GFI White Paper

PCI-DSS compliance and GFI Software™ products

The Payment Card Industry Data Security Standard (PCI DSS) compliance is a set of specific security standards developed by the payment brands* to help promote the adoption of consistent data security measures that are needed to protect sensitive payment-card information

GFI Software™

Contents:

Introduction

The standard applies to all organizations which hold, process, or exchange cardholder information from any card branded with the logo of the payment brand companies*.

*Payment brand companies include American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International.

There are 12 PCI DSS requirements that have been organized into six logically related groups. Please see **Chart A** below.

Chart A - PCI DSS summary

	PCI REQUIREMENT
1. BUILD AND MAINTAIN A SECURE NETWORK	
Install and maintain a firewall configuration to protect cardholder data.	1
Do not use vendor-supplied defaults for system passwords and other security parameters.	2
2. PROTECT CARDHOLDER DATA	
Protect stored cardholder data.	3
Encrypt transmission of cardholder data across open, public networks.	4
3. MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	
Use and regularly update antivirus software or programs.	5
Develop and maintain secure systems and applications.	6
4. IMPLEMENT STRONG ACCESS CONTROL MEASURES	
Restrict access to cardholder data by business need-to-know.	7
Identify and authenticate access to system components	8
Restrict physical access to cardholder data.	9
5. REGULARLY MONITOR AND TEST NETWORKS	
Track and monitor all access to network resources and cardholder data.	10
Regularly test security systems and processes.	11
6. MAINTAIN AN INFORMATION SECURITY POLICY	
Maintain a policy that addresses information security for all personnel.	12

Simply stated, the basis of PCI DSS compliance is that merchants must demonstrate through representative systems and processes that they meet these requirements. It is the merchants' responsibility to achieve, demonstrate and maintain their compliance across all systems and processes in their organizations.

The required annual validation of compliance (internal or external) is dependent on the volume of card transactions, with larger volumes requiring more intensive external validation and those with a smaller number of card transactions needing only internal validation. Merchants with larger volumes of transactions must also have their compliance assessed by an independent assessor, a Qualified Security Assessor (QSA), while companies handling smaller number of transactions have the option of self-certification through a Self-Assessment Questionnaire (SAQ).

How GFI can assist in PCI DSS compliance

The remainder of this document outlines how GFI can assist you in meeting PCI DSS compliance. GFI Software is not in the services space and does not have a PCI service practice, and reading this document alone will not make you PCI compliant. The intent of this document is to provide you with GFI's understanding of the requirements, and how the GFI Software product line (in particular our products - GFI LanGuard™, GFI EventsManager™ and GFI EndPointSecurity™ can help you meet the PCI DSS compliance requirements created by the PCI Security Standards Council.

We have included several reference documents as part of this guide. For more detailed information regarding PCI DSS regulations, please see:

Chart B – GFI product – use in PCI DSS requirements **outlines, by PCI sub-requirement, how GFI products can help you in meeting these requirements.** GFI Software can assist with PCI compliance with the help of specific features built into its solutions, and with reports that are available in the products.

Chart C – PCI DSS requirements – GFI product reports provides links to the actual product report. Just click on the link to see the sample report!

Chart D – Summary of all PCI DSS requirements; and

Chart E – PCI DSS requirements support in GFI products.

GFI Software has three cost-effective solutions that can assist you in meeting PCI DSS compliance. These tools, GFI EventsManager, GFI LanGuard and GFI EndPointSecurity, can help you meet the PCI DSS requirements 1, 2, 3, 5, 6, 7, 10, 11, and 12.

This paper is based on the PCI DSS 3.1 available at
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

If you have any questions after reading this document, please do not hesitate to contact our sales representatives at +1 (888) 243-4329 or +1 919 379 3397 (outside the USA).

Chart B – GFI product – use in PCI DSS requirements

GFI product	Explanation	Value of GFI product to PCI compliance	Level of compliance*
GFI EventsManager	1.2 Requests examination and monitoring of the firewall/router configuration files in order to make sure that they are built in accordance with the PCI DSS specification.	**GFI EventsManager** can monitor changes in the configuration files of the network devices and report on those changes.	F, R
GFI LanGuard	1.4 Requests that personal firewall software is deployed on the employee computers that are connected to the Internet.	**GFI LanGuard** can automatically deploy personal firewall software in the entire network and report which computers in the network do not have personal firewalls installed.	F, R
GFI LanGuard	2.1 Requires analysis to make sure that systems do not use vendor-supplied defaults.	**GFI LanGuard** offers functionality to detect vulnerabilities caused by the use of vendor-supplied defaults and can report on the computers that have such vulnerabilities. **GFI LanGuard** offers an SNMP audit tool that can provide information on the existing community strings.	F, R
GFI LanGuard	2.2.2 Requires detection of unnecessary and insecure services and protocols.	**GFI LanGuard** can detect such services and protocols, including open ports (and trojan ports) using its application detection, process inspection and services enumeration functionalities. The product can report on these findings as well as on computers that have unnecessary services or protocols installed.	F, R
GFI LanGuard	2.2.3 For a sample of system components, critical servers, etc., requires that tests be performed to verify that the system security parameters are set correctly (according to the configuration standard defined in Requirement 2.2).	**GFI LanGuard** has an operating system audit functionality which enables it to read security policies and verify if certain settings are in place or not. **GFI LanGuard** reports on local machine users as well as users who never log on, and can even disable users. It can also enumerate password policy and enable auditing policies.	F, R
GFI LanGuard	3.4 Requires the use of encryption software at endpoints and on other critical systems.	**GFI LanGuard** can detect the presence of encryption software across all network computers and report on the computers lacking this software.	F, R
GFI LanGuard	5.2 Requires that antivirus engines are kept up to date in the network.	**GFI LanGuard** can detect antivirus software that is not up to date and update it. It can also report on the computers lacking antivirus software or having outdated version of the software.	F, R
GFI EventsManager	5.2 Requires that logs of antivirus software are enabled and retained.	**GFI EventsManager** can scan and centralize the logs of antivirus software and report on the data it gathers.	F, R

GFI product	Explanation	Value of GFI product to PCI compliance	Level of compliance*
GFI LanGuard	6.1 And 6.2 Require that all system components and software have the latest patches installed. Additionally, the use of vulnerability scoring is required.	Using its vulnerability scanning and patch detection capabilities, **GFI LanGuard** can periodically scan the entire network to detect new vulnerabilities including SANS Top 20, CVE lists and OVAL. **GFI LanGuard** is CVE and OVAL certified; it can automatically deploy new patches network-wide and can assign a score and report on the vulnerabilities discovered across the network, the network patching status and on all vulnerable hosts.	F, R
GFI EventsManager	7.1 Requires that monitoring should be in place to make sure that configured user accounts and their corresponding access rights are complying with the PCI DSS standards.	**GFI EventsManager** can monitor changes to user accounts and groups as well as changes to security rights assignment and data access lists; GFI EventsManager can also report on the data it gathers in this report.	F, R
GFI EventsManager	8.1.2 Requests control over a series of processes related to user account management.	**GFI EventsManager** can monitor account management events and report on the changes. The report can be used to detect any unauthorized changes to user accounts and user account groups.	F, R
GFI LanGuard	8.2.3 Require monitoring of password policy of computers across the network in order to ensure that computers are compliant with the password-related sub requirements.	**GFI LanGuard** can perform network-wide monitoring of password policies and report on the findings.	F, R
GFI EventsManager /GFI LanGuard	8.1.3 and 8.1.4 Requires immediate revocation of the user accounts of terminated or inactive users.	**GFI EventsManager** can monitor the "user account disabled" and "user account removed" events and report on this data. The report can be used to verify if accounts of the discontinued employees or employees on leave have been disabled or removed. Specific to requirement 8.5.5, the corresponding testing procedures require that you verify that there are no inactive accounts enabled; GFI EventsManager can monitor the activities of users and hence help determine the last login times of the user accounts. **GFI LanGuard** offers a user enumeration tool that shows all user accounts in a domain, and highlights the disabled accounts. This list can also be used to cross-reference user account status with discontinued employees. **GFI LanGuard** can also disable selected user accounts	F, R
GFI EventsManager /GFI LanGuard	8.1.5 Requires that the activity of accounts used by vendors is monitored continuously	**GFI EventsManager** can monitor user account activity by monitoring security logs of corresponding computers. **GFI LanGuard** can enumerate user accounts from the network and enable/ disable them as necessary and report on this data.	F, R
GFI EventsManager	8.1.6 Requires to limit repeated access by account lockout	**GFI EventsManager** is able to monitor failed logons and alert on situations where the number of failed logons passes a preconfigured threshold and report on this.	F, R

GFI product	Explanation	Value of GFI product to PCI compliance	Level of compliance*
GFI EventsManager	8.7 Requires monitoring of access to databases holding cardholder data.	**GFI EventsManager** can perform this task and report on the findings for databases implemented on Microsoft SQL Server technology, using the SQL audit functionality. This product is able to monitor all aspects of database access and usage under the above circumstances in compliance with C2 security level.	F, R
GFI EventsManager	10.0 Requests that audit trails are recorded and retained.	**GFI EventsManager** is able to record audit trails throughout the network and retain them in a secured database. The product is able to record all information defined under section 10.3 about all necessary events/actions defined by the sub points of requirement 10. GFI EventsManager can also report on the data.	F, R
GFI EventsManager	10.2.2 Requires auditing of administrative users.	**GFI EventsManager** can alert and report on events relating to the administrator.	F, R
GFI EventsManager	10.4 Requires time synchronization of all critical system clocks.	**GFI EventsManager** is able to monitor events generated by the time synchronization mechanisms and the "out of sync" errors thrown by the operating system whenever system clocks are not synchronized.	F, R
GFI EventsManager	10.5 Requires securing audit trail data.	**GFI EventsManager** uses a database engine which is able to provide granularity in terms of access rights which is required. Additionally, it has built-in capabilities to define roles for using the audit trails. One can configure certain users for read-only access, prevent access of other users or offer full access for authorized personnel. It can also monitor object access events in order to determine which files are accessed and by whom.	F, R
GFI EventsManager	Report on Requirement 10.6	**GFI EventsManager** can automatically generate daily reports and save them or email them to the administrators for review in compliance with requirement 10.6.	R
GFI EndPointSecurity	11.1. b Requires that a tool is used to determine all wireless/ removable devices which have been used to correct the computer systems.	**GFI EndPointSecurity** is able to both detect the devices currently connected, and the ones connected in the past, and control access to them on a "per user"/"per device type"/"per connectivity protocol" basis.	F
GFI LanGuard	11.2 Requires periodic use of a vulnerability scanner.	**GFI LanGuard** is a full-fledged OVAL and CVE vulnerability scanning and patch management solution that can be used to comply with this requirement.	F
GFI EventsManager	11.4 Requires the use of IPS/IDS systems.	**GFI EventsManager** is a log monitoring and management solution that can detect security breaches at host level after they have occurred (based on logs) and hence can act as a host-based intrusion detection system.	F, R

GFI product	Explanation	Value of GFI product to PCI compliance	Level of compliance*
GFI EventsManager	11.5 Requires file integrity monitoring.	**GFI EventsManager** can achieve this task by monitoring object access events on files and folders.	F, R
GFI LanGuard	12.2 Requires an annual risk assessment process.	**GFI LanGuard** is a fully fledged OVAL and CVE vulnerability scanning and patch management solution, also offering other risk assessment features such as trojan port detection, and hence can be used to comply with this requirement.	F, R
GFI EndPointSecurity	12.3 Requires the use of technology to develop policies and control endpoints (employee-facing technologies) in order to prevent data leakage.	**GFI EndPointSecurity** offers functionality to detect and control access to all types of removable devices, including wireless devices, which the employees might use to extract cardholder information from the company systems. **GFI EndPointSecurity** also offers extensive reporting on the usage history of such devices including technical details, user information and data transferred.	F, R

*F = FEATURE, *R = REPORT

Chart C - PCI DSS requirements - GFI product reports

Required ReportPack	Sub-requirement	GFI product report link	What report provides
REQUIREMENT 1: Install and maintain a firewall configuration to protect cardholder data.			
GFI LanGuard	1.2 Examine firewall and router configurations to verify that inbound and outbound traffic is limited to only protocols that are necessary for the cardholder data environment.	PCI DSS requirement 1.2 - open ports	**Open ports report:** The report will list all open ports on target machines or devices. The product uses multiple advanced techniques for identifying the open ports and the protocols using them. It is also able to identify over 700 trojan ports, and give information about the malware using them.
GFI LanGuard	1.4 Install personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet.	PCI DSS requirement 1.4 - installed Firewall applications	**Installed firewall applications report:** This report can be customized to show all hosts having the personal firewall application installed.
REQUIREMENT 2: Do not use vendor-supplied defaults for system passwords and other security parameters.			
GFI LanGuard	2.1 Always change vendor-supplied defaults before installing a system on the network.	PCI DSS requirement 2.1 - low security vulnerabilities	**Low security vulnerabilities report:** The report shows the low security vulnerabilities found on the network; one common source of these vulnerabilities are the vendor supplied defaults
GFI LanGuard	2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).	PCI DSS requirement 2.2.2 - system information	**System information report:** This report lists detailed technical information for each host machine, including services, installed applications, policies and devices.
GFI LanGuard	2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).	PCI DSS requirement 2.2.2 - services	**Services report:** This report lists service information for each host machine, including description, status, startup type and account name.
GFI LanGuard	2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).	PCI DSS requirement 2.2.2 - open ports	**Open ports report:** This report lists open ports for each host machine, including port number and name.
GFI LanGuard	2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).	PCI DSS requirement 2.2.2 - open shares	**Open shares report:** This report lists the open shares across the network. The information is used to determine if shares other than the authorized ones are open, and need to be removed.
GFI LanGuard	2.2.3 Configure system security parameters to prevent misuse. Note: The report only covers audit policy and password policy.	PCI DSS requirement 2.2.3 - audit policy	**Audit policy report:** This report also lists the audit policy and password policy for all computers in the network. This information is used to determine if there are any computers where password policies are not set to change passwords every 90 days.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
REQUIREMENT 3: Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.			
GFI LanGuard	3.4 Render PAN, at minimum, unreadable anywhere it is stored.	PCI DSS requirement 3.4 - disk encryption applications	**Disk encryption applications report:** This report shows the hosts that have encryption software installed. It can also be customized to show the hosts that don't have the encryption software installed.
REQUIREMENT 5: Use and regularly update antivirus software or programs. Malicious software commonly referred to as "malware" – including viruses, worms, and trojans – enters the network during many business-approved activities including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Antivirus software must be used on all systems commonly affected by malware to protect them from current and evolving malicious software threats.			
GFI LanGuard	5.2 Ensure that all antivirus mechanisms are current, actively running and capable of generating logs. (5.1 covered also).	PCI DSS requirement 5.2 - antivirus applications	**Antivirus applications report:** This report shows all the antivirus applications installed throughout the network, including their up-to-date-state, grouped by the host.
REQUIREMENT 6: Develop and maintain secure systems and applications. Some individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect themselves against exploitation and compromise of cardholder data by malicious individuals and malicious software. (Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that they do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques).			
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - remediation history by date	**Remediation history by date report:** This report displays remediation information grouped by date and time.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - network Vulnerability summary	**Network vulnerability summary report:** This report is an executive summary showing vulnerability counts for different categories. The report also identifies the top most vulnerable host machines and products, as well as the most common vulnerabilities detected on the network.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - vulnerability distribution by host	**Vulnerability distribution by host report:** This report is a statistical summary showing vulnerability counts for each host machine. Statistics are categorized by severity level and vulnerability category.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - vulnerability listing by category	**Vulnerability listing by category report:** This report lists detected vulnerabilities grouped by category, and the host machines affected by each vulnerability.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - vulnerability listing by host	**Vulnerability listing by host report:** This report lists the vulnerabilities detected for each host machine on the network.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - vulnerability listing by severity	**Vulnerability listing by severity report:** This report lists detected vulnerabilities grouped by severity, and the host machines affected by each vulnerability.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - open trojan ports by host	**Open trojan ports by host report:** This report lists open ports, grouped by host machine, which could potentially serve as a backdoor for trojans.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - vulnerable hosts by vulnerability level	**Vulnerable hosts based on vulnerability level report:** This report lists the most vulnerable host machines for each network security scan, based on vulnerability level.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - vulnerable hosts based on open ports report	**Vulnerable hosts based on open ports report:** This report lists the most vulnerable host machines, based on the number of open trojan ports found.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - network patching status	**Network patching status report:** This report illustrates the status of patches and service packs for host machines on the network.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - missing security updates by host	**Missing security updates by host report:** This report lists missing patches grouped by host machine, including URL links providing further information on each missing patch.
GFI LanGuard	6.1 Establish a process to identify newly discovered security vulnerabilities.	PCI DSS requirement 6.2 - vulnerability history	**Vulnerability history report:** This report shows a list of vulnerabilities that were discovered or fixed over the configured period of time.
GFI LanGuard	6.2 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	PCI DSS requirement 6.1 - missing security updates by host	**Missing security updates grouped by host report:** This report lists missing patches grouped by the host machine, including URL links providing further information on each missing patch.
GFI LanGuard	6.2 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	PCI DSS requirement 6.1 - missing security updates by severity	**Missing security updates grouped by severity report:** This report lists missing patches grouped by severity, including the host machine names for each missing patch.
GFI LanGuard	6.2 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	PCI DSS requirement 6.1 - installed security updates by host	**Installed security updates grouped by host report:** This report lists installed patches grouped by host machine, including URL links providing further information on each installed patch.
GFI LanGuard	6.2 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	PCI DSS requirement 6.1 - installed security updates by severity	**Installed security updates grouped by severity report:** This report lists installed patches grouped by severity, including the host machine names for each installed patch.
GFI LanGuard	6.2 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	PCI DSS requirement 6.1 - remediation history by date	**Remediation history by date report:** This report displays remediation information grouped by date and time.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
REQUIREMENT 7: Restrict access to cardholder data by business 'need to know'. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on 'need to know' and according to job responsibilities ('Need to know' is when access rights are granted to only the least amount of data and privileges needed to perform a job).			
GFI EventsManager	7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	PCI DSS requirement 7.1 - user account management report	**User account management report:** The report will help you achieve the following goals - find irregular or unusual network account activities, identify administrators who abuse privileges to create or modify accounts and detect patterns of account activities that breach organizational security policies.
GFI EventsManager	7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	PCI DSS requirement 7.1 - security group management report	**Security group management report:** Placement of users into security groups, particularly users who have high privileges such as Domain, Schema, or Enterprise Admins, should occur within policy guidelines only, and they should make use of established and approved accounts or processes
GFI EventsManager	7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	PCI DSS requirement 7.1 - user right assignment policy changes report	**User right assignment policy changes report:** The report will list any change in the user rights assignment policy, with information on the type of right, who assigned it and to whom.
GFI EventsManager	7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	PCI DSS requirement 7.1 - system access granted/removed report	**System access granted/removed report:** The report will list for each computer the users that have been granted system access.
GFI EventsManager	7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	PCI DSS requirement 7.1 - failed attempts to access files and registry report	**Failed attempts to access files and registry report:** The report will list all the failed attempts to access files and registry based on the object access events.
GFI EventsManager	7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	PCI DSS requirement 7.1 - failed attempts to access files and registry report	**Successful attempts to access files and registry report:** The report will list all the successful attempts to access files and registry based on the object access events.
REQUIREMENT 8: Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes. . ***Note:*** *These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance).*			
GFI EventsManager	8.1.2 Control addition, deletion, or modification of user IDs, credentials and other identifier objects.	PCI DSS requirement 8.1.2 – user account management report	**User account management report:** The report will help you achieve the following goals - find irregular or unusual network account activities, identify administrators who abuse privileges to create or modify accounts and detect patterns of account activities that breach organizational security policies.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI EventsManager	8.1.2 Control addition, deletion, or modification of user IDs, credentials and other identifier objects.	PCI DSS requirement 8.1.2 – security group management report	**Security group management report:** Placement of users into security groups, particularly users who have high privileges such as Domain, Schema, or Enterprise Admins, should occur within policy guidelines only, and they should make use of established and approved accounts or processes.
GFI EventsManager	8.1.2 Control addition, deletion, or modification of user IDs, credentials and other identifier objects.	PCI DSS requirement 8.1.2 – user right assignment policy changes report	**User right assignment policy changes report:** The report will list any change in the user rights assignment policy, with information on the type of right, who assigned it and to whom.
GFI EventsManager	8.1.2 Control addition, deletion, or modification of user IDs, credentials and other identifier objects.	PCI DSS requirement 8.1.2 – system access granted/ removed report	**System access granted/removed report:** The report will list for each computer, the users that have been granted system access.
GFI EventsManager	8.1.2 Control addition, deletion, or modification of user IDs, credentials and other identifier objects.	PCI DSS requirement 8.1.2 – password changes report	**Password changes report:** Password resets should occur within an approved framework only. Properly configured security audit levels should record password resets in the security event logs and identify those resets that do not follow the correct procedures. The report may contain the following sections: "Change password attempts", "User account password set or reset" and "Changes to directory service restore mode passwords".
GFI LanGuard	8.1.4 Remove inactive user accounts at least every 90 days	PCI DSS requirement 8.1.4 – groups and users report	**Groups and users report:** Shows a list of all the user accounts on all the network computers. For each user, it displays the last logon date which is used to determine if the user was inactive for more than 90 days.
GFI LanGuard	8.2.4 Change user passwords at least every 90 days.	PCI DSS requirement 8.2.4 – groups and users report	**Groups and users report:** Shows a list of all the user accounts on all the network computers. For each user account, the report shows the age of the corresponding password which is used to determine if there are any accounts with passwords older than a certain period.
GFI LanGuard	8.2.4 Change user passwords at least every 90 days.	PCI DSS requirement 8.2.4 – audit policy report	**Audit policy report:** This report also lists the password policy for all computers in the network. This information is used to determine if there are any computers where password policies are not set to change passwords every 90 days.
REQUIREMENT 10: Track and monitor all access to network resources and cardholder data. Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.			
GFI EventsManager	10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.1 All individual accesses to cardholder data – requires path to the data repository to be audited on the computer holding data.	PCI DSS requirement 10.2.1 – all individual access to cardholder data stored in files report	**10.2.1 All individual access to cardholder data stored in files report:** The report displays the data relevant to the corresponding requirement.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI EventsManager	10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.2 All actions taken by any individual with root or administrative privileges.	PCI DSS requirement 10.2.2 – all actions taken by any individual with root or administrative privileges report	**10.2.2 All actions taken by any individual with root or administrative privileges report:** The report displays the data relevant to the corresponding requirement.
GFI EventsManager	10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.3 Access to all audit trails.	PCI DSS requirement 10.2.3 – access to all audit trails report	**10.2.3 Access to all audit trails report:** The report displays the data relevant to the corresponding requirement.
GFI EventsManager	10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.4 Invalid logical access attempts.	PCI DSS requirement 10.2.4 – invalid logical access attempts report	**10.2.4 Invalid logical access attempts report:** The report displays the data relevant to the corresponding requirement.
GFI EventsManager	10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.5 Use of identification and authentication mechanisms.	PCI DSS requirement 10.2.5 - use of identification and authentication mechanisms report	**10.2.5 Use of identification and authentication mechanisms report:** The report displays the data relevant to the corresponding requirement.
GFI EventsManager	10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.6 Initialization of the audit logs.	PCI DSS requirement 10.2.6 - initialization of the audit logs report	**10.2.6 Initialization of the audit logs report:** The report displays the data relevant to the corresponding requirement.
GFI EventsManager	10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.7 Creation and deletion of system-level objects.	PCI DSS requirement 10.2.7 – creation and deletion of system level objects report	**10.2.7 Creation and deletion of system level objects report:** The report displays the data relevant to the corresponding requirement.
GFI EventsManager	10.4 Synchronize all critical system clocks and times.	PCI DSS requirement 10.4 – time synchronization monitoring report	**10.4 Time synchronization monitoring report:** The report will display events generated by the Windows Time service, responsible with time synchronization in Windows environments. Use this report to: a) monitor system time changes and b) monitor the time synchronization process.
GFI EventsManager	10.5.1 Limit viewing of audit trails to those with a job-related need.	PCI DSS requirement 10.5.1 – GFI EventsManager activity audit - logons	With the correct GFI EventsManager configuration, this report contains all the logons and logoffs to the GFI EventsManager management console.
GFI EventsManager	10.5.2 Protect audit trail files from unauthorized modifications.	PCI DSS requirement 10.5.2 – GFI EventsManager activity audit	With correct GFI EventsManager configuration, this report contains all the activity that users have performed using the GFI EventsManager management console application.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI EventsManager	10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed (except for new data) without generating alerts.	PCI DSS requirement 10.5.5 – failed attempts to access log files report	**Failed attempts to access log files report:** The report will list all the failed attempts to access files and registry based on the object access events.
GFI EventsManager	10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed (except for new data) without generating alerts.	PCI DSS requirement 10.5.5 - successful attempts to access log files report	**Successful attempts to access log files report:** The report will list all the successful attempts to access files and registry based on the object access events.
GFI EventsManager	10.6 Review logs for all system components at least once a day.	PCI DSS requirement 10.6 - generic event trend per hour	**Generic event trend per hour:** The report is used to display statistical information about the trend of collected events. First it shows a section with top 10 computers with the highest number of events, then the top 10 users generating the highest number of events. The events trend chart is divided per hour and the trend of events for each computer is also shown individually. The report can be used to determine time intervals where an unusually high number of events were generated.
GFI EventsManager	10.6 Review logs for all system components at least daily.	PCI DSS Requirement 10.6 Generic Event Trend per Day	**Generic Event Trend per Day:** The report is used to display statistical information about the trend of the collected events. First it shows a section of top 10 computers with the highest number of events, followed by the top 10 users generating the highest number of events. The events trend chart is divided per day and the trend of events for each computer is shown individually as well. The report can be used to determine time intervals where an unusually high number of events were generated.
REQUIREMENT 11: Regularly test security systems and processes. Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and customer software should be tested frequently to ensure security controls continue to reflect a changing environment.			
GFI EndPointSecurity	11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices.	All devices used - grouped by device report	**All devices used - grouped by device report:** This report shows a list of devices detected by GFI EndPointSecurity agents across the network, together with a list of users that have in some way made use of each device.
GFI EndPointSecurity	11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices.	All devices used - grouped by user report	**All devices used - grouped by user report:** This report shows a list of users monitored by GFI EndPointSecurity agents across the network together with a list of devices that each user has used.
GFI EndPointSecurity	11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices.	Device access statistics report	**Device access statistics report:** This report shows the number of allowed and denied access requests made by each user for each device, grouped by file system and non-file system devices. Each row shows Read-Only and Read-Write (full) access requests that were allowed or denied.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI EndPointSecurity	11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices.	Device usage statistics per user report	**Device usage statistics per user report:** This report shows a list of external devices connected by each user together with the number of allowed and denied access requests for each device.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - remediation history by date	**Remediation history by date report:** This report displays remediation information grouped by date and time.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - network vulnerability summary	**Network vulnerability summary report:** This report is an executive summary showing vulnerability counts for different categories. The report also identifies the top most vulnerable host machines and products, as well as the most common vulnerabilities detected on the network.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - security scans history	**Security scans history report:** This report lists information and statistics on all network security scans performed. It will provide evidence that scans were performed at adequate intervals, together with information on the outcomes.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - vulnerability distribution by host report	**Vulnerability distribution by host report:** This report is a statistical summary showing vulnerability counts for each host machine. Statistics are categorized by severity level and vulnerability category.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - vulnerability listing by category report	**Vulnerability listing by category report:** This report lists detected vulnerabilities grouped by category, and the host machines affected by each vulnerability.
GFI LanGuard	11.2 Run internal and external network vulnerability scans at least quarterly.	PCI DSS requirement 11.2 - vulnerability listing by host report	**Vulnerability listing by host report:** This report lists the vulnerabilities detected for each host machine on the network.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - vulnerability listing by severity report	**Vulnerability listing by severity report:** This report list detects vulnerabilities grouped by severity, and the host machines affected by each vulnerability.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - open trojan ports by host report	**Open trojan ports by host report:** This report lists open ports, grouped by host machine, which could potentially serve as a backdoor for trojans.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - vulnerable hosts based on vulnerability level report	**Vulnerable hosts based on vulnerability level report:** This report lists the most vulnerable host machines for each network security scan, based on vulnerability level.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - vulnerable hosts based on open ports report	**Vulnerable hosts based on open ports report:** This report lists the most vulnerable host machines, based on the number of open trojan ports found.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - network patching status report	**Network patching status report:** This report illustrates the status of patches and service packs for host machines on the network.
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - missing security updates by host report	**Missing security updates by host report**: This report lists missing patches grouped by host machine, including URL links providing further information on each missing patch.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI LanGuard	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - remediation history by host	**Remediation history by host:** This report displays remediation information grouped by host machine, including remediation details such as date and status.
GFI EventsManager	11.2 Run internal 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, product upgrades).	PCI DSS requirement 11.2 - vulnerability history report	**Vulnerability history report:** This report shows a list of vulnerabilities that were discovered or fixed over the configured period of time.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - account lockouts report	**Account lockouts report:** This report lists all locked out accounts, including those that can indicate a brute force attack.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - account logons report	**Account logons report:** This report shows all successful logons grouped by users, allowing you to quickly see which computers a user has logged on to.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - failed logon count on each computer report	**Failed logon count on each computer report:** This report lists the failed logins on each computer, as well as the type of failure.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - failed logons report	**Failed logons report:** This report lists logon failures per computer, and shows the reason behind these failures.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - logoffs report	**Logoffs report:** This report lists all logoff events including the logon type.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - successful logon count on each computer report	**Successful logon count on each computer:** This report shows logons by computer and allows you to quickly view the most accessed computers.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - successful logons grouped by computers report	**Successful logons grouped by computers report:** This report lists all successful logons and shows logon type.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - successful logons grouped by users report	**Successful logons grouped by users report:** This report displays all successful logons to see all machines a user has logged on to.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.5 - failed attempts to access files and registry report	**Failed attempts to access files and registry report**: The report will list all the failed attempts to access files and registry based on the object access events.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.5 - successful attempts to access files and registry report	**Successful attempts to access files and registry report**: The report will list all the successful attempts to access files and registry based on the object access events.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - objects deleted (all) report	**Object deleted with details report:** The report will show all deleted files, registry keys, etc.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - all network activity report grouped by source	**PCI DSS requirement 11.4 - all network activity report grouped by source:** The report shows the network activity generated by each computer running Windows Vista or newer operating systems (including the server family), based on the events logged by the Windows filtering platform. This report helps you identify computers that are already compromised or about to be compromised by malware/viruses as well as identify specific network activity.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - important network activity	**PCI DSS requirement 11.4 - important network activity:** The report shows the network activity generated by each computer running Windows Vista or newer operating systems (including the server family), based on the events logged by the Windows filtering platform. This report helps you identify computers that are already compromised or about to be compromised by malware/viruses as well as identify specific network activity.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - network activity report grouped by communication port	**PCI DSS requirement 11.4 - network activity report grouped by communication port:** The report shows the network activity generated by each computer running Windows Vista or newer operating systems (including the server family), based on the events logged by the Windows filtering platform. This report helps you identify computers that are already compromised or about to be compromised by malware/viruses as well as identify specific network activity.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - network activity report grouped by destination	**PCI DSS requirement 11.4 - network activity report grouped by destination**: The report shows the network activity generated by each computer running Windows Vista or newer operating systems (including the server family), based on the events logged by the Windows filtering platform. This report helps you identify computers that are already compromised or about to be compromised by malware/viruses as well as identify specific network activity.
GFI EventsManager	11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	PCI DSS requirement 11.4 - network activity report grouped by direction	**PCI DSS requirement 11.4 - network activity report grouped by direction:** The report shows the network activity generated by each computer running Windows Vista or newer operating systems (including the server family), based on the events logged by the Windows filtering platform. This report helps you identify computers that are already compromised or about to be compromised by malware/viruses as well as identify specific network activity.
GFI EventsManager	11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files.	PCI DSS requirement 11.5 - failed attempts to access files and registry report	**Failed attempts to access files and registry report:** The report will list all failed attempts to access files and registry based on the object access events.
GFI EventsManager	11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files.	PCI DSS requirement 11.5 - successful attempts to access files and registry report	**Successful attempts to access files and registry report:** The report will list all successful attempts to access files and registry based on the object access events.
GFI EventsManager	11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files.	PCI DSS requirement 15.4 - deleted files	**PCI DSS Requirement 15.4 - deleted files:** The report lists the deleted files throughout the network. It will help you identify if any critical files are being deleted.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
REQUIREMENT 12: Maintain a policy that addresses information security for all personnel. A strong security policy sets the security tone for the whole company and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities towards protecting it. For the purposes of this requirement, "personnel" refers to full-time and part-time employees, temporary employees, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.			
GFI LanGuard	12.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - network vulnerability summary	**Network vulnerability summary report:** This report is an executive summary showing vulnerability counts for different categories. The report also identifies the top most vulnerable host machines and products, as well as the most common vulnerabilities detected on the network.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - Vulnerability distribution by host	**Vulnerability distribution by host report:** This report is a statistical summary showing vulnerability counts for each host machine. Statistics are categorized by severity level and vulnerability category.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - vulnerability listing by category	**Vulnerability listing by category report:** This report lists detected vulnerabilities grouped by category, and the host machines affected by each vulnerability.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - vulnerability listing by host	**Vulnerability listing by host report:** This report lists the vulnerabilities detected for each host machine on the network.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - vulnerability listing by severity	**Vulnerability listing by severity report:** This report lists detected vulnerabilities grouped by severity, and the host machines affected by each vulnerability.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - open trojan ports by host	**Open trojan ports by host report:** This report lists open ports, grouped by host machine, which could potentially serve as a backdoor for trojans.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - vulnerable hosts based on vulnerability level	**Vulnerable hosts based on vulnerability level report**: This report lists the most vulnerable host machines for each network security scan, based on vulnerability level.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - vulnerable hosts based on open ports	**Vulnerable hosts based on open ports report:** This report lists the most vulnerable host machines, based on the number of open trojan ports found.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - network patching status	**Network patching status report:** This report illustrates the status of patches and service packs for host machines on the network.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - missing security updates grouped by host	**Missing security updates grouped by host report:** This report lists missing patches grouped by host machine, including URL links providing further information on each missing patch.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - remediation history by host	**Remediation history by host:** This report displays remediation information grouped by host machine, including remediation details such as date and status.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - remediation history by date	**Remediation history by date report:** This report displays remediation information grouped by host machine, including remediation details such as date and status.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - baseline changes comparison	**Baseline changes comparison report:** This report compares results between a chosen computer, used as benchmark, and host machines scanned with the same profile.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - network security log by date	**Network security log by date report:** This report compares results of consecutive scans that have a common profile and target, grouped by the scan date.
GFI LanGuard	12.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.	PCI DSS requirement 12.2 - network security log by host	**Network security log by host report:** This report compares results of consecutive scans that have a common profile and target, grouped by the host machine.
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	Device usage summary report	**Device usage summary report:** The charts in this report display percentages of allowed versus denied access for different devices across all monitored computers on the network. It also lists the top 10 users with allowed or denied access.
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	Device access trends report	**Device access trends report:** This is a trend report showing the change in device access attempts over time. The graphs plot both the allowed and denied access counts per day.
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	Top active users/ computers reports	**Top active users/computers reports:** These reports show lists of monitored users/machines that have the highest amount of device activity.
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	Users who accessed devices on more than one machine report	**Users who accessed devices on more than one machine report:** This report displays the users who were accessing devices on more than one machine.

Required ReportPack	Sub-requirement	GFI product report link	What report provides
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	Machines which had more than one user accessing devices report	**Machines which had more than one user accessing devices report:** This report displays the machines which had more than one user accessing the devices.
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	Connected devices outside working hours report	**Connected devices outside working hours report:** This report shows the devices which were connected outside the working hours.
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	All devices used - grouped by device report	**All devices used - grouped by device report:** This report shows a list of devices detected by GFI EndPointSecurity agents across the network together with a list of users that have in some way made use of each device.
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	All devices used - grouped by user report	**All devices used - grouped by user report:** This report shows a list of users monitored by GFI EndPointSecurity agents across the network together with a list of devices that each user has used.
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	Device access statistics report	**Device access statistics report:** This report shows the number of allowed and denied access requests made by each user for each device, grouped by file system and non file system devices. Each row shows Read-Only and Read-Write (full) access requests that were allowed or denied.
GFI EndPointSecurity	12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.	Device usage statistics per user report	**Device usage statistics per user report:** This report shows a list of external devices connected by each user together with the number of allowed and denied access requests for each device.

Chart D – summary of all PCI DSS requirements

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
Requirement 1: Install and maintain a firewall configuration to protect cardholder data					
1.1 Establish and implement firewall and router configuration standards that include the following:				6	
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations				6	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks				1	
1.1.3 Current diagram that shows all cardholder data flows across systems and networks				1	
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone				2	
1.1.5 Description of groups, roles, and responsibilities for management of network components				6	
1.1.6 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. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.				2	Process/policy driven requirements 0 outside the scope of software solution.
1.1.7 Requirement to review firewall and router rule sets at least every six months				6	Outside the scope of GFI products
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. **Note:** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	B, D	B, D		2	
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.				2	Outside the scope of GFI products.
1.2.2 Secure and synchronize router configuration files.				2	Outside the scope of GFI products.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.				2	Outside the scope of GFI products.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	B, D	B, D		2	
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.				2	Outside the scope of GFI products.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.				2	Outside the scope of GFI products.
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.				2	Outside the scope of GFI products.
1.3.4 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.)				2	Outside the scope of GFI products.
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.				2	Outside the scope of GFI products.
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)				2	Outside the scope of GFI products.
1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.				2	Outside the scope of GFI products.
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties.				2	Outside the scope of GFI products.
1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: • Specific configuration settings are defined for personal firewall software. • Personal firewall software is actively running. • Personal firewall software is not alterable by users of mobile and/or employee-owned devices.		A, B, C, D		2	

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.					
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.					
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, Simple Network Management Protocol (SNMP) community strings, etc.).		B, C, D		2	
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.				2	Outside the scope of GFI products.
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).				3	Process/policy driven requirements – outside the scope of software solution.
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: *Where virtualization technologies are in use, implement only one primary function per virtual system component*				3	Outside the scope of GFI products
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.		B, D		3	

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. Note: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS. POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.		B, D		3	
2.2.4 Configure system security parameters to prevent misuse.				3	Outside the scope of GFI products
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. *Note: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS. POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.*		B, C		3	
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.				2	Outside the scope of GFI products
2.4 Maintain an inventory of system components that are in scope for PCI DSS.				3	Outside the scope of GFI products
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.				3	Outside the scope of GFI products

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.				3	Process/policy driven requirement – outside the scope of software solution.
Requirement 3: Protect stored cardholder data					
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.				1	Process/policy driven requirement – outside the scope of software solution
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* ☐There is a business justification and ☐The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:				1	Outside the scope of GFI products.
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: • The cardholder's name • Primary account number (PAN) • Expiration date • Service code To minimize risk, store only these data elements as needed for business.				1	

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.				1	Process/policy driven requirement – outside the scope of software solution.
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.				1	Process/policy driven requirement – outside the scope of software solution.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN. Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.		B, C, D		1	
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.				5	Process/policy driven requirement – outside the scope of software solution.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.				5	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.				5	Process/policy driven requirement – outside the scope of software solution.
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.				5	Process/policy driven requirement – outside the scope of software solution.
3.5.2 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry accepted method Note: It is not required that public keys be stored in one of these forms.				5	Process/policy driven requirement – outside the scope of software solution.
3.5.3 Store cryptographic keys in the fewest possible locations.				5	Process/policy driven requirement – outside the scope of software solution.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.				5	Process/policy driven requirement – outside the scope of software solution.
3.6.1 Generation of strong cryptographic keys				5	Process/policy driven requirement – outside the scope of software solution.
3.6.2 Secure cryptographic key distribution				5	Process/policy driven requirement – outside the scope of software solution.
3.6.3 Secure cryptographic key storage				5	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
3.6.4 Cryptographic key changes for keys that have reached the end of their crypto period (for example, after a defined period of time has passed and/or after a certain amount of cipher text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).				5	Process/policy driven requirement – outside the scope of software solution.
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.				5	Process/policy driven requirement – outside the scope of software solution.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.				5	Process/policy driven requirement – outside the scope of software solution.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.				5	Process/policy driven requirement – outside the scope of software solution.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.				5	Process/policy driven requirement – outside the scope of software solution.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.				5	Process/policy driven requirement – outside the scope of software solution.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
4.1 Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) 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. Note: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS. POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.				2	Outside the scope of GFI product.
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. Note: The use of WEP as a security control is prohibited.				2	Outside the scope of GFI product.
4.2 Never send unprotected PANs by end user messaging technologies (for example, email, instant messaging, SMS, chat, etc.).				2	Outside the scope of GFI product.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.				2	Process/policy driven requirement – outside the scope of software solution.
Maintain a Vulnerability Management Program **Requirement 5:** Protect all systems against malware 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).		A		2	
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.				2	

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.				2	
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.	B, D	A, C, D		2	
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. *Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*		B, C, D		2	
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.				2	Process/policy driven requirement – outside the scope of software solution.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
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. Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.		A, C, D		3	
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.		A, C, D		3	
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.				3	Process/policy driven requirement – outside the scope of software solution.
6.3.1 Remove development, test and/or custom application accounts, user IDs, and custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.				3	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. Code-review results are reviewed and approved by management prior to release. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.				3	Process/policy driven requirement – outside the scope of software solution.
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:				3	Process/policy driven requirement – outside the scope of software solution.
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.				3	Process/policy driven requirement – outside the scope of software solution.
6.4.2 Separation of duties between development/test and production environments				3	Process/policy driven requirement – outside the scope of software solution
6.4.3 Production data (live PANs) are not used for testing or development				3	Process/policy driven requirement – outside the scope of software solution
6.4.4 Removal of test data and accounts before production systems become active				3	Process/policy driven requirement – outside the scope of software solution
6.4.5 Change control procedures for the implementation of security patches and software modifications must include the following:				3	Process/policy driven requirement – outside the scope of software solution
6.4.5.1 Documentation of impact.				3	Process/policy driven requirement – outside the scope of software solution

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
6.4.5.2 Documented change approval by authorized parties.				3	Process/policy driven requirement – outside the scope of software solution
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.				3	Process/policy driven requirement – outside the scope of software solution
6.4.5.4 Back-out procedures.				3	Process/policy driven requirement – outside the scope of software solution
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.				6	Process/policy driven requirement – outside the scope of software solution
6.5.1 Injection flaws, particularly SQL Also consider OS Command LDAP and XPath injection flaws other injection flaws.				3	Process/policy driven requirement – outside the scope of software solution
6.5.2 Buffer overflows				3	Process/policy driven requirement – outside the scope of software solution
6.5.3 Insecure cryptographic storage				3	Process/policy driven requirement – outside the scope of software solution
6.5.4 Insecure communications				3	Process/policy driven requirement – outside the scope of software solution
6.5.5 Improper error handling				3	Process/policy driven requirement – outside the scope of software solution
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as procedures and interview responsible personnel to verify defined in PCI DSS Requirement 6.1).				3	Process/policy driven requirement – outside the scope of software solution

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
6.5.7 Cross-site scripting (XSS)				3	Process/policy driven requirement – outside the scope of software solution
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).				3	Process/policy driven requirement – outside the scope of software solution
6.5.9 Cross-site request forgery (CSRF)				3	Process/policy driven requirement – outside the scope of software solution
6.5.10 Broken authentication and session management Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.				3	Process/policy driven requirement – outside the scope of software solution
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 Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. Installing an automated technical solution that detects and prevents web based attacks (for example, a web application firewall) in front of public facing web applications, to continually check all traffic.				3	Process/policy driven requirement – outside the scope of software solution
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all applications.				3	Process/policy driven requirement – outside the scope of software solution
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.				4	Process/policy driven requirement – outside the scope of software solution
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.				4	Process/policy driven requirement – outside the scope of software solution

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
7.1.3 Assign access based on individual personnel's job classification and function.				4	Process/policy driven requirement – outside the scope of software solution
7.1.4 Require documented approval by authorized parties specifying required privileges.				4	Process/policy driven requirement – outside the scope of software solution
7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:				4	Process/policy driven requirement – outside the scope of software solution
7.2.1 Coverage of all system components				4	Process/policy driven requirement – outside the scope of software solution
7.2.2 Assignment of privileges to individuals based on job classification and function.				4	Process/policy driven requirement – outside the scope of software solution
7.2.3 Default "deny-all" setting.				4	Process/policy driven requirement – outside the scope of software solution
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.				4	Process/policy driven requirement – outside the scope of software solution
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.				4	Process/policy driven requirement – outside the scope of software solution
Requirement 8: Identify and authenticate access to system components					
8.1 Define and implement policies and procedures to ensure proper user identification management for non consumer users and administrators on all system components as follows:				4	Process/policy driven requirement – outside the scope of software solution.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.				4	Outside the scope of GFI product
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	D	B, D		4	
8.1.3 Immediately revoke access for any terminated users.	D	B, D		4	
8.1.4 Remove/disable inactive user accounts within 90 days.	D	B, D		4	

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
8.1.5 Manage IDs used by vendors 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.	B, D	B, D		4	
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.				4	
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.				4	Outside scope of GFI product.
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.				4	Outside scope of GFI product.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.				4	Process/policy driven requirement – outside the scope of software solution.
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.				4	Outside scope of GFI product.
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.				4	Process/policy driven requirement – outside the scope of software solution.
8.2.3 Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.		B, D		4	
8.2.4 Change user passwords/passphrases at least once every 90 days.	D	B, D		4	
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.				4	Outside the scope of GFI product.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
8.2.6 Set passwords/phrases for first time use and upon reset to a unique value for each user, and change immediately after the first use.				4	Process/policy driven requirement – outside the scope of software solution.
8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance). *Note: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.* *Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.*				4	Outside the scope of GFI products.
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.				4	Process/policy drive requirement – outside the scope of software solution.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods 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 any system components.				4	Process/policy driven requirement – outside the scope of software solution.
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. 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.				4	Outside the scope of GFI product.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.				4	Process/policy driven requirement – outside the scope of software solution.
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)	B, D			4	
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties				4	Process/policy driven requirement – outside the scope of software solution.
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.				5	Outside the scope of GFI products.
9.1.1 Use video cameras and/or access control mechanisms 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. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.				5	Process/policy driven requirement – outside the scope of software solution.
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.*				5	

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.				5	Process/policy driven requirement – outside the scope of software solution.
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).				5	Process/policy driven requirement – outside the scope of software solution.
9.3 Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.				5	Process/policy driven requirement – outside the scope of software solution.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:				5	Process/policy driven requirement – outside the scope of software solution.
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.				5	Process/policy driven requirement – outside the scope of software solution.
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.				5	Process/policy driven requirement – outside the scope of software solution.
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.				5	Process/policy driven requirement – outside the scope of software solution.
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.				5	Process/policy driven requirement – outside the scope of software solution.
9.5 Physically secure all media.				5	Process/policy driven requirement – outside the scope of software solution.
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.				5	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:				5	Process/policy driven requirement – outside the scope of software solution.
9.6.1 Classify media so the sensitivity of the data can be determined.				5	Process/policy driven requirement – outside the scope of software solution.
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.				5	Process/policy driven requirement – outside the scope of software solution.
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).				5	Process/policy driven requirement – outside the scope of software solution.
9.7 Maintain strict control over the storage and accessibility of media.				5	Process/policy driven requirement – outside the scope of software solution.
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.				5	Process/policy driven requirement – outside the scope of software solution.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:				1	Process/policy driven requirement – outside the scope of software solution.
9.8.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.				1	Process/policy driven requirement – outside the scope of software solution.
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.				1	Process/policy driven requirement – outside the scope of software solution.
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. Note: These requirements apply to card reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads. Note: Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.				1	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.				1	Process/policy driven requirement – outside the scope of software solution.
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.				1	Process/policy driven requirement – outside the scope of software solution.
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).				1	Process/policy driven requirement – outside the scope of software solution.
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.				2	Process/policy driven requirement – outside the scope of software solution.
Regularly Monitor and Test Networks **Requirement 10:** Track and monitor all access to network resources and cardholder data					
10.1 Implement audit trails to link all access to system components to each individual user.	A, B, C, D			4	
10.2 Implement automated audit trails for all system components to reconstruct the following events:	A, B, C, D			4	
10.2.1 All individual user accesses to cardholder data	A, B, C, D			4	

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
10.2.2 All actions taken by any individual with root or administrative privileges	A, B, C, D			4	
10.2.3 Access to all audit trails	A, B, C, D			4	
10.2.4 Invalid logical access attempts	A, B, C, D			4	
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	A, B, C, D			4	
10.2.6 Initialization, stopping, or pausing of the audit logs	A, B, C, D			4	
10.2.7 Creation and deletion of system level objects	A, B, C, D			4	
10.3 Record at least the following audit trail entries for all system components for each event:	A, B, C, D			4	
10.3.1 User identification	A, B, C, D			4	
10.3.2 Type of event	A, B, C, D			4	
10.3.3 Date and time	A, B, C, D			4	
10.3.4 Success or failure indication	A, B, C, D			4	
10.3.5 Origination of event	A, B, C, D			4	
10.3.6 Identity or name of affected data, system component, or resource.	A, B, C, D			4	
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. Note: One example of time synchronization technology is Network Time Protocol (NTP).	B, D			4	
10.4.1 Critical systems have the correct and consistent time.	B, D			4	
10.4.2 Time data is protected.	B, D			4	
10.4.3 Time settings are received from industry-accepted time sources.	B, D			4	
10.5 Secure audit trails so they cannot be altered.				4	Outside the scope of GFI products.
10.5.1 Limit viewing of audit trails to those with a job-related need.	A, B, C, D			6	
10.5.2 Protect audit trail files from unauthorized modifications.	A, B, C, D			6	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.				6	Outside the scope of GFI product.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.				6	Process/policy driven requirement – outside the scope of software solution.
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).	A, B, C, D			6	
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	A, B, C, D			4	
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	B, D			4	
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	B, D			4	
10.6.3 Follow up exceptions and anomalies identified during the review process.	B, D			4	
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).				4	Process/policy driven requirement – outside the scope of software solution.
10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.				4	Process/policy driven requirement – outside the scope of software solution.

Requirement 11: Regularly test security systems and processes.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
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. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	B, D		A, B, C, D	6	
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.		B, C, D		2	
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.				2	Process/policy driven requirement – outside the scope of software solution.
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, product upgrades). *Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*		A, B, C, D		2	
11.2.1 Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.		A, B, C, D		2	

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.					
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.		A, B, C, D		2	
11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results. Note: This update to Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. Prior to this date, PCI DSS v2.0 requirements for penetration testing must be followed until version 3 is in place.				6	Outside the scope of GFI products.
11.3.1 Perform *external* penetration testing at least annually 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).				6	Outside the scope of GFI products.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
11.3.2 Perform *internal* penetration testing at least annually 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).				6	Outside the scope of GFI products.
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.				6	Outside the scope of GFI products.
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.				6	Outside the scope of GFI products.
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.	A, B, C, D			2	
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. *Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	A, B, C, D			4	
11.5.1 Implement a process to respond to any alerts generated by the change detection solution.				4	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.				3	Process/policy driven requirement – outside the scope of software solution.
Maintain an Information Security Policy **Requirement 12:** Maintain a policy that addresses information security for all personnel.					
12.1 Establish, publish, maintain, and disseminate a security policy.				6	
12.1.1 Review the security policy at least annually and update the policy when the environment changes.				1	Process/policy driven requirement – outside the scope of software solution.
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.		B		6	
12.3 Develop usage policies for critical technologies and define proper use of these technologies. Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, email usage and Internet usage. Ensure these usage policies require the following:			A, B, C, D	6	
12.3.1 Explicit approval by authorized parties			A, B, C, D	6	
12.3.2 Authentication for use of the technology			A, B, C, D	6	
12.3.3 A list of all such devices and personnel with access			A, B, C, D	6	
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)				6	
12.3.5 Acceptable uses of the technology			A, B, C, D	6	
12.3.6 Acceptable network locations for the technologies			A, B, C, D	6	
12.3.7 List of company-approved products				6	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity				6	Process/policy driven requirement – outside the scope of software solution.
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				6	Process/policy driven requirement – outside the scope of software solution.
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.			A, B, C, D	6	
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.				6	Process/policy driven requirement – outside the scope of software solution.
12.5 Assign to an individual or team the following information security management responsibilities:				6	Process/policy driven requirement – outside the scope of software solution.
12.5.1 Establish, document, and distribute security policies and procedures.				6	Process/policy driven requirement – outside the scope of software solution.
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.				6	Process/policy driven requirement – outside the scope of software solution.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.				6	Process/policy driven requirement – outside the scope of software solution.
12.5.4 Administer user accounts, including additions, deletions, and modifications.				6	Process/policy driven requirement – outside the scope of software solution.
12.5.5 Monitor and control all access to data.				6	Process/policy driven requirement – outside the scope of software solution.
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.				6	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
12.6.1 Educate personnel upon hire and at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.				6	Process/policy driven requirement – outside the scope of software solution.
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.				6	Process/policy driven requirement – outside the scope of software solution.
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.				6	Process/policy driven requirement – outside the scope of software solution.
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:				2	Process/policy driven requirement – outside the scope of software solution.
12.8.1 Maintain a list of service providers.				2	Process/policy driven requirement – outside the scope of software solution.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.				2	Process/policy driven requirement – outside the scope of software solution.
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.				2	Process/policy driven requirement – outside the scope of software solution.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.				2	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.				6	Process/policy driven requirement – outside the scope of software solution.
12.9 *Additional requirement for service providers only*: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. *Note: This requirement is a best practice until June 30, 2015, after which it becomes a requirement.* *Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*				6	Process/policy driven requirement – outside the scope of software solution.
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.				6	Process/policy driven requirement – outside the scope of software solution.
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.				6	Process/policy driven requirement – outside the scope of software solution.
12.10.2 Test the plan at least annually.				6	Process/policy driven requirement – outside the scope of software solution.
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.				6	Process/policy driven requirement – outside the scope of software solution.

PCI DSS Requirements	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GF EndPoint Security Support Level**	Milestone*	Comment
12.10.4 Provide appropriate training to staff with security breach response responsibilities.				6	Process/policy driven requirement – outside the scope of software solution.
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion prevention, firewalls, and file-integrity monitoring systems.				6	Process/policy driven requirement – outside the scope of software solution.
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.				6	Process/policy driven requirement – outside the scope of software solution.
Requirement A.1: Shared hosting providers must protect the cardholder data environment					
A.1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.				3	Process/policy driven requirement – outside the scope of software solution.
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.				3	Process/policy driven requirement – outside the scope of software solution.
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.		A, C		3	
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.				3	Process/policy driven requirement – outside the scope of software solution.
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.				3	Process/policy driven requirement – outside the scope of software solution.

FOOTNOTES:
* Milestone - suggested order of implementation efforts to meet PCI-DSS requirements. The order is not mandatory, but is based on the PCI Security Standards Council recommendations - please see the Official PCI Security Standards Council site for more information at: https://www.pcisecuritystandards.org/index.php
A: The product offers functionality directly requested by particular PCI DSS requirements in order to achieve compliance.
B: The product offers functionality that can aid enforcement or enforce particular PCI DSS requirements once they are in place, via monitoring, alerting and/or reporting; particularly useful for periodic reviews and assessments.
C: The product offers functionality to report on compliance status of hosts related to a particular PCI DSS requirement.
D: The product is able to report on the data gathered as part of processes at support levels A and B for a particular PCI DSS requirement.

Chart E – PCI DSS requirements support in GFI products

	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GFI EndPoint Security Support Level**
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.			
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	B, D	B, D	
1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:	B, D	B, D	
1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet.		A, B, C, D	
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.			
Requirement 2: Do not use vendor-supplied default passwords.			
2.1 Always change vendor-supplied defaults before installing a system on the network.		B, C, D	
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).		B, D	
2.2.3 Configure system security parameters to prevent misuse.		B, D	
Requirement 3: Protect stored cardholder data.			
3.4 Render PAN, at minimum, unreadable anywhere it is stored.		B, C, D	
Requirement 5: Use and regularly update antivirus software or programs.			
5.1 Deploy antivirus software on all systems commonly affected by viruses.		A	
5.2 Ensure that all antivirus mechanisms are current, actively running and capable of generating logs.	B, D	A, C, D	
Requirement 6: Develop and maintain secure systems and applications.			
6.1 Establish a process to identify newly discovered security vulnerabilities.		A, C, D	
6.2 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.		A, C, D	
Requirement 7: Restrict access to cardholder data by business need-to-know.			
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	B, D		
Requirement 8: Identify and authenticate access to system components.			
8.1.2 Control addition, deletion, or modification of user IDs, credentials, and other identifier objects.	D		
Set first-time passwords to a unique value for each user and change immediately after first use.		B, D	
8.1.3 Immediately revoke access for any terminated users.	D	B, D	
8.1.4 Remove inactive user accounts at least once every 90 days.	B, D	B, D	

	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GFI EndPoint Security Support Level**
8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access	B, D	B, D	
8.2.4 Change user passwords at least once every 90 days.		B, D	
8.2.3 Require a minimum password length of at least seven characters.		B, D	
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.			
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted	B, D		
Requirement 10: Track and monitor all access to network resources and cardholder data.			
10.1 Log all individual user access to system components, especially administrative users.	A, B, C, D		
10.2 Implement automated audit trails for all system components to reconstruct the following events:	A, B, C, D		
10.2.1 All individual accesses to cardholder data.	A, B, C, D		
10.2.2 All actions taken by any individual with root or administrative privileges.	A, B, C, D		
10.2.3 Access to all audit trails.	A, B, C, D		
10.2.4 Invalid logical access attempts.	A, B, C, D		
10.2.5 Use of identification and authentication mechanisms.	A, B, C, D		
10.2.6 Initialization of the audit logs.	A, B, C, D		
10.2.7 Creation and deletion of system-level objects.	A, B, C, D		
10.3 Record at least the following audit trail entries for all system components for each event.	A, B, C, D		
10.4 Synchronize all critical system clocks and times.	B, D		
10.5.1 Limit viewing of audit trails to those with a job-related need.	A, B, C, D		
10.5.2 Protect audit trail files from unauthorized modifications.	A, B, C, D		
10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed (except for new data) without generating alerts.	A, B, C, D		
10.6 Review logs for all system components at least daily.	A, B, C, D		
Requirement 11: Regularly test security systems and processes.			
11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.	B, D		A, B, C, D
11.2 Run internal and external network vulnerability scans at least quarterly.		A, B, C, D	
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.	A, B, C, D		
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files.	A, B, C, D		
Requirement 12: Maintain a policy that addresses information security for all personnel.			
12.1.1 Review the security policy at least annually and update the policy when the environment changes.		A, B, C, D	

	GFI Events Manager Support Level**	GFI LanGuard Support Level**	GFI EndPoint Security Support Level**
12.3 Develop usage policies for critical technologies and define proper use of these technologies. Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, email usage and Internet usage. Ensure these usage policies require the following:			A, B, C, D
12.3.1 Explicit approval by authorized parties			A, B, C, D
12.3.2 Authentication for use of the technology.			A, B, C, D
12.3.3 A list of all such devices and personnel with access.			A, B, C, D
12.3.5 Acceptable uses of the technology.			A, B, C, D
12.3.6 Acceptable network locations for the technologies.			A, B, C, D
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.			A, B, C, D

**FOOTNOTES:
A: The product offers functionality directly requested by particular PCI DSS requirements in order to achieve compliance.
B: The product offers functionality that can aid enforcement or enforce particular PCI DSS requirements once they are in place, via monitoring, alerting and/or reporting; particularly useful for periodic reviews and assessments.
C: The product offers functionality to report on compliance status of hosts related to a particular PCI DSS requirement.
D: The product is able to report on the data gathered as part of processes at support levels A and B for a particular PCI DSS requirement.

About GFI

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMB) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States, UK, Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold ISV Partner.

More information about GFI can be found at http://www.gfi.com.

GFI Software™

For a full list of GFI offices/contact details worldwide,

please visit: www.gfi.com/contact-us