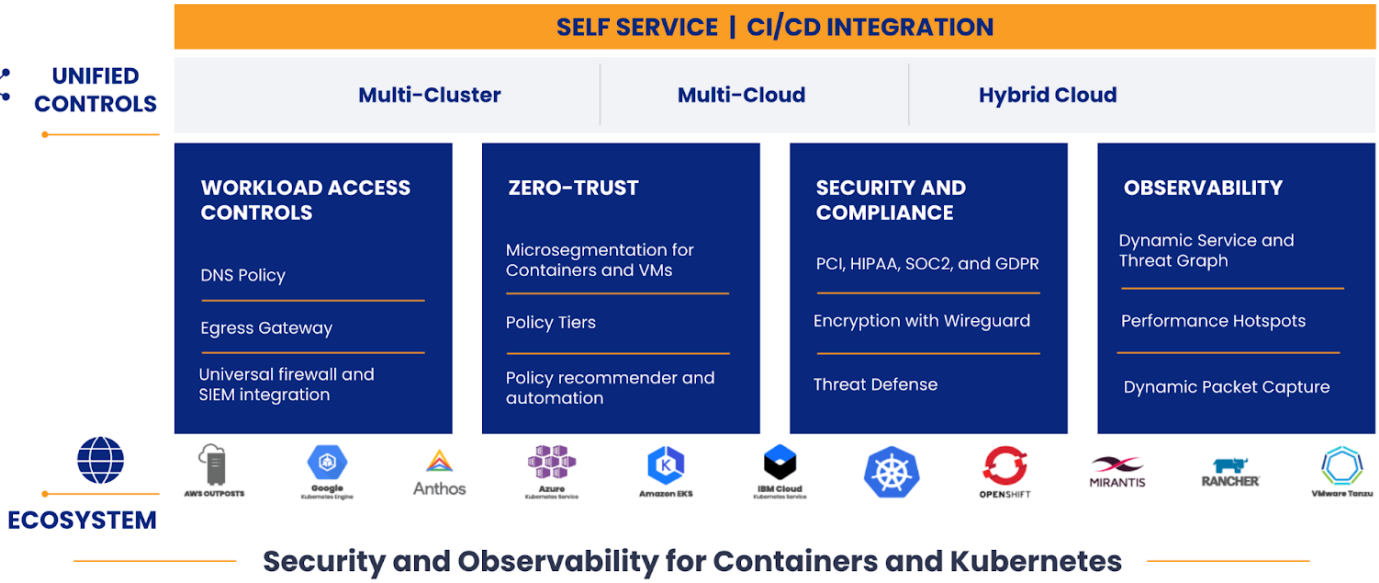
Zero-Trust Security for Red Hat OpenShift With Calico

Reduce attack surface and mitigate security breaches

Overview

Cloud platform engineers are tasked to create and maintain a secure Red Hat OpenShift platform so developers can focus on building applications. Calico provides zero-trust security to enable platform engineers to reduce the attack surface of microservices-based applications, mitigate security breaches, and deliver zero trust-based, defense-in-depth capability for cloud-native applications on Red Hat OpenShift.



Features and Capabilities

Zero-trust workload access controls

Calico provides granular, zero-trust workload access controls between individual pods, namespaces, and services in Kubernetes clusters and external resources, including databases, internal applications, 3rd-party cloud APIs, and SaaS applications. It provides two ways to enable fine-grained workload access controls: using DNS egress policies and NetworkSets (using IPs/CIDRs in network policy). Calico's workload access controls secures all communications between Red Hat OpenShift clusters and outside resources to prevent any command and control attacks.

Egress Gateway

Since pods within a Red Hat OpenShift cluster are dynamic, ephemeral, and do not have a fixed IP address, access from pods within the cluster to resources outside the cluster cannot be secured using a traditional firewall. Calico provides an egress gateway that allocates static IPs to pods to enable firewalls outside the Red Hat OpenShift cluster to identify these pods and apply appropriate security controls. This enables the cluster to securely scale while preserving the limited number of routable IPs and leveraging non-routable IPs for all other pod traffic within the cluster.

Zero-Trust Security for Red Hat OpenShift With Calico

Reduce attack surface and mitigate security breaches

Universal firewall integration

Calico's egress gateway works with any firewall, including Palo Alto Networks, Fortinet, Check Point, and others. Enterprise firewall managers can be used to create a zone-based architecture for your Openshift cluster. Calico reads those firewall rules and translates them into Kubernetes security policies that control traffic between microservices. The firewall manager can be used to explicitly white-list which microservices in Openshift cluster are allowed to traverse zones, providing the network security team with the controls they need to maintain compliance.

Identity-aware microsegmentation

By default, lateral communication between workloads in Kubernetes clusters is not secured. Calico enforces identity-aware microsegmentation to achieve workload isolation and secure lateral communication between pods, namespaces, and services. Labels and service accounts are used to establish the identity of each workload. Calico's microsegmentation works across network and application-layer protocols, and uses a dynamic workload segmentation model based on the metadata (pod name, namespace, node, labels, and annotations) attached to each workload. You can rapidly scale workloads in milliseconds in your OpenShift clusters without having to change security policies by simply using the appropriate labels when deploying new workloads.

Policy tiering

Calico enables Red Hat OpenShift platform teams to define security policies that take precedence over other users' policies in a particular sequence without overwriting an existing policy or skipping the higher priority policy. It supports the delegation of authority by organizational structure and area of responsibility (Platform, Security, DevOps, and Default) defined with Kubernetes role-based access controls (RBAC). With Calico's policy tiering, OpenShift platform teams can enforce enterprise-wide policies that take precedence over any application-specific policy, thus ensuring continuous compliance.

Policy recommendation

The Calico policy recommender inspects traffic within Red Hat OpenShift clusters and recommends appropriate security policies at workload and namespace levels to secure traffic. These policies can be reviewed and modified before staging or enforcement. With Calico's policy recommender, OpenShift platform teams can author, preview, deploy, and manage policies without writing a single line of code.

Compliance (PCI DSS, SOC 2, GDPR, custom frameworks, and more)

Calico supports major compliance standards, including PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA, and any custom frameworks. It continuously monitors OpenShift clusters and the workloads inside the clusters for compliance violations, provides the ability to easily create audit-ready reports, and provides real-time compliance monitoring and reporting to ensure enforcement. Calico allows you to write compliance controls as code, and continuously collects, correlates, and prepares data to provide proof of compliance. Calico also monitors and logs all changes to compliance policies.

Zero-Trust Security for Red Hat OpenShift With Calico

Reduce attack surface and mitigate security breaches

Kubernetes Security Posture Management (KSPM)

Calico's configuration security feature assesses your OpenShift environment against industry standard CIS benchmarks for Kubernetes to identify misconfigurations. This feature includes a periodic assessment report that shows CIS benchmark compliance across all dynamic assets that may have existed in your OpenShift environment during the report period. Organizations can set configurable pass/fail thresholds to align with enterprise security needs. Calico also analyzes Kubernetes RBAC and pod security policy (PSP) settings to detect risks within your Red Hat OpenShift environment.

Observability and troubleshooting

Calico provides a graph-based visualization of your OpenShift deployments, including pods, namespaces, and services, complete with built-in troubleshooting tools to identify and resolve security and audit gaps, performance issues, connectivity breakdown, anomalous behavior, and security policy violations. Calico's Dynamic Service and Threat Graph provides runtime visibility across the stack, from the network layer to the application layer, showing how namespaces, services, and pods are operating in your OpenShift cluster and the risks present across your environment. It also comes with Dynamic Packet Capture—a Kubernetes-native way to troubleshoot performance hotspots and connectivity issues faster by capturing packets from a specific pod or collection of pods with specified packet sizes, ports, protocol and duration.

Data-in-transit encryption with WireGuard

Calico uses WireGuard to implement data-in-transit encryption. WireGuard runs as a module inside the Linux kernel and provides enhanced performance with lower CPU consumption. Compared to standard approaches, Calico encryption eliminates operational complexity for DevOps and Security teams and can be used to address regulatory mandates that specify the use of encryption, including SOX, HIPAA, GDPR, and PCI DSS.

MARSH & McLENNAN COMPANIES · MEDIDATA · MERCK · opensource.com · orange™ · VERISIGN · SPRIBE

Want to learn more? Try a free Calico Cloud trial.

Get Started

Tigera, Inc.
58 Maiden Lane, Fl 5
San Francisco, CA 94108
+1 (415) 612-9546 / www.tigera.io