Financial Institutions Must Adopt Advanced Protection—Or Lose Billions

Whitepaper

SentinelOne

Customers Are Accessing Data Differently—Which Exposes them to New Malware Threats

For every one shift in the way customers access their banking data, two changes actually occur. One change is on the surface—for example, a customer may now conduct banking activities via their mobile app. That change produces a subtler change in turn—banks must now reconfigure their banking infrastructure in order to allow these new activities. While a boon for customer convenience and economic growth, these changes are occurring too quickly for information security to catch up—and cyber criminals have begun to take note.

Over the past few years, banks have fallen victim to increasingly large and sophisticated cyberattacks, in which attackers have looted millions, and even billions, of dollars. The most devastating variety of these attacks—for example, the Carberp Trojan—specifically attacked users' endpoints in order to carry out fraudulent bank transfers. The next generation of malware attacks, ransomware, will go on to hold users' banking information hostage. Time and again, financial organizations have proven that even tens of millions of dollars' worth of investment cannot completely mitigate attacks on banks.

That's because today's advanced malware, ransomware, exploits and other stealthy cyberattacks can easily slip through perimeter defenses and antivirus solutions—often in a fraction of the time it takes to download the latest threat signatures that endpoint and server antivirus solutions provide. Furthermore, responding to detected threats often requires additional point solutions for mitigation and forensics, which adds to the cost, complexity, and internal resources required to properly manage endpoint protection across the entire threat lifecycle.

What are the worst threats currently facing credit unions and financial institutions? How best to guard these organizations—the lifeblood of every national economy—from cyberattacks that seek to plunder their coffers?

Banks and Credit Unions: Facing Advanced Threats

Unlike nearly every other kind of organization on Earth, banks and credit unions have two types of critical information to protect. The first kind is Personally Identifying Information (PII)—the names, credit card numbers, addresses, social security numbers etc. of their customers. Most organizations have this information and must protect it. On the other hand, only banks and credit unions have, and must protect, information that represents cash, stocks, bonds, and other financial securities.

For banks, just protecting the first kind of information is difficult enough. In 2015, hackers stole the details of over 100 million people with bank accounts in what authorities dubbed "securities fraud on cyber steroids." At least nine banks and other financial institutions, including JP Morgan, plus Dow Jones—the parent company of the WSJ—were targeted by hackers who used that stolen PII to make money from illegal activities, including running a digital currency exchange, gambling websites and inflating stock prices.

This attack allowed the attackers—most of whom were later caught—to make nearly a hundred million dollars. Attackers who go after financial information directly, however, stand to make more—much more. The Carberp Trojan, previously mentioned, netted its authors over a billion dollars during a two-year period. It went after users' endpoints—specifically administrators at large banks—and then installed a legitimate remote access toolkit that allowed attackers to control those computers and transfer funds into their own accounts.

Notably, the Carberp attack highlights a key difficulty with the traditional endpoint security posture—the use of security tools that recognize malware, but don't recognize malicious behavior. Again, the authors a Carberp used the Trojan to install a legitimate remote access toolkit. This kind of software program is frequently used by IT admins, and thus neither the users nor their security software raised a red flag. It is the behavior, however—installing an unauthorized program, then using that program to access privileged accounts—that should have raised suspicions.

Financial institutions and credit unions need to move beyond antivirus-based protection. But the endeavor also presents many challenges:

1. Defending against advanced cyber threats—known and unknown—beyond file-based malware
2. Freeing up valuable IT resources from time-consuming, error-prone mitigation practices
3. Performing immediate policy-based mitigation to prevent threats from spreading to other systems
4. Establishing visibility into endpoint device activity for complete forensics
5. Protecting ATM systems running on older versions of Microsoft Windows that can't be patched

At the same time as institutions revise their protections, credit unions and banks must also contend with policy and compliance issues:

1. Maintaining compliance with SOX, CUNA, NCUA and FDIC regulations
2. Ensuring merchant account holders and vendors also maintain secure compliance
3. Optimizing compliance reporting to prevent over-burdening internal resources
4. Complying with PCI DSS when transacting payments

The Weakest (and Costliest) Links: Why a New Approach is Needed

When addressing IT security and compliance challenges, key areas of focus for credit unions and financial institutions should be their endpoints and servers—the weakest points of the organization's infrastructure. These are also the costliest components to manage when considering the multiple burdens that increase the total cost of ownership:

1. **Network**—IT resources protecting endpoints also need to consider the network infrastructure connecting those endpoints; if an attack infiltrates a single endpoint, the network may serve as the vehicle to spread the attack.

2. **Visibility**—Without automated and immediate visibility into attacks that can potentially threaten endpoints, servers and the network, IT must spend an inordinate amount of time searching for attacks.

3. **Servers**—Servers are hosting and storing valuable information, but new server vulnerabilities and zero-day exploits put these valuable servers at risk; IT must constantly stay abreast of the latest patches to make sure these systems are not exposed.

4. **Response**—IT can also spend a lot of time prioritizing which threat to respond to first; in addition to wasting their time on false positives and relatively harmless threats, this also increases the chances they will fail to respond to a major attack.

5. **Management**—Coordinating intelligence generated by security defense systems with external information that helps identify tasks requires a lot of resource time; just knowing the best resources to rely on and then parsing the information those sources provide can require a full-time resource.

Many organizations have on-going frustrating experiences with their existing endpoint and server security solutions as they fail to stop the attacks. After getting hit by major attacks, they also spend an inordinate amount of time on clean-up. In addition to taking key IT resources away from strategic initiatives, the extended mitigation process forces credit unions and financial institutions to function at less than full capacity.

Credit unions and financial institutions also discover that costs increase with each endpoint and server security element they add—each layer promising to protect, identify and respond. The potential arsenal includes antivirus, anti-malware, forensics, advanced threat protection, host-based IPS, desktop firewall, and data loss prevention. Not only are these technologies expensive from a cost perspective, they are also resource and bandwidth intensive—causing frequent blue screens and introducing negative impacts against business performance.

In addition, when deploying advanced technologies, organizations are prone to configuration errors because these solutions are usually disparate in their functions and difficult to tune. With no integration among the security tools deployed, detecting an attack does not necessarily mean the organization will have enough time to eliminate the threat and protect its IT infrastructure before serious damages occur.

With the use of disparate tools, credit unions and financial institutions also find they still rely to a large degree on people for complete end-to-end management. While intentions are good, human involvement increases the number of manual steps to advance from threat identification to threat prevention. Humans are also susceptible to errors—meaning they simply can't process and respond to all the attack information that comes their way.

Three Key Attack Vectors Targeting the Financial Services Industry

1

Ransomware is on the rampage, holding business systems and data for ransom, perhaps even threatening to destroy them if the terms are not met

2

Malware, such as Zeus (Trojan) attacks, continue to be re-packed and altered time and time again to infect financial institutions

3

Phishing (to collect account credentials/logins)

User Endpoint Protection: Recommended Solution Capabilities and Attributes

To address the deficiencies of static prevention and the shortcomings of human intervention, credit unions and financial institutions need to augment their threat prevention solutions with endpoint detection and response capabilities. The goal here is to reduce the time to detection, eliminate false positives, eliminate false negatives, and automatically mitigate harmful activities.

Here's how such a system would work. Instead of operating, essentially, at the perimeter of an endpoint—only looking at files that enter or leave the desktop—the system would interrogate its running processes. This means that it would have a comprehensive look at all the activities that the endpoint is currently undergoing, but without having a significant performance impact on any of them.

By interrogating an endpoint's running processes, the system would be able to understand malicious behavior—such as the unauthorized creation, deletion, or encryption of certain files. When it sees that behavior, the system should be able to mitigate it automatically—terminating processes, isolating the endpoint from the network, or even shutting it down completely.

The system would be able to store a comprehensive record of potential malicious behavior on each endpoint—thus satisfying a host of compliance regimes.

Server Protection Recommended Solution Capabilities and Attributes

In addition to endpoints, credit unions and financial institutions need to consider the protection that their servers require.

Cloud, on-premises and hybrid servers each present their own security challenges, so consider a strategy for protecting each type of server. While servers running the Microsoft Windows operating system have long been susceptible targets, Linux-based systems are emerging as another attack target for cyber criminals.

As you consider which endpoint detection and response solution to deploy for your servers, beware that many security solutions are resource-intensive. Host intrusion protection, antivirus and other security point solutions can push CPU utilization to beyond 50%. And each time administrators apply patches and configuration changes, they can degrade server security levels as they can change dependencies.

Essentially, when looking for an advanced server protection solution, one should look to check off the same boxes as advanced endpoint protection. As an added caveat, however, the highly networked environment of a data center means that viruses have a much greater chance to spread laterally. A good solution should be able to detect and mitigate threats at extremely high speed.

Unified Threat Prevention, Detection and Response Keeps the Focus on Financial Service Quality

Now more than ever, deploying a unified threat prevention, detection and response solution is critical for credit unions and financial institutions. They must transform how they allow customers to access banking information and how they store personal banking details while defending against malicious threats. As organizations adapt to electronic record regulatory requirements—while enabling the portability of information through electronic data storage and communication—they can take on this challenge by deploying sophisticated machine learning and intelligent automation, such as SentinelOne, which defeats advanced malware, ransomware, exploits and other cyberattacks.

By taking this approach, credit unions and financial institutions can ensure data is protected from breaches. Success in this mission also results in a major benefit for credit unions and financial institutions: the ability to keep IT systems operational and customer data safe so personnel can stay focused on delivering the best possible financial services and customer care.

1. "Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab," by Mike Lenon, Security Week, 15 February 2015: http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab

2. "Are Cybercriminals Target Banks with Ransomware?" Bedel Technology, 5 January 2016: http://chrisbedel.com/are-cybercriminals-targeting-banks-with-ransomware/

3. "Top 10 most devastating cyber hacks of 2015," by Ben Rossi, Information Age, 10 December 2015: http://www.information-age.com/technology/security/123460657/top-10-most-devastating-cyber-hacks-2015

SentinelOne

With intelligent automation becoming an obvious replacement for signature-based detection, SentinelOne offers a comprehensive solution for servers and endpoints. Full-context behavioral threat analysis that leverages machine learning captures and neutralizes both known and unknown threats, while providing a forensics package that allows administrators to visualize attack paths and remediate vulnerabilities. The solution is also extremely lightweight.

AV-TEST, a leading independent anti-virus research institute, has awarded SentinelOne Platform the Approved Corporate Endpoint Protection certification for both Windows and OS X, which validates its effectiveness for detecting advanced malware and blocking known threats and allows organizations to use SentinelOne and still meet antivirus compliance requirements. SentinelOne EPP is the only next generation endpoint protection vendor to obtain this certification on both platforms. SentinelOne EPP has also been validated against PCI-DSS by a third-party compliance assessor.

In addition, SentinelOne is the only vendor to offer financial insurance against ransomware attacks with the Ransomware Cyber warranty. SentinelOne customers are eligible for up to $1M of coverage (up to $1000 per endpoint) in the event a ransomware attack occurs.

With SentinelOne, IT teams in the Finance sector finally have a viable path forward that allows them to stay ahead in the arms race against bad actors. Instead of spending limited time, money, and manpower remediating breaches that are already in progress, security practitioners can now usefully devote their time to reinforcing the solid foundation that SentinelOne provides.