Imperva Simplifies PCI DSS 1.2 Compliance and Secures Cardholder Data

PCI Standard Bolsters Cardholder Data Security

To avert the financially disastrous consequences of a credit card breach, the five major credit card brands established the Payment Card Industry Data Security Standard (PCI DSS). The PCI standard consists of twelve high-level requirements that define the policies, tools, and controls needed to protect cardholder data. While some of these requirements are relatively straightforward and easy to implement, the Web application and database security requirements present significant technical and business challenges.

To secure Web application data, the PCI DSS mandates that merchants must protect public-facing Web applications by either installing a Web Application Firewall or reviewing their applications after any changes. The PCI standard also requires that merchants track and monitor all access to cardholder data. These audit trails must be tamper resistant and they must include the individual user that accessed the data. For organizations that use multi-tier applications with connection pooling, it can difficult to identify end users through native database logs alone. An auditing solution must be able to correctly ascertain individual user IDs even in these types of environments.

To meet security and PCI DSS compliance requirements, organizations must:

- Determine which data assets are in scope of PCI DSS
- Protect sensitive Web applications
- Protect and audit access to sensitive data
- Document and demonstrate PCI compliance to auditors

Many merchants and payment processors may consider PCI compliance as a cumbersome hurdle put in place by the top five payment brands. Such organizations may seek to implement the minimum controls and technologies to pass their PCI audit, while neglecting the underlying goal of the PCI standard – protecting cardholder data. While PCI compliance enables organizations to process credit card data and offers safe harbor protection against fines from payment card companies, it does not insulate merchants from the devastating effects of a credit card breach. Several recent security breaches at PCI-certified companies demonstrate that passing a PCI audit does not eliminate the risk of a security compromise.

The consequences of a credit card data breach can be staggering, averaging $202 per compromised record[1], due to customer loss, brand damage, lawsuits, and government fines. Merchants and processors should assess their sensitive assets, technologies, and procedures, determine risks, and undertake security best practices to prevent a costly cardholder data breach.

[1] "U.S. Cost of a Data Breach Study", Ponemon Institute, 2009

CASE STUDY

Leading European Online Retailer Turns to Imperva for PCI and Application Security

One of the largest e-commerce sites in Great Britain, attracting as many as 50,000 unique visitors each day, recognized that it needed to protect its customers and meet PCI DSS customers.

The online retailer sells a variety of products, including electronics, home appliances, sports equipment, and apparel through its online payment portal. Every day, the company received thousands of online attacks such as SQL injection, command injection, and parameter tampering. Although the retailer followed secure coding best practices, a recent application penetration test has discovered a number of critical vulnerabilities. After analyzing different options, the IT security team determined that a Web Application Firewall would provide ironclad, and immediate, defense for the company's vulnerable Web applications.

In addition, as a payment card processing merchant, the online retailer was subject to the Payment Card Industry Data Security Standard (PCI DSS). Meeting PCI section 6.6 was a key objective for the retailer. While the organization already performed regular application scans, the IT security team was reticent to rely on an outside security specialist to validate that all assessed vulnerabilities had been remediated. Therefore, the proposed solution not only needed to prevent application attacks, but also address PCI DSS requirements. The Web Application Firewall needed to:

- Satisfy PCI DSS section #6.6
- Protect the E-commerce site from attack
- Offer transparent deployment
- Provide low management overhead

Solution

After evaluating several Web Application Firewalls, the online retailer chose Imperva SecureSphere. SecureSphere required no changes to the organization's existing applications or network settings because it could be deployed transparently as a layer 2 bridge. Besides meeting PCI requirement 6.6, SecureSphere accurately identified attacks and offered virtual patching for vulnerabilities discovered in the company's E-commerce site.

Benefits

The Imperva SecureSphere Web Application Firewall enabled the online retailer to protect sensitive data, including credit card numbers, customer names, and addresses. SecureSphere also enabled the company to meet the application security requirements in the PCI DSS. With its Dynamic Profiling technology, SecureSphere adapts to application changes without manual intervention. According to the Vice President of IT, "SecureSphere learned the application by itself, saving us time and administrative costs."

Imperva SecureSphere for PCI Compliance

The market-leading Imperva SecureSphere Web and Database Security Solutions help organizations meet the most challenging PCI requirements, including sections 6.6, 10 and compensating controls for section 3.4. SecureSphere not only addresses the exacting requirements set forth in the PCI DSS document and in PCI Information Supplements, it goes above and beyond PCI requirements by discovering credit card data in network data stores, assessing security vulnerabilities in sensitive databases, and managing risk.

Overall, SecureSphere provides partial or complete coverage for eight of the twelve high-level PCI DSS requirements. More importantly, Imperva SecureSphere's highly accurate and aware Web and Database Security Solutions drastically reduce the risk of sensitive data breach.

Determine Assets in Scope of PCI DSS

In order to protect cardholder data, organizations must first locate this data. SecureSphere Database Security Solutions simplify this process by scanning a network IP range and detecting all existing databases. Then SecureSphere searches each database for sensitive information such as credit card numbers. Once databases have been discovered, SecureSphere can assess databases for vulnerabilities and configuration flaws. SecureSphere's data discovery and classification enables organizations to determine which assets are in scope of PCI DSS enforcement. Furthermore, its ability to detect prohibited CVV track data in databases helps address PCI requirement 3.2.2.

PCI #6.6 – Protect Public-Facing Web Applications

The SecureSphere Web Application Firewall is the preeminent choice for meeting the application security requirements in PCI section 6.6. The PCI DSS states that public-facing Web applications must be protected by attack by either installing a Web Application Firewall or by Web application reviews at least annually and after any changes by an organization that specializes in application security. A Web Application Firewall is the ideal solution to meet PCI DSS section 6.6 because it offers lower total cost of ownership, minimizes disruption to application development schedules, and it continuously protects Web applications.

As the leading Web Application Firewall, SecureSphere safeguards sensitive applications from attack and abuse. The ICSA-certified Web Application Firewall meets all of the requirements specified in *Information Supplement: Application Reviews and Web Application Firewalls Clarified*, including detecting the OWASP Top Ten list of application threats, preventing data leakage, enforcing both positive and negative security models, protecting HTML, DHTML, CSS, SOAP, and XML content, and inspecting encrypted SSL (HTTPS) communications.

Automated Security

The SecureSphere Dynamic Profiling technology automatically learns application structure, elements, and expected usage, eliminating manual configuration and tuning. The Imperva Application Defense Center (ADC) constantly researches the latest threats, providing SecureSphere accurate and up-to-date application attack signatures.

Transparent Deployment

Deployed as a transparent layer 2 bridge, a proxy or a non-inline monitor, organizations can roll out SecureSphere without changing their applications or network. Imperva's Transparent Inspection technology delivers multi-gigabit throughput and supports flexible high availability options that meet the most demanding data center requirements.

With SecureSphere's Database Vulnerability Dashboard and graphical Web and database security reports, you can quickly monitor, review and remediate security threats.

PCI #10 – Track All Access to Cardholder Data

Although seemingly straightforward, section 10 in the PCI DSS is one of the most difficult requirements to achieve. According to Verisign1, 71% of assessed organizations failed this requirement. Section 10 explicitly spells out twenty five requirements and sub-requirements for tracking cardholder data, including auditing individual access to cardholder data, identifying individual users, type of event, and time, and protecting audit files from unauthorized modifications.

SecureSphere Database Security Solutions meets all of the auditing requirements specified in section 10 without degrading database performance or requiring network changes. SecureSphere offers deep activity monitoring capabilities, auditing by user data accessed, SQL operation, SQL query (DML, DDL, DCL). SecureSphere can also identify changes to database values. Row-level change auditing streamlines fraud prevention, forensics and regulatory compliance. Because SecureSphere is deployed as a network appliance, it can be managed by individuals outside of the database administration staff, enabling separation of duties. A lightweight agent tracks local DBA activity.

PCI #3.4 – Render Primary Account Number (PAN) Unreadable; Compensating Controls

Like section 10, section 3.4 is one of the most challenging PCI DSS requirements. However, for some organizations, it is not possible to achieve the objectives due to a technical or business constraint. In such cases, organizations can turn to the compensating controls defined in Appendix B of the PCI DSS.

SecureSphere Database Security Solutions address the compensating controls listed in Appendix B by meeting the intent and rigor of the original requirement, providing a similar level of defense, and being "above and beyond" other PCI DSS requirements. SecureSphere provides network segmentation, IP and MAC address filtering, separation of duties, and authentication outside of standard local directory services. In addition, SecureSphere blocks database attacks and malicious activity. Note that all compensating controls should be reviewed and validated by the assessor conducting the PCI DSS review.

CASE STUDY

Hotel Chain Secures Sensitive Data and Achieves PCI

A leading economy lodging company had a wealth of Internet security products. However, despite its multiple layers of defense, which consisted of perimeter and departmental firewalls and intrusion prevention systems (IPSs), the company's sensitive online reservation system was unprotected. Neither its firewalls nor IPS systems could inspect SSL traffic or monitor sessions or cookies. With over half of all reservations performed online, the company's Web applications processed hundreds of millions of dollars in credit card transactions. Therefore, protecting these applications from attack and identity theft quickly became a paramount concern.

On top of these security requirements, the company faced an upcoming PCI compliance deadline. The hotel company needed a product that would:

- Prevent application attacks and identity theft
- Offer drop-in deployment with no changes to existing applications
- Support seamless failover
- Address PCI's application security requirements

Solution

After testing several proxy-based application firewalls, the company chose the SecureSphere Web Application Firewall because it:

- Supported transparent bridge deployment
- Did not require any changes to applications
- Offered easy, automated management
- Supported line speed performance and sub-millisecond latency

In addition, the company selected SecureSphere because it not only protected Web applications, but it could also secure backend databases. This database auditing capability allowed the firm to meet the data monitoring requirements specified in section 10 of the PCI standard. It also provided detailed audit logs for forensics purposes.

The lodging company deployed SecureSphere in front of all its public-facing Web applications and application databases, including Oracle, SQL Server, and Informix. Rolled out in just half a day, SecureSphere automatically learned application structure and acceptable usage.

Benefits

Imperva SecureSphere gateways enable the hotel chain to protect sensitive data from both external attacks and internal abuse. SecureSphere enabled the company to meet multiple PCI DSS requirements and it also automatically generated PCI and SOX compliance reports every month, documenting compliance to auditors.

With Imperva, the company achieved its initial goal of securing Web applications from session attacks without impacting applications or the network. SecureSphere provided both Web application and database security and compliance capabilities, enabling the company's IT security team to rest easy at night.

Imperva SecureSphere Helps Meet 8 of the 12 PCI DSS Requirements

Imperva SecureSphere Web and Database Security Solutions help organizations meet 8 of the 12 high level requirements in the PCI standard including several of the most challenging security requirements.

	PCI 1.2 Requirements	Imperva
1	Install and maintain a firewall configuration to protect cardholder data	✓
2	Do not use default system passwords and other security parameters	✓
3	Protect stored cardholder data	✓
4	Encrypt transmission of cardholder data across open, public networks	
5	Use and regularly update anti-virus software	
6	Develop and maintain secure systems and applications	✓
7	Restrict access to cardholder data by business need-to-know	✓
8	Assign a unique ID to each person with computer access	✓
9	Restrict physical access to cardholder data	
10	Track & monitor all access to network resources and cardholder data	✓
11	Regularly test security systems and processes	✓
12	Maintain a policy that addresses information security	

Demonstrating PCI DSS Compliance to Auditors

Imperva SecureSphere Web and Database Security Solutions provide the foundation for organizations to protect their sensitive assets and achieve PCI compliance. SecureSphere's graphical reporting engine helps demonstrate PCI compliance to auditors. Out-of-the-box PCI reports document the database assets that contain cardholder data, illustrate security vulnerabilities in these assets, track all access to cardholder data, and present application and database attacks to sensitive data. With summary and drilldown reports and multiple distribution formats, SecureSphere offers a turnkey framework for PCI compliance reporting. SecureSphere comprehensively addresses organizations' security and regulatory requirements by protecting sensitive applications and data, auditing access to sensitive data, and addressing PCI DSS compliance requirements.

"Deploying a Web Application Firewall was the most efficient and cost effective solution for us to comply with the PCI Data Security Standard.

Jean-Pierre Zaiter, CIO, Intuition Systems

"SecureSphere enables us to inspect every cookie, every parameter, every URL, and every form field to protect our customers' applications and data against layer 7 vulnerabilities. Just as important, SecureSphere helps us comply with the strict PCI DSS standards."

David Denara, CIO, Millennium Communications

Imperva
Americas Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel-Aviv 67010
Israel
Tel: +972-3-6840100
Fax: +972-3-6840200

Toll Free (U.S. only): +1-866-926-4678
www.imperva.com