Prisma Cloud Cloud Workload Protection

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

Named a Leader by Forrester in Their 2022 Wave for Cloud Workload Security	Ranked No. 1 in Container Security on IT Central Station	Cloud Workload Protection Company of the Year
Ranked No. 1 in Cloud Workload Security on IT Central Station	Named a Leader in the Frost Radar	Protects Leading Organizations and Helps Them Secure 1,900+ Global Customers

Unified Protection for Any Cloud-Native Architecture

Today's enterprises use a combination of virtual machines (VMs), containers, Kubernetes, containers as a service (CaaS), platform-as-a-service (PaaS) offerings, and serverless functions to power their cloud workloads and cloud-native applications. Prisma Cloud offers both agent-based and agentless protection from a single solution, giving you and your teams flexible deployment options that fit your unique environment.

Security Integrated Across the Application Lifecycle

Prisma Cloud integrates cloud workload protection platform (CWPP) capabilities and Web App and API Security (WAAS) 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. It also enables them to continuously monitor container registries and serverless repositories and prioritize risk at runtime across hosts, containers, images, and serverless functions. Lastly, customers can leverage an added layer of security for their web applications and APIs.

Modules

Host Security: Secure VMs on any public or private cloud.

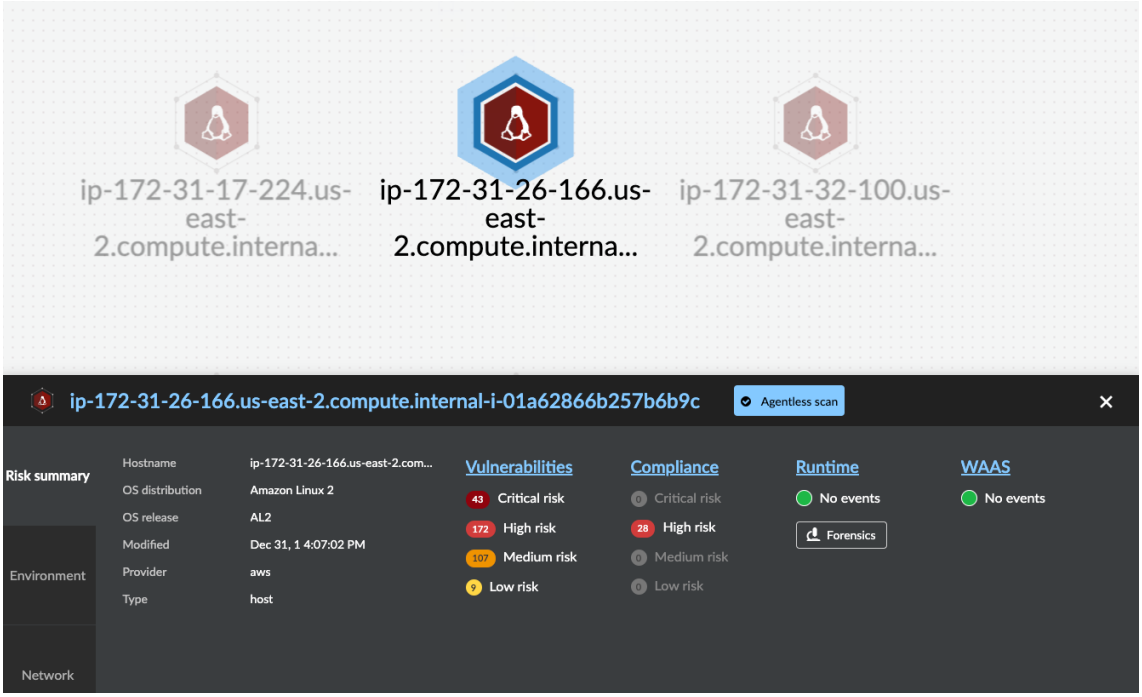

Figure 1: Host Security module

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

- **Vulnerability management**: Continuously monitor hosts for vulnerabilities, combined with powerful risk prioritization with Top 10 vulnerability lists.

- **Compliance**: Monitor and enforce prebuilt 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 malware detection, 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).
- **File integrity management (FIM)**: Continually watch the files and directories in your monitoring profile for changes.
- **Application control for hosts**: Create compliance controls that allow users to select which applications can run on their host machines and specify the allowed versions.

Container Security: Secure Kubernetes and other container platforms on any public or private cloud.

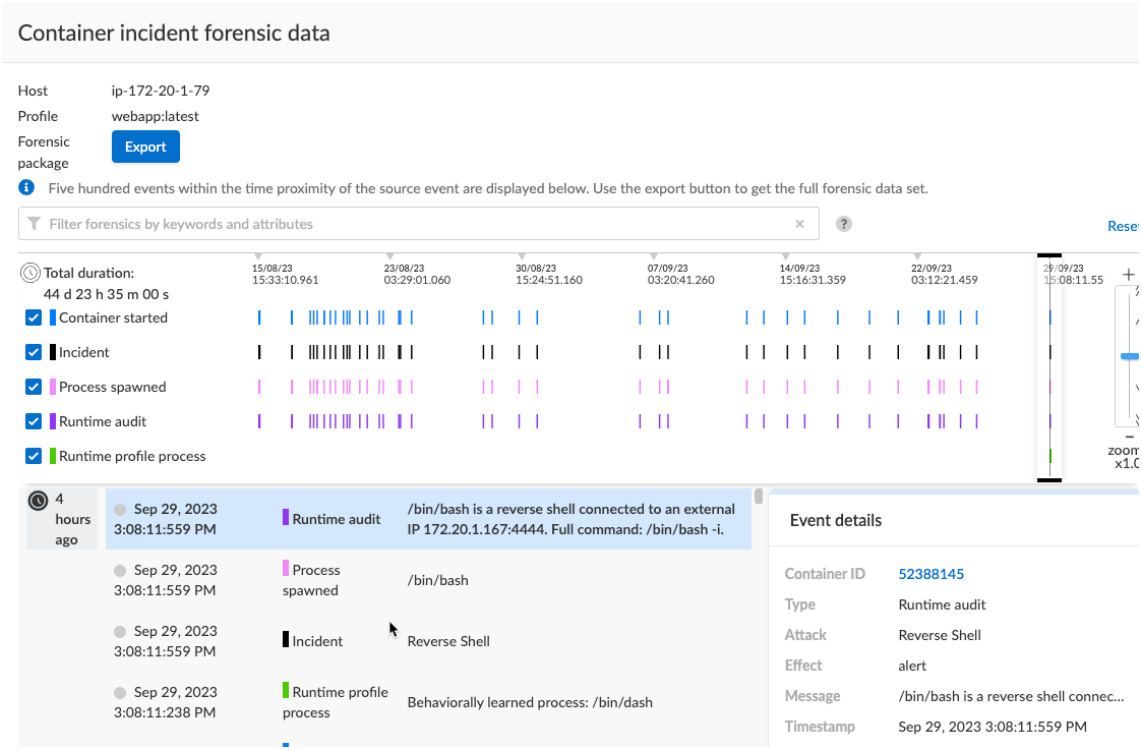

Figure 2: Container Security module

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

- **Vulnerability management**: View accurate insights into container vulnerabilities for images and metadata. Vulnerability Top 10 lists provide risk prioritization across all known CVEs and are supported with remediation guidance, per-layer image analysis, and granular tagging.
- **Compliance checks**: Leverage over 400 compliance checks, including CIS Benchmarks for Docker, Kubernetes, Linux, Windows configurations, and Istio. Prebuilt, 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 and surface incidents caused by suspicious activity.

- **Network visibility**: View all the network communications of containers and Kubernetes in real time.
- **Image analysis sandbox**: Dynamically analyze the runtime behavior of images before running them in your development and production environments.
- **Access control**: Establish and monitor access control measures for cloud-native applications across underlying hosts, Docker, or with Open Policy Agent (OPA) for OpenShift and Kubernetes. Integrate with identity and access management (IAM), secrets management tools, and other core technologies.
- **CI/CD security**: Integrate security as part of CI/CD workflows. Scan repositories and set granular vulnerability thresholds to alert on or block vulnerable images, or alert on or enforce compliance policies and analyze image behavior during runtime before deployment.

Serverless Security: Secure serverless functions across the full application lifecycle.

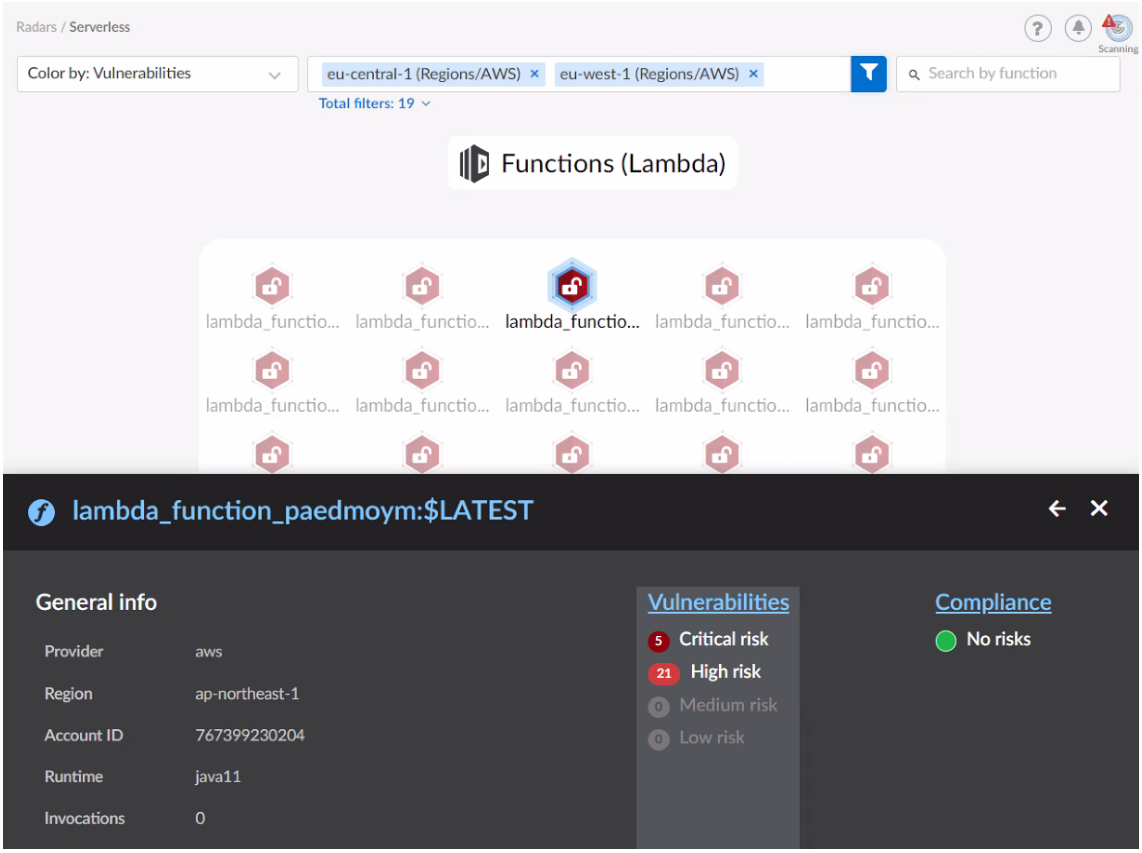

Figure 3: Serverless Security module

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 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.

Web Application and API Security: Protect against Layer 7 and OWASP Top 10 threats in any public or private cloud.

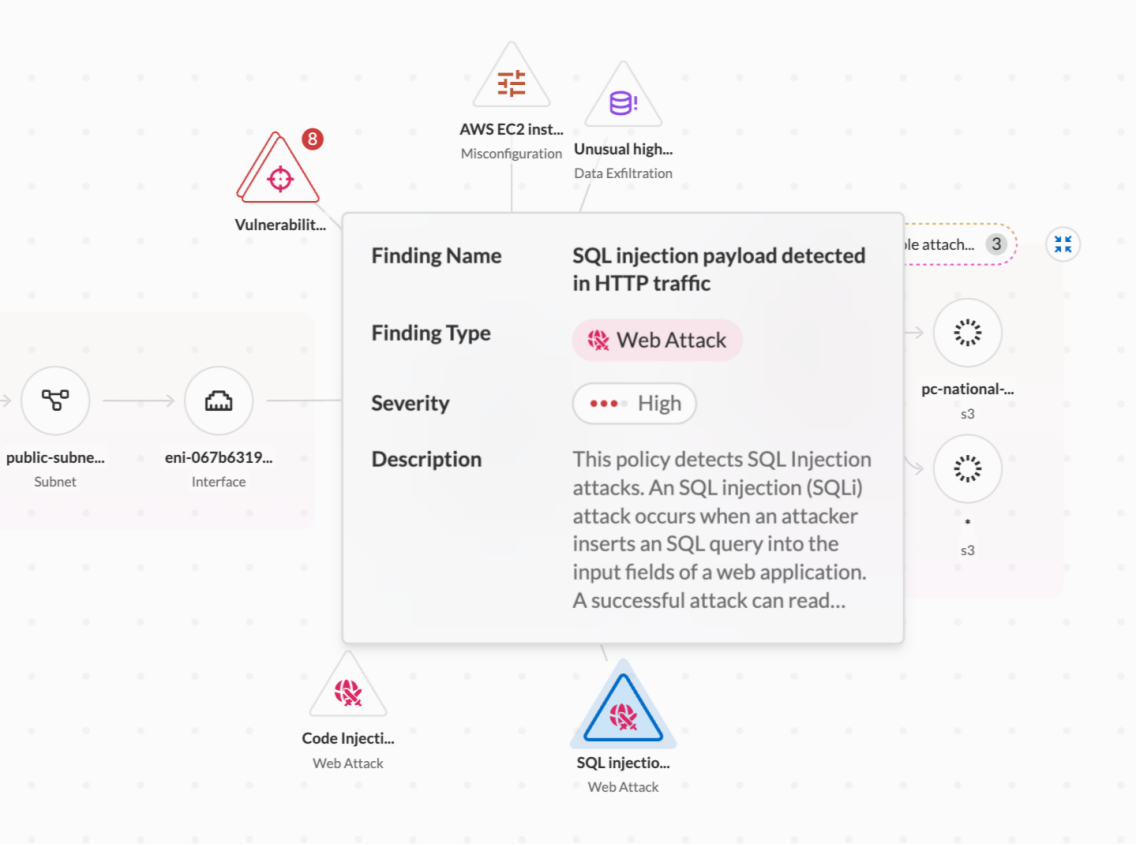

Figure 4: Web Application and API Security module

Prisma Cloud Web Application and API Security protects against Layer 7 and OWASP Top 10 threats with:

- **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.
- **API risk profiling**: Understand and prioritize risk for all APIs in your environment based on risk factors such as misconfigurations, changes, exposure to sensitive data, and access control.
- **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.
- **Bot risk management**: Protection and visibility into bad bots, known good bots, headless browsers, and other automation frameworks accessing protected web applications and APIs, including static and dynamic detections.
- **Custom rules**: An additional mechanism that gives you a precise way to describe and detect discrete conditions in requests and responses.

> **"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.**

About Prisma Cloud

Prisma® Cloud is a comprehensive cloud-native application protection platform (CNAPP) 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.

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