CYLANCE

CASE STUDY HEALTHCARE

Tufts Medical Center Takes on Cybersecurity

INDUSTRY
Healthcare

ENVIRONMENT
- 10,000 endpoints

CHALLENGES
- Protecting multiple hardware and software platforms, and industry-specific systems
- Securing endpoints against compromise and lateral intrusion techniques

SOLUTION
- Adopt CylancePROTECT® and CylanceOPTICS™ as the AV standard for the medical center, and engage Cylance ThreatZERO™ Services

TUFTS MEDICAL CENTER

The Organization

Tufts Medical Center is the oldest permanent medical facility in New England, and the third oldest in the United States. Its founding institution, the Boston Dispensary, was created in 1796 by American patriots including Samuel Adams and Paul Revere. It is now a premiere research organization and provides critical healthcare services to the Boston community.

The medical center also serves as the principal teaching hospital for Tufts University School of Medicine. The medical center cares for patients of all ages and has a full-service pediatric hospital called the Floating Hospital for Children. In addition to providing medical services, Tufts Medical Center also conducts medical and health policy research.

Tufts Medical Center is a member of Wellforce, a collaborative effort by healthcare institutions to combine both academic medicine and community care throughout Massachusetts.

The Situation

Patient safety and quality of care is of foremost importance to Taylor Lehmann, CISO of Wellforce. “Many people think of only the negative financial ramifications of having a compromised system such as having to pay up to return the system to working order,” Taylor says. For Taylor, his most important focus is to deliver on the mission of the organization, which he

says is providing “a safe system environment for our patients to receive safe, high-quality care without interruption. Making sure all of the devices, including those that play a direct role in care delivery and safety, are protected at all times”.

Tufts Medical Center selects security solutions that protect its core infrastructure while also securing its many platforms and services. Liability issues and financial loss arising from data breaches are a critical concern, but protecting the endpoints where patients receive care is vital.

“Endpoints and endpoint security are where all the action is,” Taylor says. “It’s the things that happen on those devices that need the most amount of focus if you want to disrupt an attack, even a sophisticated attack. Looking at the tools we were using in this space and looking at the tools that others use and have had success with, we came to a few conclusions: Signature-based antivirus can’t keep up with emerging attacks we see and antivirus software that needs to be online and networked to receive updates will fail. These facts create issues that prevent these solutions from performing well with attacks and never before seen threats.”

When the decision came to evaluate options that could help overcome these challenges, the organization selected CylancePROTECT, CylanceOPTICS, and ThreatZERO Services.

The Process

To get started, Taylor’s team worked with Cylance to deploy CylancePROTECT to a testbed of sixty machines. This took roughly eight hours to package and deploy. Once the initial trial period ended with positive results, CylancePROTECT was rolled out across the environment. By the end of the deployment, CylancePROTECT was present on all Windows and Linux systems. Further, Cylance installations are forthcoming for the Mac OSX systems as well as implementation of Cylance’s EDR solution, CylanceOPTICS, to select machines.

“Being deep into a platform, and then having that feature set be the same across platforms, running on a Mac as it runs on Linux as it runs on Windows, helps to ensure we have consistent visibility into protection and uniform response procedures, and that keeps things simple,” Taylor says.

The Results

During its evaluation, Tufts Medical Center’s testing showed that Cylance® identified malicious files previously undetected by existing signature-based systems. Further testing revealed a higher overall detection rate of malicious files and malware as well as a general decline in overall malware infections, once the Cylance solutions completed implementation and configuration.

Moreover, the process to deploy CylancePROTECT required less engineering time to set up and execute, providing the team with valuable time and increasing their collective ability to focus on patient-focused activities. Deploying and running CylancePROTECT has resulted in no recorded downtime to date.

These are the kinds of results Tufts Medical Center was looking for – solutions that allow the organization’s focus to remain on delivering high-quality, safe patient care without interruption.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

CYLANCE

20180807-0816