WHITE PAPER

5 Reasons EDR is not Enough

Why EDR Needs NDR

VECTRA®

Endpoint Detection and Response (EDR) remains a foundational necessity in enterprise cybersecurity

However, the rapid evolution of attacker tradecraft — including advanced evasion techniques, exploitation of unmanaged devices, and identity abuse — has revealed inherent limitations in host-centric security controls. This whitepaper examines these limitations in detail, drawing from incident response investigations, red team exercises, industry statistics, and customer case studies. It highlights why EDR cannot stand alone in protecting modern hybrid environments, and why modern SOCs must extend visibility across the network and identity layers using NDR (Network Detection and Response).

5 reasons why EDR is not enough and why every EDR needs NDR

1. EDR agents cannot be deployed everywhere
2. EDR is being bypassed, evaded, and disabled
3. EDR Visibility Misses Network and Identity Attack Paths
4. NDR Reduces Alert Fatigue, Missed Detections, and False Positives
5. NDR Delivers on the Promise of SOC Visibility, Efficiency, Efficacy

Reason 1:

EDR agents cannot be deployed everywhere

Endpoint protection platforms (EPP) and endpoint detection and response (EDR) rely on agents, which means anything without an agent is invisible to the tool.

In today's networks, many devices cannot or will not run an agent — examples include IoT devices (smart printers, HVAC sensors, medical equipment), unmanaged personal laptops or phones, network appliances, routers, and even cloud workloads. Attackers know this and purposefully target said devices. If an infected unmanaged device starts scanning your network or a compromised contractor laptop begins beaconing out, your endpoint solution likely won't notice.

1 CISA Alert Code AA24-326A titled "Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a US Critical Infrastructure Sector Organization" released in November 2024 found that

> "the assessed organization had insufficient technical controls to prevent and detect malicious activity - The organization relied too heavily on host-based endpoint detection and response (EDR) solutions and did not implement sufficient network layer protections."

2 Vectra AI network data telemetry shows up to

50%

do not have an EDR agent on them

or include devices that an agent cannot be installed on.

3 From 2023 to 2024, malware attacks on IoT/OT devices increased

↑45%-66%

or attacks are aimed at network routers

Zscaler ThreatLabz 2024 Mobile, IoT and OT Threat Report

4 More than

+50% of IoT/OT devices

are dependent on legacy, end-of-life operating systems with known vulnerbilities, high-risk legacy protocols and services

making up more than

+20%

of internal East-West network connections.

Zscaler ThreatLabz 2024 Mobile, IoT and OT Threat Report

5 Without agentless monitoring such as **NDR**

unmanaged endpoints and non-traditional devices form unmonitored corridors for attacker movement.

Case Study: Kintetsu Department Store

Facing gaps from POS systems, specialized terminals, and handheld devices lacking EDR support, Kintetsu deployed Vectra AI's NDR for agentless monitoring. Within the first month, suspicious hosts were detected that EDR would have missed.

Even when agents are deployed, attackers are finding ways to bypass them entirely – as we'll explore next.

Reason 2:

EDR is being bypassed, evaded, and/or disabled

Endpoint defenses operate on the premise of keeping attackers out, but endpoint controls can be intentionally blinded, making out-of-band detection via network and identity telemetry essential.

Team exercise observed EDR was bypassed via binary padding and by avoiding 'known-bad' signatures. As a result, the identity-focused attacks went entirely undetected.

Multiple, validated EDR bypass methods have been observed in active incidents, often shared in underground forums and sold as subscription-based tools including but not limited to:

Retrosigned Driver Bypass	Ransomware actors load malicious kernel drivers signed with expired certificates by altering system time, then terminate EDR processes.
Mounted Guest EDR Bypass	Threat actors mount VM disk images from a hypervisor, delete EDR files offline, then reboot guests unprotected.
Bring Your Own Installer	Attackers interrupt EDR agent upgrade processes to leave endpoints unprotected, bypassing anti-tamper controls.
EDR Hook Removal Tools	Commercially available EDR evasion tools used in ransomware-as-a-service kits routinely remove EDR hooks and blind agents, enabling stealthy credential theft.

EDR can be intentionally blinded, making out-of-band detection via network and identity telemetry essential. NDR assumes compromise — it works with the mindset that attackers are already operating on the network. By embracing the reality that endpoint prevention is never 100% foolproof, NDR provides a crucial post-compromise safety net for the SOC.

Case Study: Abdul Latif Jameel (ALJ)

Abdul Latif Jameel (ALJ) is a global conglomerate spanning automotive, real estate, and financial services with operations in 35 countries, required broad threat visibility across diverse networks. Traditional endpoint detection left large blind spots across ALJ's global IT footprint. Vectra AI's agentless NDR expanded visibility to network devices, identity, and cloud components—not just endpoint telemetry. Resulting in comprehensive coverage achieved outside of agent-based monitoring; Rapid detection of attacker behaviors that would have bypassed EDR; 90% reduction in false positive alerts, improving analyst focus.

And it's not just evasion at the endpoint that's the problem. Attackers are moving across the network and abusing identities in ways EDR simply can't see.

Reason 3:

EDR's host-centric visibility misses network and identity attacks

EDR focuses on what happens on an endpoint, but cannot fully monitor activity crossing between systems (East-West), occurring in cloud environments (North-South), or happening entirely in the identity layer.

1 Vectra Gap Analysis found attackers evade EDR by

embedding C2 inside already-encrypted SSL channels,

using aged domains to bypass URL filtering, exploiting identity mechanisms such as Kerberos unconstrained delegation.

2 CISA's red-team assessments revealed that EDR excels at device-level detection but

> "struggles with network-wide attacks"

leaving

> "gaps when hackers exploit lateral movement or unusual data transfers—activities that often require network-level visibility to detect."

3 CISA Red Team's SILENTSHIELD found during simulations,

adversaries pivoted freely across servers,

ultimately achieving domain compromise

Defenders only gained full situational awareness by analyzing network logs and internal traffic,

not just endpoint detections.

These sources drive home a clear fact: EDR sees individual hosts—it cannot track stealthy lateral activity slipping across internal network paths. That blind spot makes NDR—which analyzes inter-host traffic—essential to detecting, understanding, and stopping lateral propagation.

Case Study: Schaefer Kalk

A ransomware intrusion bypassed the company's EDR completely. Vectra AI's network (NDR) and identity threat detection and response (ITDR) behavior-based AI detected suspicious network and identity activity, enabling intervention before encryption.

Without visibility into lateral movement and identity misuse, security teams are left responding blindly. Worse, they're often overwhelmed by noisy, low-value alerts that bury real threats.

Reason 4:

NDR reduces alert fatigue, missed detections, and false positives

Security operations centers (SOCs) are drowning in noise.

On average, analysts face nearly 4,000 alerts every day, yet can realistically review less than half, leaving countless potential threats unexamined. The vast majority of these alerts are false positives — with research showing that less than 1% are actionable — forcing analysts to spend hours triaging meaningless signals instead of focusing on real attacks. This constant flood of low-value alerts fuels alert fatigue erodes confidence in detection tools, and leaves SOC practitioners worried each week that a critical threat will be missed.

1 Security teams receive an average **3,832 alerts per day**

SOC analysts can only review 38% of them, leaving the majority unaddressed

Vectra AI 2024 State of Threat Detection and Response Report

2 "Managing alerts" consumes nearly

3 hours per day per analyst

over 27% of their workday

and SOC teams spend

9.6 hours per day on tasks that could be automated

Vectra AI 2024 SOC Efficiency Report

3 Analysis of 1.1M behavioral signals from Vectra MDR/ MXDR customers showed that fewer than

<300 (0.02%) were confirmed malicious,

meaning

99.98%

of detections were noise filtered before reaching analysts

Vectra AI 2025 Research Brief: Reducing Noise, Elevating Threats: A Data-Driven Look at SOC Efficiency

4 For 1.73M detections, only

0.53% were prioritized for action

an average of <70 entities per month per customer

underscoring the scale of non-actionable alerts

Vectra AI 2025 Research Brief: Reducing Noise, Elevating Threats: A Data-Driven Look at SOC Efficiency

5 **71% of SOC practioners**

worry every week that a real attack is buried in the flood of alerts, and

62% believe vendors flood them with pointless alerts

to avoid responsibility for breaches

Vectra AI 2024 State of Threat Detection and Response Report

Case Study: Globe Telecom

Globe Telecom faced visibility gaps across its infrastructure, limiting its ability to detect threats that evaded traditional EDR tools. With Vectra AI's NDR platform and managed detection services, the security team gained real-time visibility across their network environment—including identity and cloud layers resulting in: Reduced alert noise by 99%, enabling security analysts to focus only on high-fidelity alerts; Improved incident response times by 78%, sharply accelerating detection and containment; cut escalation workload by 96%, significantly easing analyst burden while maintaining coverage for services used by 80 million customers.

Cutting through the noise is critical but so is seeing the full picture. That's where NDR completes the equation – delivering the broad visibility and depth of signal every SOC needs.

Reason 5:

NDR delivers on the promise of SOC visibility, efficiency, efficacy

SOC Visibility Triad

One useful way to understand NDR's importance is through Gartner's concept of the SOC Visibility Triad. Gartner® analysts have advised that to achieve comprehensive threat visibility, organizations should employ three primary detection technologies in concert:

1

SIEM / log management

for analyzing event logs and correlating alerts from across systems.

2

Endpoint Detection & Response (EDR)

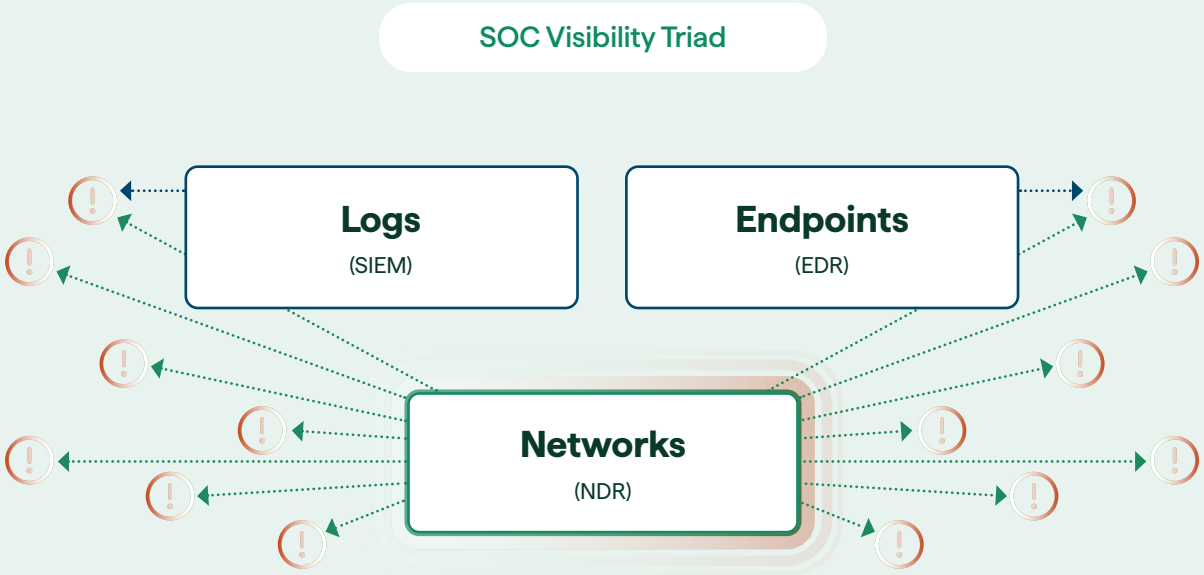
for monitoring and containing malicious activity on endpoints (workstations, servers, mobile devices).

3

Network Detection & Response (NDR)

for monitoring network traffic and uncovering threats that manifest in communications between devices.

Each pillar of this triad covers a different dimension of the environment, and together they significantly enhance a SOC's ability to detect and respond to attacks. The idea is that relying on only one or two of these will leave gaps. For example, EDR might miss what happens on the network or on unmanaged devices, while log analysis alone might not provide full visibility into live traffic. But when all three are deployed, the overlap provides defense-in-depth and cross-validation of threats — both false negatives and false positives can be minimized through their combined signals and context.



Organizations need visibility into logs (SIEM), endpoints (EDR), and networks (NDR) for comprehensive security coverage. NDR, as the network-focused pillar, catches threats evident in network traffic that other pillars cannot see.

Notably, in this triad, NDR is the component responsible for the ground truth of network activity. Network packets don't lie — if a device is communicating with an external server or with another internal host, that activity will traverse the network and can be observed because virtually all malicious operations generate network packets. Attackers may be able to erase logs on an endpoint or avoid writing files to disk (to evade antivirus), but they cannot carry out an intrusion without sending packets. By collecting those packets (or their metadata) and analyzing them, NDR provides a source of evidence that often makes it harder for attackers to cover their tracks. Additionally, attackers are often unaware that an organization is silently and covertly monitoring network traffic, so they cannot take evasive action to avoid detection on the network making NDR a powerful and essential component to any security stack.

Industry validation of the importance of NDR has been strong. The publication of the first-ever Gartner® Magic Quadrant for NDR™ indicates a maturing market, validated by other analyst firms (IDC, GigaOm, Forrester) echoing its significance. Leading voices agree that NDR is no longer a nice-to-have — it's essential for keeping pace with today's attacks. Security organizations and managed security service providers (MSSPs) building out their SOC capabilities are increasingly including NDR alongside SIEM and EDR deployments to close the gaps in visibility and catch advanced threats that would otherwise lurk undetected.

NICE framework

The NICE framework — Network, Identity, Cloud, and Endpoint — introduced at the Gartner Security & Risk Management conference in May 2025 is a model for unifying the critical telemetry domains required for effective threat detection, investigation, and response.

By integrating visibility and analytics across these four pillars, SOC teams can correlate independent signals, confirm compromises faster, and reduce false positives. Modern NDR is uniquely positioned in this model: it delivers deep native coverage for network, identity, and cloud domains while seamlessly integrating with endpoint tools to complete the picture. This unified approach allows SOC teams to detect malicious activity across managed, unmanaged, on-premises, and cloud-connected assets, and to orchestrate rapid, automated responses across the entire attack surface and spanning the entire cyber kill chain.

How modern NDR platforms align to the NICE framework

N

Network

Continuously analyzing network packets and metadata to identify behaviors such as command-and-control (C2) communications, lateral movement, and data exfiltration, even in encrypted traffic, and providing high-fidelity signal and rich context indicative of attacker behaviors on the network.

I

Identity

Detecting stolen credential use, suspicious authentication patterns, and privilege escalation attempts, mapping activity to identity context to enforce Zero Trust policies and stop account-based attacks early.

C

Cloud

Monitoring control plane events, API calls, workload behaviors, and SaaS application logs to detect risky access, malicious automation, and unauthorized data movement across AWS, Azure, and GCP.

E

Endpoint

Integrating with EDR/EPP platforms to correlate endpoint alerts with network, identity, and cloud activity, enhancing detection when agents are absent or bypassed, surfacing threats on unmanaged or IoT/OT devices, and enabling automated host containment via API or SOAR integrations.

By unifying telemetry from all four NICE domains, modern NDR platforms empower SOC teams to detect, investigate, and respond with greater speed and precision. This cross-domain correlation enables attack confirmation by stitching together multiple, independent signals or indicators of attack (IoA) — significantly reducing false positives and accelerating mean time to investigate and respond (MTTR).

NDR complements EDR through seamless integration

EDR plays a vital role in catching device-level threats, but attackers don't stop at the endpoint — and neither should detection. By integrating EDR with NDR, security teams close the visibility gap and transform disconnected alerts into coordinated, high-fidelity detections.

Here's how the two work better together:

1. **Correlate endpoint signals with network, identity, and cloud telemetry.** NDR adds context to EDR detections, confirming if an alert on the host is tied to:
   - Suspicious east-west movement
   - Privilege escalation or unusual authentication activity
   - Malicious cloud API behavior or data exfiltration
2. **Elevate weak signals into confirmed attacks.** On their own, EDR detections may lack enough context to trigger response. NDR connects low-confidence alerts with related behaviors to confirm compromise.
3. **Extend response beyond the endpoint.** When NDR spots attacker behavior (even on unmanaged or agentless devices), it can:
   - Trigger host isolation
   - Disable user accounts
   - Enrich EDR alerts with network-level evidence for faster triage
4. **Give analysts a single, connected view.** Integrated detections reduce manual effort, shorten investigation time, and improve SOC efficiency by:
   - Reducing tool sprawl and console-switching
   - Delivering richer detections with pre-correlated data
   - Enabling faster decisions from better context

Vectra AI's NDR platform integrates seamlessly with leading EDR vendors to support these workflows out of the box, including: CrowdStrike, SentinelOne, Microsoft Defender, and others.

Together, EDR and NDR form a unified detection and response layer — one that sees what's happening on the endpoint and across everything connected to it.

Together, EDR and NDR form a unified detection and response layer — one that sees what's happening on the endpoint and across everything connected to it.

Conclusion:

Modern attack resilience requires NDR

The reality is clear: EDR alone cannot deliver the coverage, clarity, and control required to defend today's complex hybrid environments and build resilience for modern attacks.

Modern attackers exploit unmanaged devices, bypass endpoint controls, and abuse identities in ways host-centric tools simply cannot see. Network Detection and Response (NDR) closes these blind spots by continuously monitoring the ground truth of network, identity, and cloud activity, reducing noise, and surfacing only the most critical threats with context. For security leaders, investing in NDR is not optional — it is the essential complement to EDR that transforms the SOC from reactive and overwhelmed to proactive, efficient, and resilient. By prioritizing NDR today, organizations ensure they can detect what matters, respond faster, and stay ahead of the adversary.

VECTRA

About Vectra AI

Vectra AI, Inc. is the cybersecurity AI company that protects modern networks from modern attacks. When modern cyber attackers bypass existing controls, evade detection and gain access to customers' data center, campus, remote work, identity, cloud, and IoT/OT environments, the Vectra AI Platform sees their every move, connects the dots in real-time, and stops them from becoming breaches. With 35 patents in AI security and the most vendor references in MITRE D3FEND, organizations worldwide rely on Vectra AI to see and stop attacks their other tools can't. For more information, visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai