

whitepaper

GLBA: How SolarWinds Ensures Compliance and Provides Proactive, Real Time Protection

Eric Siebert
Author and vExpert



GLBA: How SolarWinds Ensures Compliance and Provides Proactive, Real Time Protection

Banks and Financial institutions have a responsibility to their customers and investors to ensure all personal and financial information is protected. The "Gramm-Leach-Bliley Act" or GLBA was created by Congress in 1979 to mandate and enforce effective safeguards for personally identifiable information (PII). GLBA defines "customer information" as any record containing non-public personal information about a customer of a financial institution. The regulation impacts a broad spectrum of organizations including banks, brokerages, investment companies, insurance companies, service providers, and many others, irrespective of size.

GLBA requires financial institutions to provide administrative, technical, and physical safeguards to:

- Ensure the security and confidentiality of customer records and information;
- Protect against any threats or hazards to the security or integrity of such records;
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

To ensure compliance, Congress mandated substantial penalties should customer information become exposed. These penalties include a corporate penalty of up to \$100,000 per event and personal liability by company officers and directors of up to \$10,000 per event. Even more ominous, a regulatory finding of non-compliance opens the company up to the risk of litigation that can cost millions of dollars.

At its core, GLBA requires each financial institution to "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks."

In other words, simply correcting and reporting security breaches after an attack is no longer sufficient; financial organizations must take proactive steps to prevent unauthorized access to PII. More specifically, GLBA identified three topics of particular concern:

- Prevention and response measures for attacks, intrusions, or other systems failures;
- Information systems, including information processing, storage, transmission and disposal; and
- Employee training and management

Although GLBA requirements remain unchanged, the security environment is dramatically more complex and dangerous

Since the passage of GLBA, the volume and sophistication of internal and external threats have both grown to dangerous levels. Numerous studies by government and private organizations have documented a severe increase in the variety of attacks. For example, Symantec detected over 400,000 new malicious codes in just one quarter. Even worse, today's attacks frequently target a

particular company and involve a blend of advanced techniques that make prevention and detection extremely difficult. Such attacks may occur at the perimeter, at the PC, or anywhere in between. Even portable memory devices can be a threat. As a consequence, security practices and technologies that may have been adequate 2-3 years ago are now dangerously obsolete.

Not surprisingly, there has been a growing list of other statutes at the state and Federal level that require the protection of private personal information. For example, many states now require that organizations notify individuals whose PII may have been exposed. The need for increased security has also resulted in private sector standards that build on GLBA principles. For example, Payment Card Industry (PCI) standards impose very specific requirements to protect credit and debit card transactions. Yet PCI compliance was not sufficient to prevent some of the largest breaches in history at TJX and at Heartland Payment Systems that resulted in tens of millions of dollars of fines and restitution.

GLBA and the Need for Security Information and Event Management

Today organizations must comply with multiple, overlapping regulatory systems, while simultaneously detecting and evading a mounting barrage of sophisticated attacks. An effective security program, therefore, requires a variety of different tools including firewalls, anti-malware, intrusion detection, and data leakage prevention, each with its own set of logs and reports. But multiple security products present their own problem - system administrators simply lack the time and skills to correlate all of the data flowing from the logs of multiple different security devices in order to spot devious attacks.

Mid-size companies are particularly vulnerable in this regard as they represent an attractive target but often lack the resources to have a dedicated security staff within their IT department. Like large companies, they need comprehensive coverage and 24/7 monitoring, but unlike the bigger firms, cannot afford to have people who simply watch dashboards for trouble.

Security Information and Event Management (SIEM) technology responds to this need by providing the ability to centralize the management of security information. SIEM systems collect data from a wide variety of security devices and consolidate the log information to provide comprehensive activity and status reports. Most SIEM products also provide a dashboard that shows if a system is out of compliance or if an event has occurred that is outside of policies or looks suspicious.

Unfortunately, conventional SIEM systems are problematic for mid-size companies in two respects. First, they are passive, forensic-oriented systems that can only provide an alert after something has happened - there is no ability to prevent an attack from succeeding. Second, with respect to mid-size companies, SIEM products are often very complex to install, maintain and to use. They require full-time attention from skilled operators who must have product-specific training.

SolarWinds Goes Beyond "After the Fact" Forensics to Provide Proactive Network Defense

SolarWinds is the only SIEM designed and built to proactively defend the network. The key is real-time event analysis, combined with patented, in-memory, correlation. SolarWinds real-time event correlation engine helps midmarket IT professionals identify the "incident" needle in the haystack of log data, while automating policy creation and providing reports that prove compliance.

Additionally, SolarWinds SIEM enables IT and security teams to go well beyond the forensic functionality of traditional log management products and leverage the data that is collected for prevention. SolarWinds is the pioneer of using this data for proactive network defense to specifically address the GLBA requirement for "Prevention and Response measures for attacks, intrusions, and other systems failures."

Unlike some intrusion prevention systems that shut everything down when a problem is spotted, SolarWinds intelligent architecture allows for an appropriate, targeted response. When an attack is confirmed, SolarWinds automatically responds by actively quarantining, blocking, or disabling devices.

How SolarWinds SIEM addresses GLBA Requirements

The core objective of GLBA is to protect customer data from compromise.

Unfortunately, today massive amounts of data can be lost almost instantly. Consequently, to be GLBA compliant, financial organizations must move from simply detecting attacks after-the-fact (the forensics approach) to proactively shutting down attacks before they cause damage. Prevention is much more effective and less expensive than reaction, system restoration and customer notifications.

SolarWinds is the only SIEM solution that provides real-time log analysis to identify network attacks and policy violations as they happen, and that initiates proactive responses such as quarantining, blocking, and USB device defense. In contrast, most SIEMS simply watch the network, collect information and send out notices. This is inadequate for GLBA compliance because even a minute or two of delay can allow data to be stolen and attacks to proliferate throughout the network.

GLBA Requires Comprehensive Network Coverage - Wherever Private Data is Located

The size or type of device where data is stored is irrelevant to GLBA - appropriate safeguards need to be in place to protect all access to PII. This requirement includes everything in the network that has to do with security, or with storing or transmitting PII, including portable memory devices.

SolarWinds provides true "perimeter to PC" coverage by consolidating and analyzing log data from an expanding list of industry leading firewalls, anti-virus software, intrusion detection, operating systems, and even USB memory sticks. SolarWinds can even provide alerts if other security products, such as anti-virus protection, cease functioning and automatically restart those services to ensure continuous protection. Because SolarWinds comprehensive solution prevents unauthorized access to privileged information, there is an unbroken "chain of custody" so that offenders can be prosecuted.

GLBA requires each financial institution to "design and implement information safeguards to control the risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures."

SolarWinds addresses this requirement by centralizing visibility into the security of the environment. Utilizing SolarWinds behavioral analysis, businesses can use SIEM to continuously monitor the network and generate real-time status information that will help IT teams constantly adjust and adapt the security plan to an ever-changing landscape.

A critical feature of SolarWinds technology is the ability to add or modify rules swiftly to meet GLBA requirements for modifying security measures as conditions change. To facilitate the frequent testing that GLBA strongly suggests, SolarWinds administrators can create and test rules without triggering the pre-set Active Response actions.

GLBA requires continuous network monitoring to protect PII at rest or in motion.

SolarWinds security information manager enables mid-tier companies to monitor information security by giving IT staff complete visibility into the sea of activity happening on their network. The solution is backed up by real-time Active Response that blocks or mitigates internal and external threats and

policy violations. All of SolarWinds analysis is performed in-memory, and at network speeds to provide the continuous network monitoring necessary to reveal threatening or malicious activity.

Firewalls, routers, switches, IDS, IPS, VPN, anti-virus software and servers all produce enormous amounts of log data, but assimilating and understanding this information to identify problems is a huge and complex task. SolarWinds uses a combination of proprietary agent technology and backbone integration to capture and centralize log data from the perimeter to the endpoint. SolarWinds "event-centric" normalization and correlation process then analyzes network events in depth to detect new and sophisticated attacks.

GLBA requires the Board of Directors or other management personnel to assess risks and create and enact an appropriate security program.

Senior managers are frequently unable to determine if security policies have been effectively deployed into the organization and if the policies are actively being enforced. SolarWinds advanced, in-memory correlation engine bridges the gap between senior management and security administrators by making policy implementation easy to visualize and understand. In essence SolarWinds helps translate security policies by the Board of Directors or other senior managers into a comprehensive set of rules that enable practical and effective information security.

Only SolarWinds offers real-time, in-memory correlation across every device connected to the network - a crucial capability that helps businesses instantly identify and actively respond to abnormal network activity or policy violations. Correlation is a process that creates a "big picture" understanding by evaluating the significance of one event in relationship to all other events to determine whether suspicious or out-of-policy actions have taken place. An excellent example is a sophisticated "worm" that exhibits several seemingly innocuous behaviors. Under certain circumstances these "individual" behaviors could go unnoticed; however, when those behaviors are properly correlated the worm can be clearly recognized and blocked.

SolarWinds is the first SIEM product to use 64 bit, in-memory event correlation that is not subject to the inherent limitation of database or disk based correlation techniques. This high-speed architecture is required to prevent lightning attacks from succeeding. For faster implementation, SolarWinds comes stocked with more than 700 security and network monitoring correlation rules. Businesses can also develop and customize their own rules and reports to fit very specific requirements.

GLBA emphasizes the need for an Incident Response Plan that determines what the organization will do in the event of a breach, and who is responsible for taking certain actions.

SolarWinds Active Response and automatic notification capabilities ease the implementation of an incident response plan by ensuring that when a potential problem is identified, action is automatically taken and the appropriate people are immediately notified, regardless of their location. To keep everyone informed, security managers can implement as many SolarWinds roles-based administration consoles as desired, and each console can be customized for the particular administrator. SolarWinds administration architecture enables mid-sized companies to delegate various responsibilities to different people so that there is a clear delineation of duties.

When an event requires an action, predetermined notification rules are executed instantly - providing critical event details such as when and where the event occurred. SolarWinds easy-to-use, real-time correlation technology gives users an opportunity to customize and "tune" both rules and responses to help eliminate frequent "false positives" or unnecessary account lockouts.

GLBA not only requires that networks be secure, but clear and irrefutable proof that they have been maintained in a secure state over time.

Proving compliance is totally impractical if logs have not been consolidated and analyzed in advance. SolarWinds constant analysis of log data helps IT teams become proactive by detecting and mitigating network and security events in real-time. Automated notification and reporting provides an easy method of providing proof of continuous network and security analysis.

Examiners have the latitude to ask for a wide variety of reports that are expensive and difficult to produce manually. SolarWinds SIM comes prepackaged with more than 300 reports - including specific reports for GLBA compliance and network analysis that expedite access to the data that examiners may require.

SolarWinds provides Inexpensive and Effective Employee Management and Training Capabilities.

An important part of any security program is educating users about how to use the network safely. With SolarWinds, network users who attempt to violate company policies are stopped and receive an instant notification that explains why they were stopped. Meanwhile, IT teams can be notified of the violation and look for patterns that may suggest a need for additional training. This combination of training and deterrence is precisely what GLBA requires. SolarWinds provides rapid deployment with zero downtime. The technology is designed to be a turnkey solution that minimizes the impact on IT resources. SolarWinds training program is streamlined, does not require onsite presence, and helps IT teams quickly tune the SIEM to meet the specific requirements of their environment. The solution extends midmarket IT departments by acting like another set of eyes and hands on the network.

GLBA Responsibility Includes Protecting Data Sent to Service Providers.

SolarWinds "white listing" capability ensures that data is only transferred to servers that are known to belong to trusted partners. Should a suspicious transfer of data be detected, SolarWinds Active Response technology will immediately stop the activity.

Summary

The high-level mandates of GLBA to protect private customer information are becoming increasingly difficult to fulfill for midmarket businesses, given the rapidly mounting volume of complex targeted attacks with limited ability to increase security staff or expertise. Forensics are not enough. Midmarket businesses can't afford to simply collect log data and make adjustments to security policy because it doesn't prevent customer data from being lost.

Midmarket companies need SIEM solutions that leverage their security staff through automated information collection and analysis. Effective and "provable" defense requires real-time event correlation to detect policy violations coupled with automatic and appropriate responses. SolarWinds real-time, in-memory event correlation enables proactive network defense from perimeter to PC and includes monitoring and controlling USB storage device usage. Natural language rule setting and alerts, coupled with clear GLBA compliance reports give senior management and auditors confidence that GLBA requirements have been met.

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 more than 97,000 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>