Why Fidelis Is a Leading Provider of Network Detection & Response?

Key Highlights

- Encrypted traffic now carries most threats, making traditional packet-level inspection insufficient for modern detection needs.
- Fidelis Network® uses patented Deep Session Inspection to analyze full sessions, uncovering threats hidden across multi-packet flows.
- Over 300 metadata attributes per session enable precise detection and effective retrospective threat hunting.
- Native capabilities like DLP, sandboxing, and inline blocking eliminate reliance on third-party tools.
- Integrated XDR approach unifies network, endpoint, deception, and identity security in one platform.
- Automated terrain mapping adds context, helping analysts prioritize and respond faster.
- Proven deployments show significant improvements in detection speed, visibility, and incident response outcomes.

While there are many players in the field, Fidelis Security is a leading NDR vendor. We detect, hunt and respond to organizations most advanced threats and we've been doing it for years.

What sets us apart from other Network Detection and Response vendors then?

Fidelis Network® delivers full visibility across all ports and protocols through network traffic analysis, network behavior anomaly detection, data loss prevention, and active threat detection. It is the only NDR on the market that is also natively integrated into a full XDR platform combining endpoint security, deception technology, and Active Directory protection in one console.

Fidelis Network® (NDR)

Full visibility across all ports and protocols. Patented Deep Session Inspection, sandboxing, terrain mapping, DLP, and automated threat detection baked in natively.

Fidelis Endpoint® (EDR)

Monitors every endpoint event across Windows, Linux, and macOS. Detects and stops attacks before they move laterally across the network.

Fidelis Deception®

Deploys believable decoys and breadcrumbs across on-premises and cloud environments. Lures adversaries, reveals their techniques, and generates high-fidelity alerts with zero false positives.

Active Directory Intercept™

Combines AD-aware NDR with integrated AD deception to detect and respond to identity-based attacks and privilege abuse inside your directory infrastructure.

The integration matters because most competitors in the NDR space operate as monitoring-only tools and send their findings to a SIEM or XDR platform that you own separately. We built correlation, response, terrain context, and deception into the same platform. Your analysts work in one interface, with one dataset, and respond in one workflow.

Our Key NDR Differentiators, Explained

Not all NDR platforms are built the same. The following capabilities define where Fidelis Network® goes beyond standard detection to deliver real operational impact.

Patented Deep Session Inspection (DSI)

DSI is our patented technology that separates us from every other NDR on the market. Traditional Deep Packet Inspection examines individual packets in isolation. Our patented Deep Session Inspection reassembles and decodes full sessions across protocols, then applies behavioral analytics to spot threats spread over multi-packet flows.

We run two types of sensors. Direct Sensors are built for boundary traffic, handling many small, fast sessions such as web and email traffic. Internal Sensors handle fewer but longer sessions, including file sharing that can persist for days or weeks. Both operate without holding or delaying traffic, so you get near-zero latency.

Where DSI changes everything operationally: an attacker may send gradual, individually harmless packets to test the environment before executing a larger attack. A DPI system inspects each packet and finds nothing suspicious. DSI examines the entire session and flags the pattern immediately.

Rich Metadata

DSI provides the basis of network metadata, which is stored for every network session whether it passes real-time security analysis or not. The stored metadata enables analysis of many network sessions over time to detect data leakage and threat vectors that are missed by real-time analysis of a single network session.

Fidelis Network® is unique in its ability to go well beyond the high-level “stream” metadata and collect “rich metadata” from inside the session. For instance, with a web session, other vendors collect the source and destination IP, URL, and in some cases minimal header information. In contrast, Fidelis collects all of this plus more, including rich metadata from within the web session itself.

Do note, that our competitors do not provide the richer metadata that we capture, and at such a speed as we do.

300+ metadata attributes per session: During every network session, Fidelis Network® captures more than 300 protocol features, including JA3/TLS fingerprints, certificate chain details, cipher suite lists, handshake timings, packet-size distributions, session durations, and endpoint IP/port pairs. That is the foundation for both real-time detection and retrospective threat hunting.

Read Datasheet

Encrypted Traffic Inspection Without Decrypting Payload

Our DSI rebuilds each TLS/SSL session from mirrored packet captures. By operating entirely in memory, it extracts over 300 metadata attributes from the session without touching encrypted payloads, preserving end-to-end privacy. This gives our customers full encrypted traffic visibility without the legal, compliance, or performance trade-offs that come with full payload decryption.

Retrospective Analysis of the Metadata

The retrospective analysis provides security teams with the ability to apply new insights or threat intelligence against historical traffic (i.e., the metadata stored about prior network traffic) to determine if the environment was compromised by a previously unknown threat. The analysis is automated and continuously running against stored network metadata.

With DSI and a retrospective analysis of an organization's metadata, security teams can analyze the details of a security incident. This includes how the cyber defenses were breached, what resources were accessed, and what changes were made within the environment. This information is crucial in formulating your incident response and determining what needs to be done to prevent future breaches.

Automated Cyber Terrain Mapping

When adversaries target an enterprise, their first objective is to map the environment. They discover assets, learn each asset's role, identify operating systems, document communication paths, and find vulnerabilities before they move. We do the same thing first, automatically and continuously.

Fidelis Network® automatically detects the operating system and role of every discovered asset, including workstations, servers, IoT devices, domain controllers, and cloud workloads. It maps communication paths between assets, documents which ports and protocols are used, and assigns subnet definitions. Risk scores are calculated across multiple dimensions: asset importance, security coverage gaps, known CVEs sourced from daily database updates, and active threat alerts.

This terrain context is what makes our alerts actionable. When a detection fires, your analysts immediately know the criticality of the affected system, what it connects to, and what the probable attack path looks like. That eliminates the manual enrichment step that slows down most SOC workflows.

Multi-Layer Machine Learning Detection

Our anomaly framework evaluates five distinct contexts simultaneously: external north-south flows, internal east-west communications, application-protocol behavior, data movement patterns, and event correlation. This multi-context approach is why we surface the right outliers without flooding analysts with noise.

We combine supervised ML, unsupervised anomaly detection, a signature and rules engine, and threat intelligence in one detection stack. AI-only platforms that rely on a single methodology produce high false positive rates.

Network Data Loss Prevention

DLP is a native capability in Fidelis Network®, not a bolt-on or a third-party integration. We monitor all outbound traffic across network, email, and web channels and use DSI to detect and block unauthorized data transfers in real time, including across encrypted sessions.

Fidelis Security is the only vendor in the security market to offer a combo of NDR and Network DLP solution. With the Fidelis Network capabilities, you can benefit from visibility of data movement across all ports and protocols and get complete content and context, as well as receive indicators of compromise with data departing from your network.

Native Inline Blocking Without Third-Party Dependencies

We provide native inline and out-of-band blocking. When a threat is detected, we stop it directly.

We also offer automated response playbooks that coordinate actions across Fidelis Network®, Fidelis Endpoint®, and Active Directory Intercept™ simultaneously. When a detection fires across multiple sensors, one coordinated response executes across all three layers without manual intervention.

How We Compare: Fidelis NDR vs ExtraHop, Corelight, and Vectra

The table below compares Fidelis Network® Detection and Response against three commonly evaluated alternatives. Data is drawn from our internal competitive research, verified against each vendor’s published product documentation, and supplemented by the GBHackers NDR Solutions Guide published January 2026.

Capability Fidelis NDR ExtraHop Reveal(x) Corelight Vectra AI Deep Session Inspection (full payload context) Native, patented Stream reassembly, no malware analysis Headers only Headers only SSL/TLS Decryption Agentless, on-the-fly Agent required on each server Not available Not available Native Data Loss Prevention (DLP) Yes, granular policies Not available Not available Not available Malware Detection and Sandboxing Native cloud sandbox Not available Not available Not available Custom Detection Rules Engine Simple editor, no scripting Not available Zeek scripting (expert only) Not available Inline/Out-of-Band Blocking Native Third-party only Third-party only AD accounts only IDS/IPS Native rules engine Not available Suricata signatures Via Suricata Cyber Terrain and Asset Risk Scoring Automated, continuous Device classification only Not available Limited Email Security Native Not available Not available Not available Deception Technology Integrated XDR module Not available Not available Not available AI/ML Detection Multi-model, supervised + unsupervised Cloud-based ML SIEM required for ML AI-first platform SIEM Required for Full Analysis No, standalone CommandPost UI No Yes, required Recommended Retrospective/Historical Analysis Full metadata search, rich filters 90-day cloud record store Via SIEM only StreamPlus feature All Ports and Protocols 70+ decoders plus unknown decoder 70+ protocols, no rules support Zeek protocol set Limited

*Disclaimer: The comparison above is based on publicly available product documentation, vendor datasheets, and third-party published materials. This table is provided for informational purposes only and should not be construed as a definitive or exhaustive assessment of any third-party product.

Real-World Deployments

The following deployments are documented in our published case studies and customer pages. Every outcome below comes from a verified production environment.

Retail Enterprise: Undetected PII Transmission Found in Network Traffic

A retail organization was experiencing repeated instances of personally identifiable information and plaintext passwords being transmitted across their network without detection in their existing security logs. Fidelis Network® surfaced these transmissions through its deep session and content inspection, allowing the team to address both the security risk and the compliance exposure before a reportable incident occurred.

Read the Case Study

Industrial Manufacturing: Confidence in Security Coverage

Martin Rothaler, Director Information Technology at LAUDA, a manufacturing customer referenced on our NDR product page, stated: “I know it’s unlikely to ever be 100% secure, but Fidelis gives me confidence that our security is at the highest possible level.” For OT-adjacent environments where network visibility across device-heavy infrastructure is non-negotiable, this reflects the operational assurance our terrain mapping and protocol-level inspection delivers.

Read the Case Study

Our 30-day guarantee:

Deploy Fidelis Elevate® in your environment for 30 days. We guarantee we will find threats your current provider has never seen. If we are wrong, we will pay you $50,000 or donate $50,000 to a children’s charity of your choice.

Click for more info!

Conclusion

Overall, Fidelis Network Detection and Response provides visibility and a unique, patented contextual perspective across your network, email, and proxied web traffic. Combining this valuable contextual perspective with machine learning, sandboxing, threat intelligence and active deception defenses ensures more effective threat detection throughout the entire kill chain. This goes from the initial infection through to the data leakage by malicious outsiders or malicious insiders. Teams can rapidly respond to identified issues in the network or at the endpoint to immediately remove malware, execute a response playbook, and prevent data theft.