Netsurion™ | EventTracker

FISMA-NIST SP 800-171 Rev.1 Solution Brief

FISMA NIST SP 800-171

www.netsurion.com/eventtracker

About Netsurion

Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion's SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion's SD-WAN edge appliance.

Netsurion's Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.

FISMA NIST SP 800-171 Compliance

Commercial organizations in doing business with the U.S. government, or in possession of U.S. government data, are required to demonstrate NIST 800-171 compliance for protecting the confidentiality of Controlled Unclassified Information (CUI). The CUI requirements within NIST 800-171 are directly linked to NIST 800-53 MODERATE baseline controls, which are intended for use by federal agencies in contracts or other agreements established between those agencies and contractors/suppliers, as it applies to:

- When CUI is in non-federal information systems and organizations;
- When information systems where CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and
- Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry
- The NIST 800-171 requirements apply to all components of non-federal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.

This document provides confidential detail on how EventTracker meets the security monitoring and incident response requirements set out in the standard. Moderate baseline controls listed in NIST 800-53 will be analyzed as 800-171 directly refers to them.

The EventTracker Control Center staff, while working closely with our end user customers, delivers SIEMphonic co-managed services. These services include SIEM administration, and continuous tuning, filtering and analysis using the EventTracker SIEM software platform. The SIEM software captures logs and event data from network and system components, such as operating system logs, application logs, logs from perimeter firewalls, IDS, Antivirus and more. It integrates and correlates inbound data with threat intelligence feeds, reputation indications, application safe-listing, and uses behavioral analysis to automatically provide direct, real-time response/remediation to notify and optionally terminate processes and/or systems that may compromise an organization's security and/or ability to demonstrate compliance with NIST and similar controls.

FISMA NIST 800-171 Control Families

Access Control

NIST 800-171	Control Description	NIST 800-53	EventTracker Capability
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	AC2 Account Management AC-3 Access Enforcement AC-17 Remote Access	Role-based access control Audit Logging/Alerts/Reports Acct management or changes Provides mechanism 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.	AC2 Account Management AC-3 Access Enforcement AC-17 Remote Access	Role based access control Audit logging/Alerts/Reports Acct management or changes
3.1.3	Control the flow of CUI in accordance with approved authorizations.	AC4 Information Flow Enforcement	Monitoring activities for File and Application access; USB monitoring; Email metadata analysis
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC5 Separation of Duties	Provides reporting and alerting on attempts to cross role boundaries and 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.	AC-6 Least Privilege AC-6(1) Authorize Access to Security Functions AC-6(5) Privilege Accounts	Network connection monitoring, application execution, and system logon activities are recorded and monitored.
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	AC-6(2) Non-Privilege access for Non-Security Functions	Process execution, application installs and command execution 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.	AC-6(9) Auditing use of privilege functions AC-6(10) Prohibit non-privileged users from executing privilege functions	EventTracker captures the event logs that Windows creates when privilege/administrative functions are carried out, e.g. DNS changes, changes to system files.
3.1.8	Limit unsuccessful logon attempts.	AC-7 Unsuccessful Logon Attempts	EventTracker provides the capability to alert and report on logon failures. EventTracker console access is linked to AD Password controls. Generally, a function of AD.
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	AC-9 Previous Logon (Access) Notification	Banner can be displayed upon logon to the console. Baseline configuration checks can determine non-compliant systems.

NIST 800-171	Control Description	NIST 800-53	EventTracker Capability
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	AC-11 Session Lock AC-11(1) Pattern hiding Displays	EventTracker supports tracking of user session was locked or unlocked manually or automatically.
3.1.11	Terminate (automatically) a user session after a defined condition.	AC-12 Session Termination	EventTracker supports tracking for user session connected or disconnected for example, local workstations, databases, and password-protected websites/web-based service.
3.1.12	Monitor and control remote access sessions.	AC-17(1) Automated Monitoring Controls	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.	AC-17(2) Protection of Confidentiality / integrity using encryption	SSL is used to remote access by EventTracker Control Center personnel. EventTracker monitors connection type, SSL/TCP.
3.1.14	Route remote access via managed access control points.	AC-17(3) Managed Access Control Points	Support function by providing contextual data on activities on remote access control points for designated systems and produce alerts/reports.
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	AC-17(4) Managed Access Control Points	Support function by providing contextual data on activities. EventTracker monitors where, when and “who did what?” and “who tried to do what?” Role-based access restricts access to privilege functions.
3.1.16	Authorize wireless access prior to allowing such connections	AC-18 Wireless Access	All network devices, including wireless access can be monitored for admin and other activities. Authorization process requires wireless controller, certificates and captive portal.
3.1.20	Verify and control/limit connections to and use of external information systems.	AC-20 Use of external Information systems AC-20 (1) Limit on Authorized Use	EventTracker network connection monitoring and firewall provides contextual data on the use of external systems.
3.1.21	Limit use of organizational portable storage devices on external information systems.	AC-20(2) Portable Storage Devices	EventTracker provides visibility on all user activities pertaining to USB devices, including insert, files copied and provides the ability to block personal thumb drives.

Audit and Accountability

NIST 800-171	Control Description	NIST 800-53	EventTracker 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.	AU-2 Audit Events AU-3 Content of audit records AU-3(1) Additional Audit Information AU-12 Audit Generation	EventTracker 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. Host systems audit records generally contain all the information, such as timestamp, login ID, status, etc. EventTracker provides a complete package of predefined reports and alerts based on systems/ applications in use. This information will be useful in Incident Response and demonstration of Compliance for activities, e.g. privilege commands, session information.
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.	AU-2 Audit Events AU-3 Content of audit records AU-3(1) Additional Audit Information AU-12 Audit Generation	EventTracker fully 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 such as timestamp, login id, status, etc. EventTracker provides a complete package of predefined reports and alerts based on systems/ applications in use. This information will be useful in Incident Response and demonstration of Compliance for activities, e.g. privilege commands, session information.
3.3.3	Review and update audited events.	AU-2(3) Reviews and Updates	EventTracker Weekly analysis and Monthly reviews will fine tune, remove noise, etc.
3.3.4	Alert in the event of an audit process failure.	AU-5 Response to audit processing failures	EventTracker alerts/reports if audit logs have been received.
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.	AU-6(1) Process Integration AU-6(3) Correlate audit repositories	EventTracker supports hundreds of different manufacturer log feeds to provide wide organization risk awareness across business, information systems and security. The EventTracker Control Center (SIEMphonic) provides expertise, discipline and accountability for analyzing and prioritizing indications of compromise.

NIST 800-171	Control Description	NIST 800-53	EventTracker Capability
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	AU-7 Audit Reduction and report generation	EventTracker provides 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.	AU-8 Time Stamps AU-8(1) Synchronization with authorized time source	This is a function of Active Directory. Validation is required on all devices to ensure they are synced correctly.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	AU-9 Protection of Audit Information	Logs are cryptographically hashed upon archiving. Agent-based logs can be encrypted in transit – FIPS 140-2.
3.3.9	Limit management of audit functionality to a subset of privileged users.	AU-9(4) Access by subset of privileged users	The EventTracker console supports role-based, granular access.

Configuration Management

NIST 800-171	Control Description	NIST 800-53	EventTracker 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.	CM-2 Baseline Configuration CM-6 Configuration Settings CM-8 Information System component inventory CM-8(1) Updates during installations/Removals	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 register of all assets configured.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	CM-2 Baseline Configuration CM-6 Configuration Settings CM-8 Information Systems component inventory CM-8(1) Updates during installations/Removals	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. EventTracker Internal Vulnerability Scans and Configuration Management options are required.
3.4.3	Track, review, approve/disapprove, and audit changes to information systems.	CM-3 Configuration change control	Dependent on the logs received, audits events to changes can be monitored. In addition, EventTracker provides daily snapshot of changes to Windows systems with the Change Audit module.
3.4.9	Control and monitor user-installed software.	CM-11 User installed Software	EventTracker alerts and reports on user-installed software.

Identification and Authorization

NIST 800-171	Control Description	NIST 800-53	EventTracker Capability
3.5.1	Identify information system users, processes acting on behalf of users, or devices.	IA-2 Identification and Authorization (organizational users) IA-5 Authenticator Management	For all systems (and dependent of log feeds) EventTracker reports on user actions and processes.
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	IA-2 Identification and Authorization (organizational users) IA-5 Authenticator Management	For all systems (and dependent of log feeds) EventTracker reports on user actions and processes.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA-2(1) Network access to privilege users IA-2(2) Network access to non-privilege users IA-2(3) Local access to privilege accounts	EventTracker logs information relating to privilege, non-privilege access for local and remote accounts.
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	IA-2(8) Network access to privilege accounts -Replay protection IA-2(9) Network access to non-privilege accounts - Replay protection	Active directory – Kerberos authentication is used as a mechanism for replay protection. Kerberos authentication is logged in windows and consumed in EventTracker

Incident Response

NIST 800-171	Control Description	NIST 800-53	EventTracker 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.	IR-2 Incident Response Training IR-4 Incident Handling IR-5 Incident Monitoring IR-6 Incident Reporting IR-7 Incident Response Assistance	EventTracker provides the IR tools (flagging, escalation, acknowledgement) and processes, detailed logbooks for investigations, and detailed runbooks to fully operationalize incident handling.
3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization	IR-2 Incident Response Training IR-4 Incident Handling IR-5 Incident Monitoring IR-6 Incident Reporting IR-7 Incident Response Assistance	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 IR flow).
3.6.3	Test the organizational incident response capability.	IR-3 Incident Response Testing IR-3(2) Coordinated with related plans	Informed by EventTracker logbook (Incidents) and runbook (ops manual).

Systems and Communication protection

NIST 800-171	Control Description	NIST 800-53	EventTracker Capability
3.14.7	Identify unauthorized use of the information system.	SI-4 Inbound and Outbound Communication traffic	EventTracker monitors various logs to alert on unauthorized access and misuse by using the built-in behavioral analysis tool and log correlation. The agent logs all inbound/communication and performs reputational analysis of external connections to determine threats.

References:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

http://csrc.nist.gov/publications/nistpubs/800-171r1/sp800-171r1-excerpt.pdf