Fidelis® Cybersecurity

DATASHEET

# Fidelis Network®

**Network Traffic Analysis: The Cornerstone of Your Security Stack**

## Network Traffic Analysis — And More

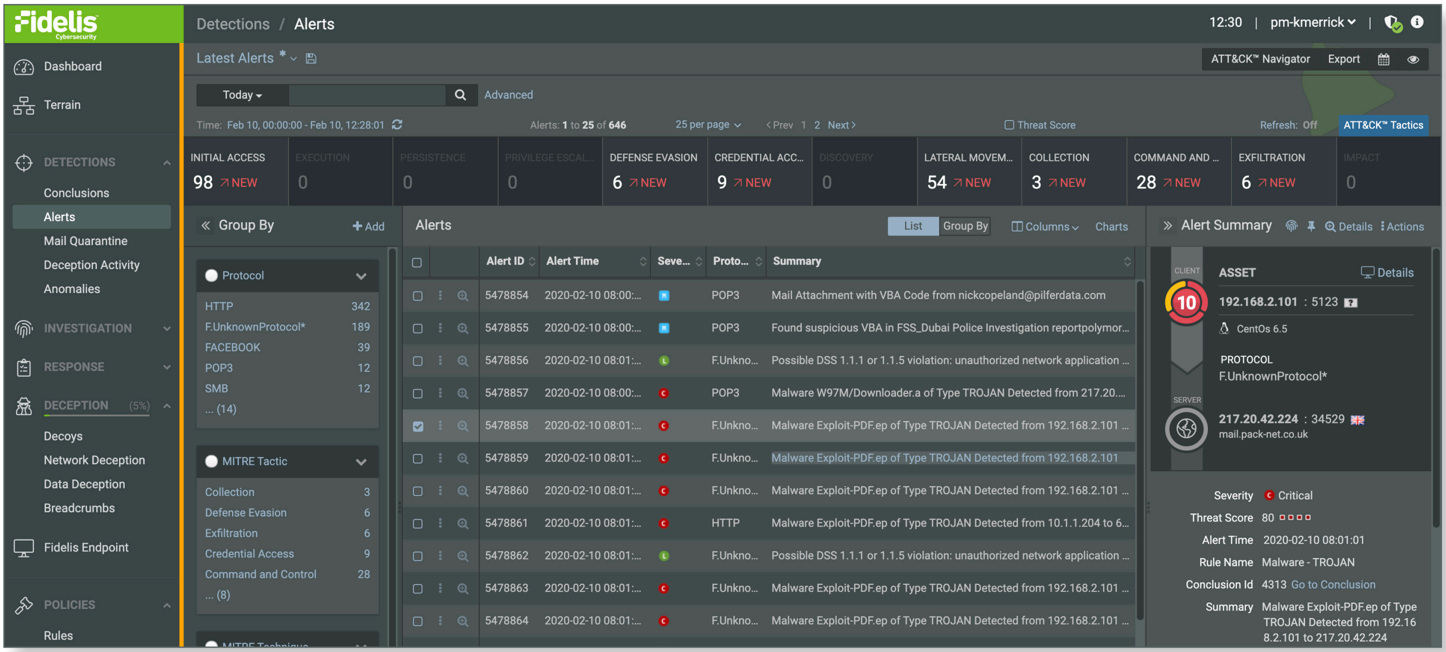
Fidelis Network goes well beyond its name by uniting real-time content analysis from five sensor locations (gateways, internal networks, email, web, and cloud) with DLP for network, email, and web traffic, plus email security including OCR of text within images. Machine-learning based anomaly detection built on top of 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.

## Key Benefits

- Map attacker TTPs to the MITRE ATT&CK™ framework for improved alert visualization and ease-of-use
- Gain bi-directional visibility of all network traffic (including TLS) across all ports and protocols
- Inspect content multiple levels deep to detect malicious activity and data loss
- Visualize the network terrain with an interactive map of device communication prioritized by risk
- Detect anomalous behavior with powerful supervised and unsupervised machine-learning models
- Aggregate alerts, context, and evidence for faster threat investigation and analysis, and reduced alert fatigue
- Know your environment by automatically profiling and classifying all networked IT assets
- Risk scoring with behavioral and historical analytics, plus policy and alert management
- Automate response via integration with Fidelis Endpoint®



Time: Feb 10, 00:00:00 - Feb 10, 12:28:01

Alerts: 1 to 25 of 646

| INITIAL ACCESS | EXECUTION | PERSISTENCE | PRIVILEGE ESCAL... | DEFENSE EVASION | CREDENTIAL ACC... | DISCOVERY | LATERAL MOVEM... | COLLECTION | COMMAND AND ... | EXFILTRATION | IMPACT |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 98 NEW | 0 | 0 | 0 | 6 NEW | 9 NEW | 0 | 54 NEW | 3 NEW | 28 NEW | 6 NEW | 0 |

| Protocol | |
|---|---|
| HTTP | 342 |
| F.UnknownProtocol* | 189 |
| FACEBOOK | 39 |
| POP3 | 12 |
| SMB | 12 |
| ... (14) | |

| MITRE Tactic | |
|---|---|
| Collection | 3 |
| Defense Evasion | 6 |
| Exfiltration | 6 |
| Credential Access | 9 |
| Command and Control | 28 |
| ... (8) | |

| □ | Alert ID | Alert Time | Seve... | Proto... | Summary |
|---|---|---|---|---|---|
| □ | 5478854 | 2020-02-10 08:00:... | M | POP3 | Mail Attachment with VBA Code from nickcopeland@pilferdata.com |
| □ | 5478855 | 2020-02-10 08:00:... | M | POP3 | Found suspicious VBA in FSS_Dubai Police Investigation reportpolymor... |
| □ | 5478856 | 2020-02-10 08:01:... | L | F.Unkno... | Possible DSS 1.1.1 or 1.1.5 violation: unauthorized network application ... |
| □ | 5478857 | 2020-02-10 08:00:... | C | POP3 | Malware W97M/Downloader.a of Type TROJAN Detected from 217.20.... |
| ☑ | 5478858 | 2020-02-10 08:01:... | C | F.Unkno... | Malware Exploit-PDF.ep of Type TROJAN Detected from 192.168.2.101 ... |
| □ | 5478859 | 2020-02-10 08:01:... | C | F.Unkno... | Malware Exploit-PDF.ep of Type TROJAN Detected from 192.168.2.101 |
| □ | 5478860 | 2020-02-10 08:01:... | C | F.Unkno... | Malware Exploit-PDF.ep of Type TROJAN Detected from 192.168.2.101 ... |
| □ | 5478861 | 2020-02-10 08:01:... | C | HTTP | Malware Exploit-PDF.ep of Type TROJAN Detected from 10.1.1.204 to 6... |
| □ | 5478862 | 2020-02-10 08:01:... | L | F.Unkno... | Possible DSS 1.1.1 or 1.1.5 violation: unauthorized network application ... |
| □ | 5478863 | 2020-02-10 08:01:... | C | F.Unkno... | Malware Exploit-PDF.ep of Type TROJAN Detected from 192.168.2.101 ... |
| □ | 5478864 | 2020-02-10 08:01:... | C | F.Unkno... | Malware Exploit-PDF.ep of Type TROJAN Detected from 192.168.2.101 ... |

CLIENT 10 ASSET
192.168.2.101 : 5123
CentOs 6.5
PROTOCOL
F.UnknownProtocol*
SERVER
217.20.42.224 : 34529
mail.pack-net.co.uk

| | |
|---|---|
| Severity | C Critical |
| Threat Score | 80 ■■■■ |
| Alert Time | 2020-02-10 08:01:01 |
| Rule Name | Malware - TROJAN |
| Conclusion Id | 4313 Go to Conclusion |
| Summary | Malware Exploit-PDF.ep of Type TROJAN Detected from 192.168.2.101 to 217.20.42.224 |

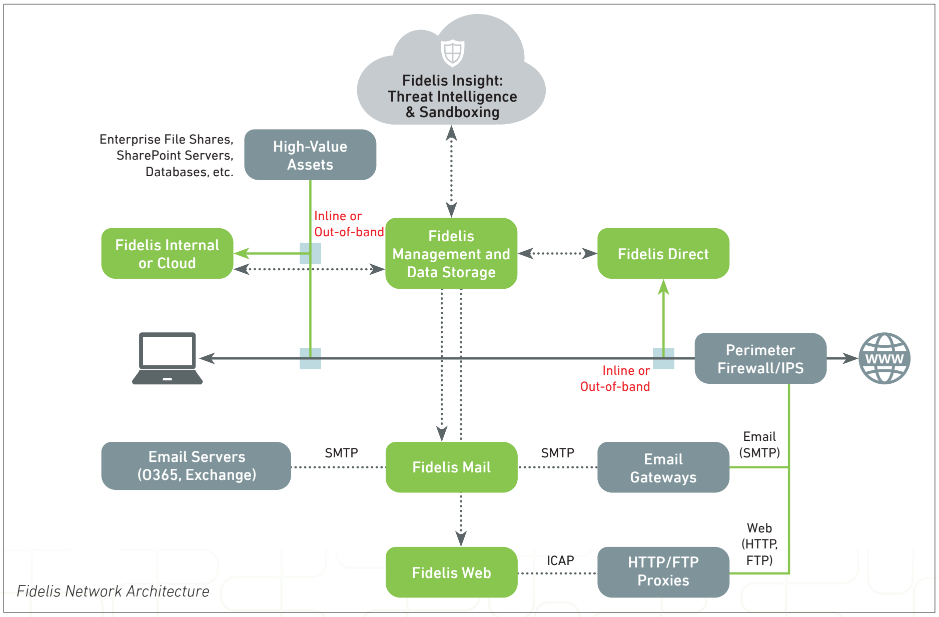
*Users gain an interactive version of MITRE ATT&CK™ with identified TTPs mapped to it for improved alert visualization and ease-of-use.*

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

You can't defend, what you can't detect. Fidelis Network provides unmatched visibility of your cyber terrain by profiling, classifying and identifying risky assets. With direct, internal, email, web and cloud sensors providing bi-directional, real-time analysis across all ports and protocols, Fidelis ensures there are no blind spots in your network. Fidelis Network also collects over 300 metadata attributes which are critical for real-time and retrospective analysis, as well as threat hunting.

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

- **Threat Detection** using cloud-based sandboxing, network behavior analysis, new threat intelligence automatically applied to retrospective metadata, plus machine learning anomaly detection
- **Threat Hunting** with real-time content analysis or retrospective indexed metadata supporting fast iterative and interactive queries to test hunting hypotheses
- **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
- **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



*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 traffic analysis, data loss prevention, 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.