CYLANCE

CASE STUDY PHARMACEUTICAL

Pharmaceutical Company Takes on Cybersecurity

INDUSTRY
Pharmaceutical

ENVIRONMENT
- Nearly 120,000 endpoints across the globe

CHALLENGES
- Prevent zero-day and advanced persistent threats that eluded the incumbent endpoint defenses, causing a breach
- Eliminate spurious events and false positives captured by the EDR system
- Reduce the time and effort required to administer and manage endpoint defenses

SOLUTION
- Engage Cylance's Threat Research team to remediate the breach
- Decommission current endpoint security solutions
- Operationalize CylancePROTECT® on all endpoint systems using Cylance's ThreatZERO™ Services

The Company

A leading pharmaceutical company with offices, R&D laboratories, and manufacturing facilities across the globe.

The Situation

The company brought Cylance® in just days after suffering a major data breach to evaluate the extent of the damage and perform a detailed threat assessment. Cylance's Threat Research team quickly traced the initial infection to a family of advanced malware that had eluded the company's existing endpoint security systems equipped with the latest signature updates. Soon after, Cylance team members joined forces with the company's security operations team to eliminate every trace of the malware and remediate the infection.

Although the company's CISO was pleased with Cylance's Threat Research team, he still questioned whether CylancePROTECT would have outperformed the company's existing endpoint security system. He demanded objective proof that CylancePROTECT was capable of defending against that particular malware strain. In response, Cylance's Threat Response team created a test environment where systems operationalized with CylancePROTECT were exposed to the original malware strain along with several new variants. All of these systems remained infection-free. Impressed but still not fully persuaded, the CISO secured evaluation licenses and directed his security team to independently test and

120,000
ENDPOINTS
PROTECTED

> "We felt a huge sense of urgency about preventing another attack, so the deployment would have to proceed as quickly as possible with minimal impact on our business operations."

verify CylancePROTECT's capabilities. CylancePROTECT clearly demonstrated its superior effectiveness by preventing infections on every test machine.

The Process

Now convinced that the breach could have been prevented, the CISO instructed Cylance's Account team to submit a proposal to decommission the company's existing endpoint security product and operationalize CylancePROTECT on approximately 120,000 endpoints. Roughly 90,000 of these were end-user machines. The remaining 30,000 systems were business-critical R&D and manufacturing assets that were tightly regulated and isolated from the Internet. A phased deployment would be necessary, beginning with 65,000 end-user systems in the Americas and another 25,000 overseas. According to the CISO, "We felt a huge sense of urgency about preventing another attack, so the deployment would have to proceed as quickly as possible with minimal impact on our business operations." RFPs were also issued to two other cybersecurity vendors.

In addition to assessing effectiveness, evaluators would consider the frequency with which each solution required signature or model updates, whether Internet connectivity was necessary, and the overall impact of each solution on system performance. Given the time pressure and geographic complexity, Cylance's proposal included both CylancePROTECT licenses and ThreatZERO Services. After careful consideration, the company awarded the contract to Cylance and implementation planning began in earnest.

The Results

Within 60 days of launch, all end-user systems had been fully operationalized with CylancePROTECT in full blocking mode, with advanced features for memory defense, script and device control, and macro prevention enabled. Another 10,000 systems are currently being upgraded, with the remaining business-critical systems scheduled to be operational within six months. According to the CISO, "It still amazes me that CylancePROTECT can be deployed so quickly and easily. The whole process has been transparent to our end-user community and business operations alike. Of course, a lot of the credit goes to our ThreatZERO team. They're doing a fantastic job for us."

The company has seen a dramatic reduction in false positives and security events. "Before CylancePROTECT, our EDR system was collecting tens of thousands of events every day, forcing us to spend countless hours collecting, evaluating, and tracking them down. Now, we're seeing only a dozen or so, and the majority of these originate from systems that haven't been operationalized yet."

Most importantly, the company hasn't experienced a malware infection or data breach on any system running CylancePROTECT. According to the CISO, "I recently came across an SE Labs report on CylancePROTECT's Predictive Advantage, which they define as the time difference between the creation of an AI model and the first time a threat is identified. Based on their tests, CylancePROTECT has an average Predictive Advantage of 25 to 33 months. That's impressive and a strong indicator of future performance. I'm delighted to report that CylancePROTECT is everything they say it is and more."

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

CYLANCE

20190222-0136