Fidelis Network® Web Sensor

Prevent Threats and Data Loss in Proxied Web Traffic

Optimize User Experience While Preventing Threats and Data Loss

User web experience is critical, and when threats or data loss are detected, providing informative web pages on policy violations is important. While many defenses can drop sessions, the user web experience is less than optimal and may lead to IT support calls. Fidelis Web Sensor integrates with ICAP (or S-ICAP) compatible network devices and web proxies to prevent threats and data loss in web requests and replies, including encrypted web traffic if inspected by your web proxy.

Product Overview

The Fidelis Web Sensor is an integral part of Fidelis Network® that comprises of several sensors including the Direct, Internal, Mail, and Web Sensors. Fidelis Network provides deep content visibility into network, email, and web proxy traffic to reveal malicious payloads or malware in web requests and detect any data leaving your network in outbound web content. The Fidelis Network Web Sensor can be connected to an ICAP/S-ICAP (Secure ICAP) capable network or web proxy device that can pass web requests and replies over ICAP / S-ICAP for content analysis.

The Fidelis Web Sensor will analyze all received content and can direct the external network device or web proxy to prevent web requests or replies, or redirect the user away to informative policy violation web pages. Since many web proxies support the decryption of encrypted traffic, the Fidelis Web Sensor can receive decrypted web content over ICAP / S-ICAP for inspection. This enables the Web Sensor to analyze all web content — even over encrypted web sessions.

Web traffic is analyzed using Fidelis’ proprietary threat intelligence and Malware Detection Engine — including signature, heuristic, sandboxing, and machine learning analysis — to identify any inbound and outbound threats such as malware, malicious attachments, and data leakage in real-time.

Identify threats and data loss in proxy traffic
When to Add Fidelis Web Sensor to Your Network

The Fidelis Web Sensor goes beyond traditional web traffic monitoring tools by using patented technology to inspect and detect threats and data leakage buried deep within web content. While the Fidelis Network Direct and Internal Sensors detect threats across all ports and protocols, the Web Sensor ensures the prevention of threats and data loss for protocols traversing network devices or web proxies supporting ICAP / S-ICAP. If your web proxy also supports network decryption, the Web Sensor is less disruptive and seamless to the enterprise than the combination of a Direct Sensor and a network decryption server. With the Fidelis Web Sensor you can:

- **Handle Decryption:** Many web proxy servers handle decryption which allows them to send unencrypted content to the Fidelis Web Sensor securely over S-ICAP with no risk of exposure. If the web proxy supports this feature, Fidelis Web Sensor can inspect all content, even encrypted network communications traversing your web proxy in a secure manner.

- **Enforce Prevention:** The Web Sensor can gracefully enforce prevention by redirecting the user to an internal web page to inform them of the security violation and company policies. This web page can be configured as needed within the enterprise and tailored to the specific reasons for the violation. Conversely when a Fidelis Direct or Internal Sensor prevents a similar web session, the user experience appears the same as a network failure to deliver web requests and may lead to IT support calls and a less than optimal user experience.

Configuration Options

The Web Sensor can be configured to handle prevention in one of two modes:

- **Dropping the Session:** The user will receive an error response from the ICAP / S-ICAP connected network or web proxy device. This is the less preferred response to users for policy violations.

- **Redirecting the User:** If the network device is a web proxy, it can redirect the user to a web page crafted and maintained by the enterprise for policy violations. This action would lead the user to a web page that informs the user of a security violation, company policies, or any pertinent message you wish to provide. The enterprise can create many such web pages and configure the response based on the details of any particular violation. The Fidelis Web Sensor chooses the correct web page redirection based on the policy violation and system configuration (i.e. malware alert, data loss prevention alert).

What is ICAP* and RFC 3507?

ICAP, the Internet Content Adaption Protocol, is a protocol aimed at providing simple object-based content vectoring for HTTP services. ICAP is, in essence, a lightweight protocol for executing a "remote procedure call" on HTTP messages. It allows ICAP clients (i.e. network devices and web proxies) to pass HTTP messages to ICAP servers (i.e. Fidelis Web Sensor) for some sort of transformation or other processing (“adaptation”).

The server executes its transformation service (i.e. threat and malware detection, data loss and theft prevention) on messages and sends back responses to the client, usually with modified messages. The adapted messages may be either HTTP requests or HTTP responses with the option of redirecting to web pages providing information for policy violations. S-ICAP is an encrypted communications version between ICAP clients and servers (i.e. Fidelis Web Sensor) for some sort of transformation or other processing.”adaptation”.

In each case, the response is performed by the network or web proxy device based on instructions provided by the Fidelis Web Sensor over the ICAP / S-ICAP response. Prevention performance is dictated by the features of the network or web proxy device. In many cases the network or web proxy device can be configured to buffer the inbound or outgoing web request or reply and wait for an ICAP / S-ICAP response. When the web proxy is configured in this manner, prevention can be guaranteed.

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 cybercrime, 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.