DATA SHEET

Calico Enterprise

Enterprise Network Security for Kubernetes

Project Calico is open source software that provides networking and network policy for Kubernetes and is trusted by the largest production Kubernetes deployments across the globe for its speed, scalability, and stability. For clusters large and small, Project Calico "just works" and is the best option available for both cloud-based and on-premises Kubernetes clusters.

Calico Enterprise layers tools and capabilities on Project Calico that enable platform engineers to accelerate the widespread adoption of Kubernetes across the enterprise.

To accelerate the adoption of a Kubernetes platform, platform engineers need to address the needs of multiple end-users, applications, and organizations.

- End-users need tools to efficiently deploy Kubernetes network policies and validate that they work as expected before committing them
- Applications have a range of security requirements and some need specific compliance reports
- Networking and Security teams will have requirements for how Kubernetes fits within the network and security architecture

Key Features

Network Policy Lifecycle Management

- Enable new and advanced Kubernetes users to create Network Policies
- Reduce risk of outages

Network Flow Visibility

- Contextual logging including namespace, labels, and policies accepting/denying

Fine-Grained Security Controls

- Securiry Gaurdrails
- Fine-grained access to resources outside of the cluster

Network Flow Visibility

- Generate reports for compliance requirements

Network Policy Lifecycle Management

By default, Kubernetes allows all workloads to communicate with each other, commonly referred to as an "open cluster". An open cluster is not good practice for supporting more than a single application, and Kubernetes Network Policies are the industry standard solution.

Network Policies are difficult to create and a misconfigured network policy can result in connectivity problems between your services or potentially outages across your entire cluster.

Calico Enterprise enables network policies to be created, tested, deployed, and updated safely in your cluster using the following lifecycle management workflow.

1. Policies can be auto-generated and a GUI builder can be used, or YAML files can be imported using a CI/CD pipeline
2. Policies are deployed in a preview mode that reports on the impact the network policy will make
3. When approved, the policy is committed and enforced
4. Changes to network policies iterate through this workflow

DATA SHEET

Calico Enterprise

Enterprise Network Security for Kubernetes

Network Flow Visibility

Kubernetes network connectivity is difficult to triage; whether for debugging or for security workflows. Kubernetes does not natively log network traffic, and host-based monitoring solutions only track the source and destination IPs of the hosts and have no visibility into the context required: namespace, pod, labels, and policies the traffic passes through.

Calico Enterprise logs all network flows, including the source and destination namespaces, pods, labels, and the policies that evaluate each flow. This enables any DevOps engineer to rapidly pinpoint which policies are allowing and denying traffic between their services.

Network flows serve many additional uses. They are used by security teams to identify malicious traffic within internet-facing applications and are a necessary dataset for most compliance audits.

Fine-Grained Security Controls

An application that interacts with customer data will have different controls than another that performs routine internal business functions.

Your Kubernetes platform must be able to apply the appropriate granularity of security controls for both. Some workloads may also need to connect to endpoints outside of the cluster: cloud services, APIs, databases, and legacy systems. Kubernetes does not offer a way to implement fine-grained access to resources outside of the cluster, and other tools like firewalls cannot help either due to the dynamic IP addresses used by Kubernetes workloads.

Calico Enterprise introduces tiered network policies that platform teams use to implement security guardrails that are applied to certain classes of applications. Calico Enterprise also extends Network Policy to add DNS endpoints, allowing only specified workloads to connect to any given resource outside of the cluster.

Compliance

Some applications will have specific compliance mandates. If an application interacts with customer data or payment card information it may have internal. regulatory, or industry compliance requirements; or laws to abide by.

Calico Enterprise monitors and provides evidence reports that auditors need to assess compliance with standards the application must meet.

About Tigera

Tigera provides zero-trust network security and continuous compliance for Kubernetes Platforms. Modern applications are dynamic and break traditional static security models. Our flagship product, Calico Enterprise, meets enterprise needs for security and compliance and supports multi-cloud and legacy environments with a universal security policy that is automated and delivered as code.

Calico Enterprise builds on leading open source projects: Project Calico, and Istio, which Tigera engineers maintain and contribute to as active members of the cloud-native community.

For more information about Calico Enterprise and how it can help you secure your modern applications and demonstrate compliance, email us at contact@tigera.io.

Tigera, Inc.

58 Maiden Lane, Fl 5
San Francisco
CA 94108

+1 (415) 612-9546
www.tigera.io