IMPERVA®

SOLUTION BRIEF

Imperva Simplifies and Automates PCI DSS Compliance

Imperva Simplifies and Automates PCI DSS Compliance

SecureSphere drastically reduces both the risk and the scope of a sensitive data breach with its best-of-breed Web Application, Database and File Security Solutions.

PCI DSS Bolsters Cardholder Security

Backed by the five major payment brands, the Payment Card Industry Data Security Standard (PCI DSS) establishes the policies, tools, and controls needed to protect cardholder data. With twelve high-level requirements and over two hundred sub-requirements, PCI compliance can be difficult for many organizations to achieve.

With such stringent demands, some merchants focus solely on passing their next PCI audit, and neglect the underlying goal of the PCI standard: protecting cardholder data. Unfortunately, as recent high profile breaches have demonstrated, PCI compliance will not insulate merchants from the devastating effects of a credit card breach. Organizations should therefore develop a holistic security strategy that satisfies the PCI DSS while maximizing cardholder security.

PCI Requirements for Web, Database and File Security

To protect cardholder data transmitted through Web applications, the PCI standard mandates that merchants must either install a Web Application Firewall or review their web applications after any changes, and then fix vulnerabilities. The PCI standard also requires that merchants track and monitor all access to cardholder data. In addition, organizations must limit user access rights to business need-to-know and ensure file integrity.

In summary, to address Web, Database and File security objectives set forth in the PCI standard, organizations must:

- Determine which data assets are in scope of PCI
- Safeguard sensitive Web applications
- Audit and protect access to sensitive data
- Limit user access rights to business need-to-know
- Demonstrate PCI compliance to auditors

PCI DSS Requirements		Imperva Solutions for PC DSS
6.1	Establish a process to identify security vulnerabilities	SecureSphere Database Assessment
6.4.3	Production data are not used in test and development	Camouflage Data Masking
6.6	Protect public-facing Web applications	SecureSphere Web Application Firewall
7	Restrict access to cardholder data to business need to know	User Rights Management for Databases and Files
8.5	Identify and disable dormant user accounts	User Rights Management for Databases and Files
10	Monitor all access to cardholder data	SecureSphere Database and File Activity Monitoring
11.5	Deploy file integrity monitoring software	SecureSphere File Activity Monitoring

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

One of the largest online electronics retailers in Great Britain, attracting as many as 50,000 visitors each day, needed to protect its customers and address PCI compliance.

Every day, the company received thousands of online attacks such as SQL injection and parameter tampering. Although the retailer followed secure coding best practices, a recent penetration test had discovered a number of critical Web vulnerabilities. After analyzing various options, the IT security team determined that a Web Application Firewall would provide an immediate and continuous defense for the company's vulnerable Web applications.

In addition, as a payment processing merchant, the online retailer was subject to the PCI DSS. Meeting PCI section 6.6 was a key objective for the retailer. While the retailer already performed regular application scans, the IT security team was reluctant to rely on an outside security specialist to validate that all assessed vulnerabilities had been remediated. Therefore, the proposed solution not only had to prevent application attacks, but also address PCI compliance.

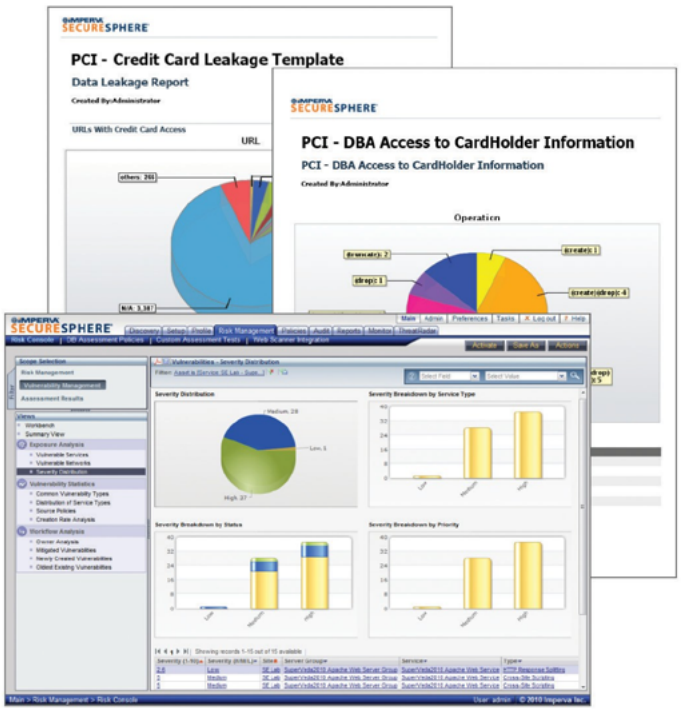
The Web Application Firewall needed to:

- Satisfy PCI section #6.6
- Protect the E-commerce site from attack
- Mitigate application vulnerabilities
- Support transparent deployment

Imperva SecureSphere Is the Ideal Choice for Challenging PCI Requirements

The Imperva SecureSphere Data Security Suite addresses 8 of the 12 high level PCI requirements including 6.6, 7, 8.5, 10, and 11.5. Organizations trust Imperva for data security and compliance because Imperva offers:

- Complete Data Protection for Web Applications, Databases and Files – SecureSphere protects data where it is stored – in databases and files – and how it is accessed – through applications – and addresses the full data security and compliance life cycle.
- Automated Security – Imperva's patented Dynamic Profiling capability automatically learns application and database usage without manual intervention. The unique ThreatRadar service further streamlines security by automatically identifying attacks from known, malicious sources.
- Full Visibility with Separation of Duties – SecureSphere monitors and audits all database and file activity, including privileged user access. Interactive audit analytics enable users to analyze, correlate and view activity from any angle.
- Streamlined User Rights Management – SecureSphere simplifies the process of reviewing and managing user rights across distributed file servers and databases. SecureSphere aggregates access rights, identifies dormant accounts and highlights excessive privileges.
- Zero-Impact Deployment – SecureSphere offers multiple, transparent deployment options for easy integration into any environment with no impact on existing applications, databases or files.



The SecureSphere web, database, and file security reports allow users to quickly monitor, review, and remediate security threats.

Solution

After evaluating several Web Application Firewalls, the online retailer chose Imperva. Imperva SecureSphere:

- Addressed PCI requirement 6.6
- Accurately detected and stopped attacks
- Virtually patched vulnerabilities discovered by the company's vulnerability scanner
- Offered transparent deployment with no changes to existing applications or network

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 Solutions for Specific PCI Requirements

Imperva security solutions offers continuous and automated compliance for web applications, databases and files. Imperva security solutions not only addresses the exacting requirements set forth in the PCI DSS, it goes above and beyond PCI requirements by discovering credit card data in network data stores, assessing security vulnerabilities in sensitive databases, and documenting compliance with out-of-the-box PCI reports.

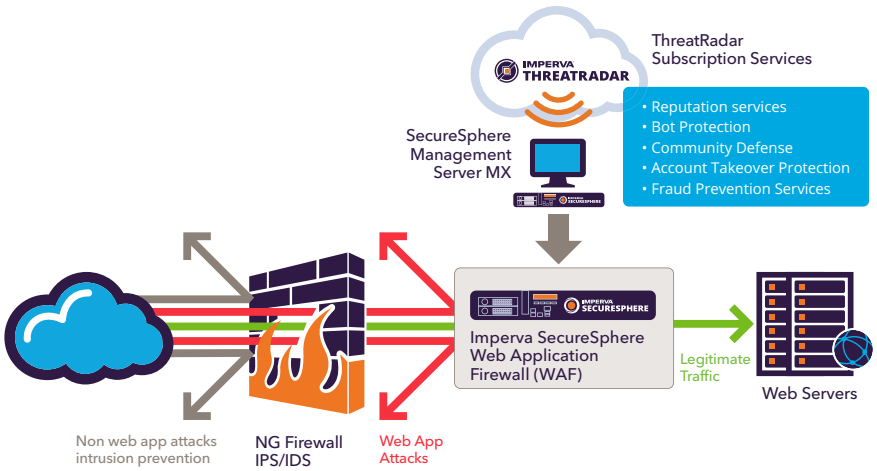
PCI #3.2.2 – Determine Assets that are in Scope for PCI

One of the first steps of any PCI compliance strategy is to locate all cardholder data in the network. SecureSphere simplifies this process by discovering all databases on the network. SecureSphere then searches each database for sensitive records such as credit card numbers and assesses databases for thousands of vulnerabilities. SecureSphere's data discovery and classification enables organizations to determine which assets are in scope of PCI 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 from attack by either installing a Web Application Firewall or by having an organization that specializes in application security perform web application code reviews at least annually and after any changes. A Web Application Firewall is the ideal solution to meet PCI section 6.6 because it offers low total cost of ownership, minimizes disruption to application development schedules, and continuously protects web applications.

As the leading Web Application Firewall, SecureSphere safeguards sensitive applications from cyber attacks which exploit application vulnerabilities and business logic abuse. SecureSphere is ICSA-certified and meets the requirements specified in the PCI DSS Information Supplement, including preventing OWASP top-10 application threats, malicious IP/Bot clients, account takeover attempts, mobile attacks, and app. level DDoS attacks. It enforces both positive and negative security models to detect web app. attacks.



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 network firewalls and intrusion prevention systems (IPSs), the company's sensitive online reservation system was largely 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 was a paramount concern.

On top of these security requirements, the company faced an upcoming PCI compliance deadline. The hotel chain 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

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 Verisign, 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 and File Security Solutions meet all of the auditing requirements specified in section 10 without degrading performance or requiring network changes.

SecureSphere offers deep activity monitoring capabilities, auditing by user, data accessed and, in the case of databases, by SQL operation. SecureSphere also identifies changes to files and databases, providing row-level change auditing for databases which streamlines fraud prevention, forensics and regulatory compliance. Because SecureSphere is deployed as a network appliance, it can be managed by individuals outside of the file and database administration staff, enabling separation of duties. A lightweight agent is available to track local activity.

PCI #7 – Limit Cardholder Access by Need-to-Know

Eliminating excessive user rights reduces the risk of a data breach. According to PCI requirement 7, organizations should limit user access to the minimum necessary to perform job functions. SecureSphere User Rights Management (URM) for Databases and Files streamlines the aggregation, management, and auditing of user access rights across all databases and file servers. URM also helps identify excessive user rights and documents user rights to auditors.

PCI #6.1 - Establish a Process to Identify Security Vulnerabilities

Attackers use security vulnerabilities to gain unauthorized access to databases and other systems. To reduce the risk that vulnerabilities pose, PCI 6.1 requires organizations scan and evaluate vulnerabilities on an ongoing basis and assign risk ranking to those vulnerabilities. SecureSphere Database Assessment identifies database vulnerabilities and misconfigurations. Database Assessment helps prioritize mitigation by calculating the risk based on data sensitivity and the severity of vulnerabilities.

SecureSphere offers deep activity monitoring capabilities, auditing by user, data accessed and, in the case of databases, by SQL operation.

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 could also protect 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.

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 enabled the hotel chain to protect sensitive data from both external attacks and internal abuse. SecureSphere also satisfied multiple PCI requirements and it automatically generated PCI and SOX reports every month, demonstrating compliance to auditors.

With Imperva, the company achieved its goal of securing Web applications from attack without impacting existing applications or network devices. SecureSphere delivered end- to-end Web application and database security, enabling the company's IT security team to rest easy at night.

PCI #6.4.3 – Production Data are Not Used for Testing or Development

Test and development environments tend to be less secure because of their constantly changing nature. As such, they are more easily compromised than production environments. Use of production data, including sensitive cardholder data, in test and development environments gives external attackers and malicious insiders the opportunity to gain unauthorized access to production data. Camouflage Data Masking reduces the risk of data theft and unauthorized access by replacing sensitive data with realistic fictional data.

PCI #8.1.4 – Disable Dormant User Accounts

PCI requirement 8.1.4 mandates that user accounts be disabled after 90 days of inactivity. In addition, access privileges of terminated users should be revoked. SecureSphere URM for Databases and Files helps organizations aggregate and report on user activity, identify dormant accounts, and generate reports for PCI compliance.

PCI #11.5 – Deploy File Integrity Monitoring Tools

As part of PCI requirement 11, organizations must monitor critical system files, configuration files and content files at least weekly for unauthorized modification. SecureSphere File Security Solutions monitor all access activity and can detect changes to critical systems, configuration, and content.

Camouflage Data Masking reduces the risk of data theft and unauthorized access by replacing sensitive data with realistic fictional data.

Demonstrating PCI Compliance to Auditors

With high-level and drilldown reports and multiple distribution formats, SecureSphere offers a turnkey framework for PCI compliance reporting.

Imperva SecureSphere's graphical reporting engine enables organizations to document PCI compliance to auditors. With high-level and drilldown reports and multiple distribution formats, SecureSphere offers a turnkey framework for PCI compliance reporting. SecureSphere addresses organizations' security and regulatory requirements by monitoring and protecting organizations' most sensitive assets: Web applications, databases, and files.