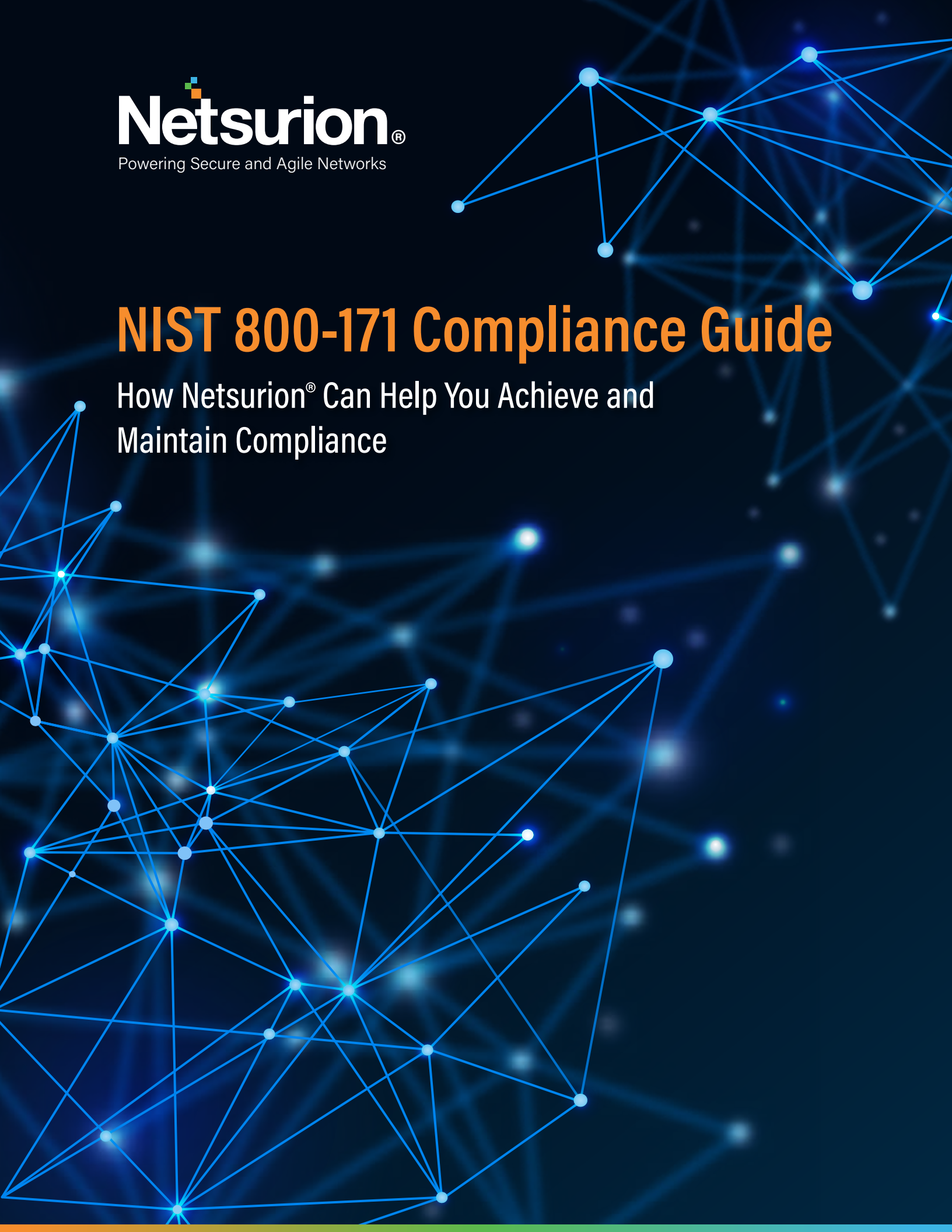
Netsurion®

Powering Secure and Agile Networks

NIST 800-171 Compliance Guide

How Netsurion® Can Help You Achieve and Maintain Compliance



Summary of NIST 800-171

The U.S. Department of Defense (DoD) added more rigor to enforce cybersecurity across its defense industrial base as adversaries increased targeted attacks on governments and supply chain partners. Defense contractors must already meet NIST 800-171 regulations, but self-certification was allowed. Cybersecurity Maturity Model Certification (CMMC) ensures that a formal third-party assessor certifies contractors for basic cyber hygiene and the protection of sensitive government information known as Controlled Unclassified Information (CUI). Our proven expertise with government entities and compliance regulations accelerates your roadmap for readiness and success.

Simplify NIST 800-171 Compliance

Managing your information security compliance is a matter of ongoing processes and is not a "set it and forget it" endeavor. There is no tool or easy button that will "make you compliant." Rather, compliance is about ongoing processes, procedures, and governance. However, having the right systems in place is foundational. And being able to produce the correct reports is necessary for audit success. Netsurion's managed threat protection platform, EventTracker(TM), provides security information and event management (SIEM) which acts as a foundation you need to log and monitor security information and effectively respond to security incidents. Also, Netsurion's platform is managed by our Security Operations Center (SOC) to provide continuous tuning, filtering, monitoring, and alerts so that your IT team can focus on business-related initiatives.

In this document, we outline specifically how Netsurion's platform and services help you achieve NIST 800-171 compliance as well as clarify other elements to consider for compliance certification. If you need additional assistance filling the gaps, contact Netsurion for further information. Our network of partners includes compliance specialists who can help.

Maximize NIST 800-171 and CMMC Certification Readiness

Netsurion provides the foundational platform necessary to achieve compliance as you establish your internal processes and governance. The following table summarizes how Netsurion addresses the 14 control families in NIST 800-171. We augment your existing IT security team with 24/7 monitoring, threat detection and correlation, and comprehensive reporting needed to become audit ready. For a full list of all the requirements, refer to the most current NIST 800-171 publication: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

NIST 800-171 Overview of Cybersecurity Requirements

Control Family		Netsurion Coverage
3.1	Access Control	
3.2	Awareness and Training	
3.3	Audit and Accountability	
3.4	Configuration Management	
3.5	Identification and Authentication	
3.6	Incident Response	
3.7	Maintenance	

Control Family		Netsurion Coverage
3.8	Media Protection	
3.9	Personnel Security	
3.10	Physical Protection	
3.11	Risk Assessment	
3.12	Security Assessment	
3.13	System and Communications Protection	
3.14	System and Information Integrity	

NIST 800-171 Control Families

Control 3.1: Access Control

NIST 800-171	Control Description	Netsurion Capability
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	EventTracker provides you with role-based access control for audit logging/alerts/reports, account management or changes, as well as mechanisms to centrally review access activities.
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	EventTracker provides you with role-based access control (RBAC) for audit logging/alerts/reports, account management or changes.
3.1.3	Control the flow of Controlled Unclassified Information (CUI) in accordance with approved authorizations.	EventTracker provides you with monitoring activities for file and application access, USB monitoring, and email metadata analysis.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	EventTracker provides reporting and alerting on attempts to cross role boundaries, and on changes to configuration that affect separation of duties.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	EventTracker provides network connection monitoring, application execution, and records and monitors system logon activities.
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	EventTracker provides process execution, application installs, and command execution, which are reported dependent on OS/application auditing.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	EventTracker can capture the event logs that Windows creates when privilege/administrative functions are carried out, such as DNS changes and changes to system files.
3.1.8	Limit unsuccessful logon attempts.	EventTracker provides the capability to alert and report on login failures. Access to the EventTracker console is linked to the Active Directory (AD) with password controls that are generally a function of AD.
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Banner can be displayed upon logon to the console. Baseline configuration checks can determine non-compliant systems.

NIST 800-171 Control Families

Control 3.1: Access Control

NIST 800-171	Control Description	Netsurion Capability
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	EventTracker connection sessions time out after a period of inactivity, which is generally a function of Active Directory. A screensaver hides contents from being viewed.
3.1.11	Terminate (automatically) a user session after a defined condition.	EventTracker sessions time out after a period of inactivity.
3.1.12	Monitor and control remote access sessions.	This control is related to remote access. EventTracker captures and reports on remote desktop sessions and VPN logs. Automated behavioral analysis provides contextual information based on time of data, multiple user connections, and after-hours usage.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	SSL is used to remote access by EventTracker Security Operations Center (SOC) personnel. EventTracker monitors connection type, SSL/ TCP.
3.1.14	Route remote access via managed access control points.	EventTracker provides contextual data on activities from remote access control points for designated systems and produces alerts/reports.
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	EventTracker provides contextual data on activities, and monitors where, when, "who did what?", and "who tried to do what?". Role-based access restricts access to privileged functions.
3.1.16	Authorize wireless access prior to allowing such connections	All network devices, including wireless access can be monitored for admin and other activities. Authorization process requires wireless controller, certificates, and captive portal.
3.1.17	Protect wireless access using authentication and encryption.	The EventTracker agent detects the wireless configuration used by a workstation and will report on the settings of that access point.
3.1.20	Verify and control/limit connections to and use of external information systems.	EventTracker Endpoint Detection and Response can monitor based on network connections and firewall rules and provides contextual data on the use of external systems.
3.1.21	Limit use of organizational portable storage devices on external information systems.	EventTracker agent provides visibility on endpoints for all user activities pertaining to USB devices such as connect/eject, and files copied and provides the ability to block portable storage device.

NIST 800-171 Control Families

Control 3.3: Audit and Accountability

NIST 800-171	Control Description	Netsurion Capability
3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	EventTracker Endpoint Detection and Response fully supports tracking, reporting, and alerting on all audit events generated by host systems. Audit events are those that are significant and relevant to the security of information systems. EventTracker provides a complete package of predefined reports and alerts based on systems/ applications in use. This information is useful for incident response (IR) and demonstrating compliance activities.
3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	EventTracker supports tracking, reporting, and alerting on all audit events generated by host systems. Audit events are events that are significant and relevant to the security of information systems. Host systems audit records generally contain all the information, including timestamp, login id, and status. EventTracker provides a complete package of predefined reports and alerts based on systems/ applications in use. This information is useful in incident response and demonstrating compliance activities, e.g. privilege commands, session information.
3.3.3	Review and update audited events.	The EventTracker Security Operations Center (SOC) provides 24/7/365 monitoring and detection with personnel conducts weekly analysis and performs monthly and quarterly security and risk reviews.

NIST 800-171 Control Families

Control 3.3: Audit and Accountability

NIST 800-171	Control Description	Netsurion Capability
3.3.4	Alert in the event of an audit process failure.	EventTracker Security Operations Center (SOC) Team alerts/reports when audit logs have been received with urgent notification for the highest priority and most suspicious events.
3.3.5	Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	EventTracker Endpoint Detection and Response delivers this service via automated tools and adds the Security Operations Center (SOC) Team to reduce false positives and provide additional context and actionable intelligence. For vulnerability assessment and risk management, the EventTracker supports hundreds of different manufacturer log feeds to provide organization-wide risk awareness across business, information systems, and security. The EventTracker Security Operations Center (SOC) Team provides expertise, discipline, and accountability for analyzing and prioritizing Indicators of Compromise (IoCs).
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	EventTracker provides many standard reports and can create custom reports on an ad-hoc basis. EventTracker also supports customers in the event of an audit or external investigation including exporting of event/log data or real-time discovery via screen sharing with your assigned Security Operations Center (SOC). Additionally, EventTracker provides audit log filtering and reporting capabilities.
3.3.7	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	This is a function of Active Directory. Validation is required on all devices to ensure they are synced correctly.

NIST 800-171 Control Families

Control 3.3: Audit and Accountability

NIST 800-171	Control Description	Netsurion Capability
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	EventTracker has strict security policies in place to prevent unauthorized access to Security Operations Center (SOC) tools. Audit logs are cryptographically hashed upon archiving, and EventTracker agent-based logs are encrypted by default in transit and at rest.
3.3.9	Limit management of audit functionality to a subset of privileged users.	EventTracker Enterprise supports Role-based Access Control (RBAC) that limits access of sensitive information and processes to privileged users with a need to know. EventTracker also enables User & Event Behavioral Analytics (UEBA) to monitor internal user actions and suspicious access.

NIST 800-171 Control Families

Control 3.4: Configuration Management

NIST 800-171	Control Description	Netsurion Capability
3.4.1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	EventTracker provides baseline configuration reports for Windows systems and detects and reports on changes. However, this is one part of configuration management. Baselines may be maintained for each system and deviations from baselines will be documented in EventTracker. EventTracker maintains a classification and categorization register of all assets configured in the IT environment.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	This relates to security settings and require settings to documented, maintained and changes or deviations to security settings to be documented. EventTracker can report on changes to settings dependent upon the type of logs received. The internal vulnerability assessment and configuration management capabilities of EventTracker are required for configuration assessments.

NIST 800-171 Control Families

Control 3.4: Configuration Management

NIST 800-171	Control Description	Netsurion Capability
3.4.3	Track, review, approve/disapprove, and audit changes to information systems.	Audit events and changes can be monitored by the EventTracker Security Operations Center (SOC) Team depending on the log data received. In addition, EventTracker provides a daily snapshot of changes to Windows systems with the Change Audit module.
3.4.8	Apply deny-by-exception (unsafe list) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (safe listing) policy to allow the execution of authorized software.	EventTracker provides operational telemetry to categorize and inventory installed hardware and software, and alerts on non-safe listed applications, suspicious processes, unpatched devices, vulnerabilities, and more.
3.4.9	Control and monitor user-installed software.	EventTracker provides operational telemetry to categorize and inventory installed hardware and software to control and monitor endpoints for user-installed software, applications, suspicious processes, unpatched devices, vulnerabilities, and more.

NIST 800-171 Control Families

Control 3.5: Identification and Authorization

NIST 800-171	Control Description	Netsurion Capability
3.5.1	Identify information system users, processes acting on behalf of users, or devices.	EventTracker agent monitors endpoints for active processes on workstations and servers. The EventTracker SOC team can set alerts based on a custom set of variables.
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	EventTracker can provide log data from Two-Factor Authentication (2FA) systems, such as Okta or Cisco Duo.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	EventTracker logs information relating to privilege, non-privilege access for local and remote accounts. EventTracker also provides Two-Factor Authentication (2FA) as an added layer of security to all users, not just privileged users.

NIST 800-171 Control Families

Control 3.5: Identification and Authorization

NIST 800-171	Control Description	Netsurion Capability
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non- privileged accounts.	Active directory – Kerberos authentication is used as a mechanism for replay protection. Kerberos authentication is logged in Windows and consumed in EventTracker.

NIST 800-171 Control Families

Control 3.6: Incident Response

NIST 800-171	Control Description	Netsurion Capability
3.6.1	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	The EventTracker Security Operations Center (SOC) team works with you to closely define your organizational objectives, establish alert and ticketing methodologies, provide monthly and quarterly analysis of your security posture, monthly and quarterly analysis of vulnerabilities and your risk posture, as well as incident response activities and containment actions with endpoint detection and response (EDR) capabilities.
3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization	Above tools capture who/how/what was investigated, processes, and the tracking and reporting of incidents involving CUI to appropriate officials (an audit trail of the Incident Response flow).
3.6.3	Test the organizational incident response capability.	Informed by EventTracker Logbook (Incidents) and Runbook (ops manual).

NIST 800-171 Control Families

Control 3.7: Maintenance

NIST 800-171	Control Description	Netsurion Capability
3.7.1	Perform maintenance on organizational information systems.	The EventTracker platform monitors systems for out-of-date software and configurations and provides reports and analysis with trends and graphs to track progress.

NIST 800-171 Control Families

Control 3.8: Media Protection

NIST 800-171	Control Description	Netsurion Capability
3.8.2	Limit access to CUI on information system media to authorized users.	Using EventTracker agent to monitor Active Directory and access logs of workstations and servers, the EventTracker SOC Team monitors events 24/7 and provides alerts where unauthorized users have attempted to access CUI on information system media.
3.8.7	Control the use of removable media on information system components.	EventTracker agent provides visibility on endpoints for all user activities pertaining to USB devices, including connect/eject, files copied, and provides the ability to block external storage device.
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	The EventTracker agent can safe list specific USB devices, and alert on non-approved device serial numbers when these are connected to endpoints (workstation, or server).

NIST 800-171 Control Families

Control 3.11: Risk Assessment

NIST 800-171	Control Description	Netsurion Capability
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	EventTracker provides continuous scanning of your internal and external networks and endpoints for vulnerabilities and risks. Your risk posture is monitored 24/7 by the EventTracker Security Operations Center (SOC) team, with monthly and quarterly risk reports reviewed with your IT team.
3.11.2	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	EventTracker Vulnerability Assessment Service (VAS) continually scans internal and external systems for vulnerabilities. The EventTracker agent leverages security controls benchmarking to provide a view into globally accepted configurations and provide analysis of your risk posture.

NIST 800-171 Control Families

Control 3.11: Risk Assessment

NIST 800-171	Control Description	Netsurion Capability
3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	The EventTracker Security Operations Center (SOC) team works with you to prioritize critical vulnerabilities and assist with severity assessment and triage of vulnerabilities. The EventTracker Critical Observations Report (COR) also uses colored risk scoring that simplifies prioritization along with its comprehensive remediation recommendations.

NIST 800-171 Control Families

Control 3.12: Security Assessment

NIST 800-171	Control Description	Netsurion Capability
3.12.1	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	EventTracker Vulnerability Assessment Service (VAS) conducts internal vulnerability assessments and completes host-based scans looking for potential vulnerabilities through security controls benchmarking and recommended configurations.
3.12.3	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	EventTracker agent provides for continuous monitoring of security controls on endpoints such as workstations and servers through security controls benchmarking.

NIST 800-171 Control Families

Control 3.13: System and Communication Protection

NIST 800-171	Control Description	Netsurion Capability
3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	The EventTracker sensor generates net flow data at egress points to the public internet and can also work off span/mirror ports for key internal subnet/VLANs and provide monitoring and alerting based on the net flow data.
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Subnets for publicly accessible system components that are physically or logically separated from internal networks are recommended to all our customers and partners.

NIST 800-171 Control Families

Control 3.13: System and Communication Protection

NIST 800-171	Control Description	Netsurion Capability
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	VoIP traffic can be monitored by an EventTracker Endpoint Detection and Response solution using an internal tap or span/ mirror configuration. If the central server (Call Manager, etc.) is providing logs via syslog, that can be used for additional context and alerting.

NIST 800-171 Control Families

Control 3.14: Systems and Information Integrity

NIST 800-171	Control Description	Netsurion Capability
3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	Detailed technical information on identified vulnerabilities and recommendations are provided by the EventTracker to remediate the vulnerability. Reports of vulnerabilities, including those that relate to specific compliance requirements, are provided by the EventTracker SOC.
3.14.3	Monitor information system security alerts and advisories and take appropriate actions in response.	The EventTracker Endpoint Detection and Response solution ingests audit alerts from other security tools, such as anti-virus and firewalls, etc. Additional user context such as attacker tactics and techniques from the MITRE ATT&CK framework are layered onto the alert, helping you make informed decisions faster.
3.14.6	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	EventTracker monitors various audit logs to alert on unauthorized access and misuse by using the built-in behavioral analysis tool and log correlation capabilities. The agent logs all inbound/ communication and performs analysis to determine threats.
3.14.7	Identify unauthorized use of the information system.	EventTracker monitors various logs and the agent logs perform reputation analysis of threats.

Reference:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

How Netsurion Can Help

Not sure where to being? 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 NIST 800-171 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.