El Camino Hospital remedies advanced threats with FireEye NX and EX solutions

Caring for information security

CUSTOMER STORY

SECURITY REIMAGINED

CUSTOMER PROFILE

El Camino Hospital is a nonprofit organization operating two facilities in the heart of California's Silicon Valley, serving communities in the extended South San Francisco Bay Area for over 50 years. The hospital relies on its staff and the deployment of advanced new technologies to achieve the stated goal of optimizing healthcare quality, service, and affordability for the benefit of its patients.

The hospital has been a leading innovator since its inception, including being recognized as implementing the world's first computer-aided medical information system, attracting attention from all over the globe. The recipient of numerous awards and accreditations, El Camino Hospital is consistently ranked among the best providers of healthcare-related services in the nation.

> "Today's cyber threat landscape is advancing so quickly that organizations need to find a new mechanism to prevent, detect, and resolve the dangers caused by these attacks."

CHALLENGES

As a healthcare provider, the hospital is subjected to many federal regulations and laws, including HIPAA, HITECH and data security standards defined by the Payment Card Industry (PCI). The organization's security team also is a staunch advocate of the HITRUST (Health Information Trust Alliance) common security framework (CSF). Hassnain Malik, CSO for El Camino Hospital, commented, "HITRUST incorporates the mandates of a broad spectrum of official bodies, so achieving compliance represents a significant demonstration of our commitment to ensuring the integrity of sensitive patient information. However, meeting the requirements obviously does require additional effort, resources, and attention to detail."

The existing environment incorporated traditional mainstream security measures but a solution needed to be identified to address the growing sophistication and volume of cyber-borne threats. "Today's cyber threat landscape is advancing so quickly that organizations need to find a new mechanism to prevent, detect, and resolve the dangers caused by these attacks," reflected Malik.

SOLUTION

Malik and his seasoned team had extensive experience across the security marketplace, so were able to move rapidly through the research and due diligence phases of the project. To achieve the levels of compliance they were targeting, a strategy was launched to deploy products from the comprehensive portfolio of security solutions from FireEye; initially the FireEye® Network Threat Prevention Platform (NX Series) and FireEye® Central Management (CM Series), followed by FireEye® Email Threat Prevention Platform (EX Series) to protect against advanced email attacks.

> "FireEye is a phenomenal solution and an integral component in our IT Security product stack. FireEye NX and EX platforms enable IT Security and Operations to expedite response to an infected device to protect the environment from advanced malware, zero-day and targeted APT attacks."

— **Hassnain Malik,** CSO, El Camino Hospital

Following a swift implementation, the scope of the FireEye deployment was expanded to include the hospital's guest wireless networks to offer patients and visitors the same levels of enhanced protection provided to internal users.

RESULTS

Robert Cotnoir, IT Security Architect for El Camino Hospital, described, "The FireEye solutions are the cornerstone of our malware and antivirus incident response strategy." All alerts are sent directly to the hospital's operations staff who follow a structured process to ensure the optimal response. Every incident generates a help desk ticket and each one is tracked through to remediation.

The FireEye CM platform has been deployed to centrally manage all devices and generate a full suite of metrics on threat-related activities. "Having all of this information centrally available has been a big time saver for us," remarked Cotnoir.

Configured in-line mode, the FireEye appliances immediately validated Malik's decision to pursue the elevated levels of compliance. "The FireEye NX platform instantly began to capture threats that had evaded the robust set of traditional data integrity measures we had in place. Our team got busy really fast!" Cotnoir recalled.

Cotnoir concluded, "We're ecstatic with FireEye, it does a phenomenal job and offers more bang for the buck than we ever anticipated. We know there are shortcomings with the end point protection suites from all vendors; FireEye fills this gap by preventing threats from ever reaching their intended destinations. I believe any company connected to the Internet that isn't using FireEye is doing themselves a huge disservice; implementing FireEye should be a mandatory part of every company's strategy!"