Operationalize Kubernetes security in AWS with Red Hat

Evolving security maturity models in cloud-native environments

The rapid growth of cloud technologies, particularly Kubernetes, demands clear and adaptable security models. Organizations are starting to turn to structured security maturity frameworks to offer robust protection in cloud-native environments.

Frameworks such as the AWS Security Maturity Model v2, National Institute of Standards and Technology (NIST) Cybersecurity Framework, NIST Special Publication 800-190, and the Cybersecurity Maturity Model Certification (CMMC) are at the forefront of this evolution. These frameworks guide enterprises through systematic, incremental enhancements of their security posture, providing clear benchmarks and maturity phases.

In this document we will show how to use **Red Hat® Advanced Cluster Security for Kubernetes to implement AWS Security Maturity Model v2** to enhance your Kubernetes Security Posture Management (KSPM).

The AWS Security Maturity Model v2 categorizes security practices into 4 distinct maturity phases:

- **Quick wins.**
- **Foundational.**
- **Efficient.**
- **Optimized.**

This allows structured progression toward advanced threat detection, automation, and continuous security improvements and guardrails.

Rise in Kubernetes adoption and associated security complexities

Kubernetes has rapidly become the industry standard for container orchestration due to its scalability, flexibility, and ability to streamline complex deployments. Enterprises use Kubernetes extensively, spanning cloud-native applications across public clouds, hybrid infrastructures, and on-premise environments.

This widespread adoption brings new security challenges. Kubernetes' dynamic infrastructure, characterized by rapidly changing workloads and continuous deployments, poses challenges for traditional security methods. The ephemeral nature of containers and the frequent interactions between multiple distributed components create an environment where security visibility, effective monitoring, and rapid incident response become exceedingly intricate.

Key challenges in operationalizing security maturity frameworks

While security maturity frameworks provide invaluable guidance, operationalizing them effectively within Kubernetes and cloud-native environments has challenges. A prominent issue is the gap in Kubernetes-specific security expertise among many security teams.

Kubernetes and cloud-native tools require specialized skills and knowledge distinct from traditional IT security frameworks. Moreover, organizations often face difficulties in integrating these maturity frameworks into existing security and compliance infrastructures, leading to fragmented visibility and inconsistent policy enforcement. Operationalizing frameworks such as AWS Security Maturity Model v2 and CMMC demands rigorous configuration management, continuous risk assessment, and automated incident responses—capabilities that many enterprises struggle to achieve without significant investments in dedicated tools and training.

Importance of Kubernetes security posture management

Kubernetes Security Posture Management (KSPM) has emerged as a critical element in safeguarding modern container environments.

KSPM involves continuous monitoring and management of security policies, compliance standards, and threat detection across Kubernetes clusters. Its importance lies in its comprehensive approach, covering everything from basic infrastructure security and vulnerability management to advanced threat detection and automated incident response.

Effective KSPM not only helps organizations maintain compliance with regulatory standards such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI-DSS), but also reduces operational risks by identifying and mitigating vulnerabilities earlier in the development cycle. The proactive nature of KSPM makes sure issues are resolved before they affect production environments, thereby reducing overall risk and operational costs.

Implementing KSPM with Red Hat

Introduction to Red Hat Advanced Cluster Security for Kubernetes and Advanced Container Security Cloud Service

Red Hat Advanced Cluster Security provides organizations with solutions to enhance the security posture of their Kubernetes environments comprehensively and consistently.

It integrates with Red Hat OpenShift®, a trusted and comprehensive Kubernetes application platform, and other Kubernetes solutions—such as Amazon Elastic Kubernetes Service or Azure Elastic Kubernetes Service—to deliver security-focused solutions across cloud and hybrid infrastructures.

Red Hat Advanced Container Security capabilities include proactive risk management, continuous runtime security monitoring, vulnerability and supply chain management, extensible security policies for all phases of the container lifecycle, network observability and policy generation, DevSecOps integration, and developer tools and extensive compliance management. Together, these capabilities help organizations to mitigate threats and vulnerabilities.

Organizations can choose between multiple deployment models for Red Hat Advanced Cluster Security:

- Self-managed Red Hat OpenShift for maximum customization and control.
- Red Hat Advanced Cluster Security Cloud Service for a fully managed experience, reducing operational overhead and management complexity.

- Red Hat OpenShift Service on AWS with Red Hat Advanced Cluster Security, which provides a fully integrated Red Hat OpenShift environment within Amazon Web Services (AWS) that has streamlined Kubernetes security options and simplified management aligned with AWS best practices.

Below we will provide suggested steps to operationalize AWS Security Maturity Model v2 using Red Hat Advanced Cluster Security.

Suggested guidance for a security-focused Kubernetes environment using Red Hat Advanced Cluster Security to meet AWS Security Maturity Model v2

Security governance

Establishing governance is a foundational step in improving Kubernetes security. Red Hat Advanced Cluster Security helps teams implement clear security responsibilities, enforce role-based access controls (RBACs), and maintain region-aware deployments aligned with organizational policies. Over time, governance evolves from basic access and region controls into architecture-level decisions and cross-team accountability models that support continuous improvement and self-service and autonomous governance.

- **Phase 1: Quick wins.** Organizations should begin by assigning security contacts and defining users, roles, and groups within Red Hat Advanced Cluster Security. This creates consistent access controls aligned with DevSecOps needs. Selecting the right regions for deployment and blocking unused regions—through IAM policies or network rules—makes sure that Red Hat Advanced Cluster Security access and operations align with compliance and latency requirements.

- **Phase 2: Foundational.** At this phase, organizations assess applicable security and regulatory standards (such as PCI and HIPAA) and use Red Hat Advanced Cluster Security compliance features to track security posture across node, platform, and workload layers. Creating a DevSecOps strategy and process that integrates Red Hat Advanced Cluster Security and creating a security training plan tailored to the deployment model (self-managed or Advanced Cluster Security Cloud Service) helps administrators and team members understand platform-specific responsibilities and how to use Red Hat Advanced Cluster Security to perform them.

- **Phase 3: Efficient.** Security governance matures into architecture design. Red Hat Advanced Cluster Security architecture supports both connected and disconnected environments, and teams can automate configuration through Infrastructure as Code (IaC) and GitOps and Policy as Code (PaC) practices. Metadata tagging within containers and pods allows for policy enforcement and helps group and manage vulnerabilities by logical attributes.

- **Phase 4: Optimized.** In this phase, organizations formalize roles and responsibilities using a responsible, accountable, consulted, and informed (RACI) model within Red Hat Advanced Cluster Security. RBACs can be applied to distribute vulnerabilities and responsibilities across node, platform, and application teams. This supports more efficient remediation, better collaboration, and reduced security fatigue through targeted and relevant alerts. RBAC will also make sure there is control over the DevSecOps process and onboarding of new applications and services.

Security assurance

Security assurance focuses on visibility, accountability, and continuous posture improvement. Red Hat Advanced Cluster Security helps organizations assess, monitor, and improve Kubernetes security across node, platform, and workload layers. By progressively implementing these practices in alignment with the AWS Security Maturity Model v2, teams can build toward consistent compliance readiness and operational resilience.

- **Phase 1: Quick wins**. Organizations can begin by evaluating KSPM using Red Hat Advanced Cluster Security built-in risk and compliance frameworks. Whether using risk-based prioritization or aligning with standards such as Payment Card Industry (PCI) or NIST, or frameworks like Center for Internet Security (CIS) Benchmarks for Kubernetes or internal security policies, Red Hat Advanced Cluster Security supports an early understanding of security posture across environments. This provides an initial baseline for addressing misconfigurations and vulnerabilities.
- **Phase 2: Foundational.** Once an initial assessment is in place, teams can use the Configuration Management dashboard within Red Hat Advanced Cluster Security to inventory their Kubernetes environments. This helps identify configuration exposure and security risks tied to nodes, clusters, and workloads, forming the foundation for a structured response to posture gaps. Mitigations to address deviations are supplied.
- **Phase 3: Efficient.** As organizations mature, they can create and customize compliance reports using the built-in standards available in Red Hat Advanced Cluster Security. These reports help track progress over time and support both internal and external audits. Continuous monitoring through the dashboard makes sure that posture improvements are sustained and measurable.
- **Phase 4: Optimized**. In this stage, organizations can automate evidence gathering to support streamlined audit and compliance workflows. Reports can be exported directly from Red Hat Advanced Cluster Security as CSV files or accessed via the user interface (UI), allowing for efficient documentation across audits and security reviews. Posture assessments are maintained continuously across node, platform, and workload layers, helping teams remain ready for evolving compliance needs.

Identity and access management

Effective identity and access management helps organizations maintain control over who can access systems and what actions they can perform. Red Hat Advanced Cluster Security provides native support for RBACs and integration with enterprise identity systems, helping organizations to apply consistent identity practices across environments. By aligning access strategies with the AWS Security Maturity Model v2, teams can reduce exposure, enforce least privilege, and support auditability at every phase.

- **Phase 1: Quick wins.** To begin, organizations should configure Red Hat Advanced Cluster Security to federate with their existing identity provider and allow multifactor authentication (MFA) for additional protection. Following deployment, the root or admin account should be restricted from daily use, with RBACs applied to enforce least privilege. Teams should also audit existing access and remove unintended roles or group assignments, making sure that only approved identities can interact with the platform.
- **Phase 2: Foundational.** Next, organizations should shift from long-lived credentials to short-lived tokens wherever possible. This includes all tokens used for integrations and service-to-service communications within Red Hat Advanced Cluster Security, helping limit risk associated with credential exposure or reuse.

- **Phase 3: Efficient.** With MFA and token policies in place, organizations can refine access further by reviewing and updating the platform's default roles. These roles can be tailored for fine-grained access control to match job functions, limiting users to only the permissions they need—read, write, or execute. New roles can also be created to reflect custom responsibilities, supporting broader least privilege enforcement.
- **Phase 4: Optimized.** At this stage, organizations can implement formal workflows for temporary elevated access and dual control. Red Hat Advanced Cluster Security supports time-bound and monitored access escalation, allowing security practitioners to request and receive additional permissions for specific tasks. These workflows reduce persistent privilege while maintaining operational flexibility and audit visibility.

Threat detection

Timely detection and response are essential for reducing the effects of security events in containerized environments. Red Hat Advanced Cluster Security allows organizations to monitor runtime behavior, detect anomalies, and integrate with external systems for centralized alerting and analysis. By mapping threat detection practices to each phase of the AWS Security Maturity Model v2, teams can grow from basic visibility to advanced, proactive defense.

- **Phase 1: Quick wins.** Organizations can begin by initiating logging and configuring built-in policy alerts in Red Hat Advanced Cluster Security to detect common threats. Behavioral analysis can be applied to runtime activity, including processes and network traffic, while logs are forwarded to a security information and event management (SIEM) platform, or a security data lake, such as Amazon Security Lake (SecLake) for centralized visibility. In parallel, API audit logs should be configured at both the Kubernetes level and within Red Hat Advanced Cluster Security, then directed to a centralized logging tool such as AWS-native services, AWS Cloud Trail, or a third-party SIEM.
- **Phase 2: Foundational.** With basic monitoring in place, teams can expand their detection capabilities. Integrating Red Hat Advanced Cluster Security with a SIEM allows organizations to correlate runtime activity with known threat patterns and respond more effectively to advanced or persistent risks.
- **Phase 3: Efficient.** Mature organizations can build custom threat detection rules using either Red Hat Advanced Cluster Security default policy sets or tailored configurations specific to their workloads. These rules can include custom network segmentation, pod-level anomaly detection, or process behavior baselining. Detected events and enriched telemetry can be forwarded to SIEM, Security Orchestration, Automation, and Response (SOAR), or SecLake platforms to support further analysis and automation.
- **Phase 4: Optimized.** At this phase, teams gain deeper insight into cluster behavior by turning on advanced networking observability. Red Hat Advanced Cluster Security supports pod-to-pod and VPC Flow Log analysis and port-scanning features that reveal communication paths between pods and external entities. This helps security teams identify suspicious flows and detect threats that may bypass traditional monitoring systems, and develop network policies to segment and restrict network traffic.

Vulnerability management

Managing known vulnerabilities across containers, applications, and infrastructure is a critical aspect of Kubernetes security posture. Red Hat Advanced Cluster Security helps organizations identify, prioritize, and respond to vulnerabilities through continuous analysis and policy-based enforcement. By aligning vulnerability management efforts with the AWS Security Maturity Model v2, organizations can move from basic triage to structured, role-aware processes that support security-focused development, DevSecOps, and operations at scale.

- **Phase 1: Quick wins.** Organizations should begin by learning and understanding how Red Hat Advanced Cluster Security ingests and prioritizes vulnerabilities. This includes learning the key sources, such as Red Hat Security Advisories (RHSA), the Common Vulnerability Scoring System (CVSS), and GitHub Security Advisories (GHSA), and how to triage issues based on exploitability and potential impact. These foundations help teams take immediate action on high-risk vulnerabilities and develop processes for ongoing risk reduction.
- **Phase 2: Foundational.** Next, teams can use Red Hat Advanced Cluster Security to analyze vulnerabilities at the node, platform, and application levels. For node scanning, Red Hat Advanced Cluster Security provides detailed visibility into host/node-level Red Hat Core Operating System vulnerabilities. For host-level scanning, Red Hat Advanced Cluster Security scans Kubernetes and OpenShift core platform components. Lastly, for applications, it offers insights into image layers and software components, all in an effort to help teams prioritize remediation efforts by severity, context, exposure and platform layer, helping address risks that matter most.
- **Phase 3: Efficient.** With a foundation in place, organizations can embed vulnerability scanning directly into their application pipeline workflows. Using tools such as roxctl, developers can scan container images from their integrated development environments (IDEs) or the command-line. This early insight allows teams to resolve issues before they reach production. Integration with Amazon Linux® Security Center as a Common Vulnerabilities and Exposure (CVE) source adds further context for organizations deploying in AWS environments. In addition, roxctl can generate Software Bills of Materials (SBOM) of container images. These "ingredients lists for software" can be uploaded and managed in SBOM management solutions, such as Red Hat Trusted Profile Analyzer. This can answer questions about usage of a certain vulnerable dependency across the software stack, dependency version drift, and (open source) license compliance, among others.
- **Phase 4: Optimized.** In this phase, vulnerability management becomes a shared responsibility across development and operations teams. Red Hat Advanced Cluster Security supports distributed workflows by allowing targeted vulnerability reporting—filtered by team, namespace, or label. Exception handling and triage workflows can also be automated to support scale, reducing alert fatigue and making sure that the right teams are accountable for the right findings.

Infrastructure protection

Putting a security focus on the infrastructure layer is essential for reducing attack surface and maintaining operational integrity in Kubernetes environments. Red Hat Advanced Cluster Security helps teams to identify exposed services, enforce container-level protections, and apply network controls to restrict unauthorized activity. Following the AWS Security Maturity Model v2, organizations can build a structured approach to infrastructure protection, from basic hygiene to advanced zero trust principles.

- **Phase 1: Quick wins.** Organizations can begin by using Red Hat Advanced Cluster Security to identify and remediate exposed ports. The platform's listening endpoints feature allows security teams to detect unused or risky ports across workloads, minimizing unnecessary network exposure. The network observability feature displays egress and ingress traffic from Kubernetes. Closing these ports helps reduce the surface area for potential attacks and strengthens initial runtime protections.

- **Phase 2: Foundational.** As teams progress, they can use Kubernetes-native network policies to segment workloads and control communication paths. Generated through Red Hat Advanced Cluster Security graphical interface or with a shift-left, developer-friendly roxctl command, these policies enforce strict access controls between pods, namespaces, or services, which reduces lateral movement and contains potential compromises within the cluster.

- **Phase 3: Efficient.** A security focus becomes integrated into build pipelines at this stage. Red Hat Advanced Cluster Security supports image scanning and policy enforcement within DevSecOps workflows, making sure that each image meets security and compliance criteria before deployment. Runtime protection is enhanced through malware detection, process monitoring, and image signature validation, while outbound network access is restricted through policies that allow only approved services to reach external systems. Using image signature validation capabilities in conjunction with Red Hat Trusted Artifact Signer adds image traceability and signature transparency to DevSecOps workflows. This only allows images that come from a trusted build system, and thus have gone through a Red Hat Advanced Cluster Security vulnerability scan and compliance check as part of the build workflow.

- **Phase 4: Optimized.** In this phase, organizations apply zero trust principles to Kubernetes infrastructure. Red Hat Advanced Cluster Security can be configured to support mutual transport layer security (mTLS), helping allow identity-aware communication between services. Abstracting application services into serverless functions reduces the attack surface. Red Hat Advanced Cluster Security supports serverless containers as it does for any container and can provide network isolation through custom Kubernetes network policies.

Data protection

Protecting the confidentiality and integrity of information is a key component of Kubernetes security posture. Red Hat Advanced Cluster Security helps organizations identify encryption secrets used within Kubernetes and access rights to them to make sure users have the least privilege they need. Security policies can be written to make sure high-risk or protected containers meet security objectives. Progressing through the AWS Security Maturity Model v2, organizations can evolve from basic classification and backup to enforcing secret handling and sensitive workload best practices across their clusters.

- **Phase 1: Quick wins.** Start by identifying and labeling high-risk or sensitive applications within the Kubernetes environment. Red Hat Advanced Cluster Security provides visibility into workloads and classification labels based on data sensitivity. These labels inform security policy development, allowing for targeted response strategies for workloads handling protected or regulated data.

- **Phase 2: Foundational.** Next, organizations should use Red Hat Advanced Cluster Security built-in backup and restore capabilities to protect critical Red Hat Advanced Cluster Security data. Regular backups make sure Red Hat Advanced Cluster Security data can be recovered in case of loss or compromise. In parallel, the Configuration Management tab can be used to discover encrypted secrets within Kubernetes, which helps teams verify that sensitive data is stored in a security-focused manner. Administrators should also confirm that encryption at rest is configured at the platform level to prevent unauthorized access to stored information.

- **Phase 3: Efficient.** In this phase, data protection extends to communications. Organizations should make sure that all Kubernetes and application workload services use mTLS to encrypt data in transit. The network observability features of Red Hat Advanced Cluster Security detect and report on inter- and intra-pod communication protocols. Certificate rotation practices, while automated with Red Hat Advanced Cluster Security, should also be established to maintain long-term security posture and meet compliance expectations.

- **Phase 4: Optimized.** Red Hat Advanced Cluster Security can be used to assess the communication protocol between agents and generative AI (gen AI) services being run within Kubernetes, as well as help restrict the traffic between identified entities. Gen AI workloads within Kubernetes are containers and therefore can be further protected using the same features of Red Hat Advanced Cluster Security as any other workload.

Application security

Adding a security focus to applications in Kubernetes environments requires continuous collaboration between development, operations, and security teams. Red Hat Advanced Cluster Security helps integrate application-layer controls into the development and container lifecycle, helping teams to detect risks early and apply policies consistently by "shifting-left" and applying during development. By following the AWS Security Maturity Model v2, organizations can move from basic external access controls to active threat modeling and adversarial testing that hardens their applications over time.

- **Phase 1: Quick wins**. Organizations can start by managing external access to Red Hat Advanced Cluster Security through proxy configuration. Red Hat Advanced Cluster Security supports network access via proxy rules, helping to limit exposure and enforce access boundaries for external connections. Administrators should follow platform-specific guidance, such as that provided in internal documentation, to help with a security focused implementation.

- **Phase 2: Foundational.** Once access controls are in place, organizations should engage development teams early in the development lifecycle and have security teams educate and guide this effort. Red Hat Advanced Cluster Security provides tools for risk assessments, CVE exposure analysis, policy enforcement, and compliance tracking. Embedding these tools into development workflows makes sure that security is a shared responsibility from the start, not an afterthought. Shifting security even further left, the Red Hat Dependency Analytics IDE Plugin (part of Red Hat Trusted Profile Analyzer) provides Software Composition Analysis (SCA), recommendations, and mitigations to developers directly in their local development environment.

- **Phase 3: Efficient.** As maturity increases, sources such as the MITRE ATT&CK Containers Platform framework for containers and container orchestration systems such as Kubernetes can help identify attack vectors and inform defensive strategies. Teams can evaluate how configurations and existing security policies would respond without affecting production. They can then refine polices and configurations to mitigate security gaps and identified risks.

- **Phase 4: Optimized.** In the most advanced phase, organizations can simulate real-world attacks to validate defenses. Teams can use the network observability, continuous security policy enforcement, and anomalous behavior alerting features in Red Hat Advanced Cluster Security to assess their security posture in response to simulated attacks based on threat modeling. Red teams can use known vulnerable software to test policies from an adversarial perspective, helping to uncover weak points and further strengthen application security posture. This structured, attacker-aware testing helps make sure that security policies are not only in place but effective against real threats.

Incident response

Responding in an effective and timely way to security events is critical to limiting risk and restoring safe operations in Kubernetes environments. Red Hat Advanced Cluster Security helps organizations to detect, analyze, and respond to violations using a combination of real-time alerts and integration with the broader security ecosystem, including incident management tools. As teams mature through the AWS Security Maturity Model v2, incident response evolves from reactive notifications to policy-focused remediation and orchestrated workflows.

- **Phase 1: Quick wins.** The initial step is to integrate Red Hat Advanced Cluster Security and audit logs and security policy violations into your existing logging or SIEM platforms. Custom webhooks can be configured to trigger notifications when policy violations occur, making sure that the right teams are alerted in real time. This provides the visibility and awareness needed to begin developing a consistent incident response process.

- **Phase 2: Foundational.** With detection mechanisms in place, organizations can begin defining formal incident response playbooks. Using Red Hat Ansible® Automation Platform and event-driven automation (EDA), teams can create workflows that respond automatically to security events. For example, Red Hat Advanced Cluster Security policies can trigger alerts or restart noncompliant containers when runtime threats are detected, accelerating containment.

- **Phase 3: Efficient.** Organizations can then automate playbooks to act on critical findings immediately. These automations are triggered by alerts from Red Hat Advanced Cluster Security and help standardize response actions. In parallel, teams can conduct root cause analysis using Red Hat Advanced Cluster Security behavioral detection and image decomposition capabilities. Understanding the origin and effects of incidents supports more resilient remediation and prevention.

- **Phase 4: Optimized.** In advanced environments, teams can implement automated response infrastructure. Red Hat Advanced Cluster Security supports declarative configurations to detect configuration drift and enforce consistent policies. It also integrates with Security Orchestration, Automation, and Response (SOAR) tools and ticketing systems, including a prebuilt integration for ServiceNow, allowing security events to be automatically logged, triaged, and resolved across established workflows.

Resiliency

Resiliency refers to the capability of security tooling to remain available and functional during failures or disruptions. Red Hat Advanced Cluster Security supports business continuity planning and disaster recovery through backup and restore, multiple instances, and multiregion deployment options. By progressing through the AWS Security Maturity Model v2, organizations can grow from basic continuity planning to automated, regionally distributed failover strategies that maintain consistent protection in any environment.

- **Phase 1: Quick wins.** Begin by evaluating and understanding your organization's current business continuity plan and Recovery Time and Point Objectives (RTO and RPO). A resiliency plan for Red Hat Advanced Cluster Security should support and comply with this plan and recovery objectives, which should include redundancy across multiple availability zones to minimize disruption during outages and improve service reliability.

- **Phase 2: Foundational.** Next, implement redundancy at the infrastructure level by deploying Red Hat Advanced Cluster Security across multiple availability zones in a hot-cold standby configuration and supporting backup replication. This reduces the risk of single points of failure. Teams should also take advantage of the platform's built-in backup and recovery features to make sure that security configurations, policies, and operational data can be restored across zones or regions as needed.

- **Phase 3: Efficient.** At this stage, organizations should test complete disaster and regional recovery plans tailored for Red Hat Advanced Cluster Security. These plans may include using Red Hat Advanced Cluster Management for Kubernetes to support regional recovery. Regular testing validates the ability to recover quickly and maintain operational continuity during incidents.
- **Phase 4: Optimized.** In this phase, disaster recovery becomes automated. Teams can use scripting or Ansible automation to manage multiregion failover, backup, and restoration. Red Hat Advanced Cluster Management regional failover capabilities combined with GitOps help make sure that Red Hat Advanced Cluster Security continues operating with minimal interruption—even in the event of a regional outage.

Real-life implementation scenario

Suncorp, a leading Australian financial services brand, adopted Red Hat OpenShift to modernize its infrastructure and accelerate application delivery.

By shifting to a container-based, microservices architecture, Suncorp reduced deployment times from weeks to minutes and allowed its teams to innovate faster. Red Hat Advanced Cluster Security and automation tools supported the implementation of a security focus across hybrid cloud environments. The platform gave Suncorp the flexibility to build once and deploy anywhere, improving resilience and operational efficiency while maintaining compliance. This transformation helped Suncorp to deliver better digital experiences and respond more quickly to market and customer demands.

Read more about Suncorp's success story.

Architecture information

Integration with AWS services

Red Hat Advanced Cluster Security can integrate with key AWS services to help organizations build and maintain a strong Kubernetes security posture. For monitoring and observability, Red Hat Advanced Cluster Security supports forwarding logs to Amazon CloudWatch or SecLake for centralized visibility into policy violations and runtime anomalies. Additionally, teams can integrate with SecLake to consolidate findings from Red Hat Advanced Cluster Security alongside other AWS-native security services, streamlining risk analysis across the entire cloud environment. For threat detection, Amazon GuardDuty complements Red Hat Advanced Cluster Security runtime detection capabilities by adding context from AWS infrastructure-level events.

Red Hat Advanced Cluster Security also supports audit log forwarding, helping organizations to capture API calls from both Red Hat Advanced Cluster Security and Kubernetes and send them to a centralized logging system for compliance tracking and incident response. Integration with identity systems, including AWS Identity and Access Management (IAM), allows organizations to apply consistent authentication policies. This includes configuring MFA through identity provider federation and applying IAM role assumptions or identity federation for centralized credential management. Red Hat Advanced Cluster Security supports temporary credentials for integrations and service tokens to limit long-term exposure.

Deployment architecture and capabilities

Red Hat Advanced Cluster Security can be deployed in a variety of architectural configurations to suit different operational and governance requirements.

Teams using a self-managed Kubernetes architecture can install and configure Red Hat Advanced Cluster Security on Red Hat OpenShift using its operator, and then use it to enhance the security focus of other Kubernetes deployments. Configuration can be automated with IaC practices, GitOps, or Red Hat Advanced Cluster Management workflows, allowing for consistent deployments across clusters and environments. Declarative configuration and API-powered management make Red Hat Advanced Cluster Security suitable for use in both connected and disconnected environments.

The platform also supports automated compliance reporting. Organizations can assess and track compliance against standards such as PCI-DSS, NIST, and HIPAA using built-in profiles. Reports can be scheduled and exported from the Red Hat Advanced Cluster Security dashboard to support audits or internal assessments. These capabilities help satisfy the AWS Cloud Adoption Framework (CAF) Security Perspective, which emphasizes continuous risk evaluation, auditability, and evidence-based control tracking.

In terms of workload protection, Red Hat Advanced Cluster Security offers network segmentation capabilities through Kubernetes-native network policies, in addition to vulnerability and supply chain risk detection. These policies allow teams to enforce zero trust access patterns, segment workloads, and restrict outbound traffic. Runtime threat detection is activated via behavioral analysis and baseline profiling for applications and services. Suspicious activity, such as privilege escalation or unusual process execution, can be automatically detected and responded to through policy enforcement and integrations with SIEM or SOAR platforms.

Start your 60-day, no-cost trial

Explore how Red Hat Advanced Cluster Security can help you improve your Kubernetes security posture in AWS environments. Start your 60-day trial of the fully managed Advanced Cluster Security Cloud Service today and see how efficiently your teams can move from basic controls to advanced protection.

Explore more resources

Looking for technical guides, deployment tips, or deeper architectural insight? Access additional Red Hat Advanced Cluster Security resources, including documentation, videos, and implementation guides, on the Red Hat website.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, 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 applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

f facebook.com/redhatinc
𝕏 twitter.com/RedHat
in linkedin.com/company/red-hat

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1 www.redhat.com	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com

redhat.com