TIGERA

Security and observability for containers, Kubernetes, and cloud

Security and observability in minutes. Any container, any Kubernetes distribution, any workload, any cloud.

Cloud-native architecture introduces a new set of security and observability challenges

The dynamic, distributed, and ephemeral nature of cloud-native applications renders traditional perimeter-based security approaches ineffective

With cloud-native workloads, security and observability need to be configured at deployment time, as code

Tigera's Calico products specify security and observability as code (SOaC), which ensures consistent enforcement of security policies, and provides observability and troubleshooting across multi-cluster, multi-cloud, and hybrid deployments

Calico Open Source

Open-source networking and security for containers and Kubernetes, powering 1.5M+ nodes daily across 166 countries

Calico Cloud

Managed cloud service for container, Kubernetes, and cloud security and observability, offered as a pay-as-you-go SaaS or an annual subscription

Calico Enterprise

Self-managed security and observability platform for containers, Kubernetes, and cloud, hosted by the organization on-premises or in the public cloud

The only solutions with a pluggable data plane architecture enabling support for multiple data planes, including eBPF, standard Linux, and Windows

Protect workloads

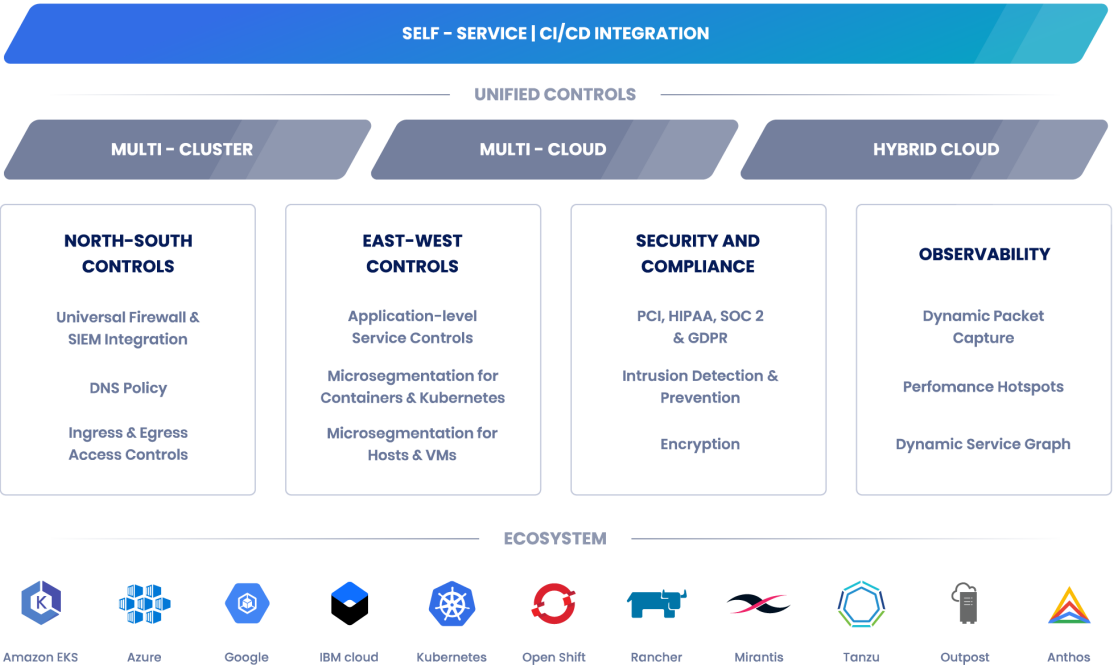
Detect threats

Achieve continuous compliance

Troubleshoot service issues

TIGERA

Solution architecture



Key customers

Ford
IBM
AT&T
DISCOVER
MERCK
L3HARRIS™ FAST. FORWARD.
Bloomberg

Key partners

aws
Azure
Google Cloud
MIRANTIS
Red Hat
FORTINET
RANCHER

Locations: San Francisco, CA | San Jose, CA | Cork, Ireland | Vancouver, Canada | London, UK