JUPITERONE

COMPLIANCE

Navigating SOC 2

SOC 2 is a robust security framework adopted by many SaaS providers. If you are thinking about SOC 2 compliance, here are some of the key controls and solutions your organization will need to implement.

Policies and Procedures Documentation

First, security teams need to develop security policies, procedures & operational playbooks that align with SOC 2 requirements.

In order to track implementation and observation of policies, map your controls & documentation to SOC 2 requirements.

Asset Inventory

Build and maintain a robust inventory of your digital environment, including services, accounts, resources and endpoints.

A clear understanding of your environment is critical to efficient identification and remediation of issues.

Access Control

Implement a SAML SSO solution and a multi-factor authentication solution. Performa monthly access reviews to ensure the right users have access to the right services.

Configuration Auditing

Leverage a configuration management & auditing tool to alert your team when a misconfiguration occurs that leaves you out of compliance.

Vulnerability Scanning

Implement an application scanner (static and/or dynamic) using a commercial code scanning tool - also implement a system scanning tool.

Centralized Vulnerability Management

Leverage an enterprise vulnerability management software or build your own internal tooling for tracking, aggregating and reporting on vulnerability findings.

Endpoint Malware Protection

Onboard a commercial endpoint management and protection solution.

Penetration Testing

Invest in an external pen test to evaluate your security practices at least once a year - also implement a responsible disclosure or bug bounty program.

User Endpoint Configuration Monitoring

Implement a Mobile Device Management (MDM) solution.

Server Endpoint Protection

Leverage a commercial or open-source server protection agent.

Risk Management & Compliance Monitoring

Leverage a governance, risk management and compliance (GRC) tool to collect and manage data and evidences.

Security Awareness Training

Engage with a security awareness training provider to proactively train your entire organizations - collect evidence of training completion to spot potential knowledge gaps.

Security Program Metrics & Reporting

Implement a solution for visualizing and charting your environments changes over time for executive and trend reporting.

Network Threat Detection

Implement cloud-native solutions like security groups, VPC flow logs, VPNs for remote access and network firewalls and protection. Don't forget to build flow diagrams for audit evidence.

Architecture Analysis & Diagram

Build and maintain a diagram of your cloud architecture.

Data Protection

Encrypt data stored and in-transit within your cloud infrastructure, configure data backups and recovery policies and ensure you can quickly collect evidence of these policies for security audits.

Change Management

Leverage a commercial tool or build and maintain custom code to integrate security into CI/CD

Vendor Management

Collect and manage a list of vendors in a centralized location using spreadsheets or a vendor management tool.

Production Monitoring and Alerting

Add a paging solution (like PagerDuty or VictorOps) as well as product status page.

Centralized Log Management

Implement a commercial SIEM or open-source SIEM/ELK tool to network flow log analysis.

Incident Response

Build out incident-response playbooks and leverage a forensic analysis solution. Combine the forensics with your reporting solution for easy visualization.

Business Continuity

Develop business continuity and diaster recovery plans, perform data backups and test recovery and run tabletop exercises.

Why Choose SOC 2?

SOC 2 provides cloud-native and software companies a way to verify their controls for protecting and securing data, as well as making sure it's accessible.

Going through this compliance process requires significant investments on both time and resources, but being certified in SOC 2 can provide a leg-up when competing for prospective customers.

SOC 2 Compliance certifications underline your company's commitment to security.

As a software provider, you have been put through the ringer of a third-party audit of your organization's availability, security, privacy, confidentiality and system integrity controls and you came out compliant.

JUPITERONE