Imperva Delivers Safe, Secure Online Shopping to Retailers

E-commerce Sites Are a Lucrative Target for Hackers

Online retail sales continue to escalate, reaching a projected $267.8 billion in 2010, according to Forrester Research[1]. With so much money being transferred online, criminals are increasingly targeting e-commerce sites. Hackers have developed a wide array of techniques to maliciously alter Web sites, impersonate legitimate users, and steal credit card and customer information.

New automation tools, smarter search engines, and widespread communication of vulnerabilities have increased the threats to online retailers. To illustrate this growing threat, in May 2008, hackers used automated scripts and search engines to conduct a massive wave of SQL injection attacks that affected over five hundred thousand Web sites[2].

Enforcing Security through Regulation

The effects of an application attack can be devastating, with consequences ranging from negative publicity and customer loss to lawsuits and fines. With so much at stake, the five major credit card brands joined together to create the Payment Card Industry Data Security Standard (PCI DSS).

To secure 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 states that merchants must 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 retailers 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 compliance requirements, online retailers must:

- **Protect sensitive Web applications**
- **Protect and audit access to sensitive data**
- **Satisfy compliance requirements**

As new regulations emerge, online retailers must adapt to meet these new requirements. The best way to prepare for an evolving regulatory landscape is to follow governance and security best practices. Retail businessess must protect sensitive data where it is stored, in databases, and where it is accessed, through applications, in order to prevent data compromise. An ideal security solution for online retailers must provide a framework to address current and future compliance requirements and it must evolve to prevent the latest application data security threats.

[1] "U.S. E-commerce Forecast: 2008 to 2012", Forrester, January, 2008
[2] "Massive Attack: Half A Million Microsoft Sites Hit With SQL Injection", Wired Blog, 2008

CASE STUDY

Consumer Electronics Giant Protects Applications and Databases without Impacting Performance

A technology and entertainment retailer generating over $40 billion annually had built dozens of Web applications for customers, partners, and employees. After scanning these applications for vulnerabilities, the security team found dozens of security issues in multiple applications, including the company's main ecommerce site. The security team decided to roll out Web application firewalls to protect all of the company's public-facing Web applications. The retailer consistently ranks as one of the top five most visited sites on Black Friday, the day after Thanksgiving. So the Web application firewall had to support ultra high performance. The security team sought a solution that would:

- Protect all public-facing Web applications
- Scale to multi-Gigabit throughput
- Offer transparent operations with sub-millisecond latency and zero network impact

A separate group within the electronics retailer determined it needed a dedicated database monitoring gateway to track and audit all database activity. This group sought a solution that would audit their SAP systems, automate SOX compliance, and not impact their existing infrastructure. The IT compliance team needed a solution that would:

- Audit database activity
- Identify individual end users accessing data
- Address multiple compliance regulations

Solution

Both the Web application and database security projects were run independently and each group insisted on an autonomous selection process. After two separate bake-offs, both teams selected Imperva SecureSphere because it delivered:

- Gigabit performance
- Ease of deployment
- Scalable management
- Application to database user tracking

Since both groups chose SecureSphere, the company was able to consolidate Web and database security on a single appliance. Not only did this lower the overall cost, it also allowed the retailer to track Web application users to the backend database through a feature, called Universal User Tracking.

Benefits

Since deploying SecureSphere, the company's security staff actively monitors the dozens of attacks blocked by SecureSphere every day. A new HTTP response capture allows the security team to notify developers of application issues, at least for custom applications. By choosing Imperva SecureSphere, the IT compliance group has reduced the resources dedicated to SOX and PCI compliance by over 50% and has improved user accountability and separation of duties initiatives.

Imperva SecureSphere for Retail and E-Commerce

As the market leader in data security, more retail organizations trust Imperva to monitor and protect their critical assets than any other vendor. Imperva SecureSphere provides complete end-to-end security and compliance, protecting sensitive transactions from the end user through the business application to the backend database.

SecureSphere Web and Database Security Solutions address retailers' key regulatory needs: protecting sensitive applications and data, auditing access to sensitive data, and addressing compliance requirements.

Protect Sensitive Web Applications

The SecureSphere Web Application Firewall safeguards Web applications, including public-facing online stores, partner sites, and internal business applications, from attack and abuse. The ICSA-certified Web application firewall leverages multiple defenses to accurately block SQL injection, XSS, session hijacking, and many other application attacks.

Automated Security

The SecureSphere Web Application Firewall automatically learns application structure, elements, and expected usage. In addition to Dynamically profiling applications, SecureSphere detects HTTP protocol violations, network and system attacks, and Web services (XML) exploits. The Imperva Application Defense Center (ADC) constantly researches the latest threats, providing SecureSphere accurate and up-to-date application attack signatures. SecureSphere combines these defense techniques together using Correlated Attack Validation to correctly identify attacks without blocking legitimate traffic.

Transparent Deployment

Deployed transparently as a layer 2 bridge, a proxy or a non-inline monitor, organizations can roll out SecureSphere without changing their existing applications or network. SecureSphere's Transparent Inspection technology inspects HTTP and HTTPS (SSL) traffic, delivers multi-gigabit throughput and supports flexible high availability options that meet the most demanding data center requirements. Fail-open interfaces offer cost-effective, single-gateway availability. Because of its accurate security, automated operations, and transparent deployment options, SecureSphere is the preeminent Web application security solution.

Protect and Audit Access to Sensitive Data

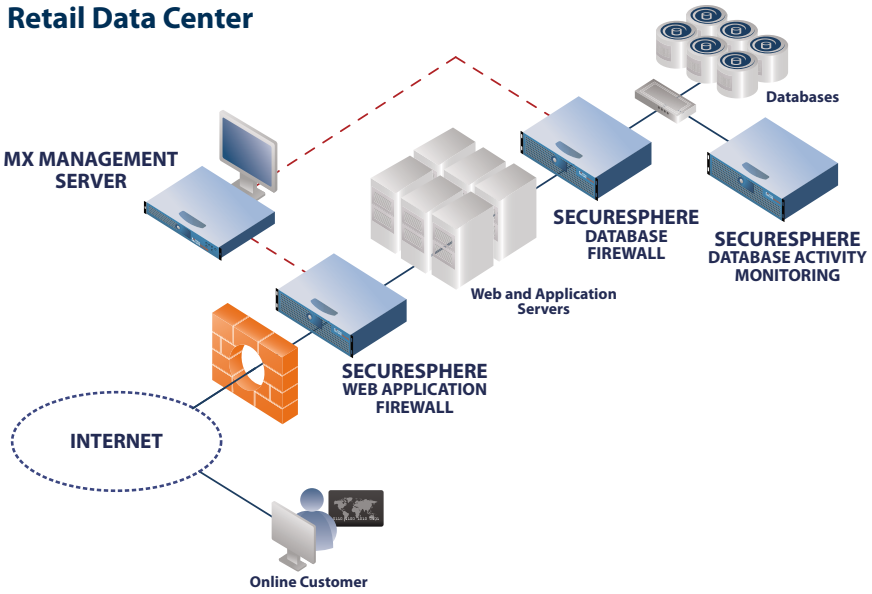
Discovery and Assessment

To protect sensitive data, businesses must first locate sensitive 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 they have been discovered, SecureSphere can assess databases for vulnerabilities and configuration flaws.

Database Monitoring and Controls

SecureSphere Database Security Solutions monitor all access to databases and can optionally enforce database access controls. SecureSphere recognizes known database attacks, SQL protocol violations, and unusual database activity. SecureSphere's Dynamic Profiling technology automatically creates and maintains baseline profiles of each user's activity. Compliance auditors can compare usage to job functions or regulatory requirements.

Retail Data Center



Audit Database Activity

SecureSphere collects a rich set of audit data for compliance and forensics purposes. With its deep activity monitoring capabilities, SecureSphere can audit by user, data accessed, SQL operation, and 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 audits activity without impacting database performance and can be managed by individuals outside of the database administration staff, enabling separation of duties. A lightweight agent tracks local DBA activity.

Database audit trails must include the individual user that accessed or changed data. For many multi-tier applications, it can be impossible to identify individual end users from database transactions alone. Imperva is the only database auditing vendor that has developed multiple methods to accurately identify end users, even in connection pooling environments. Imperva's innovative Universal User Tracking feature requires no changes to existing databases or applications.

Satisfy Compliance Requirements

Any retail organization that processes, transfers, or stores credit card data must comply with PCI DSS. SecureSphere helps retailers meet several of the most challenging PCI requirements. First, the SecureSphere Web Security Solutions address PCI section 6.6, securing public-facing Web applications. Second, SecureSphere Database Security Solutions address all of the database monitoring and auditing requirements in section 10 by auditing all access to cardholder data. Third, the database discovery, assessment, security controls, and network segmentation may be used as a compensating control for some of the more exacting requirements, such as section 3.4, rendering cardholder data unreadable. Overall, SecureSphere provides partial or complete coverage for eight of the twelve high-level PCI DSS requirements.

SecureSphere's graphical reporting engine helps document compliance with regulations such as PCI DSS, SOX, GLB, and BASEL II. Over 250 out-of-the-box reports accelerate regulatory audit processes. With summary and drilldown reports and multiple distribution formats, SecureSphere offers a turnkey framework for compliance reporting.

CASE STUDY

Grocer Secures Application Data and Achieves PCI

In early 2008, a Fortune 100 food and drug retailer faced seemingly impossible requirements. The retailer's IT staff needed to lock down the company's online store and prevent online identity theft. Unfortunately, the retailer's intrusion prevention system (IPS) could not inspect SSL traffic and it did not monitor sessions or cookies. The company also had many legacy applications and databases that could not be changed. The network operations team did not want to introduce a new point of failure into the network.

On top of these security requirements, the company faced a looming PCI compliance deadline. The Fortune 100 grocer needed a product that would:

- Prevent application attacks and identity theft
- Offer drop-in deployment with no changes to existing applications
- Support seamless failover
- Satisfy PCI DSS requirement 6.6

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
- Included fail-open network interfaces; in the event of a failure, the interface cards would automatically bridge the connection

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 food retailer deployed SecureSphere in front of all its public-facing Web applications and application databases. Because of its demanding network requirements, the company purchased 8 SecureSphere G4 Web and database appliances and 2 MX management servers.

Benefits

Imperva SecureSphere gateways enable the grocer 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, impressing the company's external auditors.

With Imperva, the IT staff 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, making the solution a runaway success for the organization.

SecureSphere Web Security Solutions

The market-leading SecureSphere Web Application Firewall is designed from the ground up to protect Web applications from all types of security threats. SecureSphere leverages multiple security defenses simultaneously – including Dynamic Profiling, HTTP protocol validation, up-to-date attack signatures, correlation, and platform protection – to provide the highest level of protection available. Dynamic Profiling automatically models an application's structure, elements, and expected user behavior, and adapts to changes over time, keeping SecureSphere's defenses up-to-date and accurate. In addition, it offers drop-in deployment, gigabit performance and automated, transparent operations. The SecureSphere Web Application Firewall provides retail organizations with a proven, highly-secure solution that addresses today's security and compliance challenges.

SecureSphere Database Security Solutions

The award-winning Imperva SecureSphere Database Security Solutions deliver comprehensive activity monitoring, real-time protection, and risk management for Oracle, MS-SQL, IBM DB2, Sybase, and Informix databases. Dynamic Profiling technology analyzes database activity and dynamically creates granular database usage profiles and security policies for every user and application accessing the database. Detailed database auditing and pre-defined compliance reports streamline regulatory processes.

SecureSphere is the industry's only complete data security and compliance solution that provides full visibility into data usage by the end-user through the application and into the database. SecureSphere Database Security Solutions, including the Database Firewall, Database Activity Monitoring, and Discovery and Assessment Server, offer full assessment, visibility, and control for mission critical databases. Automatic updates from the security and compliance experts at the Imperva Application Defense Center (ADC) ensure that SecureSphere is always armed with the latest defenses against new threats and the most recent regulatory compliance best practices.

With Imperva, Retailers Can Be Open For Business

The Imperva SecureSphere application and database security products provide the foundation for retail and e-commerce businesses to protect their sensitive assets and achieve regulatory compliance. SecureSphere comprehensively addresses retail organizations' security and regulatory requirements by protecting sensitive applications and data, auditing access to sensitive data, and addressing retailers' compliance requirements.

"We understand the need of top level security for our customers and ourselves. We chose Imperva SecureSphere because we believe they are the very best."

Bob Parsons, CEO and Founder, GoDaddy.com

"SecureSphere allows us to track and document all database users, including database administrators and developers, and trace their actions, without impacting the performance or stability of our Microsoft SQL Server database."

Scott Ficek, Sr. Director of IS, Caribou Coffee

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