PRODUCT BRIEF

Fidelis Network®

Deep Visibility and Control to Protect Against Network Threats

In today's dynamic infrastructure environments, networks represent a wealth of potential entry points into your systems and data exfiltration opportunities for your adversaries. The threats never stop, and the landscape is constantly changing. By gaining deep visibility into your network users and traffic — including encrypted traffic — you can proactively protect your assets. With contextual intelligence and rapid response tools, you'll have the ability to more proactively detect, neutralize, and protect against network intrusions, malware, ransomware, and data exfiltration attempts before they damage business operations.

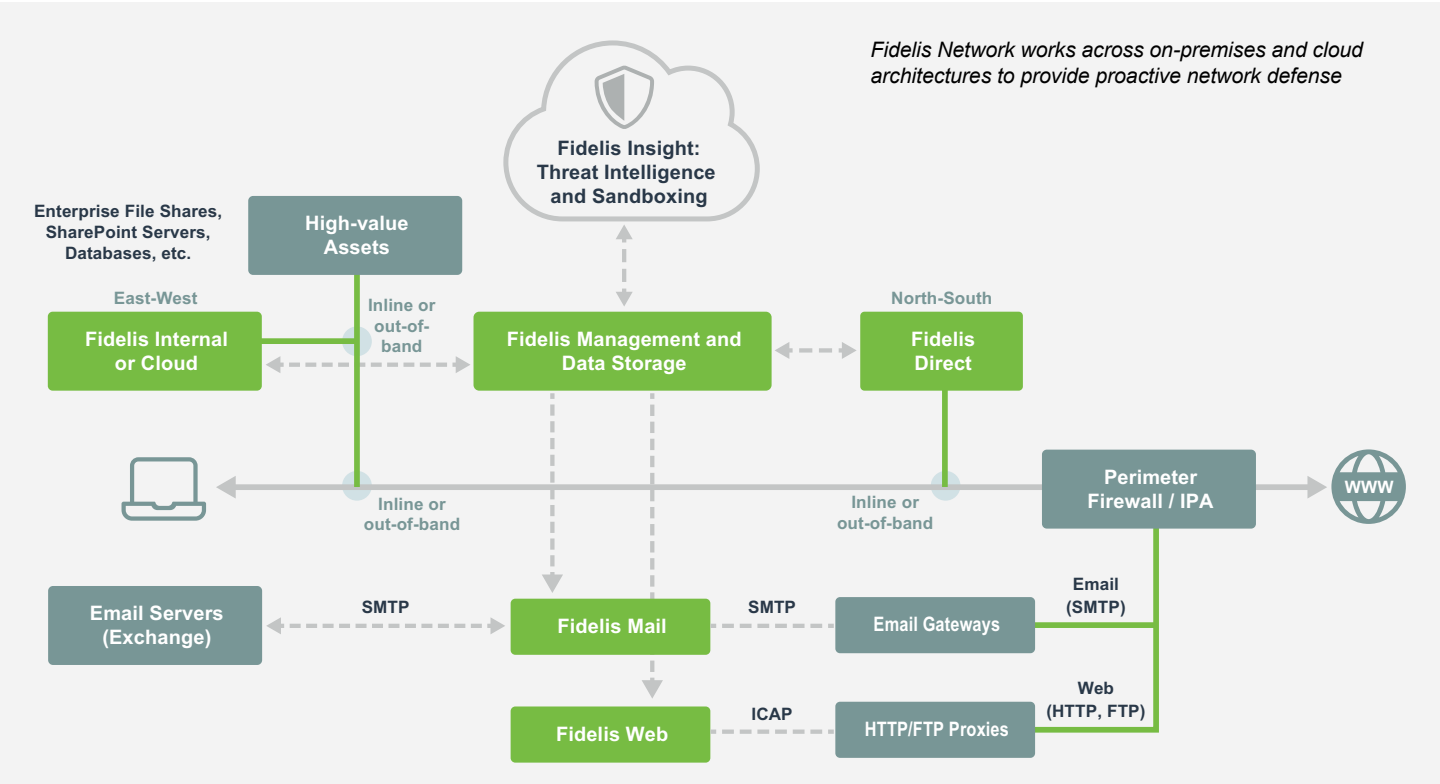
Fidelis Network

Fidelis Network® unites real-time and retrospective analysis with data loss prevention (DLP) for network, email, and web traffic. Fidelis Network scans all network traffic bi-directionally — east-west and north-south — to identify threats and signs of data leakage. Using its patented Deep Session Inspection® technology Fidelis Network employs sensors to provide contextual metadata across file formats and content, across all ports and protocols, at real-time wire speed and at enterprise scalability. With rich network visibility, multiple detection techniques, incident response workflow automation, validated alerts, and the easy-to-use CommandPost interface, you can reduce response time from hours to seconds. Unsupervised machine learning and statistical modeling based on rich metadata in Fidelis Network can uncover potential threats that may be hard to find using traditional detection methods.

NETWORK USE CASES

- Identify threats and data leakage in real-time
- Unpack and extract deeply embedded files to detect data exfiltration attempts
- Neutralize and prevent network-based attacks
- Secure email at the network level
- Conduct real-time risk analysis of networked assets
- Profile TLS encrypted traffic
- Improve threat intelligence across networks, endpoints, and cloud

Fidelis Network works across on-premises and cloud architectures to provide proactive network defense



How Network Works

You can't defend what you can't detect. Fidelis Network collects over 300 metadata attributes to provide much deeper visibility and threat detection than netflow deployments. It also identifies and classifies all networked assets and automatically calculates risk based on vulnerabilities, threat detection, security deployment, and asset priority. Combined with customizable real-time content analysis rules, you can detect and stop data theft, determine attack TTPs, perform retrospective analysis, and achieve proactive network security that keeps you a step ahead of adversaries.

Visibility and Contextual Analysis

Automatically profile and classify IT assets and services, including enterprise IoT, legacy systems, and shadow IT.

- Gain contextual visibility using cyber terrain mapping with passive identification, profiling, and classification, coupled with real-time risk analysis, vulnerability analysis, and threat detection.
- Get deep visibility into embedded, compressed, and obfuscated content, inbound and outbound, across all ports and protocols.
- Capture complete content and metadata of any network communication that violates policy, and perform analysis manually or through automation.
- Look deeper into network activity, with patented Deep Session Inspection® for direct, internal, email, web, and cloud traffic.
- Conduct packet capture (PCAP) or real-time layer 7 analysis.
- Decode content by protocol or application.
- Store metadata on-premises or in the cloud.

Automated Detection and Response

Place sensors throughout your network to detect advanced threats, lateral movement, suspicious hosts, malware, and more. Plus, analyze behavioral anomalies for faster and more accurate response.

- Derive conclusions with one solution that includes aggregated alerts, context, and evidence.
- Automate prevention and response with playbooks to enact response with EDR solutions.
- Manage traffic at ingress and egress points with Direct Sensors and gain visibility and control over how information is used (or misused) with Internal Sensors.
- Quarantine, drop, reroute, or remove attachments from email automatically using the Mail sensor.
- Automatically reroute web pages using the Web sensor.
- Stop malware intrusions, drop sessions, perform a network TCP reset, and prevent data theft.
- Expose misuse of assets and encryption, discover proxy and security circumvention, and automatically quarantine compromise assets.
- Detect internal and external threats faster, with custom protocol detection, de-obfuscation, and attack path identification.
- Compare real-time and historical data against the MITRE ATT&CK framework and intelligence feeds from Fidelis Cybersecurity and third parties to determine attack TTPs and improve response.
- Utilize risk scoring that includes behavioral and historical analytics to improve and accelerate threat hunting.
- Rely on unsupervised machine learning and automated statistical analysis to help you find threats in places you might not be looking.

Fidelis Network: Cornerstone of Proactive Cyber Defense

Sold alone or as part of the Fidelis Elevate® platform, Fidelis Network is an important step in adopting a proactive cyber defense strategy that gives you the visibility, speed and context you need to detect faster, hunt better, accelerate threat response, and stop data loss and leakage.

Fidelis Elevate is an open and extensible Active XDR platform that makes it more difficult and costly for adversaries to successfully execute their mission while making SOC teams more efficient and effective. It helps SOC analysts proactively find and stop threats before they impact business by unifying deception technologies with detection and response on endpoint (EDR), network (NDR), and cloud applications and services. Aligned with MITRE ATT&CK and MITRE Engage (formerly Shield) frameworks, Fidelis Elevate provides contextual visibility and rich cyber terrain mapping to help SOC analysts quickly detect and block attacks, perform deep inspection/analysis of the environment, assess possible compromises, and return impacted systems to normal business operations as quickly as possible. Importantly, this Active XDR platform helps answer the questions of where adversaries are lurking, how they're attacking, how to stop them now, and how to prevent future attacks.

KEY BENEFITS

Improve Visibility
Visualize your entire cyber terrain with an interactive map that's prioritized by risk. Gain bi-directional visibility of all network traffic (including TLS) across all ports and protocols.

Detect Threats Automatically
Combine deep visibility with contextual threat intelligence and automatic alerting based on rules, feeds, and anomaly detection to gain a thorough understanding of network threats at line speed and enterprise scale.

Eliminate Alert Fatigue
Automatically validate, correlate, and consolidate network alerts that provide pre-stage evidence in a single view, including suspicious network data, rich content, and files analyzed by multiple defenses, security analytics, and rules.

Unify Network Defense and Decryption
Get a clear picture of encrypted traffic with content and context in one place, allowing you to understand not just what is moving across your network, but how it's moving and who is seeing it.

Accelerate Threat Response
Automatically group related alerts to save critical time for analysts and provide malware analysis, advanced threat detection, sandboxing, network forensics, DLP, threat intelligence, and automated security rules in one unified solution.

Achieve Proactive Network Security
Improve security across networks, endpoints, and cloud and change the game on your adversaries by using Network as part of Fidelis Elevate, an Active XDR platform for proactive cyber defense.

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via rich, dynamic cyber terrain mapping and multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit www.fidelissecurity.com.