



Executive Summary

Aurora Enterprises: Providing Solutions for PCI Compliance

Overview

This paper discusses how the Aurora portfolio of security solutions can help enterprises meet or exceed the Payment Card Industry Data Security Standards requirements (PCI).

PCI affects any company that processes, stores or transmits credit card information. The standards are designed to protect client information and deter fraud. The cost of not implementing the PCI standards can be severe. However, fear should not be the motivator for implementing PCI standards.

The PCI standards can be considered best-practice standards, and can help protect credit card information as well as all of your important client and corporate data.

While each company situation is different, understanding the role of PCI, its objectives and how your company will be affected by it is important to beginning a successful path to implementation. This white paper will help you understand PCI and decide on a course of action.

Intended Audience

This white paper is intended for C-Level executives, consultants and IT Managers.

Whitepaper Sponsor

This white paper is sponsored and presented by Aurora, a leader in security consulting, data encryption and compliance. Aurora works with companies to secure their information, both internally and externally. Our areas of expertise include encrypting and securing data, and security-specific compliance issues such as PCI, Sarbanes-Oxley and HIPAA.

For More Information

If you require more information on PCI or other security issues, please call us at (310) 530-8260, email us at info@auroraent.com, or visit our website at www.auroraent.com

Aurora Enterprises: Providing Solutions for PCI Compliance

This paper discusses how the Aurora portfolio of security solutions can help enterprises meet or exceed the Payment Card Industry Data Security Standards requirements (PCI).

Overview

Visa, American Express, Diner's Club, Discover, JCB and MasterCard collaborated to create a new set of standards, based on CISP (Cardholder Information Security Policy), and known as the PCI (Payment Card Industry) Data Security Standard. All merchants and service providers that handle, transmit, store or process information concerning any of these cards, or related card data, are required to be compliant with PCI or face contract penalties or even termination by the credit card issuers.

The credit card issuers take these requirements very seriously. Since December 2006 VISA has fined violators up to \$500,000 per event ... and they are taking the money directly out of the violator's bank account. American Express is fining merchants up to \$15,000 per day for failures to comply and forcing them to bring in a third-party contractor to bring systems into compliance.

The primary purpose of this standard is to protect credit card data by reducing fraud and theft. The PCI standard seeks to accomplish this through a "defense-in-depth" strategy.

There are six primary areas covered by PCI that are divided into 12 requirements:

Build and Maintain a Secure Network

1. Install and maintain firewalls
2. Do not use vendor-supplied or default passwords

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmissions of cardholder data as well as sensitive information as it travels across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to need-to-know
8. Assign unique IDs to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Monitor and track all access to network resources and cardholder data

- 11. Regularly test security systems and processes
- Maintain an Information Security Policy**
- 12. Maintain a policy that addresses information security

Who Is Impacted?

Most industry standards are specified only for a group of companies or individuals. PCI expands the impact to include a wide variety of computer systems as well.

The types of companies who are impacted include:

- All members, merchants, and service providers that store, process, or transmit cardholder data

Additionally, these security requirements apply to all “system components” i.e., any network component, server, or application included in, or connected to, the cardholder data environment, including:

- Network components including, but not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances
- Servers including, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP
- Applications including all purchased and custom applications, including internal and external (web) applications

Aurora Security Portfolio

There are numerous options for security software that can be combined to meet the PCI requirement, along with other hardware and best-practice solutions. Aurora offers an integrated solution from Secure Computing, based on it’s ease-of-management, history for reliability and exceptional support. Aurora implements four comprehensive Secure Computing product portfolios to help you comply with all industry and government regulations.

The full suite of Secure Computing options is listed in the appendix. Viable protection in each area of PCI is important to meet compliance with the standard. Aurora selected Secure Computing’s suite because it met or exceeded the PCI standard in each of the following critical areas.

<p>Identity and Access Management Solutions</p>	<ul style="list-style-type: none"> • Provides strong, two-factor authentication tokens which never expire and can access any application, integrate seamlessly into any LDAP, and deploy with standard Microsoft tools • Provides secure anytime, anywhere access to sensitive applications, data and networks
---	--

	<ul style="list-style-type: none"> • Provides endpoint security so that only properly configured devices have network access • Easily manages remote, wired, or wireless access for employees, contractors and guests
<p style="text-align: center;">Network Gateway Security Solutions</p>	<ul style="list-style-type: none"> • Provides the most comprehensive, self-defending application proxy firewall appliance in the world, protecting the network from all types of threats, both known and unknown • Allows only tightly defined and granular application traffic through at gigabit speeds, while providing zero-tolerance for all suspicious and undesirable traffic • Protect against all classes of threats including packet fragmentation, spoofing, denial of service (DoS), viruses, worms, Trojans, spam, spyware, SQL injection, fraud and more
<p style="text-align: center;">Messaging Gateway Security Solutions</p>	<ul style="list-style-type: none"> • Protects sensitive content from leaving the enterprise, unprotected, through email, IM, peer-to-peer, FTP, or VoIP protocols • Scans all portion of a message with sophisticated technologies, including fingerprinting, clustering, image scanning, and adaptive learning • Provides multiple encryption technologies, including both “push” and “pull” to ensure usability as well as manageability • Provides 12 unique actions that can be taken when sensitive content is discovered, including archiving and end-user education
<p style="text-align: center;">Web Gateway Security Solutions</p>	<ul style="list-style-type: none"> • Protects against all inbound threats from the web, including spyware, active content, and Trojans • Protects against sensitive content from leaving the enterprise through blogs, webmail, or peer-to-peer networking • Increases employee productivity by blocking objectionable surfing • Controls encrypted traffic by applying security policies over SSL sessions

Implementing PCI Compliance

Regardless of how you decide to have your PCI compliance needs met, a secure and cost-effective PCI compliance implementation begins with a personalized assessment, followed by a comprehensive implementation plan. Solid and well-supported hardware and software also needs to be used to maintain security from end-to-end. While it is possible to use multiple vendors to meet each requirement, a proven suite of products that can successfully work together will lessen headaches and lower maintenance costs.

The following outlines features that are recommended for each of the 12 PCI requirements.

Requirement #1: Install and maintain firewalls

A firewall is the gateway to your network and is the first line of defense in securing information. Installing and maintaining your firewall can be accomplished by purchasing a firewall that:

- Contains a hardened operating system. Questions to ask when selecting a firewall include: has the firewall OS ever been compromised?
- Offers enterprise-class features that support gigabit speed stateful inspection filtering
- Numerous application-specific security proxies
- Embedded IPS, anti-virus, anti-spyware, anti-spam, and URL filtering engines natively on the platforms
- Granular audit trail in the industry
- Streaming of all logs securely and in real-time to an advanced log aggregation, event correlation and alerting system. This is critical for auditing and other compliance issues.

Requirement #2: Do not use vendor-supplied or default passwords

While this seems simple to accomplish, passwords are a single point of failure for many companies. It is important to institute a process for selecting passwords that does not leave your secure network vulnerable. One solution is to provide security tokens – handheld devices that can control access to key resources. These tokens use single-use, two-factor authentication to protect approved individuals' passwords. By combining something users have with something users know, password tokens can meet every requirement for authentication strength. These tokens can be set to never expire and require no updates. The most advanced tokens have batteries that never wear out while in the field.



Requirement #4: Encrypt transmissions of cardholder data as well as sensitive information as it travels across public networks

Encryption needs to be automated and comprehensive in order to make the PCI implementation useful and secure. The most effective systems use policy engines that allow for detailed policies to be automatically enforced, making encryption decisions based upon hundreds of different attributes, including sender, recipient, content, domain, groups, attachments and more. Removing end users from the decision-making process ensures that the messages containing sensitive or protected content are automatically sent encrypted.

A key challenge in encryption is adapting to the needs of the recipient. Depending on their capabilities, different types of encryption may be most appropriate. Choose a system that can dynamically select between different encryption methodologies to best fit the situation. Also ensure that your encryption is from gateway to gateway to ensure compliance.

Requirement #5: Use and regularly update anti-virus software

There are several different forms of anti-virus protection that can occur at different points in your network. Consider these three gateways as entry points that require virus protection.

Network gateway — Network traffic is scanned against known virus signatures. Make sure that these signatures are updated regularly and automatically, since they change often. While comparing signatures on known viruses is an important protection methodology, look for solutions that are able to separate acceptable traffic from suspicious traffic, and block suspicious threats. This approach is highly effective at preventing unknown attacks and dramatically reduces an organization's attack vulnerability by automatically eliminating exposure.

Messaging gateway — Many threats enter via emails, and can be let in by unwary users. Local virus scanning software is helpful, but messaging appliances, such as SecureComputing's IronMail, are extremely effective at stopping threats before they reach users. The best protection allows you to use multiple virus signature engines simultaneously, create custom keyword policies, delete specific file extensions, scan deep attachments, provide spam blocking (spam is a major source of threats), allow for management of sender reputation (which creates whitelists of trusted users) and to identify patterns in sender behavior. The most effective appliances can stop viruses 100% of the time, so don't settle for partial success.

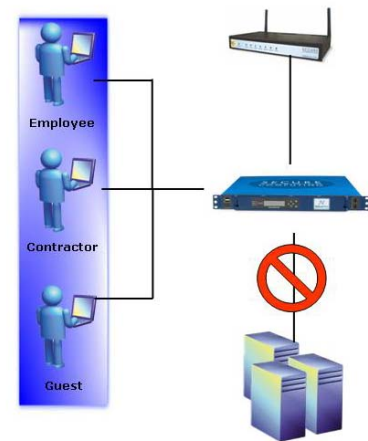
Web Gateway — many threats now originate on websites visited by your employees. Malicious viruses and codes can hijack your user machines and make your network vulnerable. Look for products that scan Web traffic and block attacks. This is a key component to keep your network secure and in compliance with the goals of PCI.

Requirement #6: Develop and maintain secure systems and applications

Implementing new hardware and software can protect your network, but compliance and best practices mandates the ongoing management of security. A secure infrastructure includes the protocols to protect the system at all levels — hardware, traffic, files and applications. Innovative systems can protect down to the file level, hard-coding access to key files and applications at the user or network card level, eliminating the opportunity for outside hackers to gain root access to a machine on your network. These types of safeguards constantly monitor attacks and changes on your system, providing ongoing security, a must for any company that has vital information on its servers and desktops.

Requirement #7: Restrict access to need-to-know

Identity and access management (IAM) is vital to PCI compliance. Software solutions, and appliances that secures access, enforces policy, and provides complete and customizable reporting for your entire network are available. A viable solution has to be very fast and built with simplicity in mind. The goal is to protect your network, without hobbling your users. A good IAM implementation provides secure access to every application and data resource in your network, hosting every access method for users both inside and outside the enterprise. With proper IAM protocols and protection in place, internal users, extranet users and key vendors can share information without fear of compromising your network security.



Look for IAM systems where you have total control: limiting access based on where the user is, what machine the user is on, and when they're accessing the data. Flexible systems allow you to segment your network into logical security zones, based upon the sensitivity of the resource. Only properly identified users with secure devices and the proper level of authentication can access these zones, which require no reconfiguration of your infrastructure. A trusted machine inside the building may have full access rights to all applications, but a remote device such as a home PC may be restricted to only Webmail or view-only rights.

Requirement #8: Assign unique IDs to each person with computer access

Security and identity protocols are compromised unless each user in your network is assigned a unique ID. PCI compliance, along with other regulations such as HIPAA and Sarbanes-Oxley, require the ability to track back access to the individual. With an integrated, secure identity

authentication system, there is proof-positive-identity for all users. For maximum flexibility, look for vendors that support several common authentication methods, including Radius, LDAP, SecurID, and digital certificates.

Requirement #10: Monitor and track all access to network resources and cardholder data

A centralized monitoring and tracking system builds upon unique ids to identify threats and security breaches. Secure systems provide centralized access setup, policy enforcement, user management, and configuration compliance, which can also dramatically simplify reporting and auditing.

Centralization is key to reducing workloads, and many organizations get overloaded when they have to run multiple reports for each access point (Citrix, VPN, Outlook web access, etc.), and then merge them together manually. Reporting overhead can lead to key reports and monitoring being neglected, a threat to your security. Advanced systems verify every access, authentication, and authorization request. Not only does this cut down on labor for auditing, reporting, and compliance, it also reduces errors integrating disparate reports, simplifies the reporting process and provides a reliable audit trail for compliance.



Real-time dashboard view of security events.

Look for systems that include the ability to collect, normalize, aggregate, and correlate the event data from firewall/security appliances, and that are able to view, understand, and distribute this information in readily understandable ways. Insist on real-time reporting for:

- Failed system-level login attempts
- Failed application-level login attempts
- Attempted exploitation of a system by a virus or worm
- Attempted exploitation of a system by unauthorized individuals
- Failed access attempts to files or application data
- Correlating multiple system events to illicit data access

Reporting is also important for all of your messaging and web traffic, as it allows you to monitor and report on all potential threats.

Requirement #11: Regularly test security systems and processes

A viable PCI implementation — in fact, any good security implementation — includes a process for regular testing. Verifying that your systems can withstand an attack, especially as attacks evolve, is critical to maintaining security. Changes in personnel, lapses in software subscriptions, or changes in

focus can create a false sense of security. Regular testing ensures that your security protocols continue to be in compliance.

This process can be simplified when you choose software and hardware that has been proven to be effective in design. While updates of virus signatures are common and necessary, shy away from operating systems on security devices that require frequent patches to protect from vulnerabilities. Selecting a secure system upfront makes testing more routine and less disruptive.

Requirement #12: Maintain a policy that addresses information security

PCI requires that you maintain a security policy. An effective policy starts with an assessment of the type of data your system needs secured, and integrates with the capabilities of your hardware and software.

Policy definition allows you to set the rules that are necessary to stay in compliance with PCI and other major legislation (SOX, GLBA and HIPAA), today and in the future.

Appliances and software that allow for flexible policy definition are easier to manage, and allow you to adapt to changes and new standards. Advanced and integrated systems allow for centralized management of policies. Since policies are enforced at the gateway, no end user training is required for the policies to become effective.

The number of devices that can be managed is also important. Your system should not be outgrown by the number of new appliances you add. Look for the upper limit of appliances that can be managed from a single console, and make sure it is in line with your anticipated growth. Give yourself even more flexibility by looking for components that combine centralized policies with user-specific policies for certain applications. Each policy can include specific security settings, including the number of anti-virus engines deployed and the order of scanning.

Over and Above the Basics

PCI compliance is important to all organizations that process or store credit card information. The steps necessary to achieve PCI compliance in a cost-effective manner also build a secure infrastructure for your company that delivers other dividends. If your company requires a higher level of security, Aurora and its partners can deliver even more stringent security processes and implementations to meet any need, including medical, financial and military grade security.

Conclusion:

PCI is one of the most comprehensive standards developed to date. The credit card companies are serious about proving to the world that consumer information is safe in their hands. Demonstrating compliance with PCI is about following best practices, which is in the enterprises' best interests as well as the consumers who trust companies with their information. Once personal information is stolen from a company, the harm to the consumer is hard to limit, and a consumer's trust in the company will be forever damaged.

For more information on the PCI compliance, or any security concern, please call us at (310) 530-8260, email us at info@auroraent.com, or visit our website at www.auroraent.com

Appendix

While Aurora can work with a variety of software and hardware vendors and solutions, we have extensive experience working with Secure Computing, one of the most trusted names in messaging and network security solutions. Our experience in integrating and managing these solutions has allowed us to create a recommended set of tools for companies looking to implement PCI compliance.

The following products have been tried and implemented by Aurora and are trusted parts of our PCI Compliance solution.

Recommended Firewall

Aurora recommends the Secure Computing Sidewinder G2

Built on unique, patented Type Enforcement security technology, Sidewinder G2 defends networks and applications from all types of Internet threats, both *known and unknown*. Sidewinder has achieved the highest level of Common Criteria certification in the world: EAL4+ on 20 unique criteria.

The NSA also bench tested Sidewinder against their very stringent standards. They liked Sidewinder so much, they use it themselves. Black Hat Consulting tried their best to break Sidewinder, and couldn't. It's the only firewall they've never penetrated. They described it as "by far the sturdiest system we've audited ... and the most stable and reliable firewall we have tested."

Recommended Messaging Solutions

In the messaging gateway IronMail[®] is unique in applying behavioral techniques to pinpoint and block direct attacks on the email infrastructure. By granularly tracking message traffic, including senders, message volume, attachments, and a variety of other statistics, IronMail can detect when incoming or outgoing traffic is out of the norm. This usually indicates some type of attack is underway. Once detected, IronMail automatically applies rules to block the offending traffic.

Recommended Web Traffic Protection

Webwasher[™] anti-virus provides in-depth protection against a multitude of blended threats while offering unmatched, lightning speed performance through its innovative anti-virus PreScan[™] technology. Webwasher anti-virus is the only solution in the market with anti-virus Multi-Scan[™], offering up to three anti-virus engines to scan Web and e-mail traffic to fulfill the most rigorous security requirements.

Recommended Identity and Access Management Protection

SafeWord[®] SecureWire[™] is a powerful identity and access management (IAM) appliance that secures access, enforces policy, and provides complete and customizable reporting for your entire network. SecureWire provides lightning fast, ultra secure access to every application and data resource in your network, hosting

every access method for users both inside and outside the enterprise—and it does so with identity, security, and simplicity in mind. As a vital component of your complete identity and access management strategy, SecureWire revolutionizes the way you provide access to employees, business partners, and extranet users.

Recommended Encryption Protection

Encrypting data is an important part of the PCI standard, ensuring that information sent is protected from unauthorized access. Aurora works with two partners to ensure a seamless encryption protocol.

PGP Whole Disk, PGP Command Line and PGP Encryption for Blackberry provides a comprehensive suite of encryption services from the laptop to remote users and portable devices.

SecurePATH combines unbreakable PGP protection with a simple, client software-free solution for sending files to employees, vendors and other sources.