Prevent, detect, and mitigate breaches in cloud-native applications

Red Hat and Tigera simplify cloud-native security by monitoring, analyzing, and managing communications between workloads. Our solutions help you:

▸ Reduce your attack surface area.

▸ Detect and evaluate threats using real-time data.

▸ Mitigate exposure risks automatically.

Traditional security approaches are not enough for cloud-native environments

Cloud-native environments require new approaches to security. These environments typically include a multitude of components and tools, resulting in large attack surface areas. The complexity and inter-connectedness of cloud-native environments can be difficult to comprehend, making it difficult to find, understand, and remediate vulnerabilities and compliance issues.

To protect your cloud-native environments—and your business—you need to minimize your attack surface area and detect threats and remediate vulnerabilities faster and with minimal manual intervention. Together, Red Hat and Tigera simplify security and compliance in cloud-native environments.

Implement cloud-native security with Red Hat and Tigera

Red Hat and Tigera help you build security into your cloud-native environments by monitoring, analyzing, and managing workload-to-workload communication. Certified with Red Hat® OpenShift®, Tigera Calico Enterprise helps you successfully operate, optimize, and protect critical containerized applications across cloud environments.

Tigera Calico is an active cloud-native application protection platform (CNAPP) with full-stack observability for containers, Kubernetes, and clouds. It works across the build, deployment, and runtime phases of application and resource life cycles to protect your platforms and workloads. It also provides unified controls, real-time monitoring and visualization, and policy definition and enforcement for consistent security and observability across multicluster, multicloud, and hybrid environments .

Red Hat OpenShift is an enterprise-ready, security-focused hybrid cloud platform with built-in DevOps tools and security capabilities—including Security-Enhanced Linux® (SELinux), security context constraints (SCC), identity and access management, data encryption, and Federal Information Processing Standards (FIPS) mode—that are activated by default.

This solution embeds natively into your application environment to provide detailed security controls and visibility between the network and microservices layers. It also works with your existing security tools, environments, and security operations centers (SOCs). Finally, the solution encrypts sensitive data to comply with regulatory mandates like Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and General Data Protection Regulation (GDPR).

Reduce your attack surface area

Red Hat OpenShift and Calico reduce the attack surface area of cloud-native environments using a policy-based, zero-trust approach. Protect your Red Hat OpenShift clusters with zero-trust workload access controls for communication between individual pods and between pods and external endpoints.

Brief   Prevent, detect, and mitigate breaches in cloud-native applications

Learn more about DevSecOps

Read the [Modernize and secure your application life cycles with DevSecOps e-book](#) to learn more about implementing DevSecOps with Red Hat and partners.

Implement detailed domain name server (DNS) policies to regulate connections between workloads and external services like cloud storage. Unify host, container, and application policy creation and management with a unified framework and intuitive declarative policy definition. Limit the impact of security breaches with identity-aware network microsegmentation for both containerized virtualized workloads. Extend your existing firewalls and security information and event management (SIEM) tools to your Red Hat OpenShift environment with included integrations.

Detect and evaluate threats using real-time data

Red Hat and Tigera help you find and assess security vulnerabilities faster using real-time data and machine learning capabilities. Safeguard your workloads from threats at runtime with workload-based intrusion detection and prevention, optimized deep packet inspection, distributed denial of service (DDoS) attack protection, and web application firewalls (WAF). Detect zero-day threats using advanced machine learning techniques that determine baseline signals from processes, file systems, system calls, and network traffic. Monitor and debug cloud-native applications and microservices using the Dynamic Service and Threat Graph and Dynamic Packet Capture tool. You can also collect contextual data from across your environment in real time, prepare it for analysis, and provide it to the appropriate staff and tools for troubleshooting and debugging without requiring direct access.

Mitigate exposure risks automatically

Red Hat OpenShift and Calico help you mitigate exposure risk and remediate issues quickly. Rapidly respond to threats and vulnerabilities using a robust, high-performance security policy engine. This engine alerts security staff about issues and—according to set policies—automatically pauses, quarantines, or terminates affected Red Hat OpenShift pods within milliseconds of discovery. Apply security best practices through the Security Policy Recommender, which scans your environments and suggests policy settings for robust security. You can also build custom policies and automation to prepare data for analysis and provide remediation guidance.

Learn more

▸ [Access](#) the Tigera operator for Red Hat OpenShift.

▸ [Try](#) Calico Cloud—a fully managed Software-as-a-Service (SaaS) version of Calico—at no cost.

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

f facebook.com/redhatinc
🐦 @RedHat
in linkedin.com/company/red-hat

redhat.com
F31587_0422_KVM