

---

# Do You Need SIEM or NDR or Both? NDR vs SIEM for Enterprise Security in 2026

## Key Takeaways

- SIEM handles compliance, log centralization, and broad event correlation; NDR catches lateral movement, encrypted threats, and zero-days logs miss.
- You need both—NDR feeds high-fidelity network alerts to SIEM, cutting false positives by 90%+ while preserving compliance.
- Fidelis NDR integrates natively with Splunk/Elastic/QRadar, maps network terrain, and adds web/email/cloud sensors/
- Deployment reality: SIEM takes months; NDR deploys in weeks with lighter SOC overhead.

Security teams in 2026 face cyber threats hitting harder than ever—U.S. breach costs now average \$10.22 million per incident. SIEM systems churn out false positives that bury security operations centers in alert fatigue, sparking heated NDR vs SIEM debates. Do you double down on SIEM solutions, pivot to network detection and response (NDR) for network visibility, or run both for comprehensive visibility?

This authoritative guide breaks down network detection capabilities versus security event management, integration strategies, threat detection differences, and deployment realities—drawing from Gartner, Verizon DBIR 2025, and real-world security operations data.

## SIEM vs NDR: Core Capability Comparison

SIEM (Security Information and Event Management) pulls together log data from everywhere—endpoint detection, servers, identity systems, cloud workloads, all the host systems. The main job? Event management: matching up security events into security alerts that actually drive incident response. Where [SIEM](#) systems really shine is compliance management tools—spitting out compliance reports for SEC rules and keeping log entries around for those long forensic investigations.

[NDR](#) solutions work completely different. They dig into network traffic—north-south perimeter traffic and the east-west lateral movement nobody watches. Through machine learning, entity behavior analytics (EBA), anomaly detection, they handle deep session inspection and encrypted traffic to catch malicious traffic that slips past everything else.

[Fidelis Network](#)® Detection and Response does this by automatically profiling assets and mapping communication patterns—giving SOC teams a baseline “network terrain” so deviations jump out immediately.

Capability	SIEM Systems	NDR Solutions
Log Aggregation & Security Data	✓ (Endpoints, apps, cloud)	✗
Compliance Reporting	✓ (Audit trails, regulations)	✗
Deep Network Visibility & Network Data	✗	✓
Behavioral Detection	✗	✓
Rule-based Detection Rules	✓	✗
Native Machine Learning & Artificial Intelligence	✗	✓
Lateral Movement Detection	Limited (log-dependent)	Strong (Network Activity analysis)
Encrypted Traffic Visibility	Limited	Advanced (Deep Packet Inspection)
False Positives Reduction	High noise (Context Free Alerts)	Low (Actionable Insights)

SIEM vendors dominate log collection but struggle with network security blind spots. NDR fills

---

this gap, providing the SOC visibility triad of endpoints, logs, and networks that many organizations now demand.

## Does NDR Replace SIEM — or Complement It?

NDR does not replace traditional SIEM tools—it complements them strategically within enterprise security architectures.

### Where NDR Reduces SIEM Dependence:

- Detects cyber attacks via network detection without log data ingestion delays or existing feeds dependency.
- Reduces false positives and false alerts by providing network context to security alerts.
- Surfaces high-fidelity early detection of potential threats before SIEM correlation processing.
- Provides full session reconstruction with file/URL metadata for faster investigations.

### Where SIEM Still Remains Critical:

- Compliance reporting—[GDPR](#), HIPAA, PCI-DSS audits don't run on network flows
- Enterprise-wide log centralization across every server, app, and cloud service
- Long-term security data storage for those 6-month forensic investigations
- Cross-domain correlation tying identity logs to [endpoint detection](#) to SaaS activity

Real-Time Insight, Real-Time Prevention with Fidelis Network

- Block attacks before damage occurs
- Prevent lateral movement inside your network
- Reduce false positives & alert fatigue

[Download the Whitepaper to Explore More!](#)



Gartner's 2025 Hype Cycle puts it plainly: NDR solutions patch SIEM's network blind spots—[lateral movement](#) and encrypted traffic—without replacing the log aggregation that compliance teams live by. SOC teams stop chasing 10,000 daily alerts and focus on actual threats.

## Can You Integrate NDR to Existing SIEM Infrastructure?

Yes, integrating NDR systems with existing SIEM infrastructure ranks as a crucial component of modern security posture. Most NDR solutions handle this through APIs, syslog forwarding, [automated response](#) mechanisms, and native integrations with leading SIEM vendors.

Architecture Flow:

---

Network Traffic → NDR (Anomaly Detection, Deep Session Inspection) → High-Fidelity Alerts → SIEM (Correlation with log entries, identity, endpoint detection) → SOC Workflow (Incident Response)

Integration Benefits:

- Faster triage through pre-filtered, context-rich security alerts.
- Comprehensive visibility combining network data with security information.
- Lower tuning burden via NDR's [behavioral analytics](#).
- Reduced false positives reaching security teams.

Fidelis NDR integrates natively with Splunk, Elastic, QRadar, and other SIEM platforms, feeding network-enriched alerts that cut through noise while preserving existing log investments.

## What Types of Cyber Threats Are Better Detected by NDR vs SIEM?

NDR outperforms SIEM against sophisticated [network-based cyber threats](#) that exploit network communications and evade log data visibility.

Threats Better Detected by NDR:

- Lateral movement in east-west network traffic (attackers pivoting servers).
- [Command-and-control \(C2\) beaconing](#) hidden in encrypted traffic.
- Malicious traffic within encrypted tunnels (TLS/SSL).
- Insider reconnaissance and network scanning.
- [Fileless malware](#) via DNS tunneling or living-off-the-land binaries (LOLBins).
- Zero-day network behavior anomalies and advanced persistent threats (APTs).

Threats SIEM Detects Well:

- Log-based policy violations and failed authentications.
- Authentication abuse, [brute-force attacks](#).
- Privilege escalation via identity logs.
- Compliance violations triggering audit security events.

Verizon DBIR 2025 confirms network device exploits surged to 22% of breaches, with ransomware exploiting unpatched network security gear—threats NDR catches via [anomaly detection](#) where SIEM users see delayed log entries.

## Deployment & Maintenance Comparison: SIEM vs NDR Technologies

SIEM deployment means pulling log collection from every host system, app, and data feeds source. That covers parsing/normalization, building detection rules, planning storage architecture, plus constant correlation tuning—usually taking months with serious SOC overhead.

NDR deployment runs much lighter: drop sensors on TAPs/SPAN ports (physical taps, virtual spans, cloud-native), mirror network traffic, run quick behavioral baselining. [Fidelis NDR](#) adds dedicated web, email, and cloud sensors running the same detection models across all those channels.

---

## Maintenance Comparison:

Factor SIEM Systems NDR Systems Tuning Effort High (manual detection rules updates) Moderate (AI-driven adaptation) Storage Scaling High cost (petabytes log data) Lower (metadata, flows-based) Rule Management Continuous manual Automatic Rule Generation via EBA SOC Overhead High false alerts volume Lower (actionable insights) Encrypted Traffic Scaling Complex Native support

NDR cuts security operations burden significantly—SANS 2025 reports SIEM generates 1.2M monthly alerts vs NDR's targeted, high-confidence detections.

## When You Need SIEM, NDR, or Both in Your Security Stack

Decision Framework for Security Leaders:

### Choose SIEM If:

- Compliance management tools and generating compliance reports are regulatory mandates.
- Centralized security data governance across hybrid IT infrastructure is priority #1.
- Long-term audit trails drive your security measures.

### Choose NDR If:

- East-west network visibility gaps expose lateral movement risks.
- [Ransomware detection](#) via network activity patterns is mission-critical.
- Encrypted traffic inspection addresses your top blind spot.

### Choose Both If:

- Comprehensive visibility across SOC visibility triad (endpoints, network, cloud).
- Hybrid/multi-cloud demands detection and response depth + compliance.
- Mature security operations require network detection and response precision alongside SIEM breadth.

IBM Cost of a Data Breach 2025 shows integrated security tools cut detection time significantly—organizations using [Fidelis Elevate](#)® XDR with network analytics alongside SIEM achieve faster threat response.

## Direct Answer Summary: SIEM, NDR, or Both?

SIEM centralizes security information and event management for compliance and broad monitoring.

NDR delivers [early threat detection](#) through network visibility and behavioral analytics.

NDR supercharges detection and response with low false positives. SIEM owns response workflows and regulatory adherence.

Mature enterprise security environments integrate both via security systems APIs for unified security posture.

***Do you need SIEM or NDR or Both?***

---

**You need both.** NDR vs SIEM isn't zero-sum—SIEM solutions handle log data volume and compliance; network detection and response exposes hidden cyber-attacks in network traffic. Gartner confirms this visibility triad as essential for 2026's threat landscape.

Teams adopting this approach often use Fidelis NDR + Elevate® XDR to unify network, endpoint, and cloud detection into a single investigation workflow across hybrid environments.

Give Us 10 Minutes - We'll Show You the Future of Security

*See why security teams trust Fidelis to:*

- Cut threat detection time by 9x
- Simplify security operations
- Provide unmatched visibility and control

[Book a Demo Now!](#)