Whitepaper

Preventing Data Breaches at Financial Institutions

A New Model for Defeating Cyber Attacks and Safeguarding Customers

Bromium®

Executive Summary

"The financial services industry attracts more directed and tenacious criminal attention than other industries. End-user devices are a factor in more than 80% of security incidents at financial services organizations, and the industry's strong BYOD adoption presents additional risks."

Cybercrime is big business today and the financial services industry is one of the top three targets. Hundreds of millions of customer records and credentials are stolen from banks, insurance firms and other financial institutions each year, costing the industry millions of dollars annually in asset thefts, business disruption, loss of reputation, and the expense of beefing up security after-the-fact. No wonder financial services organizations rank cyber risk as a top concern.

Attackers are well organized, well trained, and highly motivated, employing advanced and constantly evolving attacks. Cybercriminals target endpoint devices using a variety of customized techniques; for example, the vast majority of malware samples are unique to a single organization, and what the malware does is also distinct. Today's cyber attacks are also updated regularly, giving them a high success rate but low detection rate.

Unfortunately, the financial services industry attracts more directed and tenacious criminal attention than other industries. End-user devices are a factor in more than 80% of security incidents at financial services organizations, and the industry's strong BYOD adoption presents additional risks. Current phishing attacks against financial services institutions are highly customized, often targeting large numbers of employees in order to gain control of financial transaction approval systems.

IT staff is having a hard time keeping up with the proliferation of endpoints, rapidly evolving threats, and an endless workload of system remediation and patching. The only surefire way to protect users and safeguard financial data both on and off the network is to defend the endpoint itself. However, old-school detection and blocking defenses are incapable of defeating these targeted attacks.

> "According to the FBI, cyber attackers stole more than 500 million records from financial institutions in a recent 12-month period."

A revolutionary threat isolation approach from Bromium® has been embraced by the world's top financial services firms for its ability to prevent breaches and streamline security. Bromium defends the endpoint by isolating all content for each task—including threats—through purpose-built, micro-virtualization technology, in which micro-virtual machines are created and destroyed automatically, and in the process discarding malware and ensuring the system is unaffected.

Users benefit from uninterrupted workflow, greater productivity, and the ability to click on anything, anytime without fear of compromise. You benefit from fewer breaches, greater uptime, better compliance, and lower operations costs thanks to reduced remediation, reimaging, and urgent security-related patching.

The Challenge of Being a High-value Target

Money makes a tempting target, so it's no surprise that financial services is one of the three top industries in the cross hairs of cybercriminals. Financial services encompass a broad range of businesses that manage money, including banks and credit unions, credit card companies, insurance companies, consumer finance companies, and investment firms and stock brokerages. That gives cybercriminals a lot of targets; in 2014, there were 277 confirmed data breaches in the financial services industry.[1]

Cyber attacks against financial services institutions are becoming more frequent, more sophisticated, and more widespread. Data breaches are among the most common attacks, with customer records and credentials a key target. According to the FBI, cyber attackers stole more than 500 million records from financial institutions in a recent 12-month period. About 110 million Americans—equivalent to about 50% of U.S. adults—have had their personal data exposed in the past year.[2]

"In a survey of some 735 IT professionals by the Ponemon Institute, 52% of respondents noted that reputation loss, brand value and marketplace image was the biggest impact of a data breach."

In 2014, for example, a data breach at JPMorgan Chase & Co. compromised information from 76 million households and 7 million small businesses, including name, address, phone number and e-mail address, as well as internal JPMorgan Chase information about the users.[3] Insurance companies are also key targets of cyber attacks. In a data breach at Anthem Inc., attackers compromised a database containing up to 80 million customer records, stealing such information as names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data.[4]

Cybercrime affects every industry, but the cost to the financial services industry is particularly high, averaging $13 million annually.[5] However, losses can be much higher. For example, cybercriminals used malware first detected in 2013 to steal an estimated $300 million from more than 100 banks and other financial institutions in 30 nations. The malware targeted computers used by bank employees who process daily transfers and conduct bookkeeping. It lurked for months, allowing cybercriminals to learn a bank's daily routines and impersonate bank officers in order to transfer millions of dollars into dummy accounts and to specific ATM machines that dispensed cash to the perpetrators. Individual thefts were limited to $10 million a transaction, though some banks were hit several times.[6]

In addition to the theft of assets like cash, cyber attacks are costly in other ways. The costs of business disruption, information theft, and loss of reputation quickly add up. In a survey of some 735 IT professionals by the Ponemon Institute, 52% of respondents noted that reputation loss, brand value and marketplace image was the biggest impact of a data breach, followed by lost time and productivity to deal with the breach (46%).[7] Beefing up defenses after-the-fact is also costly. Third-party payment processor Global Payments Inc. says its 2012 data breach—which affected up to 7 million accounts—cost the company $93.9 million, mainly to enhance security and ensure compliance with the Payment Card Industry Data Security Standard.[8]

No wonder 84% of financial firms surveyed by Depository Trust & Clearing Corporation in late 2014 ranked cyber risk as one of their top five concerns (up from 59% in March 2014).[9] Furthermore, 33% ranked cyber attacks as the number one systemic risk to the broader economy, up from 24%.[10]

A New Generation of Cyber Attacks

"According to Verizon, the financial services industry attracts more directed and tenacious criminal attention than other industries. Their research shows that 97% of attacks on financial services firms came from outside, with 92% attributed to organized crime."

Cybercrime is big business today and cyber attacks are constantly evolving. Attackers are well organized, well trained, and highly motivated. And, in many cases, they're extremely well funded. According to Verizon, the financial services industry attracts more directed and tenacious criminal attention than other industries. Their research shows that 97% of attacks on financial services firms came from outside, with 92% attributed to organized crime.[11]

Financial services firms face a constant barrage of rapidly multiplying and morphing advanced persistent threats (APTs) and stealthy advanced evasion techniques (AETs). Over the past half-decade, we have witnessed a paradigm shift in the way attackers penetrate organizations' networks. Rather than targeting servers of interest directly, they have shifted to attacking primarily Microsoft Windows endpoint devices. Once a financial services worker's PC or laptop is compromised, these devices can serve as a launch pad for APT campaigns, enabling attackers to spread laterally through the network until servers of interest are identified and exploited and targeted data is exfiltrated.

According to the Verizon 2014 Data Breach Investigations Report, end-user devices were a factor in 82% of security incidents within the financial services sector.[12] The only surefire way to protect users and safeguard financial data both on and off the network is to defend the endpoint itself. Old-school detection and blocking defenses are incapable of defeating these targeted attacks—detection rates for antivirus, for example, range from only 25% to 50%.[13]

Today, attackers target endpoint devices using a variety of highly targeted and customized techniques, including:

- Spear phishing
- Whaling
- Water holing
- Baiting
- Search engine poisoning
- Drive-by downloads

“No matter how much money financial services organizations may invest in security, the bad guys always seem to find a way in.”

“Banks and other financial services companies will continue to be challenged by the speed of technological change and the increasingly sophisticated nature of threats.”

Financial services is one of the industries most affected by Web app attacks.[14] In addition, malware targeting financial institutions uses a variety of tricks to evade detection. According to a report from the Arbor Security Engineering and Response Team (ASERT), sophisticated banking malware known as Neverquest or Vawtrak is able to evade detection by using encryption, anonymous routers and even steganography. This malware has hit well over 100 of the world’s biggest financial institutions, targeting webpages at hundreds of sites with Web inject tools that infect endpoints in order to obtain banking credentials.[15]

Why Current Cybersecurity Efforts Fail

No matter how much money financial services organizations may invest in security, the bad guys always seem to find a way in. According to surveys of financial institutions, the greatest challenges to building an adequate cybersecurity program include the increasing sophistication of threats (71%) and emerging technologies (53%[16]).

The financial services industry experiences an average of 350 malware events each week[17]. Unfortunately, malware is extremely difficult to detect. For example, during a four-month long cyber attack by Chinese cybercriminals on the New York Times, the company’s antivirus software missed 44 of the 45 pieces of malware installed on the network[18].

Banks and other financial services companies will continue to be challenged by the speed of technological change and the increasingly sophisticated nature of threats. Let’s explore the reasons why.

Threats are highly customized

Unlike your everyday viruses, Trojans, and worms—which are intended to infect large numbers of organizations—advanced threats are highly customized for each attack. All cybercriminals need to do to bypass most signature-based defenses (for example, antivirus, intrusion prevention systems and secure gateways) is change a single byte of code. Doing so alters the threat’s fingerprint. And until signature-based defenses are updated, they don’t stand a chance at catching them.

> "Current phishing attacks against financial institutions are highly customized and are updated regularly, which gives them an alarmingly high success rate but a relatively low detection rate."

According to Verizon, 70 to 90% of malware samples are unique to a single organization, and what the malware does is also distinct.[19] For example, current phishing attacks against financial institutions are highly customized and are updated regularly, which gives them an alarmingly high success rate but a relatively low detection rate. These customized attacks target large numbers of financial institution employees with the goal of gaining control of financial transaction approval systems, allowing cybercriminals to initiate and approve transactions that appear to be properly authorized. Attackers are often able to browse an organization's accounts and specifically select accounts with the highest balances.[20]

BYOD is risky business for financial services organizations

Like other industries, financial services organizations are embracing the efficiencies and cost savings of the cloud, mobility, and BYOD—trends and technologies that are dissolving network perimeters and IT control. Financial services organizations lead in BYOD adoption, driven by the needs for interactive digital presentations, point-of-sale transactions, and mobile communications connectivity. For example, adoption of tablets by the financial services sector is several times the adoption rate of the next-closest industry.[21]

According to a Ponemon Institute survey of some 400 IT professionals in the financial services sector, 50% of respondents expect that the majority of their employees will be using e-mail and apps on mobile devices in the next 12 months. Although some 69% of respondents believe smartphones and tablets will replace most desktops and laptops, only 38 percent are confident they can address the risks posed by these mobile platforms.[22]

IT can't keep up

For many financial institutions, remaining competitive in a dynamic industry makes security a challenge. Experts have noted that when competition surrounding new product development is fierce—for example, deploying technologies such as remote deposit capture—security can lag behind.[23]
One area that financial services IT organizations often can't keep up with is system patching.

> “Bromium prevents breaches, removes the burden of security from users so they can click on anything, and streamlines security by eliminating false alerts, urgent patching and remediation.”

Regardless of how sophisticated and targeted the cyber attack, it’s destined to fail if the vulnerability on the host it’s targeting has been patched. Unfortunately, a recent study revealed that the financial industry takes an average of 176 days to patch security problems.[24] When patching occurs infrequently, it opens the door to attackers who design malware to exploit recently disclosed vulnerabilities. A full 99.9% of exploited vulnerabilities were compromised more than a year after the associated Common Vulnerabilities and Exposers (CVE) data was made public.[25]

Bromium—a Revolutionary Approach to Endpoint Security

Given how vulnerable financial services organizations are, how targeted and sophisticated cyber attacks are today, and how traditional security defenses don’t do an adequate detection job, there has to be a better way to defend endpoints and networks. What if there was a way to render threats harmless and make them irrelevant?

There is. Enter the revolutionary isolation approach from Bromium® which prevents breaches, removes the burden of security from users so they can click on anything, and streamlines security by eliminating false alerts, urgent patching and remediation.

Prevent breaches

Bromium’s approach far exceeds the capabilities of detection and blocking technologies like antivirus, whitelisting, Web gateways, and sandboxes. Bromium defends the endpoint by isolating all content for each task—including threats—through breakthrough micro-virtualization technology that leverages CPU hardware technology. Our unique isolation technology creates a lightweight, disposable micro-virtual machine for vulnerable operations, like Web browsing and opening untrusted documents. These operations are isolated from the host operating system, eliminating the need for any type of detection or behavioral analysis—or the possibility of compromise.

> “Traditional network and endpoint security solutions are only as good as their threat signatures. But with tens of thousands of new threats emerging every day, traditional security defenses simply can’t keep up.”

Even if malware finds its way into a micro-virtual machine, the system still protects the enterprise network, the endpoint, and the user. Micro-virtual machines are created and destroyed in milliseconds, discarding malware and ensuring that the system is unaffected. All of this occurs automatically, with minimal impact on the user experience.

Click on anything

Users in the financial services field want the flexibility to use the latest available tools, freely access the Web, and work anywhere, whether at home, branch offices, hotels or airports. Restrictive policies and security solutions can get in their way and slow them down. With Bromium endpoint security, you can give users the freedom to do their jobs anywhere and access anything—without ever worrying about security or the privacy of customer records and financial data. They can click on anything without the risk of compromise.

Streamline security

Today financial services IT professionals face a constant flood of alerts from every system. It’s a challenge to find the critical threats in a sea of false alerts or insignificant events. Bromium’s isolation approach reduces and even eliminates compromises on endpoints and streamlines security by eliminating false alerts, urgent patching, and remediation.

Users benefit from uninterrupted workflow and greater productivity. You benefit from greater uptime for the business and lower operations expenses, saving on costly remediation, reimaging and deployment of spare systems, as well as the need for urgent security-related patching. Rather than waste time and effort sorting through the noise of security alerts and chasing false positives, IT can direct its resources to more mission-critical activities. In addition, financial services institutions that have deployed Bromium’s endpoint solution report improved alignment with industry compliance standards.

Why Bromium and why now?

Traditional network and endpoint security solutions are only as good as their threat signatures. But with tens of thousands of new threats emerging every day, traditional security defenses simply can’t keep up. Newer threat emulation solutions, such as sandboxing, help detect threats at the perimeter that bypass

> "Instead of focusing on detecting and blocking threats, consider investing in solutions that make attackers and their exploits irrelevant, solutions that stop advanced threats by eliminating the attack surface they're designed to exploit, and prevent data breaches at your organization."

traditional defenses, but they're not foolproof, and they only protect hosts while they're connected to the network. If a financial services worker takes their laptop to the café down the street, their laptop and your organization are no longer protected.

The new cyber attack landscape requires a new way of thinking. Trying to keep up with the bad guys is an exercise in futility. Instead of focusing on detecting and blocking threats, consider investing in solutions that make attackers and their exploits irrelevant, solutions that stop advanced threats by eliminating the attack surface they're designed to exploit, and prevent data breaches at your organization.

Bromium pays for itself in just a matter of months. Its powerful and effective endpoint security technology helps financial services organizations virtually eliminate the risk of a data breach and the losses associated with such an event. With Bromium users can click on anything, anywhere without risk of compromise. Bromium streamlines security by eliminating false alerts, urgent patching and remediation.

Conclusion

We now live in a world where the question is no longer if your network or endpoints will be compromised, but when. We know from research studies that the most common and effective way for cybercriminals to target financial accounts and customer records is to compromise vulnerable endpoints and use them as launch pads as part of an advanced threat campaign.

To stand a chance of defeating highly sophisticated and well-funded cybercriminals, financial services organizations have to think differently. It's apparent that traditional network and endpoint security defenses simply can't keep up with today's sophisticated threats.

Bromium offers financial services organizations and their partners a fresh new approach to tackling a very serious dilemma facing their IT security teams. That's why many of the world's leading banks, insurance firms, and hedge fund operators have deployed Bromium's endpoint solution. These customers have been able to protect vulnerable devices such as executives' laptops and targeted employees such as finance personnel and research analysts, reducing disruptions to the daily workflow and the need for regular endpoint reimaging.

By eradicating the vulnerabilities that advanced threats are designed to exploit after each Internet-facing computing task is completed, we're effectively eliminating the attack surfaces of endpoints, which are almost always the initial target of APT attacks and other advanced threat campaigns. You benefit from fewer breaches, greater uptime, lower opex, and better compliance.

For more information

For more information on Bromium vSentry® and Live Attack Visualization and Analysis (LAVA™) endpoint security solutions, contact your Bromium sales representative or Bromium channel partner. Visit us at www.bromium.com.

ABOUT BROMIUM

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.

1 Verizon, “2015 Data Breach Investigations Report”, 2015

2 Kelly, Erin, “Officials warn 500 million financial records hacked”. USA Today, October 20, 2014. http://www.usatoday.com/story/news/politics/2014/10/20/secret-service-fbi-hack-cybersecuurity/17615029/

3 Weise, Elizabeth, “JP Morgan reveals data breach affected 76 million households”. USA Today, October 3, 2014. http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/

4 Riley, Charles, “Insurance giant Anthem hit by massive data breach”. CNN Money, February 4, 2015. http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/

5 Ponemon Institute, “2014 Global Report on the Cost of Cyber Crime Benchmark Study of Global Companies”

6 Sanger, David E. and Perlroth, Nicole, “Bank Hackers Steal Millions via Malware”, The New York Times, February 14, 2015. http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0

7 Ponemon Institute, “2014: A Year of Mega Breaches Date”, January 2015

8 “Global Payments Breach Tab: $94 Million”, Bank Info Security, January 10, 2013. http://www.bankinfosecurity.com/global-payments-breach-tab-94-million-a-5415/op-1

9 Higgins, Kelly Jackson, “Financial Services Ranks Cyberattacks Top Industry Worry”, Dark Reading, October 23, 2014. http://www.darkreading.com/attacks-breaches/financial-services-ranks-cyberattacks-top-industry-worry/d/d-id/1316917

10 “DTCC Risk Survey Reveals That Threat of Cyber Attack Ranks as the Principal Concern of Global Financial Institutions”, The Depository Trust & Clearing Corporation, October 23, 2014. http://www.dtcc.com/news/2014/october/23/cyber-risk.aspx

11 Verizon, “Threat Landscape Financial Services”, 2013

12 Verizon, “2015 Data Breach Investigations Report”, 2015

13 Kirda, Engin, “Most Antivirus Software Is Lousy At Detecting Advanced Malware”, Forbes, May 21, 2014. http://www.forbes.com/sites/ciocentral/2014/05/21/duck-test-antivirus-software-wont-detect-advanced-malware/

14 Verizon, “2015 Data Breach Investigations Report”, 2015

15 Korolov, Maria, “Banking malware using a variety of tricks to evade detection”, CSO Online, April 16, 2015. http://www.csoonline.com/article/2910329/malware-cybercrime/banking-malware-using-a-variety-of-tricks-to-evade-detection.html

16 New York State Department of Financial Services, “Report on Cyber Security in the Banking Sector”, May 2014

17 Verizon, “2015 Data Breach Investigations Report”, 2015

18 Goldman, David, “Your antivirus software probably won’t prevent a cyberattack”, CNN Money, January 31, 2013. http://money.cnn.com/2013/01/31/technology/security/antivirus/

19 Verizon, “2015 Data Breach Investigations Report”, 2015

20 Heimerl, Jon-Louis, “Why Phishing Works And How To Avoid Becoming a Victim”, Security Week, October 20, 2012. http://www.securityweek.com/why-phishing-works-and-how-avoid-becoming-victim

21 Arvizu, Shannon, “Tablet adoption in the enterprise”, Gigaom Research, August 27, 2013. http://research.gigaom.com/report/tablet-adoption-in-the-enterprise/

22 MobileIron “MobileIron Survey Shows Enterprise Mobility is Shifting Financial Services CIOs to a New Model of IT”, MobileIron Press Release, March 27, 2014 http://www.prnewswire.com/news-releases/mobileiron-survey-shows-enterprise-mobility-is-shifting-financial-services-cios-to-a-new-model-of-it-252622791.html

23 New York State Department of Financial Services, “Report on Cyber Security in the Banking Sector”, May 2014

24 Osborne, Charlie, “Financial sector takes up to 176 days to patch security flaws”, ZDNet, June 2, 2015. http://www.zdnet.com/article/financial-sector-takes-176-days-on-average-to-patch-security-vulnerabilities/

25 Verizon, “2015 Data Breach Investigations Report”, 2015

Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information refer to www.bromium.com
or contact sales@bromium.com