Fortune 1000 Pharmaceutical Company Tightens Security with Fidelis Deception*

The Company

This Fortune 1000 pharmaceutical products company develops, manufactures, and commercializes therapies for a variety of diseases and underserved conditions. With its Global Innovation and R&D Center in North America, the company maintains advanced manufacturing operations across multiple facilities and its products are available in more than 100 countries. The company has over 15,000 employees worldwide.

Challenges

The company maintains a broad portfolio and must ensure the security of sensitive intellectual property in accordance with FDA and DEA regulations.

Information security also extends to cover communication channels within the organization as well as information that is being shared with the company's broad network of suppliers.

As intellectual property and research assets are considered 'hot commodities' on the black market, keeping them safe is the company's number one priority. The company needed a security solution that would provide accurate alerts about malware infections and unauthorized attempts to access network assets such as endpoints, servers, and data repositories.

A New Security Mindset

The scope, complexity, and pace of malicious attacks on information assets are skyrocketing. Realizing that prevention alone cannot ensure 100% protection, the security team has shifted its mindset to work under the assumption that attackers will eventually find a way into the organization. Hence, the company was looking to move beyond perimeter and endpoint prevention to a solution that would enable them to monitor their communication channels and detect any attempt to break into organizational assets.

Benefits

- Detect advanced persistent attacks in progress
- Detect zero-day attacks
- Gain critical insight about potential threats
- Better visibility of network assets and communication channels

After assessing a number of competing solutions, the company decided to choose Fidelis Cybersecurity's intelligent deception platform, Fidelis Deception. The platform came out on top as it was able to demonstrate both accurate detection of malware — some of which went undetected by other solutions — as well as clear and easy-to-understand visibility of the company's numerous communication channels.

Deception and Visibility

Fidelis Deception automatically deploys decoys that mirror network assets. The decoys 'advertise' themselves across the network to attract the attention of attackers, lure them in, and expose their activities. At the same time, Fidelis Deception tracks network traffic at egress points to provide visibility into protocols and processes.

The Deception platform is managed via a centralized, user-friendly console that empowers security analysts with actionable threat intelligence which is correlated using multiple security engines. This allows security experts to deal only with accurate, relevant, and detailed incident alerts and eliminates the need to sort through mountains of data.

*formerly Topspin DECOYnet

Active and Adaptive Defense

Fidelis Deception is designed for today's constantly evolving enterprise environments and topologies, while keeping in mind lack of resources. An easy-to-deploy solution, Fidelis Deception does not jeopardize the communication channels of the organization and does not impose a single point of failure on the organization.

In addition, it alerts network admins to cases where there are portions of the network that are only partially visible preventing a full picture of network activities.

Working out of span ports, Fidelis Deception connects to the trunk ports in the organization in order to provide the right traffic and the right context. To maximize its efficiency, the deception layer's strategy is based on the organization's traffic. This harmonizing is done automatically and adaptively based on changing traffic behaviors so as not to require any additional efforts from the administrators.

> **"With Fidelis Deception*, we're changing the rules of the game. Now we have the attackers running for cover because they understand that we can find them even if they managed to bypass our perimeter."**
>
> *~ Fortune 1000 Company, Head of Security*

"We know that attackers will never stop trying to get their hands on data, so we'll never stop staying two steps ahead of them," said the company's Head of Security. "With Fidelis Deception, we're changing the rules of the game. Now we have the attackers running for cover because they understand that we can find them even if they managed to bypass our perimeter."

*formerly Topspin DECOYnet

www.fidelissecurity.com