EventTracker
Actionable Security Intelligence

DoDI 8500.2 Solution Brief

EventTracker | 8815 Centre Park Drive, Columbia MD 21045

DoDI 8500.2

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 DoDI (Department of Defense Institute) requirements.

DoDI 8500.2 Compliance

The Department of Defense has a crucial responsibility to protect and defend its information and supporting information technology. DoDI calls for information assurance requirements to be identified and included in the design, acquisition, installation, operation, upgrade and replacement of all DoD information systems. EventTracker believes that it is crucial to monitor for compliance in a manner as close to real-time as possible.

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 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 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. It is from this interface that all searches are performed, and detailed information on an event can be accessed. EventTracker SIEM is designed to make the user experience as easy and efficient as possible.

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 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.

Continuous Monitoring

EventTracker successfully monitors the complete audit information that comprises of information related to audit records, audit settings and audit reports. EventTracker Enterprise offers the most comprehensive and flexible search options in the SIEM/Log Management industry. Whether users are responding in real-time to a threat or system issue or looking back in time to piece together a user's activity spanning months, EventTracker Enterprise Search gets all users what they need quickly in a useable format. EventTracker Enterprise stores events in their original state and the complete contents are accessible to the user and its reporting allows users to easily report on all event data on either a scheduled or ad-hoc basis.

Extract archive data from compressed storage, smart tokens allow you to immediately see interesting fields and patterns in the results. Our dedicated knowledge team is constantly adding log information from popular products to the token library and so can users. Smart tokens free users from having to frame precise queries, which is something advanced users can do. Empower business users and junior staff to extract meaningful data from data sets. The true challenge of big data is to quickly extract meaningful information – smart tokens are an exciting innovation to satisfy this need.

EventTracker's list management features are available to all users to manage internal and external feeds of threat intelligence. Lists, once created, can be updated automatically. Lists can be used to search through log data, thereby clearly seeing if global trends are impacting your network. Open Source feeds such as those provided by the Internet Storm Center Dshield block list, Team Cymru etc can also be integrated. List look-up APIs is available for use in remedial actions. This allows efficient creation and use of both black and white lists for processes, IP addresses, services and port numbers.

EventTracker Enterprise also provides enhanced end-point monitoring and security, generating an event when USB/DVD/CD removable media is inserted including the username and device serial number; all file transfers to USB/DVD/CD devices are recorded including the time/date stamp; USB devices can be automatically disabled based on serial number.

Security of Enterprise Devices

EventTracker is a SIEM and Log Management solution that helps you secure your organization's environment. EventTracker takes the baseline snapshot of customer's IT infrastructure with which users can gather and document user activity, view group memberships, share permission levels and security settings over a timeframe to know your environment's stable state. Then at any point of time EventTracker can take current snapshot informing users when the current setting differs from that recommended by a security standard, so IT can investigate.

Ease of DODI 8500.2 Reporting and Alerting

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

Vulnerability Assessment and Intrusion Detection Services

EventTracker Vulnerability Assessment Service (ETVAS) is provided as an optional service to our EventTracker customers. The service detects and reports vulnerabilities present on IT assets including operating systems, applications, network devices etc in the target network. The report also includes possible mitigation steps. The service is provided on a periodic basis as per customer's requirement (usually weekly/monthly/quarterly). Customers of this service provide a total number of assets to be scanned for vulnerabilities (e.g., 200) and the periodic schedule for scanning (e.g., weekly/monthly/quarterly).

The EventTracker Vulnerability Assessment Service (ETVAS) has inbuilt Snort IDS which will help users to detect any attacks with the IDS/IPS and also to determine if any changes have been made to the environment that may be related to a given attack.

Snort network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol networks. Snort performs protocol analysis, content searching, and content matching. These basic services have many purposes including application-aware triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans. This ETVAS is tightly integrated with EventTracker to alert the customer and required reports will also be scheduled for the ease of our customer.

Statement of Compliance: DoDI 8500.2

DODI 8500.2 Requirements	EventTracker Capability	EventTracker Reports	Sample EventTracker Alerts
ECAN-1 ECPA-1 PRAS-1 DCAR-1 IAAC-1 ACCESS CONTROL POLICY AND PROCEDURES	EventTracker manages information system accounts, including: • Identifying authorized users of the information system and specifying access privileges. • Establishing, activating, modifying, disabling, and removing accounts. • Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;	**Active Directory: ->** User added User deleted Change Audit: Authorized changes Cisco IOS: Accounting services **Cisco NAC: ->** Guest login failed User Activity Correlated events Failed interactive logins Files Deleted Group policy activity Idle Time Printer activity Software installed Software uninstalled Successful interactive logins Successful non-interactive logins Websites visited **Security: ->** Account Management Account privileges Account renames User account disabled User account enabled User account locked User added User added to group User deleted User removed from group **Solaris BSM: ->** Disable user User management Syslog: User process events **Telemkt: ->** User calling User login User logout User Logon Failure Report **VMware ESX: ->** Failed user login Successful user login User logout	ArubaOS: DHCP client disabled **BIG-IP LTM: ->** User account deleted Serious Packet filtering disabled Cisco NAC: Guest login failed **DigitalPersona Pro: ->** Account locked out Shared account problem DNS update disabled **EventTracker: ->** USB device disabled Behavior rule deactivated Forefront Client: Scan disabled Forefront TMG: Malware inspection disabled Imperva DAM: SAP-Suspected activity in accounting documents tables McAfee EPO: OAS scanning engine disabled **RSA SecurID: ->** Account lockout Serious Agent disabled Token disabled **Security: ->** User account locked out User account disabled Sonicwall: Antispam service disabled USB Device Disabled Report

DODI 8500.2 Requirements	EventTracker Capability	EventTracker Reports	Sample EventTracker Alerts
DCFA-1, ECAN-1, EBRU-1, PRNK-1, ECCD-1, ECSD-2 ACCESS ENFORCEMENT	EventTracker manages Access control policies and access enforcement mechanisms to control access between users and objects in the information system. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.	Check Point: Administrator login **Cisco Catalyst: ->** Access control list Access control list error Cisco IOS: Access control list Cisco Switch: Access control list manager error DHCP: Database integrity **EventTracker: ->** Admin Activity CAB integrity verification FortiAnalyzer: User access profile changed LOGbinder: SharePoint access control change McAfee EPO: Enforce policy failed **McAfee Sidewinder: ->** Network access control allowed Network access control violation **MSExchange: ->** User accessed own mailbox **Wireless Switch: ->** Access control list Encryption key exchange **Syslog: ->** Authorization events Privilege authorization events	EventVault CAB integrity checksum failure
EBBD-1, EBBD-2 INFORMATION FLOW ENFORCEMENT	EventTracker monitors unauthorized use of the information system. EventTracker monitors the information system both externally and internally. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). 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)	Too many to list, including reports on Window, UNIX, Linux, network devices including firewalls (CISCO PIX, Checkpoint) routers and switches, infrastructure applications like Citrix, IIS, databases and many more…	CISCO PIX: IDS Intrusion detected **Excessive ->** Access failures in your enterprise Access failures on specific computer File deletes on a computer Access failure by user Logon failures due to bad password Logon failures in your enterprise Remote connections established Remote connections established on a local network port User Lockout **ISA Server: ->** Port Scan Detected Land Attack detected Out-of-bound attack Ping attack Spoof attack UDP attack Logon Failures Logon Failures from a specific computer **Netscreen: ->** IDS Intrusion detected Security device error

DODI 8500.2 Requirements	EventTracker Capability	EventTracker Reports	Sample EventTracker Alerts
ECLO-1 Logon	EventTracker monitors unsuccessful login attempts may be implemented at both the operating system and the application levels.	ArubaOS: Authentication failed Astaro security gateways: Authentication failed Aventail: Authentication failed BIG-IP LTM: Authentication failed Check Point: Failed login Cisco ACS: Authentication failed Cisco Aironet: Authentication failed Cisco Catalyst: Authentication failed **Cisco NAC: ->** Admin login failed Guest login failed RADIUS authentication failed Remote login failed User login failed Wireless user login failed Cisco WLAN: User login failed Citrix NetScaler: Login failed Forefront TMG: Authentication failed Forefront UAG: User login failed FortiAnalyzer: User login failed Fortimail: User login failed Imperva DAM: Database failed login **JUNOS: ->** Authentication failed Login failed Oracle: Logon failed RSA SecurID: Authentication failed Solaris BSM: Failed local logon/ logoff **Sonicwall: ->** Administrator login failed Authentication failed User login failed Syslog: User login failed VMware ESX: Failed user login	Administrative logon failure Admin Interactive/Remote Interactive login failure ArrayOS SPX: Authentication failure ArubaOS: Authentication failed Astaro security gateways: Authentication failed Aventail: Authentication failed **BIG-IP LTM: ->** Authentication failed Root login failure Cisco ACS: Authentication failed Cisco ASA: Authentication failed **Cisco NAC: ->** Admin login failed Guest login failed Remote login failed User login failed Wireless user login failed Citrix NetScaler: Login failed CISCO PIX: Authentication failed CISCO VPN: Admin Access - Authentication failure **Cisco WLAN: ->** Authentication failure User login failed Forefront TMG: Authentication failed Forefront UAG: User login failed FortiAnalyzer: User login failed Fortimail: User login failed McAfee IntruShield IPS: MSSQL User Login Failed MSExchange: Logon failure on mailbox database MySQL: Authentication failure Netscreen: Authentication failure Oracle: Logon failure **Paloalto Firewall: ->** Logon failure VPN logon failure Raritan: Authentication failure RSA SecurID: Authentication failed **Sonicwall: ->** Administrator login failed User login failed Authentication failed SOX - CISCO PIX: Authentication failure Syslog: User login failed Session setup authentication failed

DODI 8500.2 Requirements	EventTracker Capability	EventTracker Reports	Sample EventTracker Alerts
ECAT-1 ECAT-2 E3.3.9 SUPERVISION AND REVIEW – ACCESS CONTROL	EventTracker monitors audit processing failures like software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.	Active Directory: ->* Group Policy (all reports) User logons User logoffs ArrayOS SPX: Remote access traffic tunnel failure Checkpoint: Audit activities Cisco NAC: Remote login failed Forefront UAG: Remote user request denied Exchange ActiveSync: Policy compliance **EventTracker: ->** CAB integrity verification Collection master error Collection point error Disk Space low Eventlog full Initial User Network logon **NetApp Data ONTAP: ->** Delete Access Read Access Write Access **Security: ->** User logon User logoff Access Control (all reports) **Solaris BSM: ->** Audit Policy changes SU failure SU success Privileged use **Windows: ->** Account logon Account logon failure	Domain Policy Changed System Audit Log Cleared Critical Service Not Running Critical Service Not Started Event Log Full Event Log Cleared EventTracker agent service failed Collection Master Error Collection Point Error IIS Logging Shutdown MSExchange: Log disk full System Shutdown SQL Server: Transaction Log Full Admin Login Failure Admin Login Success Solaris BSM: SU failure Solaris BSM: SU success Solaris BSM: User Management

DODI 8500.2 Requirements	EventTracker Capability	EventTracker Reports	Sample EventTracker Alerts
EBRP-1 EBRU-1 REMOTE ACCESS	EventTracker monitors unauthorized remote access to the information system. It authorizes remote access to the information system prior to connection and enforces requirements for remote connections to the information system.	EventTracker: Initial User Network logon ***Security: ->** User logon User logoff Policy Change Audit Policy change Solaris BSM: Remote access events Syslog: Remote/SSH system accessed **VMware ESX: ->** Remote console connected Remote console disconnected **Windows: ->** Account logon Account logon failure	
ECAT-1 ECTB-1 DCAR-1 ECTP-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	EventTracker successfully monitors the complete audit information that comprises of information about audit records, audit settings and audit reports	**Active Directory: ->** Group Policy (all reports) Deleted Share Share Folder deleted Changed Audit: Files Deleted Checkpoint: Audit activities **File Resource Access ->** Success: Delete Access Failure: Delete Access NetApp Data ONTAP: Delete Access ***Security: ->** Policy Change Audit Policy change Solaris BSM: Audit Policy changes	Admin Login Failure Domain Policy Changed EventTracker CAB integrity checksum failed

DODI 8500.2 Requirements	EventTracker Capability	EventTracker Reports	Sample EventTracker Alerts
ECAR-1 ECAR-2 ECAR-3 ECLC-1 AUDITABLE EVENTS	EventTracker monitors and audits all types of events and captures all event information	All audit events All DNS server events All error events All file replication events All IMAP4 interface events All information events All Syslog events All warning events All altiris deployment solution events All backup exec events All citrix events All crystal enterprise events All sharepoint server events Application: Dr.Watson events Astaro Security Gateways: All events **Check Point: ->** All Checkpoint management events All firewall events All identity awareness events All IPS events Cisco Aironet: All events Cisco ASA: All events Cisco Director: All events Cisco IOS: All events Cisco PIX: All events Cisco VPN: NTP subsystem and general events Citrix NetScaler: All events Cyberoam UTM: All events Dell OMSA: All events Device and media events **DHCP: ->** *All DHCP events DHCP critical events DoubleTake: All events **EventTracker: ->** All Events No events received in last 24 hour F-Secure: All events Forefront Client: All events Forefront TMG: All events Forefront UAG: All events FortiAnalyzer: Critical error events Fortigate: All events Fortimail: All events Hyper V: *All events *(continued)*	EventTracker: No events received in last 24 hour FortiAnalyzer: Critical error events Audit event records discarded Forefront TMG: Event Log Deletion Failure High

DODI 8500.2 Requirements	EventTracker Capability	EventTracker Reports	Sample EventTracker Alerts
		(continued) **IIS: ->** Admin critical events All events ISA server: All events **Juniper SBR: ->** All error events All events **LOGbinder: ->** Noise events SharePoint search events **MSExchange: ->** All events Critical events Error events NNTP interface events POP3 interface events **MSFTP: ->** *All FTP service events FTP service critical events FTP service error events **MSSQLServer: ->** All error events All events **Netscreen: ->** All events Security device events **Oracle: ->** All oracle events Other oracle events SEP: All events **Security: ->** All security events Audit events Logon failure events Snort: All events **Solaris BSM: ->** All command execution events All events Network events Remote access events Sonicwall: All events Sophos: All events **Syslog: ->** Authorization events Clock daemon events FTP daemon events Kernel events Line printer events Mail subsystem events Network news system events Privilege authorization events Syslogd events System daemon events User process events UUCP subsystem events *(continued)*	

DODI 8500.2 Requirements	EventTracker Capability	EventTracker Reports	Sample EventTracker Alerts
		(continued) **TCPIP: ->** Critical events Error events VMware ESX: All events Windows Backup: All events Windows Firewall: All events WTS: All events	
DCCB-1 DCPR-1 E3.3.9 CONTINUOUS MONITORING	EventTracker monitors any changes to the hardware, software, and/or firmware components of the information system that can potentially have significant effects on the overall security of the system. EventTracker's list management features are available to all users to manage internal and external feeds of threat intelligence. Lists, once created, can be updated automatically. Lists can be used to search through log data, thereby clearly seeing if global trends are impacting your network. List look-up APIs is available for use in remedial actions. This allows efficient creation and use of both black and white lists for processes, IP addresses, services and port numbers.	Changed Audit: (all reports) **Active Directory: ->** Changed objects OU change CISCO PIX: Priv level changed EventTracker: Service changes **File/resource Access Failure: ->** Change property Change ownership **File/resource Access Success: ->** Change property Change ownership ***Security: ->** Policy Change Audit Policy Change **Solaris BSM: ->** Audit policy changes Set, create, change passwords Syslog: Password changed	Agent not running Audit log cleared Directory permission change Eventlog full EventTracker cab integrity checksum failure **Excessive ->** Ping failures-system(s) are not reachable File deletes on a computer Access failures on a specific computer Access failures in your enterprise
DCPP-1 ECIM-1 ECVI-1 E3.3.8 Ports, Protocols, and Services	EventTracker provides the essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services].	ArrayOS SPX: IP Access restriction Change Audit: Unauthorized changes Forefront UAG: Restricted URL access denied MSExchange: Unauthorized mailbox access attempt MSSQLServer: Unauthorized access error	Change Audit: Unauthorized changes **Imperva DAM: ->** EBS PCI-Unauthorized access to credit card no EBS PCI-Unauthorized access to credit cardholder HIPAA - Unauthorized data modification HIPAA-Unauthorized data access SAP PCI-Unauthorized access to credit cardholder SAP PCI-Unauthorized access to payment card no

DODI 8500.2 Requirements	EventTracker Capability	EventTracker Reports	Sample EventTracker Alerts
IAGA-1 IAIA-1 Individual and Group Authentication	EventTracker uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	ArrayOS SPX: Authentication success ArubaOS: Authentication successful Astaro security gateways: Authentication success Aventail: Authentication success BIG-IP LTM: Authentication success Cisco ACS: Authentication success Cisco Aironet: Authentication success Cisco ASA: Authentication success Cisco PIX: Authentication success Cisco VPN: Authentication Forefront TMG: Authentication success Juniper SBR: Authentication request success **JUNOS: ->** Authentication success Ipsec authentication McAfee Sidewinder: Proxy/Server authentication MySQL: Authentication success **Netscreen: ->** System authentication User authentication **RSA SecurID: ->** Authentication PIN successfully changed Authentication principal locked Authentication principal resolution Authentication success Sonicwall: Authentication success Teradata: Authentication success WatchGuard: Authentication	BIG-IP LTM: Authentication success RSA SecurID: Authentication success
ECMT-1 VIVM-1 VULNERABILITY SCANNING	EventTracker Vulnerability Assessment Service scans for vulnerabilities in the information system; hosted applications and new vulnerabilities potentially affecting the system/ applications are identified and reported.		