



## Why Fidelis Network?

### Threat Analysis

Cloud-based sandboxing; Network behavior analysis; New Threat intelligence automatically applied to retrospective metadata; Machine-learning based anomaly detection.

### Active Threat Detection

Automatic correlation of alerts; Threat mapping against the MITRE ATT&CK framework; High-fidelity alerts.

### Threat Hunting

Real-time content analysis; Retrospective indexed metadata; Fast, iterative, and interactive queries to test hunting hypotheses.

### Data Loss Prevention (DLP)

Data profiling and classification; Pre-built policies for known compliance regulations across network, email, and web sensors.

### Deep Session Inspection

Patented solution that looks deep into nested files; Rich content with context for deeper analysis; Full session reassembly; Protocol and application decoding; Real-time content, threat, and DLP analysis.

### 20GB 1U Sensor

Fast data processing; Less rack space.

### Email Security

Detection of internal email spray attacks for cloud SaaS (Software as a Service) email or on-premises; Pre-click URL analysis; Attachment analysis; Bi-directional quarantine; OCR image-to-text analysis.

## Part of the Fidelis Elevate®

While Fidelis Deception can be used on its own, unifying it in the Fidelis Elevate® open and active eXtended Detection and Response (XDR) platform delivers contextual visibility and rich cyber terrain mapping across the full IT landscape. These insights enable security teams to continually tune defenses and neutralize threats before they can damage business operations. They also form a foundation of intelligence to keep you ahead of the next attack.

### Profiling TLS Encrypted Traffic

Differentiation between human browsing versus machine traffic; Evolving data science models to detect hidden threats.

### Direct and Internal Sensors

Bi-directional protection against inbound and outbound advanced threats; Disruption of command-and-control communications; Prevention of data exfiltration; Active Threat Detection; Lateral movement detection; Detection of suspicious hosts; Malware detection; Anomalous behavior detection.

### Threat Intelligence

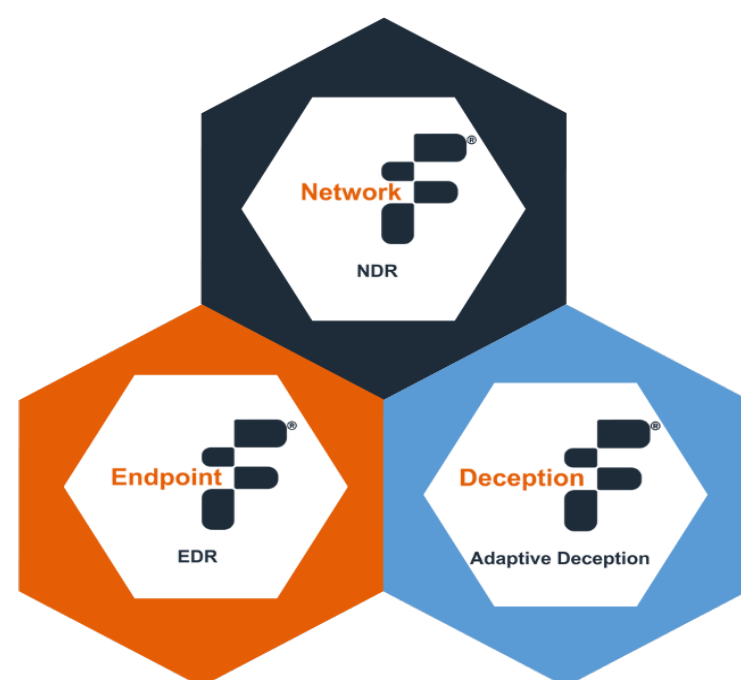
Open feeds (Fidelis Insight®, Reputation, STIX/ TAXII, YARA, Suricata); Internal threat intelligence; Custom rules and indicators.

### Flexible Deployment

On-premises hardware; virtual machine (VMware) support; Cloud deployment (customer or Fidelis Security managed).

### Integrated Deception

Automated decoy and breadcrumb deployment; High-fidelity alerting based on deception layer activity; Promotes cyber resiliency.



## About Fidelis Security®

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.



## Contact us to learn more

[www.fidelissecurity.com/contact](https://www.fidelissecurity.com/contact)  
or scan the QR Code



Copyright © 2023 Fidelis Security® LLC, All rights reserved.