CYLANCE

Healthcare **CASE STUDY**

INDUSTRY

Healthcare

ENVIRONMENT

- 400 locations
- 10,000 endpoints
- 1.3 million patients

CHALLENGES

Reduce the number and severity of malware outbreaks

Prevent theft of personally identifiable information

Protect sensitive research and development information

Assess vulnerabilities in medical devices produced by the company

Safeguard 1.3 million patient records and comply with HIPAA regulations

SOLUTIONS

Deploy CylancePROTECT® to 10,000 endpoints

Compromise Assessment service to identify if a breach occurred

Penetration Test of medical devices and supporting infrastructure

The Company

A US-based healthcare services and product provider with over 400 locations nationwide, directly supporting over one million patients.

The Situation

Despite investing heavily in their cybersecurity infrastructure, the company routinely responded to malware outbreaks. By adopting a "detect and respond" approach, the company's IT department and security budgets were funneled into acquiring network-based detection products and chasing threats after the damage had already been done. As a large medical services and product provider, the company could not risk losing patient data or being exposed to any regulation violations.

The Process

The company's CIO decided to focus on preventive endpoint malware detection as a fundamental shift in their approach to mitigating future risks. After comparing several next-generation endpoint security products, CylancePROTECT was brought in for a pilot program.

After a successful Proof Of Concept (POC) with 250 endpoints, CylancePROTECT was deployed enterprise-wide to augment their existing endpoint security technologies. Immediately, CylancePROTECT detected and blocked three types of custom-designed malware specifically targeting their organization as well as hundreds of potentially unwanted programs (PUP) that are routinely used to assist hackers in data exfiltration.

All of their existing security solutions, including FireEye™ and Symantec™ endpoint products, completely missed detecting these files.

The Results

POC deployments of 30 days are common, but in this instance, the company moved forward with a full purchase of CylancePROTECT after just two weeks. The company then removed Symantec antivirus, as well as their Host Intrusion Prevention Systems (HIPS) products from over 9,000 endpoints. This freed up system resources and reduced end-user impact, which are common challenges for traditional endpoint solutions.

The company then engaged the Cylance Consulting team to assist in the remediation and investigation of incidents stemming from the prior malware outbreaks. At the end of the engagement, the company had zero malware or PUP infections.

The company realized additional benefits, beyond their core goal of increased malware protection, in the form of lower performance impact to each endpoint and the monetary benefit of consolidating their antivirus and HIPS solutions.

Free Consultation

Want to see how CylancePROTECT and Cylance Consulting will empower your organization in the fight against cyberattacks? Contact us today for a free consultation!

Cylance Privacy Commitment
Cylance is committed to protecting your organization against advanced threats, which includes privacy disclosure. We do not publish the names of our case study partners for this reason.

"CylancePROTECT works more effectively and efficiently than any other endpoint protection solution we evaluated. On top of that, it requires less effort to manage. Switching to Cylance has improved our company's security position without disrupting end-user workflow."

-Security Manager
Healthcare Company

+1 (877) 97DEFEND
proservices@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700 Irvine, CA 92612