The Risks of Gaps Without NDR and EDR Integration

Key Takeaways

- NDR and EDR provide visibility into different layers of the environment — endpoints and network traffic — and both are necessary for complete cyber threat detection.
- When NDR and EDR operate in silos, attackers can exploit the gaps between them, leading to missed lateral movement, encrypted C2 activity, and longer dwell time.
- Integrating NDR and EDR improves detection accuracy by correlating network and endpoint signals into higher-confidence alerts.
- Unified visibility across endpoints and network traffic enables faster investigations, coordinated response, and reduced operational impact during active attacks.
- The future of detection is not NDR vs EDR, but integrated, cross-layer visibility that evolves into XDR for consolidated and proactive threat defense.

Most organizations rely on either endpoint detection and response or network detection and response as primary detection layers. While both are powerful in their own domains, deploying them in isolation creates visibility gaps that sophisticated attackers are quick to exploit.

When security teams operate EDR and NDR in silos:

- Alerts lack context
- Threat timelines remain fragmented.
- Response actions are delayed.
- Blind spots persist across hybrid and cloud environments.

This is where NDR and EDR integration becomes critical. The real risk isn't choosing between tools — it's failing to connect them.

The real question is:

What are you missing when they aren't working together?

NDR vs EDR: Understanding the Core Differences

Before exploring integration, it's important to clarify what each solution does independently.

What Is Endpoint Detection and Response (EDR)?

Endpoint detection and response (EDR solutions) focus on monitoring and protecting individual devices such as laptops, servers, mobile devices, desktops, and cloud workloads.

EDR security platforms typically monitor:

- Running processes and system behavior
- File changes and execution activity
- Registry modifications
- User authentication and privilege escalation
- Application activity

Strengths of EDR Security

- Rapid containment of compromised devices
- Malware and ransomware detection
- Deep endpoint forensics
- Device-level investigation and remediation

Limitations of EDR

- Limited visibility into encrypted network traffic
- Cannot monitor unmanaged devices or IoT systems without agents
- Reduced coverage in ephemeral cloud workloads
- May miss lateral movement using legitimate credentials

EDR is highly effective at understanding what's happening on the device — but attackers don't stay confined to endpoints.

What Is Network Detection and Response (NDR)?

Network Detection and Response (NDR) focuses on monitoring network traffic data to detect suspicious behavior and anomalies. These platforms perform detailed network traffic analysis, including:

- Network flows and metadata
- DNS queries and responses
- Encrypted traffic patterns
- East-west and north-south movement
- Command-and-control (C2) communications

- Data exfiltration attempts

Strengths of NDR Security

- Detects lateral movement across systems
- Identifies suspicious encrypted traffic behavior
- Provides agentless visibility into unmanaged assets
- Monitors hybrid, cloud, and IoT environments

Limitations of NDR

- Lacks deep insight into endpoint processes
- Cannot directly quarantine files on a device
- May require endpoint validation for high-confidence response

NDR excels at understanding what's happening across the environment — even when endpoints appear normal.

NDR vs EDR: Key Differences at a Glance

Response mechanisms and visibility layers are where NDR and EDR differ from one another.

EDR Security NDR Security Endpoint-centric monitoring Network-centric monitoring Agent-based

deployment Agentless visibility across traffic Deep device-level forensics

Deep session and traffic inspection

Focus on processes and files Focus on flows, DNS, and behavior patterns Device isolation & file quarantine Network isolation & traffic blocking

The takeaway from the ndr vs edr comparison is simple:

Running one without the other creates partial visibility. And partial visibility is exactly what advanced attackers rely on.

What You Miss Without NDR and EDR Integration

Security gaps rarely appear as obvious failures. They show up as missed signals, delayed correlation, and incomplete investigations. When endpoint detection and response and network detection and response operate separately, attackers exploit the space between them.

Here's what typically slips through the cracks without NDR and EDR integration.

1. Lateral Movement Using Valid Credentials

Modern attackers rarely drop obvious malware. Instead, they steal credentials and move laterally using legitimate administrative tools.

What EDR sees:

- Approved processes like RDP, SMB, or PowerShell
- Valid user logins
- No malicious binaries

What NDR sees:

- Unusual host-to-host communication paths
- Abnormal login sequences
- Privilege escalation patterns across systems

Without EDR-NDR integration, these signals remain disconnected.

The result?

Lateral mobility and privilege escalation are ignored until the harm is done.

2. Encrypted Command-and-Control (C2) Activity

Attackers increasingly hide communications inside encrypted HTTPS, TLS tunnels, or DNS-over-HTTPS.

EDR limitation:

- Cannot deeply inspect encrypted network sessions
- Sees normal application behavior

NDR strength:

- Detects beaconing patterns
- Identifies suspicious certificate behavior
- Spots unusual communication frequency or destinations

Without integration, C2 persistence may remain invisible.

EDR doesn’t see malicious processes. NDR detects anomalies — but lacks endpoint confirmation.

The attacker quietly maintains access.

3. Fileless & Memory-Based Malware

Fileless attacks execute in memory, leaving little or no disk footprint.

EDR challenge:

- No malicious file hash
- Minimal filesystem artifacts

NDR advantage:

- Detects unusual outbound traffic
- Flags unexpected data flows to rare destinations

When telemetry isn’t combined, detection is delayed.

Only by correlating endpoint memory activity with network behavior can teams build high-confidence alerts.

This is where EDR-NDR integration closes the gap.

4. Cloud & Hybrid Workload Blind Spots

Modern environments include:

- Ephemeral containers
- Cloud-native workloads
- Remote users
- IoT and unmanaged devices

Not all assets run persistent endpoint agents.

EDR Gap:

- Limited visibility into short-lived or unmanaged assets

NDR coverage:

- Cross-environment telemetry
- Visibility into traffic regardless of device management status

Without integration, security teams see fragments of activity instead of the full attack path. Unified visibility provides coverage across hybrid environments.

5. Insider Threat & Data Exfiltration

Not all threats are external. Compromised users or malicious insiders often operate under legitimate access rights.

EDR provides:

- User behavior visibility
- File access tracking
- Endpoint activity logs

NDR detects:

- Large outbound data transfers
- DNS tunneling
- Suspicious cloud uploads
- Traffic to rare destinations

Without correlation between endpoint behavior and network movement:

- Alerts lack urgency
- Investigations slow down

High-confidence detection requires context from both layers.

The Bigger Picture: Fragmented Visibility Equals Delayed Response

Without NDR and EDR integration, organizations experience:

- Partial attack timelines
- Higher false positives
- Longer dwell time
- Reactive instead of proactive defense

Attackers don’t operate in silos — and your security tools shouldn’t either.

How NDR and EDR Complement Each Other

This isn’t about adding more tools. It’s about aligning visibility layers into a unified strategy.

1. Detection Synergy

When integrated properly:

- NDR identifies suspicious traffic patterns.
- EDR validates endpoint-level behavior.
- Validation rules correlate alerts across layers.

Two weak alerts become one strong, clear alert. This cuts false alerts and eases alert overload.

2. Faster, Context-Rich Investigation

With EDR-NDR integration, investigations move from fragmented to holistic.

Security teams gain:

- Endpoint metadata + network telemetry
- Full attack chain reconstruction
- Cross-layer timeline visibility
- MITRE ATT&CK mapping for contextual understanding

Rather than asking, "***Is this alert real?***", analysts can focus on containment and remediation.

3. Coordinated and Automated Response

Integration enables coordinated action:

- Suspicious traffic triggers endpoint isolation
- Compromised endpoints automatically block network communication
- Automated workflows reduce dwell time
- AI-driven correlation strengthens detection confidence

The outcome is strategic:

- Faster containment
- Reduced attacker movement
- Lower operational impact

From Tools to Strategy

On their own, endpoint detection and response and network detection and response are powerful.

Together, they form a cohesive detection fabric — one that sees threats moving across devices, networks, cloud environments, and identities.

The real advantage of NDR and EDR integration isn't just better detection.
It's a shift from reactive incident response to proactive threat disruption.

Benefits of Combining NDR and EDR in a Single Security Platform

Running tools side by side is helpful. Running them as one integrated platform is transformational. NDR and EDR integration removes visibility gaps, improves detection accuracy, and speeds up response.

Here's what organizations gain when network and endpoint security operate as a unified system.

1. Unified Visibility Across Data in Motion & At Rest

Attackers move across systems — from endpoint to network, from network to cloud, and back

again.

An integrated platform provides visibility into:

- Data in motion (network traffic, DNS, encrypted sessions)
- Data at rest (files, processes, registry changes, user activity)
- Data in use (memory execution, process behavior)

Instead of switching consoles to piece together events, analysts see:

- Cross-layer context
- Asset-level risk profiling

This unified perspective increases detection accuracy while cutting down on investigation time.

2. Reduced Alert Fatigue Through Context Correlation

Alert overload is one of the most significant operational issues in cybersecurity. When EDR security and NDR security operate separately:

- Both may generate alerts on the same incident
- Alerts lack contextual enrichment
- Analysts must manually correlate events

With integration:

- Network alerts are validated against endpoint behavior
- Endpoint detections are enriched with traffic intelligence
- Weak signals are automatically correlated into high-confidence alerts

The result:

- Fewer false positives
- Higher fidelity detections
- Less analyst burnout

3. Faster Post-Breach Detection

The majority of enterprises are compromised before they are aware of it. The primary distinction is the speed at which they identify persistence and lateral movement.

An integrated approach enables:

- Rapid identification of east-west traffic anomalies
- Immediate endpoint containment
- Coordinated isolation across layers
- Reduced attacker dwell time

Teams identify attacker behavior earlier in the kill chain rather than responding to symptoms.

4. Automated Threat Hunting Across Layers

Modern threats are subtle. Automated hunting across both network and endpoints, often powered by machine learning, dramatically increases detection capability.

Integrated platforms allow teams to:

- Search network flows and endpoint telemetry simultaneously
- Pivot from a suspicious IP to affected devices instantly
- Reconstruct attack paths across systems
- Leverage AI-driven behavioral analytics

This layered hunting capability moves organizations from reactive response to proactive defense .

5. Improved Zero Trust & Risk-Aware Defense

Constant user, device, and network path verification is necessary for Zero Trust. Combining network and endpoint detection and response enables enterprises to:

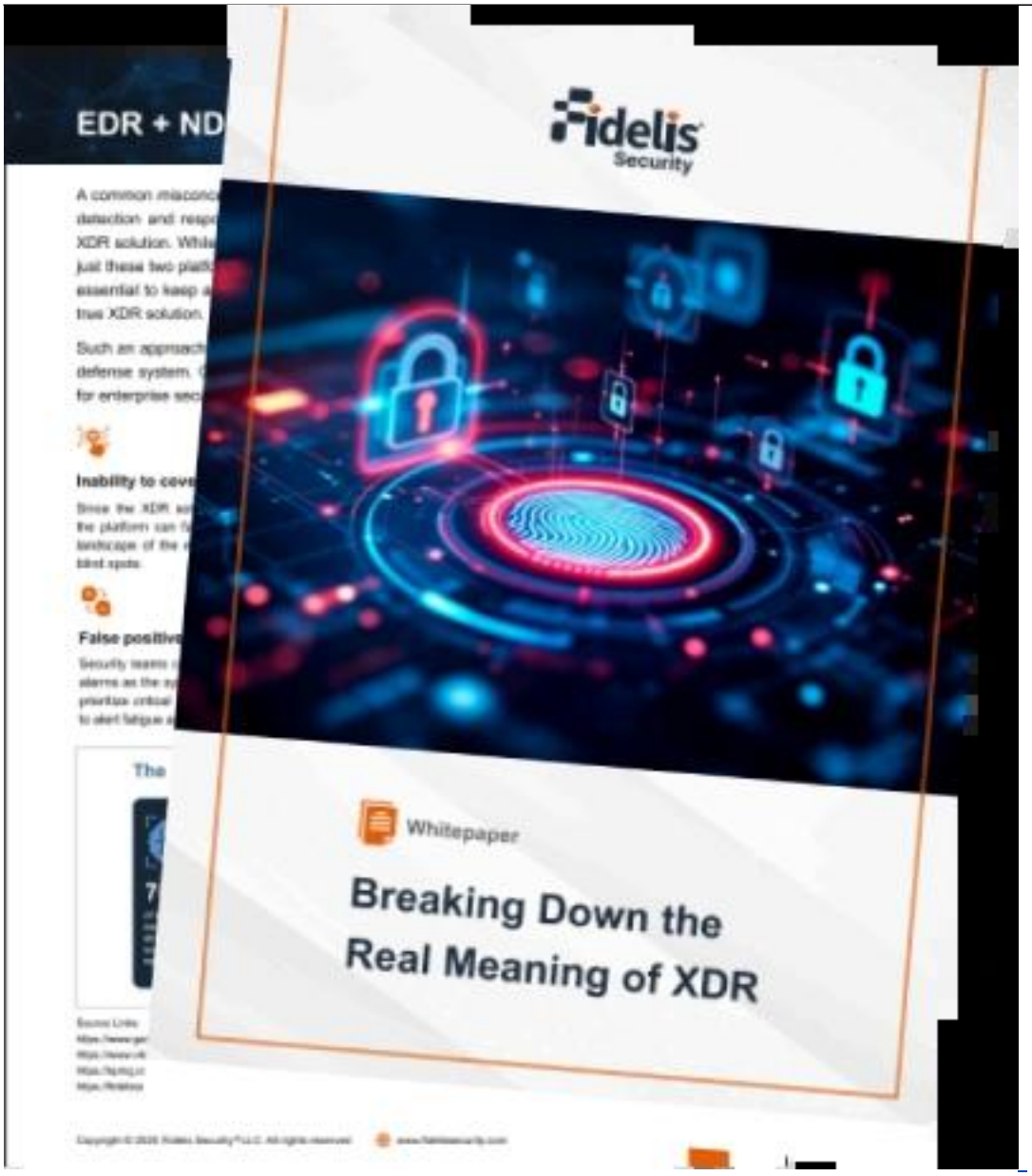
- Identify risky asset relationships
- Monitor privileged access patterns
- Detect abnormal authentication flows
- Constantly check risks across all environments

By guaranteeing that there are no blind spots between endpoints and network infrastructure, integrated visibility enhances Zero Trust architecture.

The Architecture Gap: Why EDR + NDR Isn’t Real XDR

- Not All XDRs Are Created Equally
- XDR Key Capabilities
- Choose a real solution

Get the Guide



From Integration to XDR

As environments become more complex, simple integration evolves into something broader: Extended Detection and Response (XDR).

XDR builds on NDR and EDR integration by:

- Centralizing telemetry across security layers
- Automating correlation
- Providing unified response workflows
- Delivering risk-aware insights across the entire attack surface

Instead of handling separate security tools, organizations work within one unified detection system.

How NDR and EDR Integrate with Existing IT Security Infrastructure

Integration must be practical, scalable, and open. Modern security environments rely on

interoperability — not replacement.

1. Integration with SIEM & SOAR Platforms

A unified detection approach strengthens existing security stacks.

Integrated NDR and EDR platforms typically support:

- Alert forwarding to SIEM for centralized logging
- Automated playbooks via SOAR for coordinated response
- Centralized dashboards for security operations

This ensures detection insights are operationalized — not siloed.

2. Integration with Threat Intelligence

Threat intelligence enhances both detection layers.

Integrated platforms leverage:

- Behavior-based detection rules
- Atomic and behavioral indicator feeds
- Malware sandbox analysis and scoring
- MITRE ATT&CK mapping for contextual awareness

Adding smart intelligence to alerts boosts detection accuracy and cuts manual checks.

3. Integration Across the Broader Security Stack

Effective EDR-NDR integration extends beyond endpoints and networks.

It should connect seamlessly with:

- Active Directory for identity-based attack detection
- Cloud and SaaS environments for hybrid coverage
- Vulnerability management tools for risk prioritization
- Deception technology for attacker diversion and detection
- Packet brokers and firewalls for in-line inspection

An open design with strong APIs enhances existing tools without causing disruption.

From Integration to Unified XDR: The Next Step

As organizations mature, simple integration between NDR and EDR evolves into unified protection.

Platforms like Fidelis Elevate® build on NDR and EDR integration by bringing together Fidelis Endpoint® and Fidelis Network® into a broader XDR framework. Instead of correlating tools after the fact, telemetry is analyzed natively across layers.

A unified approach connects:

- Network + Endpoint + Deception + Active Directory protection

- Risk-aware terrain mapping across assets and communication paths
- Fidelis Deep Session Inspection® across protocols
- Real-time encrypted traffic analysis
- AI-powered behavioral detection

This enables:

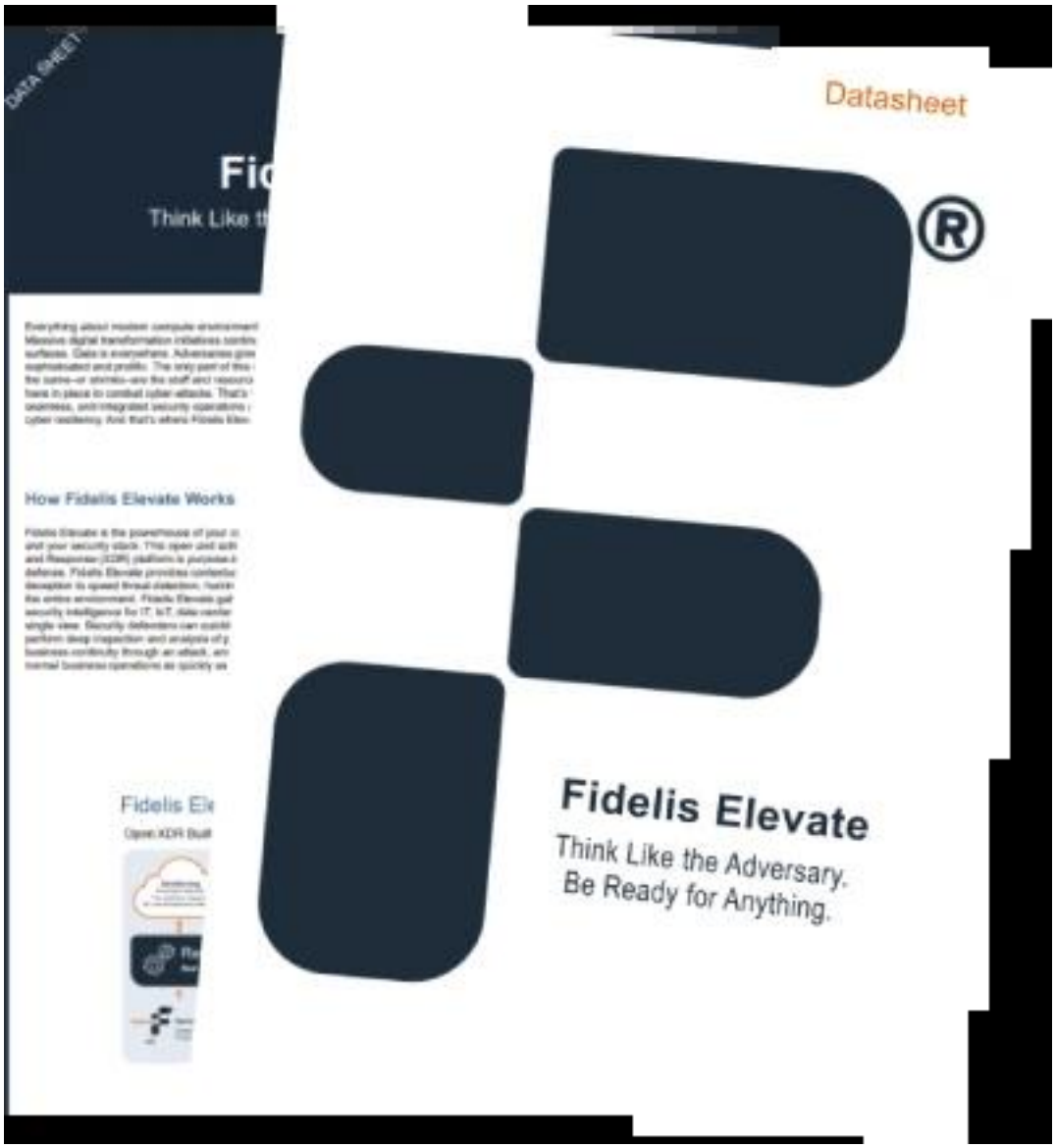
- Full visibility across managed and unmanaged assets
- Correlation of weak signals into high-confidence detections
- Coordinated response across the network and endpoints
- Reduced dwell time during active attacks

The shift isn’t about adding more tools. It’s about consolidating intelligence into a single, cohesive detection and response ecosystem.

See how Fidelis Elevate® transforms modern cyber defense with Open and Active XDR

- Unified visibility across network, endpoint, cloud, and identity layers
- Faster detection and response to advanced cyber threats
- Seamless integration with your existing security stack for a stronger defense

Download the Solution Brief Now



Conclusion: It’s Not NDR vs EDR — It’s NDR and EDR Integration

The real risk isn’t choosing between NDR and EDR — it’s running them in isolation. Threat actors move fluidly across endpoints, networks, identities, and cloud environments, exploiting gaps between siloed tools. Organizations that prioritize NDR and EDR integration gain correlated visibility, faster detection, and coordinated response across layers. In today’s threat landscape, unified insight isn’t optional — it’s essential.

Frequently Ask Questions

What is the difference between NDR and EDR?

NDR monitors network traffic to detect suspicious communication, while EDR monitors endpoint activity like processes, files, and user actions. NDR focuses on data in motion; EDR focuses on activity on devices.

Do I need both NDR and EDR?

Yes. EDR protects endpoints, and NDR detects threats moving across the network. Together, they provide broader visibility and reduce blind spots.

How does EDR and NDR integration reduce dwell time?

By correlating endpoint and network signals in real time, security teams can detect lateral movement faster and respond before attackers spread further.

Is XDR the same as NDR and EDR integration?

Not exactly. NDR and EDR integration connects two layers, while XDR extends that integration across additional areas like identity, cloud, and deception for unified detection and response.