Business White Paper

SECURITY MANAGEMENT

The Business of Health Care—More Than Just HIPAA and HITECH

Novell

Table of Contents:

Executive Summary

In response to the need for health care organizations to comply with the requirements of HIPAA and HITECH, an array of security and technology vendors have come forth with various solutions designed to facilitate compliance.

While health care organizations face significant challenges with HIPAA and the new HITECH requirements, the scope of their compliance and security concerns extends well beyond these regulations. Health care organizations must also handle a wide array of other industry regulations, such as SAMHSA, PCI, GLBA and COBIT. To address the full range of security and compliance challenges they face—including the heightened privacy, monitoring and security requirements introduced by HITECH—health care organizations need to take a unified, multi-dimensional approach to compliance. Security information and event management (SIEM) and log management solutions that deliver cross-system correlation with integrated identity management optimize the delivery of unified compliance and deliver lower TCO than a siloed approach.

Moving Beyond a la Carte Compliance

The Health Insurance Portability and Accountability Act (HIPAA) changed the landscape for how health care organizations must handle sensitive information. Its security and privacy rules have prompted organizations to take significant steps in reducing data leakage, verifying proper access and use of sensitive data, enhancing role-based access controls and more. As a result, health care organizations implemented comprehensive changes or improvements to security practices in the areas of data access protection, storage, monitoring and auditing, along with ongoing assessments of how and by whom data is being accessed.

Adding to the significant demands that HIPAA already places on health care organizations, an amendment to HIPAA recently passed to further strengthen the privacy and security protection of health information. This amendment, the Health Information Technology for Economic and Clinical Health Act (HITECH Act), requires providers to further improve their breach-notification procedures, enhance policies and procedures for individual access to "protected health information" (PHI), better account for the disclosure of and access to PHI, and put in place agreements with their business associates that provide further PHI protections.

In response to the need for health care organizations to comply with the requirements of HIPAA and HITECH, an array of security and technology vendors have come forth with various solutions designed to facilitate compliance. In particular, vendors of SIEM and log management technologies offer solutions that can play a major role in addressing the compliance concerns in the health care industry.

Often deemed "health care solutions," many SIEM and log management products offer modules that focus specifically on requirements for HIPAA, and in limited cases, HITECH as well. The degree to which these solutions or modules actually enable organizations to comply with HIPAA and HITECH in an efficient and cost-effective manner varies a great deal, and they often fall short of efficiently delivering the key capabilities that organizations really need.

By far the greatest shortcoming—and a point of major frustration for health care organizations in general—is that the majority of these solutions fail to recognize that *health care organizations need to worry about more than just HIPAA and HITECH*. While HIPAA and

HITECH compliance is a major concern for health care organizations, their business and operational landscape is much broader than those regulations alone.

Health care organizations in the United States have to abide by the laws and regulations outlined by the Substance Abuse and Mental Health Services Administration (SAMHSA), which governs confidentiality of drug and alcohol abuse patient records, reports of violation, criminal penalty for violation, minor patients, incompetent and deceased patients. Also, since most health care organizations deal with credit card transactions, compliance with Payment Card Industry Data Security Standards (PCI DSS) is required. Certain health care organizations, especially insurance providers, must also be concerned with Gramm-Leach-Bliley Act (GLBA) compliance and its auditing requirements. Organizations that want to ensure that their IT departments follow best practices for use and governance of their information technology might have additional internal mandates that they have to adhere to in accordance with the policies and practices outlined by the Control Objectives for Information and related Technology (COBIT) standard.

To address these and other regulations and standards, health care organizations are often left to find and implement specific modules for each area of concern—the a la carte method. While this approach might simplify the selling model for SIEM, log management and other technology vendors selling health care-specific solutions, it doesn't adequately address the needs of health care organizations, which are often left with a complex, disjointed mix of products and modules that are difficult to manage, inefficient, expensive, have redundant capabilities, leave gaps in coverage and fail to provide the complete visibility required.

Rather than the a la carte modules for HIPAA, HITECH, SAMHSA, PCI, GLBA, COBIT and others, what health care organizations really need is a solution that covers the broad landscape of compliance and operational requirements. They need a SIEM and log management solution that is intelligent enough to deliver a unified view of compliance for their entire organization, and not just what a particular regulation or standard requires. They need a true health care solution that takes an integrated approach to all their logging, monitoring, auditing and reviewing activities for all their compliance and operational concerns.

Delivery of the integrated approach that health care organizations want and need requires a multi-dimensional enhancement to a traditional three-legged SIM and log management model. It requires the addition of two powerful new dimensions: correlation and identity; and it requires increased attention to unique health care requirements in the area of privacy.

Multi-dimensional Approach to Health Care and SIEM

The traditional approach to SIEM and log management focuses on three main areas: operations, security and compliance. In the operations area, SIEM solutions monitor and analyze the health of the network, watching for events that can affect overall performance, failures and availability of the network and servers. In terms of security, SIEM solutions help organizations analyze and assess their risk posture, helping them identify aberrant behavior and potential threats to their infrastructure.

While event monitoring and log management in the operations and security categories are fairly standard, the area of compliance covers a variety of different profiles designed to address specific regulations, rules or requirements (i.e., HIPAA, HITECH, PCI, SAMHSA, GLBA and COBIT). SIEM and log management vendors typically address the

Delivery of the integrated approach that health care organizations want and need requires a multi-dimensional enhancement to the traditional three-legged SIM and log management model.

To deliver a complete health care solution, SIEM and log management offerings must integrate and correlate all relevant compliance, operational, security and privacy events into a single view to give administrators and managers comprehensive visibility into all relevant areas of concern for their entire enterprise.

Health care organizations have realized the need to implement solutions that automate the collection of audit logs and facilitate the identification and reporting of questionable activity according to the requirements of HIPAA.

needs of compliance by creating and offering individual modules that address the requirement of individual laws or regulations. For example, a HIPAA module will come with a prescribed set of rules for logging events that are associated with the security requirements in HIPAA. Likewise, a PCI module will have rules for logging events specific to PCI-DSS requirements.

But the lack of integration between these compliance modules creates complexity, inefficiency, ineffectiveness and functionality gaps. To deliver a complete health care solution, SIEM and log management offerings must be able to integrate and correlate all relevant compliance, operational, security and privacy events into a single view to give administrators and managers comprehensive visibility into all relevant areas of concern for their entire enterprise. They also need to be able to tie those events to user identities so they not only know when a certain event occurred, but who was involved in that event.

Multi-system Correlation and Normalization

The different applications and systems in a health care organization might each produce between several hundred and several thousand event logs per minute. That's simply too much information for a security or compliance manager to manually compile, digest, analyze and correlate to produce a meaningful report. The complexity and difficulty significantly rises as the number of individuals in the organization increases. For example, if the average hospital has 10,000 employees, it becomes a massive effort to try to keep track of all the system logs being created every time one of those employees simply looks up some information, accesses a record or performs some other activity.

Managed manually, this is a massive effort and the reason little network logging occurred within health care organizations until recently. These organizations simply didn't have the resources and time to invest in anything more than very specialized audits for high-profile patients. Audits of health care applications typically occurred only in reaction to complaints or when other concerns surfaced. The introduction of HIPAA changed everything.

HIPAA significantly stepped up the logging and auditing of events that health care organizations had to do. One of these requirements mandates that they have audit control standards for recording and examining activity in their systems that contain or use electronic PHI. From these audit records, organizations must be able to determine when suspicious activity occurs on a certain device as well as determine information about the user engaged in that activity. HIPAA also requires organizations to regularly review records of system activity, such as audit logs, access reports and security incident tracking reports.

In response to these requirements, health care organizations have realized the need to implement solutions that automate the collection of audit logs and facilitate the identification and reporting of questionable activity according to the requirements of HIPAA. It is no longer sufficient for SIEM and log management solutions to simply collect logs from network servers, workstations and other devices. While this is what traditional log managers have done in the past, today's solutions need to be able to do more.

To adequately address privacy rules, they also need to collect and correlate information from an organization's actual health care applications as well.

Unfortunately, as mentioned before, the majority of the SIEM and log management solution vendors take a modular approach, only delivering capabilities within a narrow view of HIPAA. This narrow view does not go beyond the tightly predefined boundaries of their siloed health care modules—boundaries that ironically don't address privacy and don't include the ability to collect these health care application logs or interact with other solutions that can. Organizations want and need a true *health care* solution to actively monitor different users and correlate their activities in all of the organization's different health care systems and applications.

In essence, this also means that a true health care solution needs to go beyond the traditional approach of focusing on the three areas of operations, security and compliance. It needs to add privacy as the fourth element, which is the ability to collect and correlate privacy information against compliance, security and operations for a complete view of activity in the environment. Additionally, that collection and correlation needs to be able to go beyond just HIPAA in general.

While HIPAA might be the major impetus for health organizations to take advantage of log management and SIEM solutions, it's not their only area of concern. SIEM and log management solutions need to be able to take an active feed of log events from all the various sources within health care environments and in real time correlate those events to provide a single, unified picture of what is really happening in the environment. This not only includes HIPAA, but also PCI, SAMHSA, GLBA, COBIT and others. A true health care solution needs to account for all the policies and regulatory rules that affect the organization, correlating and normalizing all their associated log events into real-time alerts, as well as easily digestible views and reports.

User Identity Correlation and Normalization

In addition to correlating activity beyond a narrow HIPAA view, a true health care solution also needs to account for what users are doing within the health care environment. The ability to account for user activity is a much needed component that is noticeably absent from most SIEM and log management solutions. The ability to monitor and tie events to specific users and their roles is a critical component in terms of satisfying the risk management criteria of HIPAA and the new regulations introduced by the HITECH Act.

To address this lack of user correlation, some organizations might deploy an identity management system in conjunction with their SIEM solution. However, most identity management solutions don't have the necessary integrations with separate SIEM products needed to tie events back to specific users. Unless the SIEM solution provides out-of-the-box identity management integration, organizations will be left to expend significant resources in an attempt to create the level of integration required—if even possible—to provide complete and accurate correlation and normalization of events based on specific users and their roles.

The challenge of creating this level of integration from scratch is exacerbated by the fact that the identity management system needs to understand all the different usernames and logins that individuals use in all the different applications being monitored by the SIEM. The only practical way to address this level of user monitoring is with a SIEM solution that has the built-in ability to monitor, correlate and normalize individual user activity in all of an organization's different systems, no matter what the user ID is in that system.

SIEM and log management solutions need to be able to take an active feed of log events from all the various sources within health care environments and in real time correlate those events to provide a single, unified picture of what is really happening in the environment.

Meaningful use goes beyond the old add, delete and modification requirements previously required by HIPAA. The new standard is very specific, laying out exactly what PHI must be logged.

Insights into HITECH

The underlying vision of the recent HITECH amendment to HIPAA is to foster the creation of patient-centered learning health systems that use information to continuously improve the health and health care of the individuals and communities they serve. It strives to do this through a variety of IT-related federal health policies, including policies and incentives that focus on improving privacy and security protections for health information, as well as facilitating individuals' access to their health information. The following represent some of the major themes in HITECH that health care providers need to be aware of and ensure that their SIEM solutions can address:

- *Meaningful use*
- *Accounting for disclosures*
- *Breach notification*

Meaningful Use

One of the main goals of HITECH is to accelerate the adoption and "meaningful use" of interoperable health information technology (HIT) and qualified electronic health records (EHRs). Under HITECH, Medicare and Medicaid program health care provider participants that adopt and successfully demonstrate "meaningful use" can become eligible for incentive payments. The official definition of what constitutes "meaningful use" will change over time as technology capabilities change and provider practices evolve, but its objectives are to promote the use of certified EHR in a manner that results in patient-centered, evidence-based, prevention-oriented, efficient and equitable health care.

With this in mind, much of the meaningful use rule focuses on how health care providers must meaningfully handle EHRs to qualify for incentive dollars. This includes capturing health information in a structured format and then securing that information to appropriately track and communicate patients' health conditions.

In terms of security, there are two main aspects to the meaningful use rule. The first aspect requires health care providers to use certified Electronic Health Records (EHRs), as defined in HITECH, that employ a certain set of security features. The second aspect of meaningful use says that organizations need to conduct risk assessments in accordance with the Information System Activity Review requirements in HIPAA and then address any identified security gaps to be HIPAA compliant.

However, in terms of system activity review and log management, meaningful use goes beyond the old add, delete and modification requirements previously required by HIPAA. The new standard is very specific, laying out exactly what PHI must be logged.

The meaningful use rule requires that organizations log all PHI actions that occur in all their systems, including the viewing of patient records. Not only does this mean that organizations need the added ability to audit the time that authorized users view a patient record, it also means they need to log patient record activity from all their different systems and normalize those activity logs in a way that allows them to determine and verify what actually happened for any particular PHI.

This requires that organizations collect event information for every electronic access to each patient's EHRs and then, upon request, present that information to the patient in a singular fashion. Organizations with multiple systems that interact with patient information need to produce an electronic medical record (EMR) that presents all collected data in a single view.

Meaningful use also requires that system users have unique user IDs and logins so organizations can identify who viewed, changed, deleted or added PHI. Thus not only do PHI-related actions have to be logged, they must be traced to the actual users. For organizations that do everything

through a single system—from admitting on the front end to bill payment on the back end—this identity requirement might be easy to address. But for organizations that employ multiple best-of-breed solutions, they need a SIEM solution that can automatically and accurately normalize individual actions based on identity across all their different systems to verify the "who" in all PHI-related events.

Ideally, the SIEM solution should also correlate users' PHI-related activities with other user events logged by the organization's non-PHI-related systems, including its network system and physical facility security systems. In other words, a SIEM solution that can correlate identity-based events across all these systems should also alert organizations to suspicious activity. For example, the system should create an alert if the health care application indicates that John Smith viewed a patient record at a certain time, yet other event logs show that John Smith wasn't logged in or even in the building at that time.

The ability to pull together multiple pieces of identity-based information from multiple sources and then automatically normalize and make sense of that information allows organizations to more accurately identify who did what and when.

Accounting for Disclosures

The accounting for disclosures requirement in HITECH gives patients the right to request that the health care provider provide information about when and to whom any of their PHI has been disclosed over a three-year period. It also requires that the health care provider's business associates produce, upon request, an accounting of disclosures of PHI for any treatments, payments and health care operations. While HIPAA has always had a similar requirement, which allowed patients to ask for a record of who has accessed their information, HITECH strengthens this requirement. Under HIPAA, organizations could satisfy the patient's request for disclosure in any form they wanted. But with HITECH, if an organization has an EHR for a patient, it must provide the disclosure information in a comparable electronic form. What this means is that the organization must collect event information for every electronic access, not only to that patient's EHR, but to all patient-related information, such as by the provider's financial systems or insurance claims by the insurance provider. This extends the log collection and correlation requirement to a much broader degree, necessitating that organizations have a SIEM solution that has the ability to integrate across the organization's broad landscape of systems and its business associates' systems.

It is no longer sufficient for SIEM and log management solutions to simply collect logs from network servers, workstations and other devices.

While the collection and correlation of access events across multiple systems can be a challenge for some SIEM solutions, the greater challenge in accounting for disclosures is identifying who accessed the information and if that access was legitimate. This requires a SIEM solution that not only has the ability to accurately correlate identity information with events, but can also clearly identify the user's current role to determine whether or not the access was appropriate.

Complicating the ability to correlate identity and role information with access events is the fact that a single user within an organization might have different usernames in the organization's different systems, such as john_smith, jsmith, johnsmith or jsmith22. This requires a SIEM solution to be smart enough to understand that all of those different usernames in the different systems are actually the same user and then correlate all

The ability to pull together multiple pieces of identity-based information from multiple sources and then automatically normalize and make sense of that information allows organizations to more accurately identify who did what and when.

The second aspect of meaningful use says that organizations must conduct risk assessments in accordance with the Information System Activity Review requirements in HIPAA and then address any identified security gaps to be HIPAA compliant.

For many organizations, this ability to correlate user identities and roles against access events will be their biggest obstacle to achieving HITECH compliance. Overcoming this obstacle requires a SIEM solution that combines identity management with an integrated, multi-dimensional approach to health care.

their associated user events. As part of that correlation, and to determine whether the access was appropriate, the solution must be able to verify the user's role at the time of the access.

For many organizations, this ability to correlate user identities and roles against access events will be their biggest obstacle to achieving HITECH compliance. Overcoming this obstacle requires a SIEM solution that combines identity management with an integrated, multi-dimensional approach to health care.

Breach Notification

HITECH also includes breach notification statutes that require organizations to notify patients if their "unsecured" PHI is accessed, acquired or disclosed as a result of a breach. Additionally, if such a breach impacts more than 500 patients, the organization must notify the U.S. Secretary of Health and Human Services as well as prominent media outlets.

To effectively address the breach notification requirement, organizations should leverage SIEM solutions that can automatically collect, correlate and normalize events and provide real-time reporting. Real-time reporting of events gives organizations early detection of potential breaches, enabling them to stop or minimize the impact of the breach quickly. Automated correlation and normalization of events also decreases the time it takes an organization to respond to potential breaches. Manually correlating information is tedious and takes significant time and resources, and it limits the organization's ability to discover and respond to breaches. This enlarges the breach window and exposes the organization to greater risk and liability. In addition to accelerating the investigation and response process, automated correlation also eliminates human errors, delivering more accurate results.

SIEM and Log Management Considerations

SIEM and log management products can help health care organizations address their HIPAA and HITECH event monitoring, auditing and reporting requirements, including those dealing with meaningful use, accounting for disclosures and breach notification. Unfortunately, the majority of SIEM and log management solutions available on the market have serious, inherent deficiencies. Many are too complex and costly, which hinders an organization's ability to achieve compliance. Most solutions provide minimal support for diverse log formats, which prevents an organization from collecting log data from all the different systems and applications needed to address audit and compliance requirements. These solutions rely on non-secure communication protocols, which can put an organization in violation of compliance rules. They utilize proprietary data storage solutions that are difficult and costly to deploy and manage.

Most SIEM and log management solutions also lack the ability to expand to meet the future needs of growing organizations and evolving compliance requirements. As an organization's security and compliance requirements expand, these solutions fail to provide a path to or integration with what is needed for a complete, identity-aware SIEM environment.

The Novell Multi-Dimensional Approach to Compliance

Only Novell leverages its expertise in SIEM and identity management to deliver integrated SIEM, log management and identity management solutions that address the full-breadth of privacy and compliance concerns that health care organizations face. Novell® Sentinel™, Novell Sentinel Log Manager and Novell Identity Manager combine to deliver the multi-dimensional, integrated approach that health care organizations want and need. The Novell solutions address the operations, security, compliance, correlation and identity concerns unique to health care organizations striving to comply not only with HIPAA and HITECH, but other regulations such as SAMHSA, PCI, GLBA and COBIT.

Novell Sentinel

As a comprehensive SIEM solution, Novell Sentinel provides a real-time, holistic view of security and compliance health across any IT environment and from virtually any data source. It allows administrators to identify both external and internal security threats and compliance-related breaches of all kinds. With Sentinel, administrators can take immediate action to address weaknesses based on roles, regulatory requirements and business policies.

Novell Sentinel makes identifying, managing and reporting on security and compliance events in health care environments faster and easier. Through best-of-breed automation, correlation and workflow management, Sentinel can help health care providers reduce the cost of meeting compliance requirements. Novell Sentinel delivers real-time monitoring and remediation for automated security and compliance. With a single view of security and compliance events across the enterprise, Sentinel combines identity management and security events management for real-time results. Novell Sentinel also enables organizations to streamline labor-intensive, error-prone processes and cut costs through automation, enabling them to implement a rigorous and efficient security and compliance program.

Novell Sentinel Log Manager

Novell Sentinel Log Manager leverages Novell Sentinel technology for advanced and flexible log data collection, including out-of-the-box syslog support and native collection from other protocols. This makes it an ideal solution for collecting data from a wide variety of systems and applications, such as intrusion detection systems, firewalls, operating systems, routers, web servers, databases, switches, mainframes, antivirus event sources and more. It supports multiple secure communication protocols for data collection. It also automatically detects log sources.

To facilitate an organization's ability to comply with industry or government regulations, Novell Sentinel Log Manager provides the ability to intelligently collect, aggregate, store, analyze and manage the data logs from all of an organization's different systems and applications. It leverages the proven Novell Sentinel data integration framework with its broad set of data collectors for databases, operating systems, directories, firewalls, intrusion detection/prevention systems, antivirus applications, mainframes, web and application servers and more. The solution provides data indexing and one-click reporting to greatly simplify report generation for audit and compliance efforts. Its ability to mount archive data stores enables organizations to seamlessly query and report on both online and archived data, further simplifying and expediting compliance efforts.

Novell Sentinel Log Manager delivers out-of-the-box integration with the real-time monitoring capabilities of Novell Sentinel, as well as with Novell Compliance Management and Novell Identity and Access Management solutions. Novell Sentinel Log Manager

To facilitate an organization's ability to comply with industry or government regulations, Novell Sentinel Log Manager provides the ability to intelligently collect, aggregate, store, analyze and manage the data logs from all of an organization's different systems and applications.

When it comes to logging, monitoring, auditing, reviewing and addressing privacy and regulatory related events, Novell provides health care organizations a single view that lets them more easily, efficiently and cost-effectively address the full array of their compliance and security concerns.

www.novell.com

provides a clear roadmap to full identity-aware security in a way that lets health care organizations seamlessly add and integrate new capabilities as their security and compliance monitoring needs evolve. Novell Sentinel Log Manager leverages the expertise of Novell in security information and event management to deliver log management that simplifies compliance, saves money and provides a compliance and security foundation to build on as needs change and grow.

Addressing the Full Breadth of Health Care Compliance Concerns

Novell understands the challenges that health care providers face with HIPAA, HITECH and all the other security, privacy and compliance regulations. Rather than delivering a la carte compliance modules, Novell takes a multi-dimensional approach to health care compliance and security. Novell offers intelligent, integrated and identity-based SIEM and log management solutions that take into consideration the broad security and privacy landscape of the entire health care environment. When it comes to logging, monitoring, auditing, reviewing and addressing privacy and regulatory related events, Novell provides health care organizations a single view that lets them more easily, efficiently and cost-effectively address the full array of their compliance and security concerns.

Contact your local Novell Solutions Provider, or call Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA

Novell