Imperva Secures Your Financial Bottom Line

Bank Regulations Yield New Data Security Complexities

Financial institutions must comply with a raft of regulations that govern the integrity, security, and distribution of sensitive data. Regulations such as Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB), California Senate Bill 1386, PCI DSS, BASEL II, and Markets in Financial Instruments Directive (MiFID) require financial firms to implement controls that protect and audit application data.

To meet the aggressive deadlines of these regulations, financial firms have invested heavily in new internal business processes and consulting and auditing services. The cost of compliance has been much higher than expected. According to Gartner, the average mid-size to large financial firm will invest $2 million to comply with these regulations. Because the current level of spending is not sustainable and penalties are substantial, financial organizations are searching for ways to lower the cost of compliance.

Governance Best Practices Start With Good Security

Many banking regulations were enacted to address security risks such as internal abuse, financial data compromise, and fraud. Financial institutions are an easy target for abuse because they transfer and store extraordinarily valuable data: customer information, bank account records, and payment card numbers. With each compromised customer record costing an average of $197, according to the Ponemon Institute, financial firms must protect their sensitive data. Security concerns also rank as a top deterrent of online banking for consumers. So it is imperative for banks to assure their clients that their bank accounts and their identity records are safe.

To meet security and compliance requirements, financial institutions must implement controls that:

- **Protect sensitive data**
- **Audit access to sensitive data**
- **Automate compliance reporting**

As new regulations emerge, financial firms must adapt to meet new compliance requirements. The best way to prepare for an evolving regulatory landscape is to follow governance and security best practices. Financial services organizations should protect sensitive data where it is stored – in databases – and control access to this data from database clients, from business applications and from direct access by DBAs. Furthermore, banks should actively monitor and audit all access to sensitive data. Ultimately, to meet new regulatory requirements, financial firms must be able to demonstrate to auditors that all necessary controls are in place.

CASE STUDY

Payment Processor Locks Down Application Data While Achieving PCI Compliance

A company that processed over 28 million electronic payments annually had developed a suite of online payment applications. Over ten thousand e-commerce sites rely on this company's applications to process their customers' credit card transactions.

Every day, the payment processor received tens of thousands of online attacks – SQL injection, command injection, and cookie poisoning were constant threats. Although the company followed secure coding best practices, the company's security team wanted to shore up its overall application security stance.

In addition, as a level 1 payment processor, the company was subject to the Payment Card Industry Data Security Standard (PCI DSS). Its first objective was to meet the application security requirement defined in section 6.6. After evaluating the alternatives, the security team determined that code reviews and vulnerability assessments would disrupt their application developers; instead, the security team opted for an application firewall solution. The company set the following criteria:

- Address PCI DSS #6.6
- Provide ironclad application security
- Support transparent operations, no application impact
- Offer easy installation and management

Solution

The company selected SecureSphere because it not only protected Web applications, but it could also protect backend databases. This capability allowed the firm to meet the data monitoring requirements specified in section 10 of the PCI standard. SecureSphere also tracked end users from external Web applications to the backend database. This feature, called Universal User Tracking, resolved one of the company's top compliance weaknesses: identifying the individual end users that accessed sensitive databases through multi-tier applications.

During the evaluation, the security team discovered that SecureSphere dynamically learned the structure and usage of the company's Web applications; it was also painless to set up and configure. Once installed, SecureSphere immediately began identifying real attacks on their Web applications. Moreover, the company was impressed by Imperva's knowledgeable sales and support staff.

Benefits

Imperva's SecureSphere gateways enable the payment processor to protect sensitive data from both external hackers and internal abuse. SecureSphere also enabled the company to meet multiple PCI DSS requirements – the company easily passed their next PCI audit by using SecureSphere.

Imperva SecureSphere for Financial Institutions

As the market leader in data security, more financial organizations trust Imperva to audit, 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.

Web and Database Security Solutions address banks' key regulatory needs: protecting sensitive data, auditing access to sensitive data, and automating compliance reporting. With Imperva SecureSphere, banks are well equipped to meet current and future regulatory requirements.

Protect Sensitive Data

Discovery and Assessment

Databases house companies' sensitive information, including customer records, bank account data and credit card numbers. To protect sensitive data, businesses must first locate it. SecureSphere Database Security Solutions simplify this process by discovering databases and sensitive information. SecureSphere scans a network IP range to detect all existing databases. Then SecureSphere searches each database for sensitive information such as social security numbers, credit card numbers and national ID numbers.

Once the sensitive databases have been identified, SecureSphere can assess the databases for vulnerabilities and configuration flaws. SecureSphere's behavior assessment analyzes database user activity and identifies bad business practices such as shared user accounts and execution of default stored procedures by standard users.

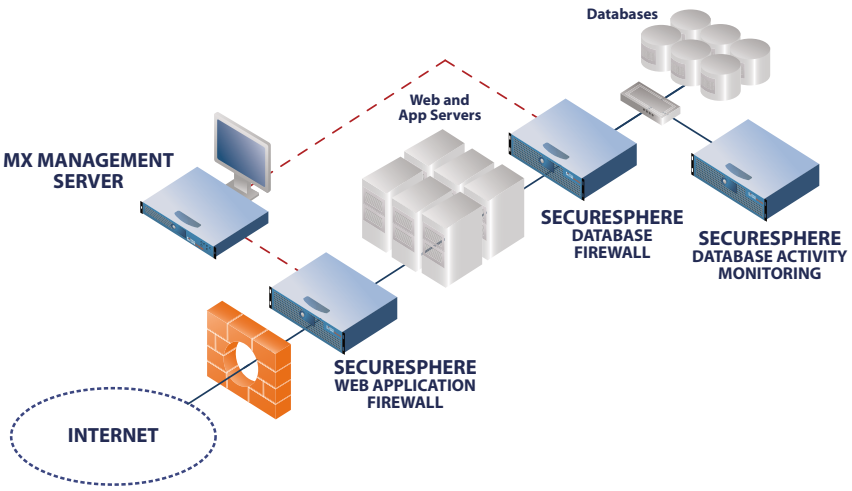
Database Monitoring and Controls

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.

Web Application Security

The SecureSphere Web Application Firewall safeguards Web applications, including online banking and brokerage, online payment, 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.

The SecureSphere Web Application Firewall automatically learns application structure, elements, and expected usage. Dynamic Profiling, in conjunction with SecureSphere's application attack knowledge, correctly identifies application exploits without blocking legitimate traffic. Deployed transparently with no changes to existing applications or network, SecureSphere can protect exposed Web applications from online threats.



Audit Access to Sensitive Data

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 (DML, DDL, DCL), SQL query, and context (source application, time, IP).

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.

SecureSphere can automatically identify and alert financial institutions to suspicious changes to database values. Row-level change auditing streamlines fraud prevention, forensics and regulatory compliance.

For many multi-tier applications, it can be impossible to identify individual end users by analyzing database transactions alone. Imperva has developed several methods to accurately identify end users, even in connection pooling environments. Imperva's Universal User Tracking requires no changes to existing databases or applications.

Automate Compliance Reporting

Many financial firms must invest inordinate amounts of time and resources manually extracting audit data and preparing compliance reports. SecureSphere's reporting framework automates compliance reporting, cutting the cost and effort of manual reporting processes. In addition, SecureSphere's automated framework decreases the number of compliance issues cited by auditors and substantially reduces the risk of failing a regulatory audit.

SecureSphere's graphical reporting engine helps document compliance with regulations that affect financial firms such as SOX, GLBA, PCI DSS, and BASEL II. Over 250 out-of-the-box reports accelerate regulatory audit processes. In addition, pre-built knowledge of business applications such as SAP, Oracle e-Business Suite, and PeopleSoft deliver dedicated application content that keeps security and compliance up-to-date. With summary and drilldown reports and multiple distribution formats, SecureSphere offers a turnkey framework for compliance reporting.

CASE STUDY

Global Bank Reduces Time and Complexity of SOX

A global financial services company, like many publicly traded businesses, was overburdened with cumbersome Sarbanes-Oxley (SOX) compliance processes that cost over $1.5 million dollars annually. Every quarter, the company's auditors, IT managers, and DBAs would define and implement audit rules to meet financial reporting demands. Once the data was collected, IT personnel would scour through reams of logs to extract the relevant data and then organize this data into presentable reports.

SOX compliance initiatives required weeks of direct oversight by key IT managers every quarter and disrupted ongoing IT projects. One IT administrator estimated that he spent 60% of his time manually auditing the company's databases to meet various regulatory requirements.

The company sought a product that would:

- Automate compliance reporting
- Improve visibility of DBA activity
- Bolster database security to protect sensitive data
- Eliminate human error in manual audit processes
- Offer low deployment and maintenance costs

Solution

After evaluating several database auditing products, the company chose the SecureSphere Database Firewall from Imperva. SecureSphere was the clear choice because it provided a rich database compliance reporting engine with pre-defined SOX reports, it was easy to implement, and it captured local access by the DBA.

SecureSphere's strong security features also impressed the bank's IT team. Using the integrated database assessment tool, the company uncovered dozens of database vulnerabilities. The company recognized the enormous costs of a data breach and used SecureSphere to prevent malicious activity before it impacted the business.

Benefits

SInce implementing SecureSphere, the company reduced the SOX compliance reporting cycle from several weeks to just a few days. SecureSphere identified materially relevant database activity and verified compliance with the bank's defined policies. SecureSphere presented the audit information in an easily understandable format, impressing the company's external auditors.

The bank's IT staff found SecureSphere technologically superior and yet easy to deploy maintain, and rolling out the solution has not affected database performance. SecureSphere has been a major success for the company and everyone involved in SOX audits.

SecureSphere Web Security Solutions

The market-leading SecureSphere Web Security Solutions are 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 financial 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, MySQL, Teradata, 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. 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. 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.

Banking on Your Future with Imperva

The Imperva SecureSphere application and database security products provide the foundation for financial institutions to protect their sensitive assets and achieve regulatory compliance. SecureSphere comprehensively addresses financial organizations' security and regulatory requirements by protecting sensitive data, auditing access to sensitive data, and automating compliance reporting.

"SecureSphere was the easiest product to deploy and configure, and delivered the best performance in our tests. With Imperva we have a complete solution for data security and PCI compliance.

Jean-Pierre Zaiter, CIO
Intuition Systems

"SecureSphere is able to transparently protect our derivatives trading platform from Internet attacks without degrading application response times."

Mamal Torfeh
Head of Global
Managed Services
AEMS

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