vmware® Carbon Black

WHITEPAPER

Risk & Response: Defending Financial Institutions

KEY BENEFITS

1. Drastically reduce your time to detect and resolve incidents
2. Proactively hunt for threats at scale
3. Respond remotely, in real-time with full control
4. Learn from every attack to evolve your posture
5. Operationalize threat intelligence from numerous sources
6. Integrate with your existing security stack
7. Collaborate with a community of over 30,000 security professionals

INTRODUCTION

For decades, the financial services industry has endured constant change and uncertainty, from the depths of a financial crisis to widespread regulation overhauls. With the advent of more advanced cybersecurity threats, the industry has responded with rapid digital transformation to remain competitive while also pushing the envelope. Today, managing and mitigating cyber-related risks not only draws government scrutiny, but increased consumer scrutiny as well, with longstanding brand reputations anchored to institutions' ability to protect its most sensitive data. In a recent survey of Americans, financial information was considered by consumers to be their most valuable personal information, worth even more than personal or family photos and videos. For consumers, failing to protect their data is a grave violation of trust, to the point where 72% would consider leaving their current financial institution if their sensitive information was taken hostage by ransomware.[1]

Not only does the financial industry need to protect data that is easy to monetize, but investment banks and other noncommercial entities are also charged with safeguarding information surrounding investment strategies, mergers and acquisitions, and market influencers that would be sought after by actors motivated by espionage. With international cybersecurity incidents impacting financial movers and shakers like the SEC and Equifax, security professionals in the industry require maximum visibility into their environments in order to prove to their boards of directors that they have not already been breached, even as new security measures are being implemented.

of consumers would consider **leaving their current financial institution** if their sensitive information was taken hostage by ransomware[1]

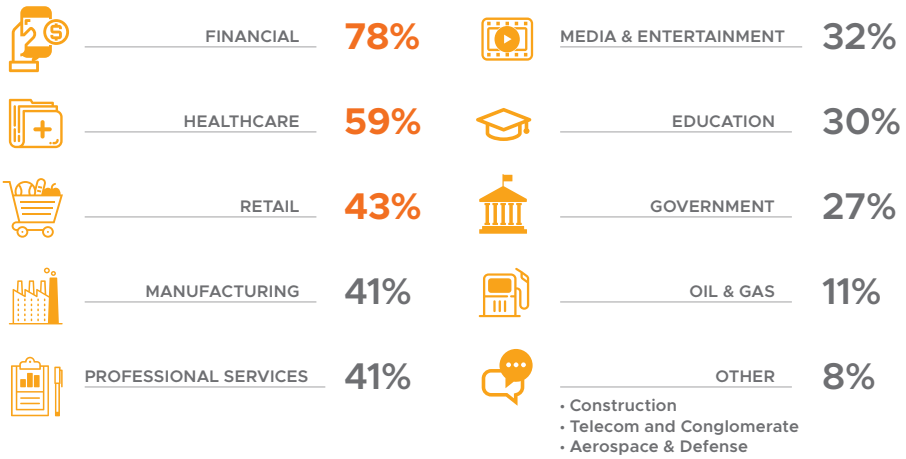
BY THE NUMBERS

76%

of breaches were financially motivated [3]

There is no question that the increase in advanced cyber threats has been significant and it can be difficult to gauge the progress being made. According to a SANS, less than one-third of security professionals felt that recent progress towards their compliance goals was significant. Compared to other industries, financial services is consistently considered to be a top target of cyberattacks.[2] A recent Verizon Data Breach Incident Report has indicated that **76% of breaches were financially motivated**.[3] With financial motives reigning supreme, it is unsurprising that financial organizations continue to face an onslaught of attacks, including banking Trojans and attacks on critical endpoints like ATMs.[4] Despite efforts to reduce vulnerable attack surfaces, financial institutions must keep up with increasing numbers of attacks, the sophistication of the attackers, and the unending rapid evolution of the technology used to stealthily deliver malicious payloads and breach these organizations.

WHAT VERTICALS ARE YOU SEEING TARGETED BY CYBERATTACKS?



TOO LITTLE, TOO LATE

Attacks that disrupt transactions or damage system integrity, even if no sensitive information is immediately exfiltrated, can result in millions of dollars in lost productivity and the possibility that attackers can implement hidden backdoors for future access, despite root cause remediation. Perhaps the most unsettling reality is that the Verizon report also found employee notification to be the most common internal discovery method for the second straight year and that there was also an uptick in detection through internal financial audits, associated with business email compromise. This points to a fundamental breakdown in financial organizations' ability to detect malicious activity. Without continuous monitoring capabilities providing comprehensive visibility down to the endpoint, financial institutions are most commonly broadsided by data breach incidents, with the first notification security teams receive coming from attack victims only after the incident. In an industry where where regulatory compliance often mandates continuous monitoring, gaps in visibility are simply not an option.

THE WEAKEST LINK

The rapid shift in mobility of the workforce has meant that traditional measures to bolster the perimeter security of corporate networks are ineffective when an executive mistakenly clicks a link in a phishing email from the perceived safety of a coffee shop, potentially thousands of miles away from the company's corporate headquarters. Cyber warfare is now being waged by sophisticated actors and highly-organized nation-states beginning on the endpoint, and most security solutions only selectively collect information about endpoint activity, with little regard for the full context incident responders will need after an incident has occurred. Without a clear picture of activity across the enterprise, financial institutions will never be able to fully understand a cyberattack in the context of the complete attack chain to effectively close security gaps and harden their defenses for the next one.

In the Wild: Emotet Banking Trojan

Perhaps the most common attack delivery method, phishing emails are often the method of choice for attackers to drop malicious payloads on corporate endpoints. The financial industry is constantly bombarded with both "spray and pray" approaches as well as targeted spear phishing strategies to lure employees into downloading seemingly mission-critical documents. An increasingly common tactic is to leverage macros or other vulnerabilities allowing attackers to execute malicious code from a seemingly harmless document.

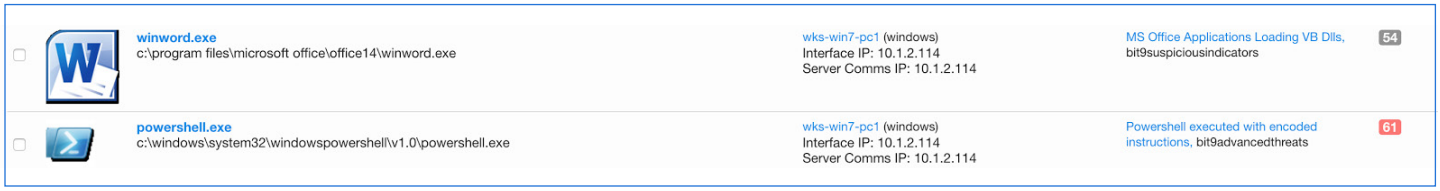
Recently VMware Carbon Black's Threat Analysis Unit (TAU) thoroughly analyzed the Emotet Trojan Dropper seen by a customer in the wild. The technique is fairly simple for the attackers to assemble and deploy, yet still effective and potentially very damaging. Regardless of the payload that is ultimately dropped, the intentions, or skill sets of the attacker in a multi-stage process, it is important to catch the attack at its earliest stages.

Having visibility into your endpoints and focusing on understanding what is normal inside your environment, allows practitioners armed with the right solution to detect malicious or suspect actions.

For Enterprise EDR users on the VMware Carbon Black Cloud, a query obtained through curated threat feeds or manual implementation can easily detect the obfuscated PowerShell commands as soon as the payload tries to execute. Another query can trigger an alerts when Microsoft Word or Excel is detected loading DLLs used by VBA macros.

```
process_name:powershell.exe AND (cmdline:-e * OR cmdline:-en* OR cmdline:-ec*)
```

```
(Parent_name:winword.exe OR parent_name:excel.exe) process_name:powershell.exe
```



Maintaining Compliance

The Cybersecurity Assessment Tool (CAT), developed by the Federal Financial Institutions Examination Council (FFIEC) and the National Institute Standards of Technology (NIST), helps financial institutions identify their risks and determine their cybersecurity preparedness. Banks can use the assessment tool's inherent risk profile to categorize their risk from areas of most concern to least. Once inherent risks are identified, they can rank their cybersecurity maturity level from having the bare baseline of security essentials to being proactive and innovative.

The FFIEC CAT spotlights the need for financial institutions to build cybersecurity risk programs into their existing frameworks for risk management. Enterprise EDR from VMware Carbon Black can assist management with initially determining their upfront risk by nature of their business transactions and operations, and then show how they can enhance their security levels to becoming more innovative.

Domain	VMware Carbon Black Cloud Enterprise EDR
Cyber Risk Management and Oversight	**Change Management** Ensure a state of continuous compliance with the ability to prove that security controls are in place and work effectively, detecting any change in your environment via file integrity monitoring. **Advanced or Automated Analytics** Enterprise EDR offers real-time threat detection and response made possible by the VMware Carbon Black Cloud, which aggregates real-time threat data across the most advanced attacks. This provides instant insight to risk rankings of files, software versions, and publishers.
Threat Intelligence and Collaboration	**Monitor and Analyze Systems and Threats** The Carbon Black Cloud is a comprehensive, aggregated advanced threat intelligence platform that combines leading software reputation, threat indicator, and attack classification services to provide some of the industry's most powerful, correlated and accurate threat insight. Leveraging the power of the Carbon Black Cloud, Enterprise EDR enables security operations and incident response professionals to define trust policies for multiple forms of advanced threat prevention, build custom detection events tailored to specific business requirements, accelerate investigations during a response, and proactively hunt for threats.
Cybersecurity Controls	**Prevent, Detect and Respond** Enterprise EDR provides real-time visibility, detection, response in the face of advanced persistent threats and zero day attacks. It allows security professionals to understand the root cause of an attack and immediately take steps to remediate and respond. The responder can isolate a particular endpoint from the rest of the environment to prevent further damage, but maintain the connection to Enterprise EDR to enable a detailed investigation into the incident.
External Dependency Management	**Segmentation and Third-party Security** Using Enterprise EDR, incident responders can contain active intrusions instantly with one click by remotely isolating one or multiple endpoints from communicating with the network. By maintaining an active connection with Enterprise EDR, even while isolated, IR teams can perform more conclusive and surgical investigations on or off the network.
Cyber Incident Management and Resilience	**Incident Detection, Response, Mitigation and Reporting** Enterprise EDR provides live response for endpoint threat inspection, termination and remediation, allowing staff to understand, perform remote live investigations, intervene with ongoing attacks, and instantly remediate endpoint threats. This enables incident responders to "see" and "touch" endpoints to take immediate action during an investigation — even while the endpoint remains isolated from the rest of the network. Enterprise EDR provides detailed alert notifications via its dashboard and via email, as well as detailed reporting.

Rethinking Your Security Strategy

95%

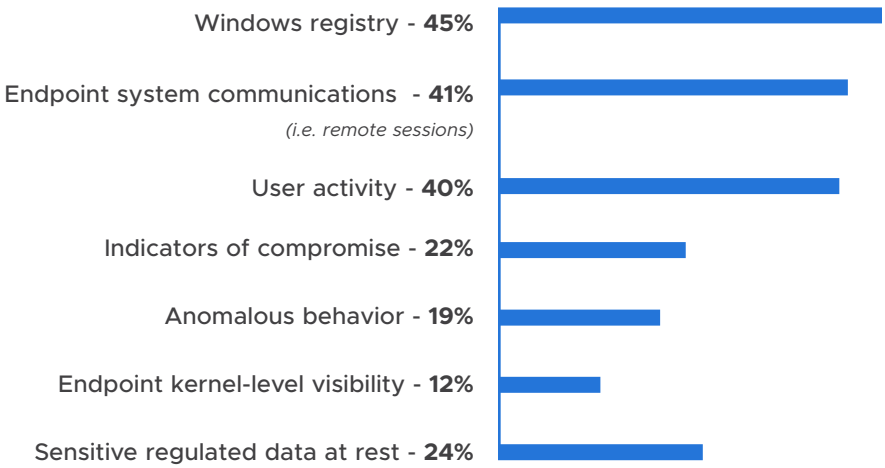
of security professionals agree, **endpoint protection is the most effective** overall control.[6]

The high value of corporate and customer data transmitted and stored by financial institutions, along with the pressure of maintaining compliance with all the relevant frameworks and policies, call for a sophisticated security strategy. Compromises take mere minutes while most organizations can only respond and contain incidents after months of tedious investigative work. an advanced threat hunting and incident response solution delivering unfiltered visibility for top security operations centers and IR teams. Enterprise EDR is delivered through the Carbon Black Cloud, a next-generation endpoint protection platform that consolidates security in the cloud using a single agent, console and dataset. Enterprise EDR allows security professionals to record and alert on every file modification, registry change, network connection, and everything in between. This comprehensive data collected and analyzed via the Carbon Black Cloud, provides cloud reputation and streaming analytics to ensure every bit of relevant information is available and correlated when a post-incident investigation is necessary.

CONTINUOUS VISIBILITY

Enterprise security teams struggle to get their hands on the endpoint data they need to investigate and proactively hunt for abnormal behavior. Security and IT professionals currently lack the ability to see beyond suspicious activity and need a way to dive deeper into the data to make their own judgments.

Enterprise EDR is an advanced threat hunting and incident response solution delivering unfiltered visibility for enterprise SOC and IR teams. By leveraging the unfiltered data collected by the Carbon Black Cloud, Enterprise EDR provides immediate access to the most complete picture of an attack at all times, reducing lengthy investigations from days to minutes. This empowers teams to proactively hunt for threats, uncover suspicious behavior, disrupt active attacks and address gaps in defenses before attackers can. Take a look at the level of visibility other security teams in the financial sector are settling for:



Utilizing advanced threat intelligence feeds (open or proprietary) and custom watchlists, SOCs can automate their detection to catch threats that other solutions often miss. Respondents of a recent SANS survey reported that they are using endpoint detection and response to more quickly identify, stop and remediate threats that penetrate the network, which they consider their most effective control, along with firewalls/IDS/IPS.[7]

RAPID RESPONSE

When an incident does occur, the speed of your response will dictate the extent to which you can minimize the impact. In the case of a malicious attack, it takes on average over 7 months to identify a breach, and nearly two and a half additional months to contain the incident. Every second counts, and while the clock is ticking, the cost of the breach is rapidly increasing as well. **Breaches that take over 30 days to contain cost companies an extra $1 million**, and depending on the severity, it can cost even more.[8] Minimizing dwell time is the name of the game; the faster you can identify root cause, the faster you can remediate.

For the financial sector, the cost of anything less than rapid response is often greater than other industries. According to the 2018 Ponemon Institute cost of a data breach report, **the mean cost of a data breach rose to $148 per compromised record. In the financial industry, that cost was nearly 40% higher, or $206 per record**.[9]

$148

per record

Mean cost of data breach

$206

per record (40% higher)

Mean cost of data breach in financial sector[9]

Enterprise EDR allows incident responders to handle both investigation and remediation from a single user-friendly unified console. A security professional responding to an alert is presented with an interactive process tree, laying out the attack chain from start to finish with full context. From here, incident responders can isolate infected hosts, blacklist suspicious file hashes, and outright ban malicious binaries across the environment with a single click. Enterprise EDR's enterprise-scale unified view enables searching of binaries and processes throughout the environment, allowing for easy correlation of events from a single screen.

For investigations where a more hands-on response is required, Live Response enables incident responders direct access to remediate endpoints no matter where they are in the world. Even after isolating an infected host, Live Response provides a secure connection to the endpoint via a command-line interface. From here security professionals can list and kill processes, drop files or other useful binaries, perform memory dumps, and much much more.

READY TO SCALE

Enterprise EDR is easy to deploy and easy to scale as your financial institution continues to grow. Whether you deploy 200 endpoints or 200,000, our innovative architecture supports growing organizations of any size. With the support of VMware Carbon Black's professional services team, customers have even been able to rapidly deploy more than 100,000 endpoints in as little as 10 days.

In an environment with hundreds of thousands endpoints, an attacker only needs to breach one. Enterprise EDR provides full visibility into every corner of your enterprise to ensure robust detection, freeform threat hunting, and easy identification of security gaps that require further hardening. At a glance, financial organizations can easily gauge the health of all their endpoints and fine-tune detection for all different types of users across the entire enterprise from one unified console. Enterprise EDR also leverages the Carbon Black Cloud's single lightweight agent for maximum performance of the endpoint without any impact on end-users' day-to-day functions.

Continuously monitoring all activity on every endpoint means that when an incident occurs that requires advanced forensic investigation, Enterprise EDR has every bit of data necessary for a full picture of all activity including detailed process analysis to identify root cause and expose all relevant tactics, techniques, and procedures (TTPs) utilized by the attacker. This data can be retained long term regardless of the number of endpoints meaning even the largest financial organizations have visibility into every process on every ATM and corporate laptop. Once that data is recorded, it is readily available for any type of analysis or automation via the robust VMware Carbon Black APIs or myriad integrations with other IT and security applications.

To recap, here's what financial institutions can expect from Enterprise EDR

CONTINUOUS VISIBILITY

Enterprise EDR continuously monitors and centrally stores unfiltered data collected from all your ATMs, servers, and employee laptops meaning regardless of what type of attack unfolds, you have everything you need to rapidly drill down to root cause and automate detection of similar threats in the future.

RAPID RESPONSE

Enterprise EDR reduces attack dwell time with real-time response that correlates IOCs and provides full context of malicious activity. In addition to the ability to blacklist hashes and ban malicious binaries, our Live Response feature allows security professionals to isolate infected hosts and establish a secure remote connection for complete investigation and remediation.

READY TO SCALE

A large financial institution can have hundreds of thousands of endpoints, but an attacker only needs to breach one. You need a solution that scales with your entire organization to hunt and stop the advanced attacker. Our sophisticated data analytics and visualization tools are purpose-built for big data at scale.

To schedule a live demo or obtain more information on how Enterprise EDR protects financial institutions, contact a VMware Carbon Black sales representative today!

Send us an email at: contact@carbonblack.com
Give us a call at: **(855) 525-2489**

1 2017 Carbon Black Ransom-Aware Report
2 From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector
3 2018 Verizon Data Breach Incident Report
4 2018 Verizon Data Breach Incident Report
5 From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector
6 From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector
7 From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector
8 Ponemon Institute 2018 Cost of Data Breach Study sponsored by IBM
9 Ponemon Institute 2018 Cost of Data Breach Study sponsored by IBM
10 Voke Research 2017 Market Snapshot™ Report: Secure Operations Automation

vmware Carbon Black

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com