

FISMA-NIST SP 800-53 Rev.4 Solution Brief

About EventTracker

EventTracker delivers business critical solutions that transform high-volume cryptic log data into actionable, prioritized intelligence that will fundamentally change your perception of the utility, value and organizational potential inherent in log files. EventTracker's leading solutions offer Security Information and Event Management (SIEM), real-time Log Management, and powerful Change and Configuration Management to optimize IT operations, detect and deter costly security breaches, and comply with multiple regulatory mandates. With this, it ensures successful protective monitoring and complies with the FISMA NIST SP 800 requirements.

FISMA NIST SP 800-53 Compliance

NIST Special Publication 800-53, Revision 4, signifies the most comprehensive update to the security controls catalog since its inception in 2005. The publication was effectively developed by NIST, the Department of Defense, the broader intelligence Community, and the Committee on National Security Systems as part of the Joint Task Force partnership put together in approximately 2009. Moreover, the update was motivated primarily by the increasing cybersecurity threats, attacks, and other malicious activities seen today. NIST Special Publication 800 53, Revision 4 is incredibly dense, detailed, and in-depth, covering numerous areas relating to the broader subject of information security

Additionally, historical publications of NIST SP 800-53, specifically Rev. 3, "Recommended Security Controls for Federal Information Systems and Organizations" have become the standard for FISMA compliance and also for implementing overall information security best practices. NIST Special Publication 800-53, Revision 4, is a major leap forward into the world of cybersecurity – a must-read for any organization serious about ensuring the safety and security of one's critical system resources.

EventTracker Offers Full View of Entire IT Infrastructure

EventTracker improves security, maintains compliance and increases operational efficiency. EventTracker can be deployed On-Premises for customers who prefer their equipment to reside in their data center. EventTracker is a software-based SIEM and log management solution that resides in a Windows Server environment. EventTracker may also be deployed in a virtual environment using VMware. In both cases, On-Premises installation implies that the EventTracker software resides at the customer's location in some form or fashion.

For some customers, the space requirements, manpower issues, or lack of technical expertise make a cloud-hosted solution more attractive, and EventTracker is deployed in a Tier 1 EventTracker data center. EventTracker will manage the following:

- Secure Virtual Private Cloud (single tenant) environment
- Installation
- Server disk space
- Platform management
- Antivirus installation and updates
- Windows updates
- Back-up/restore

EventTracker SIEM enables your organization to be aware of potential security risks and internal/external threats that can be identified and eliminated before they are exploited. It guarantees your organization the ability to respond to a security incident and have the necessary data and tools for forensic analysis. The total time required to investigate and mitigate a security incident can be reduced by up to 75 percent, minimizing the potential exposure and costs.

SIEMphonic is our professional services engagement to enhance the value of the EventTracker SIEM and EventTracker SIEM products. Our experienced staff assumes responsibility for all SIEM related tasks including daily incident reviews, daily/weekly log reviews, configuration assessments, incident investigation support and audit support. We augment your IT team, allowing you to focus on the unique requirements of your SIEM, while actively leveraging our expertise.

Strong Access Control policy and procedures

EventTracker SIEM enables automatic, unattended consolidation of millions of events in a secure environment along with incrementally scalable to meet the needs of any size organization. It also supports an infinite number of collection points, with each collection point able to process over 100,000 events per second. All this data is identified by the product based Knowledge Base, which contains detailed information on over 20,000 types of events, and automatically determines which logs are alerts, which are incidents, and which can be ignored.

Log Collection includes a flexible, agent-optional architecture providing managed real-time and batch aggregation of all system, event and audit logs. EventTracker SIEM supports UDP and TCP (guaranteed delivery) log transport and is FIPS 140-2 compliant for transmission of events from agent/collection point to console.

EventTracker complies with OWASP guidelines which enforce the product to have a strong authentication and authorization mechanisms in order to restrict the user access. It incorporates default deny policy bringing more security to customers. It monitors changes on the file system and in the system registry of a Windows system and substantially improves corporate security and availability.

EventTracker SIEM provides customizable, role-based dashboards that allow organizations to control the information visible to a user based on their role in the organization. It also allows users to remove the information they do not want to see, and rearrange the location of the information on the dashboard. For example, a system administrator may only have access to the information on the ten servers they are responsible for maintaining, while the director of security will see the relevant information concerning the entire infrastructure.

EventTracker monitors all administrators and users activities for all critical file and folder access on all servers. It monitors successful and failed logon attempts to all servers either locally or remotely. Each EventTracker user has specific user credentials and permissions. With the authentication and authorization mechanism implemented by EventTracker, access privileges are controlled.

Ease of Deployment and Scalability

EventTracker Cloud is a highly scalable SIEM and log management solution that offers several deployment options to meet the needs of small organizations with a few dozen critical systems, as well as larger organizations with thousands of systems spread across multiple locations.

Available as an option with EventTracker SIEM, Behavior Analysis enables you to quickly detect and address changes in system and user behaviors. Automatic baseline learning or flexible rules definitions determine your thresholds for alerting on anomalies in your infrastructure. Real-time processing and correlation give you the complete picture of what's new and different.

Ease of FISMA Reporting and Alerting

EventTracker has developed specific reports, rules and dashboards to help meet the Security controls detailed within FISMA-NIST. These reports, rules and dashboards can be easily and intuitively customized for specific environments.

Real-time Monitoring, Account and Configuration Management

The file system and registry of every Windows system is ever-changing. This change may be voluntary or involuntary and happens quickly and often without the user's knowledge. Under the current Windows OS architecture there is no easy way for the user to understand change, identify change and recover from change.

Change Management is a concept by which all system changes are intelligently tracked and reported on demand for the user to analyze, understand, and if needed, recover from change. EventTracker SIEM alerts you to the critical changes you need to know. EventTracker monitors unauthorized software install / uninstall on all servers. It monitors all the Agents and configuration changes on critical file and database servers. Also enforces system and application policies on critical servers using Change Audit and periodically compare policy. It monitors all security patches and updates to servers.

EventTracker SIEM Change Audit is fully integrated into the EventTracker SIEM architecture. EventTracker SIEM stores all the change audit data as both system snapshots for later comparisons and as events in EventVault. Change events can have rules written against them to trigger alerts or any other action available in EventTracker SIEM.

Protect Data and Information

As security with its first and foremost priority, EventTracker monitors network connections on all windows servers and firewall activity. Also monitors for changes or unauthorized access to routers and switches.

EventTracker SIEM is capabilities-rich, with key features that expand its competences beyond SIEM and log management. These include File Integrity Monitoring, Change Audit, Config Assessment, Cloud Integration, Event Correlation, and writeable media monitoring.

EventTracker safeguards data by ensuring stringent rules against unknown authentication and authorization. EventTracker monitors access to file and database servers. Also it monitors configuration changes on critical file and database servers and alerts the responsible to take further action. EventTracker SIEM also has an optimized, high performance event warehouse that is designed for efficient storage and retrieval of event logs. It reliably and efficiently archives event logs from across the SIEM without the need for any DBMS licenses or other overhead costs. And these logs are compressed and sealed with a SHA-1 signature to prevent potential tampering.

Statement of Compliance – FISMA NIST 800–53

Access Control

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>AC-2 – Account Management</p> <p>The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts.</p>	<p>EventTracker collects all account management activities which get generated in the system. EventTracker reports provide easy and standard review of all account management activity and also EventTracker Alert can detect any changes to Account Management.</p>	Yes	Yes
<p>AC-3 – Access Enforcement</p> <p>The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.</p>	<p>EventTracker collects all access activities which get generated in the system. EventTracker reports provide easy and independent review of access control settings and enforcement.</p>	Yes	Yes
<p>AC-5 – Separation of Duties</p> <p>The information system enforces separation of duties through assigned access organizations.</p>	<p>EventTracker collects information from production access control systems to help define role usage requirements, determine attempts to cross role boundaries, and changes to configurations that can affect separation of duties.</p>	Yes	Yes
<p>AC-6 – Least Privilege</p> <p>The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.</p>	<p>EventTracker monitors activities of both users and systems to assist in determining necessary access, frivolous access, and resource needs of production systems. Review of activities such as network connections, application access, and system logons can help identify appropriate and inappropriate use according to policy.</p>	Yes	Yes
<p>AC-7 – Unsuccessful Login Attempts</p> <p>The information system enforces a limit of specific number of consecutive invalid access attempts by a user within a certain time period. The information system automatically locks the account for a specified time period and delays next login prompt after a set timeframe has expired.</p>	<p>EventTracker collects all authentication activities which get generated in the system. EventTracker reports provide easy and standard review of unsuccessful login attempts to systems and applications. EventTracker alerts can detect & report on multiple unsuccessful login attempts.</p>	Yes	Yes
<p>AC-17 – Remote Access</p> <p>The organization authorizes, monitors, and controls all methods of remote access to the information system.</p>	<p>EventTracker collects all account management activities which get generated in the system. EventTracker reports provide easy and standard review of all account management activities.</p>	Yes	Yes
<p>AC-18 – Wireless Access Restriction</p> <p>The organization:</p> <ul style="list-style-type: none"> Establishes usage restrictions and implementation guidance for wireless technologies; and Authorizes, monitors, controls wireless access to the information system. 	<p>EventTracker collects all access activities which get generated in the system. EventTracker reports provide easy and independent review of access control settings and enforcement.</p>	Yes	Yes

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>AC-19-Access Control for Portable and Mobile Systems</p> <p>The organization:</p> <ul style="list-style-type: none"> Establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and Authorizes, monitors, and controls device access to organizational information systems. 	<p>EventTracker’s entity and network definitions allow for correlation and event monitoring based on location relative to the organizational networks, to determine inbound, outbound, and local network traffic. Remote access and usage activities from mobile devices can be monitored by observation of the logs from authentication systems, security systems and production servers.</p>	Yes	Yes
<p>AC-20 – Personally Owned Information Systems/Use of External Information Systems</p> <p>The organization establishes terms and conditions for authorized individuals to:</p> <ul style="list-style-type: none"> Access the information system from an external information system; and Process, Store, and/or transmit organization-controlled information using an external information system. 	<p>EventTracker collects remote access activities which get generated in the system. EventTracker analysis facilities and reports provide easy and independent review of external access to information systems.</p>	Yes	Yes

Audit and Accountability

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>AU-4 – Audit Storage Capacity</p> <p>The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.</p>	<p>EventTracker provides central, secure, and independent audit log storage EventTracker’s high compression of the data (> 80%) ensures extensible storage of audit log data, ensures capacity will not be exceeded.</p>	Yes	Yes
<p>AU-5 – Response to Audit Processing Failures</p> <p>The information system alerts designated organizational officials in the event of an audit processing failure.</p>	<p>EventTracker provides support for NIST 800-53 control enhancement AU-5.</p> <ul style="list-style-type: none"> By completely automating the process of centrally collecting and retaining all audit log messages. EventTracker core functionality provides alerting for audit storage over utilization. EventTracker also provides direct support for NIST 800-53 control enhancement AU-5. By collecting and analyzing audit processing failure logs. EventTracker provide alerting on processing failure activity including audit log clearing, audit logging stoppage, and failed audit log writes. EventTracker investigations, reports, and tails provide evidence of audit processing failure activity including audit log clearing, audit logging stoppage, and failed audit log writes. 	Yes	Yes

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>AU-6 – Audit Monitoring, Analysis, and Reporting</p> <p>The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, report findings to appropriate officials, and takes necessary actions.</p>	<p>EventTracker provides centralized monitoring, analysis, and reporting of audit activity across the entire IT infrastructure. EventTracker automates the process of identifying high-risk activity and prioritizes based on asset risk. High-risk activity can be monitored in real-time or alerted on. EventTracker reports provide easy and standard review of inappropriate, unusual, and suspicious activity.</p>	Yes	Yes
<p>AU-7 – Audit Reduction and Report Generation</p> <p>The information system provides an audit reduction and report generation capability.</p>	<p>EventTracker’s policy based log processing capabilities provide automatic audit log reduction. “Interesting” audit logs can be forwarded as events for immediate monitoring and/or alerting. “Uninteresting” audit logs can be filtered out and/or retained at an archive-only level. EventTracker analysis and reporting facilities provide aggregated views of audit data providing further audit reduction. EventTracker provides extensive report generation capabilities.</p>	Yes	Yes
<p>AU-8 – Time Stamps</p> <p>The information system provides time stamps for use in audit record generation.</p>	<p>EventTracker collects all user access events logs in real-time and retains the date and time stamp in which they occurred.</p>	Yes	Yes
<p>AU-9 – Protection of Audit Information</p> <p>The information system protects audit information and audit tools from unauthorized access, modification, and deletion.</p>	<p>EventTracker provides central and secure storage of all audit log data.</p>	Yes	Yes
<p>AU-11 – Audit Retention</p> <p>The organization retains audit records for an appropriate time period to provide support for after the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.</p>	<p>EventTracker completely automates the process and requirement of collecting and retaining audit logs. EventTracker retains logs in compressed archive files, easy-to-manage, long-term storage. Log archives can be restored quickly and easily months or years later in support of after-the-fact investigations</p>	Yes	Yes
<p>AU-13 – Monitoring for Information Disclosure</p> <p>The organization monitors open source information for evidence of unauthorized ex-filtration or disclosure of organizational information.</p>	<p>EventTracker provides support for NIST 800-53 control requirement AU-13 by utilizing the EventTracker feature of the Windows System Monitor. EventTracker’s independently monitors and logs the connection and disconnection of external data devices to the host computer where the Agent is running. Also monitors and logs the transmission of files to an external storage device. It can be configured to protect against external data device connections by ejecting specified devices upon detection. External USB drive storage devices include Flash/RAM drives and CD/DVD drives.</p>	Yes	Yes

Security Assessment and Authorization

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>CA-2 – Security Assessments</p> <p>The organization conducts an assessment of the security controls in the information system periodically to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system</p>	<p>EventTracker’s log analysis and reporting capabilities can be leveraged during a security assessment to help ensure implemented controls are functioning as intended and to potentially identify any weaknesses.</p>	Yes	Yes
<p>CA-3 – Information System Connections</p> <p>The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis</p>	<p>EventTracker can collect network device logs and also EventTracker’s Network Connection Monitoring feature will identify the network connections established. EventTracker’s analysis & reporting capabilities can be used for reviewing network activity to ensure only authorized communications occur. EventTracker alerts can be used for detecting unauthorized communications.</p>	Yes	Yes
<p>CA-7 – Continuous Monitoring</p> <p>The organization monitors the security controls in the information system on an ongoing basis.</p>	<p>EventTracker’s monitoring, analysis, and reporting capabilities provide for continuous monitoring of specific controls across the IT infrastructure. For instance, EventTracker alerts can detect the use of restricted accounts.</p>	Yes	Yes

Configuration Management

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>CM-3 – Configuration Change Control</p> <p>The organization: Audits activities associated with configuration-controlled changes to the system.</p>	<p>EventTracker provides support for NIST 800-53 control requirement CM-3 by collecting and analyzing all configuration change logs. EventTracker provide alerting on configuration/policy changes on critical systems. EventTracker investigations, reports, and tail provide evidence of configuration/policy changes.</p>	Yes	Yes
<p>CM-4 – Monitoring Configuration Changes</p> <p>The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.</p>	<p>EventTracker’s monitoring capability can be used to detect the following changes to the file system:</p> <ul style="list-style-type: none"> • Additions • Deletions • Modifications • Permissions <p>EventTracker analysis & reporting capabilities can be used for monitoring configuration changes. EventTracker alerting can be utilized to detect and notify of changes to specific configurations.</p>	Yes	Yes

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>CM-5 – Access Restrictions for Change</p> <p>The organization:</p> <ul style="list-style-type: none"> • approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and • Generates, retains, and reviews record reflecting all such changes 	<p>EventTracker collects all access activity and changes to access controls. EventTracker reports provide easy and independent review of access control settings and enforcement.</p>	Yes	Yes
<p>CM-6 – Configuration Settings</p> <p>The organization: Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures</p>	<p>EventTracker provides support for NIST 800-53 control requirement CM-6 by collecting and analyzing all configuration change logs. EventTracker provide alerting on configuration/policy changes on critical systems. EventTracker investigations, reports, and tails provide evidence of configuration/policy changes.</p>	Yes	Yes
<p>CM-11 – User Installed Software</p> <p>The organization enforces explicit rules governing the installation of software by users.</p>	<p>EventTracker’s monitoring, analysis, and reporting capabilities provide for continuous monitoring of specific controls across the IT infrastructure. For instance, EventTracker alerts can detect the use of restricted accounts.</p>	Yes	Yes

Contingency Planning

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>CP-9 – Information System Backup</p> <p>The organization:</p> <ul style="list-style-type: none"> • Conducts backups of user-level information contained in the information system • Conducts backups of system-level information contained in the information system • Conducts backups of information system documentation including security related documentation 	<p>EventTracker provides support for NIST 800-53 control requirement CM-9 by collecting and analyzing all software backup logs. EventTracker provide alerting on backup failures. EventTracker investigations, reports, and tails provide evidence of backup failures/success.</p>	Yes	Yes

Identification and Authentication

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>IA-2 – Identification and Authentication (Organizational Users)</p> <p>The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).</p>	EventTracker provides support for NIST 800-53 control requirements IA-2 by collecting and analyzing all authentication logs. EventTracker provide alerting on authentication failures. EventTracker investigations, reports, and tails provide evidence of all account authentication activity.	Yes	Yes
<p>IA-3 – Device Identification and Authentication</p> <p>The information system uniquely identifies and authenticates before establishing a connection.</p>	EventTracker provides support for NIST 800-53 control requirements IA-3 by collecting and analyzing all authentication logs. EventTracker provide alerting on vendor default account authentications. EventTracker investigations, reports, and tails provide evidence of all account authentication activity including those from vendor default accounts.	Yes	Yes
<p>IA-8 – Identification and Authentication (Non-Organizational Users)</p> <p>The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).</p>	EventTracker provides support for NIST 800-53 control requirements IA-8 by collecting and analyzing all authentication logs. EventTracker provide alerting on vendor or 3rd party account authentication failures. EventTracker investigations, reports, and tails provide evidence of all account authentication activity including those from vendor or 3rd party accounts.	Yes	Yes

Incident Response

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>IR-4 – Incident Handling</p> <p>The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.</p>	EventTracker provides support for NIST 800-53 control enhancement IR-4 by detecting and notifying individuals of activity that may constitute an incident. EventTracker’s analysis capabilities provide quick & easy analysis of activity to determine the incidents. EventTracker provides correlation, pattern recognition, and behavioral analysis. EventTracker’s integrated knowledge base provides information useful in responding to and resolving the incident.	Yes	Yes
<p>IR-5 – Incident Monitoring</p> <p>The organization tracks and documents information system security incidents</p>	EventTracker provides direct support for NIST 800-53 control requirements IR-5 by providing security incident tracking and documentation through the EventTracker management interface.	Yes	Yes
<p>IR-6 – Incident Reporting</p> <p>The organization promptly reports incident information to appropriate authorities</p>	EventTracker’s notification capabilities can route alerts to the appropriate individual based on group membership or relationship to the impacted system. EventTracker reports provide summary and detail level reporting of incident based alerts.	Yes	Yes
<p>IR-7 – Incident Response Assistance</p> <p>The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization’s incident response capability.</p>	EventTracker’s integrated knowledge base provides information useful in responding to and resolving incidents.	Yes	Yes

Maintenance

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>MA-2 – Controlled Maintenance The organization Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.</p>	EventTracker provides support for NIST 800-53 control requirement MA-2 by collecting and analyzing all error logs. EventTracker provide alerting on critical maintenance errors. EventTracker investigations, reports, and tails provide evidence of critical errors, process shutdowns, and system shutdowns which occur after maintenance.	Yes	Yes
<p>MA-4 – Remote Maintenance The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.</p>	EventTracker can identify maintenance related activity for analysis and/or reporting. EventTracker reports provide easy review of remotely executed maintenance activity.	Yes	Yes
<p>MA-5 – Maintenance Personnel The organization allows only authorized personnel to perform maintenance on the information system.</p>	EventTracker can identify maintenance related activity for analysis and/or reporting. EventTracker reports provide easy review of maintenance activity.	Yes	Yes

Media Protection

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>MP-2 – Media Access The organization restricts access to organization-defined types of digital and non-digital media to organization-defined list of authorized individuals using organization-defined security measures.</p>	EventTracker provides support for NIST 800-53 control requirement MP-2 by utilizing the EventTracker feature of the Windows System Monitor. EventTracker’s monitors and logs the connection and disconnection of external data devices to the host computer where the Agent is running, also monitors and logs the transmission of files to an external storage device. EventTracker can be configured to protect against external data device connections by ejecting specified devices upon detection. External USB drive storage devices include Flash/RAM drives and CD/DVD drives.	Yes	Yes

Physical Environmental Protection

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>PE-3 – Physical Access Control The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).</p>	EventTracker provides support for NIST 800-53 control requirement PE-3 by collecting log messages from physical access devices (i.e. Card Key) at all physical access points. EventTracker provide alerting on suspicious physical access. EventTracker investigations, reports, and tails provide evidence of physical access failures/successes.	Yes	Yes

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>PE-5 – Access Control for Output Devices The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.</p>	<p>EventTracker provides support for NIST 800-53 control requirement MP-2 by utilizing the EventTracker feature of the Windows System Monitor. EventTracker’s monitors and logs the connection and disconnection of external data devices to the host computer where the Agent is running, also monitors and logs the transmission of files to an external storage device. EventTracker can be configured to protect against external data device connections by ejecting specified devices upon detection. External USB drive storage devices include Flash/RAM drives and CD/DVD drives.</p>	Yes	Yes
<p>PE-6 – Monitoring Physical Access The organization monitors physical access to the information system to detect and respond to physical security incidents.</p>	<p>EventTracker can collect log messages from physical access devices (i.e. Card Key) for analysis and reporting.</p>	Yes	Yes

Personal Security

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>PS-4 – Personnel Termination The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.</p>	<p>EventTracker reports provide easy review of terminated personnel to ensure access rights have been removed. EventTracker alerts can be used to detect usage of should-be terminated user accounts.</p>	Yes	Yes
<p>PS-5 – Personnel Transfer The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.</p>	<p>EventTracker reports provide easy review of transferred personnel to ensure access rights have been terminated and/or appropriately modified.</p>	Yes	Yes
<p>PS-7 – Third-Party Personnel Security The organization Monitors provider compliance.</p>	<p>EventTracker provides support for NIST 800-53 control requirement PS-7 by collecting both physical and logical access control log messages. EventTracker investigations, reports, and tails provide evidence of revocation of cyber/physical access including access revocation, account deletion/modification, account disabling, and account locking for 3rd parties.</p>	Yes	Yes

Risk Assessment

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>RA-5 – Vulnerability Scanning</p> <p>The organization:</p> <ul style="list-style-type: none"> Scans for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported. Analyzes vulnerability scan reports and results from security control assessments. 	<p>EventTracker ETVAS provides support for NIST 800-53 control requirement RA-5 by collecting vulnerability detection log messages. EventTracker provide alerting on high risk vulnerabilities. EventTracker investigations, reports, and tails provide evidence of security vulnerabilities from vulnerability detection systems.</p>	Yes	Yes

System and Communications Protection

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>SC-5 – Denial of Service Protection</p> <p>The information system protects against or limits the effects of the following types of denial of service attacks (organization-defined list of types of denial of service attacks or reference to source for current list).</p>	<p>EventTracker provides support for NIST 800-53 control requirement SC-5 by providing central collection and monitoring of security log messages. EventTracker provide alerting on security events like any out of ordinary behavior in the environment. EventTracker investigations, reports, and tails provide evidence of security events.</p>	Yes	Yes
<p>SC-7 – Boundary Protection</p> <p>The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.</p>	<p>EventTracker can collect boundary device logs from routers, firewalls, VPN servers, etc. EventTracker can alert on unauthorized or suspicious activity. EventTracker reports provide a consolidated review of internal/external boundary activity and threats.</p>	Yes	Yes
<p>SC-15 – Collaborative Protection</p> <p>The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.</p>	<p>EventTracker will be able to identify report and/or alert on the initiation of specific collaborative computing activity.</p>	Yes	Yes
<p>SC-18 – Mobile Code</p> <p>The organization:</p> <ul style="list-style-type: none"> Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously. Authorizes, monitors, and controls the use of mobile code within the information system. 	<p>EventTracker will be able to identify report and/or alert on specific mobile code activity.</p>	Yes	Yes

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>SC-19 – Voice over Internet Protocol The organization:</p> <ul style="list-style-type: none"> Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously Authorizes, monitors, and controls the use of VoIP within the information system. 	<p>EventTracker will be able to identify report and/or alert on specific VoIP activity.</p>	<p>Yes</p>	<p>Yes</p>
<p>SC-28 – Protection of Information at Rest The information system protects the confidentiality and integrity of information at rest.</p>	<p>EventTracker provides supplemental support for NIST 800-53 control requirement SC-28 by providing details of changes to information at rest. EventTracker can be configured to monitor system file or directory activity, deletions, modification, and permission changes.</p>	<p>Yes</p>	<p>Yes</p>

System and Information Integrity

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>SI-2 – Flaw Remediation The organization identifies, reports, and corrects information system flaws.</p>	<p>EventTracker provides support for NIST 800-53 control requirement SI-2 by collecting and analyzing all error logs. EventTracker provide alerting on critical errors caused by flaws. EventTracker investigations, reports, and tails provide evidence of critical errors, process shutdowns, and system shutdowns caused by system flaws.</p>	<p>Yes</p>	<p>Yes</p>

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>SI-3 – Malicious Code Protection</p> <p>The organization:</p> <ul style="list-style-type: none"> • Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: <ul style="list-style-type: none"> – Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or – Inserted through the exploitation of information system vulnerabilities; • Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; • Configures malicious code protection mechanisms to: <ul style="list-style-type: none"> – Perform periodic scans of the information system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy – Block malicious code; quarantine malicious code; send alert to administrator in response to malicious code detection 	<p>EventTracker provides support for NIST 800-53 control requirement SI-3 by collecting log messages from antivirus software and other anti-malware tools. EventTracker provide alerting on antivirus critical/error conditions, malware infections, and signature update failures. EventTracker investigations, reports, and tails provide evidence of antivirus activity, malware infections, and signature update failures/successes. EventTracker feature of the Windows System Monitor. EventTracker’s independently monitors and logs the connection and disconnection of external data devices to the host computer where the Agent is running. Also monitors and logs the transmission of files to an external storage device. It can be configured to protect against external data device connections by ejecting specified devices upon detection. External USB drive storage devices include Flash/RAM drives and CD/DVD drives.</p>	Yes	Yes
<p>SI-4 – Information System Monitoring</p> <p>Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system.</p>	<p>EventTracker can collect logs from IDS/IPS systems, A/V systems, firewalls, and other security devices. EventTracker provides central analysis and monitoring of intrusion related activity across the IT infrastructure. EventTracker can correlate activity across user, origin host, impacted host, application and more. EventTracker can be configured to identify known bad hosts and networks. EventTracker’s Personal Dashboard provides customized real-time monitoring of events and alerts. EventTracker’s Investigator provides deep forensic analysis of intrusion related activity. EventTracker’s integrated knowledge base provides information and references useful in responding to and resolving intrusions.</p>	Yes	Yes

FISMA-NIST Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
<p>SI-5 – Security Alerts and Advisories The organization receives information system security alerts/advisories on a regular basis, issue alerts/ advisories to appropriate personnel, and takes appropriate actions in response.</p>	<p>EventTracker can alert on specific intrusion related activity. Users can be notified based on department or role. EventTracker’s integrated knowledge base provides information and references useful in responding to and resolving intrusions.</p>	Yes	Yes
<p>SI-7 – Software and Information Integrity The information system detects and protects against unauthorized changes to software and information.</p>	<p>EventTracker’s monitoring capability can be used to detect the following changes to the file system:</p> <ul style="list-style-type: none"> • Additions • Deletions • Modifications • Permissions <p>This capability can be used to detect unauthorized changes to software and information.</p>	Yes	Yes
<p>SI-8 – Spam Protection The organization employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.</p>	<p>EventTracker provides support for NIST 800-53 control requirement SI-8 by collecting and analyzing SPAM logs. EventTracker investigations, reports, and tails provide evidence of SPAM protection activity.</p>	Yes	Yes
<p>SI-11 – Error Handling The information system identifies potentially security-relevant error conditions.</p>	<p>EventTracker provides support for NIST 800-53 control requirement SI-11 by collecting and analyzing all error logs. EventTracker provide alerting on security related critical errors. EventTracker investigations, reports, and tails provide evidence of security related errors, process shutdowns, and system shutdowns.</p>	Yes	Yes

References:

- <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53.pdf>