Common Challenges in NDR Integrations (and How to Solve Them)

Key Takeaways

- NDR deployments fail when integrations are rushed, leading to blind spots in cloud traffic, encrypted sessions, and hybrid environments where attackers typically operate.
- 71% of malware now uses encrypted TLS, yet most tools cannot inspect it, requiring metadata-based behavioral analysis instead of full decryption.
- Poorly tuned behavioral baselines generate excessive false positives, with 73% of teams citing alert noise as their biggest detection challenge.
- Siloed NDR without SIEM, EDR, and SOAR integration delays response, forcing manual correlation and increasing attacker dwell time.
- Scalability limits and outdated baselines reduce detection accuracy over time, making continuous learning and distributed architecture critical for reliable threat detection.

Deploying network detection and response is the straightforward part. Getting it to work cleanly inside a live security stack is where most teams lose weeks, and where real threat detection gaps quietly open up.

The global NDR market stood at $3.68 billion in 2025 and is projected to reach $5.82 billion by 2030.1 Security teams are investing in network detection and response because endpoint tools alone cannot see lateral movement, covert data exfiltration, or command-and-control traffic buried inside encrypted sessions. An NDR solution continuously monitors network traffic, reconstructs sessions from raw network traffic data, and applies behavioral analytics to detect what signature-based tools miss entirely.

The problem is this: the promise only materializes when the integration is done right. Organizations that rush NDR deployments, bolting the tool onto an untuned SIEM, dropping sensors without cloud coverage, or leaving encrypted traffic uninspected, end up with a platform that generates noise rather than intelligence.

This guide walks through the six integration challenges that appear most consistently across enterprise deployments, explains why each one matters to your security posture, and describes what solving each one actually looks like in practice.

NDR Integration: The Cost of Getting It Wrong

$10.22M

Average U.S. data breach cost in 2025, an all-time high

241 days

Mean time to identify and contain a breach globally, the lowest in nine years

73%

Of security organizations cite false positives as their top detection challenge

71%

Of all malwares now delivered over encrypted TLS connections in Q1 2025

$1.9M

Average savings per incident for organizations with extensive AI and automation in security

85%

Of SOCs trigger incident response primarily from endpoint alerts, not network-level detections

Challenge 01:

Why Most NDR Deployments Leave Cloud Traffic Completely Unmonitored

Most NDR deployments start on-premises. Physical sensors, SPAN ports, and network TAPs cover the data center perimeter well. What they leave exposed is everything that has migrated to the cloud.

Internal east-west traffic between cloud instances rarely passes through a traditional inspection point. When an attacker moves laterally between workloads inside a VPC, or between cloud regions, that traffic stays invisible to a sensor sitting at the network perimeter. This is the precise traffic profile associated with advanced persistent threats: slow, deliberate lateral movement that specifically avoids detection at the edge.

The operational reality in 2026 is that hybrid architecture is the norm across enterprise networks. The SANS 2025 Detection and Response Survey confirmed cloud visibility as one of the most persistent blind spots, with 58% of security teams citing limited cloud expertise and 53% naming multicloud complexity as primary barriers to effective threat detection.2 Security teams that deploy NDR without addressing this gap are effectively monitoring half their network.

“Cloud environments continue to strain security programs. False positives remain the leading operational burden.”

SANS 2025 Detection & Response Survey

How to Solve It

NDR sensors must be native to each environment. AWS VPC Traffic Mirroring, Azure vTAP, and virtual sensors for containerized workloads extend coverage across all layers. The objective is not just sensor placement; it is establishing a single behavioral baseline that spans on-premises, cloud, and hybrid environments simultaneously so that east-west cloud anomalies get correlated against the same model as on-premises activity. Fidelis Network® provides full visibility across on-premises, AWS, Azure, and Google Cloud from a unified platform, closing the visibility gap that most deployments leave open.

Enhancing Detection, Response, and Visibility Through Must-Have NDR-Centric Security Integrations

- NDR and EDR
- NDR with Deception
- NDR + SIEM/SOAR
- NDR and CNAPP

Get the Guide

Challenge 02

Attackers Are Hiding Malware Inside Encrypted Traffic. Most NDR Tools Cannot See It.

Encryption has become the default for legitimate services and attackers alike. According to Google's Transparency Report, web traffic encryption has grown from roughly 48% in 2013 to approximately 95% today.[3] Attackers adapted early.

WatchGuard's Q1 2025 Internet Security Report found that 71% of all malware is now delivered over encrypted TLS connections.[4] By the second half of 2025, that figure climbed to 96% of blocked malware being delivered over TLS, according to WatchGuard's H2 2025 Biannual Threat Report.[5] Command-and-control traffic, data exfiltration, and lateral movement are all increasingly using encrypted channels specifically because most security tools cannot see inside them.

71%

Of malware delivered over encrypted TLS connections in Q1 2025

96%

Of blocked malware delivered over TLS connections in H2 2025

Full SSL/TLS decryption at scale creates its own problems. It is computationally expensive, introduces latency, and creates compliance exposure under GDPR, HIPAA, and CCPA. TLS 1.3, now widely adopted, uses ephemeral session keys that complicate traditional inspect-and-decrypt approaches further. As a result, many teams turn off inspection entirely, creating a permanent blind spot for malicious traffic hiding inside encrypted sessions.

How to Solve It

The answer is not to decrypt everything. It is to extract behavioral intelligence from encrypted traffic without breaking encryption. Modern NDR platforms analyze encrypted traffic metadata: TLS fingerprints (JA3/JA3S hashes), certificate chain characteristics, cipher suite selections, handshake timing, packet-size distributions, and session durations. These attributes reveal behavioral patterns even when the payload itself stays encrypted. Fidelis Network® uses patented Deep Session Inspection (DSI) to rebuild TLS sessions from mirrored packet captures and extract over 300 metadata attributes, operating entirely in memory without touching encrypted payloads. When C2 traffic is masquerading as HTTPS, irregular session intervals and abnormal packet-burst patterns still expose it.

Challenge 03

Too Many False Positives Are Overwhelming Security Teams and Burying Real Threats

NDR should cut through noise. When integration is not properly tuned, the opposite happens: security analysts receive floods of low-context alerts, spend their shift triaging false positives, and miss the genuine suspicious network connections buried underneath.

The scale of this problem is well documented by authoritative sources. The SANS 2025 Detection and Response Survey found that 73% of organizations cite false positives as their top detection challenge, with more than 60% encountering them frequently or very frequently.2 The same report noted that “false positives remain the leading operational burden,” a condition that has worsened year over year. Separately, the SANS 2025 SOC Survey found that 62.5% of security teams are overwhelmed by sheer data volume from their tools.6

The primary cause in NDR deployments is behavioral baseline failure. When an NDR system has not properly modeled normal network behavior for a specific environment, any deviation triggers an alert. A software deployment pushing updates across the network resembles anomalous lateral movement. A backup job at 2 AM resembles data exfiltration. The alert queue fills with normal network activity, and advanced threats hide in the noise.

How to Solve It

Reducing false positives starts with environment-specific behavioral baselines, not generic rulesets. NDR must learn what normal network activity looks like for your specific organization: which services communicate with which, over which protocols, at what times, and at what volumes. From there, enriched alerts carrying asset criticality, risk scores, and session-level context should flow to SIEM and SOAR platforms. Fidelis Network® calculates risk in real time by factoring in anomalous network activity, user behavior, and asset criticality. Every alert that reaches an analyst already carries the context needed to act quickly and with confidence.

Challenge 04

When NDR Is Siloed from the Rest of the Stack, Every Incident Takes Longer

A standalone NDR system that is not wired into SIEM, EDR, SOAR, and identity tools forces analysts to manually correlate evidence from multiple platforms during active incidents. In a breach scenario, that manual pivot between consoles is measured in hours. Those hours translate directly into attacker dwell time and increased breach costs.

The SANS 2025 SOC Survey found that 85% of SOCs trigger incident response primarily from endpoint alerts, rather than proactive network-level detections.6 When NDR and endpoint telemetry are not correlated, network-level indicators of attack go unacted upon until damage is visible on the endpoint. That sequence gets the incident timeline backwards. Integration complexity is consistently ranked among the top NDR adoption challenges alongside talent shortages and deployment costs.

NDR Integration Quality: Good vs. Broken at Each Stack Layer

Integration Point What Good Looks Like What Broken Looks Like SIEM Enriched, risk-scored events with asset context flow automatically into the SIEM timeline Raw network events flood the SIEM without context; analysts cannot prioritize SOAR / Playbooks High-confidence NDR detections trigger automated response capabilities: quarantine, block, notify NDR alerts sit in a queue; response requires manual analyst intervention for every case EDR / XDR Network anomalies cross-correlate with endpoint telemetry to confirm scope and impact Network and endpoint investigations run in parallel, duplicating analyst effort Threat Intelligence Indicators from threat intelligence feeds automatically enrich NDR detections in real time Threat intel is managed separately; analysts manually check IOCs against NDR alerts Identity / IAM Suspicious network traffic is correlated to specific user accounts for faster attribution Network detections carry no user context; attribution requires a separate investigation

How to Solve It

NDR platforms that support open APIs and standardized data formats reduce integration debt significantly. Bidirectional integration, not just pushing alerts out but pulling context in from EDR, SIEM, and identity systems, is what separates an NDR tool from an NDR capability. Fidelis Network® connects natively with SIEM platforms, EDR/XDR solutions, and SOAR platforms, enabling coordinated incident response workflows rather than siloed investigations. When an alert fires, analysts see the full picture in one place: network behavior, endpoint state, user activity, and asset criticality.

Challenge 05

NDR Platforms That Cannot Scale Create Detection Gaps at the Worst Possible Times

NDR works by ingesting raw network traffic data continuously and applying behavioral analytics in real time. At enterprise scale, that means analyzing terabytes of network data daily across dozens or hundreds of monitored segments. As cloud workloads expand, remote sites come online, and IoT devices proliferate across enterprise networks, the traffic volume grows. NDR platforms that cannot scale gracefully start creating coverage gaps.

The most common failure mode is degradation under load rather than total outage. Sensors begin sampling rather than capturing complete network traffic. Behavioral models update less frequently because the platform is processing a backlog. Coverage gaps open precisely when the network is most active. High-volume periods such as business hours, end-of-quarter data transfers, and large software deployments are also when attackers are most likely to blend malicious traffic into legitimate activity.

The computational demands of deep packet inspection are real. Analyzing network traffic models in real time, running machine learning against hundreds of metadata attributes per session, and applying behavioral analytics across multiple detection contexts all require serious processing capacity. Architectures that do not distribute this processing will bottleneck under sustained enterprise load.

How to Solve It

Distributed sensor deployment, matched to actual traffic volumes at each network segment, prevents single-point bottlenecks. For cloud environments, elastic scaling handles variable workload without manual intervention. Fidelis Network® maintains full packet capture across all ports and protocols at line rate using Deep Session Inspection, without dropping packets or introducing latency. That guarantee keeps behavioral baselines current and detection coverage complete regardless of traffic volume or time of day.

Challenge 06

Outdated Behavioral Baselines Silently Reduce NDR’s Ability to Detect Threats Over Time

NDR’s core detection method is comparing current network behavior against established baselines of what is normal. Every new cloud deployment, remote workforce policy change, business application rollout, or infrastructure migration changes what normal looks like. An NDR system that learned normal traffic patterns 18 months ago and has not updated since is making

threat detection decisions with outdated intelligence.

Two distinct problems emerge from stale baselines. The first is increased false positives: legitimate new services trigger anomaly alerts because they were not part of the original model. The second is more dangerous: after months of suppressing unfamiliar-but-benign traffic, security teams lower detection thresholds, and real malicious activity starts slipping through under the same suppression logic.

This challenge is especially acute during periods of rapid infrastructure change. A company migrating a major application to cloud-native architecture, shifting to zero-trust access management, or completing a merger will see fundamental shifts in its network traffic data patterns. Without active baseline management, the NDR model diverges from reality. When it matters most, the detections become least reliable.

How to Solve It

Machine learning-based behavioral baselines need to retrain continuously on live traffic, not just during initial deployment. The platform should detect and adapt to new normal patterns automatically: new services, new user populations, new access methods. Fidelis Network® uses unsupervised machine learning that evaluates five behavioral contexts simultaneously: external north-south flows, internal east-west communications, application-protocol behavior, data movement patterns, and event correlation. Updating across all five simultaneously gives the model enough signal to distinguish genuine environmental change from actual threat activity.

NDR Integration Challenges: Quick Reference Summary

The table below maps each challenge to its root cause and the technical approach required to resolve it, giving security teams a practical starting point for assessing their own NDR deployments.

Challenge Root Cause Technical Solution Hybrid / cloud visibility gaps On-premises-only sensors leave east-west cloud traffic uninspected Native cloud sensors (VPC Traffic Mirroring, Azure vTAP) with unified cross-environment behavioral baselining Encrypted traffic blind spots TLS 1.3 and scale constraints prevent full payload inspection Metadata-based inspection: JA3/JA3S fingerprints, session timing, cert chain analysis without decryption False positive overload Baseline not tuned to the specific environment; raw alerts forwarded without enrichment Environment-specific behavioral baselines plus risk-scored, enriched alerts to SIEM and SOAR Siloed NDR and poor tool integration Proprietary data formats; no bidirectional API integration with

EDR

, SIEM, SOAR Open APIs, standard event formats, bidirectional data flow with all major security tools Scaling under high traffic volumes Single-point sensor architecture; insufficient compute for deep inspection at scale Distributed sensor deployment; elastic cloud scaling; line-rate full packet capture Stale behavioral baselines Static models trained at deployment with no automated retraining Continuous unsupervised ML retraining across multiple behavioral contexts simultaneously

What Well-Integrated NDR Actually Delivers

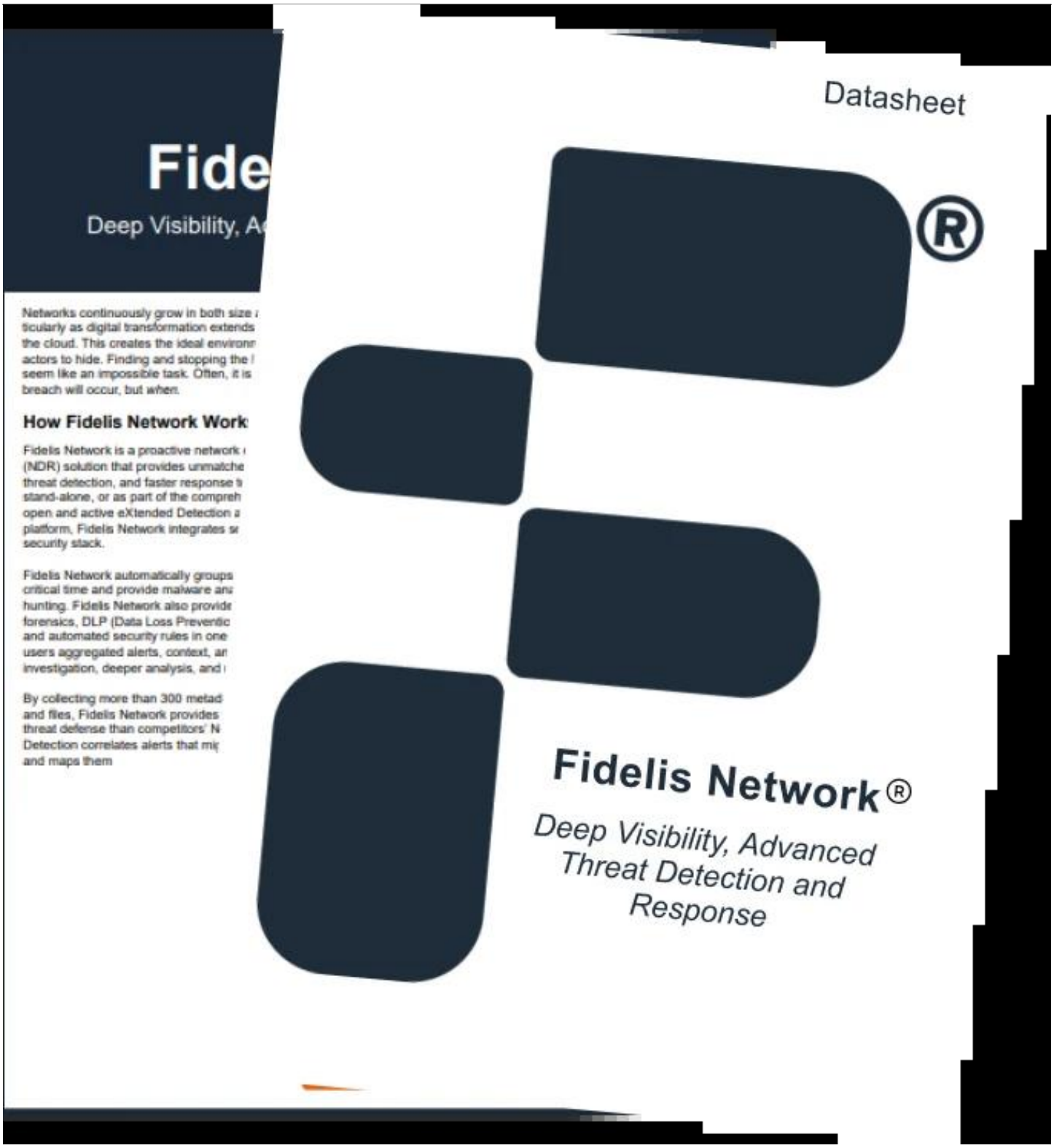
When these integration challenges are properly addressed, the operational difference is substantial. The IBM Cost of a Data Breach Report 2025 found that organizations using AI and

automation extensively in security operations saved an average of $1.9 million per incident and reduced their breach lifecycle by 80 days compared to organizations that did not.[7] The global mean time to identify and contain a breach fell to 241 days in 2025, the lowest in nine years.[7] Every day of dwell time that effective NDR eliminates translates directly to reduced cost and reduced impact.

Unlock Powerful Network Security with Fidelis NDR
See how Fidelis NDR boosts security with:

- Comprehensive Threat Detection & Analysis
- Data Loss Prevention (DLP) & Email Security
- Deep Session Inspection & TLS Profiling

Download the Datasheet



When NDR integration is done right, security operations teams gain:

- Complete visibility across on-premises, cloud, and hybrid infrastructure including east-west traffic where lateral movement happens
- Behavioral detections that surface genuine threats with the context needed for rapid, confident triage
- High-fidelity, enriched telemetry flowing into SIEM and SOAR platforms rather than raw event floods
- Automated response capabilities triggered on validated, high-confidence detections
- Reduced dwell time, cutting into the 241-day global average that still defines most

breach timelines
- Behavioral analysis of encrypted traffic without the compliance risk of full decryption

Fidelis Network® was designed to address each of these integration challenges at the architecture level. Deep Session Inspection processes traffic at line rate across all ports and protocols, collecting over 300 metadata attributes per session. Automated risk-aware terrain mapping continuously profiles and classifies assets across the full network. Machine learning evaluates anomalies across five behavioral contexts simultaneously, keeping false positive rates low while maintaining detection sensitivity against advanced threats.

Integration is native, not bolted on: direct API connections to SIEM, EDR/XDR, and SOAR platforms. For organizations working through the challenges described here, that architecture difference is what separates NDR that generates security intelligence from NDR that generates security debt.

Sources and References

1. ^PRNewswire press release: prnewswire.com/news-releases/network-detection-and-response-ndr-market-worth-5-82-billion-by-2030 Full report: marketsandmarkets.com/Market-Reports/network-detection-and-response-market-236524642.html
2. ^Direct page: sans.org/white-papers/2025-detection-response-survey-webcast-forum Survey sponsor: stamus-networks.com/blog/2025-sans-detection-response-survey-5-trends-you-cant-ignore
3. ^Google Transparency Report: transparencyreport.google.com/https/overview?hl=en
4. ^Report page: watchguard.com/wgrd-resource-center/security-report-q1-2025Official press release: watchguard.com/wgrd-news/press-releases/new-watchguard-research-reveals-171-increase-total-unique-malware
5. ^Report page: watchguard.com/wgrd-resource-center/security-report-h2-2025 Official press release: watchguard.com/wgrd-news/press-releases/over-1500-increase-new-unique-malware-highlights-growing-security
6. ^Direct page: sans.org/white-papers/sans-2025-soc-survey Webcast: sans.org/webcasts/sans-2025-soc-survey
7. ^Official report: ibm.com/reports/data-breachEditorial analysis: ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai