EventTracker
Actionable Security Intelligence

NIST Risk Management Framework (RMF) Solution Brief

EventTracker | 8815 Centre Park Drive, Columbia MD 21045

NIST Risk Management Framework (RMF)

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.

NIST Risk Management Framework

NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems", developed by the Joint Task Force Transformation Initiative Working Group, transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF).

The Risk Management Framework (RMF), illustrated at right, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

The RMF steps include:

Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.

Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

Implement the security controls and describe how the controls are employed within the information system and its environment of operation.

Assess the security controls using appropriate assessment procedures 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.

Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.Strong Access Control policy and procedures

Eventtracker and the NIST Risk Management Framework

EventTracker helps in implementing the NIST Risk Management Framework. The RMF (Special Publication 800-37) provides a framework for federal organizations to classify and protect information systems:

The RMF is conceptually quite simple and reasonable:

- Categorize systems and data based on sensitivity.
- Select appropriate controls from the SP 800-53 control set based on the sensitivity.
- Implement the controls.
- Audit the controls and remediate "significant findings".
- Authorize the resulting control package to make sure risk posture is understood and acknowledged.
- Monitor and audit the controls, and remediate deficiencies as they are found.

As with 800-53 itself, the challenge is implementing the RMF at scale without incurring unacceptable costs or wasting resources on controls that do little to actually reduce risk.

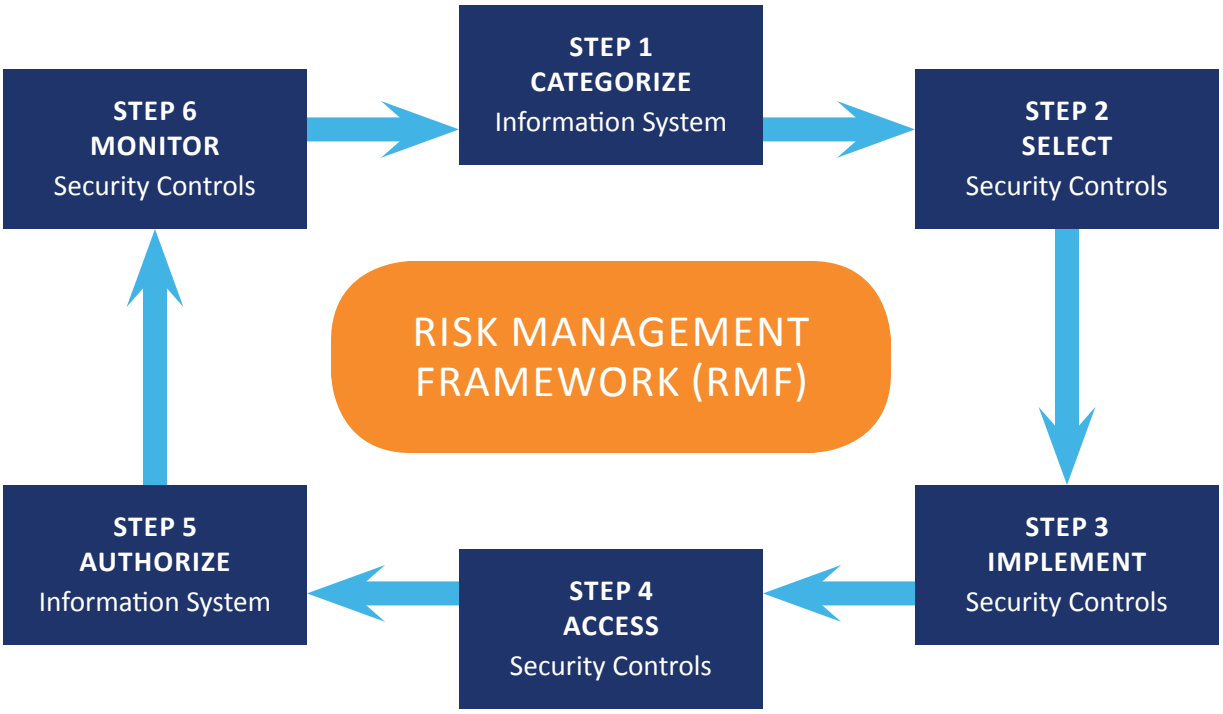
In the context of the Risk Management Framework however, EventTracker is also extremely relevant for monitoring requirements mentioned in Step 6. It is worth reviewing the guidance provided in the NIST RMF for this step:

"Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program."

EventTracker's ability to automate the assessment of network based controls on a continuous basis is essential to meeting this requirement efficiently. The manual effort required is overwhelming and beyond the resources of practically all organizations. It is also very error prone. Realistically what happens is that the network controls are not properly assessed given the amount of change in the environment and the size of the effort. This leads to actual increase in risk, not simply an audit finding. EventTracker addresses this issue by providing daily analysis of network segmentation efficacy along with detailed, actionable reporting on control deficiencies.

In addition, EventTracker helps constrain the resources required for continuous monitoring by justifying smaller subsets of controls and audit frequency for ongoing monitoring. The RMF states that the subset and monitoring frequency should be selected "based on the monitoring strategy developed by the information system owner or common control provider and approved by the authorizing official and senior information security officer." (SP 800-37, pg. 39).

Because EventTracker implements a systematic, comprehensive and repeatable process for its monitoring strategy, it provides the justification required to limit the control subset for periodic assessments (audits), decreasing effort.



Finally, EventTracker's automated approach to continuous monitoring supports reuse of assessment results, because result validation is maintained daily. This further decreases effort, as stated clearly in the RMF:

"Reuse of assessment information is critical in achieving a cost-effective, fully integrated security program capable of producing the needed evidence to determine the security status of the information system. The use of automation to support security control assessments facilitates a greater frequency and volume of assessments that is consistent with the monitoring strategy established by the organization."

Summary

With more emphasis on leveraging technology to improve intra-agency and inter-agency collaboration (specified in current FISMA guidelines), the federal government is placing a greater sense of urgency on real-time situational awareness and continuous monitoring to improve the efficiency and effectiveness of responses to emerging security threats. While a laudable goal, implementing complex control sets and frameworks such as NIST SP 800-53 and the 800-37 Risk Management Framework at scale is a major challenge, even for periodic audits. EventTracker was designed to cope with the difficulties of achieving of continuous monitoring of key NIST 800-53 controls such as topology mapping, network segmentation and vulnerability scanning. It also automates and limits the effort required to adhere to the monitoring requirement of the RMF. By implementing EventTracker, organizations can increase situational awareness, and improve control activity efficacy in an operationally efficient manner.

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 Event-Tracker SIEM product. 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 enterprise, 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 it's 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 enterprise 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 NIST-Risk Management Framework (RMF)

Access Control

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
AC-2 – Account Management The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts.	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.	Yes	Yes
AC-3 – Access Enforcement The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	EventTracker collects all access activities which get generated in the system. EventTracker reports provide easy and independent review of access control settings and enforcement.	Yes	Yes
AC-5 – Separation of Duties The information system enforces separation of duties through assigned access organizations.	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.	Yes	Yes
AC-6 – Least Privilege 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.	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.	Yes	Yes
AC-7 – Unsuccessful Login Attempts 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.	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.	Yes	Yes
AC-17 – Remote Access The organization authorizes, monitors, and controls all methods of remote access to the information system.	EventTracker collects all account management activities which get generated in the system. EventTracker reports provide easy and standard review of all account management activities.	Yes	Yes
AC-18 – Wireless Access Restriction The organization: • Establishes usage restrictions and implementation guidance for wireless technologies; and • Authorizes, monitors, controls wireless access to the information system.	EventTracker collects all access activities which get generated in the system. EventTracker reports provide easy and independent review of access control settings and enforcement.	Yes	Yes

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
AC-19 – Access Control for Portable and Mobile Systems The organization: • Establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and • Authorizes, monitors, and controls device access to organizational information systems.	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.	Yes	Yes
AC-20 – Personally Owned Information Systems/Use of External Information Systems The organization establishes terms and conditions for authorized individuals to: • Access the information system from an external information system; and • Process, Store, and/or transmit organization-controlled information using an external information system.	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.	Yes	Yes

Audit and Accountability

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
AU-4 – Audit Storage Capacity The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	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.	Yes	Yes
AU-5 – Response to Audit Processing Failures The information system alerts designated organizational officials in the event of an audit processing failure.	EventTracker provides support for NIST 800-53 control enhancement AU-5. • 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

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
AU-6 – Audit Monitoring, Analysis, and Reporting 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.	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.	Yes	Yes
AU-7 – Audit Reduction and Report Generation The information system provides an audit reduction and report generation capability.	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.	Yes	Yes
AU-8 – Time Stamps The information system provides time stamps for use in audit record generation.	EventTracker collects all user access events logs in real-time and retains the date and time stamp in which they occurred.	Yes	Yes
AU-9 – Protection of Audit Information The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	EventTracker provides central and secure storage of all audit log data.	Yes	Yes
AU-11 – Audit Retention 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.	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	Yes	Yes
AU-13 – Monitoring for Information Disclosure The organization monitors open source information for evidence of unauthorized ex-filtration or disclosure of organizational information.	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.	Yes	Yes

Security Assessment and Authorization

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
CA-2 – Security Assessments 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	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.	Yes	Yes
CA-3 – Information System Connections 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	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.	Yes	Yes
CA-7 – Continuous Monitoring The organization monitors the security controls in the information system on an ongoing basis.	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.	Yes	Yes

Configuration Management

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
CM-3 – Configuration Change Control The organization: Audits activities associated with configuration-controlled changes to the system.	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.	Yes	Yes
CM-4 – Monitoring Configuration Changes The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.	EventTracker's monitoring capability can be used to detect the following changes to the file system: • Additions • Deletions • Modifications • Permissions 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.	Yes	Yes

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
CM-5 – Access Restrictions for Change The organization: • 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	EventTracker collects all access activity and changes to access controls. EventTracker reports provide easy and independent review of access control settings and enforcement.	Yes	Yes
CM-6 – Configuration Settings The organization: Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures	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.	Yes	Yes
CM-11 – User Installed Software The organization enforces explicit rules governing the installation of software by users.	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.	Yes	Yes

Contingency Planning

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
CP-9 – Information System Backup The organization: • 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	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.	Yes	Yes

Identification and Authentication

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
IA-2 – Identification and Authentication (Organizational Users) The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	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
IA-3 – Device Identification and Authentication The information system uniquely identifies and authenticates before establishing a connection.	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
IA-8 – Identification and Authentication (Non-Organizational Users) The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	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

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
IR-4 – Incident Handling The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	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
IR-5 – Incident Monitoring The organization tracks and documents information system security incidents	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
IR-6 – Incident Reporting The organization promptly reports incident information to appropriate authorities	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
IR-7 – Incident Response Assistance 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.	EventTracker's integrated knowledge base provides information useful in responding to and resolving incidents.	Yes	Yes

Maintenance

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
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.	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
MA-4 – Remote Maintenance The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.	EventTracker can identify maintenance related activity for analysis and/or reporting. EventTracker reports provide easy review of remotely executed maintenance activity.	Yes	Yes
MA-5 – Maintenance Personnel The organization allows only authorized personnel to perform maintenance on the information system.	EventTracker can identify maintenance related activity for analysis and/or reporting. EventTracker rep orts provide easy review of maintenance activity.	Yes	Yes

Media Protection

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
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.	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

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
PE-3 – Physical Access Control The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	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

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
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.	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
PE-6 – Monitoring Physical Access The organization monitors physical access to the information system to detect and respond to physical security incidents.	EventTracker can collect log messages from physical access devices (i.e. Card Key) for analysis and reporting.	Yes	Yes

Personal Security

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
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.	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.	Yes	Yes
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.	EventTracker reports provide easy review of transferred personnel to ensure access rights have been terminated and/or appropriately modified.	Yes	Yes
PS-7 – Third-Party Personnel Security The organization Monitors provider compliance.	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.	Yes	Yes

Risk Assessment

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
RA-5 – Vulnerability Scanning The organization: • 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.	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.	Yes	Yes

System and Communications Protection

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
SC-5 – Denial of Service Protection 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).	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.	Yes	Yes
SC-7 – Boundary Protection The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	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.	Yes	Yes
SC-15 – Collaborative Protection The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.	EventTracker will be able to identify report and/or alert on the initiation of specific collaborative computing activity.	Yes	Yes
SC-18 – Mobile Code The organization: • 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.	EventTracker will be able to identify report and/or alert on specific mobile code activity.	Yes	Yes

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
SC-19 – Voice over Internet Protocol The organization: • 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.	EventTracker will be able to identify report and/or alert on specific VoIP activity.	Yes	Yes
SC-28 – Protection of Information at Rest The information system protects the confidentiality and integrity of information at rest.	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.	Yes	Yes

System and Information Integrity

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
SI-2 – Flaw Remediation The organization identifies, reports, and corrects information system flaws.	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.	Yes	Yes

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
SI-3 – Malicious Code Protection The organization: • 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: – 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: – 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	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.	Yes	Yes
SI-4 – Information System Monitoring 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.	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.	Yes	Yes

NIST RMF Requirement	EventTracker Capability	EventTracker Reports	EventTracker Alerts
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.	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.	Yes	Yes
SI-7 – Software and Information Integrity The information system detects and protects against unauthorized changes to software and information.	EventTracker's monitoring capability can be used to detect the following changes to the file system: • Additions • Deletions • Modifications • Permissions This capability can be used to detect unauthorized changes to software and information.	Yes	Yes
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.	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.	Yes	Yes
SI-11 – Error Handling The information system identifies potentially security-relevant error conditions.	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.	Yes	Yes

References:

- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- https://web.nvd.nist.gov/view/800-53/home
- http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf