



NETFORENSICS SOLUTION GUIDE

# Achieving PCI DSS Compliance with Cinxi

**Compliance with PCI is complex.** It forces you to deploy and monitor dozens of security controls and processes. Data from these quickly overwhelm compliance efforts without automation. Your organization will save time and money by automating elements of PCI compliance such as log management, event-correlation, alerting, remediation, and reporting. nFX Cinxi One from netForensics provides these functions on a single easy-to-install, simple-to-use appliance.

This guide will show you how features of Cinxi fulfill more than 75 requirements of the PCI Data Security Standard. It parses the Standard section-by-section and annotates exactly what the appliance does for compliance with each one. Some benefits are process-related. Many help you to automatically integrate security data from multiple sources for instant views on particular aspects of compliance. Reports provide automatic documentation for auditors. Examples of 15 reports are included in this guide.

## Goal – Build and Maintain a Secure Network

### Requirement 1 – Install and maintain a firewall configuration to protect cardholder data.

Cinxi assists by clearly defining and grouping your assets that protect networks with PCI data — such as PCI firewalls, PCI routers, and PCI IDS/IPS. You can then use those groups within rules and notifications to isolate and detect any potential security issues or incidents pertaining to these security devices. You can also define these assets using templates within the Requirement 1 section of Cinxi PCI reports to view asset detail, incident/case detail, violation by rule, and summary data just for those assets that protect PCI network segments.

#### 1.1 – Establish firewall and router configuration standards that include the following...

Any firewalls and routers that connect to or protect cardholder data (as defined in PCI DSS) should feed security events into Cinxi. This should include firewall configuration changes. It's important to create rules within Cinxi to look for any configuration change events related to firewalls.

##### 1.1.1 – A formal process for approving and testing all external network connections and changes to the firewall and router configurations.

Once you create this process, Cinxi can help ensure that all configuration changes conform to this process.

##### 1.1.2 – Current network diagram with all connections to cardholder data, including any wireless networks.

Cinxi's editable network topology feature might be a good place to start in creating this diagram, though many companies will want to use a dedicated application like Microsoft Visio to include devices, networks, and pathways not included as part of the Cinxi topology diagram.

##### 1.1.3 – Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.

You must implement these firewalls as required, and should feed all security event data into Cinxi.

##### 1.1.4 – Description of groups, roles, and responsibilities for logical management of network components.

The PCI Asset Detail Reports included in Cinxi will list out the network components defined as assets with their respective names, values, addresses, locations, departments, and owners.

##### 1.1.5 – Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

Use Cinxi to generate incidents on any traffic or attempted connections on ports not permitted, for added security and to inform you of a configuration change.

##### 1.1.6 – Requirement to review firewall and router rule sets at least every six months.

This does not pertain to data available within Cinxi.

#### 1.2 – Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.

These external firewalls should feed events into Cinxi.

##### 1.2.1 – Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

Cinxi rules are useful in determining when these configurations are changed.

##### 1.2.2 – Secure and synchronize router configuration files.

Cinxi configuration change rules will help confirm when rule changes take place.

**1.2.3 – Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny any traffic from the wireless environment or to control any traffic (if such traffic is necessary for business purposes).**

Cinxi rules can be used to confirm that data from the wireless network is not permitted into the cardholder data portion of the network by generating incidents any time such traffic is detected.

**1.3 – Prohibit direct public access between the Internet and any system component in the cardholder data environment.**

This is an important configuration principle which will be reflected in your Cinxi network topology diagram.

**1.3.1 – Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.**

You should define the DMZ as a separate network and/or put the assets into a separate group from your cardholder data area in the Cinxi Assets configuration.

**1.3.2 – Limit inbound Internet traffic to IP addresses within the DMZ.**

**1.3.3 – Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.**

**1.3.4 – Do not allow internal addresses to pass from the Internet into the DMZ.**

**1.3.5 – Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.**

You can create Cinxi rules to looking for this type of activity, in violation of policy and approved configurations.

**1.3.6 – Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)**

This does not pertain to data available within Cinxi.

**1.3.7 – Place the database in an internal network zone, segregated from the DMZ.**

This does not pertain to data available within Cinxi, but will be reflected in your topology diagram and asset information.

**1.3.8 – Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies — for example, port address translation (PAT).**

This does not pertain to data available within Cinxi.

**1.4 – Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.**

This does not pertain to data available within Cinxi, though Cinxi can receive events from devices that are used to control access (for example, NAC devices).

**Requirement 2 – Do not use vendor-supplied defaults for system passwords and other security parameters.**

**2.1 – Always change vendor-supplied defaults *before* installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).**

This does not pertain to data available within Cinxi. The Cinxi itself will allow you to change its own default passwords as part of the installation process. This is highly recommended.

**2.1.1 – For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.**

This does not pertain to data available within Cinxi.

**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.**

**2.2.1 – Implement only one primary function per server.**

This does not pertain to data available within Cinxi.

**2.2.2 – Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).**

Cinxi can help you determine if there are rouge services operating on particular services or devices by identifying specific ports in device messages that are not permitted for that device.

**2.2.3 – Configure system security parameters to prevent misuse.**

As with much of Requirement 1, Cinxi can let you know when configurations change.

**2.2.4 – Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.**

Cinxi itself is stripped to bare required functionality for maximum device security. You can also use it to detect rouge communications on your network by looking for messages indicating activity on specific ports from unauthorized hosts.

**2.3 – Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.**

This does not pertain to data available within Cinxi, though Cinxi itself relies on SSH and SSL for security administrative access.

**2.4 – Shared hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in "Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers."**

This does not pertain to data available within Cinxi.

## Goal – Protect Cardholder Data

### Requirement 3 – Protect stored cardholder data.

Cinxi can assist by clearly defining and grouping your assets that store and protect stored cardholder data using asset groups. You can then use those groups within rules and notifications to isolate and detect any potential security issues or incidents pertaining to cardholder data. You can also define these assets using templates within the Requirement 3 section of Cinxi PCI reports to view asset detail, incident/case detail, violation by rule, and summary data just for those assets that contain PCI cardholder data.

**3.1 – Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.**

This does not pertain to data available within Cinxi.

**3.2 – Do not store sensitive authentication data after authorization (even if encrypted). (Sensitive authentication data includes the data as cited in the following Requirements, 3.2.1 through 3.2.3.)**

This does not pertain to data available within Cinxi.

**3.3 – Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).**

This does not pertain to data available within Cinxi, though it is important to note that Cinxi will display any data it finds within messages to authorized Cinxi users. Devices and hosts should never send Cinxi messages that contain sensitive cardholder data, including PAN.

**3.4 – Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs) by using any of the following approaches...**

This does not pertain to data available within Cinxi.

**3.5 – Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.** You can have systems that manage cryptographic keys as well as systems that rely on them for authentication send event messages into Cinxi for monitoring.

### 3.5.1 – Restrict access to cryptographic keys to the fewest number of custodians necessary

### 3.5.2 – Store cryptographic keys securely in the fewest possible locations and forms.

You can create authentication template rules within Cinxi to look for any non-authorized authentication events, including those using cryptographic key systems. You can also report on all authentication events against sensitive assets within Cinxi PCI Reports, including using templates for those reports for key privileged user IDs.

### 3.6 – Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following...

This section and the subsections do not pertain to data available within Cinxi.

## Requirement 4 – Encrypt transmission of cardholder data across open, public networks.

You should feed events from any devices that are used to encrypt cardholder data into the Cinxi appliance (such as VPN devices and wireless security devices). You can then use Cinxi to implement general security rules looking for incidents pertaining to those systems, as well as report incidents, risk, and summary information across those devices. It is best to group them together within an asset group and use templates in reporting to facilitate reporting on this requirement.

### 4.1 – Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.

Send events from encryption devices into Cinxi.

### 4.1.1 – Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment; use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

Send events from wireless security devices into Cinxi.

### 4.2 – Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, and chat).

You may use an email gateway or other DLP device to ensure this type of leak does not occur. If so, send events from these devices into Cinxi.

## Goal – Maintain a Vulnerability Management Program

### 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).

Cinxi can receive feeds from a number of centralized AV management consoles. You can use this information alone or in conjunction with other events to provide an integrated picture of network security events as it relates to PCI.

#### 5.1.1 – Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

Cinxi normalized categories are able to distinguish between different types of device alerts for the different categories of malware listed here, assuming the original malware detection software makes these distinctions in its event logging.

#### 5.2 – Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

While most of this is outside of the scope of Cinxi data, Cinxi can alert users when any device (including AV servers) has failed to send parsable events into the system for a specified amount of time. This is one way to determine if you have fallen out of compliance with this section of the PCI DSS.

## nFX Cinxi One Solution

1. Use "Incident Generating Threat Classes by Week Report."
2. Add threat classes for "Malicious" and "Anomalous Behavior."
3. Use reports for Week and Month. PCI reports should have reporting period for the last 90 days.

### Reports:

- Requirement 5 – Weekly Malicious Incidents Report
- Requirement 5 – Monthly Malicious Incidents Report

- Requirement 5 – Last 3 Month Malicious Incident Report
- Requirement 5 – Yearly Malicious Incident Report

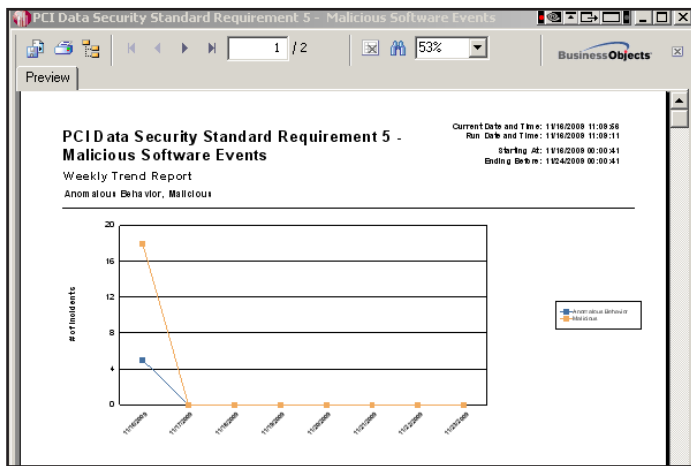


Figure 1 – Example: Weekly Trend Report

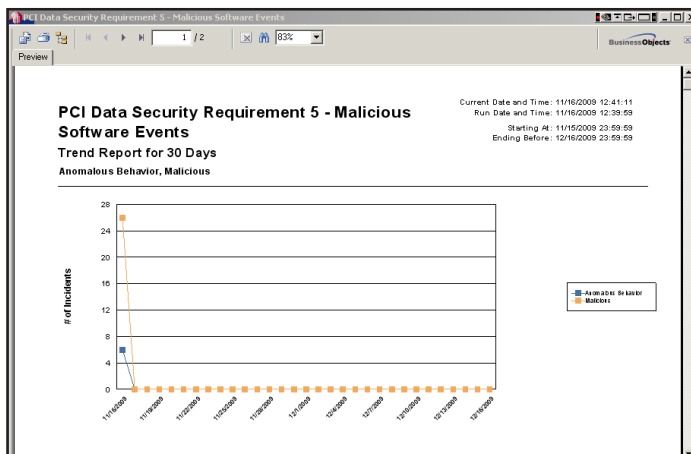


Figure 2 – Example: Monthly Trend Report

**Requirement 6 – Develop and maintain secure systems and applications.**

**6.1 – Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.**

Using Cinxi in combination with a vulnerability assessment tool and IDS/IPS will help determine where you are failing to meet this requirement, and what types of attacks have taken place on vulnerable systems. Cinxi includes a system rule that automatically detects targeted attacks on known vulnerable systems.

**6.2 – Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.**

While there are many sources of this information, Cinxi includes a built-in display area in the main GUI for key RSS feeds that pertain to new security issues and vulnerabilities. You can customize this feed display and include RSS feeds specific to your environment.

**6.3 – Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development lifecycle...**

This requirement and its subsections apply to custom-developed software applications maintained by an organization. Most of this information is outside the direct scope of Cinxi. It is important to note, however, that once custom applications are developed according to the standards of PCI DSS 6.3, you can and should send their event log feeds into Cinxi through syslog where they can be parsed using custom parsers developed within the included Cinxi Device Builder component. This will ensure that even your custom applications are supported and provide useful security information relevant to PCI.

**6.4 – Follow change control procedures for all changes to system components...**

This does not pertain to data available within Cinxi.

**6.5 – Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following...**

Similar to section 6.3, most of this is outside the scope of Cinxi other than the fact that you should feed all web application event data into Cinxi. Cinxi supports event feeds from many popular web servers and can be useful in detecting security issues associated with web applications built on these platforms.

**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.
- Installing a web-application firewall in front of public-facing web applications.

Whichever of the two methods is chosen (vulnerability scanners or firewall), you should send events into Cinxi and organize them as a device used to protect PCI assets.

### Goal – Implement Strong Access Control Measures

#### Requirement 7 – Restrict access to cardholder data by business need to know.

**7.1 – Limit access to system components and cardholder data to only those individuals whose job requires such access...**

**7.2 – Establish a mechanism for system components with multiple users that restricts access based on a user’s need to know and is set to “deny all” unless specifically allowed...**

Most of Requirement 7 is managed outside of the Cinxi system. You can, however, use Cinxi to confirm enforcement of this requirement by monitoring unauthorized system access attempts through rules and alerts, and reviewing access through reporting.

### nFX Cinxi One Solution

#### Report Categories:

- Information.ACL.Allow
- Information.ACL.Deny
- Information.Authentication.Failure
- Information.Authentication.Success

Users should be able to specify devices. Although there is no device group implementation, it would be better to specify device groups: PCI Firewalls, PCI Routers, PCI DMZ Servers, PCI Internal Servers, PCI Wireless, PCI POS Servers, PCI Database Servers, PCI DNS Servers, PCI Web Servers.

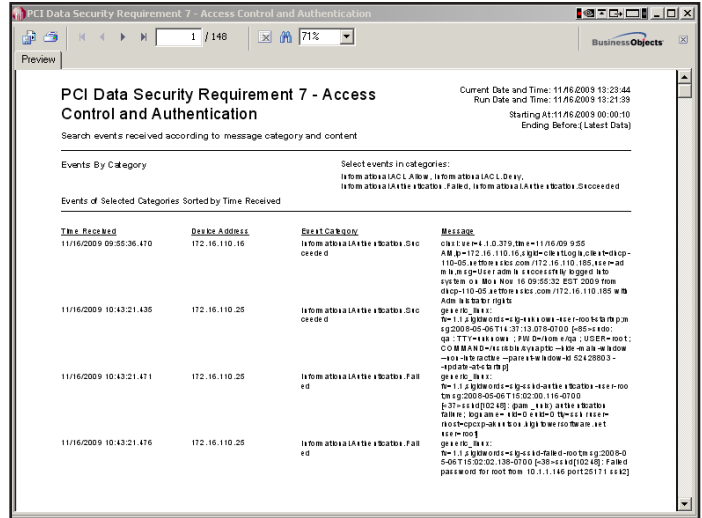


Figure 3 – PCI DSS R7 – Access Control and Authentication Report

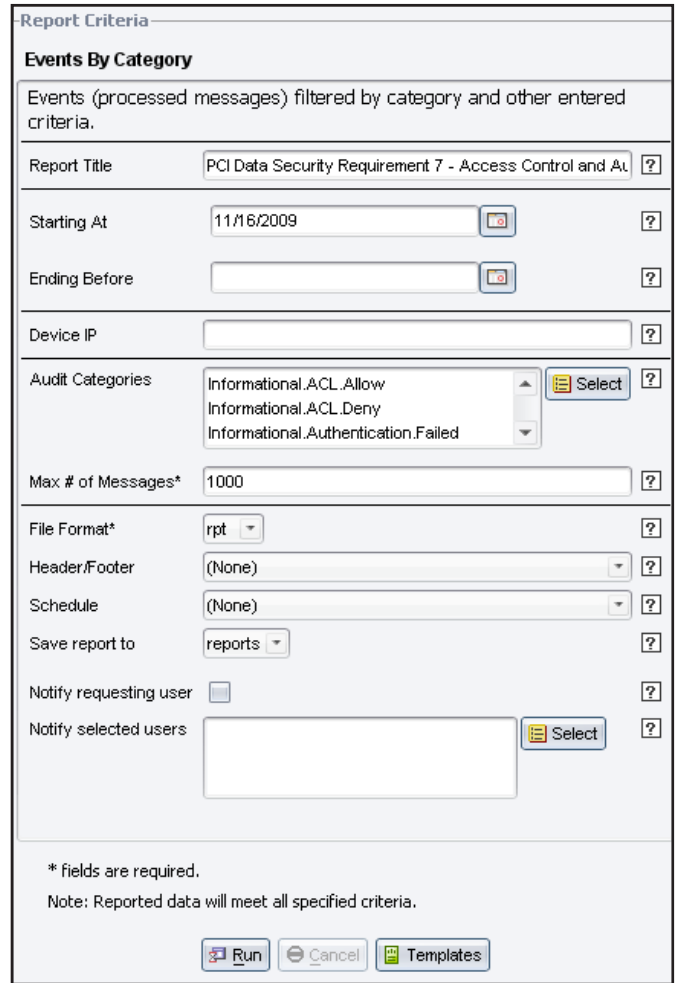


Figure 4 – Example: Events by Category Report

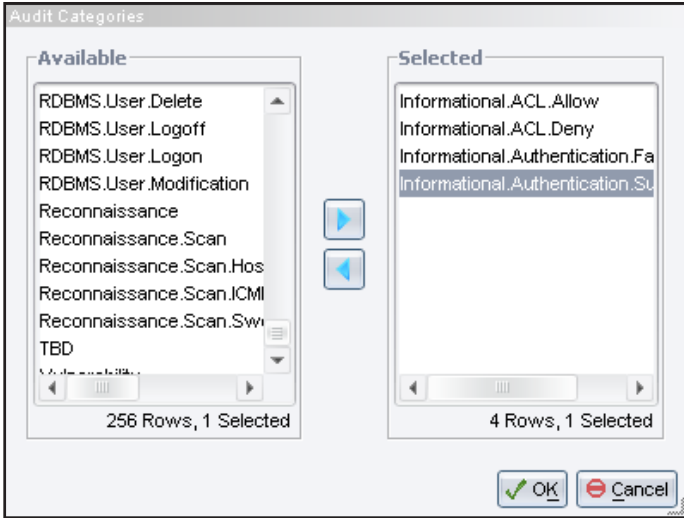


Figure 5 – Example: Audit Categories Report

**Report:** Requirement 7 – VPN Client and Remote Access Events

- Use Events by Category Report

**Report Categories:**

- Information.VPN.Client.Failed
- Information.VPN.Client.Succeeded
- PolicyViolation.RemoteAccess
- PolicyViolation.RemoteAccess.Confirm

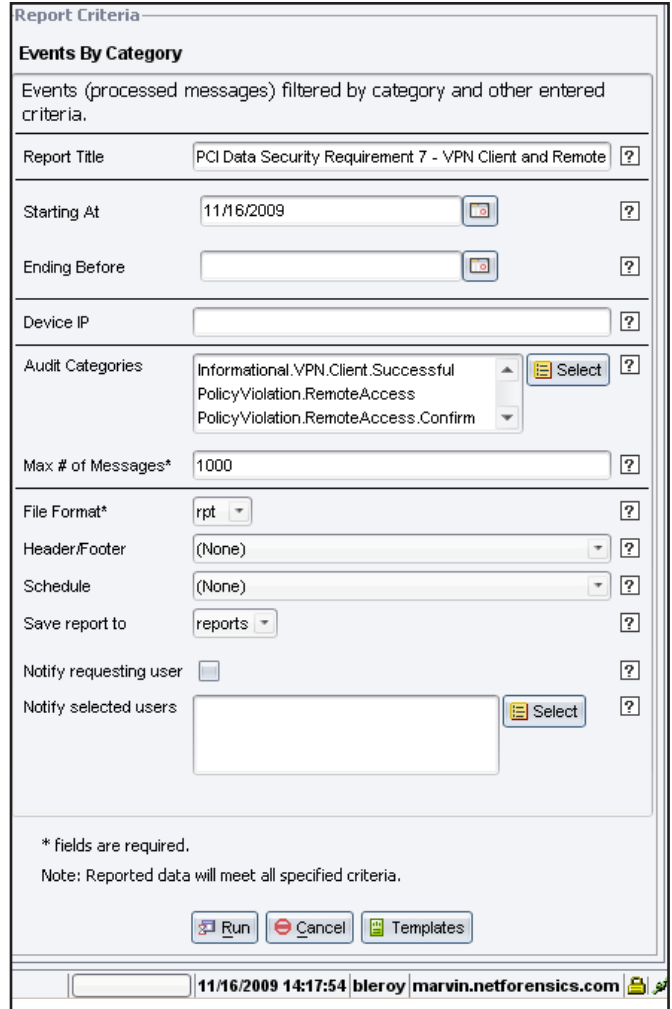


Figure 7 – Example: Events by Category Report

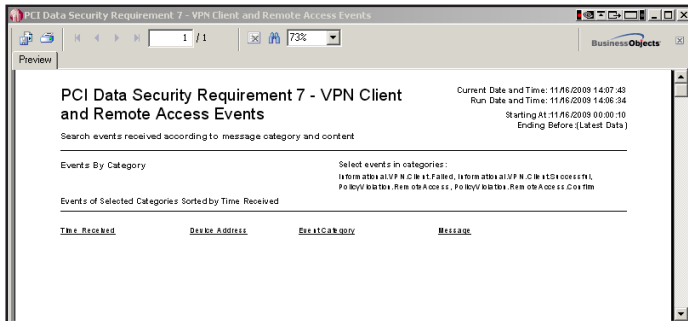


Figure 6 – PCI DSS R7 – VPN Client and Remote Access Events

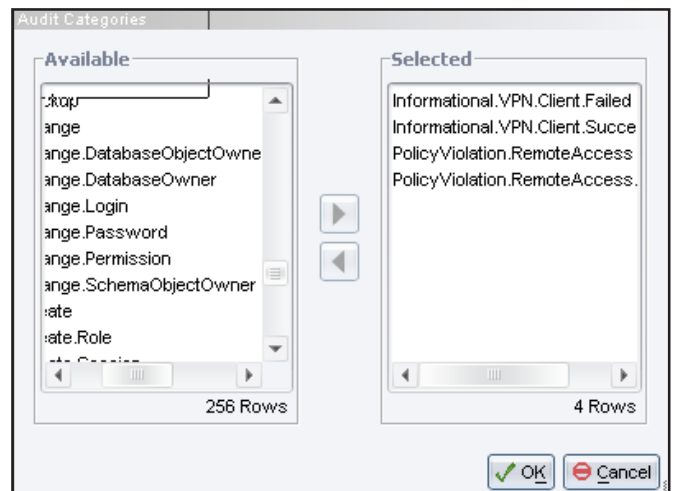


Figure 8 – Example: Audit Categories Report

**Report Name:** Requirement 7 – Restricted File Access Control

- Use Events by Category Report

**Report Categories:**

- Informational. FileAccess and File Access Created, Deleted and Modified
- Malicious. FileAccess and Malicious. FileAccess. Attempt

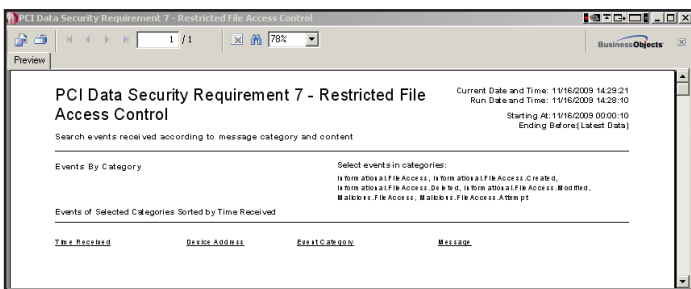


Figure 9 – PCI DSS R7 – Restricted File Access Control

**Report Criteria**

**Events By Category**

Events (processed messages) filtered by category and other entered criteria.

Report Title: PCI Data Security Requirement 7 - Restricted File Access

Starting At: 11/16/2009

Ending Before:

Device IP:

Audit Categories: Malicious.FileAccess.Attempt, Informational.FileAccess, Informational.FileAccess.Deleted

Max # of Messages\*: 1000

File Format\*: rpt

Header/Footer: (None)

Schedule: (None)

Save report to: reports

Notify requesting user:

Notify selected users:

\* fields are required.  
Note: Reported data will meet all specified criteria.

Run Cancel Templates

11/16/2009 14:34:21 bleroy marvin.netforensics.com

Figure 10 – Example: Events by Category Report

**Report:** PCI Security Requirement 7 – Weekly Authentication and Policy Access Failures

- Use Incident-Generating Message Category by Week/ Month/Yearly Report
- Change Report Name and Incident Categories to include:

**Report Categories:**

- Informational. Authentication.Failed
- PolicyViolation. Access
- PolicyViolation. FileTransfers

- PolicyViolation.RemoteAccess
- PolicyViolation.RemoteAccess.Confirm
- Information.ACL.Deny

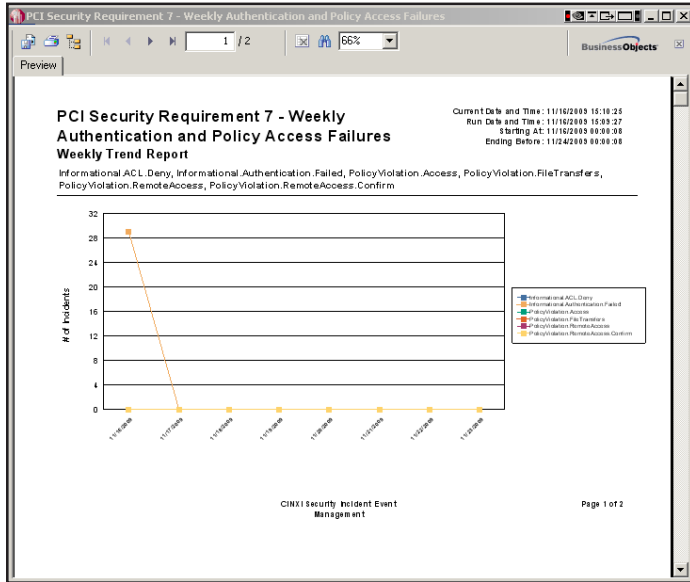


Figure 11 – Example: PCI Security Requirement 7 Report

NOTE: The current implementation of Events by Category Reports has the trending data by week, month, 2 months, 6 months, and 1 year. PCI DSS requires the reports remain online for 3 months and offsite for at least 1 year.

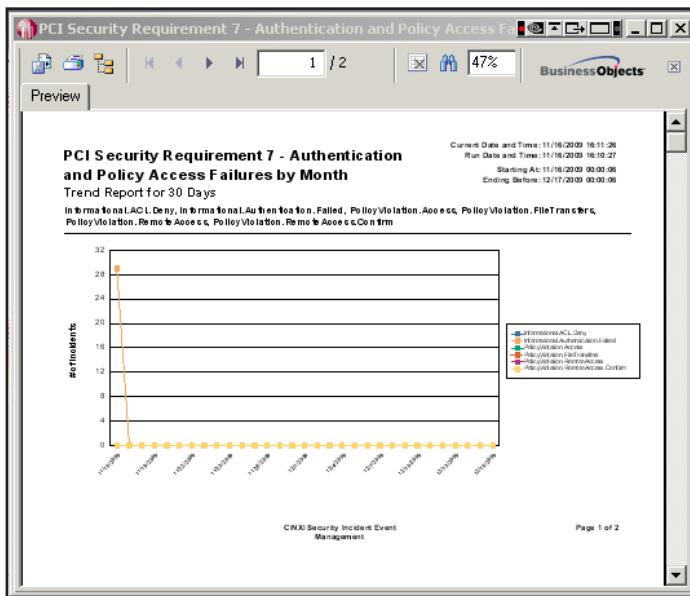


Figure 12 – Example: PCI Security Requirement 7 Report

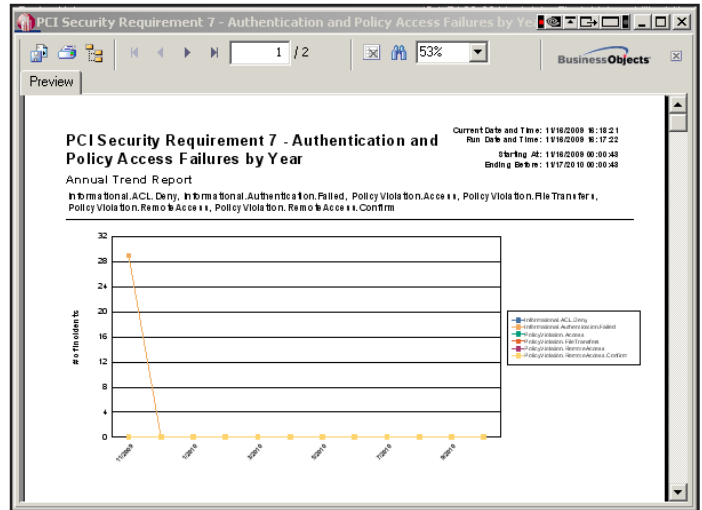


Figure 13 – Example: PCI Security Requirement 7 Report

**Report Criteria**

**Incident-Generating Message Categories by Week**

This report provides a trend of incidents involving selected message categories over a period of one week.

Report Title: PCI Security Requirement 7 - Weekly Authentication and F ?

Starting At\*: 11/16/2009 ?

Message Categories\*: PolicyViolation.RemoteAccess, PolicyViolation.RemoteAccess.Confirm, Informational.ACL.Deny [Select] ?

File Format\*: rpt ?

Header/Footer: (None) ?

Schedule: (None) ?

Save report to: reports ?

Notify requesting user:  ?

Notify selected users: [Select] ?

\* fields are required.  
Note: Reported data will meet all specified criteria.

[Run] [Cancel] [Templates]

Figure 14 – Example: Incident-Generating Message Categories by Week Report

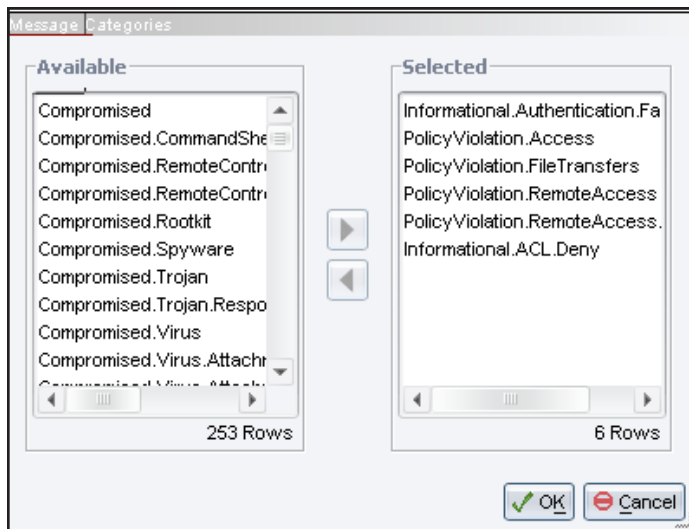


Figure 15 – Example Categories for PCI Requirement 7: Weekly, Monthly, Yearly Failed Authentication and Policy Access Failures

## Requirement 8 – Assign a unique ID to each person with computer access.

### 8.1– Assign all users a unique ID before allowing them to access system components or cardholder data.

Complying with this requirement will improve the value of the log and event data that Cinxi aggregates and correlates by helping to ensure that logged activity can be associated with specific user accounts.

### 8.2 – In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Password or passphrase
- Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)

Cinxi can normalize successful and failed authentication events through whichever of the above authentication methods you chose and implement. These can give you insight into abnormal account activity and attempted account compromises.

### 8.3 – Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access

controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates. Cinxi can monitor these authentication systems for abnormal behavior.

### 8.4 – Render all passwords unreadable during transmission and storage on all system components using strong cryptography.

This does not pertain to data available within Cinxi.

### 8.5 – Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows...

Most of the sub-requirements here outline best practices around account controls and user authentication. You can use Cinxi to highlight some key areas addressed in this section. For example, you can use Cinxi to monitor account creations, changes, deletions, including combining information about other security events with these types of account changes, highlighting potential security breaches. Cinxi rules can also incorporate temporary user account lists to dynamically monitor the account activities of recently terminated employees.

## Requirement 9 – Restrict physical access to cardholder data.

This entire requirement pertains to physical access, and therefore does not pertain to network security data available within Cinxi.

## Goal – Regularly Monitor and Test Networks

### Requirement 10 – Track and monitor all access to network resources and cardholder data.

Requirement 10 is the most relevant part of PCI DSS for Cinxi, as Cinxi is primarily a log management and security information management system.

### 10.1 – Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

Access to system components is generally linked to individual user accounts and individual users through OS-level logging as well as logging performed by other authentication systems and other tracking mechanisms. This data, along with source IP and other information in the events, should be fed back to Cinxi for central collection, monitoring, and reporting.

## 10.2 – Implement automated audit trails for all system components to reconstruct the following events...

Cinxi accepts events from devices to create an audit trail, but it does so depending on having your devices properly configured to log these events and send them to Cinxi. Assuming this is true, Cinxi will be a key part of reconstructing the events covered in this requirement.

### 10.2.1 – All individual user accesses to cardholder data.

Cinxi can obtain this information from authentication systems, object access controls, and similar logging mechanisms.

### 10.2.2 – All actions taken by any individual with root or administrative privileges.

Cinxi can obtain this information from any of your logging and audit systems, and then use this information within rules and reports. There are several privileged user account reports available out of the box within Cinxi, and it is easy to expand existing reports to cover other administrative users.

### 10.2.3 – Access to all audit trails.

If this is logged within a device, it will be available within Cinxi for rules and reporting.

### 10.2.4 – Invalid logical access attempts.

This type of activity is generally available from devices and is therefore available within Cinxi for rules and reporting.

### 10.2.5 – Use of identification and authentication mechanisms.

Cinxi can obtain this information from identification and authentication systems and make it available for use within rules and reports.

### 10.2.6 – Initialization of the audit logs.

Cinxi will track initialization and changes to audit logs and logging facilities (for example, restart of syslog or Snare service).

### 10.2.7 – Creation and deletion of system-level objects.

This type of activity is generally available from devices and is therefore available within Cinxi for rules and reporting.

## 10.3 – Record at least the following audit trail entries for all system components for each event...

### 10.3.1 – User identification.

Cinxi retains user information in a number of ways, including IP address, workstation name, and user name from raw message. Much of what we obtain is a function of the format of and information within the original device event.

### 10.3.2 – Type of event.

Cinxi preserves the original event data, which usually includes a "signature" component. Cinxi also normalizes events into categories based on the type of event it is. This greatly improves your ability to create rules and run reports on event type.

### 10.3.3 – Date and time.

Cinxi records the date and time of all received events.

### 10.3.4 – Success or failure indication.

Cinxi records the success or failure status of received events where this type of status applies (for example, successful or failed logins, and permitted or blocked ACL messages).

### 10.3.5 – Origination of event.

Cinxi records the origination of the event as the reporting device IP information, along with source and destination information contained within the event when applicable.

### 10.3.6 – Identity or name of affected data, system component, or resource.

Cinxi records source and destination data when applicable (for example, on a firewall ACL event, or on a remote logon to a VPN system). Other data (system component, service name, protocol) are retained when present in the original device event message.

## 10.4 – Synchronize all critical system clocks and times.

Cinxi system time, which is used to generate time stamps on received messages in addition to any within the device message itself, can be synchronized using the NTP protocol with a standardized time source.

## 10.5 – Secure audit trails so they cannot be altered.

This is a core function of Cinxi. One very simple way Cinxi achieves this is by simply recording the events from most devices on a different system from the device itself in real time. This means that an intruder that attempts to alter or remove the logs chronicling their activities on the server will be unable to

affect the logs on the Cinxi device. This also provides additional security through separation of duties in many cases.

Further, Cinxi employs integrity validation on raw log files aggregated on the Cinxi appliance, to ensure that modification of logs on Cinxi cannot occur undetected.

#### **10.5.1– Limit viewing of audit trails to those with a job-related need.**

By storing logs separately from the devices that generate them, and employing roles-based access controls on the log and event data within Cinxi, security administrators can easily limit access to audit trails to those with a job-related need.

#### **10.5.2 – Protect audit trail files from unauthorized modifications.**

Access controls on the raw log data stores and relational events databases on Cinxi make it very difficult if not impossible for unauthorized users to modify this data. In the very unlikely event that someone attempts to modify a raw log file within Cinxi, it will be easily detected because all raw log files have corresponding SHA512 digest files that are digitally signed with a private key. More importantly, this means that the administrator can prove that the log files stored on Cinxi are valid and retain their integrity.

#### **10.5.3 – Promptly back up audit trail files to a centralized log server or media that is difficult to alter.**

Cinxi itself is a centralized log server that provides protection against unauthorized access and modification of raw log files. Cinxi can also automate the process of archiving copies of your raw log data to another network location, providing an additional layer of security for the logs.

#### **10.5.4 – Write logs for external-facing technologies onto a log server on the internal LAN.**

Cinxi is usually placed on the internal LAN and can receive events from devices at the perimeter, DMZ, and internal LAN. By having secure copies of your logs and events on the Cinxi, you are meeting this requirement. You can also copy archives of raw logs from Cinxi to any other accessible location on the network (if, for example, Cinxi needs to sit in the DMZ for some reason).

#### **10.5.5 – Use file-integrity monitoring and 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).**

Cinxi tracks changes to log files and generates alerts when such events have occurred.

#### **10.6 – Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS); Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.**

This requirement makes it clear that logs of system components need to be reviewed daily for security devices and servers. This is impossible to do manually in most organizations, so the requirement makes it clear that automation tools may be used to meet the requirement. Cinxi provides all of the tools you need to automatically review each and every event that comes into the system. Cinxi gives you the ability to automatically correlate events spanning multiple devices over a period of time. Cinxi also provides all of the harvesting, parsing, and alerting functionality required by PCI and for a general best practices security infrastructure.

#### **10.7 – Retain audit trail history for at least one year, with a minimum of 3 months immediately available for analysis (for example, online, archived, or restorable from backup).**

Cinxi appliances are available with up to 7TB of usable internal storage space. This is more than enough for most organizations to keep 3 months of data online and ready for immediate analysis. Many organizations are able to keep far more than 3 months of storage online even with our smaller appliances. In addition, Cinxi supports the long-term archiving of log files, enabling you to free up more space of immediate online needs. The Cinxi data store is also self-managing, meaning that it will prioritize and rearrange storage without the need to manually purge data.

### **Requirement 11– Regularly test security systems and processes.**

#### **11.1 – Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.**

Physical detection of wireless access points is outside of the scope of data available within Cinxi, though a wireless IDS/IPS, if attached to the same network as Cinxi, can feed data into Cinxi.

You can configure Cinxi rules and alerts to immediately inform you when the wireless IDS/IPS detects an unauthorized wireless device.

**11.2 – Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, and product upgrades).**

Most popular vulnerability scanners can also feed their scan results into Cinxi. This is useful in detecting when an IDS/IPS event matches a known existing vulnerability for a particular destination.

**11.3 – Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment)...**

This does not pertain to data available within Cinxi.

**11.4 – Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.**

Cinxi supports most major IDS/IPS systems out of the box. netForensics also prioritizes IDS/IPS signature updates to ensure that we keep up with the latest threats. IDS/IPS devices are among the most useful devices to feed events into Cinxi. Cinxi helps you manage the huge number of events generated by such devices through prioritized correlation and alerting.

**11.5 – Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files, and configure the software to perform critical file comparisons at least weekly.**

Cinxi works with several popular file integrity monitoring tools. Cinxi receives events from the tool and can then process the event for use in rules, alerts, and reporting.

## Goal – Maintain an Information Security Policy

### Requirement 12 – Maintain a policy that addresses information security for employees and contractors.

While most of this requirement addresses the business need to create and disseminate written security policies, the enforcement of those policies can fall within the scope of security event data that Cinxi can monitor.

**12.1 – Establish, publish, maintain, and disseminate a security policy that accomplishes the following...**

This does not pertain to data available within Cinxi.

**12.2 – Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures and log review procedures).**

Daily (actually constant) log review is a primary function of Cinxi. As you develop these procedures, Cinxi will simplify the process of reviewing security events by correlating important events into a much more manageable number of incidents. Within Cinxi, you should develop a consistent process of reviewing important correlated incidents. Cinxi itself provides some guidance for dealing with specific security incidents, but the daily process of reviewing this data must fit within your organization's security policy.

**12.3 – Develop usage policies for critical employee-facing technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants [PDAs], e-mail usage, and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following....**

In general, usage policies are created outside of Cinxi and in some cases enforced on systems that can feed events into Cinxi. You can use Cinxi to create rules that alert you to violations or attempted violations of these security policies.

**12.4 – Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.**

This does not pertain to data available within Cinxi.

**12.5 – Assign to an individual or team the following information security management responsibilities...****12.5.1 – Establish, document, and distribute security policies and procedures.**

This does not pertain to data available within Cinxi.

**12.5.2 – Monitor and analyze security alerts and information, and distribute to appropriate personnel.**

Cinxi can be useful here for generating security alerts corresponding to your specific environment. The interface also includes a tool useful for monitoring RSS feeds of security alerts and information from third parties and vendors of your other security products.

**12.5.3 – Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.**

Most of this is performed outside of Cinxi, but Cinxi also includes customizable response procedure information for each rule and corresponding incident generated, as well as a best-practices incident response workflow within our case management tools.

**12.5.4 – Administer user accounts, including additions, deletions, and modifications.**

The activities of the team assigned these responsibilities, as well as those of other unauthorized parties performing this type of activity, should be fed into Cinxi for monitoring and analysis.

**12.5.5 – Monitor and control all access to data.**

The assignment of this responsibility is outside of the scope of Cinxi, but this type of activity can be monitored and analyzed within Cinxi.

**12.6 – Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.**

This requirement and its sub-requirements do not pertain to data available within Cinxi.

**12.7 – Screen potential employees prior to hire to minimize the risk of attacks from internal sources.**

This does not pertain to data available within Cinxi.

**12.8 – If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following...**

This does not pertain to data available within Cinxi.

**12.9 – Implement an incident response plan. Be prepared to respond immediately to a system breach.**

The bulk of this requirement and its sub-requirements should be performed outside of Cinxi. Cinxi, however, provides guidance and a framework for dealing with information security incidents, particularly within its rules, incidents, and case management components.

Cinxi's notification features can be used to alert specific users at specific times. This can be used to address the portion of this requirement (12.9.3) that requires 24/7 coverage. The fact that Cinxi aggregates data from IDS, IPS, file integrity, and other security systems and correlates across them also addresses sub-requirement 12.9.5.

## Meeting PCI Compliance — the Easy Way

Whether you're a small e-commerce site, mid-sized bank, large healthcare company, managed service provider, or any other type or size organization, nFX Cinxi One offers a flexible, powerful, cost-effective solution for meeting your PCI requirements. Most importantly, it can help you guard against online fraud, misuse of cardholder data, and ID theft — using one easy-to-implement, user-friendly appliance.