Netsurion®

Powering Secure and Agile Networks

SOC 2 Compliance Guide

How Netsurion® Can Help You Achieve and Maintain Compliance

SOC 2 Overview

The AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2) provides guidance for SOC 2 reports performed under the AICPA attestation requirements and guidance established in AT section 101, Attest Engagements (AICPA, Professional Standards). SOC 2 reports replace many reports formerly performed under the SAS 70 (Statement on Auditing Standards No. 70, Service Organizations). SOC 2 provides guidance that allows a service organization to disclose their control activities and processes and compliance with the applicable trust services principles to their customers (user organizations) and their customer's knowledgeable interested parties. The criteria for the applicable trust services principles are based on TSP Section 100 Principles and Criteria, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy. The service organization employs an independent accounting and auditing firm (service auditor) to examine their control objectives and control activities. The service auditor issues a Service Auditors' Report to the service organization at the end of the examination that includes the auditor's opinion.

Netsurion Provides a Full View of the Entire IT Infrastructure

Netsurion's Managed Threat Protection improves security, helps organizations demonstrate compliance, and increases operational efficiencies. We enable your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced, minimizing potential exposure and costs.

Netsurion's Managed Threat Protection is our managed services offerings to enhance the value of EventTracker implementations. Our expert staff can assume responsibility for some or all EventTracker SIEM-related tasks, including system management, incident reviews, daily/weekly log reviews, configuration assessments, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Scalable, Log Collection and Processing with Notifications based on Criticality

EventTracker SIEM provides automatic consolidation of thousands or even millions of audit events to meet the needs of any size organization. The inbound log data is identified by EventTracker's built-in manufacturers Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security standard.

EventTracker SIEM provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, Windows, Linux/Unix, VMware ESX, Citrix, databases, Azure Active Directory, EHRs and more.

Ease of Deployment and Scalability

EventTracker is available on premises or as a highly scalable cloud-based SIEM and Log Management solution. It offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports comprehensive multi-tenant implementations for MSSP organizations serving the needs of smaller customers.

EventTracker Statement of Compliance for SOC 2

SOC 2 Requirement	Netsurion Capability
Infrastructure Implementation II-5 The IT department maintains an up-to-date listing of all system software and respective level, version and patches that have been applied using system utility software.	EventTracker capable of monitoring Application installed or uninstall and patches applied on a system. EventTracker reports help to determine that which application has been installed or uninstalled.
Infrastructure Implementation II-9 The IT department monitors the system and assesses the system vulnerabilities using system utility software.	ETVAS Module can be used for system vulnerabilities assessment and reports for all the vulnerable system on environment. EventTracker analysis and reporting capabilities can be used for monitoring the production environment and assess the system vulnerabilities.
Infrastructure Implementation II-10 OS and application security events are captured in an event log and monitored; the logs are reviewed in the event of a suspected security breach.	EventTracker provides central and secure storage of all audit log data, and the log retained on the storage for 10 years depends upon the storage capacity of the device.
Logical Access LA-1 Management has established policies and procedures for computer network access and equipment responsibilities.	EventTracker monitors all logon, authorization and authentication to the system (success or failed), and reports which help to determine who, where and when done the activity.
Logical Access LA-2 Management has established policy and procedures around User Account Management.	EventTracker collects all user account management activities. EventTracker reports provide easy and standard review of all user account management activity.
Logical Access LA-3 User access is limited to the applications and related data for which they are authorized and approved.	EventTracker monitoring capability can be used to detect the changes (Additions, Deletions, Modifications and Permissions) to the file system. EventTracker analysis & reporting capabilities can be used for monitoring the changes. EventTracker alerting can be utilized to detect and notify changes to specific configurations.
Logical Access LA-5 Unique user IDs are assigned to individual users.	Complete auditing of user accounts and logons to analyze violations and prevent usage of the same ID by multiple persons (e.g. from different computers)
Logical Access LA-6 New network access is reviewed and approved by the appropriate user manager; access to client data is approved by designated manager.	EventTracker can be used to detect and report on granted access for a new user. EventTracker helps to determine that network and system access granted to the user.

EventTracker Statement of Compliance for SOC 2

SOC 2 Requirement	Netsurion Capability
Logical Access LA-7 System access for a user is terminated upon termination of the user's affiliation.	EventTracker can be used to detect and report on revoked access for Users. EventTracker helps to determine that network and system access has been revoked for the terminated User.
Logical Access LA-8 Management performs an annual review of user accounts to ensure that user accounts are valid and assigned privileges are aligned with users' functional roles.	EventTracker can be used to report and determine annual review of user accounts validity and assigned functional roles.
Logical Access LA-9 Firewalls are used and configured to prevent unauthorized access via public networks.	EventTracker capable of monitoring all authorized or unauthorized access to the firewall system. And reports to determine who accessed the system, also the capable of monitoring and reporting upon any changes done to the configuration of firewall policy, firewall rules and profile changes. EventTracker email notification can be set to alert when unauthorized access has been done to the critical firewall system.
Logical Access LA-12 Virus protection is in place to limit the possibility of disruptions that could compromise the security and confidentiality of client data.	EventTracker capable of monitoring and reporting all activity from antivirus protection software.
Logical Access LA-13 Transmission of sensitive data, its clients and its business partners is encrypted	EventTracker is capable of monitoring and reporting all the activity done by an external flash drive.

Reference:

http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx

How Netsurion Can Help

Not sure where to begin? Netsurion helps you reduce cyber risk, augment your IT team's skills, and spend less time on documentation and compliance readiness. Contact us and our experts can advise you on the path to achieve SOC-2 preparedness.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's managed platform approach of combining purpose-built technology and a team of cybersecurity experts gives customers and partners the ultimate flexibility to adapt and grow while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.