EXTRAHOP

Securing the Technology Supply Chain and SaaS Innovation

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

SOLUTION BRIEF

Industry Challenges: From Rapid Innovation to Software Supply Chain Fragility

Global technology and SaaS vendors operate where digital infrastructure is the product. Digital friction erodes customer trust and triggers immediate financial and legal liabilities. By 2026, the landscape will have shifted toward API-first architectures and AI-integrated development. While accelerating innovation, these technologies created an opaque attack surface where one CI/CD vulnerability or compromised OAuth token impacts thousands of downstream customers. As lines between internal networks and production environments disappear, vendors face critical failure points.

- **The Escalation of Nation-State and Supply Chain Sabotage:** Geopolitically motivated actors moved beyond IP theft to the functional paralysis of global software infrastructure. By infiltrating CI/CD workflows or poisoning automated build pipelines, adversaries target the integrity of the delivery process. This shift turns a single vendor compromise into a systemic crisis, transforming a trusted software update into a delivery vehicle for destructive malware across the global ecosystem.
- **The Identity, OAuth, and Non-Human Identity Sprawl:** Sophisticated attackers prioritize subverting identity layers by using AI-driven social engineering to bypass multi-factor authentication. Simultaneously, the explosion of service accounts, API tokens, and semi-autonomous AI agents created a non-human identity layer that is often overprivileged and unmonitored. Attackers exploit these lateral paths to navigate undetected from employee office suites into production databases and high-value customer environments.
- **The Visibility Gap in Cloud-Native and Microservices Architectures:** Modern SaaS platforms rely on thousands of interdependencies and third-party APIs that traditional security agents cannot monitor. This gap is critical in containerized and serverless environments where attackers prioritize disabling EDR tools immediately upon entry. Organizations must now detect post-compromise activity, such as unauthorized API calls or token abuse, directly on the wire before data exfiltration or massive service disruption begins.
- **Regulatory Rigor and the Mandate for Operational Transparency:** 2026 mandates compressed the timeline for incident response and public accountability. New SEC rules require public companies to disclose material incidents within four business days. Simultaneously, the EU NIS2 Directive and SOC 2 Type II requirements demand proof of continuous, real-time behavioral monitoring. Meeting these standards while maintaining 99.99 percent uptime requires a unified approach that eliminates the silos between security and DevOps teams.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors network interactions by decrypting and decoding over 90+ protocols at 100 Gbps to protect high-volume SaaS environments and microservices.

The Definitive Data Source for the AI-Enabled SOC

RevealX provides high-fidelity wire data required for next-generation SOC automation. Delivering unalterable ground truth eliminates investigative friction and accelerates the path from detection to remediation.

AI-Powered Cyber Threat Detection

Identifies sophisticated attacks, lateral movement, and early-stage ransomware targeting CI/CD pipelines and API gateways using cloud-scale machine learning and behavioral baselining.

Unified Agentless Visibility

Automatically discovers all assets, including unmanaged containers, serverless functions, and multi-cloud workloads, without installing software or risking system stability or production performance.

Strategic Line-Rate Decryption

Analyzes encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats and unauthorized data staging without adding latency to time-sensitive software transactions.

High-Fidelity Performance Metrics

Troubleshoots complex disruptions and verifies SLAs using over 5,000 wire data metrics for deep operational insight into application and database performance.

Continuous Forensic Capture

Maintains an unalterable record of all network transactions to satisfy SOC 2 Type II and SEC audit requirements, accelerating incident reconstruction.

The Solution: RevealX Network Intelligence

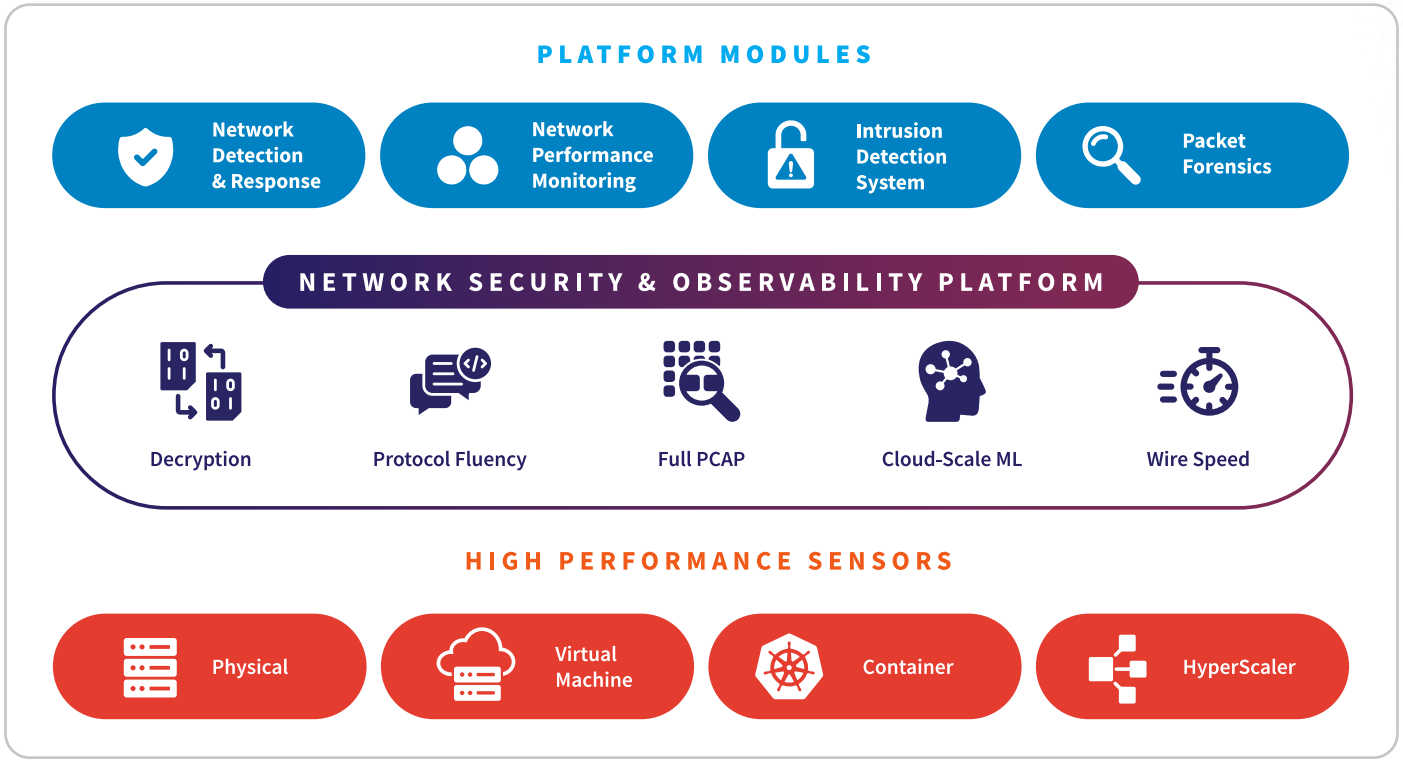
ExtraHop RevealX provides the critical network intelligence required to neutralize nation-state actors and advanced persistent threats targeting the digital supply chain. These sophisticated adversaries often use living-off-the-land techniques to compromise CI/CD pipelines or exploit vulnerabilities to gain a foothold in production. By delivering a unified view of hybrid and multi-cloud architectures, RevealX enables teams to identify the early stages of a nation-state campaign before it leads to proprietary source code theft or systemic service disruption.

Neutralizing destructive attacks requires stopping actors before they execute malicious commands. By monitoring the wire rather than relying on vulnerable agents, RevealX detects lateral movement and credential abuse used to pivot from corporate offices into mission-critical environments. This agentless approach ensures that even if a trusted third-party vendor or unmanaged API gateway is compromised, the platform identifies anomalous behavior in real time. Engineering teams can then isolate affected segments and preserve core system integrity to protect global software assets from large-scale disruption.

Supporting innovation while meeting the security demands of the technology sector requires complete visibility into network traffic. Only with a comprehensive and real-time view of network truth can teams stay ahead of unplanned outages and breaches that threaten brand reputation. Because log and endpoint data can be modified or disabled by advanced threats, the network provides the only immutable source of truth that cannot be subject to tampering or evasion by an adversary.

RevealX provides the scale and deep packet visibility required to investigate efficiently and comply with mandates like the SEC four-day disclosure rule and SOC 2 Type II continuous monitoring. By combining NDR with line-rate decryption, RevealX enables firms to deconstruct microservices complexity without tool sprawl. The platform identifies anomalous behavior such as OAuth token abuse or unauthorized data staging. A key differentiator is the line-rate decryption of TLS 1.3 and PFS, ensuring attackers cannot hide movements within encrypted traffic. This provides the independent observation required for a Zero Trust Architecture while maintaining performance for high-volume SaaS operations.

ExtraHop NDR Platform



NDR Technology Use Cases for the Technology & SaaS Industry

Nation-State Attacks	Detects stealthy lateral movement and data staging in long-term campaigns targeting proprietary source code repositories and production CI/CD pipelines.
Threat Detection & Response	Investigates hidden threats across distributed microservices and public API gateways where traditional logging often fails to provide context.
Threat Hunting	Leverages behavioral baselining to find signatureless anomalies in east-west traffic before they impact the integrity of software updates or customer data.
SOC Modernization	Unifies SOC and engineering workflows by using AI prioritization to reduce alert fatigue, accelerating response times for high-volume SaaS platforms.
Incident Response & Investigation	Delivers forensic visibility into unmanaged containers and serverless functions while providing unalterable records of administrative commands for rapid root-cause analysis.
Lateral Movement	Uses peer-group clustering to catch attackers pivoting from compromised employee accounts toward sensitive production databases or high-value service accounts.
Cloud Workload Security	Provides agentless visibility for multi-cloud environments, discovering shadow IT and unmanaged assets across AWS, Azure, and Google Cloud without adding latency.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse and OAuth token theft in real time, focusing on high-value developer workstations and jump hosts.
Ransomware Attacks	Identifies early-stage ransomware patterns, such as file staging or unusual encryption, to isolate hosts before exfiltration of customer intellectual property.
Unmanaged Devices	Fills the visibility gap for specialized DevOps tools and network appliances that cannot host security agents, ensuring 100% coverage of the digital environment.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity even when endpoint agents are disabled or bypassed, ensuring persistent visibility across the entire software stack.
AI Security	Monitors interactions with generative AI tools used for automated coding or customer support to prevent prompt injection or accidental data leakage.
Operationalizing Zero Trust	Acts as the independent observer, detecting policy drift and providing empirical proof that micro-segmentation between development and production zones is effective.

NPM Technology Use Cases for the Technology & SaaS Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for factory-floor automation and PLC-to-HMI sessions.
Operational Resilience	Resolves infrastructure degradation before it hits production continuity, ensuring availability through proactive monitoring of mission-critical SCADA services.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between plant operations (OT) and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during MES or ERP migration by auto-mapping dependencies and using OT baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for IIoT gateways and supply chain APIs.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past production outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols (e.g., Modbus, EtherNet/IP), providing real-time insights into command processing time vs. network latency.

Technology & SaaS Industry Compliance & Regulatory Use Cases

Rapid Materiality Assessment	United States	SEC Disclosure	Enables rapid forensics into SaaS and OAuth token abuse, allowing teams to assess breach materiality within the mandatory four-day window.
Continuous Security Monitoring	Global	SOC 2 (Type II)	Satisfies CC7.2 and CC7.3 criteria by proving 24/7 oversight and providing non-repudiable audit trails required for security and privacy audits.
Personal Data Attribution	European Union	GDPR (EU)	Speeds up notification by attributing data access paths and providing forensic evidence of breach scope to minimize potential regulatory fines.
Technical Proof of Monitoring	Global	ISO/IEC 27001:2022	Provides technical proof that the network is monitored for unauthorized activity and internal data movement, addressing Annex A 8.16 and 8.12.
Risk Detection and Response	US / Global	NIST CSF 2.0	Powers detect (DE) and respond (RS) function by identifying the attack blast radius in real-time to stop incidents before they become material.
Operational Resilience	United Kingdom	UK CAF	Supports NIS "Detecting Cyber Security Events" objectives via automated discovery and metadata history required for "achieved" status in audits.

Customer Benefits: Ensuring Platform Trust and Operational Resilience Across the Digital Supply Chain

Visibility into network truth is the foundation for modern software resilience. RevealX provides real-time visibility for sub-second response times in high-volume API transactions and global delivery. By monitoring the wire, SaaS providers safeguard against threats and anomalies that jeopardize uptime, productivity, and brand reputation.

Transitioning to cloud-native and AI-integrated architectures creates agility but introduces blind spots. RevealX enables organizations to maintain resilience across distributed microservices and supply chains. By observing actual traffic instead of modifiable logs, firms gain the forensic evidence needed to satisfy SEC, SOC 2 Type II, and ISO 27001 audits.

RevealX also secures the ecosystem of unmanaged devices and non-human identities. Monitoring build servers, serverless functions, and third-party API gateways eliminates blind spots in agent-based security. RevealX identifies lateral movement and credential abuse before they compromise production or exfiltrate source code. Through continuous discovery and classification, RevealX ensures that critical services and high-value data remain uninterrupted.

> "ExtraHop has fundamentally changed the way that we monitor and manage our business."

DIRECTOR OF IT
US-Based Application Provider

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 technology:
Global Semiconductor Manufacturing Leader
Wizards of the Coast
US-Based Application Provider

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

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