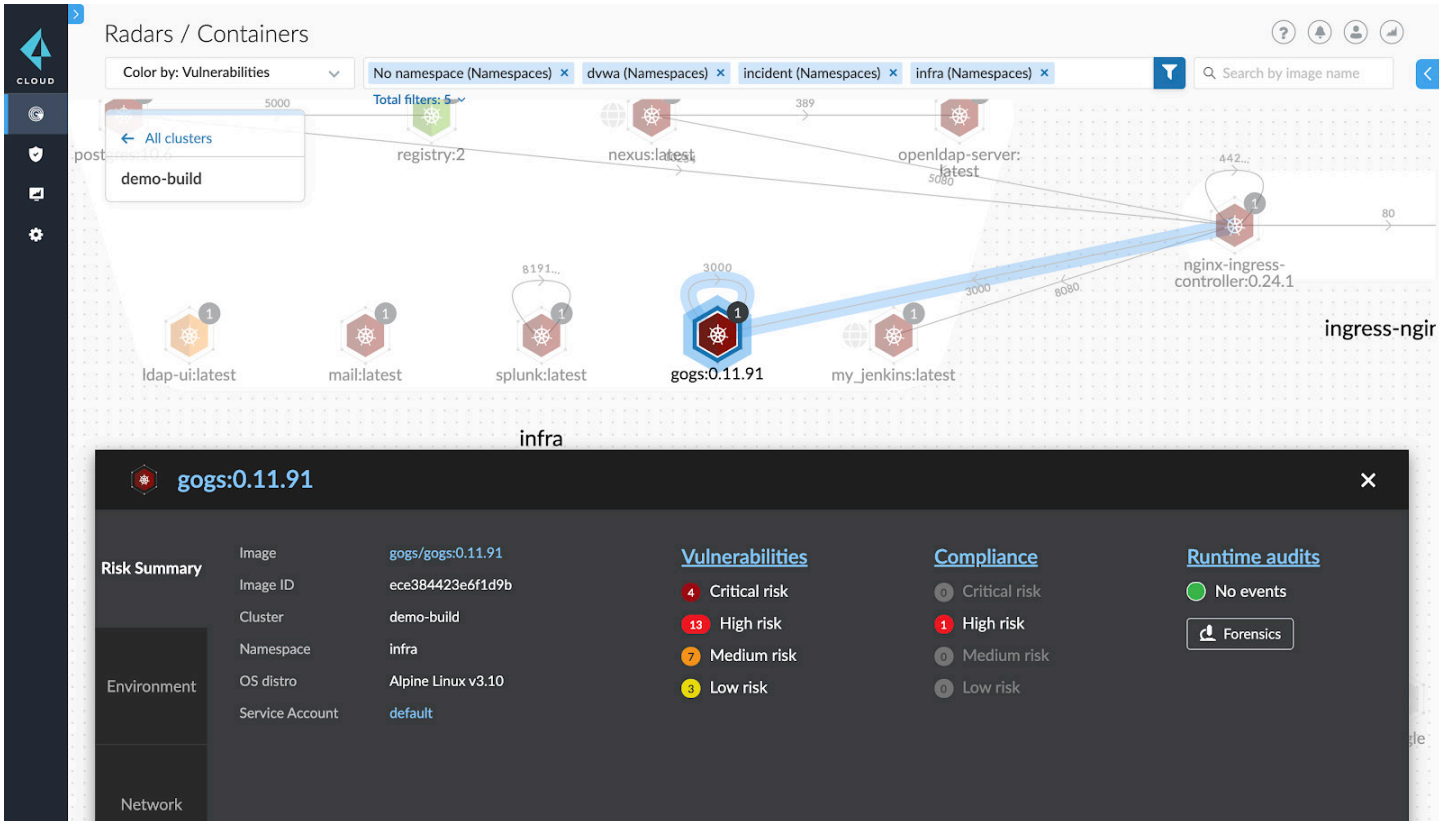

Figure 2: Container Security module

Serverless Security

Prisma Cloud Serverless Security protects serverless functions across the application lifecycle, providing:

- **Vulnerability management**: Scan and continuously monitor functions for vulnerabilities, starting with integrated CI tooling and serverless repositories and continuing through runtime for a full lifecycle view into serverless risk.
- **Compliance checks**: Identify misconfigurations, including private keys stored in function zips or broad resource access, for DevOps and security teams.
- **Runtime security**: View a live Radar visualization into running functions on AWS Lambda. See function triggers, continuously monitor vulnerability and compliance status, and see all connected Amazon and AWS services, such as CloudWatch, Elastic Cloud Compute (Amazon EC2®), and DynamoDB®. Protect running AWS Lambda functions from unwanted process, network, or file system activity.
- **CI/CD security**: Integrate security as part of CI/CD workflows. Set granular vulnerability thresholds to alert on or block vulnerable functions, or alert on and enforce compliance policies.

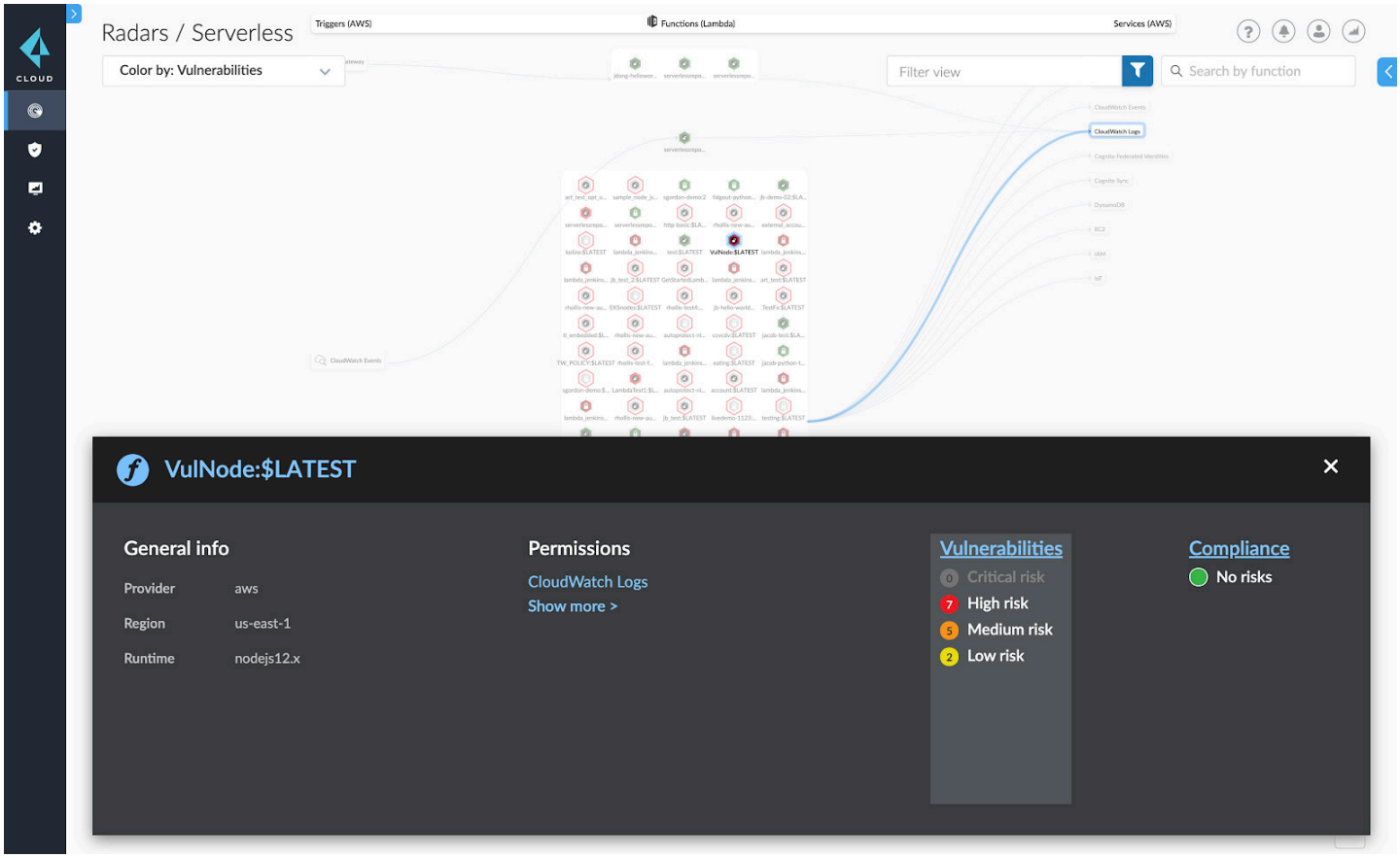

Figure 3: Serverless Security module

Web Application and API Security

Prisma Cloud Web Application and API Security protects against Layer 7 and OWASP Top 10 threats in any public or private cloud, providing:

- **OWASP Top 10 protection**: Alert on or prevent leading attack scenarios in the OWASP Top 10, including SQL injection, cross-site scripting (XSS), Shellshock protection, brute-force login attacks, and more.
- **API protection**: Identify protected and unprotected APIs, and then easily configure security rules and actions.
- **File upload protection**: Set alerts for or enforce file upload restrictions based on file extension and file content "sniffing." Fine-grained controls can allow, alert on, or block specific file formats, including audio, compressed archives, documents, images, and video.
- **Location-based access control**: Prevent web access for clients originating from specific IPs, networks, or countries.
- **HTTP header-based web application protection**: Define criteria for allowing or denying access to web applications based on HTTP header names or values.

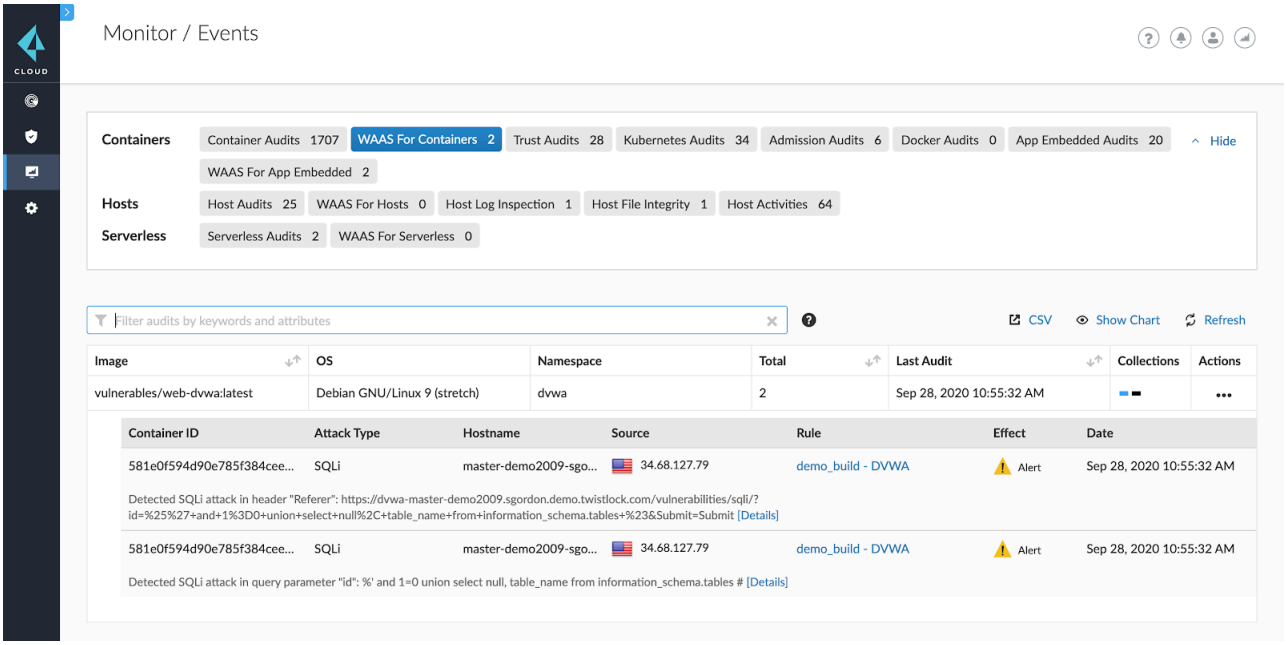

Figure 4: Web Application and API Security module

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. The integrated approach eliminates the security constraints around cloud native architectures—rather than masking them—and breaks down security operational silos across the entire application lifecycle, allowing DevSecOps adoption and enhanced responsiveness to the changing security needs of cloud native architectures.

To learn more, you can visit us online or watch a demo now.

> "Prisma Cloud helps our company reach the concept of DevSecOps, where we assess security in every phase of development. If any vulnerability or flaw is discovered, we patch it before going into production."
>
> **—Nicola Mutti, Head of Security, Cuebiq**
>
> Read the full case study

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com