FireEye
SECURITY REIMAGINED

FireEye Wards Off Advanced Malware to Help Kelsey-Seybold Focus on Patient Care

CUSTOMER STORY

SECURITY
REIMAGINED

KEY COMPONENTS

- FireEye Network Threat Prevention Platform

Since 1949, Kelsey-Seybold Clinic has pioneered state-of-the-art medical care in a patient-centered environment. In 2012, the Houston, Texas based healthcare provider healthcare provider was the first in the nation to be recognized by the National Committee for Quality Assurance as an Accountable Care Organization (ACO). The designation —one among numerous awards the clinic has garnered—identifies organizations that provide efficient, coordinated care that measurably improves patient health.

Part of that effort includes safeguarding its IT assets while keeping control of administrative costs. Kelsey-Seybold has more than 3,000 employees, 375 physicians, and 23 clinics to protect. With a diverse collection of exam room PCs, laptops, and thin-client terminals—4,500 endpoints in all—staying ahead of cybercriminals is a constant battle. The clinic has kept electronic medical records since 2007 and maintains other sensitive information, including financial data for employees and patients. Protecting it is critical to the clinic's mission and business.

FIREEYE FILLS THE SECURITY GAP

To fend off a growing wave of cyber attacks, the clinic had built up a multilayered defense-in-depth security infrastructure. It went as far as blocking traffic from entire countries known for a high volume of attacks—a step it could take because of its exclusively local customer base.

Still, malware was getting through. Clinic employees would sometimes visit malicious or compromised websites. Malware on these sites sidestepped the clinic's security measures, leading to several infections and concerns that accounts could be compromised.

Kelsey-Seybold Clinic
Your Doctors for Life

COMPANY	Kelsey-Seybold Clinic
INDUSTRY	Healthcare and healthcare research
DESCRIPTION	Kelsey-Seybold is a patient-focused, multi-specialty clinic in the greater Houston area. It provides primary care and specialty medical services.
CHALLENGES	• Protecting corporate infrastructure • Blocking web-based attacks
SOLUTION	• FireEye Network Threat Prevention Platform (NX Series)
BENEFITS	• Detecting threats that its existing measures missed • Best protection against zero-day threats

> "FireEye is a very integral component of my threat-protection landscape. I have a high level of confidence in our threat protection."
>
> — **Martin Littmann,** CTO/CISO of Kelsey-Seybold Clinic

Martin Littmann, the clinic's chief technology officer and CISO, had heard of FireEye through one of its security vendors. He signed on to a proof-of-value trial of the FireEye® Network Threat Prevention Platform for web security.

The trial soon uncovered malware that Kelsey-Seybold's existing security tools had not detected. And later during the test, someone at the clinic clicked on a malicious link—which FireEye immediately detected and blocked. At that point, justifying the purchase was easy, Littmann stated.

"We looked for competitive products, and none were found," Littmann said. "I don't think anybody else has anything anywhere close to where FireEye is."

Littmann calls installation a breeze, adding that the FireEye platform integrated seamlessly with Kelsey-Seybold's legacy security tools. Those tools included a firewall, intrusion prevention system (IPS), and web gateway.

ENHANCING PROTECTION—AND REPUTATIONS

Today, FireEye plays a central role in Kelsey-Seybold's security infrastructure. Powered by the FireEye® Multi-Vector Virtual Execution™ (MVX) engine, the FireEye Network Threat Prevention Platform blocks inbound web exploits and outbound multi-protocol callbacks to stop web-based attacks.

The FireEye platform does not rely on malware binary signatures, so it identifies attacks that traditional defenses miss.

Case in point: In a typical month, FireEye generated 23 alerts—malware that had slipped past the clinic's other defenses. Out of those, 17 required no action because FireEye blocked them automatically. The remaining six were easily thwarted, thanks to clear, actionable alerts from the FireEye platform.

"We came into this with our eyes wide open," Littmann said. "And this solution is really doing what we expected it to do." FireEye is so effective at blocking attacks that Kelsey-Seybold was even able to defer an upgrade of its IPS solution, saving a significant amount of money.

"We were instrumental in pushing the solution forward to other medical centers in the Houston area," Littmann said.

For Littmann, one of the largest benefits of the FireEye platform is less tangible: "Reputation enhancement." In other words, Kelsey-Seybold's top executives can trust that the security team is keeping the clinic's systems safe—freeing up doctors and staff to focus on patients' health.

"The product works," Littmann says. "Our overall threat environment is well managed."

To learn more about FireEye, visit:
www.fireeye.com