EventTracker
Actionable Security Intelligence

PCI DSS v3.2.1 Solution Brief

PCI DSS

EventTracker | 8815 Centre Park Drive, Columbia MD 21045

About EventTracker

EventTracker delivers business critical software and services 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 IT audit and event log files. EventTracker's award winning solutions provide capabilities to implement Security Information and Event Management (SIEM), Log Management, and real-time Threat Intelligence to help optimize IT operations, detect and deter costly security breaches, and comply with multiple regulatory mandates.

EventTracker software is designed to be implemented for organizations with 25 to 25,000 assets such as servers, firewalls, other network and security devices, workstations, applications. EventTracker SIEM Simplified managed services are right-sized to assist you with system administration, incident analysis and compliance activities through ''self- half- or full-service" options.

Payment Card Industry – Data Security Standard Compliance

https://www.pcisecuritystandards.org/security_standards/

Payment Card Industry Data Security Standards (PCI DSS) mandate that all organizations that accept, acquire, transmit, process, and/or store cardholder data must take appropriate steps to continuously safeguard all sensitive customer information. PCI DSS has improved the protection of cardholder information. PCI DSS v3.2 will remain valid throught December 31, 2018 and will be retired on January 1, 2019. Prior to the effective date, entities can validate to either standard; however, as of January 1, 2019, all entities must validate to atleast PCI DSS v3.2.1.

The PCI Security Standards Council was established in 2006 by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. and is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.

These requirements include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information. In the wake of increasingly expensive and damaging security breaches involving credit cards and cardholder information, meeting PCI DSS compliance requirements has taken on considerable importance for companies that accept credit and debit card payments. These include everyone from large retailers to small mom-and-pop stores. Compliance requires adherence to payment card data security process – including prevention, detection and appropriate reaction to security incidents.

PCI DSS Compliance Challenges

The widespread availability and use of credit and debit card payments means that today, online stores managed by one person, utilities companies, university cafeterias, and doctor's offices have joined the ranks of enterprises required to comply with PCI DSS, which had previously been the purview of merchants, banks and financial institutions. These entities rely on increasingly complex, geographically distributed networks, typically containing both structured and unstructured data. Cardholder information may be stored in a variety of different databases and versions, as well as in file server files, documents, images, voice recordings, access logs, and a broad range of other data repositories. Safeguarding cardholder data in such a wide variety of assets and locations, in a manner compliant

with PCI DSS, requires diligent administration and close cooperation between the enterprise's IT teams and the many business units that need access to the data. Finding the right balance between protecting cardholder information, avoiding any disruptions to IT infrastructure, and ensuring uninterrupted access to the information that flows through and across these networks is vital to the security and ongoing operation of the business.

The primary requirements of PCI DSS are:

- Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.
- Implement automated audit trails to reconstruct events for all system components.
- Record audit trail entries for each event for all system components.
- Secure audit trails so they cannot be altered.
- Review logs for all system components at least daily. Log reviews should include those servers that perform security functions like IDS and authentication (AAA) servers.
- Retain your audit trail history for a minimum of a one year, with 3 months available on-line.

In order to meet these PCI DSS regulations, IT organizations need the ability to manage access control, encryption, key management, and auditing of cardholder data at rest. Attempting to fulfill these requirements with a piecemeal solution would be complicated to operate and costly to implement. Organizations collecting cardholder information need a comprehensive data security solution that can cost effectively achieve and maintain PCI DSS v3.2.1 compliances, support major SIEM and log collection solutions, and does not require re-engineering of applications or databases. EventTracker fulfills these criteria and can offer cloud or big data environments while maintaining a high level of system performance that doesn't compromise service level agreements (SLA).

Ease of PCI DSS Reporting and Alerting

EventTracker offers specific reports, rules and dashboards to help meet the requirements detailed within PCI DSS 3.2.1. These reports, rules and dashboards can be easily and intuitively customized for specific environments. Audits usually are stressful, expensive and time consuming. However, you should also consider that audits serve to confirm that your PCI DSS compliance activities are both understood and practiced by your organization on a regular basis. Auditors have wide discretion to determine what constitutes compliance or non-compliance and the relative severity/intent therein. By demonstrating that your organization is aware of the requirements and is serious about your operational commitment by being ''audit-ready all the time," you are more likely to receive corrective guidance as opposed to punitive action in the audit.

EventTracker streamlines both the real-time security incident detection and the compliance report review processes. By providing ''single-click" issue flagging and report annotation on-the-fly, PCI DSS audit-ready summaries are available on demand in EventTracker to help minimize the stress and time needed to prepare for PCI DSS audits.

Real-time Monitoring

You must monitor and review logs and access reports for this covered information and information exchange in real-time, or as soon thereafter as is practicable to avoid privacy breaches and placing your organization at risk of

failing a PCI DSS audit. You must also document your policies, identify and train responsible personnel and provide evidence of incident and log review procedures on an on-going basis.

Protect Data and Information

EventTracker safeguards cardholder's data by ensuring stringent rules against unknown authentication and authorization. EventTracker monitors access to file and database servers. It also monitors configuration changes on critical file and database servers, and alerts the responsible entity to take further action. EventTracker Enterprise 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. These logs are compressed and sealed with a SHA-1 signature to prevent potential tampering.

EventTracker Provides a Full View of the Entire IT Infrastructure

EventTracker improves security, helps organizations demonstrate compliance, and increases operational efficiencies. EventTracker enables your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced, minimizing potential exposure and costs.

EventTracker SIEM Simplified is our managed services offerings to enhance the value of EventTracker implementations. Our expert staff can assume responsibility for some or all EventTracker SIEM-related tasks, including system management, incident reviews, daily/weekly log reviews, configuration assessments, PCI DSS audit reports annotation, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Scalable, Log Collection and Processing with Notifications based on Criticality

EventTracker provides automatic consolidation of thousands or even millions of audit events to meet the needs of any size organization. The inbound log data is identified by EventTracker's built-in manufacturers Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security and PCI DSS compliance.

EventTracker provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, Windows, Linux/Unix, VMware ESX, Citrix, databases, MS Exchange web servers, EHRs and more.

Ease of Deployment and Scalability

EventTracker is available on premise or as a highly scalable cloud-based SIEM and Log Management solution. It offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports multi-tenant implementations for MSSP organizations serving the needs of smaller customers.

For more information on EventTracker and Co-managed SIEM, visit www.eventtracker.com

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Statement of Compliance – PCI DSS v3.2.1

PCI DSS v3.2.1 Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Requirement 1: Install and Maintain a firewall configuration to protect data **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configuration.	EventTracker supports 1.1.1 by providing details of firewall and router configuration or policy changes via investigations, and reports.	Yes	Yes
1.1.5 Description of groups, roles, and responsibilities for management of network component.	EventTracker supports 1.1.5.a by providing details of allowed or denied, secure or insecure network protocols and ports within the organizational network infrastructure via investigations and reports.		
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	EventTracker supports testing procedure 1.1.6.b by providing details of allowed or denied network protocols and ports within the organizational network infrastructure.		
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	EventTracker supports for 1.2.1.a and 1.2.1.b by providing details of allowed or denied inbound or outbound network traffic to the cardholder data environment via investigations and reports. This will allow for verification that inbound and outbound traffic is being restricted or allowed.		
1.2.2 Secure and synchronize router configuration files.	EventTracker supports for 1.2.2 by providing alarms on firewall synchronization critical or error conditions and also by providing details of firewall synchronization conditions via investigations and reports.		
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	EventTracker supports for procedure 1.3.1 by providing details of allowed or denied network protocols or ports between the DMZ environment and the organization's internal network environment via investigations and reports.		
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	EventTracker supports for 1.3.2 by being able to detect and alert on allowed or denied network traffic between the external Internet and the organizations internal network environment via investigations and reports.		

PCI DSS v3.2.1 Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.).	EventTracker supports for 1.3.3 by providing details of allowed or denied network traffic that is inbound or outbound between the external Internet and cardholder data environment via investigations and reports.	Yes	Yes
1.3.5 Permit only "established" connections into the network	EventTracker supports for 1.3.5 by providing details of allowed or denied network traffic outbound from the cardholder data environment to the external Internet via investigations and reports.		
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: 1. Specific configuration settings are defined. 2. Personal firewall (or equivalent functionality) is actively running. 3. Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	EventTracker provides alarms, investigations, and reports to support PCI DSS control requirement 1.4.a. EventTracker supports for procedure 1.4.a by providing alarms on host firewall critical or error conditions and also by providing details of host firewall conditions via investigations and reports.		
Requirement-2: Do not use vendor-supplied defaults for system passwords and other security parameters. **2.1** Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	EventTracker provides supports investigations, and reports to support PCI-DSS control requirement 2.1. EventTracker supports 2.1 by providing alarms and details of known vendor default account authentication failures or successes via investigations and reports.	Yes	Yes
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS). • International Organization for Standardization (ISO). • SysAdmin Audit Network Security (SANS) Institute. • National Institute of Standards Technology (NIST).	EventTracker provides host activity monitoring that monitors running processes and services in support of 2.2.2.a and 2.2.2.b. Verification that only necessary services are enabled and justification for insecure services is still required.		
2.3 Encrypt all non-console administrative access using strong cryptography.	EventTracker supports for procedure 2.3.b by providing details of insecure network protocols or ports that are allowed or denied within the organizational network infrastructure and insecure processes are starting or stopping via investigations and reports.		

PCI DSS v3.2.1 Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Requirement-3: Protect stored cardholder data **3.6.7** Prevention of unauthorized substitution of cryptographic keys.	EventTracker Supports for 3.6.7 by providing details of key integrity activity via investigations and reports on EventTracker's change audit agent. EventTracker's change audit can be configured to monitor key file or directory activity, deletions, modification, and permission changes. The change audit capability is completely automated; the agent can be configured to either scan for files/directory changes on a schedule can automatically detect file integrity activity in real-time.	Yes	Yes
Requirement-4: Encrypt transmission of cardholder data across open, public networks **4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	EventTracker supports for 4.1 by providing details of insecure network protocols or ports that are allowed or denied within the organizational network infrastructure and insecure processes that are starting or stopping via investigations and reports. EventTracker is capable of alarming on conditions where a system observes unencrypted information passed when encrypted traffic is expected.	Yes	Yes
Requirement-5: Use and regularly update anti-virus software or programs **5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	EventTracker supports for 5.1 by verifying that the service is running on the systems commonly affected malware and detecting or alerting on changes to the service.	Yes	Yes
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current. • Perform periodic scans. • Generate audit logs which are retained per PCI DSS Requirement 10.7.	EventTracker supports for 5.2.b by providing alarms on antivirus critical or error conditions and also provides detailed information on malware and antivirus detection via investigations and reports. Detection for when new signatures are installed is also supported. EventTracker supports for 5.2.c by providing visibility to antivirus signature updates and scanning activities, successes and failures via alarms, investigations, and reports. EventTracker's centralized log collection, management, and archival functionality directly supports PCI-DSS control requirement 5.2.d by automating the process of collecting and retaining the antivirus software audit trails. EventTracker creates archive files of all collected antivirus log entries which are organized in a directory structure by day making it easy to store, backup, and destroy log archives based on retention policy.		
Requirement-6: Develop and maintain secure systems and applications **6.1** Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	EventTracker supports 6.1.a by providing alarms on software update critical or error conditions and also by providing details on software update conditions via investigations and reports. EventTracker is able to support 6.1.b by running reports and showing that specific patches are deployed within one month.	Yes	Yes
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	EventTracker supports for 6.3.a by providing an intelligence system for logs to be sent to rules that can be created to provide proper alarming, reporting, and enhancement to the abilities of any custom application to be used in the cardholder data environment.		
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	EventTracker supports for 6.4.1 by providing details on allowed or denied network protocols or ports between the test network environment and all other internal production network environments via investigations and reports.		

PCI DSS v3.2.1 Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
6.4.2 Separation of duties between development/test and production environments.	EventTracker supports for 6.4.2 by providing details on allowed or denied network traffic between the test network environment and all other internal network environments via investigations and reports.	Yes	Yes
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. **6.5.2** Buffer overflows. **6.5.3** Insecure cryptographic storage. **6.5.4** Insecure communications. **6.5.5** Improper error handling. **6.5.7** Cross-site scripting (XSS). **6.5.8** Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions. **6.5.9** Cross-site request forgery (CSRF).	EventTracker supports for 6.5 by providing alarms and investigation details on all detected vulnerabilities.		
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.	EventTracker supports for 6.6 by providing alarms and investigation details on detected vulnerabilities. EventTracker can address either solution by working in conjunction with web exploit systems, such as Intrusion Detection Systems, Web-Application Firewalls, Stateful Inspection Firewalls, Web Servers, and other log sources to analyze detected potential abuses as well as provide a way to investigate suspected breaches.		
Requirement-7: Restrict access to cardholder data by business need to know. **7.1.1** Define access needs for each role, including: • System components and data resources that each role needs to access for their job function. • Level of privilege required (for example, user, administrator, etc.) for accessing resources." **7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	EventTracker supports for 7.1.1 and 7.1.2 by providing details on privileged access, host authentication, application access via investigations and reports. Access to cardholder data can be monitored by the custodian(s) of the data in real-time by collecting access control system data. Account creation, privilege assignment and revocation, and object access can be validated using EventTracker.	Yes	Yes

PCI DSS v3.2.1 Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Requirement-8: Assign a unique ID to each person with computer access **8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components. **8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data. **8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. **8.1.3** Immediately revoke access for any terminated users. **8.1.4** Remove/disable inactive user accounts within 90 days. **8.1.5** Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use. **8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts. **8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	EventTracker supports for procedure 8.1 by providing details on account management activity such as account creation, account deletion, and account modification via reports. Account creation can be monitored through reporting and investigations of logs pertaining to the creation and modification of accounts.	Yes	Yes
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication method as follows: • Generic User IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer and system components. **8.5.1** Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	EventTracker supports for procedure 8.5 by providing alarms on database account access granting or revocation and details on account management, account granting or revocation, and authentication activity via investigations and reports. EventTracker also provides details on vendor account management and authentication activity via investigations and reports.		
Requirement-9: Restrict physical access to cardholder data. **9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. **9.1.1** Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	EventTracker provides alarms, investigations, and reports to support PCI-DSS control requirement 9.1. EventTracker supports for 9.1 and 9.1.1.c by providing alarms for physical access failures and details on other physical access activity via investigations and reports.	Yes	Yes

PCI DSS v3.2.1 Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Requirement-10: Track and monitor all access to network resources and cardholder data **10.2** Implement automated audit trails for all system components to reconstruct the following events: **10.2.1** All individual user accesses to cardholder data. **10.2.2** All actions taken by any individual with root or administrative privileges. **10.2.3** Access to all audit trails. **10.2.4** Invalid logical access attempts. **10.2.5** Use of and changes to identification and authentication mechanisms-including but not limited to creation of new accounts and elevation of privileges-and all changes, additions, or deletions to accounts with root or administrative privileges. **10.2.6** Initialization, stopping, or pausing of the audit logs. **10.2.7** Creation and deletion of system level objects.	EventTracker supports 10.2 by providing the core function of centralized log collection, management, and archival. EventTracker provides alarms on authentication failures from default, disabled, terminated, privileged accounts, object disposal failures and audit log initializations. EventTracker provides details of user access failures or successes to audit log files, cardholder data files, system-level objects, and applications via investigations and reports. EventTracker provides details of privileged account management such as creation, deletion, modification, authentication failures and successes, granting or revoking of access, privilege escalation and failures or successes to access files, objects, and applications via investigations and reports. EventTracker also provides details on the creation and deletion of system level objects and audit log initializations via investigations and reports.	Yes	Yes
10.3.1 User identification. **10.3.2** Type of event.	EventTracker supports 10.3 by parsing account and login information, assigning each log event a specific classification type, specifying a centralized time stamp, extracting success or failure information, identifying the host, IP, application, login originating each event, identifying affected data, components, resources and other details useful for forensic investigation of the audit logs.		
10.3.3 Date and time. **10.3.4** Success or failure indication. **10.3.5** Origination of event. **10.3.6** Identity or name of affected data, system component, or resource.	EventTracker supports 10.3.3 by independently synchronizing the timestamps of all collected log entries, ensuring that all log data is time-stamped to a standard time regardless of the time zone and clock settings of the log source.		
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	EventTracker supports 10.4 by independently synchronizes the timestamps of all collected log entries, ensuring that all log data is time-stamped to a standard time regardless of the time zone and clock settings of the logging hosts.		
10.5.1 Limit viewing of audit trails to those with a job-related need. **10.5.2** Protect audit trail files from unauthorized modifications. **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. **10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	EventTracker supports 10.5 by using discretionary access controls which allow restriction of the viewing of audit logs to individuals based on their role and Need-To-Know. EventTracker protects audit trails from unauthorized modification by immediately archiving, hashing and storing collected logs in a secure central repository. EventTracker includes an integrated change audit which can ensure that the collection infrastructure is not tampered with. EventTracker servers utilize access controls at the operating system and application level to ensure log data cannot be modified or deleted. Alerts are customizable to prevent or allow alarms on a case-by-case basis, including not causing an alert with new data being added. EventTracker securely collect logs from the entire IT infrastructure including external-facing technologies for storage on an internal LAN Network where a EventTracker resides.		

PCI DSS v3.2.1 Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	EventTracker supports 10.6 by supplying a one stop repository from which to review log data from across the entire IT infrastructure. Reports can be generated and distributed automatically on a daily basis which provides an audit trail of who did what within EventTracker and proof of log data review.	Yes	Yes
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	EventTracker supports 10.7 by automating the process of retaining audit trails. EventTracker creates archive files of all collected log entries which are organized in a directory structure by day making it easy to store, backup, and destroy log archives based on retention policy.		
Requirement-11: Regularly test security systems and processes **11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	EventTracker supports for procedure 11.1.d by providing alarms on the detection of rouge access points and also by providing details of detected rouge access points via investigations and reports.		
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	EventTracker provides alarms, investigations and reports to support PCI-DSS control requirement 11.4. Collecting logs from network and host based IDS/IPS systems, its risk-based prioritization and alerting reduce the time and cost associated with monitoring and responding to IDS/IPS alerts. EventTracker provides built-in alarms which can alert on IDS/IPS detected events such as attacks, compromises, denial of services, malware, reconnaissance activity, suspicious activity, and IDS/IPS signature update failures. EventTracker provide details around these critical IDS/IPS events via investigations and reports.		
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	EventTracker supports 11.5 by providing details of key integrity activity via investigations and reports on EventTracker's Change Audit Agent. EventTracker's Change Audit can be configured to monitor key file or directory activity, deletions, modification, and permission changes. The file integrity capability is completely automated, the agent can be configured to either scan for files or directory changes can automatically detect file integrity activity in real-time.		
Requirement-12: Maintain a policy that addresses information security for employees and contractors. **12.3.8** Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. **12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	EventTracker provides investigations and reports to support PCI-DSS control requirement 12.3 EventTracker supports for 12.3 by providing alarms on vendor authentication failures and on vendor account accounts access granting. EventTracker provides details on vendor account management activity, vendor authentication successes or failures, and remote session time outs via investigations and reports. EventTracker supports by providing real-time enterprise detection intelligence to address issues quickly to prevent damage and exposure. EventTracker provides alarms and detail on security events such as attacks, compromises, denial of services, malware, reconnaissance activity, suspicious activity, and IDS/IPS signature update failures via investigations and reports.	Yes	Yes

References

https://www.pcisecuritystandards.org/documents/PCI_DSS_Summary_of_Changes_3-2-1.pdf

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf