Difference Between Fidelis’ Deep Session Inspection ™ and Traditional Deep Packet Inspection (DPI)

Deep Packet Inspection (DPI) was once the go-to method for monitoring network traffic, but it now struggles to detect today’s evasive, multi-stage cyberattacks that are spread across multiple channels and hidden deep within payloads.
Fragmented visibility, surface-level scanning, and a lack of contextual understanding mean that malicious activity often slips through unnoticed, putting security teams constantly on the back foot.

By reassembling full sessions, inspecting deeply at every layer, and enabling automated, real-time responses, DSI delivers unmatched precision and clarity. This blog breaks down how Fidelis DSI compares to traditional DPI across core capabilities — so you can see why modern security demands more than just packet inspection.

Visibility Gap: Packet vs. Session-Level Understanding

Traditional DPI tools inspect network traffic at the packet level. While this approach helps in identifying obvious threats, it often fails to capture context — because it treats each packet in isolation. Malicious content that’s broken into pieces across multiple packets can go undetected.

Fidelis Deep Session® Inspection reassembles full network sessions, decoding every byte across the communication chain. This enables analysts to see the entire session in context—from protocol to payload—and detect threats spread across multi-packet flows.

For example: A phishing campaign may deliver a malicious file in chunks across a series of packets. Traditional DPI sees harmless fragments. Fidelis Deep Session Inspection® reassembles the entire session, recognizes the file, and flags it before it executes.

Traditional DPI Fidelis Deep Session Inspection™

- Packet-level inspection only
- No context across packets
- Misses fragmented threats
- Sees isolated data

- Full session reassembly
- Context-aware analysis
- Detects multi-packet threats
- End-to-end visibility

For example:

Misses

malware

split across packets

For example:

Reconstructs file, flags threat pre-execution

Surface-Level Scanning vs. Deep Content Inspection

Deep Packet Inspection (DPI) is often limited to scanning packet headers or using pattern-matching to detect threats. This approach falters when content is embedded within complex file types, or deeply encoded to avoid signature-based detection.

Fidelis Fidelis Deep session Inspection™ performs deep content inspection across multiple layers. Whether it's a PDF with embedded JavaScript, a macro in a Word file, or encoded content in a web payload—Fidelis Deep session Inspection can decode and inspect it all. This enables the identification of hidden threats that DPI simply misses.

For example: A seemingly benign Word file sent via email may contain an embedded macro that triggers a malware download. DPI might let it pass. Fidelis Deep session Inspection drills into the file, detects the macro, and identifies the threat within seconds.

Traditional DPI Fidelis Deep Session Inspection

- Header-based scanning
- Pattern-matching only
- Struggles with embedded threats
- Limited file inspection

- Multi-layer content decoding
- Inspects embedded scripts/macros
- Works across formats (PDF, DOC, web) – Uncovers hidden threats

For example:

Misses macro in Word document

For example:

Detects macro, flags threat instantly

Lack of Context vs. Actionable Intelligence

Traditional DPI can generate alerts but doesn't provide much context around the content, user behavior, or application. This creates gaps for security teams, who must investigate alerts manually with limited information.

Fidelis Fidelis Deep session Inspection adds a layer of content identification that builds contextual understanding around data—what it is, where it came from, and how it behaves. This allows for automated responses such as deleting malicious packets, quarantining emails, or executing predefined response playbooks.

For example: An email attachment downloads a suspicious file and initiates outbound communication. DPI might flag unusual traffic but not link it to the email or the user. Fidelis Deep session Inspection ties all components together and triggers an automated response.

Traditional DPI Fidelis Deep Session Inspection

- Basic alerts, no depth
- No user or source linkage
- Manual investigation needed
- Low response speed

- Context-rich threat insights
- Links user, file, behavior
- Enables automated actions
- Faster incident response

For example:

Detects odd traffic, lacks source info

For example:

Traces to user, email, and response flow

Static Detection vs. Real-Time and Retrospective Threat Detection

DPI typically relies on real-time scanning. If a threat isn’t recognized in that moment, it passes through unnoticed. There’s no mechanism to retroactively catch threats based on future intelligence.

Fidelis Fidelis Deep session Inspection records metadata from every session, allowing organizations to go back and analyze previously undetected threats once new Indicators of Compromise (IoCs) become available. This adds a retrospective threat detection capability that DPI lacks.

For example: A backdoor installed weeks ago might not have triggered any alerts at the time. When new IoCs emerge, Fidelis Deep session Inspection can review past sessions, identify the entry point, and help contain the threat.

Traditional DPI Fidelis Deep Session Inspection

- Real-time only
- No backward lookup
- Misses delayed threats
- No post-analysis

- Real-time + retrospective scans
- Stores session metadata
- Matches new IoCs with past traffic
- Tracks hidden compromises

For example:

Misses old backdoor infection

For example:

Revisits old session, reveals entry point

Siloed Traffic Analysis vs. Unified Channel Visibility

Traditional DPI solutions are often limited to specific traffic types—network, email, or web. They don’t provide a unified view, which results in fragmented insights and incomplete investigation paths.

Fidelis Fidelis Deep session Inspection inspects traffic across network, email, and web channels simultaneously. This unified view ensures that attacks leveraging multiple vectors—like a phishing email followed by a malicious website redirect—are identified as a single coordinated campaign.

For example: An attacker sends an email with a link that redirects users to a compromised website. DPI monitoring only network traffic won’t correlate this behavior. Fidelis Deep session Inspection sees the email, the click, the redirect, and the payload—all in one view.

Traditional DPI Fidelis Deep Session Inspection

- Analyzes one channel at a time
- No cross-channel correlation – Fragmented investigation
- Partial threat view

- Unified view across email, network, web
- Correlates multi-vector attacks
- Sees full attack flow
- Comprehensive investigation

For example:

Can’t link email to web traffic

For example:

Maps email → link → malicious site flow

Limited Threat Insight vs. Real-Time Indicators of Compromise

DPI’s rule-based detection models are often slow to adapt. Even if malicious activity is observed, DPI lacks a mechanism to generate or act on Indicators of Compromise in real time.

Fidelis Fidelis Deep session Inspection continuously analyzes traffic and triggers IoCs instantly when threats or data leakage attempts are detected. These IoCs alert security teams immediately, ensuring faster response and containment.

For example: A user unknowingly uploads sensitive data to a third-party storage service. DPI may not recognize the file or intent. Fidelis Deep session Inspection detects the content type, recognizes unauthorized data movement, and flags it instantly.

Traditional DPI Fidelis Deep Session Inspection

- Rule-based detection
- Slow to adapt
- No instant threat flags

- Can’t generate IoCs

- Real-time threat detection
- IoCs triggered instantly
- Immediate team alerts
- Swift data loss prevention

For example:

Misses sensitive file upload

For example:

Flags unauthorized file movement fast

Protocol Limitations vs. Advanced Protocol and Application Decoding

DPI is often blind to modern application protocols, encrypted traffic, and embedded document types. Its capabilities stop at recognizing common transport layers or HTTP headers.

Fidelis Fidelis Deep session Inspection identifies a broad spectrum of protocols (TCP, UDP, ICMP), application layers (HTTP, SMTP, FTP), and embedded content (PDFs, ZIPs, MS Office files). It decodes this data to understand the true intent behind sessions.

For example: A compressed ZIP file passed over TLS may look harmless to DPI. Fidelis Deep session Inspection decodes the session, unzips the file, extracts a hidden macro-laden document, and flags it for malicious behavior.

Traditional DPI Fidelis Deep Session Inspection

- Limited protocol support
- Blind to encrypted/modern traffic
- Misses embedded file types
- Basic header inspection

- Decodes modern protocols (HTTP, FTP, SMTP)
- Decrypts traffic, extracts content
- Reads embedded ZIPs, DOCs, PDFs
- Identifies hidden intent

For example:

Skips encrypted ZIP over TLS

For example:

Unzips, scans document, flags macro

Passive Alerting vs. Preventive Action and Policy Enforcement

Traditional DPI systems generate logs or alerts, but take no active steps to stop threats. This

slows down response and increases exposure.

Fidelis Fidelis Deep session Inspection enables policy-driven actions like deleting specific packets, blocking communication, or quarantining content before it reaches the endpoint. This reduces reliance on human intervention and accelerates containment.

For example: A user attempts to download a trojan-infected file from a known malicious domain. Fidelis Deep session Inspection recognizes the domain, identifies the threat in the payload, and deletes the packet mid-session—stopping the download entirely.

Traditional DPI Fidelis Deep Session Inspection

- Generates passive alerts
- No threat blocking
- High manual effort
- Slower containment

- Active threat prevention
- Deletes, blocks, quarantines
- Enforces custom policies
- Stops threats mid-session

For example:

Logs trojan, doesn’t stop download

For example:

Deletes infected packet instantly

Conclusion: DPI Falls Short Where Fidelis Deep session Inspection Excels

Traditional DPI can’t keep up with today’s advanced, multi-layered threats. Fidelis Deep Session Inspection goes beyond by offering full session visibility, deep content analysis, and automated, intelligent response across all threat vectors.

Take your threat detection to the next level. **Explore Fidelis Deep Session Inspection today and stay ahead of evolving cyber threats.**

Frequently Ask Questions

Why is session reassembly more effective than inspecting individual packets?

Session reassembly enables a complete view of communication, helping to detect threats hidden across multiple packets that may seem harmless on their own.

How does deep content inspection help against hidden threats?

Deep content inspection allows security tools to analyze nested or encoded payloads, uncovering threats concealed in formats like ZIPs, PDFs, and Office documents.

What’s the value of retrospective threat detection?

It allows teams to detect threats that were previously undetectable by reanalyzing historical data using updated threat intelligence and indicators of compromise.