DATASHEET

Fidelis Network Mail Sensor

Prevent Email-Based Threats and Data Loss, and Collect Rich Metadata

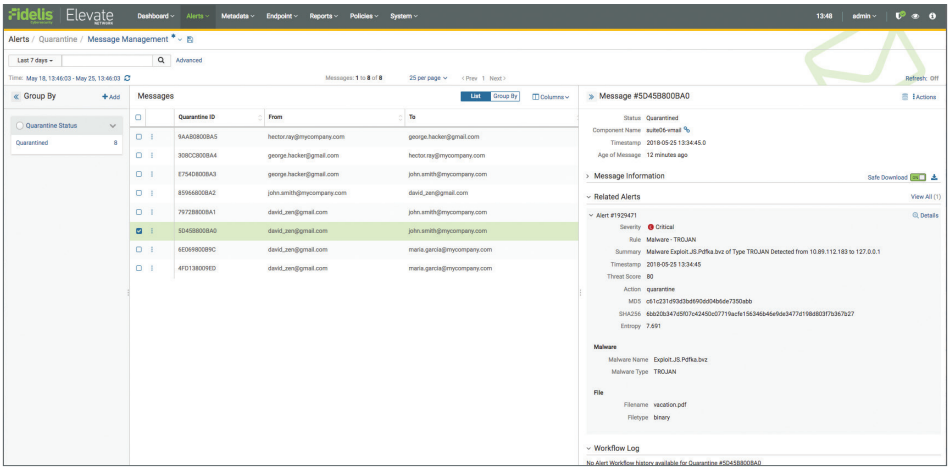
Secure Email and Stop Data Loss

Email remains a primary conduit for business communications where threats and data loss need to be prevented. More than 9 out of 10 attacks are delivered via email using phishing, macros and scripts, and social engineering for business compromise. Fidelis makes it easy to add or replace email security for threat prevention, DLP, sandboxing, and collecting rich metadata to drive detection, response, and hunting.

Product Overview

The Fidelis Mail Sensor is an integral part of Fidelis Network® that comprises of several sensors including the Direct, Internal, Mail, and Web sensors. The Fidelis Mail Sensor monitors and analyzes SMTP traffic to detect and protect against threats buried in email messages and attachments by quarantining or dropping messages that violate policy. The Mail Sensor initiates analysis once the entire email message is received from the downstream Mail Transfer Agent (MTA), so that a single action can be taken against any security violation. The Fidelis Mail Sensor can also be deployed to examine Office 365 mail traffic to and from a Microsoft Exchange® server.

Every email message is scanned in its entirety and analyzed by Fidelis' proprietary threat intelligence and Malware Detection Engine — including signature, heuristic, sandbox, and machine learning analysis — to identify any inbound and outbound threats such as malware, malicious attachments, malicious web links, and data leakage, including OCR image analysis of text.



Quarantine or prevent email delivery to stop an attack and block unauthorized data transfer in real time.

Features and Benefits

Prevent Data Theft: Quarantine or prevent mail delivery to stop the theft of or the intentional/ unintentional release of sensitive information, including OCR image analysis of text.

Detect and Investigate Retrospectively: Investigate what and where attackers have been active in the past. By collecting and storing rich content-level metadata from email (such as filenames, users, etc.), Fidelis gives you the ability to go back in time and perform retrospective analysis using current threat intelligence and quickly threat hunt on indexed metadata.

Continuous Monitoring for Email-Based Threats: Fidelis Mail Sensors track all URLs found in emails and apply pre-click analysis upon delivery, plus additional scrutiny to any subsequent related web session activity.

Turnkey Policies: Fidelis Mail Sensors come with out-of-the-box policies that provide a wide range of real-time alerts, prevention, and quarantine options as well as advanced threat detection and security forensics capabilities.

Stop Attackers: Identify an attacker or insider threat that is active on your network and unilaterally block unauthorized transfers of information in real time.

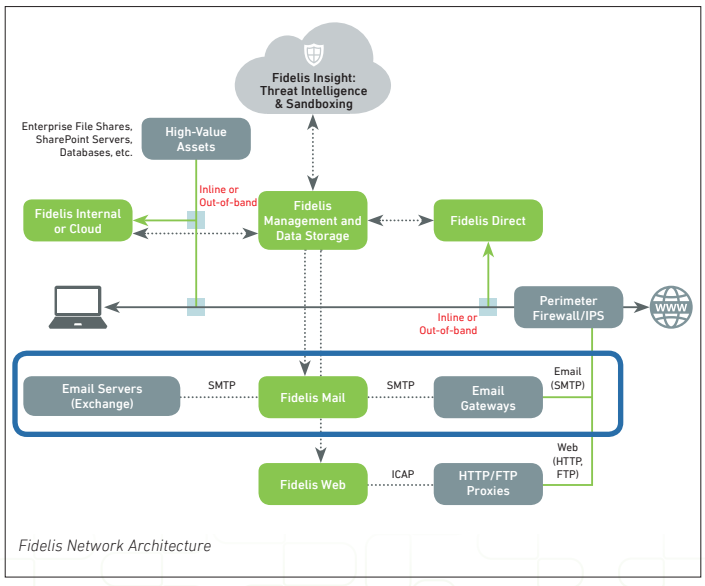
Sandboxing: Suspicious email is detained while the sandboxing capability analyzes attachments to ensure they are safe.

Fast Deployment: Typical deployments can be fully operational within a day.

When to Add Fidelis Mail Sensor to Your Network

The Fidelis Mail Sensor goes beyond traditional email security tools to inspect content and detect threats and data leakage buried deeply within email messages and attachments. While the Fidelis Network Direct Sensor detects threats across all ports and protocols with real-time access to content, the Mail Sensor ensures the prevention of email-borne threats and data loss. With the Fidelis Mail Sensor you can:

- **Analyze Emails Transmitted Over Encrypted Channels:** Email transmission encrypted using the ESMTP (SMTP over TLS) protocol can be handled directly by the sensor.
- **Quarantine Emails:** The mail sensor can quarantine an email pending further review by a system administrator or by the sender of the email. Quarantining offers guaranteed prevention with the ability to review and release (or discard) the message.
- **Prevent Email Delivery:** The Mail Sensor can choose to not accept the email from the downstream MTA or to silently discard the message without saving it for quarantine.
- **Graceful User Experience:** The Mail Sensor provides a user-friendly experience preventing email attacks. When desired, the Mail Sensor can be configured to notify the user of a security problem on outgoing email such as a quarantined email or delivery after quarantine analysis.
- **Cloud Email Visibility for Office 365:** Maintain 100% visibility of your email traffic in the cloud.



Fidelis Network Architecture

Deployment Options

The Mail sensor can be deployed in one of three modes:

- **MTA:** By serving as an MTA in the enterprise email network, the Mail Sensor can be placed in line to guarantee quarantine and prevention actions.
  - **Discard:** The email is received and then discarded.
  - **Reject:** The Sensor will reject the email. The sending MTA will be notified about the rejection and will attempt to retransmit. After several retries, the email sender will be notified about undelivered email. Notifications and retransmissions depend on the configuration of the sending MTA.
  - **Quarantine:** The email is held for analysis by a system administrator who can decide to forward or drop the email. The quarantine action can be configured to notify the sender of the email and to allow them to release the email. Appropriate quarantine actions can be configured based on the detected violation. Quarantine can be immediate, based on email inspection or can be delayed while attachments are analyzed in an execution sandbox.
- **Milter:** The Sensor is connected to an external MTA that supports the milter protocol. In this mode, the Fidelis Mail sensor receives messages from the MTA, analyzes them, and reports results to the MTA. All quarantine and prevention actions are performed and managed by the external MTA. In this mode, the Fidelis Mail Sensor is not directly in the email path.
- **BCC:** The email network can be set up to send a copy of every email to the Fidelis Mail Sensor. The sensor can analyze and alert on every message but cannot take any actions to quarantine or prevent. In this mode, the Fidelis Mail Sensor is not directly in the email path.

Fidelis Mail Sensor prevents threats and data loss, plus collects rich metadata for detection, response and threat hunting as one of five sensor locations for Fidelis Network.

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.

