Lumension SECURITY

PCI COMPLIANCE

Achieving Payment Card Industry (PCI) Data Security Standard Compliance With Lumension Security Vulnerability Management and Endpoint Security Solutions

Cardholder Data at Risk

While technology has continued to evolve, allowing ease of data access and transfer, it has also facilitated the massive threat of data and identity theft. Credit card merchants and their partners are primary targets for data theft as their systems store and move vast amounts of sensitive credit cardholders' personal and financial data. The easiest access to this sensitive and valuable data is through endpoints, with threats coming from outside and from within the corporate walls.

- 65% of financial services institutions worldwide experienced repeated external breaches within the past 12 months [1]
- 30% of these global institutions suffered repeated internal breaches during the same timeframe [1]

While it's the cardholders' data at risk, it is the organizations which are responsible for the safe and secure transaction and storage of this data.

- **Protecting Against External Threats**
  Organizations are left vulnerable to data theft due to unpatched and mis-configured endpoints. The use of Trojans provides a simple way of entering a private unauthorized computer and stealing information, and ports that remain open, as well as unsecured online information transactions, offer convenient methods for cyber criminals to hi-jack systems and transmit replicated data. Just last year, TJX Companies announced that 45.7 million credit and debit card numbers were stolen by hackers who accessed the computer systems over several years.

- **Protecting Against the Insider Threat**
  In a July 2007 SEC filing, Fidelity National Information Services Inc. disclosed that a senior database administrator responsible for defining and enforcing data access rights at one of its subsidiaries sold the personal information of about 8.5 million consumers to a data broker. Of that number, about 5.7 million records were checking account records and about 1.5 million records included credit card details. The remaining records contained only identifying information such as names, addresses, dates of birth and telephone numbers. The administrator was one of five administrators who had that level of access to the company's data.

Too many organizations' systems are not fully protected from both external and insider threats because they employ fragmented security policies with no way consistently and continuously enforce them.

PCI Data Security Standard

The continuation of massive credit card data breaches at many high profile organizations, prompted the five major credit card issuers, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to develop the Payment Card Industry Data Security Standard (PCI DSS), which standardizes how credit card data should be protected. Under the PCI DSS, a business or organization should be able to assure their customers that its credit card data/account information and transaction information is safe from hackers or any malicious system intrusion.

To achieve compliance with the PCI Security Standard, vendors and service providers must adhere to six major categories of requirements, with a total of twelve PCI-required controls, covering access management, network security, incident response, network monitoring and testing and information security policies. By adhering to PCI, organizations can standardize their security policies on a best practices approach and thus minimize the risk of data theft, however, many are still not compliant:

- 23% of Visa's Level 1 merchants (more than 6 million transactions annually) are not PCI compliant
- 38% of their Level 2 merchants (1-6 million transactions annually) are not PCI compliant

PCI DSS

Build and Maintain a Secure Network
- Requirement 1: Install and maintain a firewall configuration to protect data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data
- Requirement 3: Protect stored data
- Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program
- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
- Requirement 7: Restrict access to data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
- Requirement 10: Restrict access to data by business need-to-know
- Requirement 11: Assign a unique ID to each person with computer access

Maintain an Information Security Policy
- Requirement 12: Restrict physical access to cardholder data

Who Must Comply with PCI?

Any entity being it a merchant or service provider that stores, processes, and/or transmits cardholder data must be PCI DSS compliant - regardless the size of the entity and volume of transactions made. All merchants that acquire payment card transactions are categorized in 4 distinct levels, as determined by their number of annual transactions:

- **Level 1**: Merchants with more than 6 million card transactions and merchants which cardholder data has been compromised.
- **Level 2**: Merchants with card transactions between 1 and 6 million
- **Level 3**: Merchants with card transaction between 20,000 and 1 million
- **Level 4**: All other merchants

The Cost of Non-Compliance

Non-compliance with PCI can result in financial penalties levied against any vendor or service provider or even the denial of the ability of the merchant to accept or process credit card transactions. Costs also include:

- Monthly fines for noncompliance range from $5,000-$25,000
- Lost business - if acquirer refuses to process card payments for a merchant after data breach occurs
- Damaged reputation – consumers prefer to conduct business with company whose reputation is untarnished and never experienced data breach

Financial Impact of Non-Compliance: TJX Example

By not standardizing their security of cardholder data based on PCI requirements, TJX has taken a direct negative financial and public relations hit:

- The company announced that it took a $12 million loss, equal to 3 cents per share, because of the loss of more than 45 million credit and debit card numbers stolen from its systems over an 18-month period—one of the largest customer data breaches to date.
- The $12 million in losses was for costs incurred to investigate and contain the intrusion, improve computer security and systems and communicate with customers, as well as for technical, legal and other fees.

Lumension's Security Management Solutions Help Credit Card Issuers and Processors Comply with PCI
Lumension's endpoint security solutions enable credit card issuers and processors to ensure the confidentiality of customers' financial records and to ensure a stable and secure network environment. Lumension Security solutions include:

- **PatchLink Security Configuration Management** - Out-of-the-box regulatory and standards-based assessment to ensure endpoints are properly configured.
- **PatchLink Update** - Proactive management of threats through automated collection, analysis, and delivery of patches (all major operating systems and applications) across heterogeneous networks.
- **PatchLink Scan** - Complete network-based scanning solution enables assessment and analysis of threats impacting all network devices.
- **Sanctuary Application Control** - Policy-based enforcement of application use to secure your endpoints from malware, spyware and unwanted or unlicensed software.
- **Sanctuary Device Control** - Policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints.

Lumension proactively addresses PCI standards by continuously monitoring and assessing enterprise networks for software and configuration vulnerabilities, rapidly patching and remediating vulnerabilities and applying user access control policies across applications and removable devices.

Build and Maintain a Secure Network

PCI DSS Requirement 1: Install and maintain a firewall configuration to protect cardholder data	How Lumension Security Solutions Address PCI DSS Requirements
1.1.4 - Description of groups, roles, and responsibilities for logical management of network components	Description of groups, roles and responsibilities for logical management of network components are provided through multiple Lumension solutions: ○ **PatchLink Update** – Assigns nodes to OS and Active Directory groups, with support for custom nested grouping and role-based administration. ○ **PatchLink Scan** – integrated with PatchLink Update, displays OS, Active Directory and custom groups; also displays NT users/groups with permissions for a given machine. ○ **PatchLink ERS** – Displays roles and role descriptions ○ **Sanctuary Application Control** – Assigns user and/or group roles to specific application control functions. ○ **Sanctuary Device Control** - Assigns user and/or group roles to specific device control functions.

1.1.5 - Documented list of services and ports necessary for business	Documented lists of necessary services and ports are provided through multiple Lumension solutions: ○ **PatchLink Update** – Displays all registered services and their status. ○ **PatchLink Scan** – Scans for services and ports. ○ PatchLink ERS – Displays the services running or installed on network devices. ○ **Sanctuary Application Control** – Displays a list of all allowed applications and/or services.
1.1.7 - Justification and documentation for any risk protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented	Multiple Lumension solutions provide justification and documentation for risk protocols: ○ **PatchLink Update** – Displays list of common services binding to a risky protocol. ○ **PatchLink Scan** – Checks for vulnerabilities within plain-text protocols. ○ **PatchLink ERS** – Displays the risky protocols installed on network devices. ○ **Sanctuary Application Control** – Displays a list of all allowed applications and/or services
1.3.9 - Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network	Lumension solutions can verify required software and associated services and can ensure the installation through: ○ **PatchLink Update** – Conducts software inventory, which can reveal the presence of required software. Mandatory baseline can ensure that the software is installed. ○ **PatchLink Scan** – Detects services associated with required software.
1.5 - Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	Lumension solutions can report all IP addresses and ensure that they are masked to prevent being revealed on the internet: ○ **PatchLink Update** – Reports IP address of nodes. ○ **PatchLink Scan** – Discovers IP addresses. ○ **PatchLink ERS** – Ensures that all IP addresses have been masked.
PCI DSS Requirement 2: **Do not use vendor-supplied defaults for system passwords and other security parameters**	**How Lumension Security Solutions Address PCI DSS Requirements**
2.2.1 – Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)	Lumension's comprehensive scanning and whitelisting capabilities display services and enforce policies on servers: ○ **PatchLink Update** – Reveals current and startup state of services. ○ **PatchLink Scan** – Reveals current and startup state of services. ○ **Sanctuary Application Control** – Ensures that only specific applications/services can be installed or executed on a specific server.

2.2.2 - Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	Lumension's comprehensive scanning and whitelisting capabilities display services and enforce policies on servers: ○ **PatchLink Update** – Detects all registered services and their status. ○ **PatchLink Scan** – Reveals current and startup state of services. ○ **Sanctuary Application Control** – Ensures that only specific applications/services (e.g. FTP) can be installed or executed on a specific server.
2.2.3 – Configure system security parameters to prevent misuse	○ PatchLink Scan employs various policy-based application security checks to prevent misuse.
2.2.4 – Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and unnecessary web servers.	Lumension solutions can detect unnecessary software and services and enforce policies to remove the functionality and maintain the desired configurations: ○ **PatchLink Update** – Reports installed software and services and can remove software via PatchLink Developers Kit (PDK), an add-on to PatchLink Update. ○ **PatchLink Scan** – Reveals current and startup state of services. ○ **Sanctuary Application Control** – Ensures that only specific applications/services can be installed or executed on a specific server.
2.3 - Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	Lumension solutions utilize multiple secure methods for web-based management: ○ **PatchLink Update** – Fully supports SSL configuration for communication between agent and server. ○ **PatchLink Scan** – Uses SSH/NTLM when requesting admin access to targets. ○ **Sanctuary Application and Device Control** – Management console communicates to SXS via encrypted RPC level 6.

Protect Cardholder Data

PCI DSS Requirement 3: Protect stored cardholder data	**How Lumension Security Solutions Address PCI DSS Requirements**
3.4.1 – If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.	Sanctuary Device Control assures data is encrypted (256 AES) on authorized removable media.
3.5.1 – Restrict access to keys to the fewest number of custodians necessary.	Sanctuary Device Control restricts access to authorized devices by assigning permissions at the user or group level including other device control management functions such as password recovery.

Maintain a Vulnerability Management Program

PCI DSS Requirement 5: Use and regularly update anti-virus software or programs	How Lumension Security Solutions Address PCI DSS Requirements
5.1 - Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers) Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.	Lumension solutions can detect for machines missing anti-virus, deploy anti-virus software and enforce policy that enables only approved applications to execute: ○ **PatchLink Update** – Provides a light weight software distribution solution that can detect and deploy anti-virus software and update with the latest definitions. ○ **PatchLink Scan** – Detects if anti-virus is missing. ○ Sanctuary Application Control – Ensures that only authorized applications and processes can execute, thus protecting against known and unknown threats without requiring an exhaustive list of known bad applications.
5.1.1 - Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.	Lumension solutions ensure that machines have the correct anti-virus programs and versions, and enforce policy that enables only approved applications to execute: ○ **PatchLink Update** – Detects product name and version to ensure that the machine has the correct anti-virus program and version. ○ **PatchLink Scan** – Reveals status of installed services. ○ **Sanctuary Application Control** – Ensures that only authorized applications and processes can execute, thus protecting against known and unknown threats without requiring an exhaustive list of known bad applications.
5.2 - Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	Lumension solutions ensure that anti-virus versions are up-to-date with the latest signatures, with comprehensive auditing of activities: ○ **PatchLink Update** – Mandatory baseline enforces the installation and execution of anti-virus software. ○ **PatchLink Scan** – Detects out-of-date signatures. ○ **Sanctuary Application Control** – Provides full auditing of denied application executions and the last communications from the machine.

Maintain a Vulnerability Management Program continued »

PCI DSS Requirement 6: Develop and maintain secure systems and applications	How Lumension Security Solutions Address PCI DSS Requirements
6.1 - Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release	Lumension's network and agent-based scanning capabilities provide comprehensive vulnerability assessment with actionable information for immediate remediation: ○ **PatchLink Update** – Agent-based assessment, automated remediation and continued enforcement through mandatory baselines. ○ **PatchLink Scan** – Network-based assessment delivers actionable information for immediate remediation through PatchLink Update.
6.2 - Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	Lumension solutions discover new security vulnerabilities via network and agent-based scans, with the assessment of enterprise endpoints for prioritization and remediation: ○ PatchLink Update – Agent-based assessment, automated remediation and continued enforcement through mandatory baselines. ○ PatchLink Scan – Network-based assessment delivers actionable information for immediate remediation through PatchLink Update.
6.3.1 - Testing of all security patches and system and software configuration changes before deployment	PatchLink Update enables security patches and configuration changes to be quickly tested on any machine that is designated a member of the test group.
6.3.2 – Separate development, test, and production environments	PatchLink Update enables machines to be grouped based on any criteria.
6.3.3 - Separation of duties between development, test, and production environments	PatchLink Update and Scan provide role based access control allowing users to only manage the groups to which they are assigned.
6.4.4 – Back-out procedures	PatchLink Update provides the capability to roll back software and patches that support an uninstall command line argument.
6.5.1 – Unvalidated input	PatchLink Scan conducts various web security (webcheck and banner) vulnerability checks for known software.
6.5.4 – Cross-site scripting (XSS) attacks	PatchLink Scan conducts various web security (webcheck and banner) vulnerability checks for known software.
6.5.5 – Buffer overflows	PatchLink Scan's network-based assessment scans for known buffer overflows.
6.5.6 – Injection flaws (for example, structured query language (SQL) injection)	PatchLink Scan's network-based assessment scans for known SQL injection vulnerabilities.
6.5.9 – Denial of Service	PatchLink Scan's network-based assessment scans for DOS vulnerabilities and whitelisting capability provides execution control against unknown applications that may contain malicious code.

Maintain a Vulnerability Management Program : PCI DSS Requirement 6 continued »

6.6 - Ensure that all web-facing applications are protected against known attacks by applying either of the following methods: ○ Having all custom application code reviewed for common vulnerabilities by an organization ○ Installing an application layer firewall in front of web-facing applications.	Lumension's network and agent-based scanning ensure the identification of application layer firewall installation, as well as associated services: ○ **PatchLink Update** – Agent-based software inventory detects firewall installation. ○ **PatchLink Scan** – Network-based scan discovers services associated with application layer firewall

Implement Strong Access Control Measures

PCI DSS Requirement 7: Restrict access to cardholder data by business need-to-know	**How Lumension Security Solutions Address PCI DSS Requirements**
7.1 - Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	Sanctuary Application and Device Control provide access control to limit users to specified applications and/or devices (computing resources). All others are denied by default.
7.2 - Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	Sanctuary Application and Device Control provide access control to limit users to specified applications and/or devices (computing resources). All others are denied by default.
PCI DSS Requirement 8: Assign a unique ID to each person with computer access	**How Lumension Security Solutions Address PCI DSS Requirements**
8.5.4 – Immediately revoke access for any terminated users	Sanctuary Application and Device Control leverage the existing security accounts (AD, NDS) and policies can be automatically updated with the addition or removal of a user account with an active group.
8.5.8 – Do not use group, shared or generic accounts nd passwords	PatchLink Scan's network-based assessment detects if guest accounts are enabled.
8.5.9 – Change user passwords at least every 90 days	Network and agent-based scanning detect minimum password age policies and can validate password history: ○ **PatchLink Update** – Agent-based software can validate password history through a custom inventory collection. ○ **PatchLink Scan** – Network-based scan detects minimum password age policy.
8.5.10 – Require a minimum password length of at least seven characters	Network and agent-based scanning detect minimum password length policies and can validate password length: ○ **PatchLink Update** – Agent-based inventory capability validates password length. ○ **PatchLink Scan** – Network-based scan detects minimum password length policy.

Implement Stong Access Control Measures : PCI DSS Requirement 8 continued »

8.5.11 – Use passwords containing both numeric and alphabetic characters	Lumension solutions can detect, validate and enforce complex passwords: ○ **PatchLink Update** – Agent-based inventory capability validates password complexity. ○ **PatchLink Scan** – Network-based scan detects password complexity policy option. ○ **Sanctuary Device Control** – Enforces encrypted media passphrases to require complex passwords that include both numeric and alphabetic characters.
8.5.12 - Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used	Lumension solutions detect and validate password history: ○ **PatchLink Update** – Agent-based inventory capability validates password age. ○ **PatchLink Scan** – Network-based scan detects password history policy.
8.5.13 – Limit repeated access attempts by locking out the user ID after not more than six attempts	Lumension solutions can detect, validate and enforce limited repeat access attempts: ○ **PatchLink Update** – Agent-based inventory capability validates account lockout threshold. ○ **PatchLink Scan** – Network-based scan detects account lockout policy. ○ **Sanctuary Device Control** – Enforce policy to lock out a user from accessing encrypted media after entering an incorrect passphrase more than five times. The locked device is unusable until an administrator intervenes.
8.5.14 - Set the lockout duration to thirty minutes or until administrator enables the user ID	Lumension solutions can detect, validate and enforce lockout duration until an administrator enables the user ID: ○ **PatchLink Update** – Agent-based inventory capability validates account lockout duration. ○ **Sanctuary Device Control** – Enforce policy to lock out a user from accessing encrypted media after entering an incorrect passphrase more than five times. The locked device is unusable until an administrator intervenes.
8.5.15 - If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal	PatchLink Update's agent-based scan validates idle time and password protect on resume.
PCI DSS Requirement 9: Restrict physical access to cardholder data	**How Lumension Security Solutions Address PCI DSS Requirements**
9.9 - Maintain strict control over the storage and accessibility of media that contains cardholder data.	Sanctuary Device Control provides AES 256 encryption of authorized removable storage devices that can be used to store cardholder data, and monitors the use of these devices.

Regularly Monitor Test Networks

PCI DSS Requirement 10: Track and monitor all access to network resources and cardholder data	How Lumension Security Solutions Address PCI DSS Requirements
10.2.2 – All actions taken by any individual with root or administrative privileges	Sanctuary Application and Device Control provide the ability to track all changes made by authorized administrators to policies.
10.2.3 – Access to all audit trails	Sanctuary Application and Device Control provide the ability to track all changes made by authorized administrators to policies.
10.2.4 – Invalid logical access attempts	Sanctuary Application and Device Control log all attempts from unauthorized users to access authorized applications/devices or from authorized users to access unauthorized applications/devices.
10.2.5 – Use of identification and authentication mechanisms	Sanctuary Application and Device Control ensure that all administrative changes and device usage are correlated with either an AD or NDS authenticated user.
10.2.6 – Initialization of the audit logs	Sanctuary Application and Device Control audit logs automatically and initialize upon successful completion of the Sanctuary infrastructure components.
10.3.1 – User identification	Sanctuary Application and Device Control automatically include user identification information in all audit entries.
10.3.2 – Type of event	Sanctuary Application and Device Control automatically include event information in all audit entries.
10.3.3 – Date and time	Sanctuary Application and Device Control automatically include date and time stamp in all audit entries.
10.3.4 – Success or failure indication	Sanctuary Application and Device Control automatically include success or failure of execution or access attempts in all audit entries.
10.3.5 – Origination of event	Sanctuary Application and Device Control automatically include the origination of event in all audit entries.
10.3.6 – Identity or name of affected data, system component, or resource	Sanctuary Application and Device Control automatically include the identity or name of affected data, system component or resource in all audit entries.
10.5 – Secure audit trails so they cannot be altered.	All Sanctuary Application and Device Control audit information is stored in the Microsoft SQL Server and once written can only be read by the Sanctuary Management Console.
10.5.1 – Limit viewing of audit trails to those with a job-related need.	Sanctuary Application and Device Control employ role based access to various management functions, limiting the viewing of audit trails and ensuring that only authorized users/groups may read audit related data.

Regularly Monitor Test Networks : PCI DSS Requirement 10 continued »

10.5.2 - Protect audit trail files from unauthorized modifications.	Sanctuary Application and Device Control audit information is stored in the Microsoft SQL Server and once written can only be read by the Sanctuary Management Console.
10.5.3 - Promptly back-up audit trail files to a centralized log server or media that is difficult to alter	Sanctuary Application and Device Control auditing and logging data can be exported to CSV or XML formats via an email attachment or saved as a file on the network on a scheduled basis, enabling this data to be included in a centralized log server.
10.6 - Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).	Sanctuary Application and Device control logs can be reviewed daily via a default template.
10.7 - Retain audit trail history for at least one year, with a minimum of three months online availability.	Sanctuary Application and Device control audit-related information is stored in Microsoft SQL Server tables which can typically store more than one year of audit data.
PCI DSS Requirement 11: Regularly test security systems and processes	**How Lumension Security Solutions Address PCI DSS Requirements**
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).	Lumension solutions enable the scheduling of internal and external network scans: ○ **PatchLink Update** – Performs DAU's on an ongoing basis to ensure the most current view of enterprise vulnerabilities. ○ **PatchLink Scan** – Enables internal scans to be scheduled
11.5 - Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.	Sanctuary Application Control monitors all attempts to execute non-authorized files, which includes any authorized file that has been modified.

Maintain and Information Security Policy

PCI DSS Requirement 12: Maintain a policy that addresses information security for employees and contractors	**How Lumension Security Solutions Address PCI DSS Requirements**
12.3.3 - List all such devices and personnel with access.	Sanctuary Device Control provides detailed list of authorized devices and users.
12.3.7 - List of company-approved products.	Sanctuary Application and Device Control provide the ability to set and report on the use of authorized applications and devices.
12.3.9 - Activation of modems for vendors only when needed by vendors, with immediate deactivation after use	Sanctuary Device Control provides the ability to set temporary and scheduled permissions for modem usage by machine and report on device usage.

Maintain and Information Security Policy : PCI DSS Requirement 12 continued »

12.5.2 - Monitor and analyze security alerts and information, and distribute to appropriate personnel	Lumension solutions continuously monitor vulnerabilities or device use activity and automatically notify appropriate personnel: ○ **PatchLink Update** – Delivers summary information about each vulnerability that is displayed and provides a link to the manufacturer's knowledgebase article. ○ **PatchLink Scan** – Provides detailed description of vulnerability as well as the appropriate solution. ○ **Sanctuary Application Control** – Enables the scheduling and emailing of automated reports that document administrative changes and end point usage activity within a specified period of time. ○ **Sanctuary Device Control** – Enables the scheduling and emailing of automated reports that document administrative changes and end point usage activity within a specified period of time.
12.5.5 – Monitor and control all access to data.	Sanctuary Device Control policies can enforce and monitor use of authorized devices.
12.9.5 - Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems	Sanctuary Application and Device Control can export all auditing and logging data to CSV or XML formats via an email attachment or saved as a file on the network on a scheduled basis. This provides an integration point with an SEIM.

To Learn More

To learn more about Lumension Security solutions and how we can address your PCI compliance challenges, please contact us by any of the following means

Phone: 480.970.1025 (Option 1)
Email: patchlink.sales@lumension.com
Web: www.lumension.com

Sources:

1. Deloitte Global Financial Services Industry 2007 Global Security Survey2005 Yankee Group Security Leaders and Laggards Survey

Lumension SECURITY

Lumension Security
15880 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260
480.970.1025 / www.lumension.com