Where Fidelis NDR Fills the Gaps Left by Your Secure Web Gateway

Secure Web Gateways (SWGs) have become a cornerstone of enterprise security. They filter web traffic, enforce policies, and block known threats. But as attackers get smarter, many organizations are realizing one hard truth: a Secure Web Gateway alone is not enough.

In this blog, we'll explore the limitations of Secure Web Gateways, explain *how a secure web gateway works*, and show how Fidelis NDR (Network Detection and Response) fills the blind spots, helping you build a more complete network security gateway strategy.

Understanding Secure Web Gateways

A Secure Web Gateway solution acts as a checkpoint for outbound web traffic. It prevents users from accessing malicious websites, blocks inappropriate content, and applies organization-wide security policies.

How does a Secure Web Gateway work?

- **Traffic redirection:** All web traffic (HTTP/HTTPS) is routed through the secure web gateway.
- **Policy enforcement:** The SWG checks if requests meet security policies.
- **Threat intelligence:** Known malicious URLs, signatures, and reputation data are compared before allowing or denying access.
- **Content inspection:** Malware and phishing payloads in downloads or websites are scanned.

With cloud adoption, cloud based Secure Web Gateways (cloud security gateways) now extend these protections to remote users.

SWGs excel at:

- Blocking known malicious URLs
- Applying content filters for compliance
- Enforcing web browsing policies
- Preventing users from downloading known malware

But here's the challenge: SWGs focus only on web traffic going in and out of the network. Modern attackers have evolved, and that's where Secure Web Gateway limitations begin to show.

The Limitations of Secure Web Gateways

1. Limited Visibility Beyond Web Traffic

A cloud based Secure Web Gateway primarily monitors north–south traffic (user-to-internet).

Once an attacker gains a foothold in your environment, east–west (internal) traffic goes largely unmonitored. Malware can move laterally between devices, establish command-and-control (C2) communications, or exfiltrate data using non-web protocols, all without triggering SWG alarms.

2. Blind Spots in Encrypted Traffic

While many secure web gateways can decrypt TLS/SSL traffic, they are limited to web protocols. Encrypted traffic using DNS tunneling, SMB, SSH, or other non-HTTP channels often slips through undetected.

3. Weak Against Zero-Day or Fileless Attacks

SWGs depend heavily on known signatures and threat intelligence. They can miss:

- Zero-day exploits
- Fileless malware
- Abnormal user behavior or lateral movement
- Sophisticated, multi-stage attacks

4. Limited Threat Intelligence Context

A Secure Web Gateway threat intelligence database focuses on URLs and files. It lacks deeper context around attacker behaviors, techniques, and the relationships between alerts.

5. Alert Overload Without Prioritization

An SWG may generate large volumes of alerts in limited context. Security teams can become overwhelmed, making it difficult to identify truly dangerous threats over time.

Why SWG Alone is Not Enough

While an SWG is critical for protecting outbound web traffic, it cannot provide the deep, contextual network visibility needed for advanced threat detection and response.

This is where Fidelis NDR (Network Detection and Response) comes in.

Overcoming Detection Gaps with Deep Packet Inspection

Learn how Deep Packet Inspection (DPI) strengthens detection and response across your network.

- Uncover blind spots
- Detect threats and zero-day exploits
- Accuracy with full-session visibility

Download the Whitepaper

Fidelis NDR: Filling the SWG Blind Spots

Fidelis Network® (NDR) complements your secure web gateway solution with internal visibility, behavioral analytics, and automated response. Think of it as the other half of your network security gateway.

What is Fidelis NDR?

Fidelis NDR is a network detection and response platform designed to:

- Inspect all network traffic (north–south and east–west)
- Detect advanced threats using behavioral analytics and deep packet inspection
- Correlate and enrich alerts with threat intelligence
- Automate response actions to reduce dwell time and damage

How Fidelis NDR Addresses SWG Limitations

Broad Internal Network Monitoring

Fidelis NDR keeps an eye on every port, protocol, and type of traffic—not just outgoing web activity. By offering this kind of internal network visibility, it helps spot things like lateral movement, command-and-control traffic, and threats from within your organization. If malware avoids detection by your Secure Web Gateway, Fidelis can still reveal suspicious actions happening inside your network.

Comprehensive Session Checks and Analysis of Encrypted Traffic

Fidelis NDR uses its patented Deep Session Inspection technology to examine complete sessions instead of just focusing on packets. It works on both encrypted and uncommon protocols. This method helps find hidden payloads inside encrypted tunnels or strange traffic. It also makes it possible to catch sneaky data theft or advanced hacker tricks that traditional SWGs often miss.

Behavioral Analytics

Fidelis NDR moves beyond signature-based methods by using advanced behavioral anomaly detection. This system looks for unusual changes in normal network actions. It helps uncover unknown threats, zero-day exploits, or strange user behavior. Attackers can’t avoid detection by dodging standard Secure Web Gateway signatures or skipping threat intelligence systems.

Context-Rich Threat Intelligence

Fidelis NDR combines real-time threat insights with MITRE ATT&CK tactic mapping and past network data. It provides detailed context for each alert. This helps analysts figure out attack intent and scale faster, prioritize cases better, and avoid wasting time on false positives that come from standalone SWG alerts.

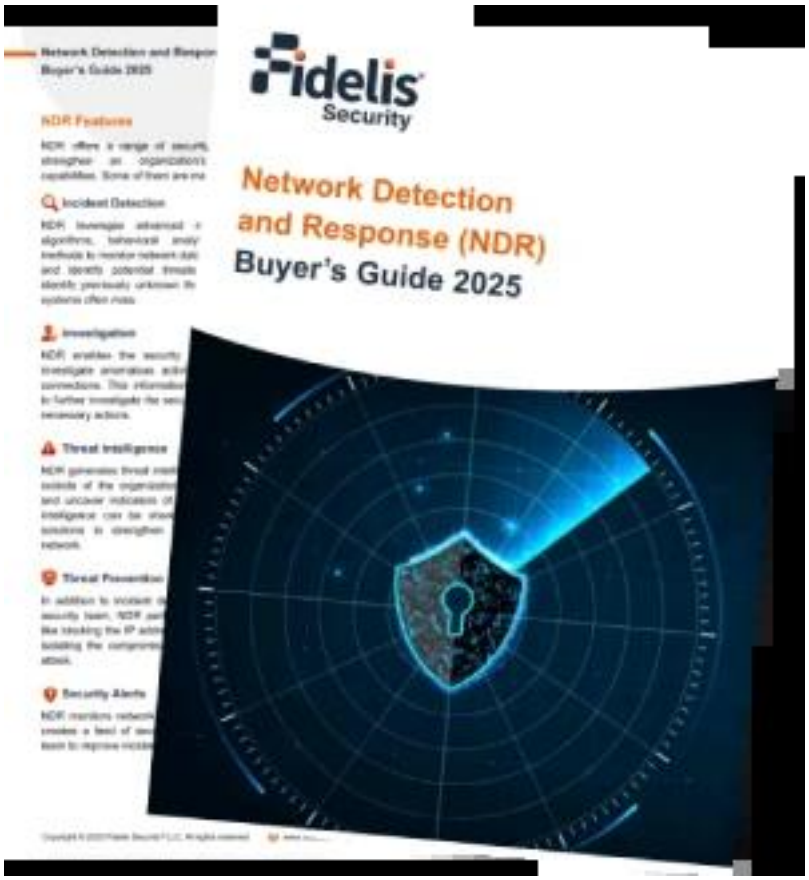
Automated Response

Fidelis NDR not finds threats but also takes action on its own. The system can cut off compromised devices, stop harmful sessions, or activate SOAR playbooks. This quick automation limits attacker presence much faster than Secure Web Gateways can manage by themselves.

Choose the Right NDR with Confidence

- Our complete checklist for evaluating Network Detection and Response solutions.
- Key features every NDR platform should offer
- Questions to ask vendors before you buy
- How to compare NDR solutions for your environment

Get the NDR Buyer’s Guide



Real-World Use Cases

Use Case SWG Limitation Fidelis NDR Solution Malware in the network SWG blocks malicious websites but misses internal C2 traffic Fidelis

detects lateral movement

and internal communications Encrypted exfiltration SWG only decrypts HTTP/HTTPS traffic Fidelis inspects all ports and protocols, including DNS and SMB Zero-day threats

Signature-based detection

misses unknown attacks Fidelis uses behavioral analytics and threat intelligence Insider threats SWG cannot see internal movement Fidelis detects abnormal user behavior and lateral movement Alert fatigue SWG alerts lack context and prioritization Fidelis correlates related alerts and prioritizes by risk

SWG + NDR = Complete Network Security

Your cloud based Secure Web Gateway still plays an essential role. But pairing it with Fidelis NDR gives you complete coverage:

1. SWG handles web traffic filtering, URL blocking, and outbound policy enforcement.
2. Fidelis NDR monitors all internal and external network traffic, adds context, and detects advanced attacks.

This combination allows you to:

- Catch stealthy attacks before data is stolen
- Monitor hybrid and remote environments end-to-end
- Reduce false positives and analyst fatigue
- Shorten mean time to detection (MTTD) and response (MTTR)

How Fidelis NDR Integrates with Your SWG

Deploying Fidelis NDR alongside your existing secure web gateway solution is straightforward:

1. Network sensors (virtual or physical) monitor traffic from data centers, cloud, and branch offices.
2. Metadata collection from your SWG or proxies is ingested by Fidelis NDR.
3. Behavioral analytics and threat intelligence correlate SWG logs with deeper traffic inspection.
4. Automated response playbooks block threats across your network in real time.

This layered approach ensures your cloud security gateway and NDR solution work hand-in-hand.

Blind Spots to Complete Visibility with Fidelis Network

A Secure Web Gateway helps manage outbound web traffic and blocks known threats. However, it cannot protect against hidden and advanced attacks. Gaps in monitoring encrypted traffic, east–west traffic, and zero-day threats allow attackers to act without being seen.

Fidelis NDR (Network Detection and Response) addresses these weaknesses. It offers complete network visibility detailed session inspection behavioral analysis, and automated actions. When combined with your cloud-based Secure Web Gateway, Fidelis NDR builds a stronger defense to catch and stop attackers before they steal data or disrupt your business.

Merging the advantages of both solutions offers a complete network security gateway setup. It helps to close key gaps cut down on alert exhaustion, and speed up how incidents are handled.

Experience the Fidelis Difference
With Fidelis Network®, you gain:

- Comprehensive visibility across all network traffic
- Deep packet and session inspection
- Automated detection and response

Book a Demo Now!