



**Enterprise Security for  
Financial Services**

## **Introduction**

The Financial Services<sup>1</sup> sector is probably the most highly targeted area of information security attacks. As more commerce and services are moved online to realize cost-savings and efficiency gains, financial services provide a lucrative target for attacks that use malicious software (malware), phishing and identity theft. This paper discusses the security responsibilities that financial services are tasked with due to standards and regulations, and how they can protect themselves and their customer data from security threats.

One of the major problems is that the enterprise is increasingly extended and increasingly vulnerable. Remote offices are often difficult to control and secure, and the organization has even less control over partners, but if their security is weak it can impact the entire organization. Furthermore, workforces are becoming more mobile. The mobile workforce is vulnerable outside the corporate environment, and they can function as an entry point for threats into the corporation when laptops infected on the road are brought behind corporate defenses, such as firewalls and network intrusion prevention systems.

Information theft using phishing attacks against financial services are particularly problematic and are on the rise. Phishing is often disguised as an official email from a financial service that tricks customers into giving away their account information by providing it to a counterfeit website.

According to the July 2005 Report of the Antiphishing Working Group, 86% of phishing attacks are on financial services. Attacks are increasingly targeting smaller organizations, leading to phishing attacks against 70 to 100 new brands every month. Furthermore, the scope of these attacks is widening to include insurance brokers, credit unions, payment services, and ATM networks.

For financial services that interact directly with their customers online, those customers are often the weakest point in the defense. Customer computers are outside the control of the organization and generally have very low security measures, since the average customer knows very little about security. Customers are the soft spot in the defenses, and are usually targeted with phishing attacks through email and malicious software installs.

## **Malware is the Key Threat**

The major threat facing financial services today is malicious software (malware), such as Trojans, viruses, worms, bots, etc. Dangerous malware steals information through monitoring the actions of the user. Malware known as keystroke loggers record the keys pressed and capture passwords, credit cards and other sensitive information. More sophisticated approaches include screen scrapers that capture text and images on screen and are effective against using image maps to input sensitive information. Another trend is using malware to search for and download documents that may contain sensitive information.

Malware is becoming the tool of choice for phishing. The July 2005 report of the Antiphishing Malicious Working Group shows that email phishing leveled off to 14,000 new incidents per month from April to July. The use of malware for phishing increased dramatically from 77 new malware instances in April to 174 for the month of July. Furthermore, the number of websites hosting Trojans increased 350% in the same period.

Malware is causing such problems partly because the defenses used, such as antivirus (AV) and patching are no longer adequate. Malware is often customized for targeted attacks, and consequently, no signatures exist for these rare variants. Malware that mutates to avoid signatures is becoming increasingly common, even in non-targeted

---

<sup>1</sup> This is sometimes known as the "Banking and Financial Services" sector – for the sake of brevity, the term "Financial Services" is used throughout this document to indicate all companies that provide financial services, including banking.

attacks. In addition, malware is incorporating payloads that turn off PC defenses, disabling software such as firewalls and AV, and blocking access to AV updates and operating system patches. Signature-based security is failing to keep up with these innovative attacks.

### **Financial Services are Subject to Many Security Regulations**

Securing financial services is made more complex by the wealth of regulations that surround the industry. This section describes the most important government legislation and private sector standards affecting the security management of financial services today.

The Gramm-Leach-Bliley has Financial Privacy and Safeguards rules that dictate how an organization should control the collection and disclosure of customer financial information, and how such information should be protected through the implementation and maintenance of safeguards. This legislation applies to all firms that provide financial products and services to consumers, including non-financials who receive or process customer information. The penalties for non-compliance are steep, with fines of up to \$100,000 per incident. Furthermore, officers and directors can be held personally liable for up to \$10,000 per incident.

The PCI Data Security Standard is an example of an important private sector standard. It consists of 12 unified requirements for VISA, Mastercard, Discover and American Express. Some of these are very specific, for example stipulations about the use of firewalls, whereas others are very vague, such as requiring organizations to “develop and maintain secure systems and applications”. The PCI Data Security Standard applies to any merchant processing relevant credit card transactions. The penalties include restrictions on merchant or even prohibition from using the credit card network as well as fines of up to \$500,000.

There are also regulations that are not specifically targeted at financial services, but that disproportionately affect them. One such regulation is the California 1386 bill, which requires organizations to inform customers whose confidential data has been compromised. It applies to all companies handling personal data of California residents, regardless of where those companies are based. It has the biggest impact on financial services because they are far more likely to store private customer data. No specific penalties are enumerated, but the consequences are wide-reaching, including civil suits, negative publicity, loss of investor confidence and other factors.

### **Security Strategy for Financial Services**

Because financial services are more highly targeted than any other sector coupled with the consequences of failing to satisfy the regulations and standards, a financial services organization must maintain an effective security solution. It needs a comprehensive security strategy that protects its data in many different ways on many different levels, as illustrated in figure 1.

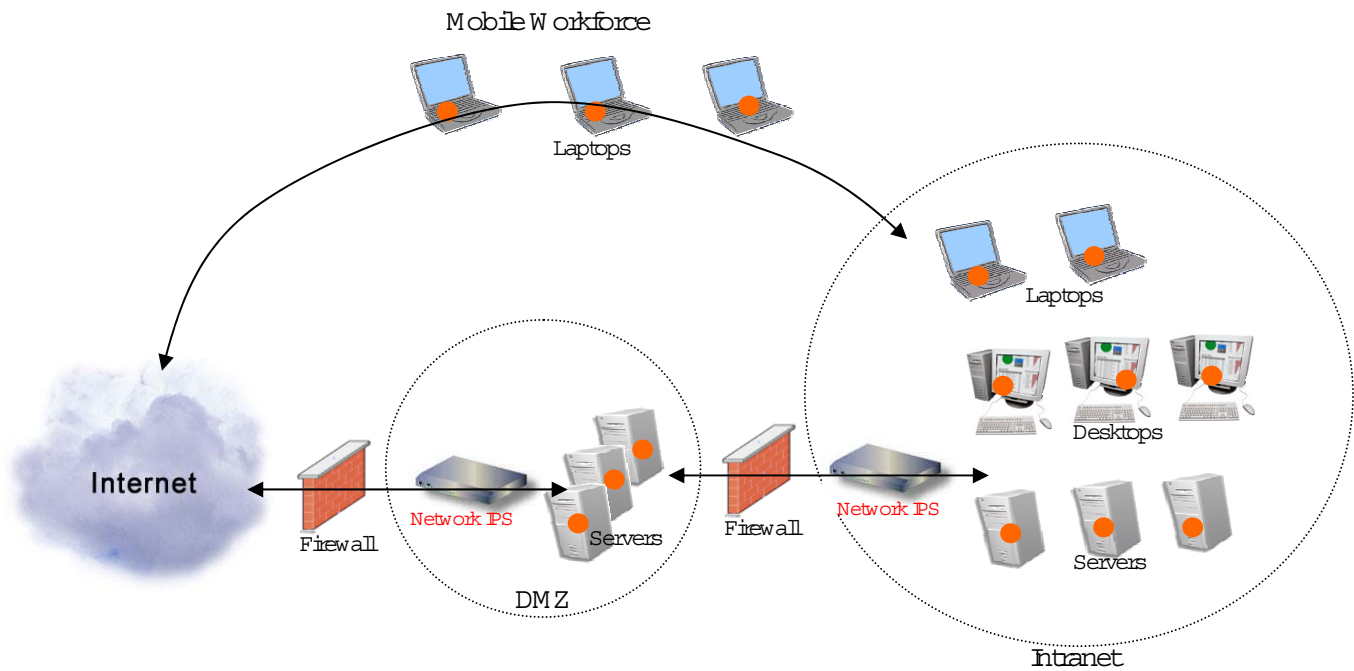


Figure 1: Layered defense strategy for the network.

The perimeter of the network should be protected by network Intrusion Prevention Systems (IPS) and Host Threat Protection. Remote access should only be allowed through VPNs and SSL. Where possible, data should be encrypted. The consequence of compromise and information theft – for example, organizations are not subject to the California 1386 Bill if encrypted data is stolen. For even greater security, all authentication should preferably be two-factor, although this may be hard to implement for a large customer base.

In addition, it is vital to protect the extended enterprise, including mobile workers and remote offices. These fall outside the protection domain of the corporation; therefore, protection down on the host – either servers, desktops or laptops – is essential.

### Primary Response Provides Layered Defenses for Hosts

Primary Response, a comprehensive host-based security product from Sana Security, can help financial service organizations meet the various security requirements, including Gramm-Leach-Bliley, California 1386, and the PCI Data Security Standard. Primary Response provides multiple types of protection in multiple layers, on both servers and PCs, profoundly reducing the chance of compromise and information theft.

Servers are typically more important than PCs, being much more likely to house private customer data. Fortunately they are usually much better controlled, residing within the corporate network and under the direct supervision of one or a few administrators. However, they are still vulnerable to insider attacks and to attacks that have penetrated the perimeter. Primary Response protects servers with several layers of defense, including buffer-overflow protection to stop code injection attacks, and Sana Adaptive Profiling Technology (SanAPT), which automatically defines normal behavior and blocks deviations caused by malware attacks, protecting the server from a wide range of attacks.

In comparison, PCs are usually much more vulnerable, much less controlled and exhibit much more varied behavior. Therefore, the security solutions that work well on servers are not necessarily suitable to PCs. Different technologies

are needed. Almost every PC today will have Anti-virus (AV) software installed, and although this is effective against known viruses and some mass attacks, it is not sufficient to ensure protection against the variety of new threats today, even if the signatures are kept fully updated.

Sana Security's Primary Response provides PCs with the additional threat protection needed to prevent unknown and targeted attacks, and to detect and stop mutating and complex malware. This protection is complementary to AV and provides a failsafe mechanism because no signatures are required. As a result, the system's defenses will never be out-of-date.

Primary Response's comprehensive threat protection consists of many layers of defense:

1. Malware prevention: Sana's Active Malware Defense Technology (Active MDT) stops any malware from running on the host and prevents any attempts to install new malware. It performs these tasks automatically, without the need for signatures, updates or any human configuration effort.
2. System protection: Primary Response protects core system components such as system services from malware attacks. It also protects the Operating System kernel, preventing the loading of unauthorized drivers and blocking kernel-level root-kits.
3. Application protection: Primary Response provides preconfigured protection for common applications such as browsers, mail-clients, word-processors and others. This is particularly important for network-facing applications such as browsers because they are points of remote access into the computer and are frequently subject to attack.
4. Policy enforcement: Primary Response enables financial services to enforce policies such as controlling the software allowed to run on specific computers. This is essential to ensure that employees adhere to company policies.
5. Auditing: Primary Response satisfies audit requirements by keeping detailed records of who accessed the security system and what actions they carried out, and detailed traces of all detected security incidents. These data are remotely and securely stored on the Primary Response management server and can be used as proof of diligence.

## **Summary**

The Financial Services sector is more targeted than any other sector and is particularly vulnerable to attack due to their customers behavior and the content of their business transactions. Furthermore, the plethora of regulations affecting financial services make the consequences of security failure particularly disastrous.

To properly secure a financial services enterprise requires multiple layers and methods of defense. This applies both at the network level and on individual PCs. Network-level defenses such as firewalls are essential to a robust defense strategy, but they alone are not adequate to ensure the security of the extended enterprise. A comprehensive strategy also requires host-based defenses.

Signature-based anti-virus and anti-spyware systems on the host do not provide sufficient protection against changing threats and today's complex attacks. To properly secure systems on the host requires additional threat protection, such as Sana Security's Primary Response, which protects against modern security threats with no reliance on signatures or updates.

Learn more about Primary Response and sign up for your free evaluation. Go to <http://www.sanasecurity.com/products/index.php> or call **1-866-900-SANA**.



2121 S. El Camino Real, Suite 700  
San Mateo, CA 94403  
650.292.7100 • Fax: 650.292.7110  
[www.sanasecurity.com](http://www.sanasecurity.com)

**About Sana Security, Inc.**

Sana Security creates award-winning, autonomous intrusion prevention software that is aware of environment change, adaptive to new threats and active in preventing attacks before they do harm across mission-critical computer systems. Sana Security's Primary Response® and Attack Shield brand products improve security and business continuity for large enterprises and government organizations on servers, personal computers, and industrial systems, while driving the emerging standards for simple, secure computing in an Internet-connected world. Sana Security is headquartered in San Mateo, Calif. (Silicon Valley), with offices in global business and technology centers and can be reached at [www.sanasecurity.com](http://www.sanasecurity.com) or 866-900-SANA.