EXTRAHOP

Strengthening Operational Resilience in the Finance Sector

Keep Critical Financial Applications and Processes Free from Threats and Disruption with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: From Resilience to Systemic Stability

For decades, digital innovation has driven global financial growth. However, this evolution has also ushered in a new era of sophisticated cyber threats with devastating consequences. In response, regulatory authorities are moving beyond simple data protection to mandate operational resilience. As this shift unfolds, financial institutions face several critical inflection points:

- **The Escalation of Nation-State and Destructive Attacks:** Geopolitically motivated actors have shifted from simple data theft to functional destruction. In early 2026, the BridgePay ransomware attack demonstrated this reality, knocking payment infrastructure offline and forcing businesses into cash-only operations. By striking trusted third-party vendors and exploiting edge devices before patches are even released, these actors disrupt Crown Jewel applications and threaten the integrity of global assets. Protecting these transactions requires absolute internal visibility to contain lateral movement before destructive commands execute.
- **The Threat to Macro-Financial Stability:** Cyber incidents now pose a systemic risk to the global economy. According to the IMF's 2024/2026 Global Financial Stability Report, extreme losses per firm have quadrupled to $2.5 billion. Beyond direct theft, indirect costs, such as reputational damage and the loss of customer trust, can jeopardize funding and solvency. With 2026 projections showing that nearly one-fifth of all global cyber incidents target financial firms, the risk of "contagion" where a single breach ripples through interconnected settlement networks is a primary concern for the WEF and central banks alike.
- **The Evolution of Ransomware and AI-Driven Fraud:** In the last year, ransomware hit 65% of financial services, with attackers increasingly targeting cloud backups and using GenAI-powered "Vishing" to bypass MFA. Whether it's the disruption of Treasury markets or the $1.5 billion Ethereum theft from Bybit, the damage is no longer localized. Financial institutions are highly interconnected; a failure in one node can drag down the nation's economy. Modern defense requires identifying single points of failure early, leveraging wire data to validate network segmentation and ensure impact tolerance during an eventual disturbance.

KEY CAPABILITIES

Depth and Breadth of NDR Performance
Monitors all network interactions by decrypting and decoding over 90+ protocols, including native support for FIX and MSMQ, at speeds up to 100 Gbps to protect high-frequency trading and critical applications.

The Definitive Data Source for the AI-Enabled SOC
RevealX powers financial SOC automation applications with unalterable network data and eliminates investigative friction to accelerate detection and remediation.

AI-Powered Cyber Threat Detection
RevealX NDR utilizes machine learning and behavioral baselining to detect sophisticated attacks, lateral movement, and ransomware targeting critical applications.

Unified Agentless Visibility
Automatically discover every asset, including unmanaged IoT devices like ATMs and point-of-sale terminals, along with hybrid cloud workloads, without installing software or risking system stability or performance.

Strategic Line-Rate Decryption
Analyze modern encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats and unauthorized data staging without adding latency to time-sensitive financial transactions.

High-Fidelity Performance Metrics
Troubleshoot complex disruptions and verify service level agreements (SLAs) using over 5,000 wire data metrics for deep operational insight into application and database latency.

Continuous Forensic Capture
Maintain an unalterable record of all network transactions to satisfy audit requirements for NYDFS 500 and DORA, accelerating root cause analysis and incident reconstruction.

The Solution: RevealX Network Intelligence

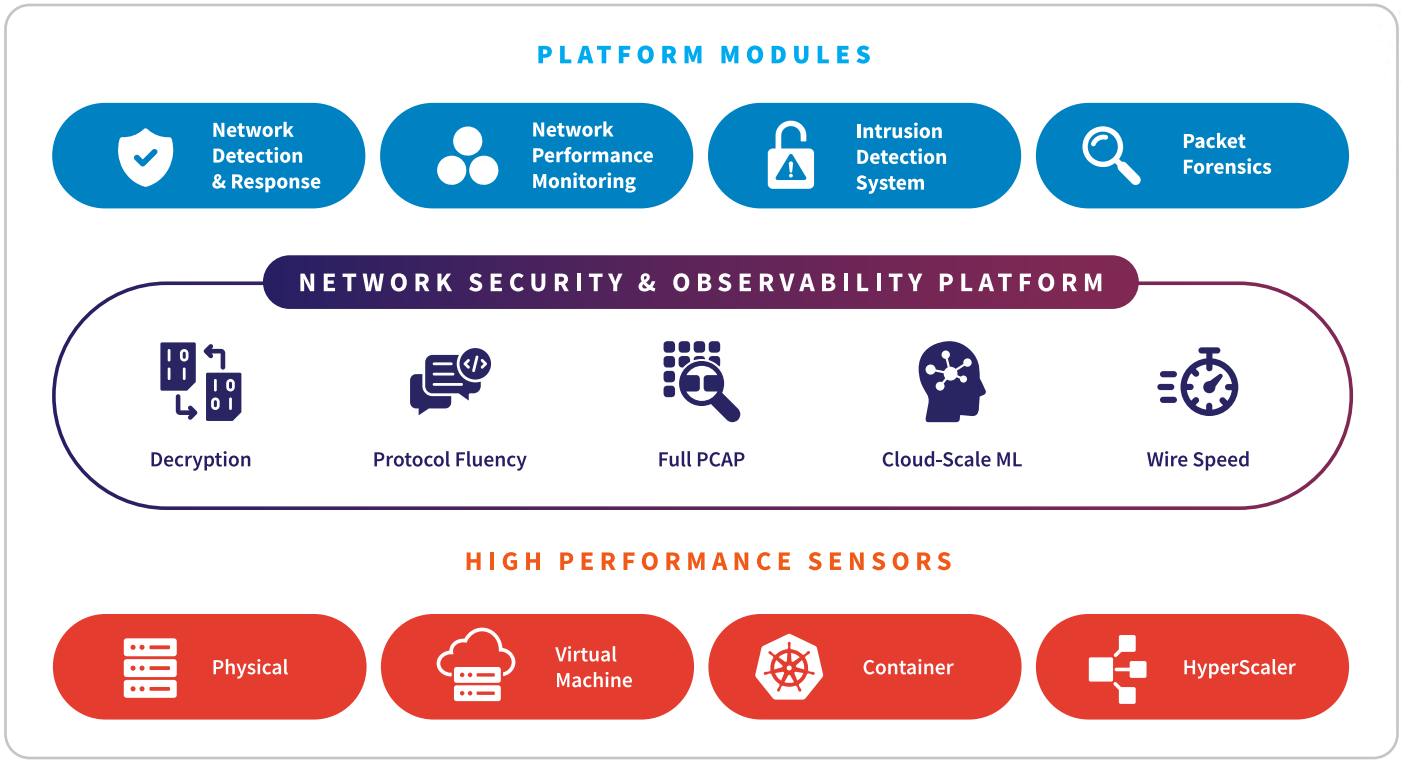
ExtraHop RevealX delivers the network intelligence required to secure sensitive financial data and maintain operational resilience. By providing a unified view of hybrid and multi-cloud environments, RevealX enables security and operations teams to detect sophisticated threats while ensuring the availability of critical financial services. Because log and endpoint data can be tampered with or disabled, the network serves as the only immutable source of truth that cannot be evaded. This ground truth is essential for financial continuity in a landscape where digital innovation must outpace sophisticated adversaries.

Neutralizing destructive nation-state threats requires intercepting actors before they execute malicious commands. By monitoring the wire rather than relying on vulnerable agents, RevealX identifies the subtle lateral movement and credential abuse used to deploy wiper malware. This agentless approach ensures that even if a third-party vendor or edge device is compromised, the platform detects anomalies in real time. This allows teams to isolate affected segments, preserving the integrity of settlement systems and protecting global assets from systemic disruption.

RevealX provides the scale and deep packet visibility required to comply with evolving mandates like the EU's DORA, NYDFS 500, and Australia's CPS 230. By combining Network Detection and Response with line-rate decryption and performance monitoring, RevealX eliminates tool sprawl and deconstructs IT complexity. This strategy ensures teams operate from objective data rather than fragmented silos, enabling faster investigations and stronger defensive postures. Using line-rate decryption of TLS 1.3, RevealX prevents attackers from hiding within encrypted payment integrations or cloud workflows.

The platform automatically discovers all IT assets and maps interdependencies to eliminate single points of failure. Using machine learning, RevealX identifies anomalous behavior in east-west traffic, such as data exfiltration hidden in encrypted protocols like Kerberos or Microsoft SQL. This intelligence allows teams to immediately understand the full blast radius of an incident, focusing remediation efforts while maintaining an unalterable historical record for legal disclosures and audit trails. By providing persistent visibility across the entire transaction path, RevealX ensures that revenue streams remain uninterrupted.

ExtraHop NDR Platform



NDR Technology Use Cases for the Financial Industry

Nation-State Attacks	Provides deep visibility into lateral movement and data exfiltration, enabling the detection of subtle, long-term nation-state campaigns targeting banking infrastructure and clearing houses.
Threat Detection & Response	Enables proactive investigation into hidden threats across hybrid environments using intuitive, query-based workflows to find what logs and agents miss within core banking and payment ecosystems.
Threat Hunting	Uncovers stealthy, signature-less threats and persistent actors by leveraging behavioral baselines to find anomalies that evade automated alerts before they can impact trading operations or institutional liquidity.
SOC Modernization	Unifies SOC and NOC workflows to eliminate data silos. It uses AI-powered prioritization to reduce alert fatigue, accelerating response times and improving operational efficiency for financial services delivery.
Incident Response & Investigation	Provides forensic-level visibility and "one-click" investigations to determine the root cause of an incident. It offers an unalterable record of all network transactions, including access to sensitive customer financial data.
Lateral Movement	Detects attackers moving internally using peer-group clustering and protocol decoding to catch pivots that bypass perimeter security toward SWIFT environments or brokerage databases.
Cloud Workload Security	Delivers agentless, full-spectrum visibility to defend critical cloud-integrated fintech workloads and discover "shadow IT" or unmanaged assets across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse and privilege escalation in real time, providing deep visibility into identity-based threats targeting high-value transaction accounts.
Ransomware Attacks	Identifies early-stage ransomware activity, such as file staging and encryption patterns. This provides the visibility needed to isolate infected hosts before the exfiltration of nonpublic financial information occurs.
Unmanaged Devices	Fills the visibility gap for unmanaged financial devices like ATMs and point-of-sale (POS) terminals by monitoring their network traffic directly since these systems may not support EDR agents.
EDR Evasion Detection	ExtraHop's out-of-band monitoring identifies malicious activity even if endpoint agents are disabled. This ensures persistent visibility across automated teller hardware where agents cannot be installed.
AI Security	AI security includes AI workloads and other containerized cloud workloads. This use case monitors interactions with generative AI platforms and autonomous agents that might be used for algorithmic trading support or automated financial advisory services.
Operationalizing Zero Trust	Acts as the independent observer in the Zero Trust Architecture loop. It detects policy drift and provides empirical proof that internal network segmentation policies are effective.

NPM Technology Use Cases for the Financial Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot complex disruptions. It provides clear visibility into latency and throughput for high-frequency trading and remote banking sessions.
Operational Resilience	Reduces disruption impact by resolving infrastructure degradation before it hits financial continuity. It ensures availability through proactive service-level monitoring.
Troubleshooting & Resolution	Accelerates root cause analysis via a 3-click workflow from metrics to packets, eliminating friction between network and financial application teams.
Migrate Workloads to the Cloud	Maintains performance during core banking migration by auto-mapping dependencies and assets, using on-premises baselines to validate successful cloud delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes environments. This ensures performance for critical business services like FIX gateways and payment APIs.
Forensic-Grade Investigations	Combines long-term metadata with scalable PCAP for an unalterable record of events, enabling deep-dive analysis into past outages or intermittent degradations.
Application Performance Monitoring	Complements APM by filling network-layer visibility gaps, decoding 90+ protocols, including FIX and MSMQ, to provide real-time insights into response and processing time versus latency.

Financial Industry Compliance & Regulatory Use Cases

Operational Resilience	EU / UK	DORA / FCA PS21/3	Maps interdependencies between critical banking services to ensure impact tolerances are maintained during cyber events or brokerage system outages.
Cybersecurity Risk Management	EU	NIS2	Addresses supply chain security and vulnerability management by providing continuous visibility into digital financial service providers and internal network hygiene.
Asset & Identity Discovery	US (NY)	NYDFS 500	Provides an automated, real-time inventory of all banking information systems, including unmanaged devices, to meet strict hardware and software tracking mandates.
Operational Risk & 3rd Party	Australia	APRA CPS 230	Manages risks from material fintech partners and brokerage service providers by monitoring network behavior for credential abuse and unauthorized access.
Cyber Hygiene & Perimeter	Singapore	MAS Notice 655	Validates egress and ingress controls at the banking network perimeter and restricts unauthorized traffic, ensuring privileged administrative accounts are secured via continuous observation.
Hybrid Cloud Risk	Canada	OSFI Guideline E-21	Modernizes risk management by alerting on unauthorized data exfiltration or behavioral deviations across legacy core-banking mainframes and distributed cloud stacks.
Data Privacy & Integrity	US / EU	PCI DSS 4.0	Safeguards sensitive cardholder data by monitoring for unauthorized staging or access within the financial cardholder data environment (CDE).
Incident Reporting	US / EU	SEC / DORA NIS2	Maintains an unalterable record of wire data to satisfy 72-hour notification windows for banking regulators and provide forensic network truth for brokerage disclosure requirements.

Customer Benefits: Strengthening Operational Resilience Across the Financial Ecosystem

Visibility into network truth is the cornerstone of modern financial resilience. RevealX provides the real-time insights necessary to ensure uptime for high-frequency trading, payment clearing, and core banking. By monitoring the wire, institutions protect firm-level liquidity and macro-financial stability against sophisticated nation-state threats.

As firms transition to hybrid and multi-cloud environments, RevealX eliminates the blind spots that often accompany FinTech innovation. It secures legacy data centers and cloud-native stacks by observing actual traffic flows like FIX, MSMQ, and RPC rather than relying on modifiable logs. This delivers the definitive forensic evidence required to satisfy global mandates such as DORA, NYDFS 500, and APRA CPS 230.

RevealX also secures the expanding ecosystem of unmanaged devices and third-party APIs, from ATMs to partner portals. By monitoring these traditionally invisible areas, the platform identifies lateral movement and credential abuse before nonpublic information is exfiltrated. With continuous discovery and classification of every network entity, RevealX ensures that high-value revenue streams and customer trust remain uninterrupted.

ExtraHop Can Help

ExtraHop NDR provides a critical advantage by delivering the comprehensive network intelligence required to surface sophisticated lateral movement and internal threats that legacy tools often miss.

Learn more about our successful customer deployments in finance and banking:

OCBC Indonesia

BAC Credomatic

RevealX Delivers Network Facts that Empower Financial Organization's Security & IT Staff

Leading Global Payments and Financial Technology Provider

Leading Global Financial Services Provider

Or contact us to schedule your personalized demo and security assessment.

> "We strive to provide the best customer experience possible, so excellent network performance is a must. RevealX provides more accurate and detailed detection information than other solutions, which means we can resolve network and application performance issues before they impact customers, and detect threats before attackers can achieve their goals."

RAHMAT NUGRAHA
Chief of Cybersecurity Architecture
OCBC Indonesia

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com