CrowdStrike Technology Partners

SUSE RANCHER

CROWDSTRIKE

Solution Brief

SUSE RANCHER AND CROWDSTRIKE FALCON

Gain greater control, speed and security when building and running applications in the cloud with Kubernetes

CHALLENGES

DevOps and security teams must ensure containers and microservices remain secure and compliant while minimizing security risks to protect their organization. Overwhelming complexity with containers managed by multiple Kubernetes clusters can cause teams to grapple with operational and security challenges given the lack of visibility and increased complexity involved. With poor visibility, fragmented and complex tools, misconfigurations for cloud workloads, and the inability to maintain compliance, the risk of a breach is elevated. DevOps and security teams need tools that address the operational and security challenges of managing multiple Kubernetes clusters across any infrastructure and provide integrated tools for running containerized workloads seamlessly.

SOLUTION

With SUSE Rancher and CrowdStrike, organizations gain layered security for their Kubernetes clusters to ensure confidence when building and running applications in the cloud. SUSE Rancher not only deploys production-grade Kubernetes clusters from datacenter to cloud to the edge, it also unites them with centralized authentication, access control and observability. To further empower your team, CrowdStrike Falcon® Cloud Workload Protection (CWP) provides comprehensive breach protection for workloads and containers by focusing on staying ahead of adversaries, reducing the attack surface and obtaining total real-time visibility of events taking place in the environment. CWP automatically protects the Kubernetes Control Plane and Worker nodes, allowing DevSecOps teams to securely build applications in the cloud with confidence. CrowdStrike Helm Chart, offered in the Rancher Apps and Marketplace, allows you to deploy and manage applications across cloud environments, ensuring multi-cluster consistency with a single deployment. By layering SUSE Rancher and CrowdStrike together, DevSecOps teams can seamlessly save time and effort with improved defense against data breaches and optimized cloud deployments.

KEY BENEFITS

Unified Multi-cluster Management: SUSE Rancher unites Kubernetes clusters with centralized authentication and access control, provisioning, version management, visibility and diagnostics, monitoring, alerting and centralized audit.

Hybrid and Multi-cloud Support: Manage on-premises clusters and those hosted on cloud services like AKS, EKS and GKE from a single pane of glass, without impacting performance.

Broad Support for Container Runtime Security: Secures applications with the new CrowdStrike Falcon Container sensor that is uniquely designed to run as an unprivileged container in a pod.

SUSE RANCHER

BUSINESS VALUE

Use Case/Challenge	Solution	Benefits
Diverse Kubernetes Cluster Management (Manage any CNCF-certified Kubernetes distribution)	SUSE Rancher manages all your Kubernetes clusters no matter where you've deployed them.	• Simple, consistent cluster operations • Centralized visibility and diagnostics • Manage across diverse infrastructure with ease
Global Policy and User Management	SUSE Rancher lets you automate processes and applies a consistent set of user access and security policies for all your clusters, no matter where they're running.	• Streamlined, consistent policy deployment and enforcement • User access and rights are easily modified and customized
Breach Prevention for Cloud Workloads and Containers	CrowdStrike Falcon Cloud Workload Protection provides comprehensive breach protection for workloads and containers, enabling you to build, run and secure applications with speed and confidence.	• Gain complete visibility across your entire cloud estate in a single platform • Prevent attacks and avoid business disruption

"After a quarter of a century of technical evolution, we're embarking on one of the most important transformations in our history. By modernizing all our legacy systems to create a cluster of cloud-native microservices, we are becoming more agile and innovative."

Anthony Andrades,
Head of Global Infrastructure Strategy, Schneider Digital, Schneider Electric

TECHNICAL SOLUTION

STREAMLINED DAY 2 KUBERNETES OPERATIONS

Once you've provisioned a Kubernetes cluster with SUSE Rancher, operations are centralized and administrators can deal with all aspects of Day 2 operations. From one console, administrators can monitor any cluster in any location, upgrade Kubernetes versions, and backup and recover degraded clusters. CrowdStrike Helm Chart is available in the Rancher Apps and Marketplace and can easily deploy the kernel sensor to your nodes for runtime control and visibility of your Kubernetes clusters.

FULL LIFECYCLE MANAGEMENT FOR HOSTED KUBERNETES CLUSTERS

Give operators full lifecycle management of the most popular cloud-hosted distributions, including node management and autoscaling, from a single pane of glass. Import, provision, upgrade, and configure and secure clusters on Amazon EKS directly using the new unified and intuitive SUSE Rancher user experience. SUSE Rancher managed Amazon EKS deployments support CIS templating and scanning to minimize configuration drift between clusters. Additionally, with CrowdStrike Falcon Horizon™ cloud security posture management (CSPM) you can scale at will and gain insight into all control plane API calls and uncover security risks within managed Kubernetes clusters. Assess the security of cloud accounts against Kubernetes CIS benchmarks with 250 out-of-the-box, adversary-focused policies saving time and reducing operational costs.

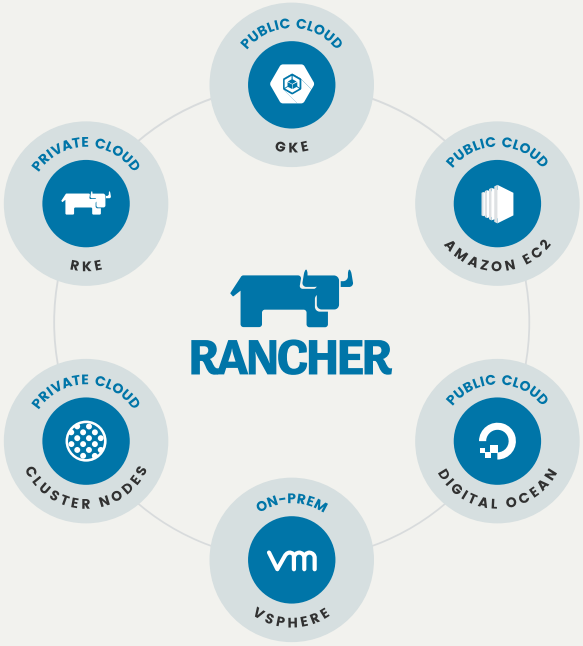
CENTRALIZED KUBERNETES AUTHENTICATION AND AUTHORIZATION

SUSE Rancher admins can work with their security team to centrally define how users should interact with managed Kubernetes clusters and how containerized workloads should operate. Once policies have been defined, assigning them to any Kubernetes cluster is instantaneous.

SUSE RANCHER

GITOPS AT SCALE FOR EDGE CLUSTERS

SUSE Rancher Continuous Delivery allows for maximum cluster consistency from core to cloud to edge. SUSE Rancher supports from 1 to 1,000,000 clusters from a single console with built-in security capabilities, running any CNCF-certified Kubernetes distribution. By streamlining application delivery across any infrastructure in any location, enterprises can use SUSE Rancher to accelerate their journey towards true digital transformation.



ABOUT SUSE

SUSE is a global leader in innovative, reliable and enterprise-grade open source solutions, relied upon by more than 60% of the Fortune 500 to power their mission-critical workloads. We specialize in Enterprise Linux, Kubernetes Management, and Edge solutions, and collaborate with partners and communities to empower our customers to innovate everywhere—from the data center, to the cloud, to the edge and beyond. SUSE puts the "open" back in open source, giving customers the agility to tackle innovation challenges today and the freedom to evolve their strategy and solutions tomorrow. The company is headquartered in Nuremberg, Germany, and employs nearly 2000 people globally. SUSE is listed in the Prime Standard of the Frankfurt Stock Exchange.

KEY CAPABILITIES

- Simplifies multi-cluster operations
- Unifies security, policy and user management
- Drives adoption with shared tools and services
- Improves visibility across the enterprise
- Delivers effective runtime protection

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**