DATA SHEET

Calico Enterprise

Enterprise Network Security for Kubernetes

Key Features

Network Policy Lifecycle Management

- Enable new and advanced Kubernetes users to easily create network policies using automated workflows

Centralized Multi-Cluster Management

- Manage security and maintain policy consistency across all clusters from a single point-of-control

Network Flow Visibility

- Enable faster discovery and resolution of Kubernetes connectivity issues with context-rich flow logs

Fine-Grained Security Controls

- Enforce IP egress policies for Kubernetes resources using existing firewalls and firewall management platforms

Compliance Reporting

- Generate global and application-specific reports from detailed audit logs for compliance purposes

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

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

Centralized Multi-Cluster Management

The Calico Enterprise Global Network Security Center (GNSC) for Kubernetes is a centralized management plane and a single point of control for multi-cluster and multi-cloud environments.

Calico Enterprise's centralized control simplifies and speeds routine maintenance, leaving more time for your platform team to address other important tasks. Calico Enterprise also includes centralized log management, troubleshooting with Flow Visualizer, and cluster-wide IDS (intrusion detection). GNSC provides compliance reporting, and alerts on non-compliance and indicators of compromise.

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 and graphically displays them in a Flow Visualizer. Logged data includes 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 Access Controls

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

Universal Firewall Access extends the scope of firewalls and firewall managers like FortiManager and Panorama to Kubernetes. With Calico Enterprise, you can automate the deployment of your existing firewalls to secure Kubernetes without the need to create complex configuration files to secure containers. A single firewall rule allows all pods within a namespace access to a resource outside 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, industry, or regulatory compliance requirements.

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

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

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

TIGERA

Tigera, Inc.

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

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.