ExtraHop

# It's Time to BREAK the Most Common Myths About NDR

Network detection and response (NDR) solutions are powerful and versatile, and they deserve their place in every enterprise's security technology stack. By detecting known threats and anomalous behaviors using the network, NDR can quickly and accurately flag the first indicators of an attack that other tools would miss.

Because NDR is a relatively new technology, it's not yet well understood, and misconceptions about what it does—and its value—are much too common. We're here to set the record straight.

## What is Network Detection and Response (NDR)?

### WHAT NDR IS...

Network detection and response (NDR) solutions ingest network traffic, using machine learning to detect malicious activities, monitor for security risks, and identify exposure. NDR operates out of band and without agents. Security teams can leverage NDR for a wide variety of use cases, such as stopping in-progress attacks before they result in data theft or business disruption.

### WHAT NDR ISN'T...

#### #1 Only Beneficial for IT Operations

HATE TO BREAK IT TO YOU, BUT...

The same detailed packet-by-packet visibility that helps network teams keep track of network performance and boost end user experience can empower security teams to identify potential attacks, investigate incidents, and facilitate a rapid response.

TOP 5 NDR USE CASES YOU MAY NOT HAVE CONSIDERED

- Ransomware detection
- Critical cloud workload monitoring
- Secure cloud migration
- Next-generation intrusion detection
- Supply chain attack detection

#### #2 Only Relevant for Network Security

PREPARE TO HAVE YOUR MIND BLOWN...

NDR fills key visibility and coverage gaps, removing blind spots across on-premises, hybrid, and multicloud environments.

Because NDR provides such comprehensive visibility, it's been demonstrated to improve overall threat response times by 87%[1]

#### #3 Labor-Intensive to Implement and Maintain

SCRATCH THAT...

Best-in-class NDR solutions use automation to reduce the burden on security teams, so their care and feeding is likely easier than you think.

Native integrations enable leading NDR solutions to play nice with every element in the modern security stack:

- Endpoint detection and response (EDR)
- Security information and event management (SIEM) solutions
- Security orchestration, automation, and response (SOAR) platforms
- Ticketing platforms
- Firewalls

## Myth: I don't need NDR because I have EDR.

### REALITY...

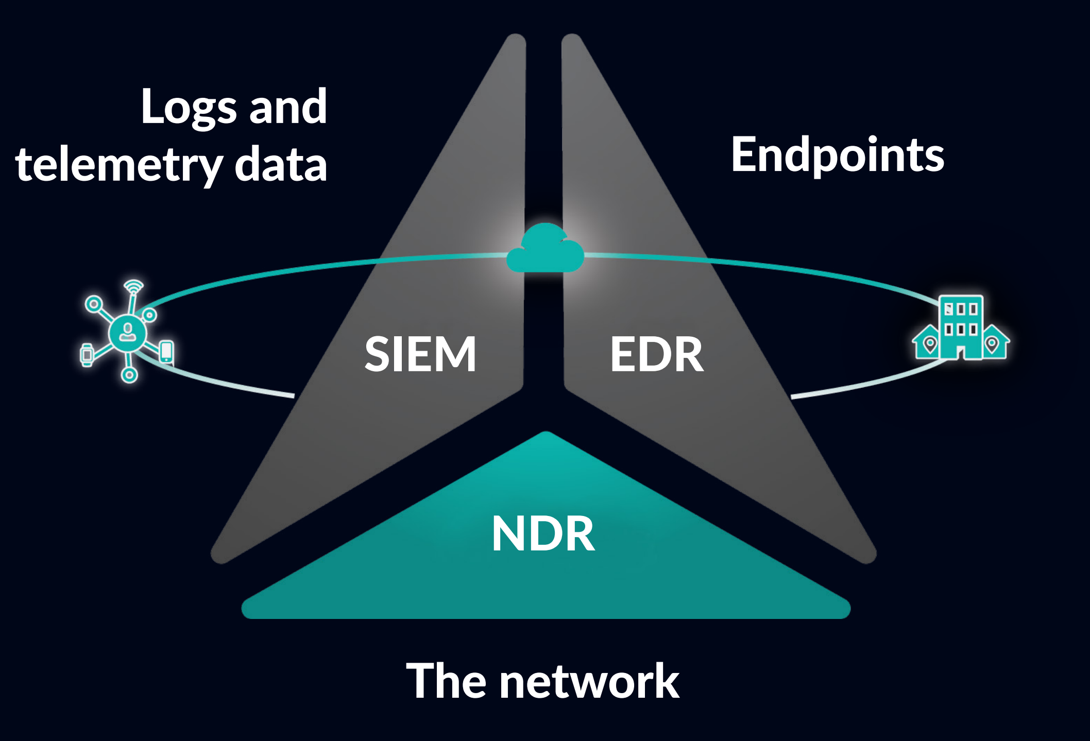
THAT'S SOME BROKEN LOGIC...

EDR alone isn't enough to deliver the enhanced visibility needed to detect and rapidly respond to advanced threats.

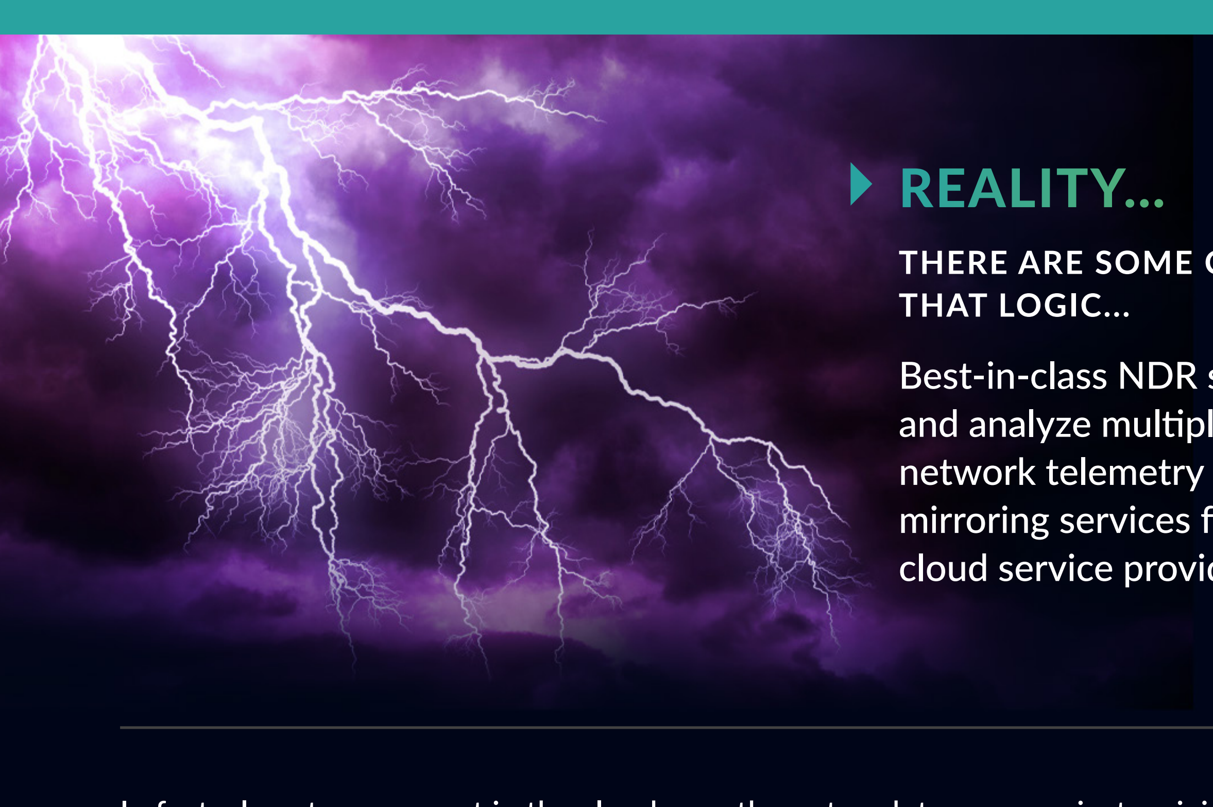
**NDR empowers defenders by shining a spotlight on malicious activities that would otherwise remain hidden.**

70% Without NDR, up to 70% of an enterprise's environment remains dark.

The full visibility that's required for effective security operations demands visibility everywhere:



## Myth: NDR isn't a cloud security tool.



### REALITY...

THERE ARE SOME CRACKS IN THAT LOGIC...

Best-in-class NDR solutions ingest and analyze multiple types of network telemetry using packet-mirroring services from all major cloud service providers (CSPs).

In fact, almost every asset in the cloud uses the network to communicate, giving NDR unique and critical visibility into traffic between cloud workloads as well as on-premises assets. In addition, NDR covers a broad variety of use cases involving other endpoint and workload types, including:

- Cloud workloads
- On-premises hardware
- Internet of things (IoT) devices
- Mobile devices
- BYOD and third-party access

## Myth: NDR can't detect encrypted or advanced threats.

### REALITY...

TIME TO SHATTER THIS MISCONCEPTION...

Advanced NDR solutions use out-of-band decryption to detect advanced threats hiding in encrypted traffic without impacting network performance.

**With packet-level visibility, NDR detects activities carried out even by the most sophisticated and capable adversaries.**

This is the case even if attackers:

- Turn off logging or erase logs
- Disable agents
- Remove antivirus software
- Make use of encryption to cover their tracks
- Leverage zero day exploits or software supply chains
- Co-opt already-installed security tools for their own purposes

## It's Time to Learn the Truth about NDR

### INTRODUCING EXTRAHOP REVEAL(X) 360

Purpose-built to secure modern enterprises, Reveal(x) 360 provides comprehensive visibility across complex environments where workloads span the edge, core, and cloud, and where on-premises and remote workforces rely on hardware, applications, and data in all of these places. Reveal(x) 360 is a SaaS-based solution that unifies security across on-premises and cloud environments, including everything from containerized deployments to IoT sensors.

Reveal(x) 360 provides agentless visibility and situational intelligence without friction, delivering immediate value with a low maintenance burden. In AWS environments, Reveal(x) 360 combines the breadth of VPC flow logs with the depth of packets for multi-layered threat intelligence.

**Want to discover more of the truth about NDR?**
**Download our NDR Myths vs. Reality e-book today.** >

ExtraHop

ExtraHop is the cybersecurity partner enterprises trust to reveal the unknown and unmask the attack. The ExtraHop Reveal(x) 360 platform is the only network detection and response solution that delivers the 360-degree visibility needed to uncover the cybertruth. When organizations have full network transparency with ExtraHop, they can see more, know more, and stop more cyberattacks. Learn more at www.extrahop.com