Flash Forward: Network Security in the Financial Services Sector

Threat Intelligence Critical to Cyber Security Protection
Financial services institutions are at the forefront of cyber-attacks and keeping information safe is critical to maintaining customer confidentiality, ensuring regulatory compliance, and protecting the brand. In order to stay protected, threat intelligence needs to evolve 24x7, 365 days a year.

With over two million threat sensors worldwide, Fortinet hardware and virtual solutions are reinforced by a team of over 200 cyber-security researchers focused solely on industry threat research, analytics, and intelligence for preventing the latest attacks and providing incident response. Fortinet protects the most valuable assets of some of the largest financial services institutions across the globe, including 7 of the top 10 global banks.

In the following report, Aberdeen Vice President and Research Fellow Derek Brink discusses how the financial services data center market is in transformation, reviews the constant attacks targeting the industry, and outlines the complex compliance requirements facing financial institutions. Brink introduces criteria for how financial services are adapting to keep ahead of the cyber-threat by enhancing their ability to detect and respond more quickly to indicators of compromise. To address requirements, organizations need to rely on trusted security vendors who can deliver:

- Agile and elastic cloud and SaaS security,
- Sophisticated threat research and intelligence services, and
- Advanced threat frameworks that integrate sandboxing into a cycle of prevention, detection and mitigation

FLASH FORWARD: NETWORK SECURITY IN THE FINANCIAL SERVICES SECTOR

Organizations in the financial services sector must deal not only with transformational technologies (e.g., virtualization and cloud computing, mobile, social collaboration), but also with ever-evolving attackers and relentless requirements from a complex array of auditors and regulators. In response, network security strategies are being adapted to provide traditional prevention at the edge, augmented by enhanced detection and response capabilities at the core.

Derek E. Brink, CISSP, Vice President and Research Fellow, IT Security and IT GRC, January 2015

Related Report: The New Enterprise Datacenter, May 2014

In the financial services sector, the transformation of the enterprise datacenter creates new stresses on traditional approaches to security, compliance and risk management.

1. The Financial Services Datacenter is in Transformation, in the Drive for Flexibility and Cost-Effectiveness

Aberdeen’s research on the transformation of the typical enterprise datacenter confirms that most organizations have generally been eager to gain the flexibility and cost-effectiveness of virtualization and cloud computing – but also shows that they have continued to be cautious about giving up visibility and control, particularly over matters of risk, data security and regulatory compliance (Figure 1).

Figure 1: Most Workloads are Virtualized, but Most Workloads Still Run in the Enterprise Datacenter

![Figure 1: Most Workloads are Virtualized, but Most Workloads Still Run in the Enterprise Datacenter](image)

Source: Aberdeen Group, May 2014

These findings are particularly true in the financial services sector. For example, the New York State Department of Financial Services Report on Cyber Security in the Banking Sector (May 2014) notes that “the vast majority of depository institutions surveyed, irrespective of size, rely on both internal and external resources to manage their IT systems. Of large institutions, 75% reported relying on a mix of in-house and outsourced IT systems. Similarly, 62% of medium and 70%
of small institutions reported the same. Notably, very few institutions rely on a completely outsourced IT environment.”

Why such a cautious approach? One driver is illustrated by the recently updated risk management guidance for third-party relationships from the US Office of the Comptroller of the Currency (OCC), which oversees and regulates all national banks and federal savings associations, for example: “The OCC expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank’s use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.”

In other words, organizations in the financial services sector, like everyone else, are leveraging virtualization and outsourcing of IT services as part of their drive for consolidation and greater operational efficiency – an important element of their ongoing recovery from the global financial crisis – as well as their flexible, consumer-oriented focus. But at the same time, it has been made clear that outsourcing the activity does not outsource their responsibilities for how it is done. In the financial services sector, the transformation of the enterprise datacenter creates new stresses on traditional approaches to security, compliance and risk management.

2. The Financial Services Sector is (Always) Under Attack, Which Places it Perpetually in the Vanguard for Security

Industry sources that illustrate the extent to which the financial services sector is perennially under attack are abundant, for example:

- Akamai’s State of the Internet Report (3Q 2014) noted that “the financial industry was targeted in 9 percent of all observed distributed denial of service (DDoS) attacks. Attacks against the financial industry are often state-sponsored or politically-driven campaigns. They gain significant media attention due to the ramifications of a successful attack.” Not surprisingly, the FDIC has recently made it clear that “financial institutions are expected to address DDoS readiness as part of their ongoing business continuity and disaster recovery plans, and to take certain specific steps to detect and mitigate such attacks” – and likewise it comes as no surprise that the financial services sector represents one of the strongest adopters of DDoS protection services.
The monthly RSA Online Fraud Report (December 2014) recently found that in the US, “regional banks and credit unions were targeted by half of all phishing volume in November 2014. Phishing volumes have started to even out as cybercriminals look to target smaller financial institutions that might not have the resources to address these attacks.” Reducing the risk from phishing attacks is complicated by the fact that in addition to protective steps that can be taken by the institution itself, much still depends on educating individual users, as evidenced by a recent investor alert by FINRA, the Financial Industry Regulatory Agency.

These are just two of the numerous attack vectors targeting the financial services sector at present, but the basic point being made is that some things never change: the risk of security-related attacks on the financial services sector, as always, remains high. In addition, their increasing web and mobile presence gives financial institutions an even greater surface area for attack.

3. The Financial Services Sector is Highly Regulated, Which Combines Security with the Complexity of Compliance

It goes without saying that the financial services sector is required to deal not only with transformational technologies and ever-evolving attackers, but also with the relentless requirements from a complex array of auditors and regulators who are in place to oversee how they do it. However, it’s worth noting that this challenge must be executed simultaneously in several dimensions, including:

- **The wide variety of data to be protected** – this includes the integrity of financial reporting information (e.g., as addressed by Sarbanes-Oxley); the privacy of consumer information (e.g., Gramm Leach Bliley, as well as a patchwork of data protection legislation); the security of cardholder data (e.g., the Payment Card Industry Data Security Standard); the accuracy of consumer transactions and credit histories (e.g., the Fair and Accurate Credit Transactions Act); and so on.

- **The large number of regulatory regimes to be satisfied** – in the United States, this includes the Federal Financial Institutions Examination Council (FFIEC) – which is itself compromised of the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the
Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) – as well as the national examination program conducted by the Securities and Exchange Commission (SEC), the NIST Framework for Improving Critical Infrastructure Cybersecurity (currently voluntary), and international regulatory standards such as those developed by the Basel Committee on Banking Supervision (BCBS).

The broad range of technical security controls from which to choose – regulatory requirements are sometimes prescriptive, sometimes based on principles, and frequently reference the guidelines, best practices and controls that are set down in management frameworks such as COBIT 5, the ISO 27000 Series, or selected publications in the NIST SP 800 Series. On the one hand, the rich and complex menu of security technologies that solution providers have made available is a testament to the importance of the security and privacy problem – while on the other, having such an overabundance of options can make it painfully difficult for any given organization to choose the mix of controls that represents the best fit for their specific business context.

4. How Financial Services Network Security Strategies are Being Adapted: Prevention at the Edge, Augmented by Enhanced Detection and Response at the Core

Aberdeen’s research confirms that traditional, protection-oriented approaches to information security are being augmented with enhanced capabilities to detect and respond more quickly to indicators of compromise – note that this is a statement of “both / and” rather than one of “either / or.” In other words, organizations are increasingly aware that prevention can’t be successful 100% of the time, and they are therefore putting themselves in a position to detect, respond and recover from security-related incidents, particularly from the new generations of advanced threats, more quickly when they do occur. Specifically with respect to network security:

- Prevention has traditionally been implemented at the edge, i.e., with network firewalls, intrusion detection and prevention, email and web security, and anti-virus at the endpoints. Technology trends in mobility, cloud computing and social collaboration have been adding their own challenges to these customary defenses.


Detection and response capabilities are typically implemented at the core, i.e., by aggregating and correlating the wealth of data being generated throughout the network, to provide new visibility and insight into what’s really happening on the network – both the normal, and the abnormal. Reducing the mean time to respond to threats, and actual incidents, becomes one of the key measures of success. Leading organizations are also using network security capabilities in this way to protect not only against external threats, but also against internal threats (e.g., to counter fraud, waste and abuse).

As this augmented and enhanced strategy emerges, capabilities that become especially important for organizations in the financial services sector to look for from their network security solution providers include:

- **Real-time performance**, to support the ongoing transformation of the enterprise datacenter, as well as the ever-growing demand for scale required by aggressive adoption of mobility, cloud computing and social collaboration technologies – without compromising expectations for response times.

- **External threat intelligence** and **analytics** about active, relevant attack campaigns – e.g., insights and actions derived from the analysis and expertise of the solution provider’s in-house researchers – which can help to provide organizations with **superiority of information** that they can use to tip the balance of power away from the attackers.

- **Incident response capabilities**, to be in a position to detect, respond and recover from security-related incidents, particularly from the new generations of advanced threats, more quickly when they inevitably do occur. Incident response (sometimes referred to as emergency response) should be thought of not as a particular set of actions for a specific incident, but as an essential set of enterprise capabilities – whether they are developed and maintained in-house, or whether they are realized by leveraging third-party expertise.