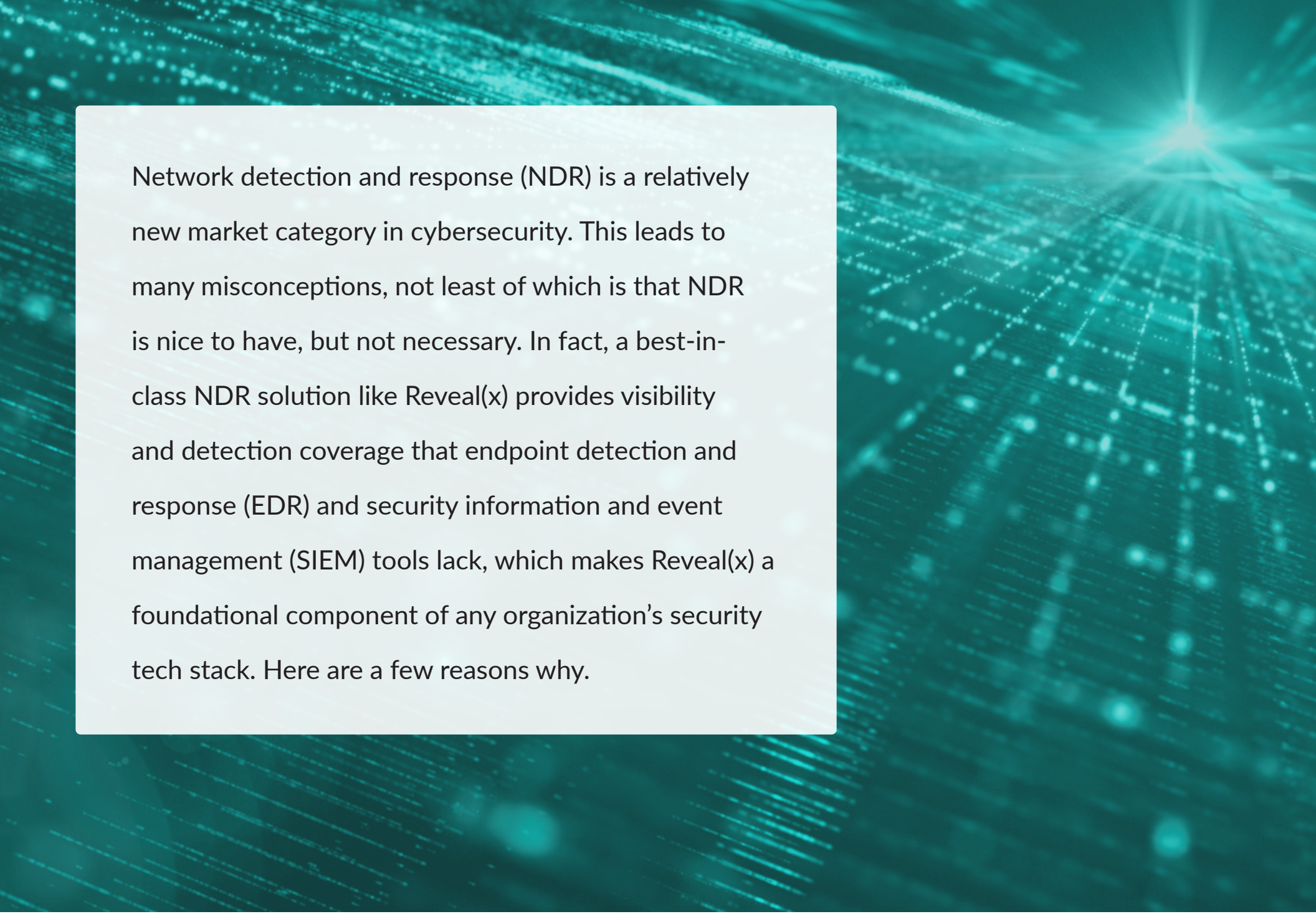
ExtraHop

5 Reasons Reveal(x) Is Indispensable to Security and IT Teams

How Packet-Level Visibility and Out-of-Band Decryption Provide What Other Tools Can't



Network detection and response (NDR) is a relatively new market category in cybersecurity. This leads to many misconceptions, not least of which is that NDR is nice to have, but not necessary. In fact, a best-in-class NDR solution like Reveal(x) provides visibility and detection coverage that endpoint detection and response (EDR) and security information and event management (SIEM) tools lack, which makes Reveal(x) a foundational component of any organization's security tech stack. Here are a few reasons why.

1 Reveal(x) Picks Up Where EDR and SIEM Leave Off

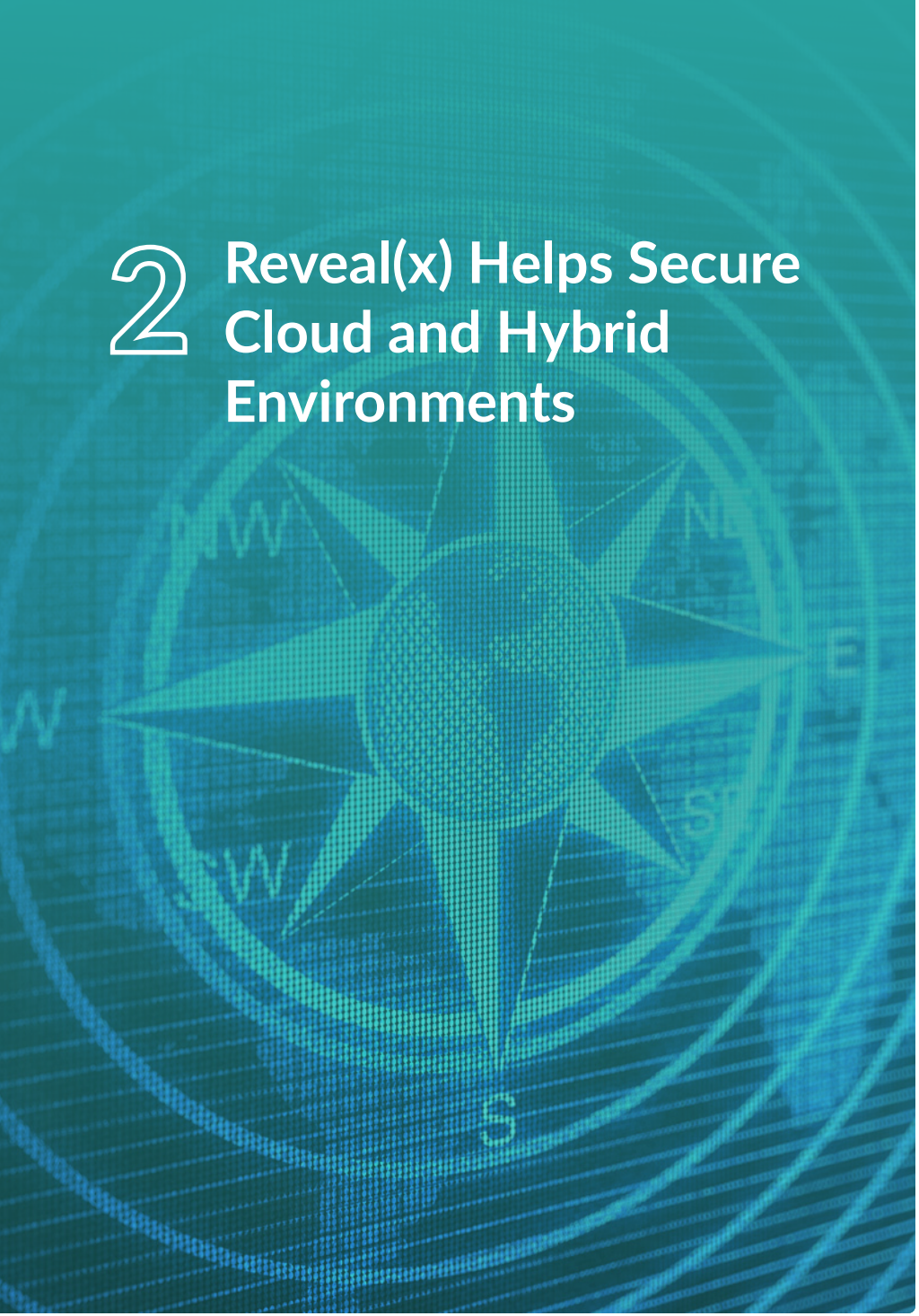
Many organizations believe they don't need NDR because they already have EDR and SIEM. While it's true that EDR and SIEM provide essential visibility into endpoints and logs, both tools have their limitations.

EDR solutions require agents to be deployed on each endpoint they monitor, but not every endpoint can support an agent. In fact, by ExtraHop estimates, as much as 40% of an organization's endpoints can't support an EDR agent. Internet of things (IoT) devices often are incapable of running an agent, and you may not be able to deploy agents on medical devices or on employees' personal mobile devices for privacy reasons. Moreover, sophisticated attackers can bypass EDR by taking advantage of these agentless devices or shutting down agents entirely.

In contrast to EDR tools, Reveal(x) is an agentless solution that monitors network traffic between endpoints. It analyzes communications between assets using advanced machine learning and peer group analysis to establish baselines based on observed behavior, identify the sometimes subtle deviations from the norm that indicate an attack, and create high-fidelity alerts. Because Reveal(x) analyzes network communications, it's easier to catch certain adversary tactics that take place in east-west traffic on the network than it is via endpoints, including persistence, enumeration, lateral movement, and more.

SIEM tools rely on logs, which can be useful when investigating an incident, but they lack context. For example, logs can tell you that two devices communicated, but packets can show you what they said. Because Reveal(x) analyzes network traffic down to packet-level detail, it provides the context necessary to identify threats in real-time and respond to attacks quickly and with confidence, unlike a SIEM.

Another advantage that Reveal(x) has over a SIEM: sophisticated attackers can delete logs, thereby covering their tracks and eliminating much of the evidence of their malicious activities, but they can't turn off the network. With Reveal(x), the network sees everything, shows everything, and leaves attackers with no place to hide.



2 Reveal(x) Helps Secure Cloud and Hybrid Environments

Firewalls and endpoint detection tools can't stop every threat from accessing your network through the cloud. That's where the east-west visibility provided by Reveal(x) comes in. Reveal(x) can rapidly identify post-compromise behaviors that indicate reconnaissance, lateral movement, privilege escalation, and more. It's also useful for a variety of cloud and hybrid use cases, including container security and secure cloud migration.

When cloud service providers released native packet mirroring services, they eliminated the friction associated with monitoring and analyzing network traffic in the cloud. Now, Reveal(x) offers the same packet-level visibility in the cloud without the need for agents as it does in on-premises environments. Since nearly every cloud asset uses the network to communicate, network telemetry is an invaluable source of information for monitoring, analysis, threat detection, and investigation. In addition to packets, Reveal(x) can ingest and analyze flow logs so you can monitor serverless environments. Reveal(x) also offers monitoring and analysis for containerized workloads and can provide packet capture (PCAP) in cloud environments, enabling deep forensic investigation.

3 Reveal(x) Detects Threats Hidden in Encrypted Traffic

Encryption can be a double-edged sword. It's increasingly required under various regulatory schemes, and updates to Microsoft Active Directory have made applying encryption much simpler. That's great news for many organizations, but it can also obfuscate data defenders rely on to detect and respond to advanced attacks. Not to mention that skilled adversaries can "live off the land" and hide their tracks by using defenders' own tools and encryption against them.

Reveal(x) leverages out-of-band decryption to uncover threats hidden in encrypted traffic, like ransomware or living off the land techniques, without impacting network performance. It also provides full-stack visibility into more than 70 protocols—including database and file sharing protocols that communicate in the east-west traffic corridor—so you can determine if the assets using them to communicate are configured correctly and do not unintentionally expose data and systems to attackers.

4 There's No Zero Trust Without NDR

The network and packet-level visibility provided by Reveal(x) is essential to **zero trust security**, but you don't have to take our word for it. In "The Forrester Wave™: Network Analysis and Visibility, Q2 2023," Senior Analyst Heath Mullins writes, "There can be no Zero Trust without visibility into what's happening inside networks."

Here's why:

According to the CISA Zero Trust Maturity Model, zero trust requires organizations to collect as much information as possible about the current state and security posture of assets, network infrastructure, and communications across their enterprises; to continually verify each user, device, application, and transaction on their networks; and to use dynamic policies to authenticate devices and users on a per-session basis. Only a leading NDR/NAV solution like Reveal(x)—that leverages strategic out-of-band decryption, processes full packets, and takes advantage of cloud-scale machine learning—can automatically discover, classify, and passively monitor all devices and communications on a network, in real time, so that organizations can make informed, policy-driven access decisions.

5 Packet-Level Visibility Benefits Security and IT Operations Teams

Your organization's network is the highest fidelity source of truth about potential security threats and performance issues, but that truth is only useful if you can see it. Reveal(x) is a boon to both security and IT operations teams because it's capable of providing real-time, packet-level traffic inspection. For ITOps, visibility up to the application layer makes troubleshooting potential network issues and optimizing app performance much easier. As importantly, Reveal(x) helps performance-focused teams rule out the network when it's not to blame for slowdowns or broken user experiences, helping to end war rooms and finger-pointing. Security teams, meanwhile, can leverage these powerful insights to identify potential attacks, investigate incidents, and facilitate responses quickly and efficiently. A tool like Reveal(x) can **eliminate friction between IT and security teams**.

If You're Not Using Reveal(x), You're Missing Out

Advanced threats require advanced defenses. Sophisticated attackers are increasingly using living off the land techniques and tactics like supply-chain compromises and zero-day exploits to evade detection. And as mentioned above, they often cover their tracks by erasing logs and disabling agents. But they still need to communicate and move laterally over the network. The network is as close to the ground truth as you can get, and attackers can't shut it off. Reveal(x) lets you use this to your advantage so your security team can efficiently detect and respond to threats that other tools miss.

ABOUT EXTRAHOP NETWORKS

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**

ExtraHop