

Prisma AIRS for Red Hat OpenShift Container Security

Securing Red Hat Clusters with Prisma AIRS Runtime Security to Implement Zero Trust for Containerized and AI Apps

Key Benefits

- Leverage your on-premises infrastructure and be agnostic to the public cloud to flexibly execute your digital transformation.
- Protect container and AI apps against malware and unknown threats and maintain consistent security across the infrastructure.
- Align with the demands of modern DevOps teams to easily deploy and manage Prisma AIRS™ network runtime security.
- Centrally manage Prisma AIRS and other Palo Alto Networks solutions with Strata® Cloud Manager or Panorama® for easier operations.

The Challenge

Navigating a cloud-native strategy and implementing a hybrid cloud infrastructure can be overwhelming. The container is a different form factor where modern apps are running. Regardless of whether apps are running on bare metal, virtual machines, or containers, they all use the same network stack and face the same foundational network threats. According to Gartner®, over 75% of AI apps will be running on containers by 2027, which will continue to drive container adoption higher.¹ If container security continues to focus on point products, the result will be an inconsistent security posture that will become a management nightmare. While shift-left security products help identify and patch known vulnerabilities at scale, apps are helpless against unknown and unpatched vulnerabilities. Additionally, without microsegmentation policies within the Kubernetes cluster, threats can easily move laterally within the cluster.

The Solution

Container apps run on the same network stack as other form-factor deployments. The network should provide consistent security for all the apps deployed anywhere and also understand container constructs such as namespaces, pods, and the fact that containers are dynamically deployed and retired. There should be visibility inside the OpenShift cluster to enable east-west threat and malware blocking between apps, pods, and namespaces within the cluster. With container-aware network security, containerized and AI apps running on containers can have the same level of security as traditional apps, and network security teams can use a familiar solution without disturbing the workflows of DevOps teams.

Red Hat OpenShift

Red Hat OpenShift is the leading hybrid cloud application platform that's trusted and comprehensive, providing a consistent experience on-premises, in the cloud, and at the edge. It's designed to meet developers, platform engineering, and IT operations teams "where they are," helping ensure a seamless journey toward application modernization, modern virtualization, and AI integration.

Red Hat OpenShift is built on a trusted container engine that delivers a scalable approach to security and reliability for critical applications. With its comprehensive set of tools and services, Red Hat OpenShift streamlines the entire lifecycle of application development—from building and deploying to running and managing. It helps simplify the complexities of application modernization efforts, including building and modernizing applications with AI across multicloud and hybrid environments—driving efficiency and productivity for developers and IT operations teams alike.

1. "Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024," Gartner, June 25, 2020.

Palo Alto Networks Prisma AIRS

Palo Alto Networks Prisma AIRS is an adaptive, purpose-built, centralized security solution that discovers, protects, and monitors every component in the container, cloud, and AI ecosystems from foundational and targeted network threats. When deployed for Kubernetes®, Prisma AIRS extends zero trust to containerized apps, helps ensure regulatory compliance, protects from known and unknown threats at both the perimeter and between segments, and confidently secures Kubernetes clusters and cloud networks in a single form factor.

Additionally, Prisma AIRS protects your AI apps by leveraging our state-of-the-art Cloud-Delivered Security Services (CDSS) to help ensure robust defense against malicious URLs to prevent data exfiltration attacks. Prisma AIRS also enables detailed segmentation of all your apps to secure every communication pathway, from port-to-port to namespace-to-namespace traffic, effectively preventing both known and zero-day application-layer attacks.

Prisma AIRS and Red Hat OpenShift

Red Hat OpenShift simplifies the complexities of application modernization efforts with AI across multicloud and hybrid environments, driving efficiency and productivity. With Prisma AIRS support for Red Hat OpenShift, organizations can use Prisma AIRS network runtime security to protect containers and AI apps running on Red Hat OpenShift clusters. Prisma AIRS protects all applications running on public or private clouds—containerized, virtualized, and AI. It provides visibility and security against unpatched and unknown threats, allowing you to enforce a consistent security posture across hybrid cloud environments. Additionally, you can enforce microsegmentation policies to help ensure threats aren't moving laterally within the multiple apps deployed on the Red Hat OpenShift clusters. NetSec and DevOps teams can continue to use the processes and tools they use today and help ensure a frictionless deployment using Helm charts and Terraform templates.

Use Case 1: Scale Network Security While Executing Digital Transformation

Challenge

A modern cloud-native application utilizes several technologies, including some open source, to enable the launch of the application to be successful. Combining, updating, and securing these technologies is a massive challenge.

Solution

Red Hat OpenShift is an application development platform built on the open-source Kubernetes project, engineered to build modernized applications for enterprise use. The OpenShift "hardened by default" posture helps ensure that clusters come with a security focus. It creates a strong foundation for teams to build the best security practices as they migrate applications to cloud native across hybrid cloud environments. Palo Alto Networks Prisma AIRS allows apps to run safely and at scale anywhere with OpenShift—by providing runtime network security for containerized apps to protect against inline threats, malware, and unpatched and unknown vulnerabilities.

Use Case 2: Protect Containerized Apps Against Unknown and AI-Related Threats

Challenge

Containerized apps face the same threats that plague traditional apps running on bare metal or virtual machines. AI apps need additional protection against AI-specific threats.

Solution

Prisma AIRS protects all applications running on public or private clouds—containerized, virtualized, and AI apps, allowing you to enforce a consistent security posture across hybrid cloud environments. In addition to enforcing microsegmentation policies, Prisma AIRS provides the same consistent application-layer (Layer 7) visibility and control inside Red Hat OpenShift container clusters. This way, you can enforce application-specific policies inside the Red Hat OpenShift cluster and help ensure threats aren't moving laterally within the OpenShift cluster. When deploying AI apps on the Red Hat OpenShift cluster, Prisma AIRS can protect against AI-specific threats at scale.

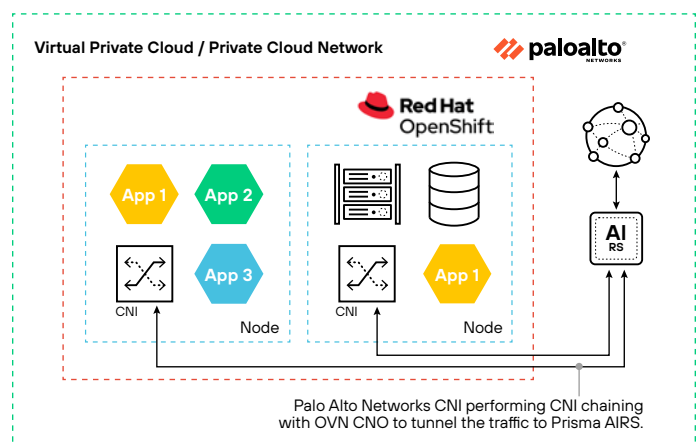


Figure 1. Enforce app-specific policies and stop lateral movement of threats for apps running on Red Hat OpenShift cluster using Prisma AIRS

Use Case 3: Centralized Management and Consistent Tooling

Challenge

When network security and DevOps teams use different tools, the result is an inconsistent security posture. Managing various products to protect different kinds of applications can be cumbersome.

Solution

Prisma AIRS can be managed with Panorama or Strata Cloud Manager like other Palo Alto Networks solutions, including physical and virtual firewalls to provide network security teams with familiar interface and capabilities through a single-pane-of-glass console. Not only that, a single AIRS product can protect container, noncontainer, AI, and non-AI apps deployed anywhere—resulting in ease of use because you don't need different products for different applications. Additionally, Prisma AIRS deployment and management easily integrate with CI/CD pipeline deployment, including deployment using the Helm charts and Terraform templates that DevOps teams are already using.

The Palo Alto Networks and Red Hat OpenShift Partnership

For more information on Prisma AIRS and the integrations between Palo Alto Networks and Red Hat OpenShift, see:

- [Palo Alto Networks Prisma AIRS](#)
- [Prisma AIRS datasheet](#)
- [Prisma Cloud integrated with Red Hat OpenShift](#)
- [VM-Series Firewall on OpenShift virtualization](#)
- [NGFW PAN-OS Ansible Automation Platform collection](#)

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions and services, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT, and automate, secure, and manage complex environments. For more information, visit www.redhat.com.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.



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

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

parent_pb_airs-for-redhat-openshift_051225