Netsurion | EventTracker

CMS Acceptable Risk Safeguards (ARS) Solution Brief

CMS ARS v3.1

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.

ARS v3.1 Compliance

The Centers for Medicare and Medicaid Services (CMS) Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR) contain a broad set of required security standards based upon the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated March 2015, as well as additional standards based on CMS policies, procedures, and guidance, other federal and non-federal guidance resources and industry leading security practices.

It is also important to note that the ARS does not address specific business-process requirements that ensure business requirements are fulfilled. The goal of the CMSRs is to provide a baseline of minimal internal/external information security and privacy assurance controls. It is the responsibility of the Business Owner of CMS systems, with direction provided by the Office of Information Services (OIS), to ensure that all applicable internal/external information security and privacy assurance controls are incorporated into CMS systems. Business Owners must document and certify the incorporated controls in their respective security plan and identify any risks in the corresponding risk assessment for their system.

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 user's 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 ARS Reporting and Alerting

EventTracker has developed specific reports, rules and dashboards to help meet the Security controls detailed within ARS. 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 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 Compliance - ARS v3.1

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability
Access Control (AC)		
AC2 - Account Management The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts.	Yes	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.
AC3 - Access Enforcement The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	Yes	EventTracker collects all access activities which get generated in the system. EventTracker reports provide easy and independent review of access control settings and enforcement.
AC4 - Information Flow Enforcement The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Yes	The EventTracker Agent incorporates a bi-directional stateful firewall that enforces the flow of data based on physical or logical addressing. EventTracker can also be used to create and manage sophisticated protection rules that allow and deny appropriate connections and alert on suspicious behavior with a minimum number of rules and maximum flexibility.
AC 5 - Separation of Duties Separate duties of individuals as necessary to prevent malevolent activity without collusion; documents separation of duties; and implements separation of duties through assigned information system access authorization.	Yes	The EventTracker Manager enables role-based access control (RBAC) and delegated administration to support separation of administrative duties with respect to creating, deploying, and auditing security policy and events that violate the policies.
AC 6 - Least Privilege The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	Yes	The EventTracker Agent incorporates a bi-directional stateful firewall that restricts network connections (ports, protocols, etc.) based on organizational policy. The EventTracker Manager enables role-based access control (RBAC) and delegated administration to support the concept of least privilege and workflow of security response. EventTracker can also be used to create and manage sophisticated protection rules that allow and deny appropriate connections and alert on suspicious behavior with a minimum number of rules and maximum flexibility. EventTracker Log Inspection capabilities provide the ability to monitor and alert on important security events that could indicate suspicious activity. In addition, EventTracker Integrity Monitoring capabilities will detect and raise events whenever critical OS or application files are modified (i.e. Windows system files, Hosts file, registry, etc.)
AC 7 - Unsuccessful Login Attempts The information system enforces a limit of consecutive invalid access attempts by a user during a time period.	Yes	EventTracker Log Inspection capabilities provide the ability to monitor and alert on important security events such as 'x' failed login attempts within 'y' time period providing administrators with visibility into unsuccessful login attempts.
AC 17 - Remote Access The organization authorizes, monitors, and controls all methods of remote access to the information system.	Yes	EventTracker offers controls for securing remote access including: • The ability to dynamically assign firewall rules based upon user location for example, remote users will have a more stringent firewall policies assigned to reduce the attack surface. • Protection against bridging attacks (wired vs. wireless), • Enforcing usage of VPN connections for remote users, etc. All of the above capabilities are augmented with the IDS/IPS, Integrity Monitoring and Log Inspection capabilities provided by EventTracker to facilitate the monitoring and control of remote access methods.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability
AC-18 - Wireless Access The organization: Establishes usage restrictions and implementation guidance for Wireless technologies; and authorizes, monitors, controls wireless access to the information system.	Yes	EventTracker offers controls for securing wireless mobile workers including: • The ability to dynamically assign firewall rules based upon user location for example, remote users will have a more stringent firewall policies assigned to reduce the attack surface. • Protection against bridging attacks (wired vs. wireless) • Enforcing usage of VPN connections for remote users, etc. All capabilities above are augmented with standard IDS/IPS, Integrity Monitoring and Log Inspection capabilities provided by EventTracker.
AC-19 - Access Control for Mobile Device 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.	Yes	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.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Audit and Accountability (AU)

AU-2 - Audit Event The information system generates audit records for events.	Yes	The EventTracker provides the ability to monitor and alert on important security events that could indicate suspicious activity. In addition, the EventTracker Agent will log Firewall, IDS/IPS, and Integrity Monitoring events and generate alerts based upon the security policy assigned. Alerts can be delivered via various mechanisms such as email, SNMP, as well as through the Manager interface.
AU-3 - Content of Audit Records The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.	Yes	EventTracker Agent and EventTracker Manager Event logs contain very granular network information about the event, including the event type, sources of events and can even capture the complete contents of the packet. The Manager also logs all important internal system events such as administrator logins and system errors.
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.	Yes	The events and logs are spooled locally at each EventTracker Agent and sent to the EventTracker Manager on a scheduled heartbeat. The size of the local spool is configurable and the Manager is limited only by the available disk space assigned to the database.
AU-5 - Response to Audit Processing Failures The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	Yes	EventTracker has several mechanisms to respond to audit processing failures. It will alert when disk space is low or as Agents go offline. It will then overwrite the oldest logs as needed so that the most recent events are available. The Agent will enforce protection even if it cannot generate events.
AU-6 - Audit Review, 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's findings to appropriate officials, and takes necessary actions.	Yes	EventTracker provides a number of features which assist with audit monitoring, analysis, and reporting such as customizable dashboards, alerting, and reporting. It forwards this valuable event information via syslog to a centralized log server or SIEM for further analysis.
AU-7 - Audit Reduction and Report Generation The information system provides an audit reduction and report generation capability.	Yes	The EventTracker Manager has several out-of-box reports that can be scheduled or produced on demand. Reports can be automatically delivered via email and can be restricted based on role-based administrative access. In addition, event information can be exported for further analysis.
AU-8 - Time Stamps The information system provides time stamps for use in audit record generation.	Yes	All alerts and logs are time stamped.
AU-9 - Protection of Audit Information The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Yes	The delivery of events to the EventTracker Manager is authenticated and encrypted using certificates and SSL encryption. Data at rest in the database is password protected. EventTracker Agent Log Inspection may also be used to forward important security events from operating system and application logs to a centralized logging server to prevent local tampering. EventTracker Manager enables role-based access control (RBAC) and delegated administration to support separation of administrative duties to a limited subset of privileged users.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability
AU-11- Audit Record Retention The organization retains audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Yes	EventTracker supports integration with SIEM solutions for long term archival of security event information. In addition, the EventTracker Manager can store audit logs and events for an indefinite amount of time, limited only by the available disk space of the database server. Native database tools can be used to back up and archive data as appropriate.
AU-12 - Audit Generation The information system: provides audit record generation capability for the list of auditable events defined in AU-2; allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and, generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	Yes	EventTracker Agent and EventTracker Manager, event logs contain very granular network information about the event, including the event type, sources of events and can even capture the complete contents of the packet. The Manager also logs all important internal system events such as administrator logins and system errors. The EventTracker Manager enables role-based access control (RBAC) and delegated administration to support separation of administrative duties to a limited subset of privileged users. EventTracker supports integration with SIEM solutions for long term archival of security event information. In addition, the EventTracker Manager can store audit logs and events for an indefinite amount of time, limited only by the available disk space of the database server. Native database tools can be used to back up and archive data as appropriate.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Security Assessment and Authorization (CA)

CA-2 - Security Assessments The organization assesses 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.	Yes	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.
CA-7 - Continuous Monitoring The organization monitors the security controls in the information system on an ongoing basis.	Yes	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.
CA-9 - Internal System Interconnections- 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.	Yes	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.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Configuration Management (CM)

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

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Identification and Authentication (IA)

IA-2 - Identification and Authentication (Organizational Users) The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Yes	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.
IA-3 - Device Identification and Authentication The information system uniquely identifies and authenticates before establishing a connection.	Yes	EventTracker provides support for 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.
IA-8 - Identification and Authentication (Non- Organizational Uers) The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Yes	EventTracker provides support for 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.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Incident Response (IR)

IR-4 - Incident Handling The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	Yes	EventTracker provides support for 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.
IR-5 - Incident Monitoring The organization tracks and documents information system security incidents.	Yes	EventTracker provides direct support for control requirements IR-5 by providing security incident tracking and documentation through the EventTracker management interface.
IR-6 - Incident Reporting The organization promptly reports incident information to appropriate authorities.	Yes	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.
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.	Yes	EventTracker's integrated knowledge base provides information useful in responding to and resolving incidents.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Maintenance (MA)

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

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Media Protection (MP)

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.	Yes	EventTracker provides support for 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.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Physical and Environmental Protection (PE)

PE-3 - Physical Access Control The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Yes	EventTracker provides support for 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.
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.	Yes	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.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Personnel Security (PS)

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.	Yes	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.
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.	Yes	EventTracker reports provide easy review of transferred personnel to ensure access rights have been terminated and/or appropriately modified.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

Risk Assessment (RA)

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.	Yes	EventTracker ETVAS provides support for 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.

ARS v3.1 Requirement	EventTracker Reports & Alerts	EventTracker Capability

System and Communications Protection (SC)

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).	Yes	EventTracker provides support for 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.
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.	Yes	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.
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.	Yes	EventTracker will be able to identify report and/or alert on the initiation of specific collaborative computing activity.
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	Yes	EventTracker will be able to identify report and/or alert on specific mobile code activity.
SC-23 - Session Authenticity The information system protects the authenticity of communications sessions.	Yes	EventTracker Support and Analyze logs against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.
SC-28 - Protection of Information at Rest The information system protects the confidentiality and integrity of information at rest.	Yes	EventTracker provides supplemental support for 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.

ARS v2.0 Requirement	EventTracker Reports & Alerts	EventTracker Capability
System and Information Integrity (SI)		
SI-2 - Flaw Remediation Identifies reports and corrects information system flaws.	Yes	EventTracker complements secure coding initiatives with strong detection and prevention of attacks against technical flaws and vulnerabilities: • Detection: Even if an application is not susceptible to a specific attack, it is important to identify attackers before they find other potential vulnerabilities. • Protection: EventTracker shields web application vulnerabilities, preventing security breaches until the underlying flaws can be addressed. EventTracker systematically monitors a wide range of vulnerability research sources to identify and deliver to customers. The deployment of new security rules can be completely automated so that downloading and installing new security rules to the appropriate systems occur without administrative intervention. EventTracker also supports the ability to schedule automatic scans of host systems – one time only, daily, weekly, and so forth – offering recommendations on the appropriate security rules to protect these hosts.
SI-3 - Malicious Code Protection The information system implements malicious code protection.	Yes	EventTracker detects and prevents attacks that target data and applications, including activity from malicious code. EventTracker alerts personnel the moment an attack has been attempted, and provides detailed logging of the event for audit purposes. For commercial applications which contain known EventTracker detects and prevents attacks that target data and applications, including activity from malicious code. EventTracker alerts personnel the moment an attack has been attempted, and provides detailed logging of the event for audit purposes. For commercial applications which contain known vulnerabilities targeted by malicious code, EventTracker virtual patching capabilities protect systems and data until vendor patches can be deployed. EventTracker systematically monitors a wide range of vulnerability research sources to identify and to customers. The deployment of new security rules can be completely automated so that downloading and installing new security rules to the appropriate systems occur without administrative intervention. EventTracker also supports the ability to schedule automatic scans of host systems – one time only, daily, weekly, and so forth – offering recommendations on the appropriate security rules to protect these hosts. Web application protection rules defend against SQL injection attacks, cross-site scripting attacks, and other Web application vulnerabilities, and shield these vulnerabilities until code fixes can be completed.
SI-4 - Information System Monitoring The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	Yes	The EventTracker Agent collects and analyzes operating system and application logs for security events. Log Inspection rules optimize the identification of important security events buried in multiple log entries. These events are forwarded to a security information and event management (SIEM) system or centralized logging server for correlation, reporting and archiving. Reports can be scheduled to run automatically and alerts can be delivered via SNMP or email, in addition to visibility from the EventTracker Manager console.

ARS v2.0 Requirement	EventTracker Reports & Alerts	EventTracker Capability
SI-5 - Security Alerts, Advisories, and Directives The organization receives, generates, and disseminates security alerts and implements security directives in accordance with established time frames.	Yes	EventTracker provides alerts that are integral to a security incident response plan. And because it can prevent attacks as well, EventTracker reduces the number of incidents requiring a response. The solution's integration with leading SIEM vendors enables a consolidated view of security incidents. Monitoring the integrity of critical system and application files such as executables, configuration and parameter files, and log and audit files – it includes support for alerting, dashboards, and reporting on events created. EventTracker enables collection of important security events from operating system and application log files, including the ability to forward all events – or only events relevant – to centralized logging servers or SIEMs via syslog in real time, in addition to sending these events to the EventTracker Manager.
SI-6 - Security Function Verification The information system verifies the correct operation of security when anomalies are discovered.	Yes	The EventTracker Manager monitors the Agents to ensure that it is in constant communication and creates an alert if an Agent terminates communication for any reason.
SI-7 - Software, Fireware, and Information Integrity The information system detects and protects against unauthorized changes to software and information.	Yes	The EventTracker Change Audit module provides the ability to monitor critical operating system files, registry keys and values, and application files for changes and generate alerts on detected changes. These events are sent to the EventTracker Manager which supports dashboards, alerts, and reporting. In addition, these events can also be sent to a SIEM for additional correlation and analysis.
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	Yes	EventTracker provides support for control requirement SI-8 by collecting and analyzing SPAM logs. EventTracker investigations, reports, and tails provide evidence of SPAM protection activity.
SI-11 - Error Handling The information system identifies potentially security-relevant error conditions.	Yes	EventTracker provides support for 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.
SI-6 - Security Function Verification The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	Yes	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.

References: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/STANDARD-ARS-Acceptable-Risk-Safeguards.html