SOLUTION DATASHEET

Calico for Kubernetes Security

Kubernetes is the de facto platform to orchestrate containerized workloads and services for hybrid and multi-cloud deployments and multi-cluster environments, all of which are the building blocks of cloud-native applications.

Security challenges

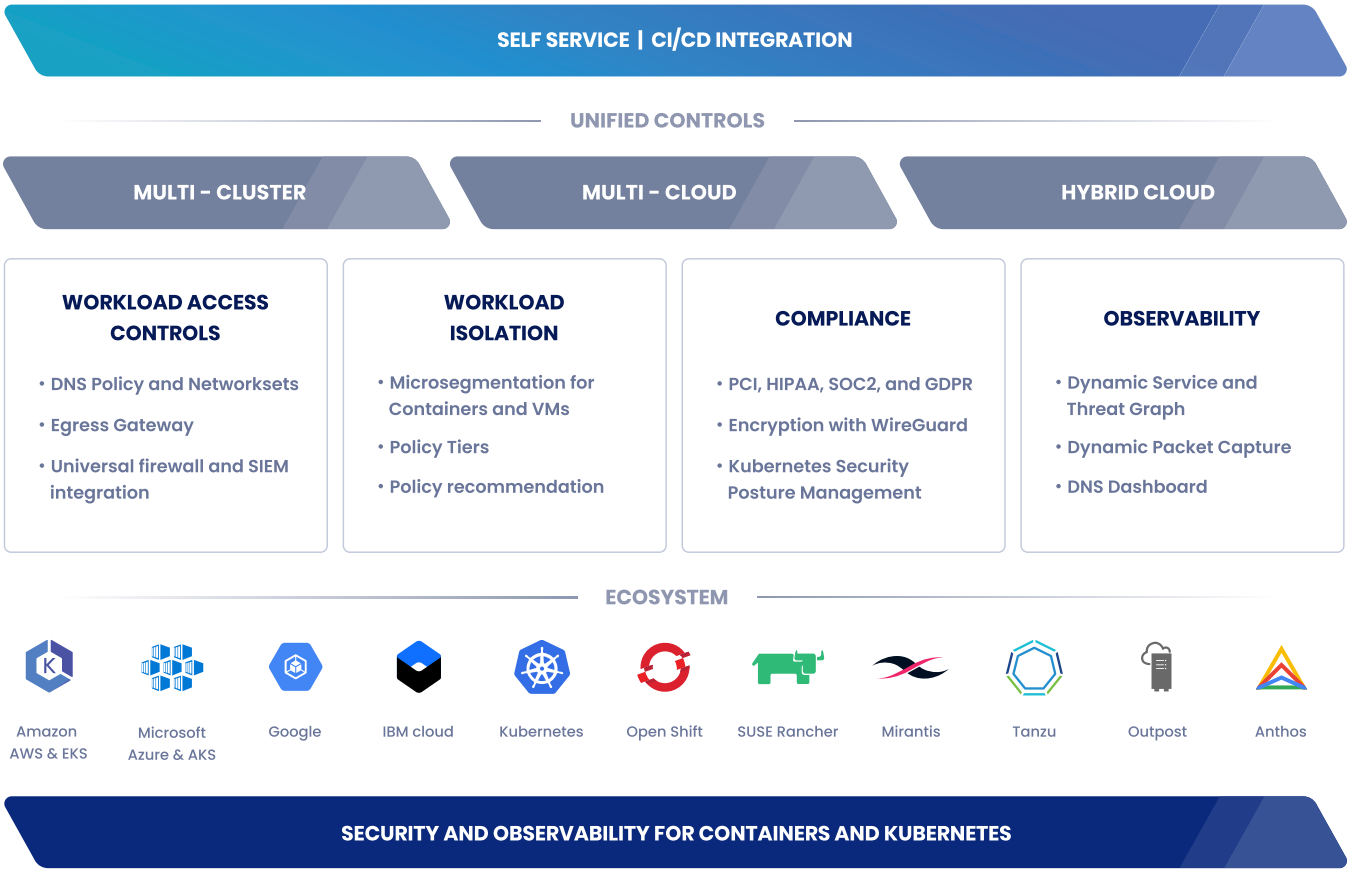
Kubernetes workloads are highly dynamic, ephemeral, and are deployed on a distributed and agile cloud infrastructure, such as Red Hat OpenShift, SUSE Rancher, Amazon EKS, and Microsoft AKS. As a result, cloud platform architects and engineers must address numerous security challenges when deploying workloads in Kubernetes.

- Secure workload communication with resources outside the cluster.
- Enable secure access to resources behind traditional firewalls.
- Isolate applications and workloads by segmenting the Kubernetes cluster.
- Provide visibility into active and inactive security policies and security gaps in the cluster.
- Ensure that Kubernetes configuration complies with industry benchmarks such as CIS for Kubernetes.
- Achieve compliance with regulations such as SOC 2, PCI DSS, HIPAA, and others.
- Simplify security policy administration with automated end-to-end workflow to create, stage, update, and delete security policies.
- Enable connectivity & secure communication between workloads & services across multiple clusters.
- Create shared services across multiple Kubernetes clusters.

How Calico can help

Reduce attack surface	Visibility and compliance	Unified security controls
Secure pod access and communication within and outside of the cluster to mitigate attacks	Gain end-to-end traffic visibility to identify security gaps, service connectivity, and performance issues	Single pane of glass to manage security policies across multi-cloud and multi-cluster Kubernetes environments

Calico is the industry's only active security platform with full-stack observability that addresses Kubernetes cluster and workload security requirements. Tigera delivers Calico as a fully managed SaaS (**Calico Cloud**) or a self-managed service (**Calico Enterprise**). Both Calico platforms help organizations manage security controls across multiple applications, clusters, and environments.



Implementing Kubernetes security with Calico

Zero-trust workload access controls

Calico provides granular, zero-trust workload access controls between individual pods in Kubernetes clusters to external resources, including databases, internal applications, 3rd-party cloud APIs, and SaaS applications. It provides fine-grained workload access controls using DNS egress policies and NetworkSets (using IPs/CIDRs in network policy).

Egress gateway

Egress gateways allow you to identify the traffic source at the namespace or pod level when it leaves a Kubernetes cluster to communicate with external resources. This makes it highly beneficial for security teams to apply access controls to specific traffic instead of opening up a larger set of IP addresses. The Calico Egress Access Gateway assigns a fixed, routable IP to a Kubernetes namespace. All egress pod traffic from that namespace with an assigned routable IP address identifies the workload running within that namespace. 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.

Universal firewall integration

Deploying traditional firewalls in Kubernetes is challenging, since firewall rules need a static source and destination IP address. The Calico Egress Gateway works with any firewall, enabling Kubernetes resources to access endpoints behind a firewall securely. With this integration, firewalls can extend their zone-based architectures (trusted, untrusted, DMZ) to Kubernetes. Tigera's Calico-Fortinet integration enables Fortinet customers to leverage existing investments in Fortinet solutions to enforce security and compliance requirements, and protect cloud-native Kubernetes workloads using the same familiar tools, processes, and security workflows that you use to protect your non-Kubernetes workloads.

Identity-aware microsegmentation

By default, lateral communication between workloads in Kubernetes clusters is not secured. Calico enforces microsegmentation to achieve workload isolation and secure lateral communication between pods, namespaces, and services. It enables teams to logically divide workloads into distinct security segments and then define granular security controls for each unique segment. Teams can isolate workloads based on environments, application tiers, compliance needs, user access, and individual workload requirements.

Security policy management

Calico provides a policy framework to create, test, deploy, and manage security policies. It recommends policies, provides hierarchical policy tiers, and a policy board to bolster Kubernetes cluster and workloads security for shared Kubernetes environment across multiple teams with different stakeholders. Calico provides platform, security, and application teams the autonomy to create and deploy cluster, namespace, and workload-specific policies. Users get real-time metrics on how policies are evaluated within and across policy tiers. They can view all active and inactive security policies for their Kubernetes cluster with a hierarchy based on roles and permissions in one interface.

Observability and troubleshooting

Calico's Dynamic Service and Threat Graph provides a graph-based visualization of your Kubernetes deployments, including images, pods, namespaces, and services. It has built-in troubleshooting capabilities to identify and resolve security and compliance gaps, performance issues, connectivity breakdowns, anomalous behavior, and security policy violations. For example, dynamic packet capture is integrated into Dynamic Service and Threat Graph to deliver a faster, Kubernetes-native way to troubleshoot performance hotspots and connectivity issues by capturing packets from a specific pod or collection of pods using specified packet sizes 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 to provide better performance and lower CPU consumption. Calico encryption eliminates operational complexity for the teams compared to standard encryption approaches. It can be used to address regulatory mandates that specify the use of encryption, including SOX, HIPAA, GDPR, and PCI DSS.

Kubernetes Security Posture Management (KSPM)

Calico assesses your Kubernetes environment against industry-standard CIS benchmarks to identify misconfigurations across your Kubernetes environments. This feature includes a periodic assessment report that shows CIS benchmark compliance across all dynamic assets in your Kubernetes environment during the reporting period. An overall score is available for each in-scope asset, which can be compared against configurable pass/fail thresholds. Calico also analyzes Kubernetes role-based access controls (RBAC) and pod security policy (PSP) settings to detect risks within your Kubernetes environment.

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

Calico Cloud supports major compliance standards, including PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA, and any custom frameworks. It provides real-time, continuous monitoring to detect compliance violations and can generate audit-ready reports.Calico allows you to write compliance controls as code, allowing you to continuously collect, correlate, and prepare data to provide proof of compliance at any time. The platform also monitors and logs all changes to compliance policies.

Clustermesh

Calico provides a centralized, multi-cluster management plane to enable security, observability, and advanced networking for workloads and services across multiple clusters in hybrid and multi-cloud environments. Calico provides unified security policy controls and federated endpoints and services.

Key customers

Get hands-on experience with our upcoming webinars and live online workshops.

Get Started

TIGERA

Tigera, Inc.

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