Insurance Firms Depend on Imperva to Safeguard Data

Insurance Data is a Lucrative Target for Hackers

Insurance underwriters must gather and correlate a vast amount of data to assess risk, determine eligibility, and decide what premium to charge clients. As part of the business, insurance companies evaluate potential clients based on a large set of data. This data can be in the form of medical information, credit history for automobile or home loans, driving records, criminal records, and other types of personally identifiable information.

The data gathered by insurers provides an attractive target for direct data theft and fraud as the personal information may be used for a variety of fraudulent purposes, most commonly to sell for profit. Additionally, insurance firms are increasingly under the scrutiny of regulations such as SOX, HIPAA, PCI, GLBA, and PIPEDA, with strong implications to their business in the event of non-compliance. More and more high profile insurance companies[1] are discovering the heavy implications of a data breach on their business in the form of decreased credibility with clients, lost revenue, and high costs of recovery from such an incident.

Protection of Core Business Data

Because collecting personal data of clients and employees is critical to how they run their business, insurance companies must assure the data is protected. In particular, they must safeguard online portals that are exposed to attack and protect databases that contain sensitive data, including monitoring of privileged users. As they face an increasing number of overlapping regulations, organizations are looking for solutions that can automate compliance processes.

To meet security and compliance requirements, insurance companies must implement controls that:

- **Discover and identify sensitive data**
- **Audit and control sensitive data access**
- **Protect online portals from attacks**
- **Automate compliance reporting**

Finally, given the investment that insurance firms have in their online portals and large-scale databases, a security solution must meet the operational requirements needed to support the business. This includes mandates to not impact system performance or require complex network or server changes.

[1] Insurance employee commits fraud with stolen information:
http://www.azcentral.com/community/westvalley/articles/2008/09/13/20080913gl-nwvstatefarm0913.html

CASE STUDY

Large Mutual Insurance Firm Monitors Databases without Impacting Performance

In 2006, a large mutual insurance provider was informed by the FBI that a former contractor had tried to sell some of its clients' sensitive data, hundreds of thousands of names and social security numbers online for profit. The insurance company had to bear the high costs of this data breach, including vulnerability remediation fees amounting to millions of dollars, as well as paying credit monitoring fees to clients whose private information had been compromised. To prevent further data theft incidents and protect its reputation among clients, the firm evaluated database auditing and monitoring solutions. The company needed a solution that would automate the process of auditing their Oracle, MS-SQL and DB2 databases.

The security team sought a product that would:

- Protect sensitive data of their clients
- Automate database monitoring process to reduce potential for human error
- Enable high performance – be able to scale to multi-Gigabit throughput

Solution

After evaluating various database auditing and monitoring products, the company chose Imperva SecureSphere. Not only did the product exhibit better performance because it inspected traffic without imposing changes to the database or network, but it also enabled the organization to deploy fewer boxes in the network than competitive products. The company also liked SecureSphere for its ease-of-use, its ability to automate the process of database usage profiling and audit policy creation, and its superior reporting options. The company also felt Imperva was the vendor that they could depend on in the long term to address their current and future database activity auditing and monitoring needs.

Benefits

By choosing Imperva SecureSphere, the cost of database activity monitoring decreased over 50% vs. the original manual solution. Using SecureSphere Database Activity Monitoring, the security team actively monitors suspicious database activity and can view real-time alerts through the SecureSphere management GUI.

Imperva SecureSphere for Insurance Institutions

Insurance companies need to audit, monitor and protect databases from data theft and abuse, and they must safeguard online customer and agent portals against all types of application threats. This is important for maintaining best practice security and for ensuring compliance with multiple regulations. Furthermore, insurance firms need to automate compliance reporting to reduce operational expenses and keep up with changing regulatory requirements.

Imperva SecureSphere solutions address insurers' key security and compliance needs: auditing and protecting data which includes enforcing separation of duties, protecting online portals, and automating compliance reporting. With Imperva SecureSphere, insurance institutions are well equipped to meet current and future application data security and regulatory requirements.

Audit and Protect Data

Discovery and Assessment

To protect core business data, you must first locate it and classify it. SecureSphere Database Security Solutions simplify this process by discovering databases and sensitive information. 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

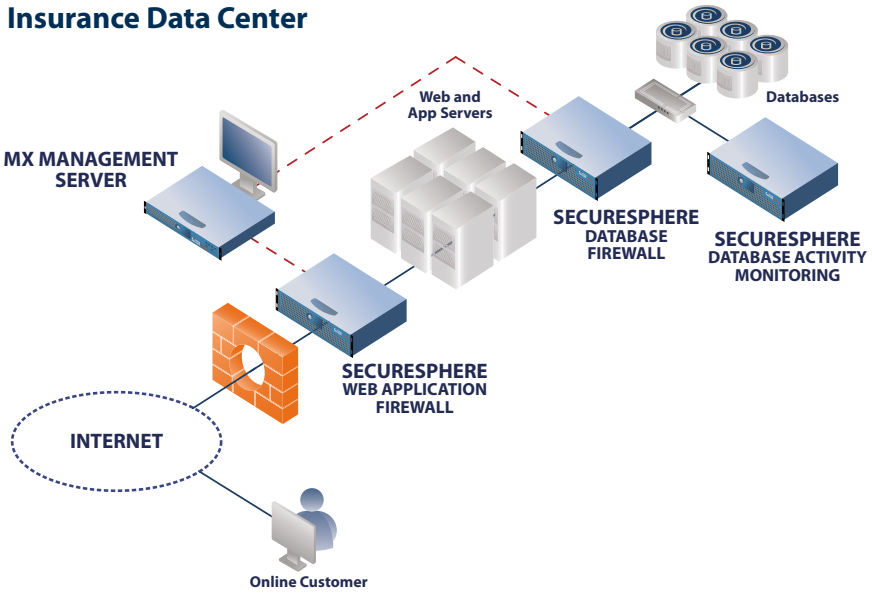
SecureSphere monitors all access to databases and can enforce database access controls. SecureSphere recognizes known database attacks, SQL protocol violations, and unusual database activity. Imperva's Dynamic Profiling automatically creates and maintains baseline profiles of each user's activity. SecureSphere keeps a record of every user's database activity and detects any material policy violations. Compliance auditors can compare usage to job functions and regulatory requirements. SecureSphere presents database information in a format accessible to non-database administrators, enabling separation of duties between security, audit, and database administration.

Audit Database Access

Insurance firms must keep a close watch on those databases which contain sensitive business data in order to identify suspicious database activity, including data tampering and data theft attempts. SecureSphere Database Security Solutions collect 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).

SecureSphere can automatically identify and alert insurance firms to suspicious changes to database values. Row-level change auditing streamlines fraud prevention, forensics and regulatory compliance. Often, when users access databases through an application, connections are pooled by the application server into a single connection to the database. Traditional database auditing solutions do not consistently link database activity with specific users when connection pooling is in use because only the application's login name is recorded. SecureSphere is unique, because through Universal User Tracking, it tracks individual user connections, not just application logins, to provide full database audit accountability.

Insurance Data Center



Protect Online Portals

Prevent Attacks and Mitigate Vulnerabilities

The SecureSphere Web Application Firewall protects online portals and all types of proprietary and packaged business applications from attack and abuse. It leverages multiple defenses to accurately block all types of application attacks by creating a baseline model of application usage and comparing it with live application traffic to check for any suspicious behavior. It utilizes a multi-layered security model based on a combination of a dynamic positive (white list) and dynamic negative (black list) security models. SecureSphere correlates information across security layers and over time to identify attacks with pinpoint accuracy.

Monitor User Activity to Reduce Risk

SecureSphere captures information on Web server (HTTP) responses and also tracks application usage (including login URLs, form fields, URL parameters, etc.) on a per user basis. As a result, application developers can easily learn about and fix flaws in the code and the security team can take action against specific users who are trying to use the application in an unauthorized way.

Automate Compliance Reporting

Reduce Operational Expenses

Insurance firms must invest inordinate amounts of time and resources manually extracting audit data and preparing compliance reports. SecureSphere's reporting framework automates this process. SecureSphere's graphical reporting engine helps document compliance with multiple regulations. Over 250 out-of-the-box reports accelerate regulatory audit processes. SecureSphere's automated framework decreases the number of compliance issues cited by auditors and substantially reduces the risk of failing a regulatory audit, while reducing the organization's operational expenses.

Keep Ahead of Evolving Regulatory Landscape

Through the Imperva Application Defense Center (ADC), SecureSphere automatically receives security defense content updates to protect applications and databases from the latest threats. ADC Insights enable organizations to streamline the compliance process and meet regulatory requirements on their application infrastructure without in-depth knowledge of the applications or mandates. ADC Insights provide continuously updated configuration packages that tailor SecureSphere for the compliance, audit, and security needs of specific business applications and regulations. With SecureSphere, organizations are prepared for changing regulatory requirements.

CASE STUDY

Fortune 100 Insurance Giant Automates Security for Online Customer Portal

One of the top ten property and casualty insurance providers in the USA planned to expand its breadth of consumer oriented insurance services. In particular, they wanted to roll out a custom-built online application that would enable it to request information from potential clients in order to evaluate eligibility and provide insurance policy quotes. Before going live with the new service, the company realized that it needed to implement a best practice security method to protect its critical business data – in particular, customer's private data – being accessed online. Thus, the insurer began looking for an application security solution.

The security architecture department sought a product that would:

- Provide accurate and automated protection for the online portal
- Enable ease of deployment without requiring changes to application or network
- Support business continuity, including HA and fail-open, which is critical to the business

Solution

The insurance firm chose Imperva's SecureSphere Web Application Firewall. It was the clear choice because it provides comprehensive protection against all type of application attacks including SQL injection, XSS, and session hijacking, due to its advanced correlation engine that combines dynamic positive and negative security models for more accurate protection with a low rate of false positives. Through Dynamic Profiling, SecureSphere automates policy creation and configuration, easing security operations. The company also appreciated that SecureSphere can be deployed inline in layer 2 bridge mode to block all types of application attacks without requiring changes to the application or network and enables fail open configuration, unlike traditional reverse proxy WAFs. It also features multiple high availability options and a fail-open configuration to ensure that the customer portal wouldn't be affected by unexpected network failures.

Benefits

The Imperva SecureSphere Web Application Firewall enables the company to reliably protect clients' personal data from being stolen. As an inline solution that directly blocks application attacks in real-time, SecureSphere helps proactively address its application security needs. A security architecture group uses SecureSphere to get an overview of the security landscape by viewing alerts logs and generating reports on any suspicious behavior with respect to the online portal so that appropriate action can be taken to address any critical vulnerabilities. With Imperva, the security team achieved its goals of securing customer data from application threats reliably while maintaining business continuity.

SecureSphere Protects Online Insurance Portals

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 insurance institutions with a proven, highly-secure solution that addresses today's security and compliance challenges.

SecureSphere Protects Sensitive Databases

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 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.

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 Automates Compliance Reporting

Imperva automates compliance reporting to lower operational expenses. SecureSphere features over 250 built-in reports for enterprise applications and data compliance mandates, a flexible reporting engine that allows customization specific to your needs and ADC Insights, which help you meet compliance requirements for your core business applications right out of the box.

"We needed a solution to detect and protect against internal compromise of data as well as monitor privileged user activity including DBAs and other powerful users. It needed to be an automated tool to ease operations and for real-time visibility into audit logs."

Brian McPhedran, Associate Vice President, IT Risk Management, Aegon

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