

whitepaper

HIPAA Compliance: Meeting the Security Challenge

Eric Siebert
Author and vExpert

HIPAA Compliance: Meeting the Security Challenge

A Closer Look: The HIPAA Compliance Challenge -

As many IT managers and HIPAA Security Officers have already discovered, HIPAA compliance requirements are daunting.

The issues are so complex that some institutions have even taken a “wait and see” approach to HIPAA compliance. Unfortunately, this approach is no longer practical nor prudent.

The fact is that within a matter of months, you’ll be expected to demonstrate that your organization can detect, prevent, and respond to attacks, intrusions, or other system failures.

More specifically, the HIPAA security standard recognizes that information security must be comprehensive, but insists that no single tool, technology, or procedure is completely responsible for overall security.

The four elements that comprise the HIPAA--mandated security goal of “data integrity, confidentiality, and availability” can be summarized as follows:

- Administrative Procedures. Documented, formal practices that manage the selection and execution of security measures
- Physical Safeguards. Protection of computer systems and related buildings and equipment from hazards and intrusion
- Technical Security Services. Processes that protect and monitor information access
- Technical Security Mechanisms. Processes that prevent unauthorized access to data that is transmitted over a network.

Each of the HIPAA security goals has a number of tenets designed to fully implement the objective. Here are the tenets that are met or assisted by the implementation of the SolarWinds Log & Event Manager.

Administrative Procedures

Addresses the processes that allow access to, and protect, health information electronically maintained, transmitted, and/or received.

- Information access control
- Internal audit
- Security configuration management
- Security incident procedures
- Security management process

Physical Safeguards

- Measures to control the physical access to computer systems and facilities
- Assigned security responsibility
- Media controls
- Physical access controls

Technical Security Services

Protecting information as it is being processed or maintained

- Access control
- Audit controls
- Authorization control
- Data authentication
- Entity authentication

Technical Security Mechanisms

Guarding against unauthorized access to data transmitted over a network

- Communications/network controls

SolarWinds Capabilities

SolarWinds provides many of the features needed to meet or exceed HIPAA security standards compliance in the areas of administrative procedures, physical safeguards, technical security services, and technical security mechanisms.

Third Party Tool Integration

- Integrates best-of-breed security products and operating systems found in existing networks to increase their effectiveness
- Provides a security solution for coordinated protection from viruses, external and internal intrusions through the integration of multiple tools
- Increases your ROI on existing security infrastructure and provides a cohesive enterprise security solution
- Consolidates various individual security alerts and reports into a centralized system for automated analysis, response, and event correlation
- Integrates with native operating system tools
- Detects and reports security incidents from firewalls, intrusion detection systems (both network-based and host-based), anti-virus programs, and the operating system

Security Reporting and Audits

- Provides security reporting to facilitate readiness for internal and external audits
- Collects enterprise-wide threats and provides reports in multiple formats to provide a picture of security to both technical staff and non-technical management
- Detailed audit analysis from the network perimeter to the individual user
- Creates reports to document and track changes
- Securely maintains forensic data to preserve trail evidence
- Provides summary and detailed reports of consolidated enterprise-wide information:
 - Security Event Summary/Virus Events/Firewall Events
 - Host-Based Intrusion Detection System (IDS) Events
 - Network-Based IDS Events/Internal Security Events/Operating System Events/Notification Activities
 - Severity of Events
 - Events based on IP address

Policy-based Automated Responses and Notification

Rules-based engine, allows you to decide what security violations trigger an active response or an instantaneous notification

- Detects specific attacks and coordinates defensive actions to protect the entire network against repeated attacks
- Active response protects the enterprise at network speed (i.e. quarantine a single computer from the network when a virus is detected)
- Instantaneous notification of a security breach via email, on-screen pop-up message, cell phone text messaging, or pager

Network Monitoring and Control

- Centralized management console to view all security issues and tools across the network
- GUI that allows access to multiple SolarWinds appliances simultaneously
- Controls network access through policy definition and enforcement
- View and receive alert screen notifications from multiple locations
- Aggregate security events and audit trail activities, from numerous devices, into one easily managed database on a secure network appliance
- Vastly improves IT administration efficiency

SolarWinds provides just what you're looking for - Real-Time Threat Analysis and Automated Remediation

SolarWinds Log & Event Manager was created for an important purpose - to assist system administrators grappling with the task of monitoring existing security tools and the increasing complexity and volume of security threats.

SolarWinds can help you with HIPAA compliance because it's designed as an overlay to existing best-of-breed security products (firewalls, anti-virus programs, intrusion detection systems, etc.), as well as the operating system.

You see, SolarWinds "wraps" them and collects the data from each of these tools in real time, and aggregates, correlates, filters, and integrates this data into data into a centralized control console.

SolarWinds then provides instantaneous alerts, both on-screen and via cell phones, pagers and/or email, if an important system security event is detected.

SolarWinds is unique in its ability to actively and instantly respond to these critical security events, stopping them at network speed, before they cause widespread damage or significant loss.

Plus, SolarWinds generates the detailed audit trail reports needed by your IT staff, auditors and regulators. These reports will help you clearly demonstrate your commitment to event analysis, notification and remediation.

You're protected by 

The name of our patent-pending technology is drawn from the fifth article of the NATO alliance. It states: "An attack on one, is an attack on all."

NATO5 is the result of nearly six years of research conducted at one of the top security institutes in the nation. This breakthrough research was conducted on behalf of numerous government agencies including the NSA, NASA, Army, Air Force, and the National Science Foundation. The result is an unprecedented solution to network security threats.

Protection through coordination

With NATO5 protection, your firewall, intrusion detection system, and anti-virus software can finally communicate and coordinate responses to both internal and external attacks.

In essence, NATO5 creates a defensive shield that envelopes and secures the entire network. An attack on any server, node, or appliance is seen as an attack on all, and the NATO5 response is swift and complete.

- **EXAMPLE:** If a serious virus is detected on a workstation in the network, the system administrator is instantly notified, and the infected workstation can be automatically quarantined off the network. As a result, the virus is contained and the network is protected from further infection and downtime.

SolarWinds also provides custom reports that enable system administrators to meet regulatory requirements and identify trouble spots and trends in network activity. What's more, you can dramatically increase the ROI of your current security investment by integrating your tools into the SolarWinds management console. This provides you with a single, simple access point into your corporate security environment.

Two Important facts you should know

FACT #1: Perimeter security is simply not enough. It has become clear that having a firewall does not mean your network is secure. A firewall is an imperfect defense against hostile outsiders and it does absolutely nothing to protect against internal threats.

FACT #2: According to the FBI and a Computer Security Institute study, 60% of successful intrusions and security breaches happen from the inside.

To help you meet these threats, SolarWinds extends the capabilities of your firewall, corporate anti-virus, and intrusion detection system by fully integrating these tools and others, into a unified security system - a system that prevents attacks through coordinated defensive actions. SolarWinds also isolates and secures all log data, so that in the event of an intrusion, you'll have the analysis capability to know precisely what occurred.

Check out with the SolarWinds product line has to offer

- Integrates existing best-of-breed third party security tools and operating systems into a single cohesive system
- Provides a security solution for coordinated protection from viruses, external and internal intrusions through the integration of multiple tools
- Increases your ROI on existing security infrastructure and provides a unified enterprise security solution
- Monitors computer security remotely, and in network time
- Consolidates various individual security alerts and reports into a centralized system for automated analysis, response, and event correlation
- Provides detailed security event and activity reporting to facilitate readiness for internal and external audits

- Collects enterprise-wide threats and provides reports in multiple formats to provide a picture of security to both technical staff and non-technical management
- Detects specific attacks and coordinates defensive actions to protect the entire network against repeated attacks
- Hierarchical architecture provides additional layer of management and administration from remote locations. Allows you to watch security at clinics and urgent care facilities from a centralized IT department
- Rules-based engine, allows you to decide what security violations trigger an active response or an instantaneous notification
- Active response protects the network at electronic speeds
- Instantaneous notification of a security breach via email, on-screen pop-up message, cell phone text messaging, or pager
- Centralized management view of all security issues and tools across the network
- GUI that allows access to multiple SolarWinds appliances simultaneously
- View and receive alert screen notifications from multiple locations
- Reduces exposure to and increases detection of unauthorized network changes

HIPAA Compliance - a final word

If you are struggling to comply with HIPAA regulations, or are simply looking for a better way to secure your network, we can help.

You see, the SolarWinds Log & Event Manager greatly simplifies network management and monitoring. The sense of control you'll get when you use SolarWinds is immediate and liberating. Once your network security has been centralized, you'll find that your HIPAA auditing, reporting, and certification procedures will be dramatically easier.

Please remember...the SolarWinds security system is a comprehensive solution to many of the computer security problems facing healthcare institutions that are trying to defend their networks and implement HIPAA regulations.

SolarWinds was designed to help keep your data secure, and allows administrators to take action against would-be intruders. It also permits coordinated, active responses against attacks, and reports violations in real-time to a centralized console.

SolarWinds unique NATO5 protection turns your existing network security tools into a powerful defensive shield. That's because it combines the power of your firewall with the intelligence of your IDS, anti-virus software and operating system. The result is a truly formidable defense to both internal and external attacks. It is a solution that improves the return on investment (ROI) on your existing computer security devices and allows your system administration staff to be more efficient by providing a state-of-the-art monitoring, actions, and alerting system that spans your entire enterprise.

As you prepare to meet HIPAA regulations and examine your existing (or proposed) network security infrastructure, ask yourself this question: "Can I really detect, prevent and respond to attacks?" If you're in any doubt, let us show you how SolarWinds will help make you HIPAA Compliance easier than you ever thought possible.

Let us prove it - Give us a call, or register online, and join us for a live presentation where you can see SolarWinds in action under real-world conditions. Watch as we capture, correlate and respond to network attacks and policy violations - all in real-time. See SolarWinds for yourself, and find out what's in your network.

About the Author

Eric Siebert is an IT industry veteran, author and blogger with more than 25 years of experience, most recently specializing in server administration and virtualization.

Siebert has published books, including his most recent, Maximum vSphere from Pearson Publishing and has authored training videos in the Train Signal Pro series. He also maintains his own VMware information web site, vSphere-land.com, and is a regular blogger and feature article contributor on TechTarget's SearchServerVirtualization and SearchVMware web sites. Siebert has presented at VMworld in 2008 and 2010 and has been recognized as a vExpert by VMware in 2009 and 2010.

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide - from Fortune 500 enterprises to small businesses. The company works to put its users first and remove the obstacles that have become "status quo" in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users' management priorities. SolarWinds online user community, <http://thwack.com>, is a gathering-place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of the company's products. Learn more today at <http://solarwinds.com>.

For additional information, please contact SolarWinds at 866.530.8100 or e-mail sales@solarwinds.com. To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx

Did you like this white paper? Tweet about it.  <http://www.twitter.com>