WhiteSheet

Navigate Your Way to PCI DSS Compliance

CORRELOG

CorreLog for PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a series of IT security standards that credit card companies must employ to protect cardholder data from disclosure. The standards also apply to organizations these credit card companies share cardholder data with.

The Payment Card Industry Data Security Standard (PCI DSS) secures cardholder data that is stored, processed or transmitted by merchants and other organizations. The standard is managed by the PCI Security Standards Council (PCI SSC) and its founders — American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Input for proposed changes to the standard is also made by PCI SSC stakeholders —participating organizations, including merchants, banks, processors, hardware and software developers, point-of-sale vendors and the assessment (QSA & ASV) community. The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information. Initially created by aligning Visa's Account Information Security (AIS)/Cardholder Information Security (CISP) programs with MasterCard's Site Data Protection (SDP) program, the standard provides an actionable framework for developing a robust account data security process — including preventing, detecting and reacting to security incidents.

Q: What is defined as "cardholder data"?

A: Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data.

Background facts

The Payment Card Industry Security Standards Council (PCI SSC) was launched on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.). Note: the payment brands and acquirers are responsible for enforcing compliance, not the PCI council.

Companies and industries impacted

PCI applies to ALL organizations or merchants, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data. Therefore, if a customer of that organization pays the merchant directly using a credit or debit card, then PCI DSS requirements apply.

Penalties and fines for non-compliance

Any fines and/or penalties associated with non-compliance with the PCI DSS and/or confirmed security breaches are defined by each of the payment card brands. As a guideline, non-compliance fines up can range from $25,000 to $100,000 per incident based on a variety of criteria.

WhiteSheet

Navigate Your Way to Compliance — CorreLog for PCI DSS

Ship's Log: True Tales of PCI DSS

1. An ex-employee uses the password of an associate to enter your private system.

a) CorreLog keeps track of user activity on your system, automatically tracking when users have logged into the system and what changes they have made to critical data items.

b) You can quickly see when a user has accessed an invalid machine, perhaps during odd hours, and be notified of suspicious behaviors, such as clearing log files, installing software, or simply running an editor or application.

c) You are notified of the event via e-mail, pager, or some other method — so you can take immediate action to block unauthorized access.

d) A permanent log of all activity is saved, allowing you to investigate further.

2. A disgruntled administrator decides to install a key logger on your personal PC; then clears the event logs to cover his tracks.

a) CorreLog receives log messages from your intrusion detection system, and immediately sends this information to Correlog, maintaining a permanent record of this malicious event, including the event log being cleared on your PC.

b) Clearing your PC's event log (or other activity, such as stopping your Virus protection) serves only to further incriminate the Administrator, since this data has already been logged by CorreLog in real-time.

c) You are notified of the attack, and correlate this activity with other possibly malicious events on your network, such as modifications to firewalls and loosening security policies by this administrator.

d) The data is permanently archived and available for forensic analysis.

e) Archive data includes encrypted checksums and security codes, which will be available if criminal charges are filed against the employee.

3. A mistake permits a private disk to be exported to a public area.

a) Correlog detects the disk changes and immediately notifies administrative personnel.

b) CorreLog determines who may have accessed the data — and what other activities they may have done prior to and following the illegal access.

c) CorreLog takes automatic action upon certain events, such as shutting down firewalls or public Internet access.

d) The advanced correlation features of CorreLog greatly reduce false alarms, so that action is taken only if the problem is truly critical.

4. A customer or client accuses your company of negligence with your data.

a) CorreLog provides a clear record of security violations, and supports an over-arching security policy that incorporates all types of platforms, network devices and application programs.

b) Tamper-proof archives, with encrypted checksums, provide clear evidence of security breaches (or the absence of security breaches).

c) Correlog monitors thousands of security points within your enterprise and provides a clear audit trail — demonstrating your commitment to security and data privacy.

d) If a breach does occur, immediate assessment of the actual severity can be obtained, as opposed to your customer or client assuming the worst-case scenario.

Navigate Your Way to Compliance — CorreLog for PCI DSS

Q: Does Requirement 3.4 apply to mainframes?

A: Requirement 3.4 of the PCI DSS must be applied to mainframes that contain cardholder data. If the company has legitimate business or technical constraints to meet this or any other requirement, compensating controls may be applied. Compensating controls must be commensurate with additional risk imposed by not adhering to the original requirement. Specific to compensating controls, please refer to Appendices B and C of the PCI DSS.

CorreLog at the Helm of PCI DSS Compliance

The CorreLog system monitors thousands of security points; logging all activity on your system (in excess of ten-million events each day) and correlating this data into alerts and actionable data – more clear and detailed than any other technology today. The solution incorporates a sophisticated, indexed search engine to furnish extremely fast, interactive searching — saving your organization man hours and reducing expertise requirements. With CorreLog, businesses can reach PCI DSS compliance. Below, please find out how CorreLog addresses PCI DSS guidelines:

Install and maintain a firewall configuration to protect cardholder data.

CorreLog monitors changes to firewall rules and all attempts to bypass firewalls. CorreLog also interfaces with Intrusion Detection Systems, including SNORT and many others — indicating that a firewall may have been breached or a security policy changed.

Do not use vendor-supplied defaults for system passwords and other security parameters.

Correlog tracks changes to security parameters, detecting when unauthorized changes are made to these rules and tracking users by name. Example A – CorreLog detects when a security policy associated with strong passwords on a system has been modified, indicating that someone may have returned a vendor-supplied security setting to its default condition. Example B – CorreLog catches all cases where the default “guest” login is used on a network.

Protect stored cardholder data.

CorreLog detects logins to those computer systems processing cardholder data and protects this data in a variety of ways: it ensures that the system is performing as expected (with regard to performance, access and software updates) and it detects break-in attempts to computers, databases, websites and storage disks. Correlog monitors disk activities, disk mount points and use of removable storage including CD/DVD burners and removable USB storage devices.

Encrypt transmission of cardholder data across open, public networks.

CorreLog encrypts data, so there is never a worry that Correlog might reveal cardholder data parameter or other system description. CorreLog is FIPS-compliant — incorporating strong encryption algorithms for data transfers.

Use and regularly update antivirus software.

CorreLog monitors messages created by antivirus software programs, indicating when antivirus software has changed, has been enabled. CorreLog keeps a permanent record of virus detection activity — on all the computers in your enterprise — including servers and PCs. CorreLog works with all major antivirus software programs on both Windows and UNIX® platforms.

Assign a unique ID to each person with computer access.

CorreLog indicates when a user logs into the system at an unexpected time, signifying that someone else (other than the identified user) is accessing records.

WhiteSheet

Navigate Your Way to Compliance — CorreLog for PCI DSS

Develop and maintain secure systems and applications.

CorreLog furnishes ability to make Windows platforms more secure (using the CorreLog Windows agent). For UNIX and other platforms, CorreLog leverages the existing native agent (i.e. the syslog process) to make the managed system more secure. CorreLog is a substantial "development component" of an enterprise-wide security system that incorporates a standards-based, easy-to-use API to allow you to extend your security to any streaming log file or home-grown application.

Restrict access to cardholder data by business need to know.

CorreLog monitors the creation, deletion and modification of user accounts and groups so it can detect when access has been given to a user to a particular system. Additionally, CorreLog keeps track of user logins to these systems, including by time of day, so that "after hours" unauthorized access is easily detected.

Restrict physical access to cardholder data.

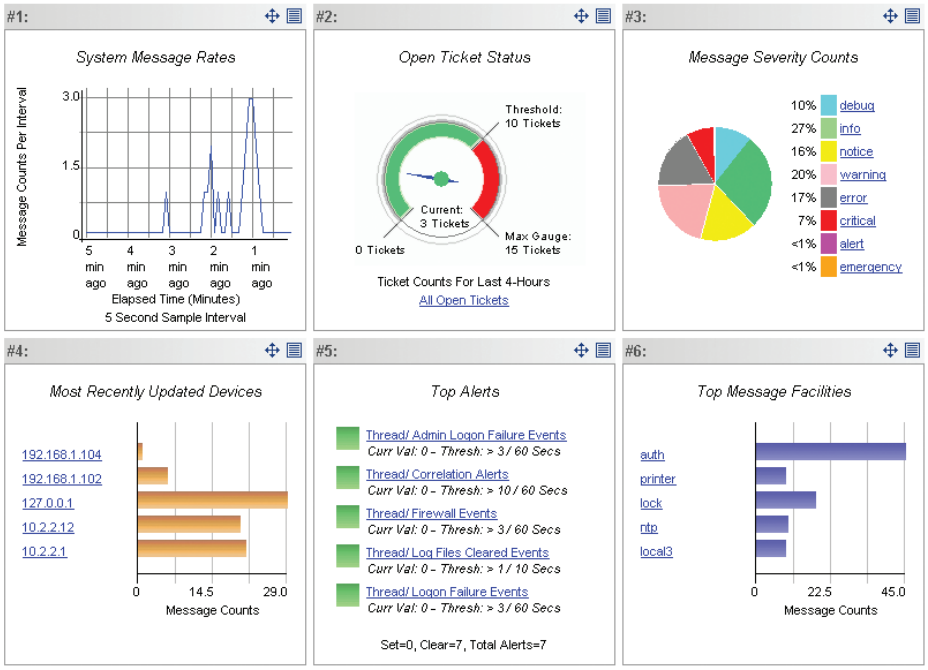
CorreLog detects when systems are restarted (via a cold-start trap or via syslog messages) indicating that physical access may be breached — and systems may have been tampered with. This includes detection of USB and computer driver activity; indicating that somebody may have physical access to a restricted machine.

Track and monitor all access to network resources and cardholder data.

This is the main role of CorreLog as a security monitor. It provides visibility into who is logging into what areas of the enterprise and keeps track of what users are doing on the system. This is achieved through monitoring log messages and mapping activity back to security protocol. The correlation is presented in detailed event reports and dashboards like the one below.

Regularly test security systems and processes.

CorreLog schedules periodic tests of network integrity and verifies that certain messages are logged, indicating successful tests. CorreLog interfaces easily with common, security-test software, including port scanners, to verify that CorreLog is successfully monitoring system security. CorreLog has a self-test associated with AES encryption that permits users to verify that CorreLog encryption is working.



Sample of CorreLog Custom Dashboard Reporting

Navigate Your Way to Compliance — CorreLog for PCI DSS

Maintain a policy that addresses information security.

An organization cannot claim to have a comprehensive information security policy without monitoring the security message being constantly logged on platforms within your enterprise. An enterprise that installs CorreLog, with no other action, takes a major step forward in creating and maintaining an enterprise security policy.

Navigate Your Way to PCI DSS Compliance Today

To learn more about how CorreLog can help, contact CorreLog toll-free in the US at 877-CorreLog or 239-514-3331 or visit www.correlog.com.

Installation Requirements

The CorreLog Security Server system requires Windows Vista, XP, 2003, or 2000 workstation or server platforms. There are no hard limits on CPU, disk space, or memory resources. The CorreLog Security Server download package incorporates the Apache HTTP server, easy, Windows-based installation dialog, a ready-to-run configuration, and an encompassing user manual. The system also includes a copy of the CorreLog Syslog Windows Tool Set and manual so users can easily add Syslog capability to an existing Windows platform, making the CorreLog Security Server full-enterprise capable.

Free, 30-Day Evaluation

Download CorreLog for Windows 200x, XP, and Vista systems. NOTE: the CorreLog server system is designed for easy installation. A typical installation does not require the host platform to be rebooted and can be performed in less than five minutes. Download a free evaluation at: www.correlog.com/download.html.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution. CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog automatically identifies and responds to network attacks, suspicious behavior and policy violations by collecting, indexing and correlating user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners.
Visit www.correlog.com for more information.

1004 Collier Center Way, Suite 103 · Naples, Florida 34110 · 1-877-CorreLog · 239-514-3331 · info@correlog.com