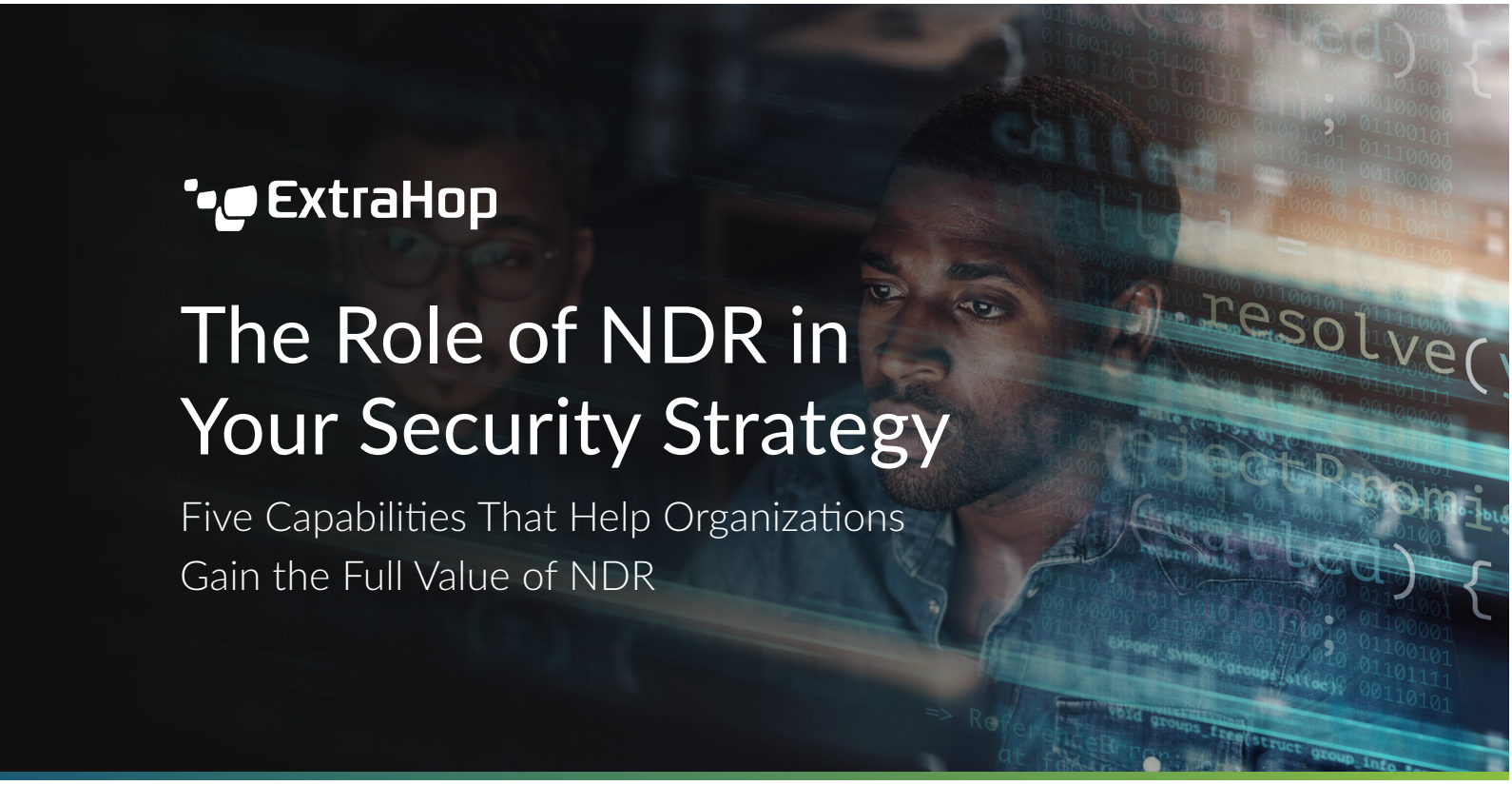

ExtraHop

The Role of NDR in Your Security Strategy

Five Capabilities That Help Organizations Gain the Full Value of NDR

Traditionally, security operations centers (SOCs) have relied on endpoint detection and response (EDR) and security information and event management (SIEM) tools to prevent cyberattacks. While EDR and SIEM products have improved threat detection for many organizations, these solutions can be difficult to deploy, operate and manage, and they often lack key features and capabilities that organizations need to detect and stop threats earlier in the attack cycle to minimize business impact.

For example, to gain broad endpoint visibility, organizations need to deploy agents on all of their endpoints–a potentially costly and time-consuming proposition, especially for large enterprises, that can degrade the performance of those endpoints. The need to deploy so many agents on so many endpoints complicates maintenance of the EDR solution. Additionally, savvy attackers can shut down or remove agents. Meanwhile, SIEM products–due to their reliance on log data–tend to generate a lot of false positives that distract security analysts and lead to alert fatigue. Logs also contain limited information, which leads to limited context and insight, and logs can also be destroyed or modified by attackers.

The challenges associated with EDR and SIEM have prompted forward-leaning security teams to implement network detection and response (NDR) solutions. These organizations have come to understand that the network, not logs or endpoints, is the highest-fidelity data source for early threat detection. The network, afterall, is where adversaries first land, where they expand their reach, establish command and control (C2) communications, move laterally, and employ stealthy "living off the land" techniques to evade detection by traditional endpoint security solutions. The network also can't be compromised by attackers the way endpoint agents and logs can. And that's why early adopters have been drawn to NDR: because it provides security teams with complete visibility inside the network—into north-south and east-west traffic—something SIEM and EDR solutions simply aren't built to do. And through that visibility, security teams can catch the anomalous network behaviors that often signal an early stage attack.

> Organizations rely on NDR to detect and contain postbreach activity such as ransomware, insider threats, or lateral movements.[1]

The caveat? Not all NDR solutions are created equal. As the Gartner® Market Guide for Network Detection & Response, December 2022 explains, finding the truth about which features are more valuable can get murky. This white paper describes five capabilities your NDR solution should provide in order to help your organization understand its attack surface and detect, investigate, and respond to threats faster across cloud, on-premises, and hybrid environments: cloud-scale machine learning (ML), continuous and on-demand packet capture (PCAP), strategic decryption of internal traffic, investigative workflows, and asset discovery.

These five capabilities may not appear in every NDR buyer's guide, but they're essential because they go above and beyond the traditional, "table stakes" features like metadata enrichment and alert aggregation. Moreover, these capabilities are the differentiating features that really help organizations extract full value from their NDR solution.

Read on to learn more about these five capabilities, why they're so critical, the impact they can make on your organization's security posture, and how to determine if an NDR solution you're considering (or currently using) actually supports them.

Capability #1: Cloud-Scale Machine Learning

The ability to quickly identify, investigate, and respond to advanced threats and performance issues is critical for organizations. NDR solutions that offer cloud-hosted and cloud-scale ML, rather than relying on "on-box" compute power for analysis and detection, benefit hybrid and multi-cloud organizations in several key ways.

Detections and Analytics: Cloud-hosted ML workloads are able to leverage sophisticated, compute-intensive predictive models and identify suspicious or malicious behavior in real time to create high-fidelity alerts. In order to produce the best analytical results specific to each customer, ML algorithms should be able to automatically infer customer-specific contextual information—including peer groups, security policies, and device and user roles—based on the observed unique behaviors of every entity on the network.

Scalability: Analyzing data with machine learning is a compute-intensive practice that requires exponentially more processing power than is available "on box" in an appliance or via a supplemental virtual machine. When machine learning workloads run in the cloud, they take advantage of the cloud's virtually limitless computational resources, which is especially valuable for "bursty" tasks like retraining models. Thus, cloud-hosted ML allows organizations to analyze data from across their hybrid and multi-cloud environments.

[1] *Gartner, Market Guide for Network Detection and Response, Cybersecurity Research Team, 14 December 2022*

Global Coverage: Running ML locally and independently on each network appliance limits the coverage organizations derive from their NDR deployment. In contrast, when NDR products use cloud-scale ML, they provide global coverage across all on-premises and cloud networks within a single ML engine instance. This global coverage provides organizations with more accurate analytics and detections based on the behavior of an entire hybrid environment, ranging from campus networks to private data centers to public cloud workloads, instead of individual network regions. Cloud-scale ML also allows organizations to benefit from the network effect of the algorithms working across customers to identify suspicious behavior.

Rapid Security Updates: Security threats evolve so quickly that daily firmware updates and weekly model updates are no longer fast or frequent enough. NDR products that leverage the cloud for ML can push live updates and continuous ML engine deployments to ensure customers always get the latest iterations of ML analytics without any manual interaction.

Hybrid and multi-cloud environments will continue to be a mainstay of many organizations. Consequently, having cloud-scale ML will allow organizations to secure their various environments without slowing down their business.

Capability #2: Continuous and On-Demand PCAP

Network data is the ultimate source of truth for hybrid and multi-cloud security and observability, so the ability to capture network packets provides organizations with additional depth and context. PCAP enables security and IT teams to understand exactly what is happening in a network. PCAP also enables security teams to hunt threats, respond to sophisticated attacks, and conduct forensic analysis and investigation to determine how the attacker infiltrated the environment and what the blast radius might be. On the compliance side, PCAP is a core requirement for organizations that need to comply with U.S. federal government cyber modernization mandates, including Executive Order 14028 and OMB M-21-31.

Depending on the NDR solution, organizations can leverage continuous PCAP that's always on, precision PCAP that's triggered by events, or both.

Continuous PCAP traditionally collects and saves all packets that pass across a network. Because this always-on method of packet capture is not triggered by specific detections, it enables security and IT teams to analyze packets from before, during, and after a security event or performance issue. Continuous PCAP also helps security teams proactively hunt threats and retroactively investigate data when new threat intelligence becomes available. Storage is one drawback of continuous PCAP.

Precision PCAP can be triggered by detections related to specific events, or it can be spun up on demand. Because it's not continuously running, precision PCAP requires far less storage space than continuous PCAP. However, the drawback of NDR tools that offer only precision or on-demand PCAP is that it only gathers information when it's "turned on," whether manually or via a trigger. As a result, if a security team investigating a breach needs information from before an event and on-demand PCAP were triggered, they may be out of luck. Similarly, if a breach doesn't set off a detection (i.e., false negative), on-demand PCAP won't be prompted.

Because organizations can benefit from both continuous and on-demand PCAP when investigating breaches, it's important to look for an NDR provider that can offer both.

Capability #3: Strategic Decryption of Internal Traffic

Attackers are getting better at bypassing perimeter controls and leveraging users' credentials to get to the heart of corporate network infrastructures, where companies keep their crown jewels. Once inside the network, attackers increasingly employ sophisticated techniques to evade detection. For example, they may encrypt any traffic they produce to access the outside world, such as command and control communications to their external servers. They may also leverage traffic in your organization that's already encrypted. As more network traffic becomes encrypted due to compliance requirements and other factors, attackers gain more ways to hide without having to deploy any of their own special tools. It also makes it harder for defenders to detect lateral movement.

However, if you deploy strategic decryption–that is, you only decrypt the traffic for which your organization created the encryption keys–you gain the ability to see into this traffic without compromising privacy because you don't decrypt any traffic for which you don't have the keys (e.g., employees accessing their online banking or personal email accounts).

Note that you'll want to perform strategic decryption not only on SSL/TLS, but also on MS-RPC, WinRM and SMBv3. The ability to decrypt traffic moving across those other protocols enables organizations to catch attackers as they attempt to move laterally, which usually happens very early in the attack cycle. The earlier you can detect attackers, the greater your chance of stopping them before they steal sensitive data or cause any other long term damage to your organization.

Capability #4: Investigative Workflows

When evaluating different NDR vendors, one of the most important aspects is function and user interface (UI). According to Gartner, "One of the benefits of NDR technology is the ability of its management and monitoring consoles to facilitate incident response workflows."[2]

Unfortunately, the UI for some NDR workflows can be clunky and difficult to navigate. Users may also need to swivel between user interfaces for different environments like on-premises or cloud. A great UI also helps security and IT teams understand the data they're trying to read. With a growing number of attack vectors and increasing levels of sophistication, your team needs to be able to react without getting bogged down in overly complex investigative workflows that take too much time to complete.

Look for an NDR solution that provides clear, intuitive investigation workflows that help analysts better understand and contain advanced threats. By gathering data and conducting analytics ahead of time with cloud-scale ML, NDR tools should be capable of automating many of the steps associated with security investigations, providing unprecedented visibility, definitive insights, and immediate answers for quick, confident response.

Capability #5: Complete Asset Inventory

You can't secure an environment that you don't understand, so having the ability to discover all assets on your organization's network and examine its attack surface from the inside out is critical—especially in industries that are highly reliant on legacy systems or burdened with a proliferation of unmanaged devices. In October 2022, the Cybersecurity and Infrastructure Security Agency (CISA) released a Binding Operational Directive 23-01, which aims to improve asset visibility and vulnerability detection on federal networks, but can (and should) apply to every industry.

As your attack surface expands to include new (and potentially unmanaged) devices—including shadow IT, internet of things (IoT) devices, BYOD, and third-party contractors or service providers—you may not be able to fully audit your security or that of your third parties. Thankfully, these challenges can be mitigated with the right NDR solution.

Automated asset discovery is crucial to having an accurate inventory of what's on a network. Best-of-breed NDR products can automatically discover new devices as soon as they communicate. Plus, these NDR solutions should also be able to auto-classify devices by their observed behavior, map dependencies, and use ML-powered detections to create accurate alerts whenever a device exhibits behavior that's anomalous to other similar devices in the environment.

[2] *Ibid.*

NDR: The Missing Link in Improving Your Security Posture

EDR and SIEM solutions will always have their place in cybersecurity, but NDR is the missing piece that offers complete visibility and context into what's actually going on inside your network. As threats evolve and become more advanced, your security posture needs to evolve alongside them. NDR eliminates blind spots by showing you what EDR and SIEM solutions can't. Just make sure your NDR solution can scale with your business. Whether you have an existing NDR solution or you're in the market for one, make sure to ask vendors the following questions:

1. **Can your NDR solution provide cloud-scale ML to protect my growing business?** Some will only offer a solution that requires more people and resources. To truly benefit the enterprise, NDR should be able to grow at scale, keep workflows simple, and all in one place.

2. **How does your solution capture packets?** An NDR provider's architecture needs to be able to store what you need when you need it. If you don't have the option to retain data beyond a few hours, or if PCAP is only turned on when there's a detection, it's not going to provide accurate information when you need to investigate or hunt threats.

3. **Can your solution streamline investigations?** It's not uncommon for cyber attacks to go undetected for weeks or months. Consequently, your NDR solution should empower analysts to respond quickly by automatically connecting related events together with enriched local context.

4. **Can your solution discover every asset connected to my network?** Hybrid and remote work are here to stay, which means unmanaged devices will continue to expose organizations to potential security risks. Thus, having an NDR solution that can account for all devicesis critical.

5. **Does your solution allow you to decrypt traffic?** Attackers attempt to be stealthy by using your own software and resources against you; these techniques are known as "living off the land." They also rely on the encryption of network protocols that happens as a default on almost all enterprise networks today. The ability to decrypt not just SSL/TLS traffic, but also MS-RPC, WinRM and SMBv3 takes away their ability to hide in the crowd.

Production-quality environments are the best proving grounds for cutting through vendors' carefully-crafted product claims. Speak to analysts, scrutinize third-party reviews, read product documentation, check out live demos, and of course, solicit your skilled team's sound judgment, formed through their extensive hands-on product experience. When you're closing in on making a decision, make sure you see exactly what your prospective NDR solution can do in real time.

About ExtraHop

ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyzes all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customer to identify suspicious behavior and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI 50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop Breaches 84% Faster. **Get Started at www.extrahop.com/freetrial**

ExtraHop

info@extrahop.com
www.extrahop.com