White Paper

TIGERA

SOC 2 security compliance for hosts, VMs, containers and Kubernetes

Whether you are using Hosts, VMs, Containers or Kubernetes, Calico can help you achieve granular visibility into your cloud environment, address security risks and meet SOC2 compliance and audit requirements.

Table of Contents

Introduction

System and Organization Controls (SOC) is a set of criteria developed by the American Institute of CPAs. Specifically, SOC Type 2 or SOC 2 offers guidance and certification for organizations that handle sensitive customer data, especially in the cloud. It is essential for IaaS, PaaS, and SaaS service providers to comply with this certification. The certification provides confidence for organizations to entrust third-party service providers with their sensitive information.

SOC 2 is based on five overarching Trust Services Criteria (TSC): security, availability, processing integrity, confidentiality, and privacy. Specifically, the security criteria are broken down into nine sections called common criteria (CC):

- **CC1** – Control Environment
- **CC2** – Communication and Information
- **CC3** – Risk Assessment
- **CC4** – Monitoring Activities
- **CC5** – Control Activities
- **CC6** – Logical and Physical Access Controls
- **CC7** – System Operations
- **CC8** – Change Management
- **CC9** – Risk Mitigation

Organizations running Kubernetes often encounter challenges for CC6 (logical and physical access), CC7 (systems operations), and CC8 (change management) when trying to comply with SOC 2 standards.

SOC 2 security requirement challenges

Many of the security and compliance challenges involved in container and Kubernetes deployments exist because conventional security solutions weren't designed for service-oriented, containerized applications. In a world of ephemeral IP addresses, changing applications, and dynamic environments in which containers move around clusters, traditional security approaches based on static IP addresses are simply unable to perform the observability and security functions necessary to protect a Kubernetes-native environment and meet audit requirements.

Meeting SOC 2 security criteria for hosts, VMs, containers and Kubernetes with Calico Enterprise and Calico Cloud

Hosts, VMs, containers, and Kubernetes, are particularly vulnerable to the spread of malware because of the open nature of cluster networking; by default, any pod can connect to any other pod, even across namespaces. The foundation of Calico's approach to security and compliance for Kubernetes is zero trust, or the assumption that there are attackers both within and outside the cluster network. By default, no users or machines, inside or outside of the network, are trusted. Zero trust is one of the most effective ways for organizations to control access to their Kubernetes networks, applications, and data.

Zero trust policies rely on real-time visibility into applications and workloads and can only be successful if organizations are able to continuously monitor and validate that a requested connection has the right privileges and attributes. One-time validation won't suffice, because threats and connection attributes are all subject to change. Zero trust ensures that all access requests are continuously vetted prior to allowing connection to any of your enterprise or cloud assets. Calico enables a zero trust environment built on three core capabilities: encryption, least privilege access controls, and defense-in-depth.

Here's how Calico helps organizations meet the specific requirements for the SOC 2 security criteria.

Logical and physical access controls (CC6)

Ingress/egress access controls

Calico provides three methods to enable fine-grained access controls between your containers, microservices and external databases, cloud services, APIs, and other applications. Access controls can be enforced from within the cluster using DNS egress policies, from a firewall outside the cluster using the egress access gateway, and with security groups if you are deployed on AWS.

Least privilege access controls

The concept of least privilege requires that a process, user, or application must be able to access only the information and resources that are necessary for its legitimate purpose. All other access is denied. Calico implements least privilege access controls by denying all network traffic by default and allowing only those connections that have been authorized. This applies to traffic between microservices (east-west) as well as ingress and egress outside the cluster (north-south).

Encryption

Calico encrypts data in transit using WireGuard, which runs as a module inside the Linux kernel and provides better performance and lower CPU utilization than IPsec and OpenVPN tunneling protocols. WireGuard eliminates the need for SSL certificates and reduces complexity and operational overhead.

System operations / monitoring

Monitoring and logging ephemeral, containerized workloads is a key observability and security challenge. Calico monitors and logs all workloads, making it possible to see the past performance of workloads during an audit, for example.

Calico's threat detection and defense solution protects sensitive workloads against threat actors deploying APTs, zero-day attacks, and other exploits, using automated detection, response, and mitigation.

Calico monitors north-south and east-west traffic traversing the cluster environment. Using machine learning, Calicoidentifies anomalies and can create a security moat around critical workloads. Honeypods capture zero-day attacks and automatically quarantine potentially malicious workloads to thwart an attack.

Alerts generated by Calico can trigger automated remediation. First, the rogue microservice is immediately isolated from the network. Calico then generates policy recommendations to prevent future attacks. The quarantined workload can be left running to allow your SOC team to complete a forensic analysis.

Change management

Calico compliance policies are Kubernetes-native and based on metadata and labels—not IP addresses—making them simple, scalable, and easy to enforce.

Calico policy tiers define the order in which security policies are evaluated and leverage Kubernetes' role-based access controls (RBAC) to provide granular control over who is authorized to make changes to policies, endpoints, and namespaces. Calico also logs any changes, allowing administrators to easily access the change history during an audit or internal review.

Security policies, represented as code, are deployed alongside your workloads and applications. With policy as code, you can fully automate the end-to-end deployment process including any necessary security changes.

When used in conjunction with a comprehensive security and observability solution, Kubernetes can be highly secure without compromising performance. Tigera makes this possible.

Tigera SOC 2 requirements mapping

The following table addresses requirements from sections 6, 7, and 8 of SOC 2 and provides Tigera guidance for using Calico Enterprise or Calico Cloud (collectively referred to as Calico in the charts below) to bring your systems into compliance. Note: Not all requirements are covered. For some requirements, appropriate guidance will require more specific information about your environment.

Control #	Requirements	How Calico meets this requirement
CC 6.1, 6.6, 6.7, 6.8	Implement logical access security measures to authorized systems only, implement controls to prevent or detect and act upon introduction of malicious software	• Calico can control ingress and egress between microservices and external databases, cloud services, APIs, and other applications • Calico can apply least privilege access controls to a cluster, denying all network traffic by default and allowing only those connections that have been authorized • Calico can encrypt data in transit for added protection against data tampering • Calico can organize all SOC 2 endpoints in one or more namespace • Calico configures the namespace for default-deny and whitelists all ingress and egress traffic
CC 7.1	Monitor and detect configuration changes	• Calico continuously monitors and logs all workloads for compliance against existing security policies • Calico alerts on any configuration changes that may impact existing security policies

CC 7.2, 7.3, 7.4	Monitor systems and components for anomalies and indicators of compromise	• Calico anomaly and threat detection capabilities:
		  • Monitor and analyze threats
		  • Automatically quarantine compromised workloads
		  • Review network flow logs for statistical and behavioral anomalies

Control #	Requirements	How Calico meets this requirement
CC 8.1	Change Management: Authorize, Track, Approve changes to the system	• Calico records all policy changes and provides a change history for audit • Calico provides granular control over who is authorized to make changes to policies, endpoints, and namespaces

Managing SOC 2 audits with Calico

The following table outlines how to prepare for SOC 2 audits related to sections 6, 7, and 8 using Calico. Note: Not all requirements are covered. For some requirements, appropriate guidance will require more specific information about your environment.

Control #	Requirements	How Calico meets this requirement

CC 6.1, 6.6, 6.7, 6.8	Implement logical access security measures to authorized systems only, implement controls to prevent or detect and act upon introduction of malicious software	• Calico provides evidence of compliance with these reports:
		  • Inventory report
		  • Network Access report

CC 7.1	Monitor and detect configuration changes	• Calico provides evidence of compliance with Policy Audit report
CC 7.2, 7.3, 7.4	Monitor systems and components for anomalies and indicators of compromise	• Calico provides real-time visual monitoring of cluster components via a graphical user interface
CC 8.1	Change Management: Authorize, Track, Approve changes to the system	• Calico provides evidence of compliance with Policy Audit report • Calico provides a record of any policy or configuration changes

Learn more about compliance and audit with Calico

Learn More

Jumpstart your SOC 2 compliance initiative by signing up for Calico Cloud

Try Now

About Tigera

Tigera is the industry leader in Kubernetes security and observability, and the inventor and maintainer of Calico Open Source. Our commercial products include Calico Enterprise, a self-managed security and observability platform, and Calico Cloud, a next-generation, Kubernetes-native cloud service that extends the declarative nature of Kubernetes. Calico specifies "security and observability as code," which ensures consistent enforcement of security policies and compliance, and provides observability and troubleshooting across multi-cluster, multi-cloud, and hybrid deployments. Tigera's solutions are used by leading companies, including AT&T, Discover, Merck, ServiceNow, HanseMerkur, RealPage, L3Harris, and Mindbody.

TIGERA

Tigera, Inc.

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