CrowdStrike Technology Partner

Red Hat

CROWDSTRIKE

Solution Brief

CrowdStrike and Red Hat

Consolidating hybrid cloud management and security

Challenges

As organizations expand their cloud-native initiatives and increase their use of containers, Kubernetes and cloud services in production, they face challenges in consistently monitoring, securing and enforcing compliance. Not only do modern workloads require new security tooling, the traditional tools that worked in the data center don't scale to the footprint of public cloud providers.

To address these challenges and lay a secure foundation for modern workloads, operations teams need solutions that seamlessly protect workloads on-premises and in the cloud, monitor containers and Kubernetes, and can holistically assess the risk of the cloud estate.

Solution

Together, CrowdStrike and Red Hat drive positive security outcomes for customers by facilitating endpoint and cloud protection, cloud adoption and scalability through seamless integrations, streamlined workflows and real-time security posture and response. This helps organizations protect, detect and investigate attacks that span multiple environments and different types of workloads, pivoting from endpoint to compute instances to containers from build to runtime.

The CrowdStrike Falcon® platform provides proven endpoint security through a cloud-delivered platform via a single lightweight agent for Red Hat Enterprise Linux, an enterprise Linux operating system that provides a consistent foundation across environments and the tools needed to deliver services and workloads faster for any application. Red Hat Enterprise Linux reduces deployment friction and costs while speeding time-to-value for critical workloads, enabling development and operations teams to innovate together in any environment.

CrowdStrike also offers complete cloud-native security and compliance for applications on Red Hat OpenShift Container Platform. Red Hat OpenShift is a consistent hybrid cloud foundation for building and scaling containerized applications, allowing developers to build and deliver better applications faster. The Falcon platform can scan throughout the entire development lifecycle, whether during a pre-runtime image assessment and scan for vulnerabilities, CIS misconfigurations and malware; or at runtime to scan containers and Kubernetes clusters for active attacks.

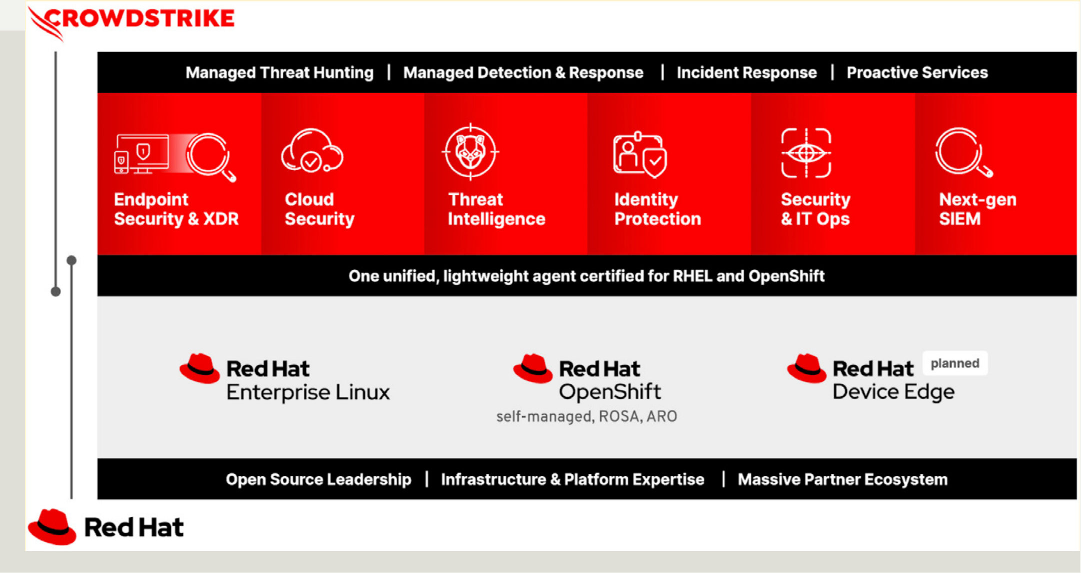
Key benefits

Protection for the hybrid cloud with certified offerings for RHEL, OpenShift (self-managed, ROSA, ARO) and Ansible, as well as EKS, AKS and other public cloud resources

Seamless integration with a large ecosystem of security and IT operations partners — including overlap with Red Hat's partners

Cloud-native platform with a single lightweight agent that delivers immediate time-to-value and reduced complexity

Finally, CrowdStrike Falcon® Cloud Security provides cloud security posture management (CSPM) to detect security and compliance misconfigurations of cloud resources including storage buckets, identity accounts and firewall security groups. Together with endpoint protection on RHEL and workload protection on OpenShift, Falcon Cloud Security ensures production workloads in the cloud are secure, however they're deployed.



CROWDSTRIKE

Managed Threat Hunting | Managed Detection & Response | Incident Response | Proactive Services

Endpoint Security & XDR

Cloud Security

Threat Intelligence

Identity Protection

Security & IT Ops

Next-gen SIEM

One unified, lightweight agent certified for RHEL and OpenShift

Red Hat Enterprise Linux

Red Hat OpenShift
self-managed, ROSA, ARO

Red Hat Device Edge planned

Open Source Leadership | Infrastructure & Platform Expertise | Massive Partner Ecosystem

Red Hat

Business value

Use Case/Challenge	Solution
Complicated security stack on RHEL slows down operations	Legacy security stacks with many disparate tools can slow the growth, adoption and upgradeability of RHEL. With one Falcon agent certified for RHEL 6.7 to 9.0, organizations gain access to an endpoint detection and response solution that offers machine-learning-powered incident prevention, remote response, attack context and more in a single platform.
Traditional security tools are not compatible with OpenShift	Host-based security tools that work for RHEL may be incompatible with OpenShift's cloud-native architecture. The Falcon agent is certified for OpenShift (self-managed, ROSA and ARO) and provides advanced breach prevention for container workloads running on OpenShift, and for OpenShift itself.
Security and compliance challenges in the public cloud are increasing	Many organizations struggle to understand and secure cloud resources. The Falcon platform detects security and compliance misconfigurations in AWS and Azure environments (e.g., S3, IAM, security groups), giving organizations confidence when deploying production workloads to the public cloud.

Key capabilities

Protection for RHEL and OpenShift

- Proactively detect and prevent malicious behavior using machine learning trained on CrowdStrike's leading threat intelligence.
- Deep visibility into processes, containers, files and vulnerabilities provides protection for both RHEL and CoreOS operating systems, as well as workloads running inside containers.
- The lightweight Falcon agent has minimal impact on system performance and is ideal for physical, virtual, on-premises and cloud-hosted environments.

Security automation with Ansible

- Simplify agent deployment on Linux, Windows and Mac systems with a certified collection for Ansible Automation Platform.
- Respond to Falcon detections automatically with Event-Driven Ansible to orchestrate enrichment, mitigation and restoration.
- Dynamically target both managed and unmanaged hosts through an inventory plugin.

Comprehensive security in a unified platform

- Keep cloud accounts free of risky misconfigurations with Falcon Cloud Security's cloud security posture management.
- Collect, search and alert on log events from anywhere with a next-gen security information and event management (SIEM) solution.
- Understand and respond to risky behavior in domain accounts before they cause a breach.

Integration details

CrowdStrike supports the following OpenShift implementations:

- Red Hat OpenShift Container Platform (self-managed)
- Azure Red Hat OpenShift (ARO)
- Red Hat OpenShift Service on AWS (ROSA)
- OpenShift on IBM Cloud

CrowdStrike and Red Hat product integrations:

- Certified CrowdStrike Falcon Sensor for RHEL 6 to 9
- Certified CrowdStrike Falcon Operator for Kubernetes-native installation on OpenShift
- Certified CrowdStrike Ansible Collection for easy sensor deployment on RHEL, Windows and other operating systems

Product Certifications

Red Hat Enterprise Linux

Red Hat OpenShift

Red Hat Ansible Automation Platform

CrowdStrike products available in the Red Hat Marketplace:

- CrowdStrike Falcon Cloud Security
- CrowdStrike Falcon® Insight XDR extended detection and response
- CrowdStrike Falcon platform

Red Hat is a trusted **CrowdStrike Cloud Partner**, providing integrated solutions with CrowdStrike to deliver comprehensive cloud workload protection.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity, and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**