

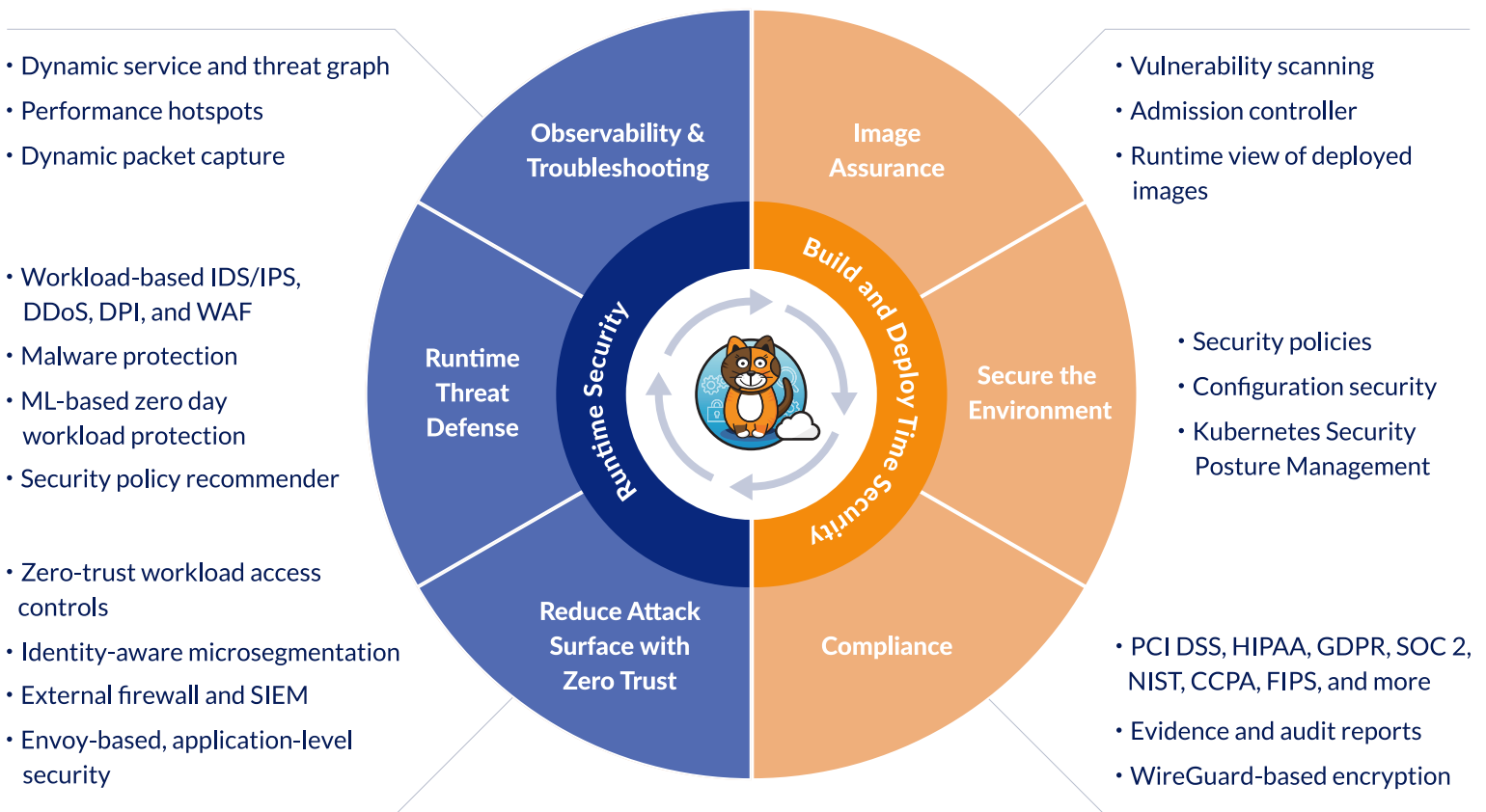
# Calico Cloud

Active security for containers and Kubernetes

Calico Cloud is the industry’s only active security platform with full-stack observability for containers and Kubernetes. Delivered as a fully-managed SaaS, the platform prevents, detects, troubleshoots, and mitigates security risks across multi-cloud and hybrid Kubernetes environments.

With Calico Cloud, users only pay for services consumed and are billed monthly, getting immediate value without upfront investment.

## Prevent, detect, and mitigate security breaches in containers and Kubernetes



# Calico Cloud

Active security for containers and Kubernetes

## Vulnerability management

Calico Cloud provides comprehensive vulnerability management with support for image scanning, automated admission controller, and policy generation to reduce the risks of vulnerable workloads in production. Using Calico's admission controller, you can review overall and individual risk scores for vulnerabilities and enforce automated deployment rules. The runtime view of vulnerable workloads combined with the security policy recommender provides a real-time risk-mitigation strategy to prevent an attack from spreading within a cluster.

## Zero-trust workload access controls and universal firewall integration

Calico Cloud provides granular zero-trust workload access controls between individual pods in Kubernetes clusters and external resources, including databases, internal applications, 3rd-party cloud APIs, and SaaS applications. It provides three ways to enable fine-grained workload access controls: using DNS egress policies to enforce controls, NetworkSets for access control (using IPs/CIDRs in network policy), and an Egress Gateway to identify and secure cloud-native workloads via network firewalls.

## Identity-aware microsegmentation

Calico Cloud enforces microsegmentation to achieve workload isolation and secure lateral communication between pods, namespaces, and services. Labels and service accounts are used to establish the identity of each workload. Calico's microsegmentation works across network and application layer protocols and uses a dynamic workload segmentation model based on the metadata (pod name, namespace, node, labels, and annotations) attached to each workload. You can rapidly scale a service without having to change security policies by using appropriate labels when deploying new workloads.

## Runtime threat defense

Calico Runtime Threat Defense provides coverage for the most common MITRE attack techniques for container and network-based attacks by combining signature and behavior-based techniques to detect known and zero-day threats. It continuously monitors and analyzes network and container behavior for Indicators of Attack (IOA) without the need for writing complex rules, freeing up valuable resources that would otherwise be spent on writing and maintaining security rules. It continuously monitors container activity data across processes, file system activity, and system calls. Calico's global threat intelligence feed integrates with AlienVault and other threat intelligence providers to alert and block attacks from known malicious IPs. Calico's workload-centric WAF monitors the HTTP traffic in your cluster and blocks common OWASP Top 10 attacks. By ensuring that services are always available, Calico Cloud protects your containerized workloads from DDoS attacks.

## Policy management

Calico Cloud provides policy UI to create, stage, preview, and enforce security policies using Calico Cloud's policy recommendation, policy tiers, and policy board. Calico Cloud provides platform, security, and application teams the autonomy to create and deploy cluster, namespace, and workload-specific policies.

# Calico Cloud

Active security for containers and Kubernetes

## Observability and troubleshooting

Calico Cloud provides a graph-based visualization of your Kubernetes deployments, including images, pods, namespaces, and services, complete with built-in troubleshooting tools to identify and resolve security and audit gaps, performance issues, connectivity breakdown, anomalous behavior, and security policy violations. The Dynamic Service and Threat Graph provides runtime visibility across the stack from the network layer to the application layer, showing how namespaces, services, and pods are operating in your Kubernetes cluster and the risks (including the level of severity) present across your environment. Dynamic packet capture is a Kubernetes-native way to troubleshoot performance hotspots and connectivity issues faster by capturing packets from a specific pod or collection of pods with specified packet sizes and duration.

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

Calico Cloud supports major compliance standards, including PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA, and any custom frameworks. It continuously monitors Kubernetes and containers for compliance violations, provides the ability to easily create audit-ready reports, and provides real-time compliance monitoring and reporting to ensure enforcement. Calico Cloud allows you to encode compliance controls as code, and continuously collects, correlates, and prepares data to provide proof of compliance. The platform also monitors and logs all changes to compliance policies.

## Data-in-transit encryption with WireGuard

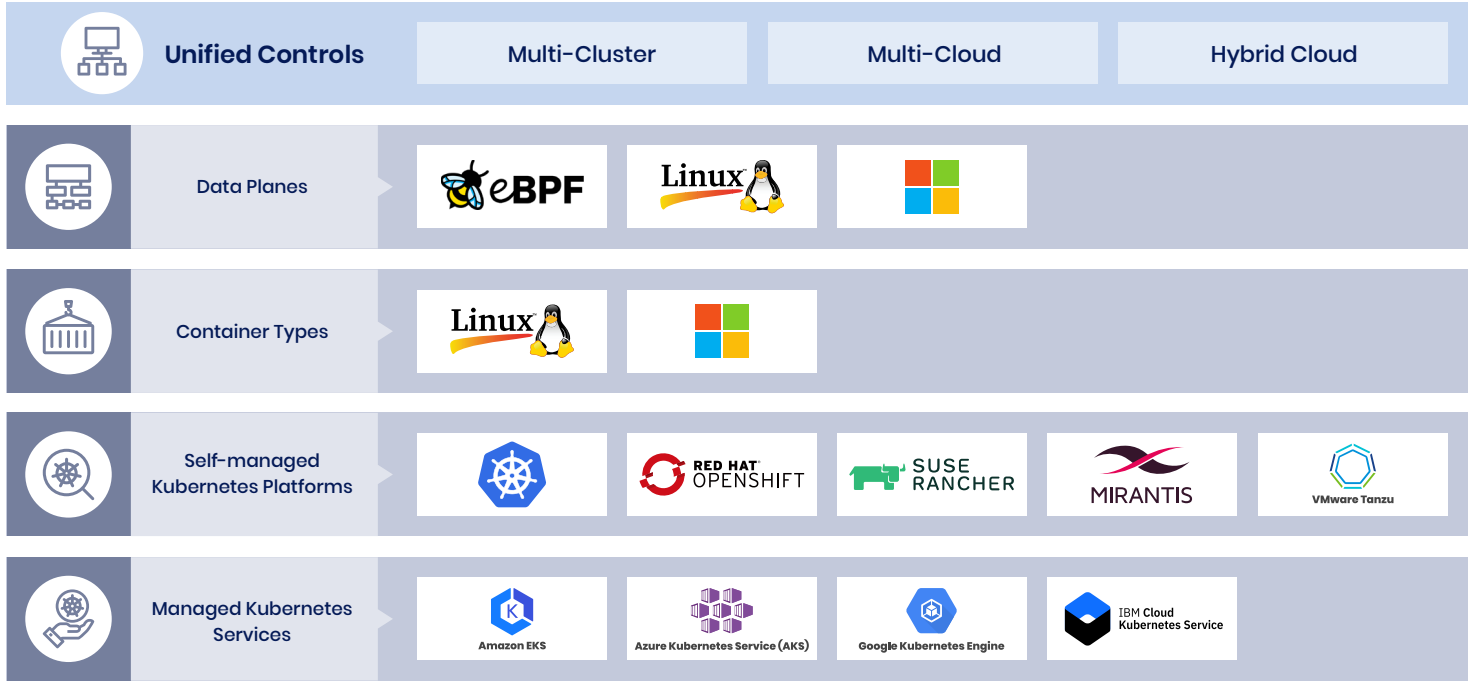
Calico uses WireGuard to implement data-in-transit encryption. WireGuard runs as a module inside the Linux kernel and provides better performance and lower CPU utilization. Calico encryption eliminates operational complexity for DevSecOps teams vs. standard approaches, and can be used to address regulatory mandates that specify the use of encryption, including SOX, HIPAA, GDPR, and PCI DSS.

## Kubernetes Security Posture Management (KSPM)

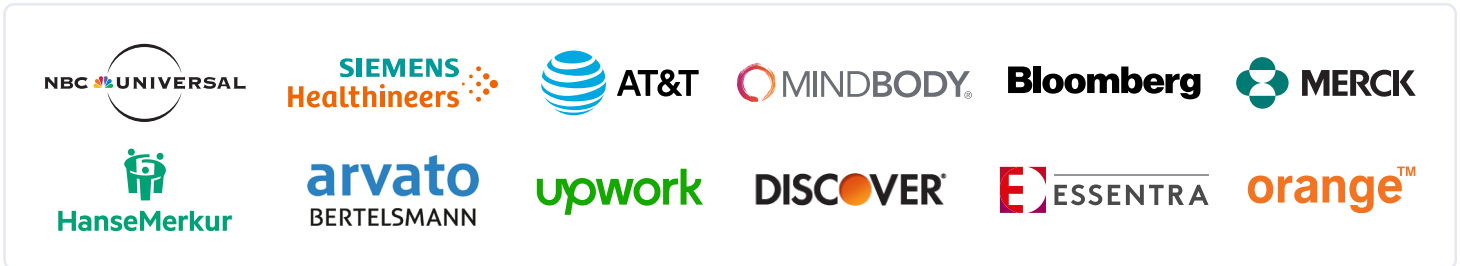
Calico Cloud's configuration security feature assesses your Kubernetes environment against industry standard CIS benchmarks to identify misconfigurations across your Kubernetes environment. This feature includes a periodic assessment report that shows CIS benchmark compliance across all dynamic assets that may have existed in your Kubernetes environment during the report period. An overall score is available for each in-scope asset that can be compared against configurable pass/fail thresholds. Calico Cloud also analyzes Kubernetes role-based access controls (RBAC) and pod security policy (PSP) settings to detect risks within your Kubernetes environment.

# Calico Cloud

Active security for containers and Kubernetes



## Trusted by



## Ready to try Calico Cloud?

[Get Started](#)