CYLANCE™

CASE STUDY HEALTHCARE

Hospital Takes on Cybersecurity

INDUSTRY
Healthcare

ENVIRONMENT
- 5,000 endpoints protected by CylancePROTECT®

CHALLENGES
- Existing AV solution providing false confidence
- Malicious activity targeting endpoints

SOLUTION
- Implement CylancePROTECT to prevent malicious activity targeting endpoints before it can endanger sensitive patient and payment information, and hospital operations.

PHOENIX CHILDREN'S®

The Company

Phoenix Children's Hospital is Arizona's only children's hospital recognized by U.S. News & World Report's Best Children's Hospitals with rankings in all ten specialties. Phoenix Children's provides world-class inpatient, outpatient, trauma, emergency, and urgent care to children and families in Arizona and throughout the Southwest. As one of the largest children's hospitals in the country, Phoenix Children's provides care across more than 75 pediatric specialties. The Hospital is poised for continued growth in quality patient care, research, and medical education. For more information about the hospital, visit http://www.phoenixchildrens.org.

The Situation

Phoenix Children's CISO, Daniel Shuler, and its IT security team are responsible for protecting 5,000 endpoints in the Hospital and across more than 20 clinics in the region. Endpoints include physician and staff laptops and desktops, nursing stations, servers, Windows-based clinical devices, credit card payment processors, and point-of-sale terminals. These endpoints are used to store and/or process personal health information (PHI), and payment and credit card information. They must comply with HIPAA for PHI and voluntarily comply with the Payment Card Industry Data Security Standard (PCI-DSS) for credit card data.

The IT security team's existing industry-leading AV solution claimed to provide visibility into malicious activity aimed at the endpoints. It continuously reported all endpoints were safe, sound, and secure. This caused Daniel to be suspicious. He knew from experience that such low levels of endpoint malicious activity was highly unlikely.

5,000
ENDPOINTS
PROTECTED

The Process

Daniel and team began looking at host-based AV solutions to replace the poorly performing incumbent AV vendor. He came across Cylance in multiple venues, including a local security industry association meeting. Other association members had proofs of concept underway with Cylance with good results, so he put Cylance on the short list of vendors to consider.

Daniel and Phoenix Children's IT security team reached out to a couple advanced AV vendors and soon narrowed the options to Cylance. Phoenix Children's team was impressed Cylance could handle any malware type including unknown threats, and works on devices on and off the network. The team was also immediately satisfied with the responsiveness and support experienced with Cylance's sales and support. They feel Cylance is an extension of their team, committed to help.

The Results

The Hospital's IT security team ran a proof of concept (POC) for one month on 100 machines. From the inception of the POC, Cylance newly identified endpoint malicious activity. Among certain threats identified during this period, Cylance found a video plug-in packaged with a potentially unwanted program that was deployed on multiple machines.

This new visibility into malicious activity confirmed Daniel's suspicions about the incumbent AV system and drove the decision to replace it with Cylance. At the conclusion of the POC, the hospital engaged Cylance's ThreatZERO™ consulting team to manage the transition from its incumbent AV system to CylancePROTECT.

CylancePROTECT was initially deployed in line with the incumbent AV system. As a threat came in, the incumbent was the first line of defense — the first security layer on the endpoint to identify and repair the problem. The threat was then passed onto CylancePROTECT to prevent execution or interaction on the endpoint. Over a two-month period, the ThreatZERO team worked with the hospital security team to review potential alerts and make the necessary exceptions for internal applications. As a result of this review, the Phoenix Children's and ThreatZERO teams were able to progress to the highest policy level of Cylance protection. The end result of this engagement is a state of prevention.

Once CylancePROTECT was deployed across all endpoints and the team had enabled full protection, CylancePROTECT effectively identified and prevented a ransomware attack, an attack that could have locked up sensitive patient and payment data.

Phoenix Children's takes the security and safety of its patients very seriously, and is confident knowing its endpoints have a level of protection unattainable through other sources or vendors.

"The CylancePROTECT product outperforms others we've seen and experienced," said Daniel Shuler, Phoenix Children's CISO and Director of IT Security. "We rest a little easier knowing this level of protection is on our endpoints."

About Cylance Consulting

World-renowned experts work synergistically across our practice areas to deliver consistent, fast and effective services around the world.

- Incorporates artificial intelligence into tools and processes to more efficiently and effectively secure the environment to prevent attacks from happening
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organization
- Techniques are designed to avoid impacting operations in any way
- Integrated practice areas include ThreatZERO Services, Incident Containment and Compromise Assessments, Red Team Services, Industrial Control Systems Security, IoT and Embedded Systems, and Training

+1-844CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE™

©2018 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170214-0415