ExtraHop

FINANCIAL SERVICES

The Threat Inside Your Network: Supply Chain Global Risk and Financial Services

EXECUTIVE SUMMARY

Cyber criminals are taking advantage of vulnerable supply chains, digital transformation efforts, distributed operations, and the ongoing post-pandemic upheaval to increase attacks on financial services institutions and their providers. Exploits have shown that sophisticated attackers will find a way onto your network—and complex, hybrid computing infrastructures make detecting nefarious activity within the network more difficult because of a lack of visibility. The question organizations must ask is: How would you know if your network was compromised? This paper discusses the challenges financial institutions can face when working to mitigate these risks. It offers practical advice on how to detect both known and unknown attacks and ensure your network is protected.

TABLE OF CONTENTS

Introduction 3

The Challenges: Cybersecurity, Covid, & Digital Transformation 4

Digital Transformation & Distributed Environments 4

Evolving From DevOps to DevSecOps 4

Concerns for Financial Services Security 5

Responding to Attacks 5

Threat Landscape: Supply Chain 5

Third Party Vendors Equate to High Risk 6

Vulnerable Protocols Still Present in Environments: NotPetya & WannaCry 7

Visibility & Detection: If Your Network Was Compromised How Would You Know? 8

Encryption 8

Internet of Things 9

Taking the Advantage Away from Attackers 9

Stopping Threats Inside the Network 10

Better Together: NDR + EDR + SIEM 10

NDR Solution: What To Look For 11

ExtraHop Reveal(x) 12

Conclusion 12

INTRODUCTION

The financial services industry and its sectors are a foundational element of a well-functioning society. Those tasked with protecting this important industry, including its intellectual property, customer data and privacy, have an important (and difficult) job. Today's challenges, including work-from-home and other operational challenges, have led to an increase in both attempted and successful cyberattacks

As a storehouse of confidential information with direct access to monetary funds, the financial service industry ranks near the top of the most often attacked industries. Verizon's 2022 DBIR research shows that financial and insurance companies experienced more than 2,500 security incidents, 690 of which resulted in breaches. When an attack is successful, the damage is measured in millions of dollars. According to IBM's Cost of a Data Breach Report 2022, the global average total cost for a data breach in the financial services industry is almost $6 million.

Despite an increased investment in cybersecurity, attackers continue to breach networks. Cyber criminals are taking advantage of an industry that is busily reconfiguring vulnerable supply chains. According to the 2022 Verizon DBIR, 73% of the attacks in this sector are perpetrated by external actors who exfiltrate and monetize stolen data, while 27% are credited to insider attacks. It is clear that even as financial institutions continue to transform their digital landscapes, security and risk teams must move beyond compliance check boxes, learning to assess how they can use these network changes to their advantage.

THE CHALLENGES: CYBERSECURITY, COVID, & DIGITAL TRANSFORMATION

The COVID-19 pandemic and associated economic disruption resulted in a sudden and tremendous change that forced everyone to adjust their priorities.

The shift to "this work-from-anywhere" environment further exacerbated already complex network and cloud visibility challenges. As IT teams struggled to understand what devices employees were using and what network services they were accessing, ensuring proper VPN access became both a performance and security issue—and an immediately critical issue at that.

It also led financial service companies to reimagine their strategy and technology choices for the future.

Digital Transformation & Distributed Environments

Digital transformation offers the promise of increased agility to respond to market changes and deliver better digital experiences. On top of already in-progress transformations, remote work prompted a seismic shift in the use of digital services by financial services' customers. This, in turn, required that some banks and other financial enterprises revise policies to accommodate new ways of accessing services, like changing virtual transaction limits and enabling electronic signatures.

> "(Web applications) provide a useful venue for attackers to slip through the organization's 'perimeter' by using clever tricks like (spoiler alert) stolen credentials.

Evolving From DevOps to DevSecOps

As containerization and serverless computing adoption increases and applications are spun up or moved to the cloud, risk rises. DevOps teams gain portability and flexibility—and with minimal effort compared to past methods—but this is not always done with a security-first mindset. If new applications are being added and removed quickly, are these fledgling resources being monitored and secured?

And while the CI/CD tool chain has enabled teams to automate much of the application development process, delivering cloud-native apps with record speed, these serverless computing options come with a cost. The very speed and automation that make these processes attractive also leave them more vulnerable. Leaving application security as a final step or as an afterthought results in weak security that can make the DevOps pipeline itself an attractive target to attackers.

Advanced attacks are bold and persistent, using increasingly sophisticated, well-resourced attacks to identify and compromise high-value targets. Attackers recognize the opportunities presented by the distributed nature of modern architectures, including supply chain relationships and Internet of Things (IoT) vulnerabilities. They continue to find new ways to get on the inside, while still also employing traditional attacks (e.g., phishing and email compromise,) to deploy malware, ransomware, and DDoS attacks.

Web applications were involved in 56% of breaches

(Verizon 2022 Data Breach Investigations Report)

CONCERNS FOR FINANCIAL SERVICES SECURITY

For the Financial sector:

79% of breaches were performed by organized crime

#1 action performed was the use of stolen credentials

14% of breaches affected availability

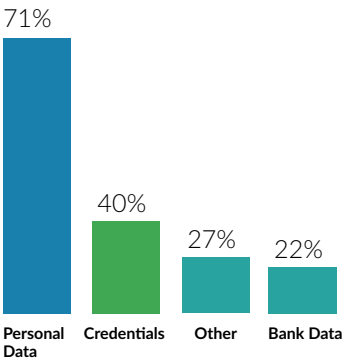
[Source: Verizon 2020 Data Breach Investigations Report]

Responding to Attacks

The security level for any given enterprise depends on how well they are equipped to respond to vulnerabilities and attacks both at the edge of, and inside, the network. Smaller organizations, (such as regional banks and smaller credit unions), tend to have a lower level of cybersecurity investment and management. This lack of resources places them at a higher risk. For attackers, organizations in this position are low-hanging fruit.

Conversely, larger financial organizations, such as insurance companies and multinational banks, are more likely to have greater funding and larger IT and security teams to focus on security and attract experienced talent. This focus often makes such organizations better at defending against attacks. Yet, even as more resources for defenses can mean a greater challenge for attackers, the rewards are also higher: larger organizations means more data, more resources, and more revenue.

Data compromised in breaches



[Source: Verizon 2022 Data Breach Investigations Report]

Threat Landscape: Supply Chain

The complexity of the software supply chain increases risk for any organization, and supply chain attacks are stealthy and destructive. Third-party connections create a potential vulnerability that is difficult, if not impossible, to detect until it's too late. For attackers, going after an element of the supply chain is an unobtrusive way to infiltrate organizations, either for financial gain or to simply disrupt operations.

As financial services organizations work with third-party providers to meet specific strategic and operational goals, they must also pay attention to the potential risk. Given the volume and sensitive nature of data managed by financial institutions (not to mention strict privacy regulations and standards, such as GLBA, CCPA, GDPR and PCI), financial service organizations must be extra cautious and vigilant when it comes to security.

Managing risks in the supply chain requires internal controls and transparency, and due diligence over the security policies and procedures of third-party vendors. But oftentimes, that isn't enough. Phoning home, a process of exfiltrating data, happens with third-party vendors, often without the knowledge or permission of data owners. Add to this unpatched software and vulnerable code leaving millions of devices open to attack (as in the cases of Ripple20, Log4j, and Spring4Shell), we see that there are many ways for motivated hackers to find their way inside and those doors, quite often, have little to do with your organization.

Common elements in many successful supply chain attacks:

- Meticulous preparation and surveillance
- "Legitimate" entry with stolen credentials
- Remote command and control
- Stealthy movement
- Post-execution coverup and removal of digital footprints

[Source: SUNBURST, Why Supply Chain Attacks are So Disruptive, ExtraHop]

Typical suppliers in the financial services supply chain include clearance and settlement suppliers, payment handling, information technology providers, servers and data centers to store and process data, customer call centers, facilities management, marketing and advertising, and other services and departments. For branch operations and ATMs, the supply chain also includes the physical equipment that processes and distributes currency to customers. In short, there are many opportunities for compromise across the software supply chain.

In the US, there are regulations in place that recognize the vulnerabilities that expose financial institutions to third parties. The Frank-Dodd Act, for example, created the Consumer Finance Protection Bureau (CFPB) that requires financial services companies to ensure their suppliers comply with all CFPB regulations. The firms themselves can be held accountable for violations within their supply chain, giving them even more incentive to conduct cybersecurity due diligence.

The Network Visibility Problem

In today's distributed computing environments, we need a greater understanding of what is connected to the network. With so many third-party connections on hybrid networks, the number of unmanaged devices and IoT, and all of the different services that are communicating on our networks, it's imperative to increase network visibility.

In the case of SUNBURST, the attack was built into the software's update, allowing SolarWinds to bypass all perimeter controls and sit in a very privileged position within the network. To identify breaches like these, security teams need insight into the east-west corridor to see any unusual activity inside the network that would indicate an attacker was trying to move laterally. And, frankly, without a perimeter breach, watching lateral movement tends to be pushed to the bottom of the list.

The breach was only discovered when two major customers, Visa and Mastercard, notified Heartland of suspicious credit card processing activity.

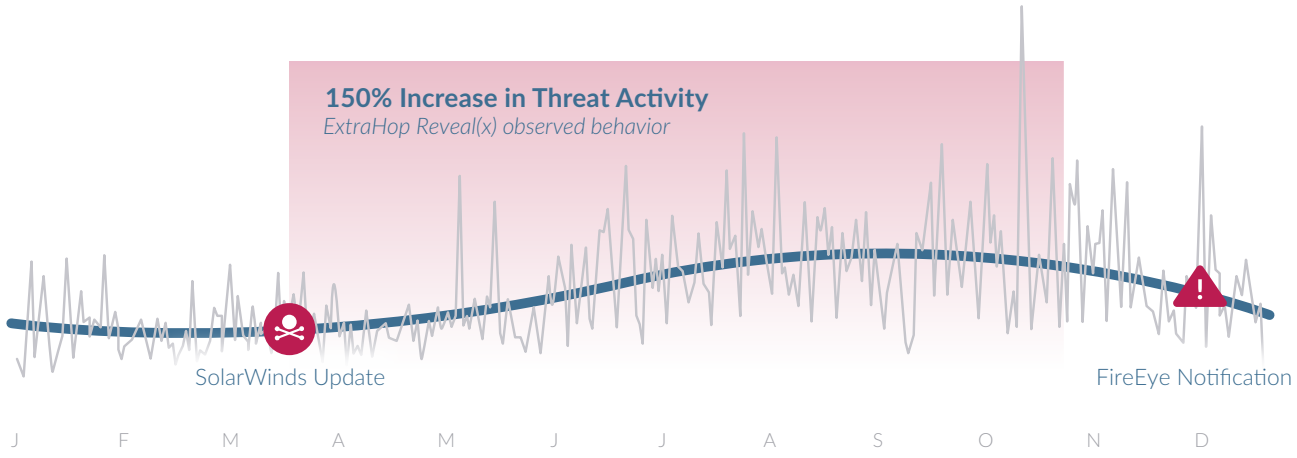
Investigations into the attack highlight the network visibility problem, with examples of a few financial services organizations who discovered SolarWinds servers that they didn't know about and hadn't secured. By exploiting third-party relationships, the attackers, believed to be state-sponsored, were able to breach the networks of government agencies, insurance companies, each of the top five US accounting firms, as well as banks. Research by ExtraHop showed that between late March and early April 2020, there was a suspicious and visible change in network behavior—threat detections had increased by 150%. While a direct line cannot be drawn to the attack, this activity did align with the height of SUNBURST post-compromise activity.

Vulnerable Protocols Still Present in Environments: NotPetya & WannaCry

Not all attacks are designed to steal credit card data or financial data; some are designed to disrupt. In 2017, operations at Maersk shipping, Merck Pharmaceuticals, and a FedEx subsidiary ground to a halt. It has been called the most devastating malware in history, costing FedEx and Merck almost $1 billion to recover. For global shipping leader Maersk, the attack crippled operations around the globe and led to one of the most stunning IT recoveries in history.

The attack used a legitimate update to accounting software called M.E.Doc, a tax preparation program the Ukrainian government required all its vendors to use, to add backdoors and then install ransomware. The ransomware, known as NotPetya, used credentials that it harvested from the system it had infected to spread to other, laterally-connected systems. Through this, it was able to spread rapidly throughout the globe, disabling and destroying systems as it went. The motive appears to have been nothing more than to permanently destroy data.

Like NotPetya, WannaCry also leveraged the EternalBlue vulnerability, which exploits issues found in older versions of Windows, specifically those that still use the SMBv1 protocol. And while protocols like SMBv1 and LLMNR are still a vulnerability and should be deprecated to ensure organizations can't be hit with WannaCry again, research shows that this is not necessarily happening.



An ExtraHop study shows that 70% of enterprises still use devices that contain the SMBv1 protocol. For financial services organizations, it's critical to remove these vulnerabilities. These breaches are examples of some of the biggest supply chain attacks in recent history, representing losses of billions of dollars for financial services and other firms. If NotPetya was an anomaly, SUNBURST was a wakeup call. These attacks are here to stay and the complexity of supply chains increases security risks for any organization along the line.

Visibility & Detection: If Your Network Was Compromised How Would You Know?

Complex, hybrid computing infrastructures make detection of nefarious activity within the network more difficult because of a basic lack of visibility. Add in the ever-increasing numbers of unmanaged devices, BYODs and IoTs, as well as the transition to remote work, and network security has grown even more complicated. Recent exploits have also shown us that once inside, attackers have free reign and virtually unlimited time to move laterally and undetected as they escalate privileges until they hit their desired target. Network security has become a veritable Where's Waldo of attacks: the larger the picture, the more difficult they are to find.

Encryption

With the broad adoption of TLS 1.3, visibility becomes even more challenging. According to EMA research in 2022, 86% of survey respondents indicated that data security was the greatest benefit of TLS 1.3 adoption. However, 89% of respondents said they were concerned that TLS 1.3 would disrupt their existing network and security monitoring. Not all organizations have adopted TLS 1.3, and almost everyone in that group (96%) stated that the loss of visibility was the primary reason.

While it's important to upgrade encryption to TLS 1.3 with perfect forward secrecy (PFS), it's also wise to consider how you will inspect encrypted traffic for malicious code. There are two standards to consider: Encrypted Traffic Analysis and Decryption. Both are required for a better security posture, however decryption is the only way to uncover advanced threats like SQL injection, cross-site scripting, SSRF (used in Microsoft Exchange attacks), Kerberos Golden Ticket, and DNS exploits, just to name a few. For a detailed overview on the importance of decryption while maintaining compliance, read: Encryption vs. Visibility: Why SecOps Must Decrypt Traffic for Analysis.

Internet of Things

IoT has grown exponentially, especially in the financial sector. There are a broad range of IoT devices that provide benefits and drive value—from banking apps on wearables, to beacons in bank branches that help track customer flow and traffic, to using scanners or personal mobile phones as authentication and identification devices.

The caveat is that IoT devices broaden the attack surface exponentially. They are most often insecure and often go unserviced (i.e., they are not patched or given software upgrades), providing potential entry points into the network. Once inside, IoT devices can provide a place to hide. Their existence on the network changes the shape of incident detection and response.

Case in point is Ripple20. The initial disclosure revealed nineteen different vulnerabilities (largely connected to TCP/IP Protocols) in connected devices manufactured by Treck. These vulnerabilities left one in three environments exposed. The affected TCP/IP protocol suite library is embedded in millions of IoT devices that are nearly impossible to trace. While an attack has yet to surface from these devices, the potential is immense.

TAKING THE ADVANTAGE AWAY FROM ATTACKERS

Financial services firms are at the upper echelon of investments in information security controls, yet there are still gaps in coverage. As recent attacks have demonstrated, sophisticated attackers will find a way onto your network. Whether it's through third-party-controlled connected devices, or the supply chain, a vulnerability anywhere along the chain can affect your network, even with rigorous vendor management and due diligence. The question organizations must ask is: How would we know if our network was compromised?

Strong initiatives like zero trust and practices like network segmentation aren't enough when trusted IT solutions leave partner organizations vulnerable. Traditional sources of security data, such as logs, and agent-dependent solutions (like endpoint detection and response [EDR]) still leave major blind spots within modern networks; some legacy protocols don't track activity at all and many devices can't support agents. Our ever-expanding interconnectivity is a wild card, able to be played at any moment, and used in unexpected ways.

Compliance requirements for reporting a breach

FINRA: Immediately report to the FBI and FINRA Regulatory Controller
PCI-DSS: Engage a Payment Card Industry Forensic Investigator (PFI) for relevant cases
GDPR: Inform relevant supervisory authority
SEC/SOX: Inform investors

Stopping Threats Inside the Network

There are three core elements to consider that will empower financial security IT teams to stop threats once they are inside the network: visibility, real-time threat detection, and the ability to perform both proactive and retrospective investigations.

Complete Visibility

- Complete visibility starts with a real-time understanding of everything that is connecting to the network, including unmanaged and IoT devices. It's not just about the ability to understand that an asset exists, but to know what its intended function is and how it should behave on the network, including who/what it is allowed to talk to.
- Next is directional visibility, both the east-west traffic inside the organization, as well as the north-south traffic into and out of the organization.
- Encrypted traffic: The deprecation of TLS 1.0 and accelerated adoption of TLS 1.3 requires visibility inside the payload to understand if the traffic is safe.

Real-Time Threat Detection

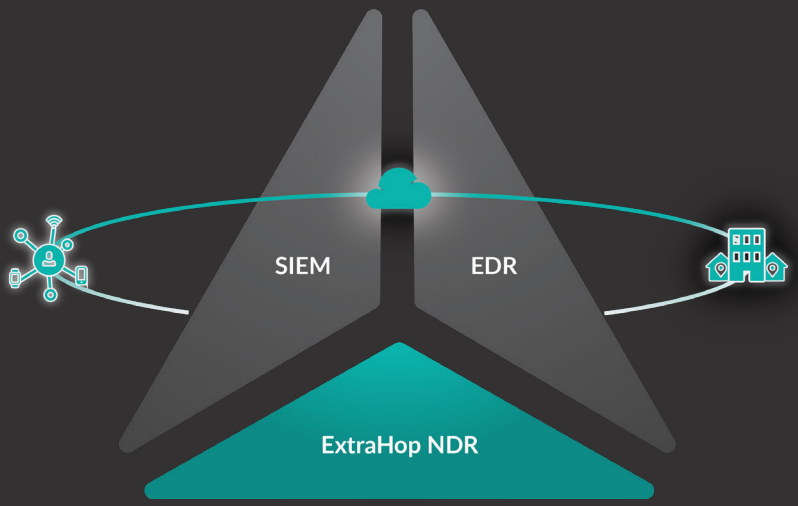
- Machine learning offers the opportunity to understand normal behavior and detect unusual activity on a hybrid network.
- Detecting threats in real-time is not just about one event; you need the context and correlation of every related activity inside the network to identify and stop malicious behavior.

Investigation & Response

- Your analyst's time needs to be spent on the alerts that matter most, not chasing false positives. Having the right data, context for insights, and intuitive workflows can improve your investigations to stop advanced threats faster. Investigations into whether you have been impacted by a vulnerability and Threat Hunting require not only data in the present, but in the past as well.

Better Together: NDR + EDR + SIEM

Network detection and response (NDR) is uniquely suited to stop threats once an attacker is inside the network. Continuous monitoring detects intrusion as soon as possible, and is invisible to attackers. NDR can detect both known and unknown attacks, and presents a trusted source of truth—if the system says it happened, it happened. Using machine learning, NDR solutions learn the network and how it should behave, and respond when they recognize something out of the ordinary.



SOC Triad

- EDR: Real-time endpoint monitoring is critical in identifying the first sign of an attack, but agents can be tampered with and complete coverage is rare.
- SIEM (security information and event management): Monitoring users and entities and logging activity provides intelligence. As you may know, however, logs can be voluminous and potentially turned off or deleted by attackers to cover their tracks.
- NDR: NDR fills in the gaps left by EDR and SIEM. By monitoring traffic inside the network for unusual behaviors, an NDR can detect, investigate, and respond to threats inside the network in real-time.

NDR Solution: What To Look For

The ideal NDR solution has the following characteristics:

1. Real-time, automated discovery and asset inventory
2. Automated investigation with 90-day lookback
3. Out-of-band decryption
4. Investigation outside of a detection
5. Turn Tier 1 analysts into threat hunters
6. Cloud-based machine learning
7. Peer group detection
8. Confident response orchestration
9. Supports NIST cybersecurity framework
10. Supports the MITRE ATT&CK framework

EXTRAHOP REVEAL(X)

Conclusion

In today's distributed computing environments, financial institutions face significant challenges when securing their networks. Major breaches like SUNBURST, NotPetya, and WannaCry have caught organizations and their suppliers off guard. These sophisticated attackers have had free rein and ample time to move undetected. The answer to this is network detection and response, along with EDR and SIEM. Together, these three provide a defense-in-depth security solution that is uniquely suited to stop these types of threats.

For financial services, data and privacy breaches have a great potential for catastrophic financial and reputational damage. Limiting damages and avoiding regulatory fines requires a strategy that includes monitoring network data and ensuring PCI Data Security Standard (DSS) compliance. While the network will never be completely impenetrable, the opportunity to stop a breach lies in the ability to detect threats pre-compromise as we learn how to monitor both east-west and north-south traffic, detecting vulnerabilities, and spotting unusual behavior before it becomes an attack.

ExtraHop Reveal(x) provides financial services organizations with complete visibility into hybrid and multi-cloud networks to stop advanced threats before they breach. Try our demo and learn how ExtraHop Reveal(x) can help your financial services organization to stop more threats and lower your overall risk.

About ExtraHop

ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyzes all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customer to identify suspicious behavior and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI 50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop Breaches 84% Faster. **Get Started at www.extrahop.com/freetrial**

ExtraHop

info@extrahop.com
www.extrahop.com