ExtraHop

Accelerate Detection and Response in Financial Services

Stop attacks before the breach with ExtraHop Reveal(x).

From large institutions and insurance companies to credit unions and regional banks, financial services manage high-asset values, and are one of the most targeted sectors around the globe. The industry must comply with a multitude of data privacy and financial regulations, manage gigabytes of real-time data representing billions of dollars of transactions, and combat the constant risk of intellectual property and financial theft, loss, and fraud.

To remain competitive and deliver seamless customer experiences, financial services organizations are at the forefront of digital transformation. With distributed deployments that employ multi-cloud, container, and serverless architectures, a mix of modern, legacy, and third-party applications, and a wide variety of endpoints including IoT and other unmanaged devices, financial services infrastructure is complex. This complexity increases risk and requires real-time visibility into every communication on the network.

> Financial services have the second-highest cost of a data breach—**$5.85 million per breach,** with an average per-capita cost of **$210 per record.**[1]

The Challenge: Financial Services Under Constant Attack

Global uncertainty and its associated economic turmoil increase risk and heighten existing security challenges. From the reactions to market changes, like the rapid movement to remote work and increasing customer demand for digital access, new attack vectors are born.

To address the increasing volume and sophistication of threats, financial services are challenged to:

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, responsible for fraud, loss of intellectual property, financial loss, and reputational damage

Improve operational efficiency and resilience with greater network visibility

The Opportunity: Gain Visibility, Reduce Risk, and Respond Quickly

Securing modern financial services organizations require that you monitor the activity of remote workers, satellite offices, and branch locations across a complex, distributed web of applications with data spread across edge, core, and cloud deployments.

A greater understanding of every network asset and communication will boost your IT team's ability to protect your sensitive data and deliver an efficient and secure customer experience. By stopping advanced threats before they result in a breach, and quickly troubleshooting events to eliminate unplanned downtime and ensure compliance, you will improve your organization's overall security posture and reduce risk.

UNIFY VISIBILITY AND IMPROVE CYBER HYGIENE

Network visibility is the cornerstone of risk management frameworks, such as NIST, FSSCC, and MITRE ATT&CK, and regulations like SOX, GDPR, PSD2, NYDFS, Gramm-Leach-Bliley Act, PCI DSS, and Consumer Data Right (Australia).

- Real-time visibility into every asset and communication across your entire hybrid network is critical to stop threats, prove compliance, and ensure application performance
- Transaction and administrative workflows that span numerous systems and apps, data centers, and cloud-based resources require greater visibility
- Up-to-date and complete asset inventory and classification (including IoT), is essential to improve security and the health of your network

TAKEAWAY

Financial services IT functions that gain greater visibility and closely collaborate to identify gaps, blind spots, and uncover threats will improve security posture and meet compliance while ensuring the speed and scale of transactions.

STOP THREATS POST-COMPROMISE

Attackers are increasingly able to find their way inside the network and move laterally undetected. The sophistication and increased volume of today's threats require that you monitor the behavior of both north-south and east-west network traffic to detect unusual activity before a breach occurs.

- War rooms and the IT blame game slow response times and distract from resolving incidents and delivering major initiatives
- To understand if you have been compromised in the past, you need the ability to look back into historical data to hunt for threats and IOCs

TAKEAWAY

Financial services security teams that monitor and analyze network data will increase their speed and efficacy with all the data you need to investigate and respond to an incident before it escalates into a breach.

REDUCE THREATS FROM ENCRYPTED TRAFFIC, UNMANAGED DEVICES, AND CLOUD WORKLOADS

Financial services organizations are at the forefront of cloud adoption. Monitoring cloud workloads with context of what is happening in the rest of the network, and decrypting traffic where necessary, are essential to detecting advanced threats.

- Encrypted traffic leads to dark spaces, which attackers can exploit to gain access
- Internet of Things (IoT) and unmanaged devices present a large risk to distributed, hybrid, and multi-cloud financial services entities
- DevOps and increased cloud adoption result in disparate network, cloud, and security operations, and increase risk

TAKEAWAY

Financial services IT leaders must monitor all encrypted and unencrypted traffic on hybrid networks to reduce their overall risk.

The Solution: Reveal(x) Cloud-native NDR for Financial Services

ExtraHop Reveal(x) cloud-native network detection and response (NDR) provides the scale and the intelligence needed to analyze financial services hybrid environments from the inside out to detect and respond to threats before they cause damage.

Reveal(x) passively monitors your network and analyzes all network interactions to deliver complete visibility, real-time detection, and intelligent response to improve your organization's ability to stop advanced threats, troubleshoot downtime and slow applications, and improve your network and security hygiene.

Achieve 360-degree visibility to quickly detect, investigate, and respond to threats with an integrated workflow for unparalleled insight across the hybrid network, cloud workflows, and IoT devices.

Detect suspicious activity with cloud-based machine learning and advanced behavioral analysis to uncover indicators of compromise, like command and control, brute force, lateral movement, privilege escalation, unusual protocol communication, and data staging and exfiltration. Decrypt traffic to identify threats and anomalies within SSL/TLS encrypted traffic.

Stop advanced threats that other solutions won't see, streamline your operations, and accelerate investigations into any incident with a click. No war rooms. No waiting on other teams.

Complete Visibility

Discover and classify all assets communicating on the hybrid network

Eliminate frictions between NetOps, SecOps, and CloudOps teams

Real-Time Detection

Improve analyst efficiency with a single integrated workflow with real-time threat detection

Enable faster answers through cloud-based machine learning

Intelligent Investigation & Response

Troubleshoot incidents and investigate root cause in less time

Use historical data to hunt threats and discover if you have been previously impacted

Automate and orchestrate responses through integrations with SIEM, EDR, SOAR, NGFW, and more

99% FASTER TROUBLESHOOTING

84% FASTER THREAT RESOLUTION

50% FASTER DETECTION

ACCELERATE YOUR SUCCESS WITH EXTRAHOP REVEAL(X) ADVISOR

On-demand access to ExtraHop security experts provides you with guidance and deep expertise to close skills gaps, gain visibility, and improve your analysts' ability to detect, investigate, and respond to performance and security incidents in the context of your financial services organization's unique environment.

ABOUT EXTRAHOP NETWORKS

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions and applies advanced machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring delivery of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com

Sources: [1] 2020 Ponemon study