# Table of Contents

Table of Contents

Introduction 3

Challenges with Meeting the SOC 2 Security Requirements 4

How Tigera Helps Meet SOC 2 Security Criteria on Kubernetes 4

  - Logical and physical access controls 4
  - System Operations / Monitoring 5
  - Change Management 5

Tigera SOC2 Requirements Mapping 5

Managing SOC 2 Audits with Tigera Secure 6

About Tigera 8
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 companies that handle sensitive customer data, especially in the cloud. It is quite important for IaaS, PaaS, SaaS service providers to meet and adhere to 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 on Kubernetes often run into challenges with network security for CC6 logical and physical access, CC7 systems operations and CC8 change management when trying to meet SOC 2 standards.
Challenges with Meeting the SOC 2 Security Requirements

Many of the compliance and security challenges involved in Kubernetes deployments come from the fact that traditional security solutions weren’t designed for service-oriented, containerized applications. In a world of shifting IP addresses, ephemeral applications that run and then disappear and dynamic environments in which containers move around clusters, traditional firewall-type security provides neither the actual security assurances nor the visibility into the application needed to pass an audit.

With traditional security solutions designed for a monolithic application, the focus is on preventing application access by building a wall around the application. That approach doesn’t work in a Kubernetes environment as the internal network is extensively used by workloads to communicate.

How Tigera Helps Meet SOC 2 Security Criteria on Kubernetes

The foundation of Tigera’s approach to security and compliance for Kubernetes is Zero Trust, or the assumption that some parts of your network are compromised at all times. A way to centrally administer your security configuration, even across multi-cloud deployments, is also essential to avoid errors at the configuration stage that leave the door open for an attack. Here’s how Tigera helps meet the specific requirements for the SOC 2 security criteria.

Logical and physical access controls
With Tigera, all endpoints can be organized into a single or several consolidated namespaces. Tigera allows you to set all namespaces to deny traffic by default, requiring all ingress and egress traffic to be properly defined.

**System Operations / Monitoring**

The ability to monitor and log ephemeral, containerized workloads is one of the key challenges to security in a containerized application. Tigera monitors and logs all workloads, making it possible to see the past performance of workloads during an audit, for example.

More importantly, Tigera provides automated anomaly and threat detection. This makes it possible to immediately detect services that are behaving unusually by reviewing network flow logs and analyzing them for anomalies. For example, Tigera’s threat protection would automatically quarantine and isolate a service that is suddenly making a large number of requests.

**Change Management**

Tigera leverages Kubernetes’ role-based access controls to provide granular control over who can make changes to endpoints, namespaces, and policies. Tigera also records and audits any changes, allowing administrators to easily access the history of changes to the Kubernetes environment during an audit for internal review.

When used in conjunction with the right tools, Kubernetes can be highly secure without compromising performance, data availability or portability between environments. Tigera can make this possible.

**Tigera SOC2 Requirements Mapping**

The following table addresses requirements from sections 6, 7, 8 of SOC2 and Tigera guidance for bringing your systems into compliance with them. Note: Not all the requirements are covered. Some may require more specific information about your environment for you to know how to become fully compliant.
<table>
<thead>
<tr>
<th>Control #</th>
<th>Requirements</th>
<th>Tigera Guidance</th>
</tr>
</thead>
</table>
| 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 | • Tigera Secure helps organize all SOC2 endpoints in one or more namespace  
• Tigera Secure configures the namespace for default-deny and whitelist all ingress and egress traffic |
| CC 7.1 | Monitor and detect configuration changes | • Tigera Secure keeps a running inventory of all ephemeral workloads |
| CC 7.2, 7.3, 7.4 | Monitor systems and components for anomalies and indicators of compromise | • Tigera Secure anomaly and threat detection capabilities help  
○ monitor and analyze the findings  
○ automatically quarantine the workloads with confirmed compromise  
○ review network flow logs for statistical and behavioral anomalies |
| CC 8.1 | Change Management: Authorize, Track, Approve changes to the system | • Tigera Secure record and review all policy changes that impact connectivity to/from in-scope assets |

Managing SOC 2 Audits with Tigera Secure

The following table outlines how to prepare for SOC 2 audits sections 6, 7, and 8 with Tigera. Note: Not all the requirements are covered. Some may require more specific information about your environment for you to know how to become fully compliant.
<table>
<thead>
<tr>
<th>Control #</th>
<th>Requirements</th>
<th>Tigera Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC 6.1, 6.6, 6.7, 6.8</td>
<td>Implement logical access security measures to authorized systems only, implement controls to prevent or detect and act upon introduction of malicious software</td>
<td>• Tigera Secure provides evidence of compliance with these reports: ○ Inventory Report ○ Network Access Report</td>
</tr>
<tr>
<td>CC 7.1</td>
<td>Monitor and detect configuration changes</td>
<td>• Tigera Secure provides evidence of compliance with Policy Audit Report</td>
</tr>
<tr>
<td>CC 7.2, 7.3, 7.4</td>
<td>Monitor systems and components for anomalies and indicators of compromise</td>
<td>• Tigera Secure provides this through the graphical interface</td>
</tr>
<tr>
<td>CC 8.1</td>
<td>Change Management: Authorize, Track, Approve changes to the system</td>
<td>• Tigera Secure provides evidence of compliance with Policy Audit Report</td>
</tr>
</tbody>
</table>
About Tigera

Tigera delivers solutions for secure application connectivity for the cloud native world. Tigera technology is used by the world's largest enterprises and public cloud providers to power connectivity for application development and deployment and to address the connectivity and security challenges that arise in at-scale production. Tigera Secure meets enterprise needs for zero trust network security, multi-cloud and legacy environment support, organizational control and compliance, and operational simplicity. Tigera Secure builds on leading open source projects Kubernetes, Calico, and Istio, which Tigera engineers help maintain and contribute to as active members of the cloud native community.

tigera.io

email: contact@tigera.io

phone: +1.415.612.9546

Tigera, Inc. 58 Maiden Lane, Fifth Floor, San Francisco CA 94018 USA

“Tigera”, the Tigera logo, “Tigera Essentials”, “Tigera Secure” and “ZT-Auth” are trademarks of Tigera, Inc. All rights reserved. Other trademarks are the property of their respective owners. Copyright © 2019 Tigera, Inc.