TIGERA

Calico Cloud: Plug-and-Play Active Container Security

Cloud-native applications running on containers and Kubernetes are exposed to a large attack surface throughout the entire application lifecycle, from development to deployment and production. This large attack surface, combined with the highly dynamic and ephemeral nature of cloud-native workloads, demands a different kind of security posture.

Calico Cloud is a next-generation container security platform that balances prevention and risk mitigation with threat detection to reduce the attack surface, actively detect threats, and deploy mitigating security controls to limit the risks of exposure. Calico Cloud is the industry's only active security platform with full-stack observability. It enables organizations to prevent attacks using zero-trust, and to detect, troubleshoot, and automatically remediate exposure risks from security breaches across multi-cloud and hybrid deployments. Calico Cloud is built on Calico Open Source, the most widely adopted container networking and security solution.

Security challenges

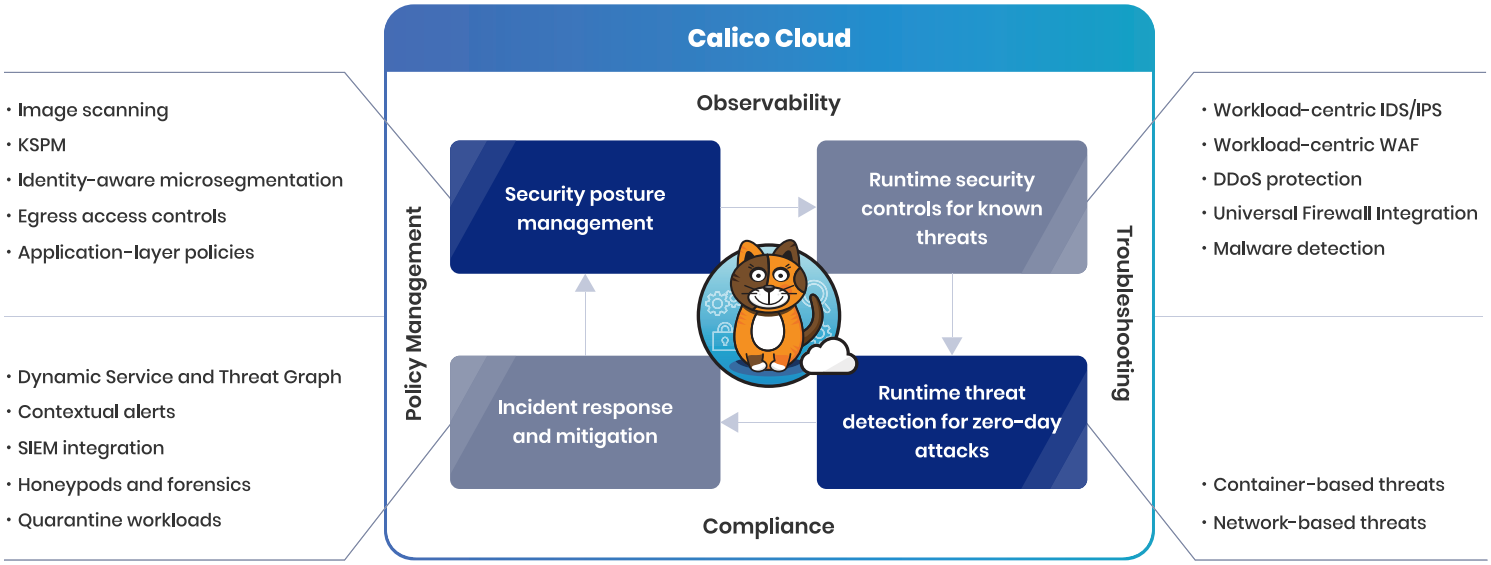
- Large attack surface throughout the application lifecycle
- Lack of visibility creates security blind spots
- Detection-centric security creates false positives that result in alert fatigue and overburdened security teams
- Achieving compliance with regulations such as SOC 2, PCI DSS, HIPAA, is cumbersome
- Given the flat Kubernetes network, traditional perimeter security is inadequate

How Calico can help

Calico is the industry's only active plug-and-play security platform with full-stack observability to prevent, detect and mitigate security breaches in containerized applications.

Reduce attack surface	Detect and stop attacks	Actively mitigate risks
Secure workload access and communication within and outside of the cluster to mitigate attacks	Protect workloads from known and zero-day threats in containers and the network during runtime	Deploy recommended security controls to mitigate exposure risks

How Calico transforms Container Security



Robust security posture for containerized workloads

Automated vulnerability management

Continuously scan images for known CVEs and prevent vulnerable workloads from being deployed using an automated and fully integrated CI/CD pipeline. Leverage runtime view of vulnerable workloads to assess risks and deploy mitigating security controls to minimize blast radius.

Kubernetes Security Posture Management (KSPM)

Harden your Kubernetes environment against industry-standard CIS benchmarks to identify and fix misconfigurations across your dynamic Kubernetes environments.

Zero-trust workload access controls

Deploy 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. Secure pods using fine-grained DNS egress policies and NetworkSets.

Identity-aware microsegmentation

Secure lateral communication between pods, namespaces, and services. Achieve workload isolation based on environments, application tiers, compliance needs, user access, and individual workload requirements.

Application-layer policies

Enforce application-layer policies for microsegmentation and access control with L7-specific attributes such as HTTP methods and URL paths.

Tigera. San Francisco, CA | San Jose, CA | Cork, Ireland | Vancouver, Canada | London, UK

Runtime protection from known threats

Workload-centric IDS/IPS

Block communication to known malicious IPs and receive alerts about suspicious domains using global threat intelligence feed integration.

Workload-centric WAF

Protect workloads from HTTP-based attacks such as OWASP Top Ten and other non-conforming HTTP headers, especially for lateral communication.

Malware detection

Detect and alert on known malware with a signature-based approach. Uncover ransomware and crypto mining incidents with curated detection capabilities and alerts.

DDoS protection

Prevent and mitigate DDoS attacks with host and application level security policies.

Universal firewall integration

Extend zone-based architectures (trusted, untrusted, DMZ) to Kubernetes. Protect cloud-native Kubernetes workloads using familiar tools, processes, and security workflows that protect your non-Kubernetes workloads.

Runtime protection from zero-day threats

Network-based anomaly detection to detect zero-day attacks

Stop zero-day attacks with heuristics-based learning of anomalous network activity. Detect Indicators of Attack (IoA) from network flow logs, DNS, and HTTP logs.

Container-based anomaly detection to detect zero-day attacks

Detect zero-day threats with out-of-the-box, behavior-based detectors that analyze container activity using process, file system, and system call collected with eBPF probes.

Incident response and risk mitigation

Observability and troubleshooting

Get complete visibility with a graph-based visualization of your Kubernetes deployments, including images, pods, namespaces, and services with Calico's Dynamic Service and Threat Graph. Purpose-built with troubleshooting capabilities to identify and resolve security and compliance gaps, performance issues, connectivity breakdowns, anomalous behavior, and security policy violations.

Alert and quarantine

View and manage all security, network, and performance-related actionable alerts from a single alert dashboard with customizable filters. Apply quarantine policies to isolate vulnerable workloads to enable remediation efforts.

Management and compliance

Data-in-transit encryption with WireGuard

Eliminate the operational complexity of standard encryption approaches with Calico's WireGuard integration. Address regulatory mandates for encryption, including SOX, HIPAA, GDPR, and PCI DSS.

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

Achieve and maintain compliance with real-time continuous monitoring to detect violations and generate audit-ready reports. Supports PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA, and any custom frameworks.

Security policy management

Author, stage, preview, enforce and manage security policies with our unified policy framework. Calico recommends policies and provides hierarchical policy tiers based on roles and permissions. The manager UI comes with a policy board so teams can easily view and manage all active and inactive security policies in the Kubernetes cluster.

Key customers

NBC UNIVERSAL · SIEMENS Healthineers · RBC Royal Bank · DISCOVER · Bloomberg · MERCK · upwork

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