CrowdStrike Cloud Security Extends to New Red Hat Enterprise Linux Versions

May 19, 2022

Brett Shaw Endpoint & Cloud Security

As organizations increasingly move to hybrid cloud environments to increase agility, scale and competitive advantage, adversaries are correspondingly looking to exploit these environments. According to the CrowdStrike 2022 Global Threat Report, cloud-based services are "increasingly abused by malicious actors in the course of computer network operations (CNO), a trend that is likely to continue in the foreseeable future as more businesses seek hybrid work environments."

Having unified security and visibility across hybrid cloud environments is critical for DevSecOps to be efficient and ultimately protect the organization.

CrowdStrike continues to innovate and provide customers with the protection they need across hybrid environments. We are pleased to announce our support of Red Hat Enterprise Linux 9 through CrowdStrike Falcon Cloud Workload Protection (CWP), providing comprehensive breach protection for workloads and containers. This empowers customers to build, run and bolster cloud-native applications with deeper security capabilities, speed and confidence.

Red Hat recently announced the release of Red Hat Enterprise Linux 9, which provides a flexible and stable foundation to support hybrid cloud innovation. Red Hat Enterprise Linux 9 is designed to meet the needs of distributed IT workloads inside and outside of the data center, providing a consistent, reliable foundation for modern computing in hybrid cloud environments, from the data center to public clouds and out to the enterprise edge. Optimized for both cloud innovation and production stability, Red Hat Enterprise Linux 9 enables organizations to deploy applications and critical workloads faster with a more streamlined experience across physical, virtual, private and public cloud, and edge deployments.

By running Falcon CWP to protect Red Hat Enterprise Linux 9, you can:

1. Gain complete visibility across your entire cloud estate in a single platform. Organizations receive complete visibility into workload and container events and instance metadata, enabling faster and more accurate detection, response, threat hunting and investigation so that nothing goes unseen in your cloud environment.
2. Prevent attacks and avoid business disruption. Organizations can protect their cloud-native stack on any cloud and across all workloads, containers and Kubernetes applications. Automate security and detect and stop suspicious activity, zero-day attacks and risky behavior to stay ahead of threats and reduce the attack surface.
3. Eliminate friction and build in the cloud with confidence. Key integrations support continuous integration/continuous delivery (CI/CD) workflows, allowing organizations to protect workloads at the speed of DevOps without sacrificing performance.

As a member of Red Hat's partner ecosystem, CrowdStrike delivers cloud security technologies and expertise that are tested and validated to work on Red Hat Enterprise Linux 9, offering organizations a solution that is equipped to run with consistency and stability across the full scope of hybrid cloud environments.

"Red Hat Enterprise Linux 9 pairs innovation with stability as the backbone for enterprise workloads from the datacenter to the edge," said Gunnar Hellekson, vice president and general manager, Red Hat Enterprise Linux Business Unit, Red Hat. "Backed by a robust partner ecosystem built on open source principles, Red Hat Enterprise Linux 9 is truly a platform designed for hybrid cloud innovation. By collaborating with partners like CrowdStrike to develop and certify solutions on the basis of Red Hat Enterprise Linux, we are able to support customers at every stage of their cloud journey."

In addition to the Red Hat Enterprise Linux 9 support, today CrowdStrike supports the following Openshift implementations:

- Red Hat OpenShift
- Azure Red Hat OpenShift (ARO)
- Red Hat OpenShift Service on AWS (ROSA)
- OpenShift on IBM Cloud
- OpenShift Dedicated 4

As organizations are looking to adopt newer Red Hat Enterprise Linux versions, having protection across the different operating systems without impacting application development is critical. Falcon CWP, with its machine learning, artificial intelligence, indicators of attack, deep kernel visibility, custom indicators of compromise and behavioral blocking, helps protect workloads across public and hybrid cloud environments from Day One.

This expansive support helps organizations gain visibility into their entire cloud and Red Hat infrastructure, continuously monitor for misconfigurations, provide security policy and compliance enforcement, and proactively detect and prevent threats, enabling DevSecOps teams to “shift left” and fix issues before they reach production, saving valuable time and money.

Try and buy CrowdStrike Cloud Security products in the Red Hat Marketplace.

Additional Resources

- Learn more on the Falcon for Red Hat webpage.
- Visit the CrowdStrike webpage in the Red Hat Marketplace.
- Visit the Falcon Cloud Workload Protection webpage and download the solution brief.
- Watch the webinar “Proactive Threat Hunting in Red Hat Environments with CrowdStrike.”
- Learn more about CrowdStrike Cloud Security products.