SPOTLIGHT

*Sponsored by: Lumu*

**Adversaries work in the dark, often bypassing conventional controls. However, when attacking a network, they often leave markers of their activities and will inevitably become visible on the network at some point.**

# What EDR Cannot See: The Critical Role of Network Detection and Response in Cybersecurity

*June 2025*

**Written by:** Chris Kissel, Research Vice President, Security and Trust Products

## Introduction

Central to a business' operations, the network is a complex organism that hosts employee productivity tools, customer experience applications, and operations such as payroll and product distribution. Rich with intellectual property, personally identifiable information, and access to goods and capital, it is also a key target for adversaries.

Business networks are heavily guarded, but their defense is becoming increasingly difficult. The first problem is that the quantity of generated and retained data is soaring. According to *Worldwide IDC Global DataSphere Forecast, 2024–2028: AI Everywhere, But Upsurge in Data Will Take Time* (IDC #US52076424, May 2024), the quantity of generated data is expected to grow by 24% from 2023 to 2028. Second, the network is expanding horizontally, often comprising a mixed estate with on-premises, cloud, Wi-Fi, mobile, SaaS, and operation technologies sharing the same architecture. Last, the network faces instability due to power surges, load balancing, integration of new applications and users, and capacity issues.

## AT A GLANCE

### KEY STAT

In IDC's June 2024 *Future Enterprise Resiliency and Spending Survey, Wave 6,* 28% of surveyed companies could use network detection and response to block a ransomware attack. In addition, 24% could block ransomware using specific analytics that measure insider threat movements.

### WHAT'S IMPORTANT

An adversary can gain entry to the business network in many ways, including malware, security controls evasion, and improper access. However, NDR can reveal activities that other cybersecurity technologies often miss.

Businesses invest care and thought into building proper defenses. Identity and access management (IAM) tools mitigate unwanted access. Perimeter defenses include web application firewalls, next-generation firewalls (NGFWs), antivirus software, and intrusion detection and prevention systems. Endpoint protection platforms ward off potential attackers, and data monitoring systems and encryption ensure files remain uncorrupted. Cybersecurity architecture is built on two principles: defense in-depth and zero trust.

Unfortunately, network security breaches are a daily occurrence. Embattled security practitioners often categorize networks into two types: "Networks that have been breached, and networks that have not been breached yet."

This Spotlight examines some of the flaws in cybersecurity tooling but does not imply that cybersecurity is hopeless. Specifically, network detection and response (NDR) not only is an important frontline detection and response capability but also illuminates gaps in other security tools' visibility, enhancing and providing necessary context to alerts that other defenses generate to indicate nefarious activities more accurately and efficiently.

## The Flaws in Cybersecurity Prevention and the Shortcomings of Tooling

Even in the most stable networks, properly applying cybersecurity controls is difficult. IDC identifies four control planes: endpoints, applications, data, and identity. Although this list does not include the network, that is the medium where these planes meet. Cybersecurity posture considers each device's ideal configuration, data, and user access default to zero trust principles, generating highly reliable detections. Practical problems can cloud perceptions about a network's safety. In detail:

- **Security tools can be bypassed.** Firewall bypass is common. Vulnerabilities CVE 2024-21762, CVE 2024-22394, CVE 2023-20198, and CVE 2024-3400 can be directly attributed to the ability to bypass next-generation firewalls. An attacker can bypass endpoint detection and response (EDR) tools by manipulating a kernel callback or kernel Event Tracing for Windows (ETW), ETW Userland, and Antimalware Scan Interface (AMSI). Unfortunately, EDR bypass kits are increasingly available on the dark market. Fileless malware, living-off-the-land binaries, and in-memory attacks routinely slip past endpoints.
- **The network is dynamic.** If businesses undergo a merger or acquisition, several devices may need to be quickly added to the network. In this case, IT and security operations (SecOps) would need to reconfigure SIEM filters, combine detection and response rules, and change routing tables, among other adaptations. External conditions, such as power surges, can change the network itself. The cumulative effect is that, even when a SecOps team believes it has properly updated an application or OS, these changes may not have been applied to the device or application, resulting in unmanaged devices.
- **Configurations are hard to manage.** Although cloud environments are secure by default, if a DevOps worker wants to return to a bucket to update an application, they may need internet access to make upgrades, exposing the closed bucket. Other configuration errors may not be addressed to account for malicious IPs/domains or malware.
- **False alerts are common, and even verified alerts have limited value.** In IDC's 2024 *AppSec Survey* and March 2024 *Web Application and Availability Protection Buyer Insights Survey*, end users cited concerns with disruptive alerts that lead to unnecessary investigations (30%), degrade end-user experience (26%), and have poor performance from core detections leading to negative alerts (27%). Alert generation can arise from several factors. Before investigating an alert, security operations must understand its context, the types of compromised assets, and the momentum an adversary can gain before an investigation begins.
- **There are too many gaps in security tooling.** The following factors can lead to security gaps: siloed data, lack of automation, poor collaboration between IT-related teams (operations, DevOps, IT, and security), lack of appropriate data from the edge, data from private and public clouds, and patches and software upgrades that devices fail to incorporate. Gaps also arise from a lack of ubiquity in code syntax or the speeds and feeds of security orchestration applications.

Security tools themselves are often the medium of an exploit. In 2024, the Salt Typhoon espionage campaign went undetected for nearly two years as attackers quietly infiltrated the core infrastructure of major U.S. telecom providers (AT&T and T-Mobile), exposing the limits of traditional security tools in identifying stealthy threats. Cybersecurity is a tough game, because the adversary can get through, bypass, or embed itself onto a cybersecurity platform, agent, or scanning mechanism.

However, there is reason for hope. The network is the common ground for all threats, making it ideal for detection and response. Adversaries can hide on endpoints, but their actions generate traffic patterns and anomalies. Network-level visibility closes gaps EDRs miss and adds critical depth to detection. NetFlow is a protocol that provides an immutable forensic trail, logging and creating a time stamp of how machines have ingress/egress to the internet, which applications were accessed, and the sequence of events leading to a vulnerability. Proper network monitoring can lead to indicators of compromise (IoCs), which become invaluable in threat detection.

## How the Network Influences Detections and Responses

NDR involves two simple but nuanced premises. First, increasing the capability of any of its three elements (network, detection, and response) enhances the overall platform. For instance, a security vendor can elevate the platform's quality if it can recognize an EDR bypass other vendors might miss. Second, NDR outcomes should be greater than the sum of their three parts. The network gives various signals, but a central platform should correlate alerts or other IoCs to minimize the security analyst's effort in triage; collate artifacts that describe the alert/threat in precise terms; lead to a single version of truth; trigger remediation, including ephemeral response and threat hunting; and ultimately return the network to a state of innocence.

Ideally, NDR outcomes should be greater than the sum of their three parts.

NDR can provide detections of very high quality. For instance, beaconing involves a specific signal that is transmitted or received (Tx/Rx) in a regular cadence that looks like a machine-oriented activity. A device located in Boston that transmits a signal involving a router in Barcelona indicates impossible travel and is likely an IoC. If a security team looks at a passive domain name server (DNS) log with a domain that is not on a known goodlist, it will require further investigation. More than 65,000 ports are available in network communication, and the use of a new port is a solid IoC. Last, if rules moderating activity about which users have access to specific servers or applications are broken, this is a high-quality incident worth investigating.

The ability to respond to security incidents is as important as detecting them in the first place. IDC believes that response should be both ephemeral and permanent. For instance, in the DNS example, once a domain is determined suspicious, antivirus, web/email defenses, and firewalls should all be updated, at speed, to block access to it (ephemeral response). After further examination, the domain can be goodlisted. However, if a device has accessed the suspicious domain, NDR metadata can help determine if the device has incurred further damage. Remediation then occurs, which may involve a patch or a machine reimaging to repair any damage (permanent response).

When considering NDR options, it is important to ensure the vendor has strong foundational capabilities (port anomaly detection, anomaly detection, threat intel correlation, and AI-driven detection of threats, tactics, and procedures [TTPs]) and can expand its detections and responses to include operational technology (OT), Internet of Things (IoT), virtual machines, and public cloud. Another desirable capability is a security analytical engine that reduces noise and includes

specific analytics dedicated to use cases such as security tools bypass, malware, phishing, and command and control (C&C) activities.

## Considering Lumu for Network Detection and Response

Lumu addresses important components of cybersecurity shortcomings. In addition to fundamental NDR capabilities, such as the ability to check port anomalies and unusual domain access, Lumu has built analytics to establish baseline user behavior and to look for IoCs such as security controls bypasses, malware families, and ransomware. Lumu states its NDR currently helps protect over 3 million endpoints.

### Lumu's Capabilities

Any given cybersecurity technology can find IoCs. However, key differentiators to look for include the ability to provide the security analyst with meaningful context, to extract signal from noise, and to contextualize artifacts for incident detection and response in real time. The following capabilities differentiate Lumu:

- **Comprehensive ingestion of telemetry sources.** Lumu collects conventional NetFlow logs from Windows and Linux machines, but it can also ingest OT logs such as SCADA, endpoint logs, firewall logs, DNS logs, logs from virtual machines, and public cloud logs for heterogeneous network visibility. Lumu customers can consolidate the network's principles into one platform.

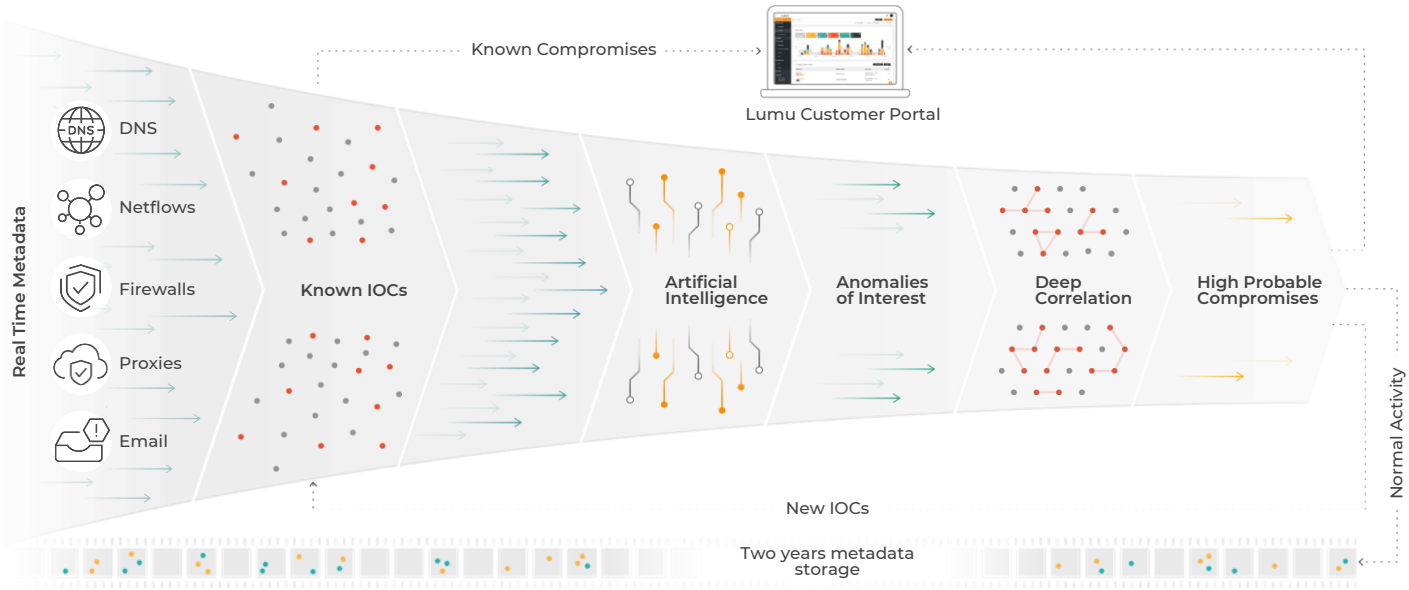
  Lumu brings discipline to telemetry collection. First, it offers a labeling wizard with which an ITSecOps team can group similar assets and assign business values to more critical assets. Second, it retains metadata for two years; if forensic details are ever needed, the labeling helps in investigations. Third, the Lumu dashboard tracks attack information by the total number of queries and the type of adversarial activity, such as malware, phishing, C&C, and network scans. Last, Lumu tracks IoCs through the MITRE ATT&CK framework.

  Lumu is designed for security operations with dashboards that monitor malware, phishing, C&C, and network scan events.

- **Reduction of noise in security operations.** Lumu's method of ingesting and managing telemetry is necessary for security operations workflow optimization. Figure 1 shows the collection process for various forms of telemetry. A natural first step is to apply AI to look for duplicate alerts (an EDR, a firewall, and an antivirus may detect the same thing); the next might be to compare time stamps and signatures from these devices.

  Lumu's labeling wizard helps with the next steps in analytics. An alert might show that an adversary has traversed several groups in a lateral movement. The system helps determine an asset's sensitivity and pushes the queue toward better prioritization. Deep correlation considers the likelihood of a breachable incident, a significant blast surface, or potential damage from exploited vulnerabilities to a valuable asset, such as a web/mail server, a financial server, or a DNS resolver.

FIGURE 1: ***Lumu Illumination Process***




*Source: Lumu, 2025*

Lumu works best as a collaborator rather than the sole determinant of detection and response. It adds resiliency and redundancy to a cybersecurity stack. While EDR bypass is not uncommon, EDR remains a strong detection technology. If an IoC is discovered in a server in an array, Lumu can take it from EDR and use it to initiate investigations on similar servers, either by geography, OS, or function. Bidirectional inputs from NGFW, IAM, web/email servers, and other telemetry sources can provide the necessary context to reduce the blast surface and conduct proper mitigation and remediation.

Lumu is designed for security operations with dashboards that monitor malware, phishing, C&C, and network scan events. Like other NDR vendors, Lumu sensors are placed onto SPAN ports, so they require little configuration. Lumu Autopilot creates detections when no analyst is on duty. Lumu creates a customized heatmap that shows the distribution of activities by days of the week. Last, a crucial part of the incident dashboard is the automated response that Lumu Defender suggests.

Security tools often require configuration, but Lumu is easy to install and has 217 out-of-the-box integrations to complement existing security stacks. Its use of labels helps establish which assets are critical and can detect if end users attempt unwanted access. Finally, Lumu can create visualizations that help security analysts, from novices to experts, detect and mitigate known and unknown threats.

The pricing options offered by Lumu make it a viable option for small and midsize businesses (SMBs), and it offers a freemium trial solution. The company also includes free reporting and training with the licensing of a platform.

### Challenges

In the past several years, security practitioners have recognized NDR's status as a valuable observability fabric that unifies control planes, and Lumu competes with NDR vendors with larger install bases. Some of these vendors may be able to offer discounts if a client wishes to bundle other services, such as web/email security or endpoint protection/detection.

However, a second challenge may provide an opportunity for Lumu. NDR is considered both complex and expensive. Enterprises deploying it often pay for it in an ingestion model. NDR use cases include large on-premises estates as well as heterogeneous networks. However, SMBs usually do not consider NDR for additional visibility. Lumu's per-asset pricing model extends the benefits of NDR to SMBs.

## Conclusion

NDR is an essential detection and response technology. An NDR platform provides the continuous visibility necessary for heterogeneous networks and occasions when endpoint agents fail. NDR can also integrate metadata from appliances such as NGFWs, EDR, IAM, OT/IoT logs, and public clouds for additional context, leading to alerts prioritization and threat hunting for a single version of truth.

Lumu has refined this promising technology. Its security analytics reduce a network's noise and lead to a single version of truth. To the extent that Lumu can address the challenges described in this paper, the company has a significant opportunity for success in the NDR market.

# About the Analyst

***Chris Kissel,*** *Research Vice President, Security and Trust Products*

Chris Kissel is a research vice president in IDC's Security and Trust Products group, responsible for cybersecurity technology analysis, emerging trends, and market share and forecast reporting. Mr. Kissel's primary research area is security operations and AI security analytics. The major technology groups within this practice are SOAR; firewall automation; network detection and response (NDR); threat detection and investigation, and response (TDIR); threat intelligence; and cloud-native XDR.

## MESSAGE FROM THE SPONSOR

Lumu is a cybersecurity company that helps organizations operate cybersecurity proficiently by measuring and responding to confirmed compromise in real time. Through its Continuous Compromise Assessment model, Lumu illuminates blind spots across network infrastructure, user devices, cloud environments, and remote connections—offering unmatched visibility into active threats. Designed to integrate seamlessly with existing cybersecurity stacks, Lumu enables automated threat response and reduces time to containment. Organizations of all sizes—from mid-market to enterprise—leverage Lumu to strengthen their security operations and make evidence-based decisions. Learn more at http://www.lumu.io/.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

**IDC Research, Inc.**
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com