ARE YOU READY FOR RANSOMWARE?

How to investigate smarter and see threats faster.

EXTRAHOP®

Table of Contents

Introduction

Ransomware is a business problem with the potential to wreak devastating consequences on an organization. Our latest research and conversations with customers and cybersecurity professionals confirm that ransomware remains a constant source of anxiety. Results from our "2024 Global Cyber Confidence Index" found that 58% of organizations experienced 6 or more incidents in 2023, up 32% year over year. The number of companies with zero incidents dropped from 9% in the 2023 survey results to 5% in 2024.[1]

The potential economic impact is alarming, as ransom payments grow larger and more frequent, averaging $2.5 million in 2023.[2] But paying the ransom only gets you the decryption key. There are other significant costs required for full remediation, which is why the analyst firm Gartner warns that the total cost of recovery from an attack can be 10 to 15 times more than the ransom.[3]

The potential effects of a ransomware attack on your revenue, reputation, productivity, and market value are daunting. But what if you could stop a ransomware attack *before*…

- the true costs of a breach come to bear?
- the contentious, emergency board meetings and gut-wrenching payouts?
- the stock plunges, along with investors' trust?
- customers feel the sting of betrayal?
- life grinds to a halt for everyday people?

There are moments, before all of this happens, that make these outcomes preventable. Moments where, with the right tools, you can prevent the chaos before it starts. But you have to be ready for anything — any anomaly, any variable — whatever X-factor comes your way.

The first step to being ready for [X] is full network visibility

Ransomware has become a lucrative business. And like most businesses, those steering the ship are creative and driven. While firewall and endpoint detection and response (EDR) solutions are vital to a holistic cybersecurity strategy, organizations can no longer rely on prevention-focused defense. Ransomware attackers are evolving their tactics, finding new ways to evade and manipulate these traditional perimeter security and IT tools. Once on the network, attackers are free to enumerate targets, move laterally, and establish command-and-control connections.

Network detection and response (NDR) solutions, on the other hand, passively monitor network traffic to provide complete visibility into all activity on your network—identifying ransomware threats that other tools can't. NDR tracks and records ransom-driven attackers as they breach the network and attempt to maneuver through your infrastructure, giving cybersecurity professionals the ability to detect, investigate, and stop an attacker before systems are compromised and encryption begins.

This eBook will expand on this conversation by:

- Exploring the current state of ransomware
- Weighing the strengths and weaknesses of EDR
- Discussing the value of NDR and how it prevents a threat from becoming an attack
- Sharing how organizations are achieving business outcomes with NDR
- Introducing the ExtraHop RevealX NDR platform

1 While the survey didn't define an incident as a successful ransomware attack, based on the numbers reported by survey respondents, we take "incident" to mean an attempted ransomware attack.

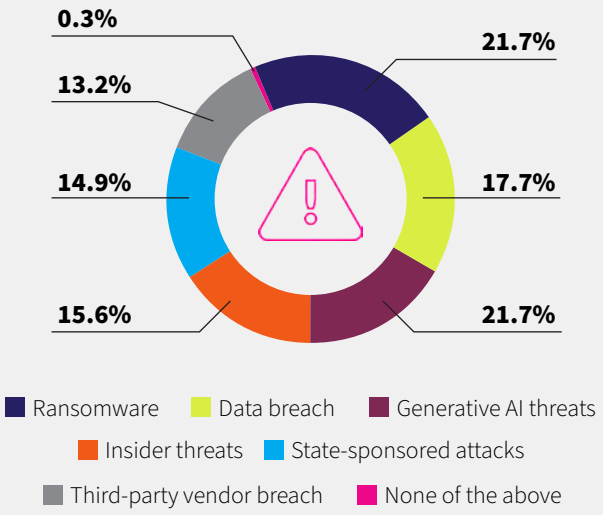
2 https://hop.extrahop.com/resources/papers/global-cyber-confidence-index-2024/

3 Gartner, How to Prepare for Ransomware Attacks, Mark Harris, Brad LaPorte, Paul Furtado, November 16, 2020

RANSOMWARE ATTACKS ARE MORE PROLIFIC, SOPHISTICATED, AND DESTRUCTIVE

Ransomware attacks increased 95% year over year[4] and accounted for nearly 25% of all breaches in 2023[5], with payments topping $1 billion last year for the first time.[6] The risk of falling prey to a ransomware attack is increasing as threat actors continually find smarter and sneakier ways to launch attacks and gain access to (and hide in) endpoints and networks. Consequently, respondents to our 2024 survey say ransomware attacks pose the greatest risk to their organization (21%) vs. other threats, and they report on average experiencing nearly eight ransomware incidents in the last year, including both successful and unsuccessful attacks.[7]

The greatest threat to today's organizations[8]



Attackers are so successful because they are constantly innovating–changing tactics, techniques, and procedures to avoid detection and magnify impact. They evade EDR-enabled endpoints by applying living-off-the-land techniques, hiding in encrypted traffic, and exploiting the prevalence of unmanaged servers, Linux hosts, and IoT devices. They also use a variety of tactics to trick and manipulate users, including phishing/smishing, exploiting supply chain vulnerabilities, and aggressive social engineering.

Nearly every organization we surveyed paid at least one ransom last year (91%), and 75% of respondents say they paid more than half the time. The number of organizations never having paid a ransom has significantly decreased in a shocking downward trend: whereas in 2022, 28% of respondents reported never having paid the ransom, that number dropped to 17% in 2023 and 9% in 2024.[9]

Organizations are likely paying the ransom out of necessity or desperation, believing it will give them the quickest path to restored business operations. But this strategy is likely to backfire; paying the ransom doesn't guarantee an organization will recoup its data, in fact, quite the opposite. In addition to securing ransom payments, attackers are selling their victims' sensitive data to other threat actors through the Ransomware-as-a-Service (RaaS) economy, increasing their own ROI and their victims' chances of re-exploitation. Those organizations that have fallen victim to a ransomware attack are six times more likely to be targeted again over the next three months.[10] And 90% of our survey respondents suffering ransomware attacks reported experiencing at least two additional ransomware incidents in the last year.[11]

4 https://www.securitymagazine.com/articles/100051-there-were-11-more-ransomware-attacks-in-q3-than-q2-2023
5 https://www.verizon.com/about/news/2023-data-breach-investigations-report
6 https://www.nbcnews.com/tech/security/ransomware-hackers-raked-1-billion-last-year-victims-rcna137445
7 https://hop.extrahop.com/resources/papers/global-cyber-confidence-index-2024/
8 https://hop.extrahop.com/resources/papers/global-cyber-confidence-index-2024/
9 https://hop.extrahop.com/resources/papers/global-cyber-confidence-index-2024/
10 https://www.akamai.com/lp/soti/ransomware-on-the-move
11 https://hop.extrahop.com/resources/papers/global-cyber-confidence-index-2024/

TRADITIONAL SECURITY PRODUCTS ARE NOT ENOUGH

Endpoint detection and response (EDR) tools are critical components to a successful cybersecurity strategy. They are designed to protect an organization's ever-expanding number of endpoints, like computers and phones, web servers, even branch offices. EDR agents monitor activity on those endpoints and raise alerts if they suspect suspicious activity like malware. There is a long list of benefits to organizations using EDR including:

- Proactive threat hunting by continuously monitoring endpoints
- Automated response to detect threats, reduce response time, and mitigate risk
- Enhanced visibility into endpoints and what is happening on a device in real time
- Advanced analytics to identify suspicious patterns and behaviors that could signify a threat

Despite these benefits, EDR solutions on their own are not enough to completely protect an organization from ransomware attacks. The reality is that intelligent and creative threat actors are continuously evolving their attack techniques, finding new ways to evade and manipulate EDRs and leaving a critical gap for cybercriminals to exploit. For example, EDR tools can't identify malicious actors abusing valid credentials, and many tools like IoT devices and operational technology can't use EDR for threat detection. Additionally, attacks can originate elsewhere or avoid endpoints altogether, rendering EDR ineffective in those cases.

Emotet: "The world's most dangerous malware" EDR can't detect

Living up to its ominous title given by Europol, the European Union's law enforcement cooperation agency, Emotet is sophisticated, polymorphic malware, which means its code and identifiable features are constantly changed to evade detection by EDRs.[12] The goal of the attackers is to compromise an organization's entire infrastructure by spreading credential-stealing Trojans across employee accounts and using them to authenticate itself within the network. Eventually, the malware can shutdown systems, freeze computers, and make the organization's network unusable.

12 https://www.cisecurity.org/insights/white-papers/ms-isac-security-primer-emotet

NDR DELIVERS FULL NETWORK VISIBILITY AND PROACTIVE SECURITY

Many EDR products focus only on the enterprise perimeter, screening for known, bad IP addresses, URLs, emails, and DNS queries. Others aim to protect endpoints by scanning payloads for telltale signatures. The problem with these approaches is that the origination vectors and even payloads used in ransomware malware change constantly, even throughout the course of a single day. 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 detect, investigate, and stop ransomware before the attack is executed and the fallout begins. Having complete visibility into both real-time and historical activity on your network is critical to detecting and stopping a ransomware attack before it's successful, something only network detection and response (NDR) tools can provide. NDR is so powerful because, unlike EDR, it can detect ransomware threats after a network has been compromised but before the threat actor has the chance to exfiltrate data or encrypt their target.

Change Healthcare suffers the largest cyberattack on the U.S. healthcare system

In February 2024, Change Healthcare experienced a ransomware attack by the BlackCat/ALPHV RaaS group. BlackCat employs a variety of attack techniques, for example, using stolen credentials and exploiting known and unknown software vulnerabilities. The Change Healthcare breach cost an estimated $100 million daily, due to disruptions to providers' ability to bill and process medical forms and patients' ability to fill their prescriptions.[13] As of April 9, 2024, it's believed a second ransomware gang is holding stolen Change Healthcare data for ransom. The company has disconnected its systems to prevent further impact as a result of an ongoing cybersecurity issue.[14]

RevealX has been helping organizations detect and stop BlackCat ransomware attacks since 2022. There are a number of points throughout a BlackCat attack where RevealX detects anomalies other solutions can't–e.g. account enumeration, network share enumeration, network discovery enumeration, BloodHound enumeration with Active Directory, suspicious SMB requests, executable file transfers, the use of DCSync to harvest administrative credentials, suspicious use of RDP on a host, command, Tor node connections, data staging, and data exfiltration control.

13 https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html
https://www.cbsnews.com/news/change-healthcare-cyberattack-losing-up-to-100m-a-day/

14 https://healthitsecurity.com/news/change-healthcare-disconnects-system-amid-cyberattack

Why EDR needs NDR for full coverage

The "post-compromise" space between a breach and the attack is critical. A ransomware attack has three phases. In phase one, the attacker evades EDR to gain a foothold in the environment. Phase two, post-compromise, begins when the attacker has compromised at least one device and begins pivoting through the infrastructure and enumerating targets. This is where attackers can remain undetected and have the most freedom of action. They will begin reconnaissance of the target network, stealing usernames, setting up persistence mechanisms, and attempting to compromise additional systems. In phase three, data has been exfiltrated and the ransomware has been launched onto the network; the organization is now fully compromised.

NDR can detect threats in the post-compromise phase that EDR can't. Unlike EDR, NDR can identify ransomware actors as they navigate across your infrastructure by passively monitoring raw network traffic feeds. It provides visibility into encrypted network traffic and all the devices and workloads where you can't deploy an endpoint agent–without degrading network or endpoint performance.

How NDR stops ransomware

Like EDR, NDR security solutions do not prevent malicious activity. Instead, they aim to alert security teams earlier in the attack chain, so they can stop attack activity in progress before it can result in harm.

NDR passively captures network communications and applies advanced analytic techniques, including behavioral assessment and machine learning, to identify both known and unknown attack patterns, detect malicious activity and understand security risks and exposure. This granular, packet-level data can also be used to perform real-time investigation into post-compromise activity and to forensically investigate incidents. While not all NDR solutions can decrypt network traffic, the most advanced solutions provide targeted decryption capabilities to help identify threats hiding within encrypted traffic.

NDR is so powerful because, unlike EDR, it can detect ransomware threats after a network has been compromised but before the threat actor has the chance to exfiltrate data or encrypt their target.

Benefits of NDR for organizations

Detect, investigate, and intelligently respond to cyberattacks in real time to prevent breaches

With complete visibility across your enterprise architecture, you'll be able to put controls around the unknown or unmanaged assets in your environment while reducing the time needed to pinpoint root cause and move to resolution.

Simplify IT operations to eliminate complexity and costs

Streamlined operations can increase staff and business productivity and reduce burnout, leading to accelerated innovation–not to mention the improved customer experience and reputation enabled by reduced downtime.

Reveal unknown threats and stop intruders in their tracks

Leave ransomware operators no place to hide with continuous visibility across all devices and workloads—including encrypted authentication and Active Directory ticket escalation attempts. RevealX is designed from the ground up for continuous packet capture, detecting intruder probing activities, lateral movement, remote procedure calls (RPC), and C2 communications. Accelerate mean-time-to-detect (MTTD) and investigate cyber threats and remove layers of tool complexity with a solution that leverages cloud-scale machine learning to produce high-fidelity network-based detections.

Deter and stop attackers from returning

Using RevealX investigation workflows with traffic record lookback and a scalable PCAP repository, incident responders can pinpoint the root cause and scope all compromised assets and data. Incident Response teams can then develop repeatable and defensible incident response playbooks based on this network intelligence. Gain real-time risk insights about your organization's attack surface, vulnerabilities, and security hygiene to reduce the risk of data exfiltration from a successful ransomware attack.

YOU NEED TO BE READY FOR [X]

Protecting your organization from ransomware requires visibility, insight, and control of post-compromise activity in your networks. The ExtraHop RevealX NDR platform gives organizations just that with 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 from RevealX, organizations can:

- **Investigate smarter** by improving efficiency and business resilience with real-time network insights and high-fidelity machine learning detections.
- **Stop threats faster** by eliminating blind spots and responding to threats in their earliest stages to prevent business disruption and minimize financial impact.
- **Move at the speed of risk** to enable the business and keep operations running by revealing hidden risks across your organization and implementing compensating controls.

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%

Wood County Hospital takes a proactive stance against ransomware

Challenge: Alert fatigue, coupled with lack of visibility into threats inside the network, left Wood County with a crucial security gap.

Results: Using RevealX, Wood County Hospital:

- Identified a new strain of ransomware (two weeks before being notified by its MSSP) and quickly identified and neutralized the threat before it could impact operations.
- Is saving more than $70,000 per year in technical resources.

> **“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!”**
>
> — CIO, Wood County Hospital

DETECT AND STOP THREATS BEFORE IT'S TOO LATE

Experts warn that the damage of ransomware costs to organizations could exceed $265 billion by 2031.[15]

While traditional approaches like EDR that focus on the perimeter and rely on signatures play an important role in any security strategy, they are not enough to protect you from ransomware attacks on their own. Once ransomware evades EDR, they are powerless to provide additional defenses, allowing threat actors to navigate freely through the network as they plot their final attack.

NDR gives organizations complete visibility, insight, and control over their network so they can detect, investigate, and stop ransomware threats before they do damage. Enterprises large and small are using the ExtraHop RevealX NDR Platform today to detect and shut down ransomware activity in real time. You don't have to wait for the industry to catch up with cybercriminals. Get the visibility you need today to detect, investigate, and stop ransomware threats before they can compromise your business.

15 https://securityintelligence.com/news/ransomware-costs-expected-265-billion-2031/

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. Learn more at extrahop.com.

EXTRAHOP®

info@extrahop.com
extrahop.com