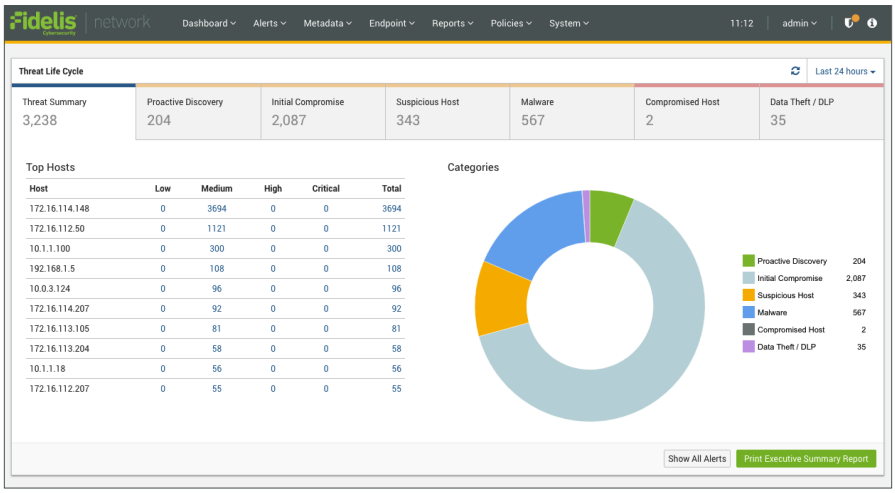
Fidelis Network Threat Evaluation

Complimentary evaluation offers visibility into threats on your network.

Overview

The Network Threat Evaluation provides a simple, straightforward option to experience the benefits of Fidelis Network™ in your own environment. Unlike other trials and proof of concept approaches, this evaluation only requires 3 to 4 hours of your time. You get results based on your actual network traffic as well as a detailed report that summarizes threats identified in your environment.



Key findings include suspicious activity across each stage of the attack lifecycle and risks that warrant further investigation.

What You Get

During this seven-day assessment, you place physical or virtual sensors on a segment of your network. Then, we analyze both inbound and outbound traffic across all application protocols (e.g. HTTP, SMTP, DNS, SMB, Oracle, MAPI) and all 65,535 ports.

At the end of the evaluation you receive two deliverables:

- **Guided Review of Findings:** Your account team will review the findings, in detail, during your assessment wrap-up meeting. In addition to explaining what the alerts mean, your account team will demonstrate the underlying data that Fidelis Network captures and how it can assist in investigating and resolving suspected security incidents.
- **Executive Summary Report:** This report summarizes and prioritizes all of the threats Fidelis Network identifies across each stage of the attack lifecycle so you can share it with other stakeholders.

Getting Started

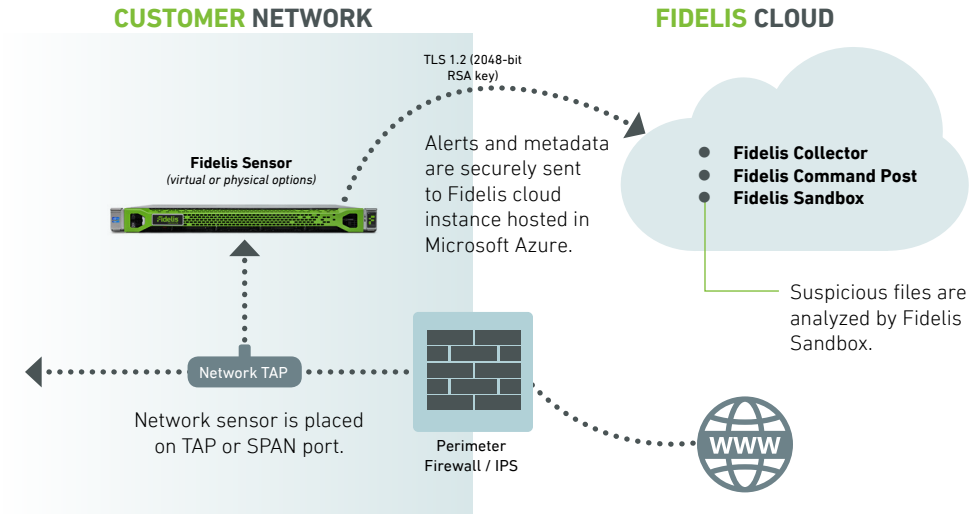
The Fidelis Network Threat Evaluation only requires 3 to 4 hours of time. Key activities required to support the evaluation include:

- Review objectives and potential outcomes
- Complete and execute an online click-through agreement
- Select a physical or virtual sensor based on required network capacity
- Deploy and configure the sensor including:
  - Provide network information to configure sensor and firewall rules
  - Ensure the sensor has two-way communication on UDP port 1194
  - Install and position the Fidelis Network sensor properly within your network
- Attend wrap-up meeting to review findings

The straightforward evaluation uses Fidelis Network to identify threats at each stage of the attack lifecycle.

How It Works

Once the sensors have been positioned in your network, our patented Deep Session Inspection® engine picks up every single packet that traverses the network, reassembles those packets into session buffers in RAM, and recursively decodes and analyzes the protocols, applications and content objects in those session buffers while the sessions are occurring. Alerts and metadata are streamed to the management console in the Fidelis Cloud where we apply Fidelis' proprietary threat intelligence to further evaluate whether attackers or malicious insiders are (or have been) present in your environment.



What We Look For

Based on our work with hundreds of organizations across every major industry, our Threat Research Team has developed a set of high-level categories to help you understand and prioritize suspicious activity. Each alert is grouped within a particular category that corresponds to different stages of the attack lifecycle. This classification accelerates your response time and helps prioritize alerts.

> "With Fidelis we are 60% more efficient in identifying compromises. We reduced response-related costs by 17% and are able to recover 50% faster from incidents."
>
> *– CISO, Financial Services Firm*

Attack Stage	Examples of What We Detect
Proactive Discovery	Alerts in this category indicate that an attack is in the earliest phases. They include signs of active reconnaissance as well as common vulnerabilities that attackers can easily identify and exploit.
Initial Compromise	This stage includes signals that attackers are trying to gain an initial foothold within the environment. Indicators we look for include spear phishing, malware sent over SMTP, webshells, drive-by attacks, botnet activity, SQL injection, the use of exploit kits.
Suspicious Host	This phase evaluates the status and behavior of your endpoints. Alerts include suspicious application behavior, applications using unusual ports and insufficient session ID entropy.
Malware	These alerts tell you when malware is present and how an attacker is using it. Indicators in this phase include advanced and commodity malware, including remote access tools (RATs), keyloggers, worms, and other suspicious executables.
Compromised Host	These alerts indicate when attackers have gained unauthorized access to an endpoint in your environment. Alerts in this phase include command and control activity, beaconing to known sinkholes, ransomware and keyloggers.
Data Theft	Alerts in this category include transfer of personally identifiable information (PII) and characteristics that are common to most data theft attempts such as the transfer of encrypted files, and communication with known exfiltration vectors.

Request a Network Threat Evaluation: **www.fidelissecurity.com/nte**

Contact Us Today to Learn More About Fidelis

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity protects the world's most sensitive data. We reduce the time it takes to detect attacks and resolve security incidents. With Fidelis you'll know when you're being attacked, you can retrace attackers' footprints and prevent data theft.

 DS_Fidelis_NTE_1609