



5 WAYS

Financial Institutions
Use ExtraHop
Network Intelligence

INTRODUCTION

When a security issue emerges, how do you quickly detect, investigate, and resolve the situation? If a performance issue appears, how do you quickly pinpoint and address the root cause before an impact is experienced?

Financial institutions are increasingly leveraging cloud and hybrid infrastructures as they strive to deliver high-quality digital experiences to customers. These companies are also under increasing risk of cyberattack as the attack surface continues to grow. At the same time, many institutions are innovating rapidly and experiencing frequent M&A activity. They must meet the challenge of integrating disparate systems and applications, maintaining security and compliance, and ensuring performance is not negatively affected.

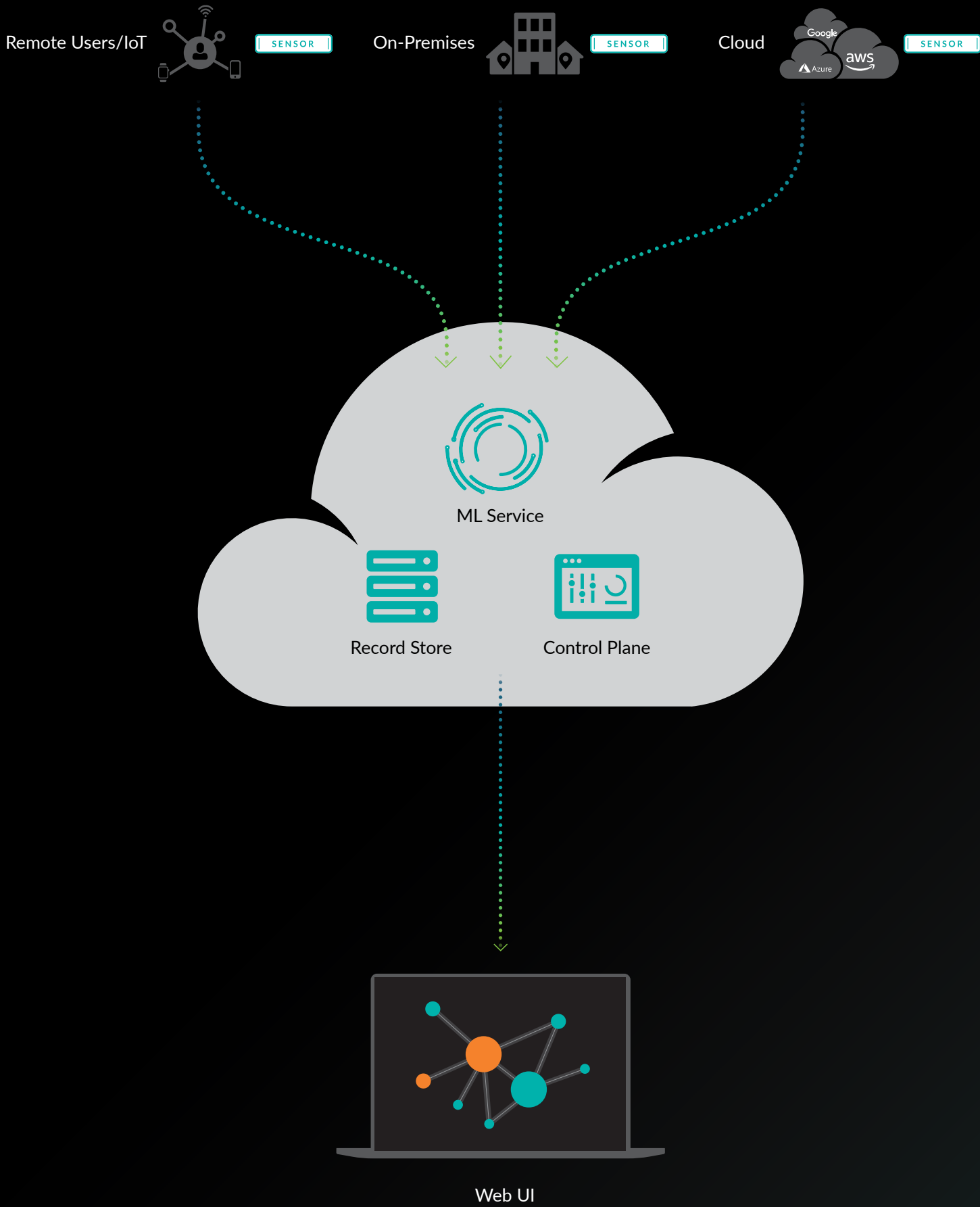
These changes bring new challenges and additional visibility is required to understand and prevent potential issues across distributed networks that span hundreds of branch locations, multiple clouds, and numerous third-party applications. Meanwhile, IT security and operations teams are spread thin, using multiple tools to triangulate issues to determine root causes and address problems and must find ways to increase efficiency.

ExtraHop Reveal(x) 360 arms IT security and operations teams with the visibility and context needed to quickly identify, understand, and resolve potential security or performance issues. The solution delivers the 360-degree visibility needed to quickly understand the situation and circumstances, speeding efficiency and resolution times.

TABLE OF CONTENTS

Key benefits for financial customers using ExtraHop

REDUCE THE RISK OF CYBERTHREATS	5
OPTIMIZE PERFORMANCE.....	7
ACCELERATE INFRASTRUCTURE MODERNIZATION.....	9
INCREASE SECURITY HYGIENE AND COMPLIANCE	11
IMPROVE OPERATIONAL EFFICIENCY AND MAXIMIZE EXISTING INVESTMENTS	13



Reduce the Risk of Cyber Threats

Financial institutions are targeted by attackers at a very high rate. These organizations face complex challenges such as multiple branch locations and increasing use of digital banking and open banking technologies. They also handle highly sensitive data including account and transaction details. Without the right visibility, financial service institutions cannot secure and protect this data.

CHALLENGES

Financial institutions face an increasingly difficult threat environment and are under relentless, sophisticated, and ever-present cyber-attacks. The attack surface has grown to include sprawling networks, multiple clouds, and a multitude of devices and applications, which all interact. Security must be addressed, and gaps closed, despite budget and staffing constraints.

SOLUTION

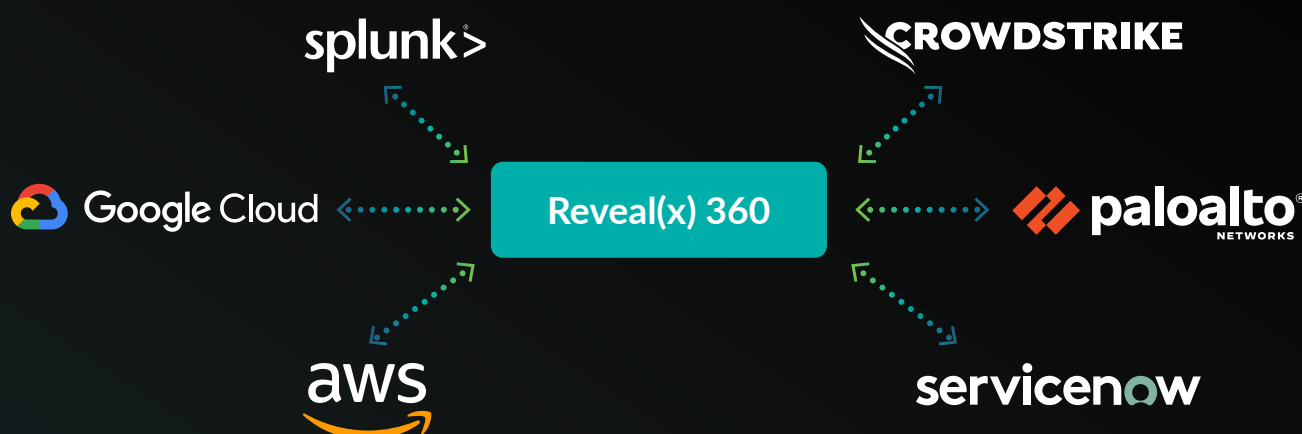
Reveal(x) 360 helps financial institutions easily detect and respond to threats with complete visibility that spans hybrid and multi-cloud environments. With Reveal(x) 360, organizations can:

- Eliminate blind spots in encrypted traffic, without compromising security and privacy.
- Speed forensic analysis and threat hunting operations with a 90-day history including packet capture.
- Integrate easily with other best-in-breed systems to correlate insights and automate response.

IMPACT

With ExtraHop Reveal(x) 360, financial institutions gain better visibility across their infrastructure to detect threats and resolve problems faster.

INTEGRATION CAPABILITIES OF REVEAL(X) 360



“

We chose ExtraHop Reveal(x) because it efficiently accelerates the detection of threats with superior visibility across our entire ecosystem.”

**CYBERSECURITY MANAGER,
CENTRAL AMERICA BASED FINANCIAL SERVICES FIRM**

Optimize Performance

When performance issues arise at financial institutions, the impact to employees and customers can be severe. Teams must work to ensure transactions are processed promptly and accurately and that customer experience always remains positive. IT operations teams must proactively identify potential issues before an impact or outage is experienced.

CHALLENGES

Financial institutions handle time-critical operations such as payment transactions. Performance issues can easily impact applications and customer experience. Detecting and resolving performance issues before the impacts are visible is a crucial step in delivering a high-quality experience. There can often be blind spots in application delivery chains and off-the-shelf SaaS products, where limited documentation may exist.

SOLUTION

Reveal(x) 360 empowers IT operations teams with complete context for root cause analysis, and to quickly understand all of assets and the dependencies between them. Reveal(x) 360 helps to:

- Easily monitor all interactions between every application in a hybrid environment and gain insight into off-the-shelf commercial applications.
- Detect performance issues automatically and take rapid action to correct the potential impacts.
- Quickly collaborate across ITOps, DevOps, and SecOps teams with a single source of cybertruth, for faster resolution and without siloed activity.
- Get meaningful insights about network, application, and cloud performance with custom dashboards.

IMPACT

As a result, financial organizations can deliver exceptional customer experiences at an enterprise scale and enable employees to be highly productive.

“

ExtraHop is the foundation of our application performance improvement efforts. We can understand the contribution each tier makes to overall response time and how different components affect others in n-tier applications. This visibility has helped us to continually find efficiencies and improve our response times.”

**DIRECTOR OF IT,
US-BASED ONLINE BROKERAGE FIRM**

Accelerate Infrastructure Modernization

The cloud has opened new doors to the way organizations innovate. The power to scale cloud resources has accelerated application development, iteration, and delivery with the ability to dynamically adjust to meet demand. However, with new infrastructures come new challenges to network visibility.

CHALLENGES

Financial services companies seeking to improve the customer experience while lowering costs are increasingly migrating applications and databases to the cloud. However, these migrations can introduce new risks to security and performance that must be managed. Leveraging cloud infrastructure is more complex and cloud workloads are more ephemeral than those in on-premises environments. Cloud-native telemetry sources are log based and may aid historical analysis, but often do not offer real-time behavioral insight. As the attack surface grows, visibility is needed for detection and response.

SOLUTION

ExtraHop Reveal(x) 360 provides a common data source that both SecOps and ITOps can leverage for insight to ensure that cloud workloads are secure and performing as expected, so organizations can modernize operations and further digitize transactions with speed and confidence. Reveal(x) 360 allows financial institutions to:

- Automate discovery and classification of all devices on the network and see how they are communicating in real time across on-premises and cloud infrastructure.
- Monitor roundtrip time and troubleshoot database errors and slow applications.
- Detect threats and performance issues at enterprise scale with contextual awareness of workload architecture, decoding more than 70 enterprise protocols and leveraging 5,000 metrics.
- Identify vulnerabilities and issues and map application dependencies automatically.

IMPACT

With Reveal(x) 360, financial institutions can innovate more quickly and accelerate time-to-market with complete visibility to simultaneously ensure security and performance.

“

As much as Reveal(x) is a security tool, it's also really helped us mature our security and business practices to completely modernize our SOC and power our adoption of the cloud.”

**IT SECURITY MANAGER,
NATIONAL FINANCE INSTITUTION**

Increase Security Hygiene and Compliance

Securing modern financial institutions requires visibility across offices and branch locations, colocation and sovereign datacenters, and a remote workforce, with data spread across a distributed hybrid infrastructure. Stopping advanced threats before they result in a breach and maintaining compliance with an array of evolving mandates is no small task.

CHALLENGES

The infrastructure of financial institutions has become more complex, and a holistic view is difficult to gather in one place. Insight into vulnerabilities across this vast attack surface is even more difficult and often requires multiple tools and manual operations. At the same time, legislation continues to evolve, and financial institutions must keep pace with the changes to maintain compliance, without losing sight of the underlying security objectives.

SOLUTION

With Reveal(x) 360, financial institutions gain 360-degree visibility across on-premises and cloud environments, along with the insight to identify and rapidly remediate vulnerabilities with an integrated workflow. Reveal(x) 360 helps:

- Gain complete, automatic, always-up-to-date asset inventory.
- Automatically detect vulnerabilities like Log4j, Sunburst, PrintNightmare, ProxyShell, Spring4Shell without manual configuration or pattern writing—and detect suspicious activity using advanced behavioral analysis.
- Quickly pinpoint assets handling cardholder or personal data, simplify the process of finding expired certificates and weak ciphers, and protect sensitive data from data leaks, such as employee use of ChatGPT and other large language models.
- Easily document compliance with regulations with robust reporting capabilities.

IMPACT

Reveal(x) 360 provides financial institutions the visibility to reduce risks, proactively maintain security hygiene and ensure regulatory compliance on a massive scale across on-premises infrastructure and the cloud.

“

We were up and running with Reveal(x) 360 in less than a day, and we were getting viable network information right away. We'd never had this level of visibility before and were able to strengthen our security posture on day one.”

**DIRECTOR OF CYBERSECURITY,
FINANCIAL SERVICES**

Improve Operational Efficiency and Maximize Existing Investments

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 cybertruth. Financial institutions also benefit from integration with existing tools, such as ticketing solutions, SIEM, SOAR, next-generation firewalls, and others to accelerate response to potential issues.

CHALLENGES

Chasing false positives, manual configuration processes, and culling information from multiple platforms can all lead to wasted time and inefficient practices. Hiring and retaining security talent remains a challenge across industries and many teams are understaffed, asking their team members to do more and more. And when ITOps and SecOps use different sources of data, time spent getting to a common understanding of the cybertruth could be better spent resolving issues.

SOLUTION

With Reveal(x) 360, financial institutions improve end user productivity through automation, additional context, alignment across teams, and integration with existing tools. With Reveal(x) 360, organizations can:

- Integrate high-fidelity network data with other best-in-breed systems to correlate insights and automate response.
- Quickly cut through alert noise to focus on the issues that matter most with abundant context.
- Improve speed and productivity via threat briefings, which provide correlated, contextualized data about notable cyber-attacks or attack techniques, and easy-to-use investigative workflows, which provide drill-down capabilities to dig deep into the underlying data.

IMPACT

By leveraging ExtraHop Reveal(x) 360, financial institutions can optimize their teams' efficiency and reduce overall costs and operational complexity. By eliminating overlapping tools and allowing individual analysts to work more efficiently, companies can boost their profitability. According to a report by Forrester¹, based on interviews conducted, a composite organization using Reveal(x) 360 experiences \$1.4M in cost savings over three years, representing a 193% return on investment. Additionally, Reveal(x) 360 decreases time to threat detection by 83% and time to threat resolution by 87% and saves 1,065 hours on investigating unplanned outages.²

¹ <https://www.extrahop.com/resources/papers/forrester-tei-study-2023/>

² <https://www.extrahop.com/resources/papers/forrester-tei-study-2023/>


“

The way that ExtraHop is architected means that we've been able to make the platform accessible to colleagues across other operational teams. The wide range of capabilities and functionality of the ExtraHop platform is driving value across our entire technology function.”

**NEIL BEATTIE,
HEAD OF DIGITAL SECURITY AND RESILIENCE,
BREWIN DOLPHIN PLC**

UNIFIED VISIBILITY FOR FINANCIAL SERVICES INSTITUTIONS.

Increase performance, protection, and
resilience for whatever happens next.

Learn more 



ExtraHop is the cybersecurity partner enterprises trust to reveal the unknown and unmask the attack. The ExtraHop 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