



FORTINET WHITEPAPER

SECURING YOUR NETWORK TO ENSURE THE INTEGRITY OF CONSUMER FINANCIAL DATA AND GLBA COMPLIANCE

FORTINETTM
REAL TIME NETWORK PROTECTION

www.fortinet.com

Contents:

OVERVIEW	Page 3
THE PROBLEM	Page 4
SOLVING THE PROBLEM OF BUSINESS ADHERENCE TO BROADLY-APPLICABLE FINANCIAL INSTITUTION REGULATIONS	Page 4
ONSLAUGHT OF REGULATORY REQUIREMENTS, OPEN TO INTERPRETATION	Page 4
INCREASING THREATS, INCREASING REGULATION	Page 5
TRADITIONAL NETWORK SECURITY SOLUTIONS INADEQUATE	Page 6
REQUIRE SOPHISTICATED IDS/IPS	Page 6
SOLUTIONS MUST ADDRESS FUTURE THREATS AND INCREASED REGULATION	Page 7
THE PROBLEM IN SUMMARY	Page 7
THE SOLUTION	Page 8
THE SOLUTION INVOLVES FIRST ASSESSING THE RISK	Page 8
REAL TIME COMPLETE NETWORK PROTECTION IS REQUIRED	Page 8
FULL NETWORK SECURITY INCLUDED	Page 10
AUTOMATIC, REAL-TIME RESPONSE TO NEW ATTACKS	Page 10
COMPLETE REAL TIME PROTECTION SOLUTION	Page 11
BUYING VS. SUBSCRIBING TO SECURE NETWORKS: MSSP AS A SOLUTION	Page 12
CONCLUSIONS	Page 13
ABOUT FORTINET	Page 14

OVERVIEW

>> With the onslaught of email, browser, and application vulnerabilities growing daily, the sources of attacks threatening corporate resources are coming from every direction

Organizations of all types and varying sizes are experiencing a significant escalation in the quantity and severity of cyber-attacks. These attacks are becoming increasingly blended, sophisticated and more difficult to intercept. At the same time, organizations are working to halt threats at the perimeter of their networks instead of relying on detect-and-destroy processes. Attacks are no longer coming from just external sources. With the onslaught of email, browser, and application vulnerabilities growing daily, the sources of attacks threatening corporate resources are coming from every direction, including the Internet, the internal network, and remote mobile employees and partners. Further complicating efforts to improve network security is the emergence of applications such as enterprise VoIP and the popularity of 802.11 wireless networks and applications.

Those organizations handling consumers' financial data have the additional challenge of being compliant with security and privacy regulations imposed by the Gramm-Leach-Bliley Act (GLBA). Companies that handle such data - for example, accountants, auto dealers and travel agents - may not be aware that these regulations, previously applicable only to traditional financial institutions, apply to them as well. As a result, a wide range of companies that have relationships with other companies where consumer financial data is exchanged are essentially responsible as "financial institutions" for compliance with GLBA regulations.

New network security products are available that help protect the corporate network at its continually changing perimeter, by identifying and preventing malicious blended security threats coming from both external and internal sources. Security platforms using ASIC engines can go well beyond traditional network protection provided by traditional firewalls and stand-alone Intrusion Detection Systems (IDS), and protect the network from both viral and worm-based attacks propagated via email and web traffic. Protecting the business network and infrastructure is critical for ensuring the security and privacy of consumer financial data and bringing an organization into compliance with GLBA regulations.

Fortinet's FortiGate™ series of ASIC-accelerated gateway antivirus firewalls are the newest generation of real-time network protection systems. They combine a number of security functions to detect and eliminate the most damaging, content-based threats from e-mail and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time - without degrading network performance. FortiGate appliance systems perform traditional network protection and security functions as well, including ASIC-based gateway antivirus, firewall, VPN, anti-spam and traffic shaping capabilities. The FortiProtect™ Network service automatically and instantly updates FortiGate antivirus firewall systems worldwide to provide detection for the newest attacks. IT professionals can implement FortiGate systems at the perimeter as well as

critical choke-points where deep packet inspection and complete content protection are required - such as high security server farms and critical departmental subnets.

THE PROBLEM

SOLVING THE PROBLEM OF BUSINESS ADHERENCE TO BROADLY-APPLICABLE FINANCIAL INSTITUTION REGULATIONS

>> In May 2003, auto dealers, accountants, travel agents and other businesses not previously subject to GLBA regulation were identified as "financial institutions" and therefore required to come into compliance or face fines up to \$11,000 per day from the Federal Trade Commission (FTC)

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" (GLBA) requires that financial institutions protect consumers' personal financial information. The GLBA Financial Privacy Rule and the Safeguards Rule apply to a wide range of businesses that handle financial products and provide services to consumers.

In May 2003, auto dealers, accountants, travel agents and other businesses not previously subject to GLBA regulation were identified as "financial institutions" and therefore required to come into compliance or face fines up to \$11,000 per day from the Federal Trade Commission (FTC). The FTC has the option to declare each day of non-compliance as a separate violation going back to the 2003 effective date. This creates the potential for million dollar fines for small to medium size businesses including auto dealers and their financial service providers.

Further, being out-of-compliance could jeopardize business relationships between service providers and the non-compliant business customers.

ONSLAUGHT OF REGULATORY REQUIREMENTS, OPEN TO INTERPRETATION

The GLBA requirements are stated at a high level, and are part of larger body of regulations and practices that affect the security of financial information. In surveying financial institutions, Deloitte's 2004 Global Security Survey characterizes the situation as an "onslaught of regulatory requirements", with "many of them open to interpretation" and "global financial institutions ... doing their best to adopt better practices and security standards".

The GLBA regulations state the following:

"...You shall develop, implement, and maintain a comprehensive information security program that is ...appropriate to your size..."

Unfortunately, the FTC does not provide detail on what the information security program needs to include. The FTC does, however, outline compliant program requirements:

"(a) Designate an employee or employees to coordinate your information

>> *Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness....*

security program.

(b) Identify reasonably foreseeable internal and external risks ... At a minimum, such a risk assessment should include

(1) Employee training and management;

(2) Information systems, ...

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness....

(d) Oversee service providers, ...

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section..."

Of these requirements, two are particularly difficult to achieve without the addition of multi-purpose security appliances:

- Conducting a risk assessment that identifies all "reasonably foreseeable internal and external risks..."
- Monitoring the system effectiveness and "detecting, preventing and responding to attacks, intrusions or other..."

Additional regulations include the ISO 17799 standard for information security, regulations from the Office of the Comptroller of the Currency (OCC) and guidelines from National Institute of Standards and Technology (NIST). Performing the necessary risk assessment and wading through the regulations to identify actionable security solutions is a challenge to experienced financial institutions, and even more so to those organizations newly identified as having to comply with GLBA and associated regulations and guidelines.

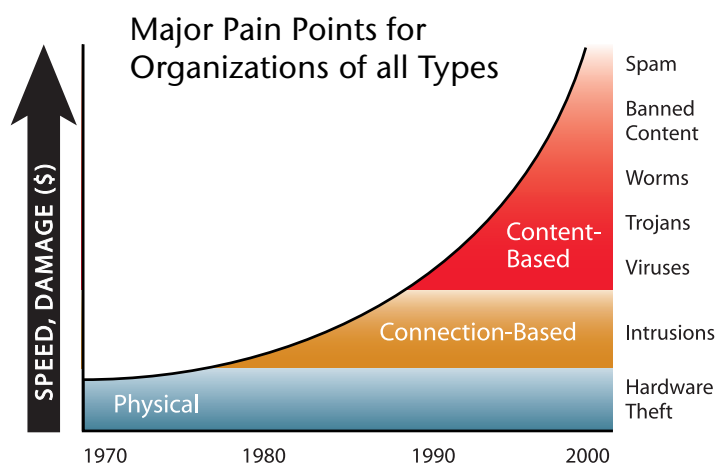
INCREASING THREATS, INCREASING REGULATION

At the same time that the quantity of attacks is increasing, they are becoming increasingly sophisticated as well. Light Reading Insider (June 2004) states: "The sophistication of threats is rapidly evolving and their ease of launch is increasing...the cost of such attacks is high: ...estimates the worldwide impact of attacks has grown from \$3.3 billion in 1997 to \$ 12 billion in 2003."

The nature of the threat has also evolved, as diagramed in the figure below. Today, the most damaging and sophisticated attacks leverage blended content. Unlike connection-based attacks, blended content-based attacks don't require sustained connections in order to cause damage. Once a virus or worm has been inserted into a network or computer, it can act on its own and spread. Without the ability to apply a combination of security functions like IDS/IDP, gateway antivirus and firewalling to the threat, it can often bypass single functions undetected. The big challenge with content-based threats is that they are almost always delivered using connections that are inherently trusted - like

>> *The need for additional security was made more explicit in January 2004 with the NIST requirement that states "Continually monitoring threats through intrusion detection systems (IDSs) and other mechanisms is essential"*

email and Web traffic. Deloitte found that 70% of respondents to their survey rated viruses and worms as a high intensity threat ^v.



And these newest vulnerabilities won't be the last. Frost and Sullivan in their 2003 report "World Managed Security Service Provider Markets" expects "ceaseless discovery of new vulnerabilities" through at least 2009. And along with this will be continued "regulatory pressure demanding security".

TRADITIONAL NETWORK SECURITY SOLUTIONS INADEQUATE

Traditionally, networks use stand-alone IDS/IDP systems, software-based firewalls or anti-virus add-ons to provide security. However, a conventional firewall at the network perimeter only protects against connection-based attacks. Allowing content-based attacks to penetrate into the network and then arresting them at the server or desktop PC is no longer acceptable. As businesses become more global, security must now reach further to ensure that corporate resources are protected from all sources of corporate information access.

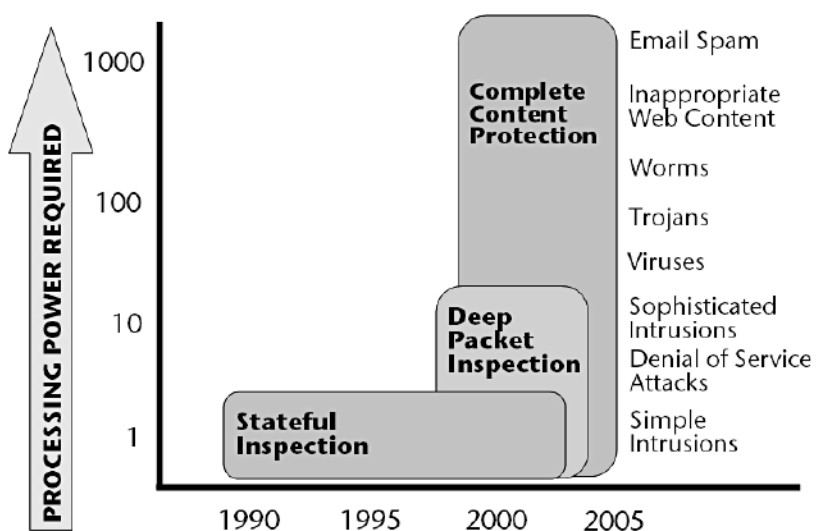
As such, reliance on a standard firewall at the network perimeter can no longer be considered to provide "reasonable" protection. In May of 2000, the OCC informed banks that "management should consider additional security behind the firewall, such as intrusion detection". The need for additional security was made more explicit in January 2004 with the NIST requirement that states "Continually monitoring threats through intrusion detection systems (IDSs) and other mechanisms is essential".

Demonstrating the ease with which attackers could attack today's networks, 83% of the Deloitte Survey respondents acknowledged their systems had been compromised last year. The threats were of both internal and external origin.

REQUIRE SOPHISTICATED IDS/IPS

Most current generation firewalls use stateful inspection and, some more recently use deep packet inspection to address a portion of today's threats.

However, these older technologies are insufficient to detect and eliminate more serious and pervasive threats such as viruses, worms, Trojans, and the like. But as shown in the figure below, detecting and preventing viruses, worms Trojans and other content based attacks requires enormous processing power. As a result, it has been difficult until now to field network-based solutions that can address these threats and still provide adequate network performance. Recent advances in security technology have now made possible powerful, ASIC-based systems that combine antivirus, firewall and IDS/IPS functionality, thereby providing complete security without compromising performance.



SOLUTIONS MUST ADDRESS FUTURE THREATS AND INCREASED REGULATION

While there may not be clear guidelines as to exactly what level of protection is required and what type of threat that must be handled, at the same time, any solution put in place must address the very real problem of blended threats that a single security function system will be unable to prevent. A combined approach to security that delivers high performance in a combined solution with IDS/IDP, antivirus and firewalling functionality will help all size companies halt the advance of blended threats. These types of threats are increasing in frequency and sophistication and are expected to do so for the foreseeable future. The system must have the flexibility to handle new types of threats in the future as they are discovered, and the capability for automatic, real-time updates to detect and stop new attacks in process.

THE PROBLEM IN SUMMARY

- Extension of GLBA regulations to cover all companies handling consumer financial information.
- Onslaught of regulatory requirements, open to interpretation, not directly actionable.
- Increasing threats.

>> *The challenge in doing this assessment is dealing with the lack of regulatory guidance provided by GLBA. However, further guidance is found in standards and guidelines available from NIST.*

- Traditional network solutions not adequate.
- Sophisticated solutions are required that protect against content-based attacks as well as connection-based attacks without compromising performance
- Solutions must be extensible and rapidly updated to address future threats.

THE SOLUTION

THE SOLUTION INVOLVES FIRST ASSESSING THE RISK

Prior to implementing a compliance program, organizations typically perform a security risk assessment to determine how and where to best spend their security dollars.

The challenge in doing this assessment is dealing with the lack of regulatory guidance provided by GLBA. However, further guidance is found in standards and guidelines available from NIST.

Commercially available software products draw from this complex regulatory framework to create assessment templates, methods and procedures that are used by organizations required to comply with GLBA. One such product is the GLBA Compliance Kit™ from MDi Network Security Systems, Atlanta, GA (www.mdisecurity.com). A section showing the top 5 threats from a typical risk analysis table taken from the MDi compliance software package is shown below.

Threat Source	Vulnerability	Likelihood	Impact	Score
Malicious insider	Data retrieval	Medium	high	50
Malicious insider	Procedure implementation	Medium	high	50
Malicious insider	Internal controls	Medium	high	50
Malicious insider	Data acquisition	Low	high	25
Malicious insider	Data storage	Low	high	25
Malicious insider	Data modification	Low	high	25
Malicious outsider	Data storage	Low	high	25
Malicious outsider	Procedure implementation	Low	high	25
Malicious outsider	Internal controls	Low	high	25

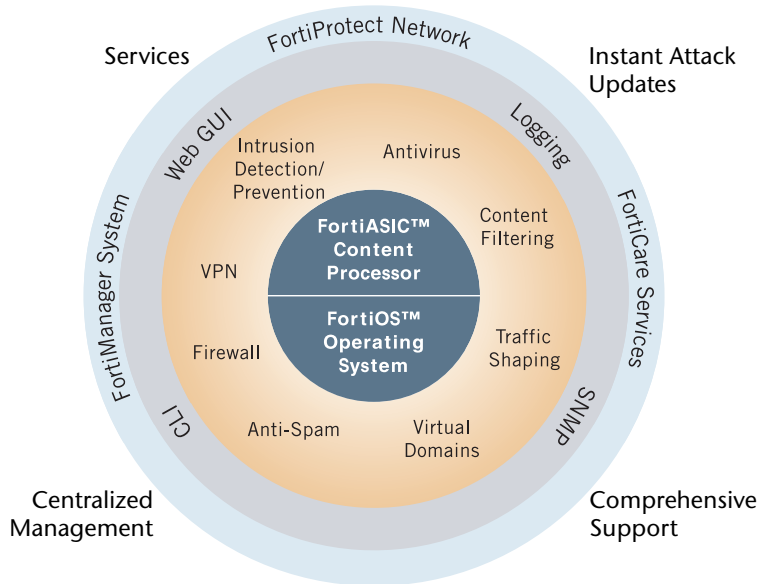
More organizations are deciding to install the best available solutions. The Deloitte Study shows that a higher percentage of respondents in 2004 compared to 2003 wanted to be "world class and bullet proof".

REAL TIME COMPLETE NETWORK PROTECTION IS REQUIRED

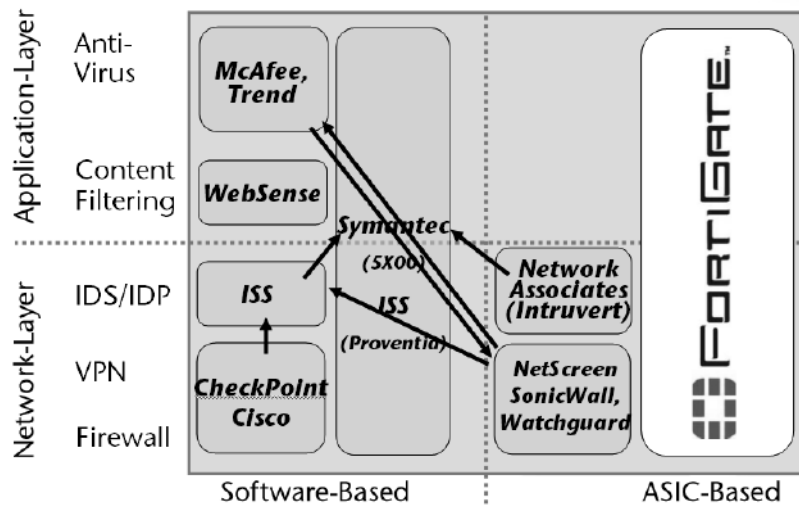
All content entering and leaving the network must be scanned and analyzed in real time to prevent disruption of existing network applications, support financial transactions, web and email services, and also to support future real-time

applications such as VoIP.

To provide true content-based threat protection at the network perimeter requires a hardware-based solution that can provide the processing power needed to completely analyze traffic without degrading application performance. Fortinet's FortiGate Antivirus Firewalls were designed to meet these stringent requirements. Based on the proprietary FortiASIC™ Content Processor, which includes an intelligent content scanning engine, FortiGate systems readily handle the computationally-intensive operations required to provide antivirus, firewall, VPN and IDS/IDP capabilities in a single, integrated system.

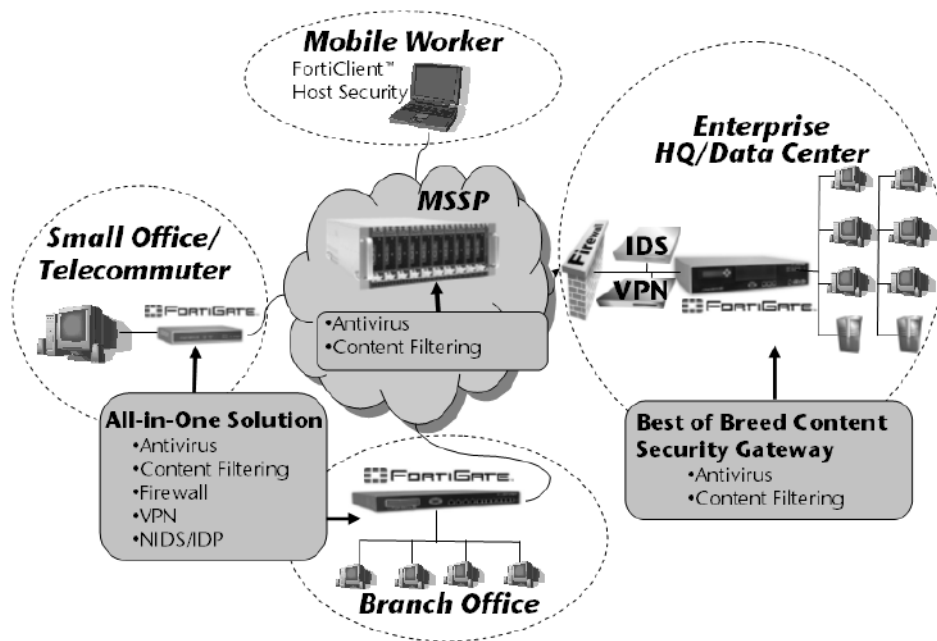


Fortinet offers the only security appliances that combine an ASIC solution with the robust operating system required for real-time, complete network protection, at both the network-layer and the application layer.



FULL NETWORK SECURITY INCLUDED

In addition to providing application level protection, the FortiGate appliance systems deliver a full range of network-level security services - firewall, VPN, intrusion detection and traffic shaping - delivering complete network protection services in dedicated, easily-managed platforms, with solutions ranging from mobile worker, up to large enterprise and service provider.



AUTOMATIC, REAL TIME RESPONSE TO NEW ATTACKS

Fortinet provides its FortiProtect™ services which automatically updates FortiGate units worldwide in real time with protection for the newest attacks. The FortiResponse Bulletin details new security threats (issued daily by the Fortinet Threat Response Team) and is sent to FortiGate users. By automatically pushing a new threat detection database to all FortiProtect service subscribers, Fortinet protects thousands of FortiGate users from fast-moving worms or viral threats.

Fortinet Threat Response Team and Update Distribution Servers

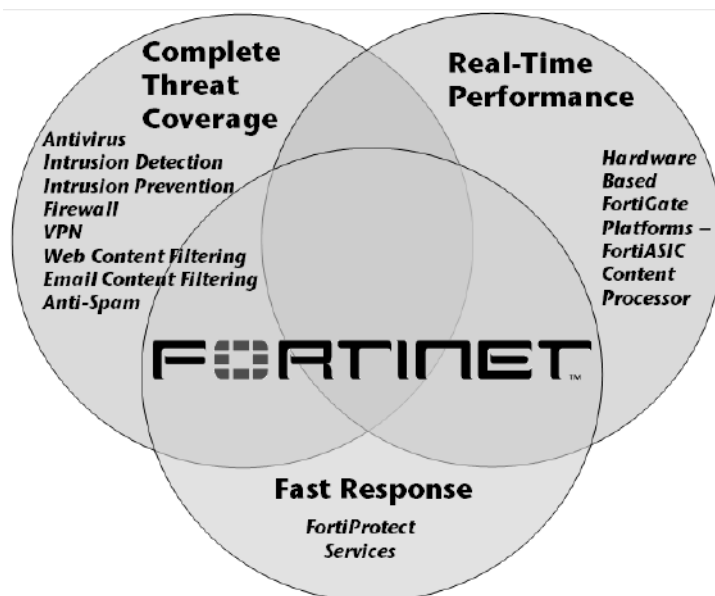


FortiProtect Center Web Portal and Email Bulletins



COMPLETE REAL TIME PROTECTION SOLUTION

The combination of the FortiGate ASIC-powered appliance offering a full suite of network and content level functionality with the FortiProtect instant update service provides unmatched capability for complete, real-time network protection.



Feature	Fortinet	Cisco	Juniper (Netscreen)	Check Point
Inline Antivirus Scanning Protection for Large Networks	Yes	No	No*	No
ASIC Accelerated FW/VPN/Antivirus	Yes/Yes/Yes	No	Yes/Yes/No	No/Yes ¹ /No
Automatic Protection against New Threats	Yes (FortiProtect Network)	No	No*	No ¹
Pricing includes All Functionality	Yes	No	No (Includes only FW/VPN)	No (Base pricing only covers FW)
Platform provides Complete Content Protection	Yes	No (stateful inspection only)	No (deep packet inspection only)	No (deep packet inspection only)

* Only on low end units; utilizes Trend Micro software.

¹ Only on certain units; additional charge applies.

>> *The 2004 Deloitte Survey showed that only slightly more than half of the financial institutions in the US felt they had adequate skills and competencies to respond to the increasing number of threats.*

BUYING VS. SUBSCRIBING TO SECURE NETWORKS: MSSP AS A SOLUTION

Managing sophisticated security solutions requires an organization to either have access to a highly skilled IT staff or to use the services of a managed security service provider (MSSP). Small and medium sized businesses are increasingly turning to MSSPs to provide all or a portion of their IT security needs. Managed security services are expected to grow at least 50% to \$1.5B between 2002 and 2006.

There are a number of reasons why businesses are moving towards managed security services, including:

- Security is not a core function for many organizations;
- The sophistication of threats is rapidly evolving and their ease of launch is increasing;
- The cost of security is increasing, with the total cost of in-house security rising 24% in 2003, with labor costs relating to security increasing 31.7%.
- Leveraging MSSP expertise and infrastructure to obtain the latest in security technology.

Even large financial organizations with significant experience in protecting their networks are having difficulties with the current threat environment. The 2004 Deloitte Survey showed that only slightly more than half of the financial institutions in the US felt they had adequate skills and competencies to respond to the increasing number of threats.

The MSSP model greatly benefits vertical market applications, where a number of organizations have a direct financial services relationship with financial service providers. An example would be auto dealers and their service providers who offer loan and credit services. In such an example, the financial services provider would provide an MSSP solution for all the auto dealers it works with. They could set themselves up as an MSSP, or choose to outsource the solution to a third party MSSP.

Key advantages include:

- Ensure GLBA compliance across all partners which share financial data; in this case, all the auto dealers who work with the financial service provider;
- Control over the level of protection provided to the participants;
- Ability to run group-wide tests to demonstrate compliance, as needed.

CONCLUSIONS

GLBA compliance affects many organizations, often these companies are unaware they are even susceptible to a significant escalation in the quantity and severity of cyber-attacks. All organizations handling financial data are required

to be compliant with GLBA including accountants, auto dealers and travel agents. Compliance requires a robust and intelligent security system like the Fortinet FortiGate Antivirus firewall. FortiGate represents a new breed of network security system now available to help protect the corporate network at its continually changing perimeter, by identifying and preventing malicious blended security threats coming from both external and internal sources. IT professionals and business managers alike can comply with GLBA using FortiGate systems at the perimeter as well as critical choke-points where deep packet inspection and complete content protection are required - such as high security server farms and critical departmental subnets. With the emergence of regulations like GLBA, securing customer personal information, from both external and internal threats, is a critical activity.

ABOUT FORTINET (WWW.FORTINET.COM)

Fortinet's award-winning FortiGate™ series of ASIC-accelerated antivirus firewalls, winner of the 2003 Networking Industry Awards Firewall Product of the Year and the 2004 Security Product of the Year Award from Network Computing Magazine, are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from e-mail and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time - without degrading network performance. FortiGate systems are the only security products that are quadruple-certified by the ICSA (antivirus, firewall, IPSec, NIDS), and deliver a full range of network-level and application-level services in integrated, easily managed platforms. Named to Red Herring Top 100 Private Companies, Fortinet is privately held and based in Sunnyvale, California.

For more information

More information about Fortinet, FortiGate Antivirus Firewall products, FortiProtect Center and other services provided by Fortinet is available from the following sources:

Sales

Please contact us at sales@fortinet.com, toll-free in the U.S. (866) 868-3678 or +1(408) 235-7700.

Potential Partners

Please contact us at partners@fortinet.com or visit us at www.fortinet.com.

- i Gartner Dataquest Research Brief "Managed Security Services Bring IT Value" 10 January 2003
- ii Deloitte Touche Tohmatsu "2004 Global Security Survey"
- iii Gramm-Leach-Bliley Act (GLBA), 15 USC 6801 etc, and FTC 16 CFR Part 314 Final Rule for Standards for Safeguarding Customer Information.
- iv Light Reading Insider, Vol 4, No. 6, June 2004, "Managed Security Services: The Safe Bet"
- v Deloitte Touche Tohmatsu "2004 Global Security Survey"
- vi Frost and Sullivan "World Managed Security Service Provider Markets" # 7426-74, ©2003
- vii Office of the Comptroller (OCC) 2000-14
- viii Executive Summary, NIST 800-61
- ix Deloitte Touche Tohmatsu "2004 Global Security Survey"
- x Deloitte Touche Tohmatsu "2004 Global Security Survey"
- xi Light Reading Insider, Vol 4, No. 6, June 2004, "Managed Security Services: The Safe Bet"
- xii Light Reading Insider, Vol 4, No. 6, June 2004, "Managed Security Services: The Safe Bet"
- xiii Deloitte Touche Tohmatsu "2004 Global Security Survey"

Copyright 2004 Fortinet, Inc. All rights reserved. Fortinet™, FortiGate™, FortiContent®, FortiOS™, FortiBIOS™, and FortiASIC™ are either registered trademarks or trademarks of Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. GLBA Compliance Kit™ is a trademark of MDi Network Security Systems, Atlanta GA. are trademarks of Fortinet, Inc. WPR1040407



www.fortinet.com