

Refense VMS™

Ensuring a GLBA Compliant Network

Overview

In our age of network access anytime and anywhere, organizations within the financial industry must take action to secure their network infrastructure in order to protect the confidential financial information that they store, transmit, and receive. This isn't just a security best practice, it is federally mandated through the Gramm-Leach-Bliley Act (GLBA). GLBA, among other things, mandates the privacy and security of sensitive information from the various threats and vulnerabilities associated with information management. As it relates to the security of network devices, the GLBA requirements are comprised of a set of information security best practices including:

- Risk assessment to determine which systems, devices, applications and data are vulnerable
- Implementation of proper authentication, access control, and logging systems
- Ongoing auditing of information systems to test for newly discovered vulnerabilities

In summary, financial institutions must comply with the GLBA regulations now and ensure continued compliance in order to effectively protect sensitive information and help prevent legal liabilities. In addition, any business partners or service providers of financial institutions must have adequate safeguards in place to protect sensitive information while it's in their possession

Verifying and Maintaining GLBA Compliance

Detecting vulnerabilities and verifying the implementation of logging systems and authentication across thousands of network devices is a tedious and difficult, if not an impossible task. However this task is vital for compliance with the GLBA regulations and to ensure a strong security posture.

Refense VMS provides an scalable, automated method of managing vulnerabilities within network devices. Refense VMS provides financial organizations the ability to quickly determine the vulnerabilities and if proper authentication, access controls, logging systems have been implemented within network devices.

Refense VMS assists in GLBA compliance by:

- Validating the implementation not only of logging, but a sufficient, secure logging level
- Detecting vulnerabilities within common and market leading network devices
- Verifying the implementation of security access control measures
- Performing regular scheduled scans for the continual process of auditing network devices



About Refense

Refense Technologies is a leading provider of vulnerability management solutions for network devices. The company develops solutions that address security concerns within network devices, the foundation of an IT infrastructure. With Refense VMS, organizations can proactively identify and mitigate threats and vulnerabilities within wireless and wired network devices.



Refense Technologies, Inc
105 Brooks Ave
Raleigh, NC 27607
Phone 1.888.792.7892
sales@refense.com
www.refense.com

The following table outlines how Refense VMS can automate the key compliance requirements associated with GLBA:

GLBA Compliance	
KEY GLBA REQUIREMENTS	REFENSE VMS CAPABILITIES
Assessing Risk	Refense VMS delivers the industry's most accurate network security audits with the largest database of vulnerability and configuration checks
Manage and Control Risk	With Refense VMS , Companies can prioritize remediation efforts and manage risk based on asset value and key compliance objectives
Oversee Service Provider Arrangements	Refense VMS makes it convenient to verify that third-party affiliates, subsidiaries and service providers are GLBA compliant by supporting on demand security audits that are time/date stamped, anytime, anywhere.
Adjust the Program	The highly flexible and distributed nature of Refense VMS's appliance/agent-less solution gives organization the ability to modify policies across the entire enterprise as needed.
Report to Board	Refense VMS executive reports provide a high-level snapshot with trend analysis of an organization's network security posture and business risk