EXTRAHOP

DATA SHEET

RevealX Network Detection & Response (NDR)

Reveal and Respond to Cyber Risk Faster with Complete Network Visibility

With on-premises, hybrid, multi cloud, and remote environments, the attack surface is now too complex for the traditional security approach to keep up with modern advanced threats.

While log data and endpoint data offer value for threat detection, they can be turned off, evaded, or modified by an adversary. Yet, all devices and all activities on the network generate traffic on that network. Luckily, this network traffic can be passively observed and not subject to any tampering and not be evaded.

ExtraHop enables organizations to leverage the network as a central source of cybertruth and transparency. Our RevealX platform provides the 360-degree network visibility you need to see and stop advanced threats already inside your on-premises, cloud, hybrid, and distributed environments. With our advanced AI, behavioral analytics, and decryption to live network telemetry, you can detect, investigate, and resolve threats 87% faster—including almost 90% of MITRE ATT&CK techniques.

With no agents to instrument or logs to enable, ExtraHop RevealX protects your business operations without slowing down or introducing friction for your stakeholders.

With RevealX NDR, you can reveal your cyber risk and build business resilience.

Investigate smarter. Stop threats faster. Move at the speed of risk.

KEY CAPABILITIES

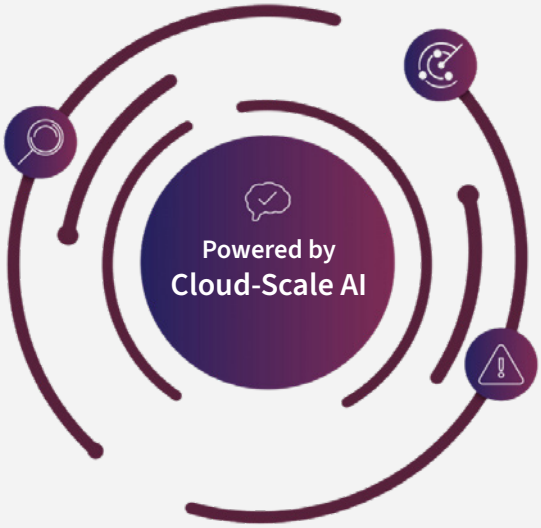
- Detect threats and anomalies with Cloud-Scale AI scaling your entire attack surface
- Auto-discover your attack surface and classify all devices and assets on the network
- Decrypt traffic covertly while remaining out-of-band for no performance impact
- Automatically collect all packets at records and be able to reference them anytime
- View and investigate across all environments and deployments from one unified UI
- Enrich every detection with an attack timeline, risk score, and ability to drill down
- Push-button response by automating investigation with full context and guided workflows
- Know the latest global threats and if you're affected with our Threat Briefings
- Deploy SaaS-based or self-managed, both with the full benefits of cloud-native NDR
- Unlock more value in one platform with our Network Performance, Forensics and IDS modules

Security Use Cases

- Asset & Application Discovery
- Dependency Mapping
- Workload & Data Monitoring
- Security Hygiene
- Vulnerability Assessment
- Insider Threat Detection
- Advanced Threat, Ransomware & Malware Detection
- Breach Detection & Response
- Threat Hunting
- Forensic Investigation
- SOC Transformation
- Audits & Compliance
- Tool Consolidation

Simplified & Streamlined Investigation

Automatically curated and intuitive forensics workflow to quickly scope, respond to, and contain incidents.
If it happens, you can stop it.



Automated Attach Surface Discovery

Instant complete visibility into everything on your network: every user, application, asset, transaction, service, and workload.
If it happens, you see it.

High Fidelity Detection

Leverage decryption and cloud-scale machine learning to zero-in on distinct/unique transactions and minimize incidents.
If it happens, you'll know it.

Complete Visibility

RevealX automatically discovers and classifies every device communicating across the network, with real-time, out-of-band decryption so security teams can see hidden attackers and crucial transaction details without compromising compliance or privacy.

With full East-West visibility from the data center to the cloud to the edge, you'll understand your enterprise from the inside out.

Real-Time Detection

RevealX catches threats in real time by applying Cloud-Scale Machine Learning and AI across real-time analytics extracted from 5,000+ L2-L7 features.

RevealX automatically identifies critical assets and compares peer groups to deliver high-fidelity detections, correlated with risk scores and threat intel so you can prioritize the highest risk threats for human attention.

Intelligent Response

The RevealX workflow takes you from security event to associated packet in a few clicks, erasing hours spent manually collecting and parsing data. Instant answers enable immediate, confident responses. Robust integrations with security tools including Crowdstrike, Splunk, Palo Alto Networks, and more help you rise above the noise of alerts, automate investigation, and act in time to protect your customers.

Spectrum of Detection

Hygiene

Activity that represents risk: ports, protocols, cryptographic compliance, and vulnerable or non-compliant services

Known Attacks

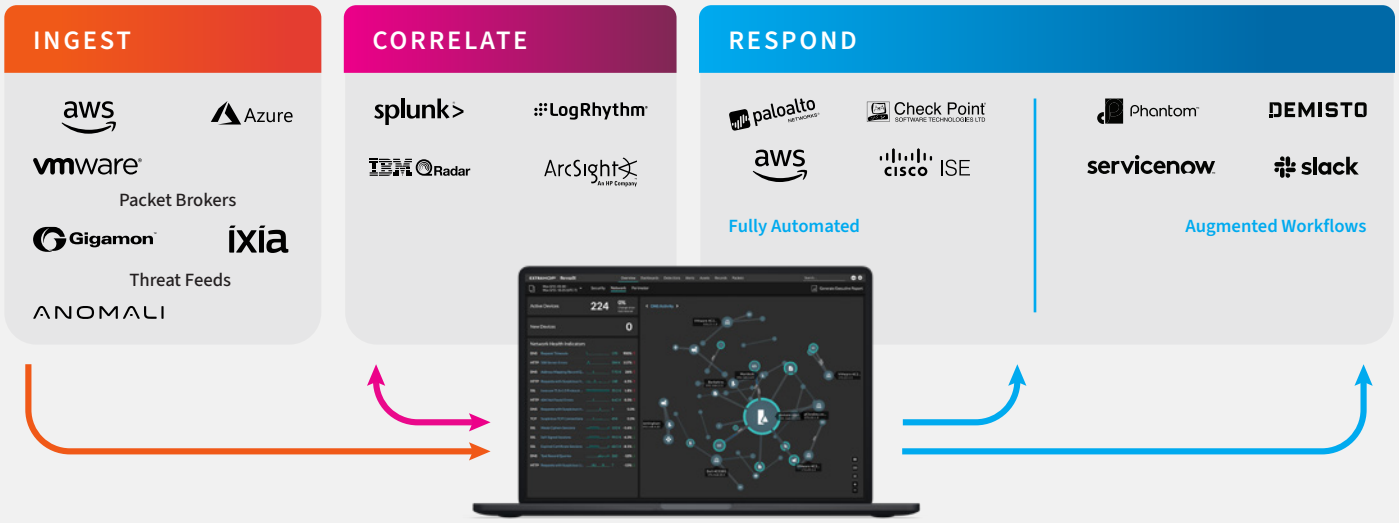
IP addresses, domains, file names, payload strings, or protocol behavior observed in past attacks (including intelligence feeds)

Unknown Attacks

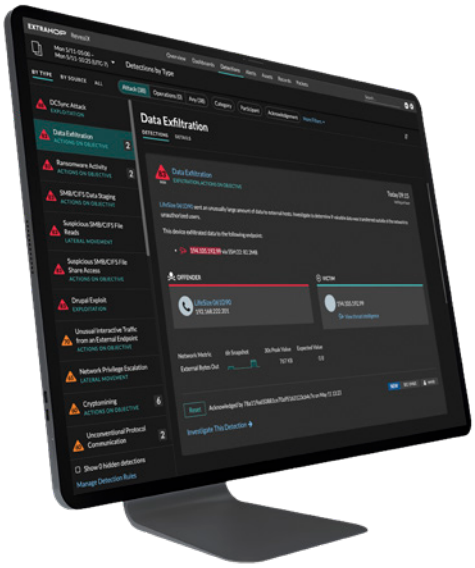
Attacks that do not have a previously known identifier, but exhibit anomalous behavior that can be linked to part of the attack lifecycle

Rule-Based Detection | **Robust Anomaly Detection** | **Sophisticated Behavioral Detection** | **Peer Group Detection**

230+ Integrations & Partnerships



ExtraHop RevealX

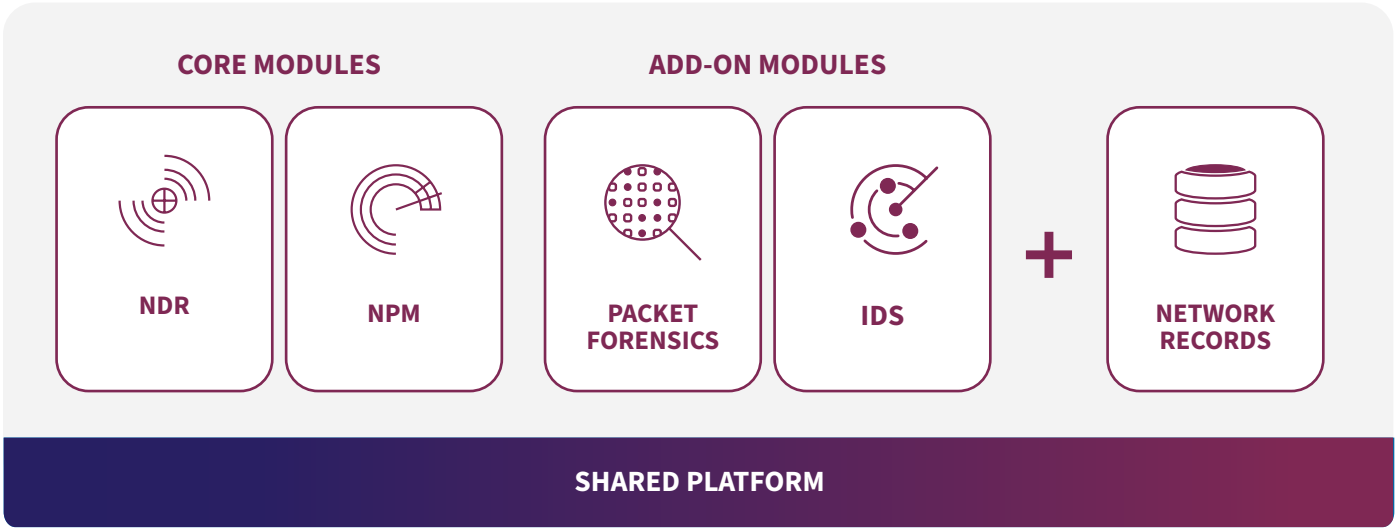


The RevealX Platform

Get more from the NDR module of ExtraHop RevealX. Integrate it with our Network Performance module to instantly identify network and application performance issues. Fully address IT, network, and security operations use cases from a single RevealX platform, while having dedicated workflows for each team.

Further strengthen your security capabilities with the Network Forensics add-on module, allowing for real-time packet capture and digital forensics, and the IDS add-on module, offering Intrusion Detection with Premium Threat Intelligence.

RevealX 360 or RevealX Enterprise



Single Tier with Modules

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk.

EXTRAHOP