Safeguard essential workloads

3 use cases combining CrowdStrike and Red Hat Advanced Cluster Security

Following the massive adoption of cloud-native technologies and DevOps practices, Kubernetes has become the de facto standard for container orchestration. However, with its widespread adoption comes the imperative need to make sure comprehensive security policies are in place to safeguard the infrastructure, applications, and data it hosts. According to the State of Kubernetes security report, 2 out of 3 organizations experience delayed deployments due to Kubernetes security concerns.[1]

Organizations can strengthen their security posture by combining Red Hat® Advanced Cluster Security for Kubernetes and CrowdStrike Falcon®. Here are 3 use cases where this joint solution can help advance safeguarding measures.

1 Misconfiguration and malware detection in containers

Prioritize risk and enforce "no-go" policies.

As more applications move to containers, DevOps teams must standardize on best practices and implement guardrails for both container images and Kubernetes deployment configurations.

Red Hat Advanced Cluster Security allows these teams to configure policies and check them during continuous integration/continuous delivery (CI/CD) pipelines, at deploy time, and at runtime to make sure there is application consistency and stability. Developers also gain visibility into deployed applications, vulnerabilities, and other sources of risk so they can prioritize the most critical configuration problems.

Even when following best practices, sophisticated attackers can exploit small misconfigurations and zero-day vulnerabilities to breach container applications. The CrowdStrike Falcon sensor's machine learning models are trained on the most current global attack tactics, to detect and prevent malicious behavior inside containers before they lead to a breach.

Security teams can use the CrowdStrike admission controller to enforce "no-go" policies for risky Kubernetes deployment configurations, further reducing an adversary's potential attack surface.

2 Centralized container and virtual machine security

Save time on tickets and support, to gain more time for enterprise security.

Red Hat OpenShift® offers powerful capabilities for teams to manage containers and virtual machines (VMs) in a unified environment with Red Hat OpenShift Virtualization.

While Red Hat Advanced Cluster Security excels at adding a security focus to containers with built-in capabilities, organizations can further strengthen their overall security posture by using CrowdStrike for advanced endpoint security for unprotected VMs. CrowdStrike provides coverage for Red Hat OpenShift's underlying operating system, as well as hosted guest machines.

Additionally, a CrowdStrike extension to the Red Hat OpenShift Console web interface puts CrowdStrike security data right in the hands of the engineers who manage those VMs.

This way, engineers and security analysts spend less time answering tickets and chat messages and more time collaborating on enterprise security.

1 Red Hat overview. "Kubernetes adoption, security, and market trends report 2024." 20 June 2024.

3 Cloud-native security operations center

Aggregate tools to offer a single stream for search and alerting.

Modern security operations centers are moving beyond basic endpoint and network alerting and into cloud-native telemetry.

Logs and alerts from Red Hat OpenShift and Red Hat Advanced Cluster Security represent an important piece of an organization's application security landscape and can be ingested into CrowdStrike Falcon Next-Gen SIEM.

Next-Gen SIEM aggregates security telemetry from dozens of tools to provide security analysts a single stream for search and alerting. Giving DevOps teams access to the same aggregated telemetry can accelerate incident response—whether due to a security finding or an operational issue.

Learn more

The CrowdStrike Falcon operator is certified for Red Hat OpenShift and supports self-managed Red Hat OpenShift Service on AWS, Microsoft Azure Red Hat OpenShift, and other Kubernetes distributions. Additional resources can be found in the Red Hat Ecosystem Catalog or on the CrowdStrike website.