TIGERA CASE STUDY

Automobile manufacturer accelerates application delivery while improving security posture and compliance with Calico

Highlights:

- Reduced application delivery time by two weeks by eliminating Kubernetes-related firewall changes
- Addressed compliance gaps by gaining visibility into Kubernetes workloads
- Deployed a zero-trust security model to protect against emerging threats

Overview

This manufacturer is a global leader in producing and selling automobiles. The company produces millions of automobiles annually and employs several hundred thousand workers worldwide.

The company's vision is beyond merely manufacturing automobiles; they want to connect with their drivers and passengers digitally. This relies on their ability to interact with customers online and will require an agile delivery model. The company chose to build a Kubernetes platform to serve their needs for agility and scalability. The company deeply cares about their customer's data, which drove the need for an agile security and compliance solution that could support the dynamic nature of their Kubernetes platform.

With Calico, the company was able to:

- Remove bottlenecks caused by firewall rule changes, thereby accelerating application delivery
- Meet their internal and external compliance requirements with proper identification of workload traffic
- Protect east-west workload traffic within their Kubernetes clusters against emerging threats
- Achieve security and compliance objectives across containers, virtual machines, and bare metal servers

Business problem

The company faced two major challenges after adopting Kubernetes. First, the expected benefits of fast and agile application delivery did not materialize. Upon closer inspection, application deployment was crippled by the constant need to implement firewall changes to handle the provisioning of ephemeral Kubernetes workloads. The process of provisioning firewall changes for Kubernetes workloads took weeks to complete and required oversight and constant coordination with the security and networking teams, significantly slowing down application delivery. Kubernetes workloads generate exponentially greater network churn when compared to traditional or VM-based architectures. The company's traditional security approaches of custom automation and manual firewall provisioning were not designed for a Kubernetes architecture.

Automobile manufacturer accelerates application delivery while improving security posture and compliance with Calico

The second challenge that the company discovered was that traditional network logs did not capture denied traffic at the container level and provided insufficient details for compliance requirements. These dated capture methods only provided limited 5-tuple flow logs and required additional context to be useful. Traditional 5-tuple information containing IP and port information was unable to provide context specific to Kubernetes workloads that cycle through IP addresses. The company discovered that monitoring Kubernetes workloads is significantly different than monitoring traditional host-based systems and requires visibility into the Kubernetes constructs. These constructs where the application runs are entirely invisible to traditional network monitoring systems that stop at the host. Kubernetes construct information such as containers, pods, nodes, namespaces, and labels are needed beyond just IP addresses for compliance requirements.

After realizing the limitations of the traditional security model and technology, the company needed its security and compliance infrastructure to support a new level of agility as developers embraced Kubernetes.

Solution

The company investigated multiple alternatives before deciding to adopt Tigera's Calico Enterprise for multi-cloud zero-trust security. Calico Enterprise stood out because it supports both Kubernetes applications as well as legacy workloads running on bare metal and VMs. Calico was also preferred because its technology is embedded in Amazon, Microsoft, Google, and IBM's Kubernetes services, as well as embedded in Docker EE and integrated into Red Hat OpenShift. This provides the company with the flexibility to change their mind about the Kubernetes distro they use, or to use multiple distros.

The company's focus on security motivated the team to implement a zero-trust security posture, with dynamic, policy-driven, distributed enforcement of network security rules. The company's cross-functional team, including security, networking, compliance, site reliability engineering, development, and technical operations all leverage Calico's security architecture for the following capabilities:

- Calico's hierarchical security policies replaced the firewall for east-west traffic and enabled the security and networking teams to define security controls that cannot be overridden. Developers can now define how their applications communicate without the risk of violating a security control. This approach removes the need for firewall changes each time a new workload is deployed.
- Calico flow logs capture data at the container level and append Kubernetes metadata. The network flow logs include workload identity and other metadata that provides visibility into which workload did what, for compliance auditing and security forensic purposes.
- Calico's security framework provides declarative, intent-based policies. These fine-grained security policies are enforced at multiple points including the host, container, and edge of the application. Network attributes, application-layer attributes, and workload metadata are all evaluated against the policies. This approach alerts the SOC when any anomalous traffic is detected.
- Calico enforces security around each workload, whether it's running on a container, VM, or host. The product supports next-generation containerized applications in Kubernetes as well as legacy workloads running on bare metal and VMs.

TIGERA CASE STUDY

Automobile manufacturer accelerates application delivery while improving security posture and compliance with Calico

Benefits

Calico Enterprise is now a critical component of the company's Kubernetes platform. Calico provides the company with a consistent security framework for Kubernetes and legacy workloads.

Before Calico Enterprise, the typical turnaround for changes to firewall policy was two weeks. The company now uses Calico to deliver same-day changes to accelerate developer agility while maintaining its zero-trust security posture. Calico enabled the increased agility that has come from adopting Kubernetes, together with reducing the time to deploy a new microservice from months to days.

About Tigera

Tigera empowers organizations to secure, observe, and troubleshoot containers, Kubernetes, and cloud. Its products enable organizations of all sizes to protect workloads, detect threats, achieve continuous compliance, and troubleshoot service issues in real time. Tigera is also the creator and maintainer of Calico Open Source, the most widely adopted container networking and security solution. The company's software powers more than 100M containers across 1.5M nodes in 166 countries, and is supported across all major cloud providers and Kubernetes distributions.

Additional resources

O'Reilly ebook: Kubernetes security and observability

Click Here

eBook: Kubernetes networking and security

Click Here

Do you have a question about security, observability, or compliance for containers or Kubernetes?

Contact Us

TIGERA CASE STUDY

Automobile manufacturer accelerates application delivery while improving security posture and compliance with Calico

Getting started

Get hands-on experience with container networking, security, and troubleshooting

Try Now

Become a container and Kubernetes security and observability expert. Sign up for free online training and certification programs

Click Here

TIGERA

Tigera, Inc.

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