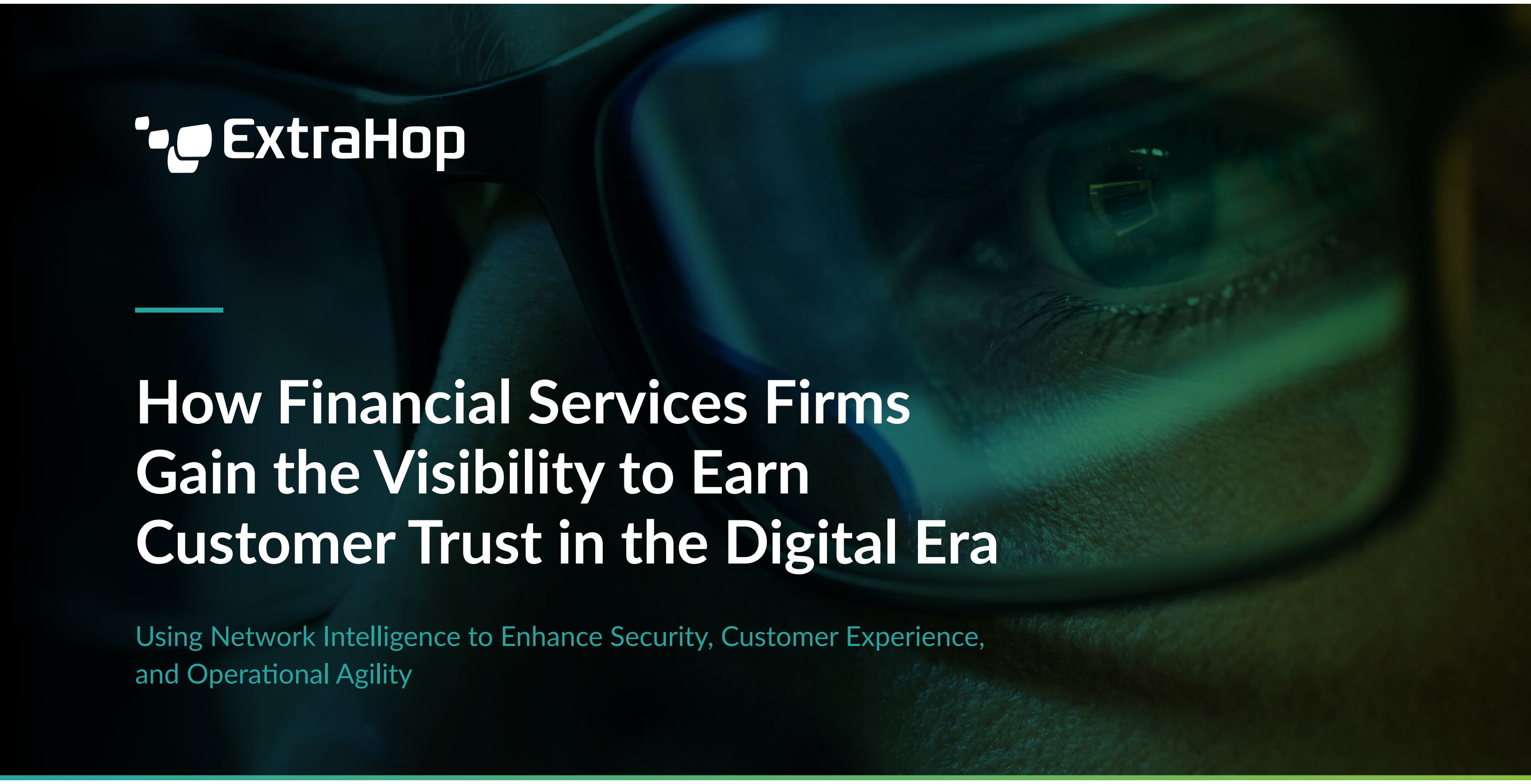

ExtraHop

How Financial Services Firms Gain the Visibility to Earn Customer Trust in the Digital Era

Using Network Intelligence to Enhance Security, Customer Experience, and Operational Agility

Executive Summary

The financial services sector has become highly competitive as financial institutions, fintechs, and large technology players innovate at a rapid pace. To be successful, organizations must remain agile in the face of challenges and changes, while strengthening trust and loyalty with their customers. When customer trust is strong, financial services firms reap competitive and reputational benefits. Trust drives revenue, but trust is easily lost.

This white paper explores how financial services organizations can bolster their competitive agility with better network visibility, which enables security and IT operations teams to deliver excellent customer experiences, maintain the security of sensitive data, and drive organizational efficiency. Complete visibility across distributed networks and the ability to take quick action on insights play essential roles in the operational success of financial institutions today.

Introduction

As more and more services have shifted to online and hybrid models, customers increasingly expect frictionless, personalized, and intelligent digital experiences from their financial services institutions. With fewer in-person interactions, customer loyalty is harder than ever to earn. Furthermore, recent concerns over economic uncertainty, the prospect of a recession, and a handful of bank collapses have led customers to reassess the trust they have placed in financial institutions. Delivering a reliable and secure digital customer experience is not only foundational, but also critical to cultivating strong customer relationships, leading to a larger number of accounts, and increasing the number of services utilized per customer.

As the infrastructure that supports the customer experience shifts to the cloud and customers have new concerns about cloud service providers, new levels of visibility are required to understand and prevent potential issues across distributed networks. Meanwhile, security teams are spread thin, monitoring multiple security products and performing time-consuming manual tasks, such as ticketing and reporting. To remain competitive, organizations must optimize efficiency and be quick to respond to potential incidents, while ensuring that controls don't hinder performance or innovation.

> To remain competitive, organizations must optimize efficiency and be quick to respond to potential incidents, while ensuring that controls don't hinder performance or innovation.

The Challenges of Change

When it comes to their digital presence and IT infrastructure, financial services institutions face three major challenges: protecting critical and sensitive data against ever-present threats, delivering the best customer experience, and operating efficiently with the agility to maintain a competitive position.

Protecting Data in the Face of Never-ending Threats

Financial services institutions inherently deal with highly sensitive data, including personally identifiable information (PII), business loan applications, and global financial transactions. As a result, these firms are increasingly under attack from bad actors including emerging threats from nation states and organized hacking groups that seek to steal data, commit fraud, or disrupt business. One recent report shows that 25% of malware attacks now target financial services companies.[1] According to a report from Deloitte, 82% of financial services organizations had experienced between one and 15 cyber incidents or breaches between 2020 and 2021.[2]

Attackers are changing their methods to exploit the industry's move toward digital transformation. The 2022 Verizon Data Breach Investigations Report indicates that servers were involved in 90% of data breaches of financial companies, up from just 50% in 2016 — with a marked rise specifically in web application servers (51%, up from 12%).[3] The shift to more interconnected digital experiences has brought with it new risks and opened new methods of attack. Defending critical data against these attacks is increasingly vital to maintaining the success of the business.

[1] "Introduction to Financial Services: Financial Cybersecurity," Congressional Research Service, Jan 2023.
[2] "Cybersecurity in a post-pandemic world: A focus on financial services," Deloitte, 2022.
[3] "Data Breach Investigations Report," Verizon, 2022.

The Changing Network Landscape

The modern network landscape has evolved, and financial institutions now must secure not only a single internal corporate network, but also assets in multiple clouds, colocation data centers, in the homes of remote workers, and across third-party software and service providers on distributed networks. Properly securing these modern networks alongside legacy infrastructure, requires additional visibility to fully understand what devices are connected and what data is moving between them—wherever the devices may be located. This requires a cybersecurity solution that is not environment specific. Some important elements to consider include:

Real-Time, Continuous Device Inventory

The first step on the path to security is to see and clearly understand everything that's connected to the network. Without an accurate, up-to-date inventory of devices, security teams won't know what needs to be secured or what potentially poses a threat. Devices with firewalls or other protections may not respond to ping requests or port scans, so new methods of discovery are needed. This is also incredibly valuable to identify assets that companies inherit during mergers and acquisitions.

Visibility at Enterprise Scale

Institutions need complete visibility across their entire infrastructure, including their remote sites, thousands of branch locations, and all applications. Companies need to identify suspicious behaviors and potential threats in real-time, leveraging cloud-scale machine learning to analyzes petabytes of anonymized threat telemetry daily, without impacting performance.

Visibility into Threats Hiding in Encrypted Traffic

Encrypted traffic presents a unique problem. While designed to maintain confidentiality of data in motion or at rest, encryption can also create a blind spot in which malicious activity can hide. Methods of selectively decrypting network data are important to reveal activity that may be obscured, without compromising the intended security aspects.

Protocol Fluency

Similarly, to get a deeper understanding of what data is moving within the network, financial institutions need capabilities to analyze the network protocols used, including application-layer protocols. This can shed additional light into the nature of the data and the interaction and into whether any activity is suspicious.

Historical Analysis

When a new zero-day vulnerability is announced, it's important to be able to look back at historical data to evaluate exposure based on patterns that may indicate the vulnerability has already been exploited within the network. Access to months of historical data is more useful than access to just a few weeks of data.

Third-Party Risk

Software supply chain attacks are now a common point of ingress for attackers. These attacks infiltrate a less secure third-party organization to exploit an existing trusted connection to the financial institution. Companies must work to secure third-party software to ensure these applications do not introduce gaps in their protection. Understanding how data is flowing to and from these applications can immediately illuminate when there is activity that indicates a compromise.

Rapid Response

When detecting a compromise and preventing an attacker from achieving their full objectives, timing is critical. Analysts need easy investigation workflows with full context to help them make educated decisions quickly on high-impact risks, and they need high-fidelity data to confidently automate low-impact risks. Additionally, access to packet-level data can provide the depth necessary to support deep forensic investigations.

Expanding Compliance Requirements

Financial services institutions are also subject to a multitude of security standards, compliance regulations, and reporting requirements, such as PCI DSS, PSD2, GLBA, GDPR, ISO 27001, and others, including state-specific legislation. These measures are designed to help protect customers and ensure confidentiality and security of their personal data, as well as the integrity of records.

Financial services institutions must demonstrate they are acting properly through implementation of strict security controls and audits that assess compliance with the regulatory requirements. Gaining a full understanding of how assets relate and connect across the network is key to identifying risk scenarios and implications, as well as improving security hygiene and compliance. For companies undergoing merger and acquisition activities, it is equally important for both the acquiring organization and the acquired to have confidence that compliance standards have been well met.

The Consequences of Non-Compliance or Breach

If the financial institution is unable to demonstrate compliance with regulations, it can be subject to increased scrutiny, hefty fines, and negative public perception. Financial services institutions simply cannot afford to miss the mark on these measures. If a breach succeeds, institutions also need access to deep forensic information to understand the details of the breach, the data involved and the period of time that the breach was active to properly respond and report on it.

$5.97 million

Average breach cost for financial organization in 2022[6]

A breach can also lead to a loss of customers, beyond the hard costs of remediation and insurance premium increases. According to research by Ponemon Institute, the average cost of a data breach for financial organizations in 2022 was $5.97 million.[4]

The reputational damage can also have a massive impact. Research by McKinsey found that 87 percent of survey respondents said they would not do business with a company if they had concerns about its security practices.[5] To maintain operations, financial institutions must take every measure to avoid breaches.

[4] "Cost of a Data Breach Report 2022," IBM, Research by Ponemon Institute, 2022.

[5] "The consumer-data opportunity and the privacy imperative," McKinsey & Company, April 2020.

[6] "Cost of a Data Breach Report 2022," IBM, Research by Ponemon Institute, 2022.

Delivering Best-in-Class Customer Experiences in the Face of Rapid Change

The financial services sector faces stiff competition as innovation continues to drive organizations to deliver more innovative and highly complex finance-related applications. Fintechs are competing with traditional players, and they have fewer ties to legacy systems, allowing them to move quickly to take market share for the services they offer. As financial services companies look to maintain and advance their positions, IT operations teams must address new challenges.

Rising Customer Expectations

Customers have come to expect streamlined, personalized experiences to meet their evolving needs. They want access to these services online and on-the-go. Customer onboarding and servicing is now driven by digital verification and authentication technology supported by the cloud. These new digital processes generate vast amounts of data, which can be analyzed by algorithms in the cloud to provide insights into the exact point in time the business needs to help the customer.

Applications may connect to core banking platforms, third-party applications, or data located across multiple services, multiple clouds, and multiple tiers. With the application delivery chain often spanning hybrid environments, it is critical for IT operations teams to be able to accurately detect and pinpoint performance issues before the customer experiences any latency or downtime.

> It is critical for IT operations teams to be able to accurately detect and pinpoint performance issues before the customer experiences any latency or downtime.

Cloud Migration

Many companies are migrating data and applications to the cloud for the ability to scale rapidly while reducing costs. However, as they perform these migrations, it is important to identify any negative performance impact as each component is moved. This requires having a clear understanding of application dependencies and potential risks, as well as having access to performance metrics before and after migration. Unified visibility can help to identify vulnerabilities and pinpoint the root causes of performance issues across a hybrid, multicloud environment.

M&A Activity

Financial institutions are also going through M&A activity at unprecedented rates in recent years. According to one report, U.S. M&A activity in the financial services industry rose 38% in 2021 over the previous year, to more than $284 billion.[7] This activity can introduce both cyber risks and potential performance issues. If the acquired organization handles their sensitive data irresponsibly, or has existing vulnerabilities, threat actors may exploit these gaps to obtain access to the acquiring company. Furthermore, companies must integrate networks and applications without introducing performance or availability issues. In both cases, the acquiring company needs complete visibility into the acquired organization to swiftly mitigate risk. Companies must ensure a seamless experience for the end customer.

Meeting the Challenge

Financial institutions must meet customer expectations to succeed. According to a report by Qualtrics, 70% of financial services customers leave their institution because of a series of minor failures to meet expectations over time.[8] IT operations teams must ensure performance issues do not negatively impact customer experience. To ensure performance from source to screen, teams need complete visibility from layers 2 through 7 of the OSI model.

The Open Systems Interconnection (OSI) Model

The OSI model provides a standard for different computer systems to communicate with each other.

7	**Application Layer** Responsible for the protocols (for example, HTTP, SMTP, DNS) and the data manipulation on which the software relies to present meaningful data to the user	← Complete Network Visibility →
6	**Presentation Layer** Responsible for compressing, encrypting, and decrypting data as well as translating data into a syntax that can be understood by applications, networks, and devices	
5	**Session Layer** Opens and closes communication between devices, ensuring the session stays open long enough to transfer all required data, and then promptly closes it to avoid wasting resources	
4	**Transport Layer** Transmits data using transmission protocols (for example, TCP, UDP); handles flow control (ensuring optimal transmission speed) and error control (ensuring data is complete) for inter-network communications	
3	**Network Layer** Facilitates data transfer between different networks, breaks segments into smaller packets on the sender's device and reassembles packets on the receiving device, and routes data via the best path	
2	**Data Link Layer** Facilitates data transfer between devices on the same network; handles flow and error control for intra-network communications	
1	**Physical Layer** Transmits the raw bit stream (1s and 0s) over physical equipment such as the cables and switches; uses electricity to place a stream of raw bits from the data link layer onto physical pins and wires	Hardware Visibility

[7] "Financial Services M&A 2022," Law Business Research Ltd, February 2022.

[8] "Experience Leadership in Financial Services," Qualtrics, n.d.

Improving Operational Efficiency

The same economic uncertainties in the current market that are worrying customers also impact how financial services institutions must operate. Companies must strive to increase revenue and retain customers while minimizing costs and maximizing the return on investments. This can take the form of accelerating their deployment of cloud infrastructure to reduce costs and gain scalability, by providing greater depth of visibility to speed up response to security and performance issues, or by driving efficiency through cross-team cooperation.

Financial institutions can also benefit from integration with the tools they have already invested in. Network visibility solutions should fully integrate with ticketing solutions, SIEM, SOAR, next-generation firewalls, and other existing tools to accelerate response to potential issues. By integrating high-fidelity network data into their systems, financial institutions can better prioritize risks and enable smarter automation. Teams can reduce time spent manually writing rules for IDS/IPS, orchestrating service tickets and responding to low impact threats, freeing them up to take on more strategic tasks.

Breaking Down Silos

To deliver excellent customer experience efficiently, both IT and security operations must work in support of common goals. Both teams can identify and resolve potential problems faster with complete visibility provided by network data.

As the observed record of every communication between every system, network data is unique in its integrity. Logging alone may miss key activity, and agents may fail to capture critical data. Furthermore, log files can be erased, and agents can be disabled. Network data, however, cannot be erased and provides a record of all activity. This unobstructed visibility is a critical benefit across IT and security teams. In an era when companies are looking to reduce spending and consolidate toolsets, network intelligence can be a trusted investment.

When companies integrate common data into the systems and processes used by multiple teams, they can eliminate siloed activities and enhance efficiency. Each team can quickly understand what the other is seeing with a common source of the "truth." Research by Forrester found that 79% of respondents see an integrated solution that benefits both networking and security objectives as appealing or very appealing.[9] The report also found that 65% of respondents believe integration between tools and technologies is the most significant factor requiring improvement to achieve better collaboration.[10]

> In an era when companies are looking to reduce spending and consolidate toolsets, network intelligence can be a trusted investment.

[9] "20/20 Visibility Clarifies Network Security," Forrester, July 2022.

[10] "20/20 Visibility Clarifies Network Security," Forrester, July 2022.

The Impact of Network Visibility and Intelligence

A new level of visibility is required to meet organizational needs, and it should provide greater depth into network activity and better integration with existing processes and tools. Network visibility refers to being aware of everything connected to and moving through the network. A network visibility solution should provide the necessary data and actionable intelligence to multiple parts of the organization, and it should be able to help overcome the challenges institutions face, empowering teams to deliver on security, customer experience, and business operational goals.

> Forrester research found that security and network leaders agree that better network visibility improves security and response (81%), performance (76%), and operational efficiency (72%).[11]

Benefits for Security Operations

In financial services institution, threats can include a range of sources–from external hackers to malicious insiders. With complete visibility of network activity, security teams can better identify and more quickly mitigate suspicious behavior, advanced persistent threats, and attacks. In particular, teams gain:

- Real-time, continuous device discovery and classification of all activity communicating on the network.
- Unified views across local data centers, colocation data centers, and hybrid and multicloud environments to ensure consistent monitoring.
- Visibility that extends across third-party applications, leveraging machine learning and artificial intelligence to analyze and recognize patterns.
- Detection of hidden threats within encrypted traffic.
- Real-time detection capabilities along with actionable intelligence to detect suspicious behavior and stop known and unknown threats.
- Identification of vulnerabilities and improved security hygiene.
- Integration with existing security tools and processes to speed response.
- Packet-level data collection and retention to support forensic analysis when needed.
- The ability to meet compliance requirements and prepare for evolving legislation around breach disclosures and reporting.

[11] "20/20 Visibility Clarifies Network Security," Forrester, July 2022.

Benefits for IT Operations

Likewise, IT operations teams gain the insight they need to quickly locate and resolve performance issues before issues impact customer experience. Benefits for these teams include:

- A more complete view of what on the network is impacting performance and where problems are, with visibility into more layers of the OSI model.
- Consistent views across on-premises, cloud, and third-party provider environments.
- The ability to confidently manage cloud migrations or M&A related network integrations, without impacting performance.
- Deep investigative capabilities to pinpoint problems and resolve them more quickly.
- The ability to support the infrastructure that enables a modern customer experience.

Benefits for Business Operations

Improved network visibility can benefit the business in both direct and indirect ways, enabling companies to:

- Make teams more effective and break down silos.
- Leverage integrations with existing tools to increase efficiency and speed response.
- Take advantage of cost-saving technologies without impacting performance.
- Reduce or eliminate point solutions providing overlapping (but less complete) information.
- Deliver excellent customer experience, retain customers, and stay competitive.
- Prepare for next moves and remain a step ahead with complete visibility to inform business operations.

Conclusion and Final Thoughts

Remaining competitive in the financial services sector requires agility to accommodate changes, deliver superior customer experience, maintain security and compliance, and operate efficiently. To achieve these objectives, security and IT operations teams need increased visibility to work more efficiently, to identify and mitigate issues more quickly, and to maintain business operations.

About ExtraHop

Reveal(x) 360 from ExtraHop delivers this visibility, acting as a single source of information for both security and IT operations teams, eliminating blind spots, and enabling efficiency. The solution helps organizations:

- Stop advanced threats that result from successful phishing scams, ransomware, and supply chain attacks.
- Manage third-party partners and cloud migration risks while ensuring regulatory compliance and improving the effectiveness of existing security controls.
- Detect and respond to insider threats, both malicious and accidental, that are responsible for fraud, loss of intellectual property, financial loss, and reputational damage.
- Automatically detect and easily troubleshoot performance issues with real-time visibility into all network traffic.
- Improve operational efficiency and resilience.

The ExtraHop Reveal(x) 360 Impact

87%
Reduction in time to threat resolution[12]

193%
ROI[14]

66%
Decrease in unexpected outages[13]

3 days
Total implementation and deployment time[15]

> “From the onset of our relationship, ExtraHop has been a top-quality partner and valued subject matter expert. They helped us get up and running with their technology and helped mature our vision for leveraging the unique insights and data from their platform to [deliver on] our service development and user experience improvement goals.”

DIRECTOR
BANKING INDUSTRY,
FIRM SIZE US $10 billion to $30 billion[16]

ABOUT EXTRAHOP
ExtraHop is the cybersecurity partner enterprises trust to reveal the unknown and unmask the truth. The company’s Reveal(x) 360 platform is the only network detection and response solution that delivers the 360-degree visibility needed to uncover the cybertruth. When organizations have full network transparency with ExtraHop, they see more, know more and stop more cyberattacks. Learn more at **www.extrahop.com**

ExtraHop

info@extrahop.com
www.extrahop.com

[12] “The Total Economic Impact™ Of ExtraHop Reveal(x) 360,” Forrester, December 2022.
[13] “The Total Economic Impact™ Of ExtraHop Reveal(x) 360,” Forrester, December 2022.
[14] “The Total Economic Impact™ Of ExtraHop Reveal(x) 360,” Forrester, December 2022.
[15] “The Total Economic Impact™ Of ExtraHop Reveal(x) 360,” Forrester, December 2022.
[16] Gartner Peer Insights Review