StackRox

Solution Brief

SOC 2 compliance in container and Kubernetes environments

SOC (System and Organization Controls) 2 is a set of compliance requirements that applies to companies that store, process, or transmit customer data. A broad range of companies, including SaaS providers, may need to comply with SOC 2 to be competitive in the market and keep customer data secure.

Public cloud providers such as Amazon Web Services, Google Cloud Platform, and Microsoft Azure are subject to SOC 2 and make their audit reports publicly available. Companies that leverage these providers still need to achieve SOC 2 compliance to demonstrate that they're controlling access to their customers' data.

Unlike some compliance specifications, SOC 2 "compliance" provides a framework with pertinent areas of controls but is not a prescriptive specification that spells out specific individual controls. Instead, companies determine the controls, policies, and procedures they will follow to ensure the security, availability, processing, integrity, and confidentiality of customer data. Companies share their defined policies in their SOC 2 Type 1 reports and demonstrate adherence with those policies in their SOC 2 Type 2 reports.

Because the controls, policies, and procedures that are relevant to SOC 2 will differ by company situation, no single security tool can enable or demonstrate SOC 2 compliance. Despite this variance, several companies working to achieve SOC 2 certification, including many SaaS providers, have found the security controls available and documented in the StackRox platform helpful in enabling policies and providing evidence for SOC 2 audits in container and Kubernetes environments.

Customers leverage StackRox to provide evidence for SOC 2 audits of the following trust principles:

Security

This trust principle ensures systems are physically and logically protected against unauthorized access. To help demonstrate this principle, StackRox provides:

- **vulnerability scanning and mitigation** – StackRox identifies vulnerabilities in images as well as running deployments and enables companies to block builds or deployments using images with such vulnerabilities.
- **network segmentation** – StackRox automatically identifies unnecessary communications paths amongst containers, pods, and namespaces and can automatically generate updated network policies that prevent these communications.
- **runtime monitoring** – StackRox detects suspicious or malicious processes and can kill compromised pods.

Availability

This trust principle addresses whether the company is providing the level of availability customers expect. To help demonstrate this principle, StackRox provides:

- **security incident response** – StackRox identifies suspicious processes and takes action, such as killing pods in response to an attack that could compromise system availability.

Process Integrity

This trust principle ensures that systems deliver complete, accurate, and authorized data in a timely manner. To help demonstrate this principle, StackRox provides:

- **process detection and whitelisting** – StackRox enables customers to define all allowed runtime processes, preventing any others from executing
- **policies for insecure images** – customers can leverage StackRox policies to prevent insecure images that could enable infiltration from deploying in the environment
- **configuration management** – StackRox provides out-of-the-box policies to ensure proper configuration of images and Kubernetes and enforce compliance with various organizational security policies and checks, including for orchestrator secrets, role-based access control, adherence to labeling/annotation standards, network policies, secrets, volume mounts, running privileged containers, and other attributes
- **change management** – because StackRox applies all access controls as Kubernetes policies, customers can leverage Kubernetes records to document all system changes

Confidentiality

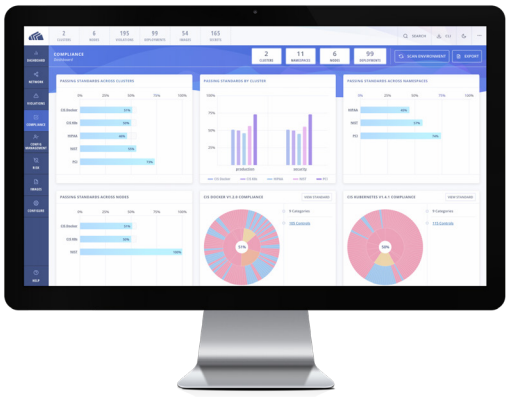
This trust principle ensures protected access to customer data. To help demonstrate this principle, StackRox provides:

- **encryption policies** – customers can define policies in StackRox to ensure specific data is sent with encryption
- **network segmentation** – customers can leverage StackRox policies to restrict access to sensitive data stores
- **secrets management** – customers can create StackRox policies that enforce best practices for secrets management

Privacy

This trust principle ensures PII (Personally Identifiable Information) is not exposed. To help demonstrate this principle, StackRox provides:

- **access control segmentation** – customers leverage StackRox policies to enforce segregation of duties and least privilege principles and to monitor Kubernetes RBAC configuration.



Ready to see StackRox in action?

To learn more about StackRox customers leveraging the StackRox Kubernetes Security Platform to enable these controls or to see how StackRox can help you with evidence for audits, you can request a personal overview at https://www.stackrox.com/request-demo/.

StackRox

StackRox helps enterprises secure their containers and Kubernetes environments at scale. The StackRox Kubernetes Security Platform enables security and DevOps teams to enforce their compliance and security policies across the entire container life cycle, from build to deploy to runtime. StackRox integrates with existing DevOps and security tools, enabling teams to quickly operationalize container and Kubernetes security. StackRox customers span cloud-native start-ups Global 2000 enterprises, and government agencies.

LET'S GET STARTED

Request a demo today!

info@stackrox.com
+1 (650) 489-6769
www.stackrox.com