EXTRAHOP™

SOLUTION BRIEF

Stop Ransomware Attacks with Unparalleled Network Visibility

Your goal is to enable the business while reducing risk. But what happens when a cyberattack exploits an unknown risk—a security blind spot? With RevealX, you gain complete visibility into the network so you can eliminate blind spots and quickly identify ransomware indicators that evade your existing security and IT tools.

HOW CAN YOU DEFEND AGAINST THREATS YOU CAN'T SEE?

The risk tied to ransomware is only increasing, with attacks up 95% year over year and ransomware payments topping $1 billion in 2023, a first. Threat actors continually find smarter and sneakier ways to launch ransomware attacks and gain access to (and hide in) endpoints and networks. They exploit emerging vulnerabilities and constantly change tactics, techniques, and procedures to evade detection and magnify impact.

While traditional Endpoint Detection and Response (EDR) solutions are vital to a holistic cybersecurity strategy, they can be evaded and manipulated, leaving a critical gap for cybercriminals to exploit. Furthermore, EDR tools won't detect a malicious actor abusing valid credentials. Once ransomware attackers bypass EDR, they can hide on the network, executing a sophisticated kill chain of post-compromise activities, sometimes waiting days or even weeks before completing their mission. Defenders need a smarter way to utilize this window to catch and stop ransomware before the damage is done.

GAIN COMPLETE VISIBILITY OF YOUR NETWORK

Having full visibility into both the real-time and historical activity on your network is critical to stopping a ransomware attack before it's successful, something only Network Detection and Response (NDR) tools can provide. The ExtraHop RevealX NDR platform gives organizations granular visibility into the cyber threats, vulnerabilities, and network performance issues that evade their existing security and IT tools. Using AI-driven behavioral analysis and machine learning, RevealX tracks and records ransom-driven attackers as they breach the network, attempt to maneuver through an infrastructure, enumerate targets, escalate domain privileges, or send C2 beacons over noisy DNS channels. It spots data staging and other suspicious behavior patterns that can indicate ransomware attacks *before* encryption starts.

With full network transparency, organizations can investigate smarter, stop threats faster, and move at the speed of risk.

Resolve Threats 87% Faster with RevealX

Eliminate Blind Spots
Gain complete coverage

Detect Threats That Other Tools Miss
Detect threats 83% faster

Act Quickly to Defend Your Business
Decrease time to remediation by 86%

Benefits

Complete Network Visibility

Gain full visibility into everything on your network—every user, application, asset, transaction, service, and workload—from the user and the office to the data center or the cloud. If it happens, RevealX can see it, even in encrypted traffic.

Broad Spectrum Detections

Detections are driven by machine learning/artificial intelligence, fed by multiple proprietary and third-party intelligence sources, and delivered with rich context to accelerate triage and mitigation. Threat briefings developed by our expert research team provide guided detection and investigation workflows for emerging and critical vulnerabilities.

Enterprise Scale Platform

Offering a single platform for datacenter, cloud, and distributed environments, RevealX provides unified network intelligence, delivered wherever the user needs. It offers decryption and analysis of global traffic in real time, up to 100 gigabits per second, with no degradation of service or added latency.

Modern Extensibility and Integrations

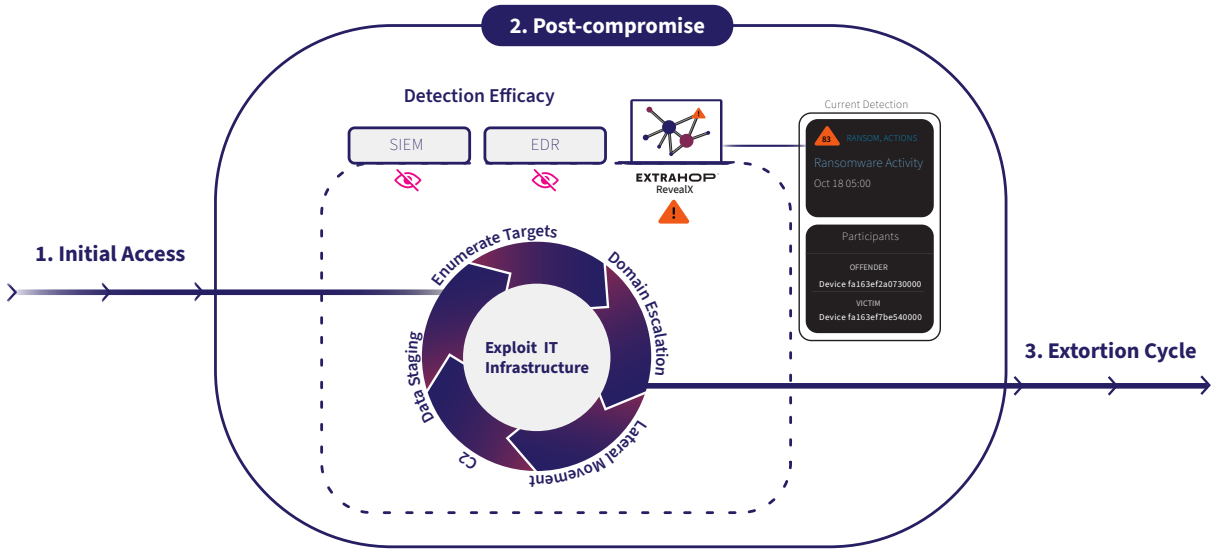
Publicly available APIs and documentation, including REST and trigger types, enable teams to integrate RevealX with their existing tech stacks across on-premises and SaaS deployments.

"Without ExtraHop, the investigation would have taken days or weeks, exposing the hospital to potentially catastrophic risk. Even the FBI was impressed when they found out how quickly we identified and contained the [ransomware] threat!"

—Joanne White, CIO, Wood County Hospital

How RevealX Works

Stop the Ransomware Kill Chain



USE CASES

DETECT COMPROMISED ASSETS	Network telemetry gives a superior understanding of baseline behaviors and quickly detects deviations. RevealX spots ransomware intruders other methods miss, dynamically adjusting cloud-scale ML to your changing environment.
APPLY COMPENSATING CONTROLS FOR EDR EVASION	Ransomware attackers evade EDR-enabled endpoints by applying living-off-the-land techniques—plus exploiting the prevalence of unmanaged servers, Linux hosts, and IoT devices. Using passive network observation, RevealX has unique visibility into these evasive behaviors.
PROTECT SENSITIVE DATA	With RevealX, you can prevent data theft and uncover signs of data encryption of high-value databases and file systems–before they're held hostage. Enable faster, more confident actions with immediate context.
HUNT RANSOMWARE THREATS	RevealX provides intuitive threat hunting workflows, with AI-driven prioritization and recommendations, so analysts of all skill levels can hunt like old pros. Analysts form and test hypotheses faster with automated and efficient investigation workflows.
RECOVER FASTER WITH NETWORK FORENSICS READINESS	Incident responders jump into action with 90 days of continuous traffic record lookback and long-term PCAP repository scalable to 24 petabytes. They can apply lessons learned to future response by creating incident response playbooks using smart investigation features.

TAKE THE NEXT STEP

Visit our website to learn how you can achieve full network visibility for your organization to stop ransomware threats and reduce risk to the business.

About ExtraHop Networks

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. Learn more at www.extrahop.com.

EXTRAHOP™

info@extrahop.com
extrahop.com