CYLANCE

CASE STUDY ENERGY

Energy Takes on Cybersecurity

INDUSTRY
Energy

ENVIRONMENT

- Two main offices
- Multiple remote sites

CHALLENGES

- A traditional antivirus solution was failing to prevent a substantial quantity of malicious software from installing on machines, resulting in employee downtime and a continual need to reimage machines
- Applications unique to the oil and gas industry were causing numerous false positives with the company's antivirus solution
- A need to improve detection rates without impacting business continuity or taking excessive measures to lock down machines

SOLUTION

- Deploy CylancePROTECT® to all endpoints
- Remove previously deployed product from all systems

The Customer

A U.S. regional oil and gas company.

The Situation

The company was looking for a solution that would be more effective than the traditional antivirus technology it had been using for several decades. It switched antivirus technology in 2011 in a bid to improve detection rates, but the new product failed to show significant advantages and resulted in excessive latency on many machines.

The Process

The firm responded to an ad which promised that the Cylance® next-generation endpoint solution, CylancePROTECT, would have far higher efficacy in stopping malware and would not slow machines or otherwise hurt performance. The company started with a six-week Proof of Concept (POC) during which CylancePROTECT ran on a limited number of endpoints. CylancePROTECT was so successful in this initial pilot that halfway through the POC, the company chose to go ahead with an aggressive rollout, putting CylancePROTECT on all of their endpoints as quickly as possible.

The Results

The company continued to run its traditional antivirus product for about a month after deploying CylancePROTECT, but then pulled it off all systems after realizing a second solution was no longer needed. Seven months after deployment, the firm's director of information services reported that the company had not identified a single piece of malware that had gotten past CylancePROTECT.

The transition was seamless to the company's users, who were no longer interrupted by false positives and the other annoyances typically associated with deployment of a new security product.

Stop Attacks

Energy attracts sophisticated attacks. Vital to any country's national security and stability, the energy industry is a prime target for sophisticated cyberattacks. As the industry becomes more connected, attackers are taking advantage of the vulnerabilities created by the gap between IT security and operations. Cylance has built a new technology to close the gap and make it harder for attackers to penetrate critical systems.

CylancePROTECT is a next-generation antivirus product that redefines what antivirus can and should do for energy industry organizations by leveraging artificial intelligence to detect AND prevent malware from executing on every endpoint in real time.

The fundamentals of malware detection have remained the same for more than three decades. In the face of constant innovation from attackers, traditional antivirus vendors continue to focus on aging technologies that use signatures and post-attack behavior analysis to protect computers. A new approach is required.

Algorithmic science and machine learning are fundamentally shifting the equation, offering new ways to effectively identify, diagnose, categorize and control the execution of every file. Cylance is leading this revolution with predictive and preventive products such as CylancePROTECT.

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.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE™