

CYBERSECURITY FOR BANKS AND CREDIT UNIONS

By addressing core security areas, financial institutions can protect themselves from advancing threats.

Executive Summary

Banks and credit unions have more types of cybersecurity tools at their disposal today than ever before, and it's increasingly difficult to determine which of these tools are truly needed for any particular environment. Monetizing the budgetary value of individual security expenditures is incredibly challenging for IT security teams, so it may not be feasible to make purchasing decisions on that basis. Rather, financial institutions must assess where their security weaknesses are and identify the tools that can mitigate these weak links efficiently and cost-effectively.

Unlike many other organizations, banks and credit unions tend to have solid security tools already in place. However, threats continue to intensify, so financial institutions should periodically reassess their security posture and identify tools that can augment or replace existing solutions. This can help them avoid the data breaches that have led to significant losses and major embarrassment for other financial institutions.

Based on today's threats and security tools, most financial institutions will find the greatest benefit from focusing on four core security areas: web security, advanced persistent threat detection, security resource consolidation and virtual environment security.

Table of Contents

- 2 The Current Threat Landscape
- 2 Web Security
- 3 Advanced Persistent Threat Detection
- 3 Security Resource Consolidation
- 4 Virtual Environment Security
- 4 CDW: A Security Partner That Gets IT

The Current Threat Landscape

Cybercriminals are increasingly focusing their attention on specific segments. The banking and credit union industry has emerged as one of the most attractive targets. Although financial institutions have long been leaders in terms of security control adoption, any organization can have weak spots in its defenses, and attackers have been taking advantage of these.

Last year, one of the nation's largest financial firms suffered a major data breach that exposed sensitive personal information for over 76 million households and 7 million businesses. The attackers leveraged known vulnerabilities in the firm's web applications and other software to gain unauthorized access to this data and to elevate their privileges to administrator level on dozens of the company's servers.

Security professionals at financial institutions are already aware that their data and applications are being targeted by attackers, but they may not be aware of the increasing volume and sophistication of these attacks. [Symantec's 2015 Internet Security Threat Report](#) has some startling statistics. For example, in 2014, attackers released more than 300 million new variants of malware. Older security tools simply cannot detect these new attacks effectively.

It's not surprising to hear that targeted attacks are on the rise, but many of these attacks are now targeting small and midsize organizations. No enterprise is safe from today's threats, and losses continue to increase. According to the [2014 Cost of Data Breach Study by the Ponemon Institute](#), the average cost of a data breach is up to \$3.5 million.

To counter today's threats, financial institutions need to increase and accelerate their efforts to protect their data and systems. Each financial institution needs to find the balance of speed and security that meets its own unique requirements and environment.

WHAT ARE APTs?

Advanced persistent threats are stealthy attacks that often linger within an enterprise for months or even years. Once an attacker gains unauthorized access to a financial institution's computing resources, the attacker slowly and methodically expands that access over time to locate and steal sensitive data. Traditional security controls that detect attacks, such as anti-virus software and intrusion detection systems, often miss APTs, allowing these compromises to go on for extended periods of time. APTs don't necessarily utilize advanced attack methods, so the name is a bit of a misnomer, but they certainly are persistent.



62%

The percentage of banks that have implemented policies and procedures to mitigate information security risks associated with cloud computing

SOURCE: New York State Department of Financial Services, "[Report on Cyber Security in the Banking Sector](#)," May 2014

Web Security

The technologies that support web security have evolved over the years. Even an institution that thinks it has solid web security tools and practices in place needs to periodically reassess them to keep up with the latest threats and the newest tools. Several core IT security controls must be included in any robust solution to provide multilayered security. Having multiple layers of security is more important than ever because no single security tool is effective against most threats.

Unified threat management: UTM technologies bundle several security capabilities into a single network-based device to protect both web servers and web client devices. UTM capabilities include firewalling, intrusion detection and prevention, virtual private networks, anti-malware and web content filtering. These functions are all critical for any modern IT environment, and by bundling them into a single device, greater performance and lower costs can be achieved. Examples of UTM technologies include Palo Alto's PA-5000 series, Cisco Systems' Adaptive Security Appliance and Fortinet's Unified Threat Management solution.

Endpoint security: These solutions are similar to UTM technologies in that they bundle multiple security capabilities into a single product, but endpoint security solutions are software-based and are targeted toward user devices, such as desktop and notebook computers, smartphones and tablets. Symantec Endpoint Protection, Trend Micro Enterprise Security for Endpoints and McAfee Total Protection for Endpoint are examples of products in this space.

Typical capabilities offered by endpoint security solutions include anti-malware functions, firewalling, and intrusion detection and prevention. Because they are host-based, not network-based, endpoint security solutions travel with the device, so they can protect it from threats no matter where the device may be used, including external environments that do not provide network-based security controls. Keeping web client devices "clean" of malware and other forms of attack is key to reducing web server and application compromises caused by leveraging user access.

Web and email security: Dedicated devices or server add-ons can examine web and email traffic for suspicious or malicious content

79%

The percentage of financial institutions reporting that their information security budgets will increase in the next three years

SOURCE: New York State Department of Financial Services, "[Report on Cyber Security in the Banking Sector](#)," May 2014

and handle this traffic appropriately. It may not be immediately obvious that email security is necessary for web security, but many of the attacks that involve malicious web activity are initiated through malicious emails. Examples of email security gateways are Cisco's Email Security Appliance, Proofpoint's Enterprise Protection and McAfee's Email Protection. Web security gateways include Cisco's Web Security Appliance and McAfee's Web Gateway.

Encryption of data at rest: Most financial institutions are well aware of the need to encrypt sensitive data in transit over unprotected networks, but it is increasingly important to encrypt sensitive data at rest (on storage) as well. Banks and credit unions have a wide variety of enterprise storage encryption products to choose from. While they all provide the same basic encryption and key management functionality, these tools support encryption of different kinds of storage. Some products support endpoint encryption only (for example, hard drives or removable media), while others also support encryption on file shares, cloud storage and other network-accessible locations. Examples of products that possess this functionality include Sophos SafeGuard Enterprise Encryption, the Symantec Encryption family, RSA Data Protection Manager and McAfee Complete Data Protection (for endpoints only).

Authentication: Vendors such as RSA and 2FA provide a variety of software and hardware-based products for enterprise authentication services. These services support web security because they enable the use of diverse authentication methods, including multifactor authentication with cryptographic tokens, smart cards and biometrics. Using multifactor authentication greatly reduces the chances that an attacker can steal a legitimate user's credentials and reuse them. Some enterprises choose to use multifactor authentication for administrators only, while others have moved toward multifactor authentication for all internal users.

Advanced Persistent Threat Detection

The rise of advanced persistent threats has caused a shift in the entire security paradigm. Before APTs, financial institutions could

count on their security controls to stop almost all attacks before they succeeded. However, these security controls may not be effective against many newer threats, including APTs. So financial institutions are powerless to stop a larger number of these attacks from succeeding.

The security community has finally begun to shift from a prevention mindset — striving to identify and block every attack attempt — to a detection mindset. In a security environment that focuses on detection, security controls are based on the assumption that compromises will occur, and detecting those compromises as soon as possible is critical so the damage can be minimized.

Accordingly, advanced threat defense tools have emerged that focus on detecting APTs and other compromises — for example, FireEye Endpoint Security (HX series). Such tools work by searching hosts for indicators of compromise (IOCs), which are basically traces of an attack that can be used forensically to pinpoint the root cause of a compromise. These IOCs are constantly being mined from a wide variety of sources of threat information. This data is then analyzed to create what is known as threat intelligence. Threat intelligence is frequently updated on each client running the tool so that new threats can rapidly be identified and mitigated.

Security Resource Consolidation

Because so many different controls are needed to achieve robust security, and because financial institutions face a challenge in monitoring, updating and managing each product, many vendors offer bundled products. Each of these products contains several security capabilities that were previously available only as separate stand-alone products. UTM technologies and endpoint security solutions are examples of bundled products.

Another bundled product type that consolidates several security functions is the next-generation firewall. An NGFW offers advanced firewalling capabilities that perform deep packet inspection. DPI,

WHAT IS DPI?

Deep packet inspection occurs when network packets are inspected not just at the header level, but also at the payload level. The header or headers, which contain critical information for protocols such as Internet Protocol, Transmission Control Protocol and User Datagram Protocol, are traditionally the focus in firewalling. DPI goes past the headers into the payloads of these protocols to examine their contents for malicious activity. Most attacks today are carried in packet payloads, not headers, so it makes sense to examine both headers and payloads when making decisions about which traffic to allow into or out of the enterprise.



To learn more about security and other critical IT topics, check out CDW's infographic "[Top Tech Trends for Banks in 2015](#)."

in turn, enables an NGFW to offer additional security capabilities. These usually include intrusion prevention system (IPS) capabilities and may also include virtual private networking, anti-malware functionality, web content filtering and other features. Examples of NGFW products are Check Point Next Generation Firewall, Fortinet NGFW and Sourcefire NGFW.

On the surface, NGFW technologies sound much like UTM technologies. They tend to offer similar security capabilities, and they both bundle those technologies into a single product. However, in the past, UTM solutions have been designed primarily for small and midsize organizations, while NGFW technologies have been focused on large enterprises. Increasingly, this is no longer the case; vendors are making UTM products for larger enterprises and NGFW products for smaller environments. Financial institutions that are considering the acquisition of NGFW or UTM technologies should look at products with both of these labels.

Virtual Environment Security

Some security tools don't always work well in virtual environments such as the cloud, depending on the cloud architecture and service model. Many security tools aren't optimized to take advantage of the particular characteristics of cloud technology, nor are they respectful of the costs associated with resource consumption within clouds. Virtual environments also have unique security needs that aren't fully met by general (noncloud-specific) security tools.

To improve security and reduce security costs in clouds and other virtual environments, financial institutions should acquire security tools that are specifically designed for those environments, such as Trend Micro Deep Security. Virtual environment security tools offer some of the same capabilities as UTM and NGFW technologies, including firewalling, intrusion prevention and anti-malware, as well as additional capabilities such as storage encryption and log monitoring. Virtual environment security controls also provide centralized management of security across cloud workloads, and in some cases

they even facilitate centralized management of both cloud and noncloud-based resources from a single management interface.

CDW: A Security Partner That Gets IT

For financial institutions, keeping an ever-stronger security posture against today's threats has become a necessity. As a leading provider of technology solutions for financial institutions, we get it. CDW can support you through the security lifecycle, for everything from planning your security product acquisitions and evaluating solutions to integrating new solutions with existing products and ensuring that the solutions are maintained properly over time. CDW can leverage its strong relationships with a wide variety of product and service vendors to assist with all of these lifecycle steps.

The CDW approach to customer service includes:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future environment design and proof of concept
- Procurement, configuration and deployment of a security solution
- Ongoing product lifecycle support

To learn more about CDW's security solutions for financial institutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/financial.

SHARE THIS
WHITE PAPER



The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW-G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.

All other trademarks and registered trademarks are the sole property of their respective owners.

Together we strive for perfection. ISO 9001:2000 certified

MKT2976-150216 - ©2015 CDW LLC

