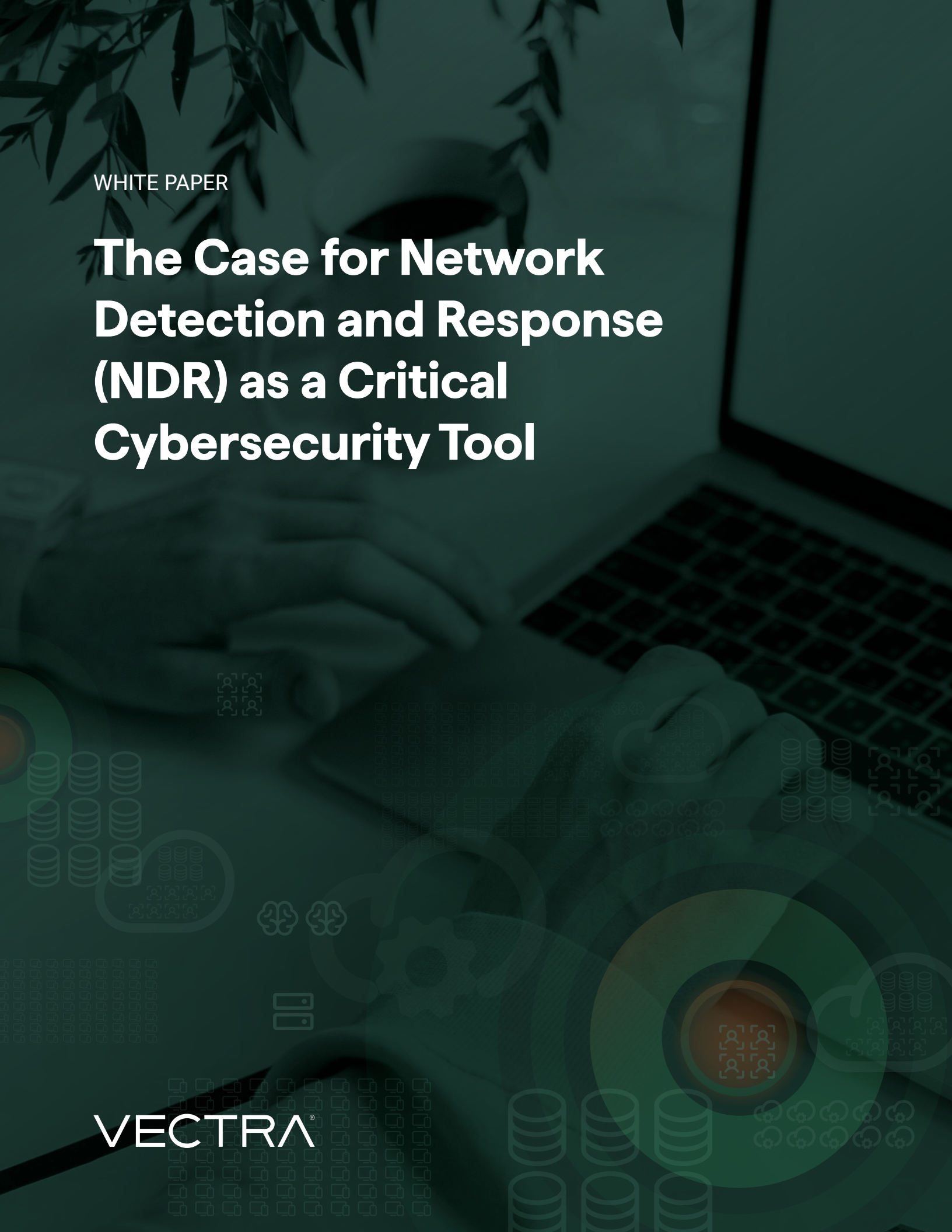


WHITE PAPER

The Case for Network Detection and Response (NDR) as a Critical Cybersecurity Tool

VECTRA®

Cyber-attackers constantly evolve to be more efficient and effective in how they execute their campaigns.

They have learned to evade traditional defenses, employ tactics like social engineering, fileless malware, and living-off-the-land techniques to slip past firewalls, intrusion detection systems (IDS) and prevention, and endpoint controls. Like attackers, organizations' network environments have evolved to operate across hybrid cloud infrastructures, support remote workforces, and include countless unmanaged IoT and OT devices. The evolution of the modern hybrid network has expanded the attack surface and enlarged visibility gaps that give modern attackers an unfair advantage post-compromise.

Hybrid networks, hybrid attacks

This whitepaper argues that network detection and response (NDR) is no longer optional but essential for SOC teams tasked with defending the modern network from modern attacks. This paper answers the fundamental questions security leaders, builders and operators have when it comes to investing in NDR:

- **Why NDR is a critical component for the SOC**
- **When NDR is needed as a SOC line of defense**
- **How NDR addresses an evolving threat landscape**
- **Where NDR fits in SOC architectures and frameworks**
- **What value outcomes does NDR deliver the SOC**

Table of Contents

Why NDR is a critical component for the SOC

Market drivers fueling NDR adoption

The rise of Network Detection and Response platforms is driven by macro forces reshaping enterprise IT and security operations. These drivers reflect both escalating threats and evolving requirements for security teams:

1 **Hybrid network complexity**

Organizations now operate across on-premises data centers, IaaS environments, SaaS platforms, operational technology (OT), and remote work setups. Attackers exploit this complexity to move undetected across segments. NDR provides the lateral visibility needed to monitor interactions across the full hybrid attack surface.

2 **Identity as the new perimeter**

Cloud-first architectures have made identity — not endpoints — the control plane of choice for attackers. Privilege escalation, token theft, and lateral movement via federated identity are common tactics. NDR platforms with identity-layer detections expose credential misuse and privilege abuse even when attackers avoid traditional endpoint tools.

3 **Signal clarity amid alert overload**

SOC teams are overwhelmed by alert volume. According to Vectra AI's 2024 State of Threat Detection and Response: The Defenders' Dilemma report, security professionals receive an average of 3,832 alerts per day but only review 38% of them. Of those, just 16% are deemed real attacks. Security leaders now demand high-fidelity detection platforms that reduce alert fatigue, accelerate triage, and elevate only the most relevant threats for analyst review.

4 **Operational technology (OT) risk expansion**

The continued alignment of IT and OT networks introduces unmanaged and often unmonitored assets into the security ecosystem. Attackers increasingly target OT environments due to inconsistent visibility. NDR platforms extend detection into these operational domains without creating operational impact, not relying on agents, and addressing a critical and growing exposure point.

5

Enterprise adoption of generative AI and associated risks

As business units rapidly deploy generative AI (GenAI) technologies security teams face new risks: data leakage, abuse of GenAI models for reconnaissance, and a lack of visibility into user behavior. NDR products capable of detecting GenAI-specific behaviors — such as model abuse or suspicious access — are becoming essential to protect intellectual property and ensure safe AI use.

6

Regulatory pressures and sovereignty requirements

Governments and industry regulators continue to introduce new mandates around data residency, sovereignty, and privacy. In sectors such as critical infrastructure, public services, and finance, air-gapped or appliance-based solutions are often mandated. NDR platforms that support on-premises and sovereign deployments — without sacrificing detection capability — are increasingly valued by compliance-conscious organizations.

These drivers are not speculative — they reflect the present-day realities of security operations.

As hybrid networks continue to evolve and adversaries adopt stealthier, multi-domain tactics, NDR has become a core pillar of the modern detection and response strategy.

The truth is in the packet

Industry experts and analysts now regard NDR as a must-have component of modern security operation centers (SOC).

This is because a more comprehensive approach is needed to monitor what is happening on the network itself — the truth is in the packet — and this is where NDR comes in. NDR is essential for complete situational awareness across an enterprise's digital environment. It focuses on monitoring and analyzing network traffic — both on-premises and in the cloud — to detect and respond to malicious activities in real time. Instead of looking only at endpoint data or logs, NDR directly inspects the packets, flows, and communications traversing an organization's networks spanning on-premises data centers, cloud, and remote locations. By doing so, it provides a layer of visibility and context that endpoint or log-based tools miss.

An NDR platform continuously captures network traffic and uses advanced analytics (often AI/ML-based) to identify patterns or indicators of attack (IoA). It analyzes network behavior for each device, user, and application — not just simple signatures — but to understand what is security relevant and distinguish malicious from benign. This behavior-centric approach allows modern NDR platforms to catch threats that traditional methods might miss, providing visibility and context beyond what EDR, EPP, IDS, and network firewall tools provide.

Critical capabilities of modern NDR

NDR platforms come with a rich feature set designed for effective post-compromise detection and response:

AI/ML behavioral analytics

NDR leverages AI/ML algorithms and statistical models to detect attacker behaviors without predefined signatures. It can learn the typical patterns of network usage (e.g., what normal DNS query volume for a workstation looks like) and surface outliers. This is how NDR identifies threats like data exfiltration via DNS tunneling or insider abuse — by recognizing behaviors that fall outside normal bounds. Over time, these models refine themselves to improve accuracy and reduce false positives

Detection of unknown threats

Because of its behavior-based analytics, the NDR platform is adept at catching stealthy attackers living off the land. It does not require that the threat be previously seen or catalogued in threat intelligence feeds. By focusing on abnormal behaviors (e.g. a device executing a never-before-seen protocol sequence, or a spike in external connections after hours), NDR provides a proactive way to spot emerging threats before they are publicly known. This non-signature approach is crucial for identifying new, unknown threats that traditional signature-based can't detect.

East–west traffic monitoring

Unlike many security tools, like firewalls or secure web gateways, that concentrate on north–south traffic (in/out of the perimeter), NDR also inspects east–west traffic — the internal communications between systems. Once attackers get presence internally, only vigilant monitoring of east–west network flows can reveal their presence. For example, when a modern attacker like Scattered Spider compromises an account (human or machine) and begins to move laterally inside the network, NDR will track the attacker's movement across the hybrid network (data center, cloud, SaaS) that is often invisible to endpoint, IDS/IPS, firewalls and signature-based tools

IoT and unmanaged device visibility

NDR provides visibility for devices that lack an endpoint agent. By analyzing all network communications, NDR can identify when an IoT sensor or other unmanaged devices behave oddly. In addition, NDR platforms are used to discover unknown devices on the network — for instance, detecting a rogue wireless access point or an employee's shadow IT system communicating on the network. Many security teams struggle with IoT and BYOD visibility, but NDR fills that gap by flagging abnormal communication patterns from any device, managed or not.

Encrypted traffic analysis

With the majority of network traffic now encrypted, attackers frequently abuse encryption to hide malicious data flows (like C2 communications or data exfiltration). NDR products tackle this challenge in a few ways. Some NDR tools can perform selective TLS decryption or use certificate inspection to examine suspicious encrypted streams. Vectra AI analyzes metadata and behavior of encrypted sessions (such as packet timing, sizes, and sequence patterns) to infer malicious activity without decrypting content. For example, an NDR might detect a malware beacon within HTTPS traffic by its unusual periodic timing or by recognizing an anomalous TLS handshake. In any case, NDR adds crucial capabilities to shine a light on threats in encrypted traffic, whereas many traditional tools would be blind once data is encrypted.

Incident investigation & response

Beyond detection, NDR platforms provide tools for analysts to investigate and respond to incidents. They often record rich metadata (and sometimes full packet captures) which can be searched to trace an attacker's actions step-by-step. NDR alerts come with context — showing the sequence of events, related connections, and affected hosts surrounding a detected threat, which accelerates incident response. Many NDR products also integrate with response workflows, where they can trigger automated actions or send data to other systems. For example, upon detecting a confirmed threat, an NDR might automatically communicate with a firewall to block the offending IP address or send an alert to a security orchestration, automation, and response (SOAR) platform to execute a containment playbook. In summary, NDR not only spots threats but helps security teams understand what happened in detail and act on them quickly.

In essence, modern NDR platforms provide a network + identity-centric approach to attack detection and response that complements endpoint approaches. In essence, NDR acts as an ever-vigilant "neighborhood watch" over the places endpoint tools can't.

When NDR is needed as a SOC line of defense

Traditional security controls, while foundational and necessary, have well-known limitations in detecting and stopping the kinds of attacks described above. Understanding these gaps helps illustrate when NDR provides unique value:

When endpoint controls get bypassed

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

1. **Retrosigned Driver Bypass**
   Ransomware actors load malicious kernel drivers signed with expired certificates by altering system time, then terminate EDR processes.

2. **Mounted Guest EDR Bypass**
   Threat actors mount VM disk images from a hypervisor, delete EDR files offline, then reboot guests unprotected.

3. **Bring Your Own Installer**
   Attackers interrupt EDR agent upgrade processes to leave endpoints unprotected, bypassing anti-tamper controls.

4. **EDR Hook Removal Tools**
   Underground tools like disabler.exe remove EDR hooks in user-mode libraries and kernel callbacks, enabling stealthy credential theft.

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 defense-in-depth — a crucial post-compromise safety net for the SOC.

When endpoint coverage is limited (Unmanaged devices, IoT/OT)

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 won't notice — but NDR would see and alert on the network activity.

When alert noise is high

SIEMs and log management systems ingest huge volumes of event data from various sources. They often generate floods of alerts, many of which are benign or low priority, contributing to alert fatigue. The signal-to-noise ratio can be poor, meaning true incidents get missed in the noise. Without expert tuning and ample analyst time, purely log-based detection will likely miss subtle correlations that indicate a stealth attack. NDR tools leverage machine learning to understand network activity, highlighting behavioral deviations (e.g. a device suddenly sending an unusual volume of data externally at 3 AM) rather than alerting on every anomaly or indicator of potential threat. NDRs focus on analyzing live network flows and metadata, flag behaviors indicative of an attacker, and attribute entities (host or accounts), which produces more integrated and accurate alerts.

When overdependent on signature-based detection

Many legacy defenses (firewalls, anti-virus, intrusion detection systems) primarily match threats to known malicious signatures, domain blacklists, or threat intelligence reports. This approach fails against novel, unknown attacks or adversaries using and abusing legitimate credentials and tools. As described earlier, APT actors might use standard IT administration software or newly registered domains for C2 — things a signature-based system can't flag. In some real-world breach cases, gigabytes, sometimes terabytes of data were quietly exfiltrated over a period while attacker communication went undetected because the tools used were common admin programs (a tactic known as living off the land). The organization's traditional defenses did not recognize the activity as malicious. However, customers with NDR in place detected behavioral IOAs in network activity that revealed the ongoing data theft. This example highlights how NDR's AI-driven behavior-based monitoring can catch slow, stealthy attacks that evade signature-based tools.

In summary, when other tools miss — NDR sees and alerts.

The network is the one common denominator because even the stealthiest adversary leaves a trace (e.g. a connection, a data transfer, a protocol misuse) and NDR becomes the source of truth.

How NDR addresses an evolving threat landscape

Digital infrastructure is transforming at a relentless pace. Organizations now operate in hybrid, multi-cloud environments where data flows through on-premises data centers, cloud workloads, SaaS applications, remote locations, and IoT/OT environments.

Simultaneously, the nature of attacks constantly evolves — and with it — new attack methods emerge. Modern attackers rely on more than malware or hardware/software vulnerabilities to get in. They create their own way in by compromising an account whether that account is human or machine. Once they are in and on the network, they blend in with legitimate traffic, live-off-the-land, move laterally, escalate privileges, and pivot to crown jewel services whether on-premises or cloud hosted.

Compounding the challenge is the expanding attack surface of today's hybrid enterprises. The shift to cloud services and remote work means more traffic traverses public networks and locations outside the traditional perimeter. Employees, partners, third-party contractors connect from personal or unmanaged devices that many times are not fully secured. The boom in IoT devices — from smart sensors in factories to medical IoT in hospitals — introduces a legion of network-connected devices that often lack built-in security controls. Many security teams have little visibility into these unmanaged devices, which can become easy footholds for attackers. In short, organizations are facing more entry points and more ways for threats to hide within their networks. Below are a few modern attack examples:

1

Scattered Spider: Identity Abuse and Cloud Pivot

What happened

Scattered Spider used SMS phishing and SIM swapping to steal credentials, then logged into Microsoft Entra ID (Azure AD) and pivoted into M365 and Azure workloads. Attackers modified mailboxes, created backdoor trust relationships, and moved laterally across the cloud environment.

Why it was missed

Because the attackers used valid credentials, traditional IAM, SIEM, and CASB tools treated the logins as normal activity. The SOC only saw signs of the compromise after critical systems were already exposed.

How NDR would have helped

NDR detects risky sign-ins, mailbox manipulation, and privilege anomalies in real time, surfacing identity abuse and cloud pivots that log and endpoint tools overlook.

2 Volt Typhoon: Persistence Through DNS Tunneling

What happened

Volt Typhoon compromised home office routers and used tools like Earthworm to establish persistence. They relied on DNS tunneling for command-and-control traffic and expanded access with brute force and PowerShell abuse.

Why it was missed

DNS tunneling blended into normal traffic, while valid credentials and PowerShell scripts looked like legitimate IT operations. Endpoint and log tools failed to flag the behavior.

How NDR would have helped

NDR identifies hidden DNS tunnels, correlates brute force attempts, and flags abnormal PowerShell execution patterns, exposing stealthy persistence early.

3 Mango Sandstorm: Hybrid Attack from On-Prem to Azure

What happened

Mango Sandstorm exploited an internet-facing server to gain initial access, then moved laterally using RDP and RPC. From there, they pivoted into Azure AD and ultimately destroyed resources such as servers, disks, and databases.

Why it was missed

EDR agents could not connect the dots between on-premises lateral moves and cloud pivots. SIEM logs were siloed and failed to correlate across environments.

How NDR would have helped

NDR surfaces RPC reconnaissance, privilege escalation, and anomalous Azure activity, allowing SOC teams to intervene before large-scale destruction occurs

4 UNC3886: Exploiting Zero-Days in Trusted Zones

What happened

UNC3886 exploited zero-day vulnerabilities in Fortinet and VMware vCenter, installed custom malware on ESXi hypervisors, and used DNS tunneling to exfiltrate data.

Why it was missed

These environments could not run EDR agents, SIEM had no visibility into east-west traffic, and prevention controls had no known indicators to detect the activity.

How NDR would have helped

NDR analyzes packet flows and metadata directly to detect hidden HTTPS or DNS tunnels, suspicious admin anomalies, and lateral reconnaissance in trusted infrastructure, exposing attackers that other tools cannot see.

Regardless of an organization's size, maturity, policies, or firewall and endpoint controls, determined attackers will find a way in — the key question is whether you can detect their presence in time to prevent serious damage? It is in this context that NDR has risen to prominence as a tool purpose-built for the realities of modern cyber-attacks.

Where NDR fits in SOC architectures and frameworks

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)

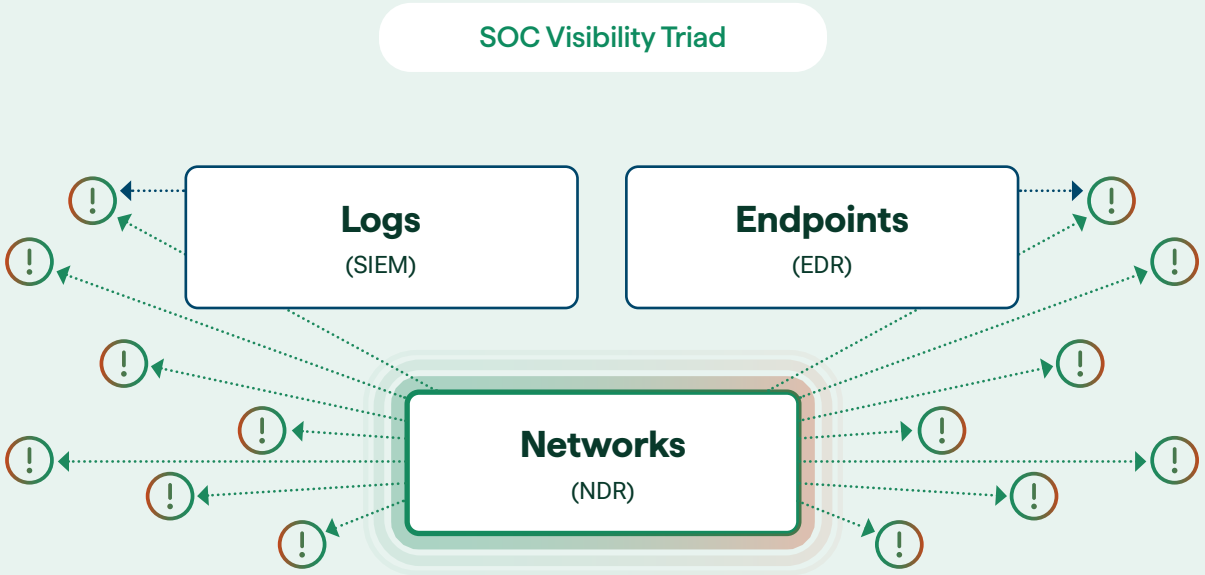
for monitoring and containing malicious activity on endpoints (workstations, servers, mobile devices).

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 cohesion 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 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 is harder, if not impossilbe, for attackers to cover their tracks on. Additionally, attackers are often unaware that an organization is covertly monitoring network traffic. As a result, attackers cannot take evasive action to avoid detection — 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 an essential security control to detect and facilitate stopping 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).

NIST

The NIST Cybersecurity Framework (CSF) outlines five key functions—Identify, Protect, Detect, Respond, and Recover—to help organizations manage cybersecurity risk. Network Detection and Response (NDR), aligns strongly with these functions, providing critical capabilities for SOC teams.

Function	NDR Capabilities	NDR Key Features	NIST Controls
Identify & Protect	Asset visibility, Behavioral baselining	• Discovers cloud, on-prem, and SaaS devices • Establishes behavioral norms for anomaly detection	ID.AM-1, PR.AE-1
Detect	Real-time AI-driven threat detection	• Detects C2, lateral movement, privilege abuse • Prioritizes behavior over signatures	DE.CM-1, DE.AE-1
Respond	Investigation and automated response	• MITRE ATT&CK mapping • SOAR/SIEM/EDR integrations for containment	RS.AN-1, RS.MI-1
Recover	Forensic support and improvement insights	• Detection history • Post-incident analysis for playbook tuning	RC.IM-1
Extended Alignment	Compliance-ready technical mappings	• Audit trails • Incident handling workflows • Continuous system monitoring	AU-6, IR-4, SI-4 (NIST 800-53), 3.14.6, 3.6.2 (800-171)

What value does NDR deliver?

The following sections distill insights from real-world NDR deployments across major industry verticals, summarizing the problems organizations face, the approach organizations take, and the measurable outcomes they achieve with NDR.

*Source: case studies and interviews with NDR customers: https://www.vectra.ai/resources

Financial services

Problem

- High-value targets for credential theft, business email compromise, and ransomware.
- Native Microsoft tools miss advanced attacker techniques (e.g., AiTM, living-off-the-land).
- Expanding distributed attack surface from hybrid cloud adoption.
- Expanded risk with Copilot AI adoption – sanctioned and unsanctioned.
- Alert fatigue and fragmented telemetry slowing incident response.

Approach

- Deploy NDR with identity and cloud telemetry correlation to close gaps beyond EDR and SIEM.
- Integrate with Microsoft Sentinel, Azure AD, and M365 for full kill chain visibility.
- Use 24/7 Managed Detection and Response (MDR) to escalate and contain identity-based threats quickly.
- Simulate attacks (MAAD-AF) to validate coverage and detection accuracy.

Outcomes

- Early detection and containment of credential and identity attacks that native tools missed.
- Reduced incident response time from days to hours.
- Centralized, low-noise telemetry supporting faster triage and cross-surface correlation.
- Proved capability to detect all simulated advanced attacks while reducing false positives by >90%.

Retail

Problem

- Large, distributed store networks and POS systems that can't support EDR agents.
- Threats span cloud, IoT, and unmanaged devices.
- Limited SOC staffing combined with overwhelming alert volume.
- Need to secure customer data and payment infrastructure while maintaining uptime.

Approach

- Deploy NDR for agentless monitoring of POS, IoT, and legacy systems.
- Integrate with EDR for layered defense and automated investigation workflows.
- Use MDR to provide continuous monitoring and expert triage.
- Roll out phased coverage from network to cloud identities (M365/Entra ID).

Outcomes

- Noise reduction of 80–98%, saving tens of thousands of analyst hours annually.
- Detection of threats in non-EDR-covered devices within days of deployment.
- Streamlined investigations with high-confidence, human-readable alerts.
- Faster response to ransomware and identity threats, preventing business disruption.

Healthcare

Problem

- Critical patient safety and data protection requirements.
- Proliferation of medical IoT and legacy systems with unknown security posture.
- Cloud adoption (M365, AWS) increases risk of undetected credential abuse.
- Regulatory compliance pressures and limited security staff.

Approach

- Deploy NDR across medical IoT, data center, and cloud to detect hidden attackers in real time.
- Integrate with existing endpoint and SIEM tools to enrich alerts and speed triage.
- Use AI-driven prioritization to focus on threats aligned with patient safety risk.
- Combine on-prem and cloud packet data for holistic view of threat activity.

Outcomes

- 80%+ reduction in critical alerts and significant drop in false positives.
- Gained visibility into lateral movement and ransomware precursors that were previously invisible.
- Reduced mean time to detect (MTTD) and mean time to respond (MTTR) from days to hours.
- Improved regulatory assurance and operational resilience.

Manufacturing

Problem

- Global, hybrid environments with limited visibility into identity behavior and unmanaged devices.
- High-value intellectual property and operational technology (OT) targeted by ransomware and supply-chain attacks.
- Legacy EDR unable to monitor all systems; alerts lacked context.

Approach

- Deploy NDR with integrated Identity Threat Detection & Response (ITDR) to correlate account activity with network behaviors.
- Use MDR for 24/7 threat monitoring, rapid escalation, and incident response guidance.
- Implement clientless monitoring for OT and IoT devices.
- Detect and respond to threats in both IT and OT environments (e.g., ransomware via infected USB, malware from phishing).

Outcomes

- 92–99.98% noise reduction and massive false positive drop.
- Detected and contained ransomware and malware incidents in under 30 minutes.
- Reduced storage and investigation costs by capturing only relevant packet data.
- Enhanced OT resilience by identifying abnormal machine and device traffic in real

Telecommunications

Problem

- Large-scale, geographically distributed infrastructure including OT systems.
- Gaps in EDR coverage for legacy/proprietary systems.
- Heavy alert load with limited correlation between endpoint and network threats.
- Complex cloud and AWS deployments requiring compliance reporting.

Approach

- Deploy NDR integrated with EDR for full network and endpoint coverage.
- Use AWS traffic mirroring for visibility into Nitro-based instances and VPC workloads.
- Leverage MDR for expert-led, around-the-clock monitoring and escalation.
- Enrich SIEM data with NDR context for advanced threat hunting.

Outcomes

- 96–99% noise reduction, 78% faster response times.
- Closed visibility gaps in OT and legacy systems.
- Improved compliance reporting efficiency.
- Detected advanced threats in AWS and on-prem that evaded endpoint tools.

Automotive

Problem

- Lean security teams tasked with securing manufacturing, R&D, and supply-chain networks.
- Compliance mandates (ISO 27001) and zero-trust initiatives demand high visibility.
- Gaps in detection where EDR cannot be deployed.

Approach

- Deploy NDR for simplified detection and analysis across hybrid infrastructure.
- Fill EDR gaps with real-time visibility into unmanaged devices and east-west traffic.
- Use MDR to reduce workload and provide expert-led incident triage.

Outcomes

- 92% noise reduction, >95% reduction in escalations.
- Improved ransomware prevention through early visibility into abnormal behaviors.
- Boosted SOC skill growth and decision-making efficiency.

Energy & Utilities

Problem

- Critical infrastructure targeted by sophisticated attackers using AI and automation.
- Legacy detection tools unable to catch unknown or unconventional threats.
- High operational risk from false positives and slow investigations.

Approach

- Benchmark multiple NDR vendors with live, unannounced penetration tests.
- Select NDR with advanced AI/ML capable of detecting non-signature-based threats in real time.
- Integrate seamlessly into existing Cyber Fusion Center operations.

Outcomes

- Significant false positive reduction, faster investigative workflows.
- Detection of complex attacker behaviors invisible to previous tools.
- More coordinated and agile incident response at global scale

Government & public sector

Problem

- Large hybrid networks (on-prem + cloud) with constant alert overload.
- Limited visibility into Active Directory and identity-based attack paths.
- Compliance and regulatory mandates requiring fast breach detection.

Approach

- Deploy NDR with Stream and Match for enriched context and known-threat detection.
- Integrate with AWS Security Hub for faster incident correlation and investigation.
- Prioritize alerts by risk to reduce analyst fatigue.

Outcomes

- MTTR reductions from multiple days to under an hour for key attack types.
- Closed gaps in AD, VLAN, and encrypted traffic threat visibility.
- Enabled junior analysts to investigate effectively with actionable alerts.

Across industries, AI-driven NDR consistently delivers measurable results — cutting alert noise by over 90%, reducing mean time to respond from days to hours, and enabling lean SOC teams to focus on true threats.

Organizations gain full visibility across cloud, identity, and network, detect attacks earlier in the kill chain, and contain incidents before they disrupt operations or lose control of data. These outcomes translate into stronger security posture, improved compliance, and sustained business resilience in the face of modern, evolving and emerging attacks.

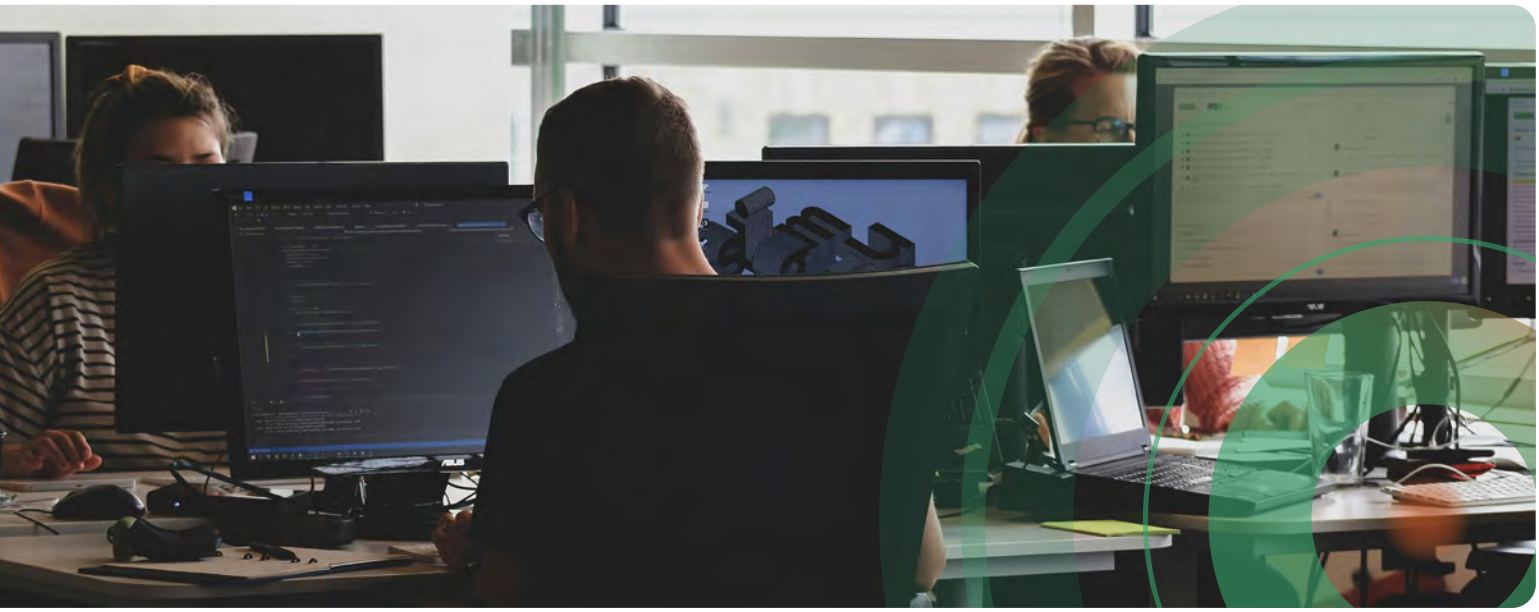
Conclusion

In an era of stealthy attackers and sprawling networks, NDR has become indispensable — a critical tool to detect, hunt, and neutralize threats before they escalate into full-blown crises.

Empowering your cybersecurity team with NDR means giving them the visibility to see attackers in every corner of the network and the intelligence to respond decisively. By deploying NDR, organizations gain the ability to detect intrusions that evade endpoint, log and signature-based defenses, monitor parts of the environment that other solutions can't (IoT devices, unmanaged devices, encrypted channels) — and ultimately respond faster to contain damage.

The case for NDR rests on a simple truth: no matter how strong your preventive defenses are, modern attackers will bypass or evade them. When compromise happens, the only way to minimize harm is timely attack detection and response. NDR provides the nervous system for your security operations, constantly monitoring for behavioral indicators of attack (IoA) to reveal signs of trouble across your digital terrain. It serves as a critical protection tool for the unknown attack — the second line of defense that catches what others miss and arms SOC teams to act swiftly and confidently.

As organizations modernize their cybersecurity and SOC strategies to protect against modern attacks, the consensus among experts is clear: incorporating NDR is no longer optional, it's essential. Forward-looking security programs are integrating NDR into their SOC workflows, alongside log analytics, identity, cloud and endpoint security, to achieve a more complete and resilient security posture. The investment in NDR pays off with attack surface coverage that reduces exposure, AI-driven signal clarity that removes latency and workload, and intelligent control that maximizes the value of existing SOC tools and talent.



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