Fidelis Cybersecurity

CASE STUDY

Leading Technology Solutions Manufacturer Relies on Fidelis Deception* to Detect Zero-Day and APT Attacks

The Organization

The company is one of the most prestigious brands in the technology solutions market. A leading developer of cutting-edge devices, the company has over 5,000 employees and offices across North and South America, Europe, and APAC.

Information Security in a Collaborative Environment

"As a truly global organization, we implement a wide variety of 3rd-party and in-house-developed applications that encourage the sharing of ideas and designs," said the company's Information Protection Principal. "This is how we maintain our technological edge while continuously improving productivity and quality." The company also maintains numerous external communication channels for collaboration with vendors and key customers as well as across internal groups that congregate virtually anywhere in the world. Developing tomorrow's leading tech devices, the company jealously zealously guards its intellectual property and data integrity. "We take security very seriously," says the company's Information Protection Principal. "To keep our network safe, we use an array of security tools that protect thousands of end-points, maintain firewalls and DMZs, and secure access to networks while supporting cross-continent data exchange and collaboration."

The Need

As global networks grow in size and complexity, it is increasingly difficult to control access and protect data. "With so many communication channels and entry and exit points, it is extremely challenging to maintain control of security," said the company's Information Protection Principal, "and since the nature of attacks is always changing, trying to keep up with white and black lists places a burden on security personnel. Furthermore, there are so many unknown potential vulnerabilities that we have not even encountered yet."

Benefits

- Complete network traffic visibility
- Exposes threats missed by other security tools
- Detailed analysis and forensics
- Central management console with simple, intuitive UI
- Delivers quick ROI

The company needed a solution that would allow deep and wide visibility into and across their network, enabling them to understand the way traffic flows within the organization and to the Internet.

The solution would have to guide the company in assessing potential risks and security vulnerabilities. It could not interfere with the many already-installed security tools, coexisting seamlessly, and even enhancing their capabilities.

The solution would also have to identify and protect against new security threats from virtually unlimited sources, even those that were not yet known (zero day).

The Solution: Fidelis Deception

After evaluating several systems, the company selected Fidelis Deception. This solution seamlessly maps all the communication channels across and beyond the organization, tracking the flows of internal and external network traffic to expose shadow IT tools, home-grown apps, unqualified IoT devices and more.

*formerly Topspin DECOYnet

"If you don't see bad stuff in your network, you're not using the right tools. Attackers are already inside. Fidelis Deception* knows where to look and how to show you the right way to eradicate threats."

~ The company's Information Protection Principal

The solution automatically identifies the complex behavioral patterns within and across the network from the vast number of assets, and quickly creates a clear, real-time view of all communication channels and network activities.

Fidelis Deception provides a clear and accurate view of attackers' movements and activities. Not based on black and white lists, it protects against malware that has not yet been identified anywhere. New, highly complex attacks are identified and mitigated while false alarms are minimized.

Fidelis Deception provides invaluable risk-assessment data, anticipating attacker intentions based on actions, lateral movements, and access attempts. The accumulated information can be readily viewed via the user-friendly dashboard, and can be can be fed into any existing Security Information and Event Management (SIEM) software.

Fidelis Deception Brings into Focus New Insights and Behaviors Across any Network

The company's deployment of Fidelis Deception obtained eye-opening results and demonstrated immediate value. Upon installation in the data center, Fidelis Deception went to work, unobtrusively sniffing all egress traffic. Right away, it found command-and-control communication over HTTP that exhibited the characteristics of a malware tool and raised an alarm. Upon further examination, this tool was identified not as actual malware but, in fact, a remote data management tool. Despite not being white-listed, it was not detected by any of the other security solutions, only by Fidelis Deception.

*formerly Topspin DECOYnet

"Fidelis Deception has an incredible value proposition," says the company's Information Protection Principal. "It finds threats that other software simply misses. Lots of packages can help us discover white and black-listed apps. Only Fidelis Deception helps us deal with unknown unknowns — the threats that haven't even been reported yet."

As Fidelis Deception continued to run, it found several additional security events that were not detected by other defensive mechanisms installed in the network. All the while, this solution provided clear visibility of data flow, including who is uploading files from and to where, ports in use, protocols, and more. All in real time.

Benefits

Fidelis Deception delivers fast ROI and provides significant immediate and ongoing advantages. "Fidelis Deception quickly provided us with clear visibility of all the network assets, applications, and tools. The threat analysis dashboard is very intuitive, so it enables our security personnel to quickly understand what is happening across the network," says the company's Information Protection Principal.

Fidelis Deception dramatically minimizes false positives while providing actionable intelligence. By only reporting correlated quality incidents instead of thousands of events, it provides step-by-step forensics to help neutralize any threat. Because Fidelis Deception is not based on signatures or black/white lists, it is not restricted to a fixed set of malware types, but can find all untoward activity in the network.

"If you don't see bad stuff in your network, you're not using the right tools," says the company's Information Protection Principal. "Attacks are already inside. Fidelis Deception knows where to look and how to show you the right way to eradicate threats."

Contact Us Today to Learn More About Fidelis

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis is the leader in automated detection and response. The Fidelis Elevate platform dramatically improves the effectiveness and efficiency of security operations by delivering comprehensive visibility, intelligent deception, alert validation, and automated response across network and endpoints. Fidelis is trusted by the most important brands in the world. See what you've been missing. For more information go to www.fidelissecurity.com.