

Attachmate

PAGE 16

3 STEPS TO SIMPLIFY AUDITS,
DEMONSTRATE COMPLIANCE
AND MANAGE RISK ACROSS
THE ENTERPRISE

Application Security, Inc.

PAGE 17

PROBLEM SOLVED

Data Security & Compliance



Keeping Data Security in Line

WHILE THERE WERE NUMEROUS hacker attacks throughout 2011, data security experts say even more data is being compromised by a lack of controls that are often exploited by insiders for personal gain or even industrial espionage. Designed to steal valuable proprietary information by infiltrating database infrastructure, these malicious attacks require organizations to implement stronger controls to defend themselves.

However, as a new survey of 355 companies shows, many IT security and database professionals have not done enough to secure their data from either insiders or external entities exploiting insider access. The results of the study, conducted in July among members of the Independent Oracle User Group (IOUG) and sponsored by Oracle, are presented in a report, "Databases Are More at Risk Than Ever: 2011 IOUG Data Security Survey." The survey finds that one-fourth of respondents felt that a data breach over the coming year was likely or inevitable, and most believe that these breaches are most likely to come from "inside," whether carried out by someone in the organization or an external attacker. Nonetheless, barely one-third of organizations, 36%, have taken steps to ensure their applications are not subject to SQL injection attacks, and more than 70% take longer than 3 months to apply critical patch updates, leaving data vulnerable to new exploits. In fact, most respondents are unable to tell whether there has been unauthorized access or changes to their databases. At many organizations, a breach could go undetected for months or longer—only 40% of organizations audit their databases on a regular basis.

Many of the challenges to data management are management-related, versus technical flaws. To identify the best practices that data managers and professionals need to know to protect sensitive data, *DBTA* went to a number of industry experts to get their insights. Here is what they told us:

Information security is a moving target. Don't assume the technology and processes you put into place in 2010 are still effective today. "We're seeing too many cases of data center managers assuming that just because their security was sufficient in the past, it's still good enough today," Alan Brill, senior managing director for the information security, forensics and data breach practice for Kroll, tells *DBTA*. "If you're not constantly challenging your assumptions about your security, you may already be in trouble and not know it." Aaron Simpson, a partner in the Privacy & Information Management Practice Group at Hunton & Williams LLP, agrees, noting that "given the ever-changing threats and vulnerabilities, businesses need to regularly re-evaluate their security systems and policies."

*'Recognize that
at some point
you're going to have
a security incident.'*

Get change management right. Keep track of changes in security solutions and processes. "Despite the fact that network security policies are in constant flux to enable new business requirements and combat evolving threats, very few organizations do a good job managing security changes," Dr. Avishai Wool, CTO for AlgoSec, tells *DBTA*. "From a security standpoint, poorly handled changes can introduce new vulnerabilities. From an operations standpoint—poor processes require security professionals to spend too much time on manual, repetitive tasks—time that can be better spent thinking about the organization's security strategy, Wool says. "As an example, a whopping 20% of firewall changes are not needed."

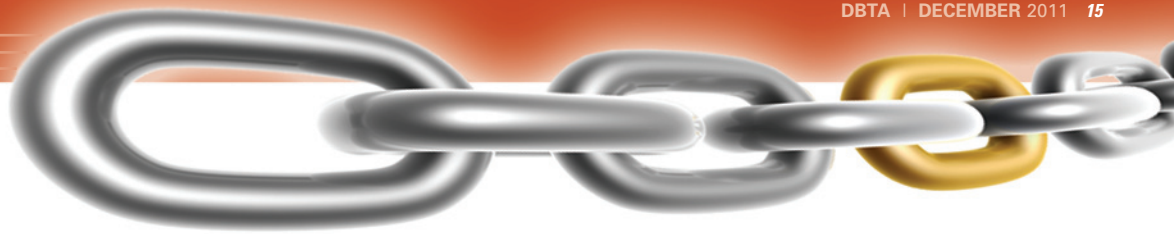
Take an enterprise view. Too often, while data is increasingly shared across enterprises, data security is approached

as a siloed initiative. "CIOs are concerned about data privacy, compliance and cross-jurisdiction requirements within their cloud deployment strategies," Pravin Kothari, founder and CEO of CipherCloud, tells *DBTA*. "Traditional approaches focusing on network or physical security do not address such issues and fail to secure the most critical asset—enterprise data. Innovative technologies such as cloud data encryption gateways are proving to be effective in overcoming emerging cloud threats by encrypting data on-the-fly before it's sent to the cloud."

Inventory your data assets. Understand what data actually exists within the enterprise, and how much is at risk. "We encourage clients to complete data element inventory to figure out which elements are most important and where they are," Carolyn Holcomb, partner, risk assurance services for PwC, tells *DBTA*. Often, critical data is centered around environments such as ERP systems, she adds.

Achieve data visibility. While the content of sensitive data needs to be kept under wraps, it's important that administrators understand where the data is flowing, and who is using it. "When it comes to protecting data, visibility to any kind of activity, is key," says Sharon Besser, vice president of technology for Net Optics. "Without visibility it would be impossible to identify unauthorized operations. Without visibility it would be impossible to identify data theft. It would also be impossible to identify suspicious and wrong behavior patterns. Solutions for data-centric visibility have many names and flavors—activity monitoring, IPS or IDS, or anything else. But the key for protecting the data—assuming you know where it is—is to see how and who is using it."

Consider private-cloud approaches. "Enterprises must store and protect sensitive data and ensure that it is available when needed," Thom VanHorn, vice president of marketing for



Application Security, Inc. tells *DBTA*. “The private cloud allows enterprises to more easily deploy a well-managed and secure cloud. The private cloud provides many of the advantages of cloud computing and less risk of potential public cloud problems related to accountability and security.”

Move to a software-based network. “By deploying next-generation networking solutions in the form of software, you can replicate traditional, hardware-centric network security policies via virtual machines,” according to Tom McCafferty, vice president of marketing for Vyatta. “With a software-based network infrastructure, enterprises are afforded more flexibility in the build out of their networks and move from flat networks to n-tier networks.”

Get away from the “block-everything” mentality. Faced with relentless attacks from all directions, the temptation is to throw a wall up around everything. However, Chris King, director of product marketing for Palo Alto Networks, advises against going too far. “Network security teams should move away from traditional ‘if it’s risky, block it’ philosophies and implement ‘safe enablement’ policies,” King tells *DBTA*. “As more and more applications for business fall into the high-risk, high-reward category, IT security must be a bit more granular and more business-focused. For example, blocking social networks just because they carry threats is increasingly untenable because organizations have strategic initiatives based on things like Facebook.”

Automate as much of the security process as possible. “Data security and compliance is not just a function of the right technology. IT and data center managers should try to select solutions that they can easily control and manage; for example, tasks such as provisioning should be automated in order to keep employees from accessing sensitive corporate data upon their termination,” says Rainer Enders, CTO, Americas for NCP Engineering. AlgoSec’s Wool agrees

that organizations “should strive to automate as many steps of the process as possible, to not only increase accuracy but also to ensure accountability and maintain corporate governance.”

Hope for the best, plan for the worst. As noted above, one-fourth of IT and data managers in the IOUG survey expect a data breach over the coming year. Actually, 100% of these managers should expect to suffer a security incident, according to Simpson of Hunton & Williams. “In the information security context, ‘when will the next breach occur’ is a far more pragmatic question than ‘will another breach occur,’” he says. “Every company should have an information security breach response plan in place for these purposes, and the plan should be tested on an annual basis.” Such a plan should assign a member of management to oversee responses to incidents by an interdisciplinary team.

“Recognize that at some point you’re going to have a security incident,” Kroll’s Brill agrees. “It may be a data breach, or a natural disaster, or an employee, temp or contractor who turns out to have criminal intent,” he says. “In all the years I’ve been working with companies, it’s those who accept that they are not immune to problems, no matter how hard they try to protect themselves, who develop and test incident response plans and get through incidents with the least trauma.”

Beware of false positives. While always being ready for the worst, be prepared not to jump to conclusions when something seems amiss, Brill also advises. “We see many corporations that start sending out notifications of a breach, offering credit monitoring, and following the necessary steps to inform affected populations, which is great, except that sometimes they discover later that the incident never happened,” he says. “Every breach law gives you time to investigate, but too many companies don’t bother. Be prepared with the resources—in-house or external—

to conduct a fast and thorough forensic analysis so that you get the best information possible for your decision making process.”

All communication is sensitive. “Businesses should always view all communications, whether internal or external, as sensitive data,” Dave Lowenstein, CEO of Federated Networks, tells *DBTA*. “When you look at every email, memo and report from that perspective, you should also understand that all computer users are operating in a highly hostile digital environment where information gets compromised every day. Your company might not hold a trove of valuable financial information that could prove detrimental if hacked, but the increase in these incidents indicates a trend that should not be ignored.”

Properly erase data before disposing of a device. “One of the most overlooked areas of securing a company’s critical data comes at the end of a device’s lifecycle, Abhik Mitra, product manager of data recovery for Kroll Ontrack, tells *DBTA*. “Failure to erase data properly at the end of a device’s lifecycle leaves a company susceptible to data breach. Deleting files from a hard drive only marks the files to be rewritten, which may never occur. Certified data wiping software that overwrites all the data on the hard drive is one of the safest methods to ensure private data is wiped properly. Another method would be to use a hardware device called a ‘degausser,’ which uses strong magnetic fields to demagnetize a drive—destroying the data in the process.”

Don’t forget about basic physical security. “Data centers need to have several layers of physical and electronic systems security in place,” according to Tom Stimmel, director of operations for CoreLink Data Centers. “Working 24/7, these systems should include things like monitored closed circuit televisions, on-site support and security teams, biometrics security systems, military-grade key cards and various alarms and sensors tied to fire and police departments.” ■



3 Steps to Simplify Audits, Demonstrate Compliance and Manage Risk Across the Enterprise

TRUSTED EMPLOYEES commit more compliance violations than anyone else. Government and industry groups have responded by enacting regulations designed to protect public and shareholder interests. But your business generates enormous volumes of network traffic every day. Tracking all user activity and then sifting through it for abuse, misuse and error can feel like an impossible task. Fortunately, technology does exist to help you overcome these challenges. It's called Attachmate Luminet.

What if you could:

- Quickly piece together data on multiple systems in multiple departments to create a comprehensive audit trail and demonstrate compliance?
- Analyze data and respond to auditor requests for information more quickly and efficiently than you ever thought possible?
- Test your level of compliance prior to an external audit?
- Respond to updated regulations by changing a few rules rather than remapping log outputs to compliance requirements?
- Retrieve clear and actionable evidence—long after the user activity occurred?

With Attachmate Luminet software you can do all that and more—without adding controls or changing a single line of code. You can:

- **See user activity**
Luminet captures a comprehensive, real-time, over-the-shoulder view of user activity across multiple applications—from mainframe to the web. It lets you define adaptable business rules that pinpoint suspicious behavior, help identify risk and demonstrate controls to flag noncompliant behavior.
- **Record user activity**
Luminet records user activity—including queries—directly from the network and stores it in a secured

repository. With Luminet in place, you can test your level of compliance prior to an external audit, and even adjust reports to meet auditor expectations.

- **Analyze user activity**
Luminet provides robust behavior pattern analysis and profiling capabilities to detect suspicious patterns and anomalies—even in high demand environments. With Luminet, continuous monitoring, dynamic risk-scoring and customizable alerting thresholds help identify the activities that truly warrant further scrutiny.

In these ways, Luminet can help you meet key requirements of these and many other regulations: PCI DSS, FACTA Red Flag Reporting, FFIEC, GLBA, HIPAA, HIPAA-HITECH, SOX, FISMA, PIPEDA, Basel II.

MOVE BEYOND TRADITIONAL LOGGING AND IMPROVE AUDITING CAPABILITIES

In the absence of true application monitoring technology, application logging has become the de facto method used to demonstrate compliance. But as enterprise applications become more distributed and encompass more complex functionality, the ability to force traditional logging to function as a modern fraud, audit and compliance solution has become increasingly untenable. Without current controls or auditing functions, they can't provide a full or accurate picture of who did what, and when. Fortunately, the next generation monitoring technologies can.

What if you could:

- Stop scrambling to piece together incomplete data on scattered enterprise systems in order to produce an audit trail?
- Determine if policies and procedures are being followed?
- Run historical queries, pattern analysis and behavioral analytics against user activity to place keystrokes into context?

With Attachmate Luminet you can. Here's how

- **Step 1: Capture the data**
Luminet records user activity in real time—screen by screen, keystroke by keystroke—creating an audit trail directly from the network. This audit trail includes both update and read-only actions for both regular and privileged users. Stored in a secured, digitally signed repository, this information can visually play back screens, keystrokes, and activities to effectively support your audit.
- **Step 2: Analyze the data**
Luminet's analytics engine tracks user behavior in real time, detecting cross-channel patterns and visually revealing activities and relationships. In this way, it can pinpoint suspicious actions—based on business rules and weighted scores that you've defined—and generate real-time alerts while helping to eliminate false positives.
- **Step 3: Generate relevant, custom audit reports**
Auditors expect precise and detailed information about how the thousands of people across your enterprise are accessing sensitive information on hundreds of applications each day. They also expect to see this information presented in a format that aligns with their unique regulatory requirements. With Luminet, you can easily access specific audit information at any time. There's no need to manually extract more or different data from log files—or worse, force auditors to guess what happened when log files fall short.

With Luminet, audit and compliance just got a whole lot easier. ■

APPLICATION SECURITY, INC.®

Database Security. Risk and Compliance

PROBLEM SOLVED

PINPOINT SUSPICIOUS DATABASE ACTIVITY FAST AND DEPLOY CUSTOMIZED, AUTOMATED BLOCKING ACTIONS WITH ACTIVE RESPONSE—NEW FROM APPLICATION SECURITY, INC.

Application Security, Inc. (AppSecInc), the leading provider of database security solutions for the enterprise, has put an end to the Database Activity Monitoring (DAM) blocking conundrum with the introduction of DbProtect Active Response.

Designed to provide an added layer of security around valuable and sensitive data, DbProtect Active Response gives organizations the flexibility to react accordingly to suspicious or unauthorized activity by blocking a connection or initiating a custom automated incident response based on company-defined policies.

For years, organizations have been faced with a trade-off between risk mitigation and business continuity. One security methodology characterized by this trade-off is the “blocking” function

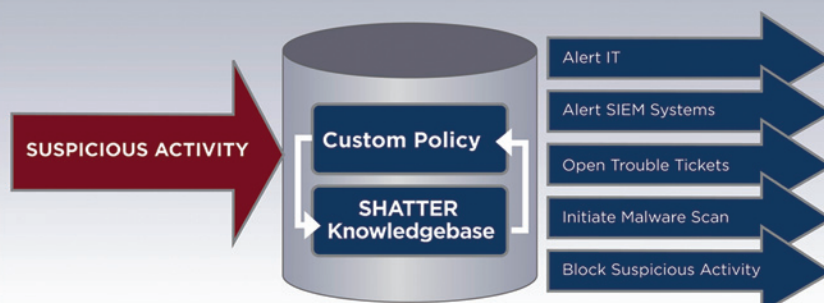
WHAT CAN ACTIVE RESPONSE DO FOR YOU?

- Block suspicious activity
- Initiate malware (and other security scans)
- Disable inappropriate application users
- Notify SIEM systems of suspicious activity for correlation with web applications
- Open trouble tickets and assign to appropriate system
- Configure databases to deny access to suspicious users or machines
- Send alerts to IT staff to initiate investigation and response
- Revoke administrative privileges

DbProtect Active Response is now available and included as part of the DbProtect Database Activity Monitoring module. CALL TODAY!

1-866-927-7732
www.appsecinc.com

DbProtect Active Response



(aka virtual patching or intrusion prevention) found in most database activity monitoring offerings.

Unfortunately, these most basic blocking capabilities fail to consider that environments and applications differ—and not all bad actions have the same impact. As a result, typical blocking functionality can erroneously block authorized activity or create “false positives,” resulting in costly and unnecessary business interruption.

Now with Active Response, AppSecInc takes intelligent threat monitoring—and reaction—to the next level. ■

APPLICATION SECURITY, INC.

350 Madison Avenue, 6th Floor, New York, NY 10017 • 1-866-927-7732

www.appsecinc.com