NetIQ
An Attachmate® Business

The Last Line of Defense: Protecting Your Databases from Malicious Attacks

White Paper

Contents

As attacks on databases increase and government regulations regarding confidential personal information tighten, corporations can no longer look at database security as optional. Private data—such as healthcare data, financial data, credit card data, customer information, and intellectual property—housed in company databases must be diligently protected to avoid serious reputational and financial consequences.

This white paper addresses the database protection issues (such as data discovery, activity monitoring, and compliance with regulations such as PCI DSS) faced by corporations today—and discusses solutions from NetIQ that can help you address these challenges.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

Database Security: The New Priority in Data Protection

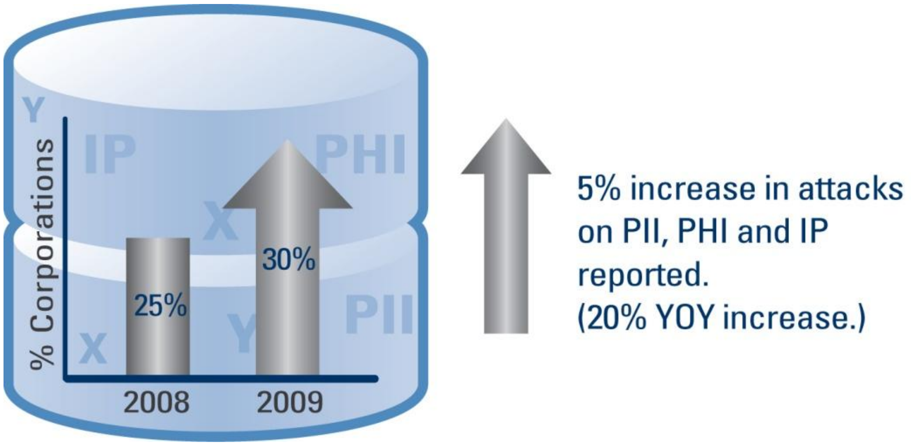
One of the most critical issues businesses face today is the ability to safeguard private data such as credit card data, social security numbers, healthcare data, and other critical information that is stored within company databases. As government regulations regarding privacy and confidential personal information tighten, corporations can no longer look at database security as optional. A security breach involving such data not only puts an enterprise's reputation at risk, but also may initiate lawsuits and regulatory fines that can have a significant long-term financial impact on the organization.

According to a 2009 Forrester research report,[1] "Database security is the last line of defense, so it deserves greater focus on the protection of private data from both internal and external attacks than IT pros have traditionally given it." One of the reasons for this shifting prioritization is the need to defend against a growing number of attacks on databases, caused primarily by two issues: 1) an increased targeting of private data because of its use in other crimes, such as identity theft; and 2) databases have historically been one of the least-protected areas of the IT infrastructure, making them an attractive target.

Because of these security trends, many enterprise organizations are shifting their data protection focus away from the perimeter, and are now focused on monitoring data located within databases. This new priority, along with the need to reduce costs and maximize IT resources, is creating a greater need for a specialized and integrated solution that monitors access to these critical databases.

Figure 1. Attacks on Corporate Databases are Growing[2]

Most Personally Identifiable Information (PII), Personal Health Information (PHI), and Intellectual Property (IP) reside on corporate databases, making them an attractive target.



[1] Noel Yuhanna, "Your Enterprise Database Security Strategy 2010: Stronger Measures Have Become Essential To Defend Against Growing Attacks," Forrester Research, Inc., September 28, 2009, http://www.forrester.com/rb/research.
[2] Sarah Peters, Senior Editor, "2009 CSI Computer Crime and Security Survey," Computer Security Institute, December 2009, http://gocsi.com/survey.

Data Protection Issues

The need to protect data from internal and external threats by applying advanced security measures, such as database auditing and monitoring, is critical. However, many information security managers have found the implementation of a comprehensive, effective database security program to be a daunting task. In addition to working in a heterogeneous environment with threats that are increasingly complex, there are monumental challenges specific to protecting information housed within relational databases. This is due in part to the large volume of both data and transactions that must be sorted through.

In order to provide adequate data protection, three key questions must be answered:

1. Which data needs to be protected?
2. Where is the critical data located?
3. Who is accessing the data?

It may seem obvious that one would need to identify his organization's sensitive data; however, with increasing pressure to comply with government privacy and security regulations, it is more critical than ever to know what data needs to be protected. Care must be taken to identify which records fall under compliance mandates such as PCI DSS, HIPAA, Sarbanes-Oxley (SOX), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), and others.

One of the most difficult challenges, especially with the large volume of data typically housed in corporate relational databases, is locating the data that needs to be secured. In a recent study[3] of corporate data breaches, 66 percent of breaches involved data that the victim did not know was there. This phenomenon stems from a general lack of awareness, not only of where critical customer data is located, but also of how it is being used. For example, test labs may be using actual customer data, thus exposing the data to risk on test servers that do not have adequate safeguards. In today's virtual environments, information can also be copied easily from a database into other documents, exposing the organization to risk of data leaks.

Finally, it is critical to know who is accessing the data. Only then can normal patterns of behavior be established in order to detect anomalies and effectively prevent data loss. Knowing who has access to critical data is also necessary to demonstrate regulatory compliance, and to perform forensics during an audit or after a data breach. Information security managers must be able to determine what privileged users are doing, which applications and tools are accessing which databases, and which databases have been the targets of unusual activity. The high number of transactions typically handled by a large enterprise database makes this a daunting, if not impossible, task if specialized monitoring tools are not deployed. Case in point: In 82 percent of corporate data security breaches, the evidence was visible in logs beforehand.[4] However, because there was so much data, the evidence was missed.

[3] Wade H. Baker, C. David Hylender, and J. Andrew Valentine, "2008 Data Breach Investigations Report," Verizon Business, June 2008, http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

[4] Baker, Hylender, and Valentine, "2008 Data Breach Investigations Report."

PCI DSS Requirement 10: A Practical Example

The Payment Card Industry (PCI) Data Security Standard (DSS)[5] is a contractual requirement for businesses that handle cardholder information for Visa, MasterCard, Discover, American Express, and Diner's Club. Although many PCI DSS requirements are straightforward and can be met as a side effect of ordinary security best practices, others, such as Requirement 10, are much more challenging to meet.

PCI DSS Requirement 10 requires that corporations:

- Know where all critical data resides.
- Maintain detailed audit trails for all PCI data access events.
- Review audit logs daily.
- Prove their ability to reconstruct a wide range of events associated with cardholder information.

Security Information and Event Management (SIEM) and Application Log Management systems provide a good starting point for complying with PCI regulations. Unfortunately, these fall short of the requirements in PCI DSS Requirement 10 because they cannot capture, manage, or report on the detailed event data that links specific users with critical data activity. Specifically, conventional application logs ignore "read" access to cardholder data. Similarly, typical SIEM logs do not capture specific access details for sensitive PCI data.

PCI DSS Requirement 10 requires the implementation of automated audit trails to reconstruct events such as accesses to cardholder data, actions taken by individuals with root or administrative privileges, invalid logical access attempts, use of identification and authentication mechanisms, access to audit trails, and creation and deletion of system-level objects. For all system components, extensive audit trail entries for each event must be captured, including the following information:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

Capturing and logging comprehensive, detailed information about all cardholder data access events is a fundamental provision of PCI DSS Requirement 10. The captured information must link specific users to specific data fields and parameters. If the audit trail cannot correlate this data, it falls short of the requirement. This is a common shortcoming when using traditional Identity and Access Management (IAM) logs or SIEM logs.

[5] PCI Security Standards Council, LLC, "About the PCI Data Security Standard (PCI DSS)," https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (accessed February 18, 2010).

Not only must access to cardholder data be tracked and monitored, but there must also be a process for linking access to system components (especially those done with administrative privileges) to an individual user. This helps prevent data theft or tampering by privileged users, which is one of the leading causes of corporate information security breaches today. Another required safeguard to prevent abuse by a privileged user is that audit trails must be secured so they cannot be altered. This means that audit trail files must be protected from unauthorized modifications and must be backed up to a centralized log server or media that is difficult to alter. Once again, traditional log files alone fall short of meeting these requirements because they do not reflect changes that can be made at the root level by an administrator with privileged access.

Finally, PCI DSS Requirement 10 requires that log files for all system components be reviewed daily in order to demonstrate knowledge of what is occurring within the system and to discover any anomalous activity. The log review must include not only the databases where the cardholder data is stored, but also the servers that perform security functions, such as Intrusion Detection System (IDS) and authentication servers. This can be a serious challenge for security departments where workloads are high and integration between system components is either limited or nonexistent, forcing administrators to perform multiple audits each day and putting a company's information at risk if the data cannot be adequately correlated.

NetIQ Change Guardian for Databases: Meeting Data Security and Compliance Challenges

With millions of cardholders and billions of data access events, a specialized and integrated solution is necessary for organizations to effectively monitor and secure access to critical databases and meet the compliance challenges of regulations such as PCI DSS.

NetIQ® Change Guardian™ for Databases provides a comprehensive auditing and monitoring capabilities necessary for organizations to help achieve compliance with PCI DSS, as well as SOX, HIPAA, FISMA, GLBA, and other regulations. This non-intrusive, non-inline appliance works across heterogeneous environments to monitor and audit access to critical data stored in databases, detect suspicious user activity, and protect against data theft or leakage.

By combining comprehensive auditing, real-time monitoring, and extensive reporting capabilities in a hardened appliance for added security, NetIQ Change Guardian for Databases helps ensure compliance with mandates, such as PCI DSS Requirement 10, while helping to secure critical data through the following essential protection measures:

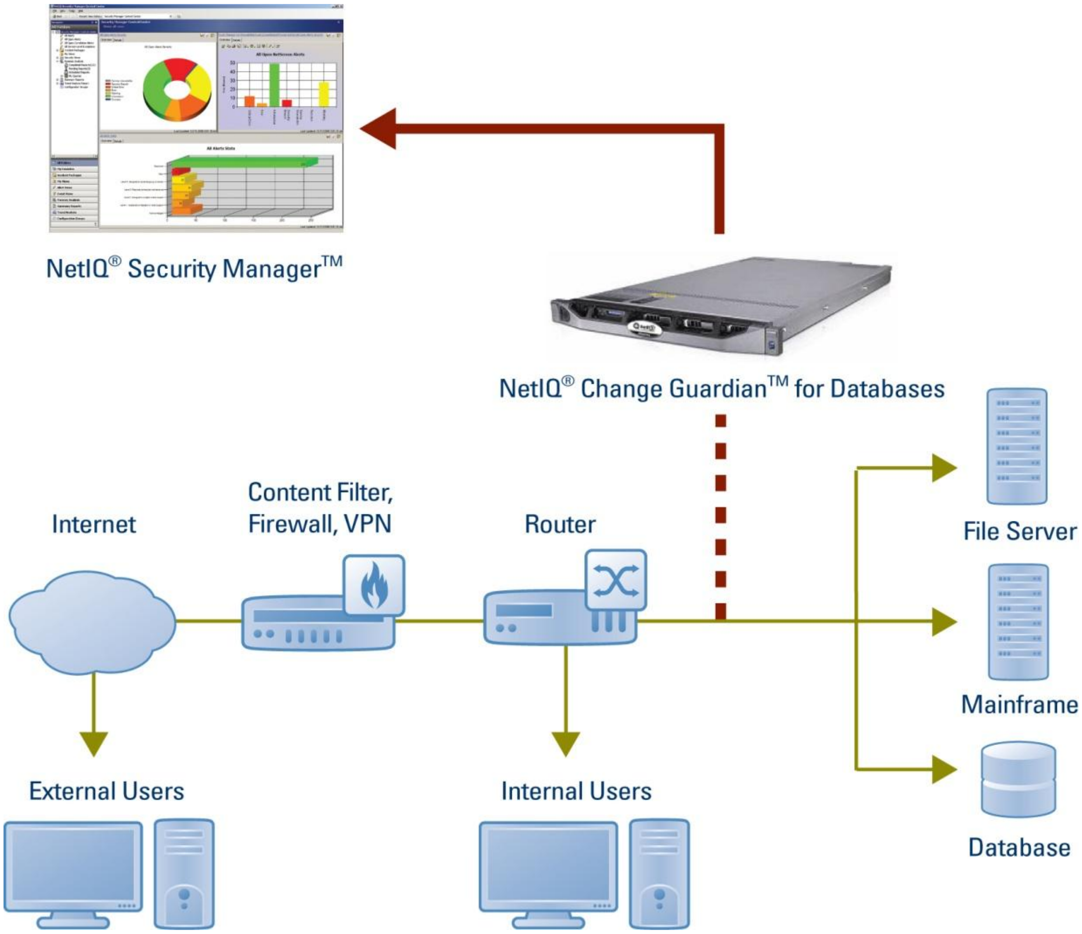
- **Identifying data at risk** – scans content for high-risk items, such as social security numbers and credit card data.
- **Automating data discovery** – finds data at rest or in motion and identifies databases on the network that may need monitoring.
- **Monitoring privileged users** – audits and monitors the activities of database administrators and other privileged users to reduce the risk of insider attacks.
- **Alerting in real time on suspicious behavior** – provides real-time visibility to activity that may indicate data theft or attack, so action can be taken before any damage is done.
- **Automatically identifying and blocking risky activity** – fingerprints suspicious behavior, reducing the likelihood of attack or data loss.

With its easy-to-use interface and strong automation capabilities, NetIQ Change Guardian for Databases offers a low total cost of ownership. In addition, it offers maximum scalability across the enterprise that helps facilitate both rapid analysis and long-term audit data storage and forensic capabilities.

By combining auditing, compliance, and security capabilities, NetIQ Change Guardian for Databases helps companies to quickly and easily deploy a 3-in-1 solution that cost-effectively meets core data protection and compliance needs while improving operations, reducing costs, and increasing customer trust.

Figure 2. NetIQ Change Guardian for Databases

A passive, non-inline appliance that provides critical data discovery, security, and database access monitoring in real time.



Completing the Picture: Building a Secure Environment with NetIQ

In security, each bit of information is like a puzzle piece: it is most valuable when seen as part of the bigger picture. If multiple pieces of security and forensics data are assembled and integrated, your ability to make effective and intelligent security decisions drastically increases. Part of the NetIQ Change Guardian product family, NetIQ Change Guardian for Databases works in conjunction with NetIQ® Aegis® to perform security workflow automation, and with NetIQ® Secure Configuration Manager™ to help achieve compliance and perform entitlement reporting. This combination of products helps to form a powerful, integrated, and automated security and compliance management solution.

Together with NetIQ's award-winning Security Information and Event Management (SIEM) solution, NetIQ® Security Manager™, these powerful tools enable system administrators, compliance officers, and information security officers to see the bigger picture – by delivering the visibility necessary to understand trends and make informed decisions - while also providing detailed analysis and automated enforcement of compliance and security policies. With optimum performance and exceptional scalability, this integrated solution helps you build a secure network while meeting the ever-changing requirements of a highly distributed and demanding computing environment.

Conclusion

Every day, millions of records housed within corporate databases are being accessed by users both inside and outside the enterprise. Organizations expose themselves to serious risk for data breaches, as well as significant financial penalties for non-compliance with regulations such as PCI DSS, when they do not adequately monitor and audit access to this critical data. NetIQ Change Guardian for Databases provides a powerful, cost-effective solution for addressing both security and compliance challenges faced by organizations seeking to protect data in their relational databases.

For more information on how NetIQ can help you protect the sensitive data in your organization's databases, visit **www.netiq.com.**

About NetIQ

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. For more information on NetIQ's portfolio of award-winning products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications, please visit **www.netiq.com** or contact sales@netiq.com.

About Attachmate

Attachmate delivers advanced software for terminal emulation, application integration, and secure communications. Our NetIQ business provides solutions for automating IT processes and managing the performance, security, and compliance of your distributed IT. With our technologies, more than 65,000 businesses worldwide are putting their IT assets to work in new and meaningful ways.

Attachmate has been helping businesses extend, manage, and secure their IT investments for more than 26 years. Headquartered in Seattle, Washington, Attachmate has offices and partners all over the globe. We are widely recognized for our innovative products, easy business transactions, and exceptional customer service. Please visit us at **www.attachmate.com**.