Fidelis® Cybersecurity

DATASHEET

Fidelis Network®

Cornerstone Security Stack Architecture for Network, Web and Email Traffic Analysis and DLP

Much More Than It's Name

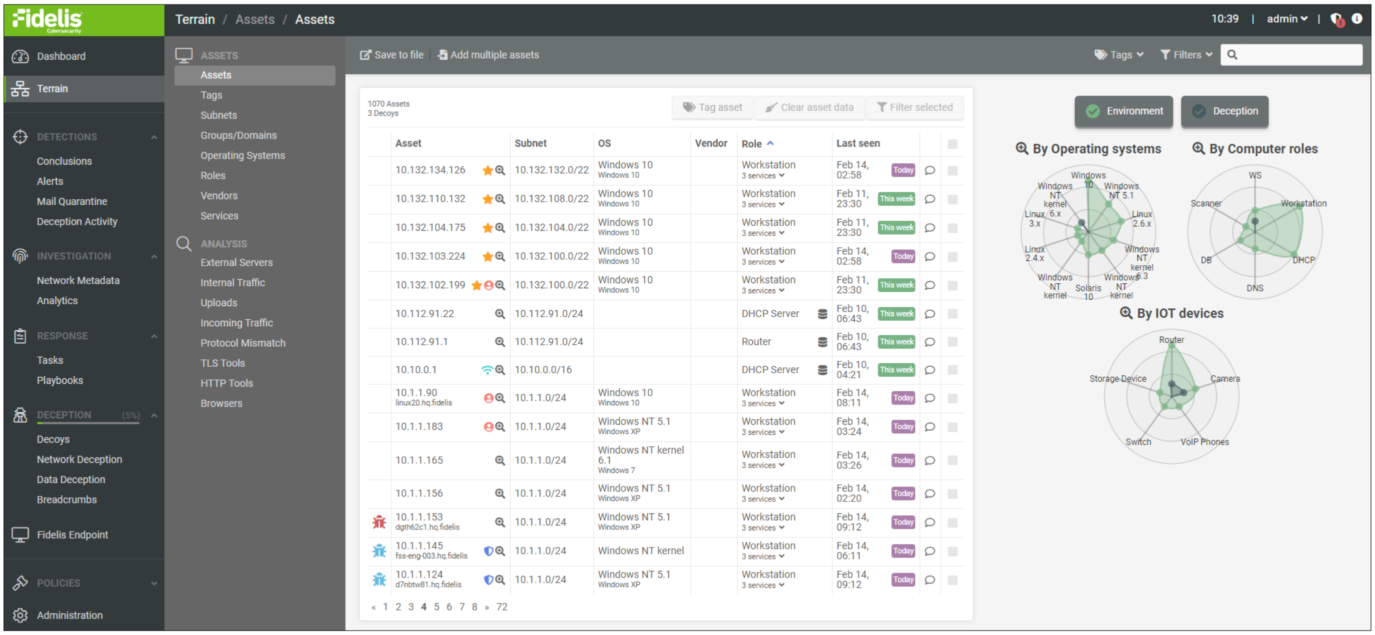
Fidelis Network goes well beyond its name by uniting real-time content analysis from five sensor locations (gateways, internal networks, email, web, and cloud) with DLP for network, email, and web traffic, plus email security including OCR of text within images. Context rich metadata also enables detection and threat hunting across a cyber terrain mapped continuously by Fidelis Network with asset profiling and classification. Open by design for threat intelligence feeds, it is the modern day core of your security stack.

Metadata as the DNA of Your Security Stack

Security information based on logs, events and alerts have their limitations. The future of machine learning and data science for security is based on rich metadata at the content and context level. And depending on real-time prevention and detection, or retrospective analysis with new threat intelligence indicators, the metadata needs to be continuous, not generated hours or days later. Fidelis Network uses patented Deep Session Inspection® (DSI) to enable full session reassembly, protocol and application decoding, deep content decoding, and content, threat and DLP analysis in real-time.

Identify, Classify, Detect, Block and Respond in One Solution

- Derive conclusions within one solution with aggregated alerts, context, and evidence
- Automate prevention, detection, investigation and response with playbooks and custom scripts
- Expose misuse of assets and encryption, plus discover proxy and security circumvention
- Custom protocol detection, de-obfuscation, attack paths, and internal threat detection
- Risk scoring with behavioral and historical analytics, plus policy and alert management
- Multi-tenant VLAN sensors with policy author permissions supporting multiple teams
- Open policy interface, plus sending alerts and data to SIEM or SOAR solutions
- FIPS 140-2 complaint for federal use



1070 Assets
3 Decoys

Asset	Subnet	OS	Vendor	Role	Last seen
10.132.134.126	10.132.132.0/22	Windows 10 Windows 10		Workstation 3 services	Feb 14, 02:58 Today
10.132.110.132	10.132.108.0/22	Windows 10 Windows 10		Workstation 3 services	Feb 11, 23:30 This week
10.132.104.175	10.132.104.0/22	Windows 10 Windows 10		Workstation 3 services	Feb 11, 23:30 This week
10.132.103.224	10.132.100.0/22	Windows 10 Windows 10		Workstation 3 services	Feb 14, 02:58 Today
10.132.102.199	10.132.100.0/22	Windows 10 Windows 10		Workstation 3 services	Feb 11, 23:30 This week
10.112.91.22	10.112.91.0/24			DHCP Server	Feb 10, 06:43 This week
10.112.91.1	10.112.91.0/24			Router	Feb 10, 06:43 This week
10.10.0.1	10.10.0.0/16			DHCP Server	Feb 10, 04:21 This week
10.1.1.90 linux20.hq.fidelis	10.1.1.0/24	Windows 10 Windows 10		Workstation 3 services	Feb 14, 08:11 Today
10.1.1.183	10.1.1.0/24	Windows NT 5.1 Windows XP		Workstation 3 services	Feb 14, 03:24 Today
10.1.1.165	10.1.1.0/24	Windows NT kernel 6.1 Windows 7		Workstation 3 services	Feb 14, 03:26 Today
10.1.1.156	10.1.1.0/24	Windows NT 5.1 Windows XP		Workstation 3 services	Feb 14, 02:20 Today
10.1.1.153 dgth62c1.hq.fidelis	10.1.1.0/24	Windows NT 5.1 Windows XP		Workstation 3 services	Feb 14, 09:12 Today
10.1.1.145 fss-eng-003.hq.fidelis	10.1.1.0/24	Windows NT kernel		Workstation 3 services	Feb 14, 06:11 Today
10.1.1.124 d7nbtw81.hq.fidelis	10.1.1.0/24	Windows NT 5.1 Windows XP		Workstation 3 services	Feb 14, 09:12 Today

« 1 2 3 4 5 6 7 8 » 72

Network Terrain Discovery and Mapping

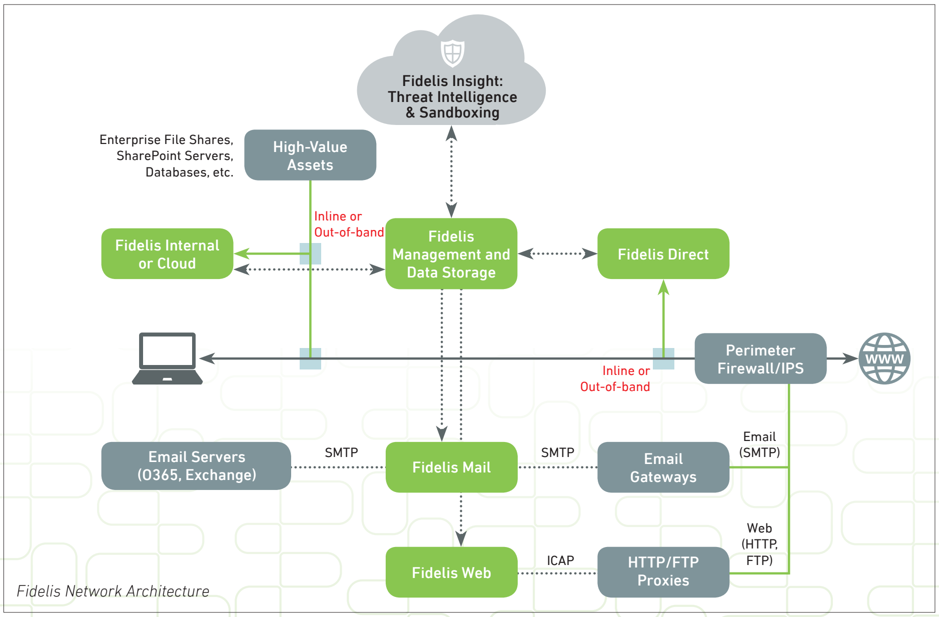
Consolidate Prevention, Detection, and Response

Building your security stack starts at the core with real-time visibility including:

- All ports and protocols with DPI, DSI (Layer7), and PCAPs
- Bi-directional analysis with full session reassembly
- Protocol, application, and deep content decoding with recursive extraction
- Direct, internal, email, web and cloud traffic sensor locations for wide visibility
- Cyber terrain asset profiling and classification including importing external sources
- Structured metadata for over 300 attributes, indexed for fast queries
- Enhanced metadata (e.g. alerts, threat intel, geo-location, policy tagging, ID2IP)
- Custom tags from content of decoded objects (e.g. author, footer, keyword)
- Metadata storage on-premises or cloud for 360+ days for retrospective analysis

The real-time visibility then enables multiple defenses within Fidelis Network including:

- **Threat Prevention** using static signatures, multi-dimensional behavior rules, threat intelligence feeds, plus emulation and heuristics
- **DLP** using data profiling and classification with pre-built policies for known compliance regulations across network, email and web sensors to alert on policy violations
- **Data Leakage/Theft** where direct and internal sensors drop sessions, email sensors quarantine, drop, re-route, or remove attachments, and web sensors redirect web pages or drop sessions
- **Email security** including internal email spray attacks for cloud SaaS email or on-premises with pre-click URL analysis, attachment analysis, and OCR image to text analysis for data leakage
- **Security analytics** based on high and low frequencies, plus sequencing analysis
- **Threat Detection** using cloud-based sandboxing, network behavior analysis, new threat intelligence automatically applied to retrospective metadata, plus machine learning anomaly detection
- **Profiling TLS** encrypted traffic based on metadata and certificates, determining human browsing versus machine traffic, plus evolving data science models to detect hidden threats
- **Threat intelligence** open feeds (Fidelis Insight, Reputation, STIX/TAXII, YARA, Suricata) plus internal threat intel including custom rules and indicators
- **Threat hunting** with real-time content analysis or retrospective indexed metadata supporting fast iterative and interactive queries to test hunting hypotheses


Fidelis Insight: Threat Intelligence & Sandboxing
Enterprise File Shares, SharePoint Servers, Databases, etc.
High-Value Assets
Inline or Out-of-band
Fidelis Internal or Cloud
Fidelis Management and Data Storage
Fidelis Direct
Perimeter Firewall/IPS
WWW
Inline or Out-of-band
Email Servers (O365, Exchange)
SMTP
Fidelis Mail
SMTP
Email Gateways
Email (SMTP)
Web (HTTP, FTP)
Fidelis Web
ICAP
HTTP/FTP Proxies

Fidelis Network Architecture

Build upon the cornerstone of Fidelis Network with the seamless integration of Fidelis Endpoint® and Fidelis Deception®.

Using Network, Endpoint and Deception products together to form the Fidelis Elevate platform provides unmatched insight into your organization's cyber terrain, including the vulnerable attack surface. Fidelis fully integrates, automates and orchestrates robust capabilities including asset discovery and classification, network data loss prevention, threat detection and response, endpoint detection and response, and deception.

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.