Prisma Cloud—Executing on NIST SP 800-190

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-190 provides guidance on securing application containers and related ecosystem components. While it thoroughly describes the security risks and associated countermeasures for protecting containerized apps, it leaves organizations to fend for themselves on the tactical front. Unfortunately, there are only a few disparate open source solutions, and traditional commercial offerings are still struggling to address the concerns unique to containers.

Prisma Cloud is purpose-built to secure cloud native workloads. From the beginning, it's been developed to address the types of risks NIST SP 800-190 describes.

Table 1: Prisma Cloud				
Image	**Registry**	**Orchestrator**	**Container**	**Host**
Prisma Cloud provides comprehensive common vulnerabilities and exposures (CVE) data for all popular base layers.	Policies can block images from being pulled from non-approved locations, forcing users to access only the registries that support encrypted transfer.	Orchestrators should use a least-privileged access model. Prisma Cloud Access Control ships with a default "deny all" access control rule for Docker® and Kubernetes® commands. Any permitted activity must be explicitly whitelisted.	Running containers are continually reassessed for vulnerabilities at a configurable interval (24 hours by default). Newly created containers are immediately assessed for vulnerabilities before instantiation.	Explicitly supports container-optimized OS, such as CoreOS and Google's Container-Optimized OS, in addition to providing runtime defense for hosts using the model-based approach to secure system services.
Prisma Cloud plugs into all phases of the container lifecycle: • CI/CD pipeline • Registry • Images and running containers on hosts • Development	Prisma Cloud continually scans, reassesses, and reports on vulnerabilities and compliance issues in images stored in registries. The scanner can be integrated into your build pipeline so that images can only be pushed to your registry after they pass a vulnerability scan and compliance assessment.	Prisma Cloud supports various deployment models for strict isolation and shared clusters. It scans the underlying host for compliance issues from the following industry-standard benchmarks: • CIS Docker Benchmark • CIS Kubernetes Benchmark • CIS General Linux Benchmark (to secure the host OS) Host runtime protection extends to our model-based approach to secure system services running on your hosts.	Runtime defense builds predictive models for each image in your environment, and then uses those models to detect abnormal activity. This offers several controls to address rogue containers: • Role-based access control (RBAC) • Pattern-matching expressions	Prisma Cloud can direct all audit events to syslog in RFC 5424-compliant format. Runtime models automatically determine where containers should write in the file system, and then enforce those rules.

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