White Paper

Reducing Risk, Raising Governance, Improving the Bottom Line

Integrating IAM and SIEM to Drive Continuous Compliance

By David Kearns

“By having a single digital identity for each user, we can track user behavior in real time and also build a history to see exactly which users are accessing which accounts at what time. This tightens security while facilitating compliance with myriad regulatory guidelines.”

– Christine Deger
Department Manager, Network Security
GaVI

Reducing Risk, Raising Governance, Improving the Bottom Line

Table of Contents:

2 . . . . . Why Is That Integration Important?

3 . . . . . A Real-time, Enterprise-wide System

4 . . . . . The Financial Impact of a Data Breach

4 . . . . . An Integrated Solution Is Hard to Find

4 . . . . . Compliance Implies Governance

5 . . . . . Always On, Always Visible, Always Available

5 . . . . . The Solution

6 . . . . . Platform Components

6 . . . . . The Bottom Line

7 . . . . . References

Reducing Risk, Raising Governance, Improving the Bottom Line

Today, most organizations are subject to a myriad of regulations governing the acquisition, use, maintenance and disposal of information. Multinational regulations (Basel II[i]), national laws (Gramm-Leach-Bliley[ii]), regional rules (California SB 1386[iii]), business-sector regulations (HIPAA[iv]) and contractual rules of partners and vendors (PCI DSS[v]) control the collection, storage, maintenance, distribution and removal of private and/or personal data. Commercial enterprises, government agencies, educational institutions, non-profit groups and even fraternal societies are subject to some or all of these regulatory strictures. Most of these regulations, rules and laws contain remarkably similar statements and requirements when talking about personally identifiable information (PII) and data protection. The statements tend to be bromides such as "protect client/patient/member data" or "restrict access to data" without in any way telling you how to do that. When actions are defined, they tend to involve extensive auditing. The idea seems to be that the auditing will do three things: show if something "bad" happened, show when it happened and show who did the bad thing.

Not surprisingly, a large industry has arisen to satisfy the audit-log requirements of these various rules, laws and regulations. Most major identity and access management (IAM) companies have searched far and wide to acquire or partner with security information and event management (SIEM) vendors to provide the audit logs that are required. What's often overlooked, though, is that the two focuses—IAM and SIEM—need to be tightly and thoroughly integrated.

Why Is That Integration Important?

As just one example, most identity management (IdM) systems can tell which users have been provisioned to a particular application. What they don't tell you, though, is which employees are actually using that application, as well as when they use it and what they actually do within the application. Only a tightly integrated IdM and SIEM system can log the answer to those questions. And only a well-designed, security-conscious system can not only monitor those activities for audit purposes, but can also intervene (with warnings or remedies) at the time the activity is occurring.

Most contemporary applications which are called compliance management systems (and which, at best, are SIEM systems) simply write potentially interesting events to a log file. When compliance must be documented, someone (or some service) must read, digest and extract the data in these files. But, according to the "2010 Data Breach Investigations Report" from Verizon Business[vi], while 86 percent of data breach victims had evidence of the breach in their audit logs, 61 percent of victims didn't uncover the breach themselves—they were notified by a third party! As the report states: "Verizon's past research consistently finds that breaches are not found by the victim organization, but by an outside party. We would like to be able to proclaim that this was the result of caseload bias and that things really aren't all that bad outside our sample, but alas, we cannot. Data obtained from the USSS [United States Secret Service] show a very similar finding."

Not only are organizations who have evidence of breaches in their audit logs not able to discover this evidence for themselves, but the length of time needed for a third party to discover the breach is inordinately long. Looking again at the Verizon Data Breach report: "Over the last two years, the amount of time between the compromise of data and discovery of the breach has been one of the more talked about aspects of this report. It is not without reason; this is where the real damage is done in most breaches. That a breach occurred is bad enough but when attackers are allowed to capture and exfiltrate data for months without the victim's knowledge, bad gets much worse." The report then adds, "For Verizon cases, 2009 was actually the worst year yet in terms of the time-to-discovery metric," noting that fully 70 percent of breaches go undetected for months or more.

A Real-time, Enterprise-wide System

What's needed is a system that provides a real-time, enterprise-wide view of those events. What does that mean? It means the system is constantly correlating identity, access and policy information in real-time, as the events happen across the entire enterprise domain. If anomalous behavior is observed, then the proper people can be notified immediately—not six months (or more) after the damage has been done. Here's an illustration of why that's important.

In January 2010, Lincoln National Corp., a financial services company based in Radnor, PA disclosed a security vulnerability that may have leaked personal data of 1.2 million customers[vii]. The vulnerability was discovered in August of 2009 (five months before Lincoln National disclosed it), but not by Lincoln National. Someone had sent an anonymous tip to the Financial Industry Regulatory Authority (FINRA) who notified Lincoln National. A forensic security company was hired to do an investigation which revealed that some employees of Lincoln National and another one of its subsidiaries, Lincoln Financial Advisors, were using shared usernames and passwords to access the portfolio information management system. Six shared usernames and passwords, which were created as early as 2002, were found.

> "Regulatory compliance is often about reporting problems after the fact. Today's agile enterprise should focus on preventing the problem from occurring thus obviating the need to report it later and, at the same time, vastly improving the bottom line.

It really should go without saying, of course, that sharing usernames and passwords was a violation of Lincoln National's security policy. Yet, it wasn't until eight years after the policy violation had first occurred that the organization became aware of the activity. Had a real-time, enterprise-wide view of the enterprise been in place in 2002, the breach of the policy forbidding the shared use of usernames and passwords would have been noted; security personnel would have been notified; action could have been taken to enforce the policy; and those persons using the shared credentials could have been identified and dealt with immediately. As a consequence, no adverse publicity would have been generated, no regulatory admonishments would have been given and no questions would have been asked of the organization's management. Rather, the management would have been praised, the publicity would have been positive and the regulations would have been complied with.

The Financial Impact of a Data Breach

The effect of the adverse publicity cannot be emphasized enough. According to Channel Insider magazine[viii], the average cost of a data breach in 2009 was US$3.43 million, equivalent to $142 per compromised personal record. Averages by country per breach and per record included:

Data Breach Average by Country

Country	Average Cost per Breach[1]	Average Cost per Record
Australia	$1.83 million	$114
France	$2.53 million	$119
UK	$2.57 million	$98
Germany	$3.44 million	$177
US	$6.75 million	$204

[1] All amounts in U.S. Dollars

"Novell expertise in compliance-related solutions is second to none. The company is not only an established leader in identity and security management, but is also a solution provider to thousands of organizations around the globe. That deployment experience allows Novell to go beyond just installing a patchwork of products"

That's almost $7 million for each and every data breach in the U.S. Interestingly, the article attributed half of the cost of each breach to the cost of lost business resulting from the incident (i.e., bad publicity). So in the Lincoln National incident, the 1.2 million records that were compromised would have, on average, incurred $244,800,000 in costs, half of which (approximately $125 million) would have been in lost sales. A system that provided a real-time, enterprise-wide view could have saved the company millions of dollars.

An Integrated Solution Is Hard to Find

Don't all vendors' solutions integrate identity, access and SIEM technology to provide a real-time, enterprise-wide view of all network events?

It's true that most IAM products on the market today can validate identity, provision resources and enforce access roles. And most SIEM solutions are excellent aggregators of security data from throughout the organization. Unfortunately, they really aren't that good at talking to each other. The result is two distinct sets of data: who has access to the organization's resources (via the IAM access policies) and who is accessing the organization's data (via the SIEM system). What's needed is a way to coordinate the two systems, to see if the "who" that is accessing the data is also a "who" that is authorized for the data. Only a tightly integrated system can handle the communications to do this.

Many vendors will tell you that they have a tightly integrated system, but very few actually deliver on the promise of out-of-the-box integration. Instead, these vendors provide an IAM system with a SIEM system tacked on, leaving customers to build the integration themselves, or pay consultants to do it for them. This not only results in a poor-quality product, but also impacts the solution's return on investment (ROI).

Compliance Implies Governance

To be "in compliance" with regulations generally means that the organization has policies in place permitting some actions while forbidding others, mandating some activities and proscribing others. Enforcing these policies generally falls to the area called "Governance."

In 2008, France's second largest bank, Société Générale, reported that "rogue" trader Jerome Kerviel had misappropriated over $7 billion—the single largest fraudulent act ever in the securities industry.

Just as at Lincoln National, shared usernames and passwords were at the heart of the fraud. But, according to an article in Network World[ix], "the real 'secret' to the scandal was the amount of entitlements that Kerviel built up as he moved from one position to another, and from one department to another."

Société Générale had policies in place prohibiting this accretion of entitlements. This is usually called a "separation-of-duties" (SoD) policy and specifically forbids someone with one authorization (such as invoice approval) from having other authorizations deemed to conflict (such as check signing).

Any SIEM monitoring system worthy of the name would help monitor SoD policies. The best should actively prevent violations. But Kerviel didn't simply acquire authorizations for his own account; he also tapped into accounts shared among traders (and others) in violation of the bank's policies.

Only an integrated IAM and SIEM system can monitor and correlate this type of nefarious activity. Only a system that provides a real-time, enterprise-wide view can prevent it from occurring.

Always On, Always Visible, Always Available

What does a real-time, enterprise-wide view imply? By correlating identity, access and policy information in real-time through monitoring all activities on the network, the organization always knows who is accessing what, when they are doing it and if they are authorized to do it. If unauthorized access is attempted, the system can automatically and immediately remedy any violations of the organization's business policy.

At the same time a system should be flexible and business-driven. The organization is never locked into someone else's view of how the business should be run. At any time the business policies and information systems can be quickly and easily modified to adapt to changing regulations or market opportunities.

The Solution

While most vendors give lip service to tight integration of IAM and SIEM, one vendor actually delivers. Only the Novell® Compliance Management Platform integrates identity, access and SIEM technology to provide a real-time, enterprise-wide view of all network events. This tight integration eases implementation while creating the ultimate governance solution—ensuring business policy becomes automated IT practice.

In the example given of the Lincoln National breach, proper installation of the Novell Compliance Management Platform would have uncovered the sharing of usernames and passwords when that activity first occurred—eight years before the bank became aware of the activity.

The case of Société Générale is, though, even more compelling. Novell Compliance Management Platform would have prevented (through SoD policies) Kerviel from ever acquiring the rights and privileges that were so necessary for him to carry out the scheme, which defrauded the bank of over $7 billion.

"Coupling Novell Identity Manager with Novell Sentinel reduces risk by providing the necessary controls over identity. By having a single digital identity for each user, we can track user behavior in real time and also build a history to see exactly which users are accessing which accounts at what time. This tightens security while facilitating compliance with myriad regulatory guidelines."

- Christine Deger, Department Manager, Network Security GaVI

"By combining user provisioning, access control and security monitoring, the Novell Compliance Management Platform delivers business process automation that provides users with the appropriate resources, validated in real time, to ensure compliance with company policies—eliminating the gaps that have left so many companies at risk."

About the Author

Dave Kearns is the former Technical Editor of Networking Solutions magazine. His "Wired Windows" column appears in Network World magazine. He also writes frequently for PC World, The Novell Companion, World Wide Windows and NC World. He's written, edited and contributed to a number of books on networking and frequently speaks to both trade and business groups.

Platform Components

Novell Compliance Management Platform is much more than a simple policy policeman, though. This fully integrated package consists of a number of components designed from the ground up to work together seamlessly. Among these are:

- *The detection and resolution of threats in real-time through an enterprise-wide view of critical network applications and user events*
- *Automated integration of all events associated with a user (even across multiple user IDs) to that user's full identity using a simple, clear, high-level dashboard and detailed reports of user activity*
- *Tools for data analysis, data cleansing, data reconciliation and data monitoring/reporting*
- *Best practices and preconfigured provisioning policy from years of successful deployments across the globe*
- *Automated user provisioning, roles-based access control and password management*
- *A centralized way of accessing enterprise assets, including web single sign-on, standards-based identity federation, multi-factor authentication, data encryption, an SSL VPN for local and remote users, as well as native support for a broad range of platforms and directory services with no changes to applications*

By combining security monitoring, access management and user provisioning, the Novell Compliance Management Platform delivers business process automation that provides users with the appropriate resources, validated in real time, to ensure compliance with company policies—eliminating the gaps that have left so many companies at risk.

The Bottom Line

Examples such as the data breach at Lincoln National, the fraud at Société Générale, and hundreds of similar situations demonstrate that companies around the world continue to struggle with issues of policy compliance. Security and business policy violations continue to multiply and evolve, even as spending increases—leaving many organizations with a feeling that they have little recourse but to spend more. And that is why the Novell Compliance Management Platform is different from the piecemeal offerings that are in the market today. By blending its award-winning identity, access and security technology, Novell delivers a platform that provides a real-time, enterprise-wide view of the enterprise to mitigate the risk posed by internal and external threats and, ultimately, to ensure an organization's image, brand and reputation are safe.

Novell expertise in compliance-related solutions is second to none. The company is not only a recognized leader in identity and security management, but is also a solution provider to thousands of organizations around the globe. That deployment experience allows Novell to go beyond just installing a patchwork of products. The Novell Compliance Management Platform combines powerful technology with preconfigured policies and documented best practices to provide a comprehensive approach to policy compliance— plus the most impressive ROI available anywhere.

To learn more about the Novell Compliance Management Platform and how it can help organizations bolster security, boost performance and lower operating costs, go to: **www.novell.com/cmp**.

References

i Basel II is the second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. The purpose of Basel II, which was initially published in June 2004, is to create an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face. The second pillar provides a framework for dealing with all the other risks a bank may face, such as systemic risk, pension risk, concentration risk, strategic risk, reputation risk, liquidity risk and legal risk, which the accord combines under the title of residual risk. [http://en.wikipedia.org/wiki/Basel_II]

ii The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999) is an act of the 106th United States Congress (1999-2001) signed into law by President Bill Clinton which repealed part of the Glass-Steagall Act of 1933, opening up the market among banking companies, securities companies and insurance companies. The Glass-Steagall Act prohibited any one institution from acting as any combination of an investment bank, a commercial bank, and an insurance company. The act includes the Financial Privacy Rule [which] requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. It also includes the Safeguards Rule [which] requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. (The Safeguards Rule applies to information of any consumers past or present of the financial institution's products or services.) [http://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act]

iii SB1386, amending civil codes 1798.29, 1798.82 and 1798.84 is a California law regulating the privacy of personal information. Essentially, it requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed). [http://en.wikipedia.org/wiki/SB_1386]

iv The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) [HIPAA] was enacted by the U.S. Congress in 1996. The Privacy Rule took effect on April 14, 2003, with a one-year extension for certain "small plans". The HIPAA Privacy Rule regulates the use and disclosure of certain information held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.) It establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of an individual's medical record or payment history. [http://en.wikipedia.org/wiki/Hipaa]

v The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard defined by the

Payment Card Industry Security Standards Council. The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands. The current version of the standard (v1.2 as at October 1, 2008) specifies 12 requirements for compliance, organized into six logically related groups, which are called Control Objectives: Build and Maintain a Secure Network; Protect Cardholder Data; Maintain a Vulnerability Management Program; Implement Strong Access Control Measures; Regularly Monitor and Test Networks; Maintain an Information Security Policy. [http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard]

vi *"2010 Data Breach Investigations Report," Verizon RISK Team in cooperation with the United States Secret Service (www.verizonbusiness.com/go/2010databreachreport/)*

vii *"Lincoln National Corp Reveals Potential Breach of 1.2 Million Accounts," Bank Info Security*

viii *"Security: What a Data Breach Really Costs," by Ericka Chickowski, 5/5/2010 Channel Insider*

ix *"Was it lack of governance at Societe Generale that allowed rogue trader to do harm?" Security Identity Management Alert By Dave Kearns, Network World 2/13/2008*

www.novell.com/cmp