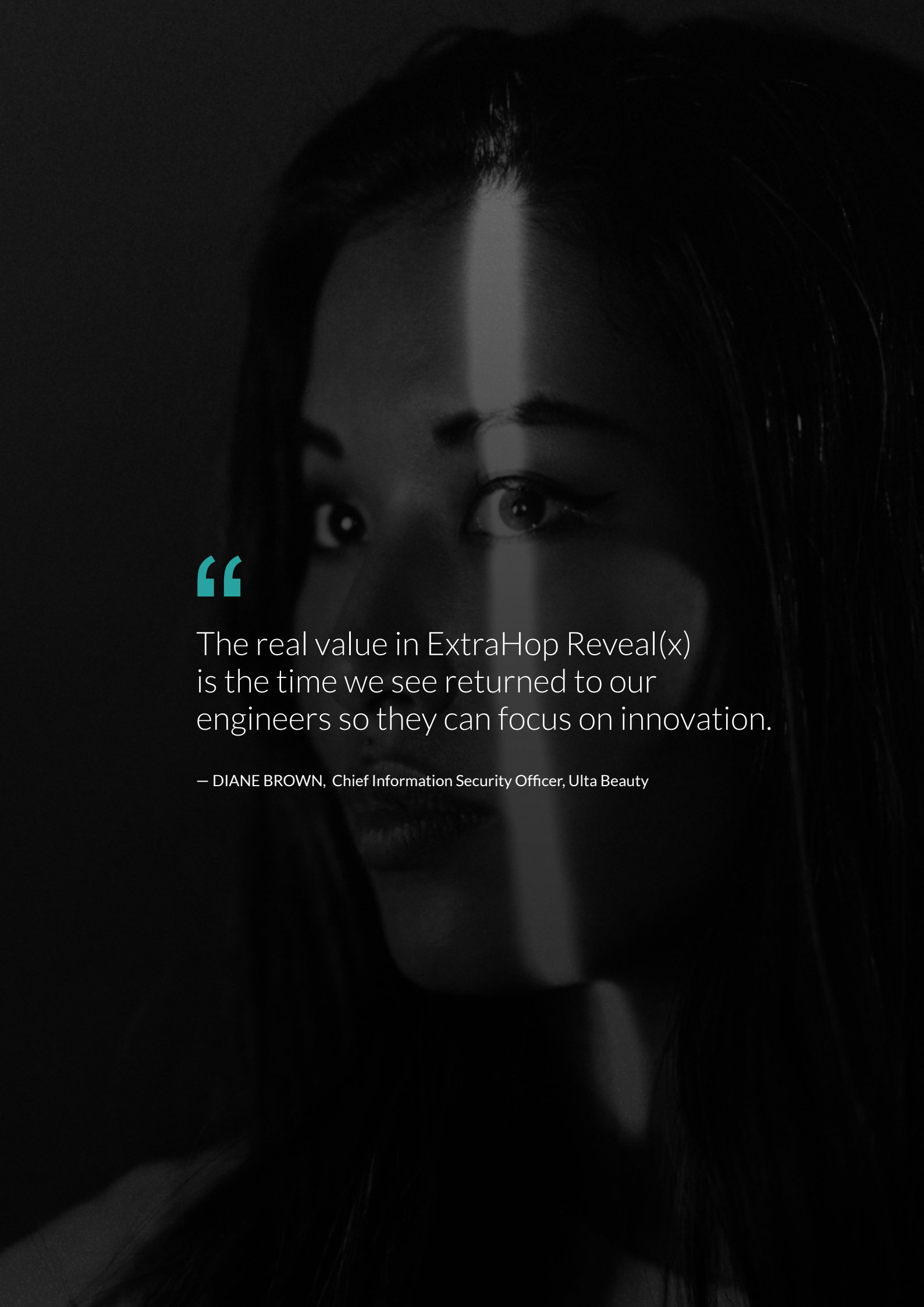
NDR

Beginner's Guide to Network Detection and Response

for Hybrid Security

ExtraHop

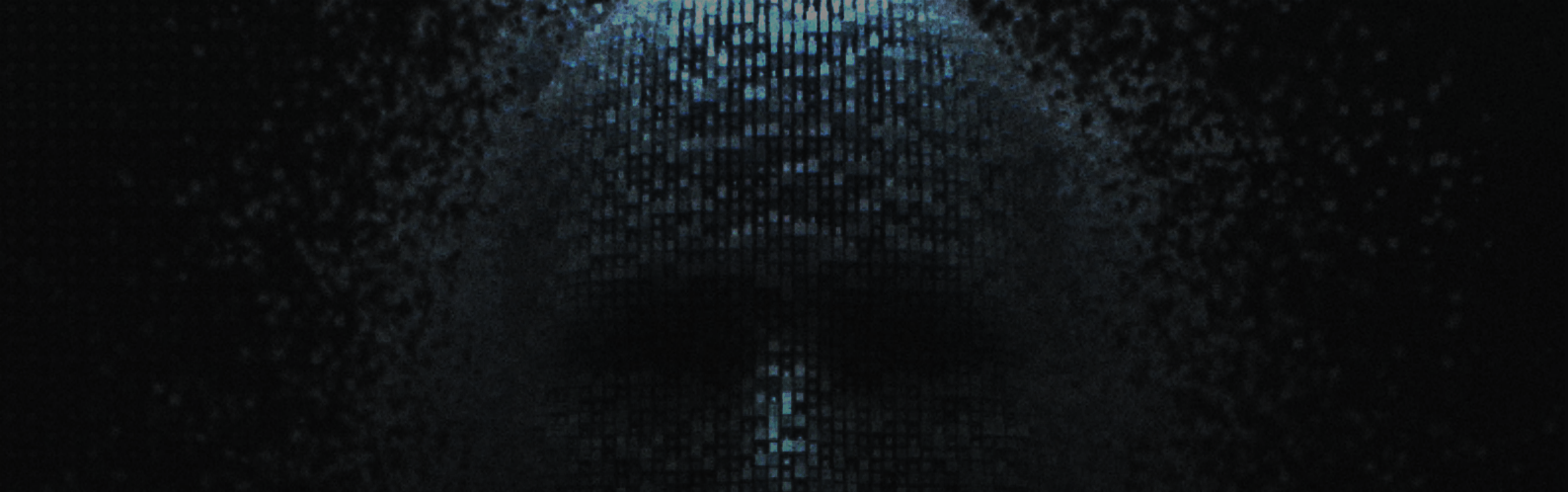


“

The real value in ExtraHop Reveal(x) is the time we see returned to our engineers so they can focus on innovation.

— DIANE BROWN, Chief Information Security Officer, Ulta Beauty

Table of Contents



Network Detection and Response 101

What Is Network Detection & Response?

We live in exceptional times. The pandemic has driven an unprecedented surge in digital investments, to the point that some experts are claiming many businesses will be forever transformed. But where there is cloud-based innovation, there is also risk. These same investments, while enabling new business opportunities and ways of working, have broadened the enterprise attack surface. And they've unwittingly left gaps in visibility and coverage that threat actors are only too capable of exploiting, whether through vulnerabilities, ransomware, software supply chains, or any number of advanced threats.

The NDR market currently stands at more than $1 billion and is the second-fastest growing cybersecurity category with an expected 17% compound annual growth rate (CAGR) over the next three years.

That's why many organizations are looking to network detection and response (NDR), a category of cybersecurity solution that detects malicious activity through network traffic analysis. While NDR security solutions do not prevent malicious activity, they identify post-compromise activities and provide an early warning signal that something is wrong—enabling organizations to stop attacks before they cause major damage.

NDR does not use an agent to gain insight into malicious activity, relying instead on a network or virtual tap for analysis of traffic across on-premises and cloud workloads. That's important, because without agents, NDR solutions are able to:

- Reduce deployment complexity
- Reduce security friction in DevOps processes
- Provide greater scale than agent-based solutions

Why Organizations Need NDR

Despite the rapid pace of recent digital transformation initiatives, some workloads are likely to always remain on-premises. That's why almost all organizations use hybrid cloud deployments. Additionally, more than 90% of organizations use either two or more cloud service providers (CSP) or are unsure how many different cloud environments they use.

Yet this blend of environments increases the enterprise attack surface, inviting the attention of financially motivated and state-backed threat actors. They have an increasingly broad range of tactics, techniques, and procedures (TTPs) available to them. And, in the case of cyber-criminals, an underground economy worth trillions via which to share tooling, knowledge, and stolen data.

Additionally, stretched security teams are increasingly outnumbered. They're struggling with visibility gaps in their hybrid infrastructure, particularly in east-west traffic. Incomplete or inefficient telemetry leaves too many shadows where adversaries can hide. As does encrypted traffic, which many tools can't probe for signs of malicious behavior.

The same security teams are often overwhelmed by too many tools. In fact, 68% of organizations say they want to reduce the number of tools they use. Many only work in one environment (on-premises or cloud; IaaS, Paas, or Saas), creating coverage gaps and silos between security and operations teams. The bottom line: it becomes even more challenging to detect post-compromise behaviors inside the perimeter.

Many organizations rely on logs and agent-based data, using tools like SIEM, EDR, firewalls, and tooling specific to cloud service providers (CSPs). But time and again, attackers have been able to evade perimeter tools. Additionally, it's impossible to instrument every asset with an agent and logs are rarely comprehensive.

The end result: unacceptably long dwell times before threat actors are discovered, as was the case with the SolarWinds exploit. And the longer they go undetected, the more damage is done, such as via data exfiltration, or ransomware deployment. Many victims find out too late that they've been hit.

Why NDR Matters

Unacceptably long dwell times are one reason why many organizations are turning to NDR solutions to complement or even replace legacy and CSP-native security tools. SIEM and EDR are deployed for good reason, but they leave blind spots in the east-west corridor where adversaries can hide after they've slipped past perimeter defenses. By taking a network-based approach instead, NDR fills those critical visibility and coverage gaps. How? Because every asset, whether in the cloud or the on-premises data center, uses the network to communicate. That makes NDR the ultimate source of truth for cloud and hybrid security.

Best-in-class NDR solutions also provide a unified management pane where users can:

- Visualize telemetry from on-premises, hybrid, multi-cloud environments
- View and investigate detections across deployments via a single pane of glass
- Respond to threats, either via human intervention or automated response integrations

When combined with EDR and SIEM products, NDR solutions fulfill Gartner's SOC Visibility Triad on-premises and in the cloud. They also offer much-needed help to organizations struggling with security analyst shortages. The global shortfall of cyber professionals stood at 2.7m in 2020, including 402,000 in North America

8 Questions to Ask NDR Vendors

When considering an NDR solution, it's crucial to understand your use cases and how you'll get value out of adding a new tool. To help evaluate competing NDR products, ask vendors these eight essential questions.

- Does it solve real, identified business problems?
- How cost-effectively does the product scale?
- Does it decrypt traffic for analysis, and if so, how?
- Does it integrate with other products you already use?
- Can it automate investigations?
- How does it enable automated response and remediation?
- Does its AI/ML provide real value?
- Is it cloud-native, to seamlessly provide full NDR capabilities across the hybrid enterprise?

How NDR Provides Threat Defense

Today's organizations run mission-critical apps and workloads across on-premises, hybrid, and multi-cloud environments. This has expanded their attack surface and created critical visibility and coverage gaps, which log and agent-based tools struggle to fill. Best-in-class NDR tools shine a light on suspicious behavior to close gaps and help organizations minimize cyber-risk, regardless of deployment environment.

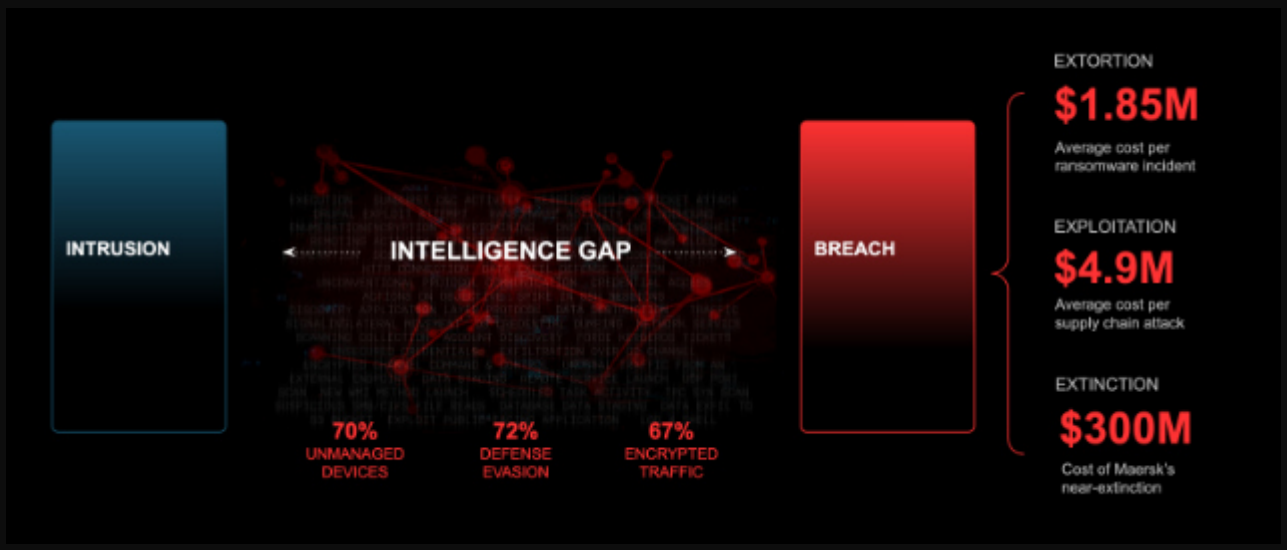
Eliminate Blind Spots

Prevention at the perimeter is only one component of cybersecurity. Products focused at this layer have only one goal: to keep threats out. But what happens when attackers manage to sneak inside, using stolen credentials or other tactics? Perimeter tools are blind to malicious activity inside enterprise networks.

NDR delivers crucial visibility in this east-west corridor where attackers hide, analyzing every transaction and surfacing high-fidelity alerts with context in real time. It can also offer out-of-band decryption of SSL/TLS encrypted traffic, even when perfect forward secrecy (PFS) is enabled. That's increasingly important as more threat actors use encryption. It's estimated that over 90% of malware is hidden this way.

> Visibility is required all the way through the OSI Layer 2–7 stack, but most often such visibility is not available.
>
> — IDC Technology Spotlight

From a cloud perspective, the kind of network-based visibility NDR delivers into workloads is increasingly important. Under the Shared Responsibility Model for cloud security, CSPs broadly secure the infrastructure of the cloud, while customers bear the responsibility for protecting their infrastructure in the cloud. Effectively, this means customers are in charge of managing their own workload security, and Gartner predicts 99% of cloud security failures will occur on the customer side of the Shared Responsibility Model. Defense-in-depth backed by NDR has never been more important.



ExtraHop Reveal(x)360 Eliminates Blind Spots

As the leading cloud-native enterprise NDR solution, Reveal(x) 360 provides complete visibility by leveraging several essential capabilities, including:

- Automatic, continuous asset discovery and classification
- Out-of-band decryption of SSL/TLS 1.3 (PFS) encrypted traffic
- Out-of-band monitoring of on-prem and cloud communications
- Access to packets and VPC Flow Logs in AWS
- Layer 2 through Layer 7 payload analysis of packet data
- Real-time and historical visibility in containerized environments

Threat Detection

Cloud-scale success

Perimeter-focused tools can stop some attacks from compromising the corporate network. But attackers have a range of TTPs available to them, and only need to get lucky once. After bypassing preventative measures at the perimeter, they use the east-west corridor to move laterally and conduct reconnaissance. Often, they use encrypted traffic to hide suspicious activity or commandeer legitimate credentials and tooling to avoid tripping any alarms.

Threat detection products that rely exclusively on rules and log data are ill-equipped to spot and block such activity. Rules can't take into account fast-evolving threats, and logs don't provide the depth of packets for forensic investigation and threat hunting. Because it's not generated in real time, log data is also of limited use in stopping breaking attacks.

> 62% of organizations admit their current toolsets leave coverage gaps. 83% use logs, flow, endpoint, or a combination of those data sources.
>
> — ExtraHop 2021 Cloud & Hybrid Security Tooling Report

Best-in-class NDR products combine rules and behavioral detections by machine learning-powered and/or AI to identify threats inside the perimeter. But not all NDR is created equal. It takes a great deal of compute power to execute machine learning (ML) advanced and robust enough to detect threats in real time. That makes cloud-hosted ML/AI essential to offloading resource-intensive modeling and providing continuous, automated updates to NDR detection models. Cloud-scale ML like this is the only way for NDR products to operate at true enterprise scale—offering the fast, contextual threat detection needed to reduce attacker dwell time and cyber-risk.

How quickly can your current detection tools identify a breach? Read these four ways to reduce dwell time.

How ExtraHop Reveal(x)360 Delivers Advanced Threat Detection

With full-spectrum detections and custom models, Reveal(x) 360 identifies suspicious behaviors, prioritizes high-risk threats, and automates or augments response. Here's how:

- Real-time stream analysis that extracts more than 4,800 features
- Advanced cloud-scale ML for precise behavioral analysis
- Automatic peer group categorization for devices
- Context-rich detection cards that act as a force multiplier for security teams
- Access to VPC Flow Logs and network packets in AWS

Forensic Investigation

Driving rapid incident response

To minimize dwell time, organizations must shorten the window between an attacker's initial penetration into an environment and threat detection to begin investigation and response. Yet too often, stretched analyst teams must sift through thousands of alerts to find what they're looking for. Sometimes they must also "swivel chair" between multiple tools to obtain the right intelligence for their investigation. All of which adds vital time.

What's more, log-based tools can only record what they're told to. And logs can be modified or destroyed by attackers. They also fail to provide the granularity needed to validate events, determine with certainty what data was impacted during a breach, and discover whether threats are still active.

> Fast, contextual detections **reduce the dwell time** between threats breaching your perimeter defenses and your team responding to those threats.

NDR solutions should be able to provide deep forensic investigation to help analysts understand advanced threats and attacks. Top NDR products will also offer continuous packet capture (PCAP) for on-premises and cloud environments to provide the highest-fidelity evidence source available to investigators—network packets. By leveraging AI/ML algorithms for faster detection, and correlating the results with threat intelligence, best-in-class NDR offers an indispensable forensics tool. Analysts have everything at their fingertips to validate, triage, and establish root cause—driving rapid incident response in just a few clicks.

> In 2021 it took an average of 287 days to identify and contain a data breach, a week longer than in 2020
>
> – IBM Cost of a Data Breach report

How ExtraHop Reveal(x)360 Speeds Investigations

By automating the first few steps of investigations and providing access to the richest data source in hybrid security, Reveal(x) 360 forensics empower analysts, incident responders, and forensic investigators to act quickly and with confidence. Here's how:

- Access to 90 days of records, securely stored in the cloud
- Single management pane for unified investigation across environments
- Optional continuous packet capture (PCAP) for always-on incident response
- Ability to drill down into packets for forensic evidence in clicks

Intelligent Response

Break down silos for improved outcomes

Global cybersecurity skills shortages and gaps have reached critical levels. With the number of vacancies expected to reach 3.5 million by 2025, there's a rapidly growing need for more smart automation and third-party integrations.

NDR integrations with SIEM, Next-Gen Firewall (NGFW), security orchestration, automation, and response (SOAR) platforms, and more, can help in this regard. By automating mundane tasks, stressed SecOps teams can free-up time to spend on higher value work. And enhanced insight into attacks will provide clearer indications when analyst intervention is required.

NDR products can also help organizations to fill cybersecurity skills gaps by using their IT team. Often the first people to spot breaking threats are IT team members monitoring the corporate network and application performance. This first line of defense can be enhanced with NDR products to eliminate silos and reduce tool sprawl. By unifying data and processes in this way, organizations not only bring IT and security teams closer but also increase visibility and control across the attack surface.

> 95% of security workers feel like skills gaps have not improved in recent years, with heavier workloads (62%), unfilled positions (38%) and worker burnout (38%) all contributing factors
>
> — ISSA/ESG

Best-in-class NDR products also improve cyber-hygiene and compliance thanks to customized alerts, fine-tuned detections for unique policies, and dynamic activity groups that help deliver high-fidelity behavioral detections. Many NDR tools support a wide range of security frameworks for on-premises and cloud environments, including:

- MITRE ATT&CK
- CIS Top 20 Controls
- NIST Cybersecurity Framework
- OWASP Top 10 and more

How ExtraHop Reveal(x)360 Supports Intelligent Response

With the ability to pivot from detection to forensic evidence in clicks, Reveal(x) 360 provides security teams with the information they need to prioritize response and resource allocation. ExtraHop also offers dozens of integrations and automations through solution partners, including:

aws, splunk>, cisco ISE, servicenow, vmware, IBM QRadar, paloalto, Phantom, Azure, ArcSight, Check Point, DEMISTO, AlienVault, LogRhythm, Google Cloud, slack, ANOMALI, CROWDSTRIKE, FIREEYE

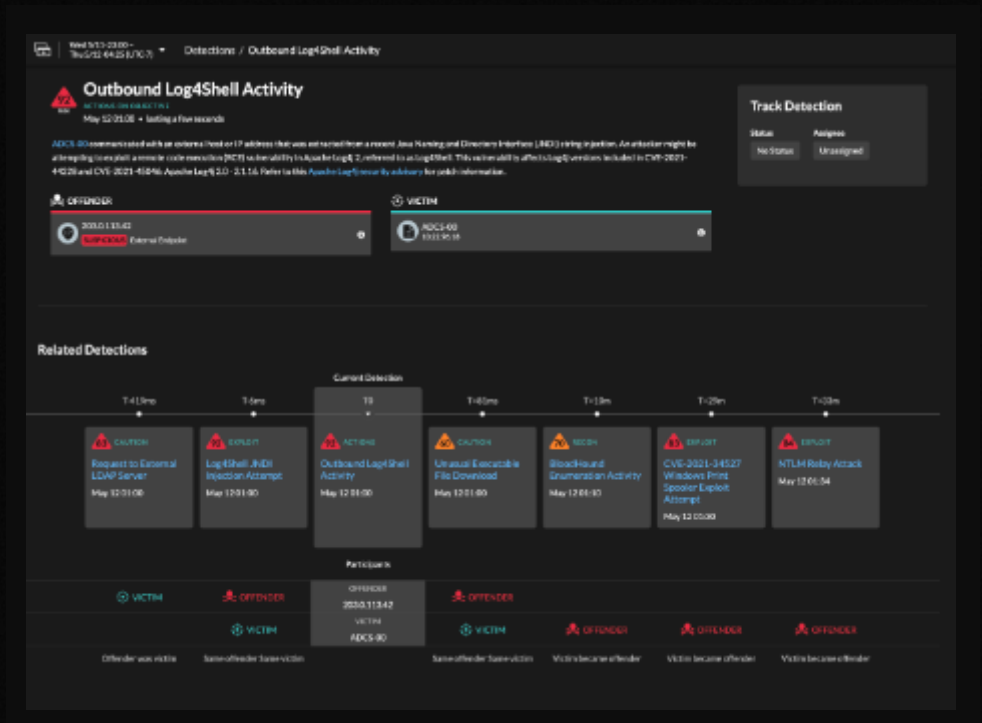
NDR Use Cases

Whether you're transforming your enterprise's digital footprint or need to enhance your existing cloud or hybrid security, NDR solutions provide frictionless coverage for a wide range of use cases. You can also explore the Reveal(x) 360 Use Case eBook or our interactive use case periodic table for more information.

Ransomware Detection and Response

Advanced ransomware attacks use a sophisticated killchain of post-compromise activities to accelerate and amplify propagation of their malware across the infrastructure. To mitigate ransomware, NDR products should provide:

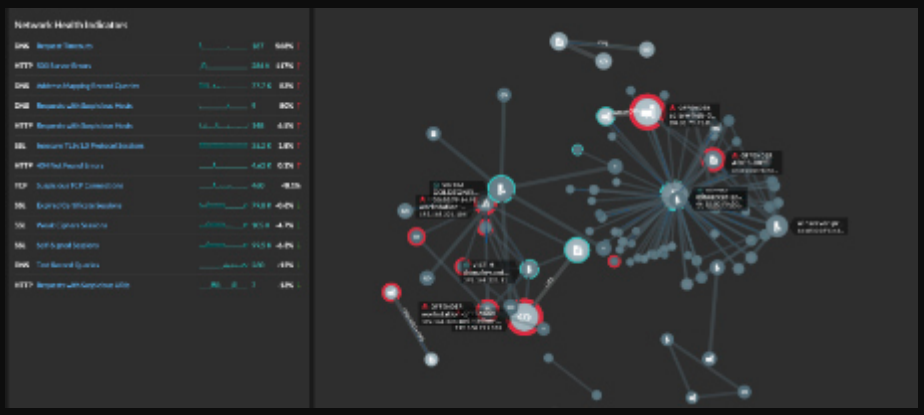
- Visibility into which clients received malicious files and suspicious IP addresses
- AI-powered detection of malicious post-compromise behavior
- Fast investigation and response for tactical isolation of only compromised systems



Critical Cloud Workload Monitoring

As organizations move to the cloud, they need the ability to monitor critical cloud workloads and sensitive data from a network perspective. It's the only way to truly get context into behavior and data flows. NDR solutions should provide:

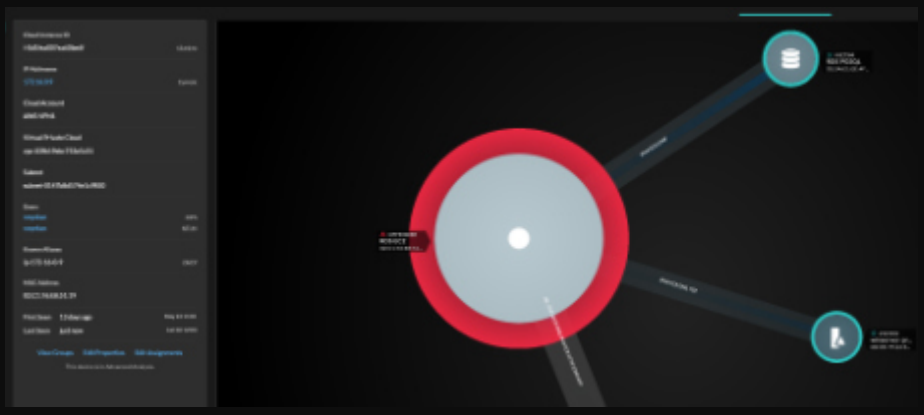
- Real-time visibility and insight into suspicious or malicious activity
- High-fidelity alerts about behaviors that go against established baselines
- Context about suspicious behaviors and data movement for deep investigation



Secure Cloud Migration

Migrating workloads to the cloud can be risky due to unforeseen broken user experiences, unknown dependencies, and an expanded attack surface. To support secure cloud migration, NDR products should provide:

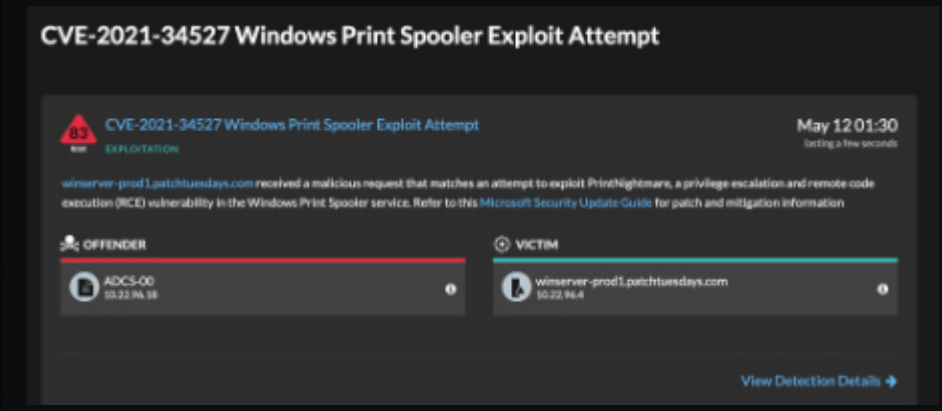
- Automatic discovery, classification, and mapping of all assets
- L2–L7 monitoring to prove out performance before, during, and after migration
- Real-time detection and threat intelligence from across the hybrid attack surface



Next-Generation IDS

While traditional intrusion detection systems are still popular tools, especially for compliance programs, they're an ineffective, signature-based technology against modern threats. NDR products that offer next-gen IDS capabilities can provide:

- Intrusion life cycle detection on-premises and in the cloud
- Full-spectrum detection powered by AI and rules-based analytics
- High-fidelity alerts with context for deeper investigation



Software Supply Chain Attack Detection

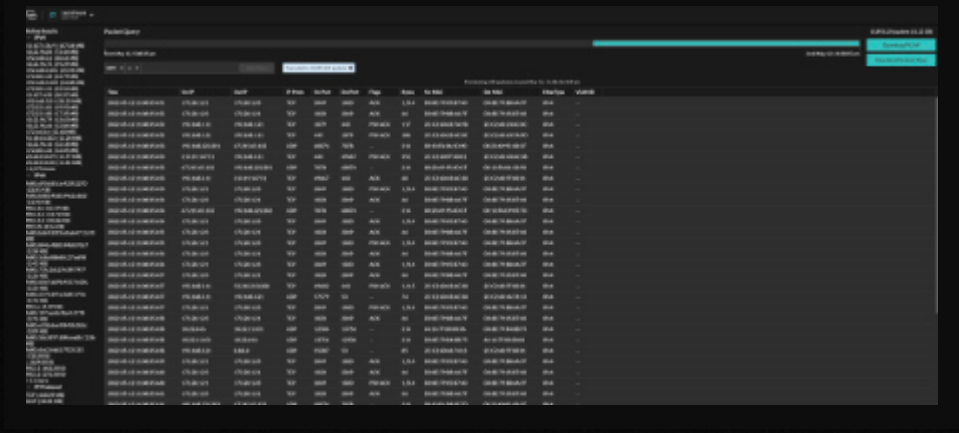
The ability to monitor workloads for unexpected changes or communications with untrusted or unknown entities is essential to stopping software supply chain attacks. To decrease risk and potential damage, NDR tools should provide:

- Continuous monitoring to quickly surface unexpected changes to cloud workloads
- AI-powered inference into which assets house critical data
- Forensic evidence via rapid investigation to respond quickly and stop attacks

Network Forensics

Endpoint data and logs provide investigators and incident responders with surface-level insight, but they can't offer the depth of network forensics available in packets. For forensic investigation, NDR products should provide:

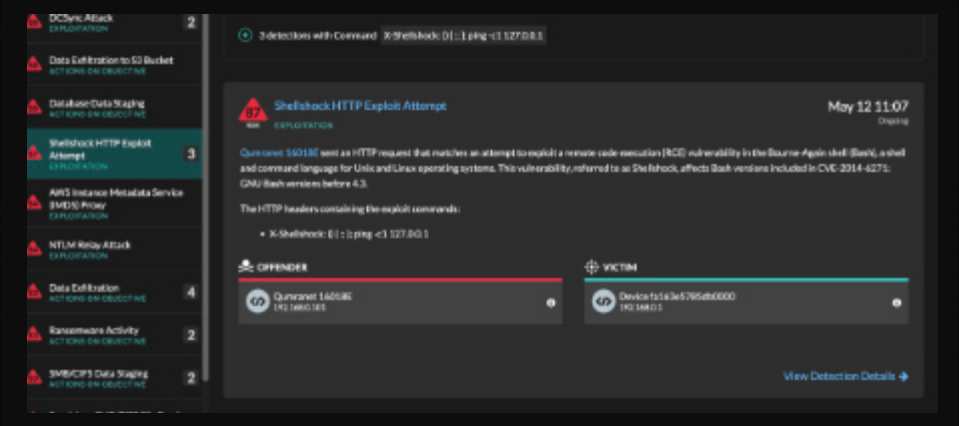
- 90 days of continuous traffic record look back
- Access to network packets for deep investigation
- Tracking of assets and data exploited or compromised by attackers



Threat hunting

For many organizations, threat hunting is only aspirational, whether because of SOC maturity or inexperienced security analysts. To support an effective threat hunting program capable of testing hypotheses and finding indicators of compromise, NDR solutions need to provide:

- Transaction data and intuitive query-based starting points
- Augmented workflows for faster hunting
- Ability to hunt threats across hybrid environments



Reveal(x) 360

Cloud-Native Network Detection and Response Delivered as SaaS

50%
FASTER THREAT DETECTION

86%
FASTER THREAT RESOLUTION

99%
FASTER TROUBLE SHOOTING

ExtraHop is the leading provider of cloud-native network detection and response for the hybrid enterprise. With complete visibility, real-time threat detections, and automated investigation powered by cloud-scale machine learning, ExtraHop enables security teams at leading enterprises including Credit Suisse, The Home Depot, Caesars Entertainment, and Liberty Global to rise above the noise of alerts, organizational silos, and runaway technology in order to accelerate investigations, unify policies across hybrid environments, and build their security the way they're building their business: cloud-first.

To experience the power of ExtraHop, explore our interactive online demo or connect with us on LinkedIn and Twitter.

ExtraHop