WHITE PAPER

Reduce Your Breach Risk: File Integrity Monitoring for PCI DSS Compliance and Data Security

A key capability of any information security program is the ability to rapidly detect and help correct data breaches. Yet every day, sensitive corporate data is accessed without detection. Whether the breach is a result of a targeted attack perpetrated by cybercriminals or an inadvertent error caused by a privileged user, the impact is major. When the breach remains undetected for a long period of time, the impact can increase significantly.

This paper discusses the importance of file integrity monitoring (FIM), which facilitates the detection of attacks by cybercriminals, as well as insider threats that may result in costly data breaches. It also discusses file integrity monitoring as a critical component of Payment Card Industry Data Security Standard (PCI DSS) compliance, and shows how NetIQ addresses both security and compliance challenges through the NetIQ Identity and Security Management family of products.

NetIQ

NetIQ | WHITE PAPER

Table of Contents

Introduction

If there were ever an era in which the saying “you can’t be too careful” rings true, it’s this one. Despite growing awareness and implementation of protective security measures, data breaches continue to dominate the headlines. The numbers are huge: 143 million records were compromised in 2009, capping off a six-year run in which a total of over 900 million records were compromised.[1] Even more alarming is the fact that these breaches happened right under the noses of information security teams, as evidenced by cases such as Heartland Payment Systems, where a breach of approximately 100 million credit card accounts went undetected for 18 months.[2]

File Integrity Monitoring: A Critical Piece in the Security Puzzle

File integrity monitoring (FIM) has become a critical piece of the security puzzle, especially given the evolving nature of the threat to sensitive corporate data. Today, a new class of attacker has emerged: organized groups of criminal operators that systematically and methodically gain access to systems and remain undetected over a prolonged duration, enabling them to achieve defined objectives, which typically extend beyond immediate financial gain. This scenario is referred to as an Advanced Persistent Threat (APT) and often manifests through breaches that leverage trust relationships such as legitimate accounts to access and compromise targeted systems. Additional layers of protection, including FIM, are needed to protect sensitive corporate data against this type of threat.

According to the 2010 Data Breach Investigations Report by Verizon Business, in cooperation with the United States Secret Service[3], 48 percent of breaches involved insiders, a notable increase of 26 percent from 2008. In most cases, the evidence clearly pointed to elevated privileges being a precursor to the larger breaches. The scope of insider threat expands exponentially with the realization that once an attacker (such as one utilizing a malware infection) is in the system, it is almost impossible to distinguish him from an insider.

According to the Verizon report, many of these cases follow a pattern in which an attacker hacks into the victim’s network (perhaps through stolen or weak credentials) and installs malware on systems to collect data. While the use of custom malware in attacks has remained stable, the malware itself has become increasingly difficult to detect, enabling it to successfully bypass standard anti-malware controls. Case in point, custom malware was utilized successfully in the Heartland breach as well as other major credit card breaches.

Forrester Research[4] notes that the best way to reduce the risk from this type of attack is to deploy file integrity monitoring tools that provide immediate alerts if unauthorized software is being installed or if critical files are modified or accessed by a privileged user.

The deployment of FIM software is not only a best practice to help safeguard against security breaches, it is also a requirement of the Payment Card Industry Data Security Standard (PCI DSS.) Specifically, the PCI DSS standard calls for the deployment of FIM software in order to alert personnel to unauthorized modification of critical system files, configuration files, or data. According to Verizon Business, over 79 percent of data breach victims surveyed in its 2010 Data Breach Investigations Report were not compliant with PCI DSS.

By detecting unauthorized access and unmanaged change to system files, FIM reduces the risk of:

- **Data breaches** – from insiders, privileged users, and attacks using malware.
- **System instability** – caused by unplanned or unauthorized changes to system configuration.
- **Poor performance** – often caused by changes outside of managed change control processes.
- **Compliance failure** – resulting from an inability to demonstrate due care and a lack of capability to monitor access to sensitive data.

FIM is an important component of any effective information security program.

---

1 Verizon Business RISK Team in cooperation with the United States Secret Service, “2010 Data Breach Investigations Report,” Verizon Business, July 2010, http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf?&src=/worldwide/resources/index.xml&id=.

2 John Kindervag, “PCI X-Ray: File Integrity Monitoring,” Forrester Research, Inc., October 26, 2009, http://www.forrester.com/rb/research.

3 Verizon Business RISK Team in cooperation with the United States Secret Service, “2010 Data Breach Investigations Report.”

4 John Kindervag, “PCI X-Ray: File Integrity Monitoring.”

A Closer Look at Insider Threat

At the most basic level, there are two kinds of insider threats: malicious and non-malicious.

Non-malicious threats include the exposure of critical systems or data through mistakes, poor judgment or unintentional acts. They may occur through the use of e-mail or other applications, and can be attributed to the loss or theft of laptops and smartphones. As employee- and company-owned mobile devices increasingly enter the IT security landscape, existing security controls and defense strategies may not be adequate to cover exposure through these vectors. As a result, non-malicious insider threats are becoming a growing concern.

Malicious insiders, often motivated by financial gain or anger at their employer, can do significant damage over a long period of time and can contribute to external breaches. Historical evidence has shown that the most damaging breaches are caused by authorized users with elevated privileges who were not being monitored effectively, or by users whose access privileges were not managed appropriately throughout the identity lifecycle. In the most recent Verizon Risk report, 24 percent of insider attacks were perpetrated by employees who recently underwent some kind of job change.

Cyber Attacks for Profit

Several of the most financially significant security breaches of the past decade have been the result of targeted, custom attacks perpetrated by sophisticated hackers. The breach of Heartland Payment Systems stands as one of the most infamous examples of such an attack. A breach of immense magnitude, security experts estimate that 100 million credit cards issued by 650 financial services companies may have been compromised. With a $300 million loss in market capitalization and over $30 million in direct losses, the financial impact to Heartland has been earth-shattering.[5]

The Stuxnet Worm is another good example of a sophisticated multi-vector attack. According to Bruce Schneier[6], the Stuxnet Worm "is a 'groundbreaking' piece of malware so devious in its use of unpatched vulnerabilities, so sophisticated in its multipronged approach, that the security researchers who tore it apart believe it may be the work of state-backed professionals." To date, the program appears to have wiped out roughly a fifth of Iran's nuclear centrifuges helping to delay, though not destroy, the country's ability to make its first nuclear arms.[7] Designed to infiltrate industrial control systems, experts warn that it could be used as a blueprint to sabotage machines that are critical to power plants, electrical grids and other infrastructure.

Catching the Cybercriminal

One of the greatest changes in attacker techniques is the high degree of stealth exhibited in the more sophisticated attacks. This enables the breach to go undetected for a prolonged period of time – during which targeted systems are exploited. For example, in the case of Heartland Payment System, the breach went undetected for 18 months. Even then, it was not discovered by Heartland's internal security team, but by third parties.

These sophisticated attacks take a variety of forms and use multiple attack vectors. However, a typical online fraud attack will exhibit several shared steps and characteristics. In its 2010 Data Breach Investigations Report, Verizon Business found that in just under half of their cases in 2009, there was at least some indication of pre-attack reconnaissance, most often in the form of system foot printing, scanning, and enumeration. Once the perimeter of the victim organization was breached, almost 40 percent of hackers were able to compromise the system in a matter of minutes or hours.

---

[5] John Kindervag, "PCI X-Ray: File Integrity Monitoring."

[6] Bruce Schneier, "Schneier on Security: The Stuxnet Worm", http://www.schneier.com/blog/archives/2010/09/the_stuxnet_wor.html (accessed February 10, 2011).

[7] William J. Broad, John Markoff, & David E. Sanger, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, New York Times, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (accessed February 10, 2011).

According to the Verizon report, in about 68 percent of cases, it took organizations weeks and even months to discover the breaches. If the breach is detected at all, it is usually through back-end monitoring by credit card companies through a technique known as Common Point of Purchase (CPP), which is typically used to triangulate fraud.

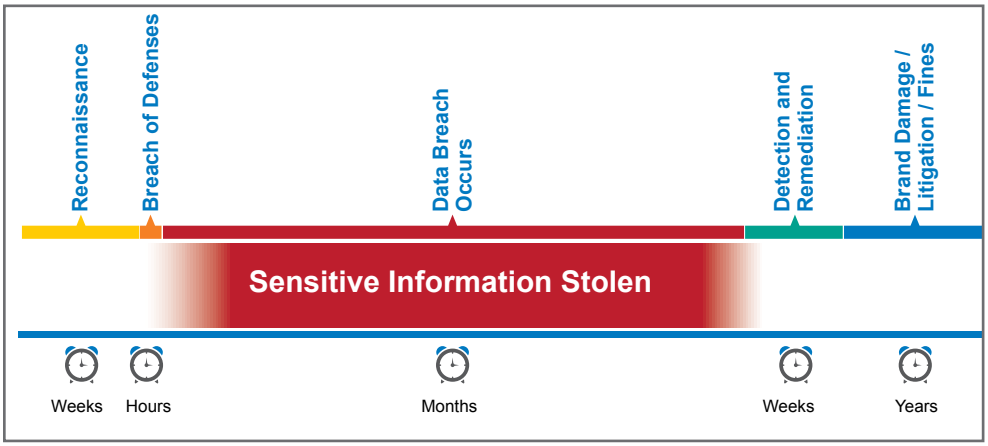

***Figure 1**. Timeline of a Typical Data Breach*

Combating the Threat: Inside and Out

The sharp increase from last year's figures (+26 percent) for breaches involving insiders may lead one to wonder if there is an epidemic of insider attacks. Regardless of the source of this growth, there are simple strategies that can be implemented to ensure that sensitive corporate data is protected. From the Verizon report, we learned that employees are often granted more privileges than they need to perform their job duties and privileged-user activity is often not monitored adequately. The simple solution is to monitor privileged users in real time to identify unauthorized or unusual activity. Because privileged users are often given access to sensitive or critical system and data files, the use of FIM technology can help track access and changes to critical system files, security log files, sensitive data files, or shares. In the case of system files on business-critical systems or sensitive data files, real-time alerts for changes can be set, enabling the immediate recognition of a problem.

Remember that once an attacker gains access to an internal user account, their behavior can be indistinguishable from legitimate activity. The use of FIM can detect the modification of files associated with an APT. This activity could then be investigated immediately, before a more costly breach can occur. Early detection of such a threat would enable a security team to significantly cut the response time and contain any damages incurred.

A Case for Corporate Compliance: PCI DSS

In addition to helping reduce the risk of data breach, compliance is another reason for file integrity monitoring. The Payment Card Industry Data Security Standard is a contractual requirement for businesses that handle cardholder information for Visa, MasterCard, Discover, American Express, and Diner's Club.[8] PCI DSS specifies FIM in requirements 10 and 11.

Requirement 10.5. Ensure audit trails (log files) are secure

> *"Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert.)"*

By mandating file integrity monitoring or change-detection software on logs, and specifying that any changes must be accompanied by an alert, PCI DSS Requirement 10.5 helps ensure audit trails remain secure.

Requirement 11.5. Access and changes to critical content and system files

---

[8] PCI Security Standards Council, LLC, "About the PCI Data Security Standard (PCI DSS)," https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (accessed March 29, 2010).

"Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly."

The intent of PCI DSS Requirement 11.5 is to give companies a solid defense against the exploitation of critical resources, especially servers. For companies to ensure the protection of critical systems, they must know about and be able to document changes to files and file systems, including:

- Who made the change
- What exactly was changed: files, registry, or configuration settings
- When it was changed
- What the value was before the change
- What the value was after the change
- If this change was authorized as part of the change management process

Managing FIM for Security and Compliance: NetIQ Change Guardian

The threat landscape that security professionals face today is complex. Whether the concern is a crippling malware attack or unauthorized access to sensitive data by an insider, the risk to critical data and infrastructure can be significantly reduced through the real-time detection of access and changes to sensitive files and systems that is provided by a FIM solution.

In addition to taking vital steps to protect their sensitive data, corporations that implement FIM also ensure that they meet the requirements of compliance mandates, which specifically call out file integrity monitoring solutions – thus avoiding costly fines and other negative effects of non-compliance.

The NetIQ® Change Guardian™ family of products encompasses a real-time file integrity monitoring approach that:

- Provides real-time detection of changes to critical systems and files.
- Enables alerting even if the content was simply viewed and not changed.
- Integrates that alerting into leading Security Information and Events Management (SIEM) solutions such as NetIQ® Security Manager™.
- Ensures the alerting process provides rich information, such as when the change was made, who made the change, what was changed, and what the state was before the change.
- Helps achieve compliance by demonstrating the capability to monitor access to sensitive data.
- Detects changes on your most important platforms: Microsoft Windows, Active Directory (including Group Policy objects), UNIX and Linux.

The NetIQ Change Guardian family of products provides real-time detection of unmanaged changes to critical files, system configurations, and Active Directory (including Group Policy objects), to ensure your security teams can proactively protect sensitive corporate information and customer data both from malicious attacks and accidental damage. These solutions provide the information necessary to rapidly make intelligent decisions, limit the risk of corporate data loss, and maximize the return on your existing security investments.

Working Together: NetIQ Identity and Security Management Solutions

Unmanaged change to the configuration of critical systems and infrastructure represents a significant and growing risk to the security of organizational data, customer information, and system stability. NetIQ Change Guardian enhances your ability to detect any unmanaged changes and respond efficiently to vastly reduce the risk of malicious activity and to support comprehensive data protection.

NetIQ provides an integrated solution that enables security teams to build a more complete security and compliance infrastructure that is scalable and reduces workload. NetIQ Change Guardian works in conjunction with best-in-class workflow automation tools and with NetIQ® Directory and Resource Administrator™ for granular control of administrative access, to form a powerful, integrated, automated solution for identity and security management. NetIQ Change Guardian also integrates tightly with SIEM solutions such as the award-winning NetIQ Security Manager in order to present correlated, rich, and relevant information in real time to security and compliance teams. Together, these products help companies not only protect their data, but also comply with important regulatory mandates such as those in PCI DSS.

Conclusion

Because of its ability to rapidly detect unauthorized access to critical systems, FIM is fundamental in the prevention of data breaches that occur due to custom malware attacks and malicious (or non-malicious) insider activities. FIM is also an important component of PCI DSS compliance, specifically referenced in Requirements 10.5 and 11.5 to help ensure that access and changes to critical systems are known about and securely documented. In order to effectively maintain both security and compliance, FIM software should also be integrated with SIEM solutions to provide correlation with other security events and ensure that critical data and systems stay secure.

The NetIQ Change Guardian family of products provides you with real-time detection and alerting for changes to files and system configurations for critical hosts. In addition to reducing the risk of data breaches and insider attacks, it provides the "who, what, when and how" for changes to other essential components within your infrastructure, such as Active Directory and Group Policy objects.

Leveraged in conjunction with traditional SIEM solutions, this family of products provides a powerful and effective way to reduce time spent gathering information, accelerate decision making, and reduce the risk of breaches.

For more information on how to address your requirements for file integrity monitoring, visit www.netiq.com or call your local NetIQ representative or partner.

About NetIQ

NetIQ is a global, IT enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly-distributed business applications.

Our portfolio includes scalable, automated solutions for Identity, Security and Governance, and IT Operations Management that help organizations securely deliver, measure, and manage computing services across physical, virtual, and cloud computing environments. These solutions and our practical, customer-focused approach to solving persistent IT challenges ensure organizations are able to reduce cost, complexity and risk.

To learn more about our industry-acclaimed software solutions, visit **www.netiq.com**.

Worldwide Headquarters

1233 West Loop South, Suite 810
Houston, Texas 77027 USA
Worldwide: +713.548.1700

U.S. / Canada Toll Free: 888.323.6768
info@netiq.com
www.netiq.com

http://community.netiq.com

For a complete list of our offices

In North America, Europe, the Middle East Africa, Asia-Pacific and Latin America, please visit **www.netiq.com/contacts**.