CYLANCE™

Insurance Takes on
Cybersecurity

INDUSTRY
Insurance

ENVIRONMENT
- 2,100 employees
- 6,500 sales representatives
- 8,600 endpoints

CHALLENGES
- Address a compromise event that spanned a number of hosts
- "Detect and respond" solutions not eliminating all threats
- Replace existing, less effective traditional antivirus solutions

SOLUTION
- Zero-day malware is blocked in near real-time
- More than 30 malware variants detected and quarantined that other technologies missed
- User-friendly console took the pain out of managing deployment
- A lower total cost of ownership for a solution with greater efficacy

The Company

An insurance holding company listed on the New York Stock Exchange, which operates through its wholly-owned subsidiaries providing life insurance, annuity and supplemental health insurance products.

The Situation

The company suffered a compromise event that spanned a significant number of hosts. They were notified about the breach by an outside agency during a security assessment and were urged to seek assistance immediately. As a result of this breach, the company began evaluating endpoint security products in order to provide increased security to their infrastructure.

The insurance company previously evaluated a product platform that was based on a "detect and respond" approach to security and requested a Purchase Order (PO) from the provider. Just before completing the acquisition of this security product, the company's IT consultant suggested they evaluate CylancePROTECT® before signing the PO.

The company had several issues; first they needed to immediately block the malware used in the initial attack campaign, second they needed to ensure the rest of their infrastructure and endpoints were not compromised, and third, they needed to replace their current endpoint security product with a solution that would detect and block future malware with greater efficacy.

The Results

The Cylance solution is an elegant, yet sophisticated, approach to detecting and stopping previously "unknowable" malware, like those used in advanced persistent threat campaigns. The Cylance solution not only blocks zero-day malware in near real time, but it also provides additional context around these threats as demanded by top corporate Incident Response teams. When a company's security posture can effectively shift to prevention instead of response, the benefits are clear.

Cylance solved many of the problems the company was experiencing.

Unprecendented Malware Detection

Within minutes of a simple product demonstration, the company deployed CylancePROTECT to compromised hosts in order to test its efficacy against two existing "advanced threat" technologies. CylancePROTECT detected and blocked more than 30 malware variants that had been completely missed by Symantec Endpoint Priotection® and the Crowdstrike Falcon® platform.

Easy To Deploy and Manage

CylancePROTECT can be easily deployed using the most common software deployment solutions. A user-friendly web management console takes the pain out of managing large deployments and is accessible from anywhere with an Internet connection. CylancePROTECT can easily integrate into SIEM consoles for reporting.

Low Total Cost of Ownership

Not only does Cylance replace traditional endpoint antivirus and anti-malware products, it also precludes the need for other detection, forensic recording and host intrusion prevention technologies. It does this while reducing the need for experienced threat response teams to investigate, deconstruct and remediate attacks.

21,000
EMPLOYEES

8,600
ENDPOINTS PROTECTED

OVER 30
MALWARE VARIANTS DETECTED

The Process

After seeing a CylancePROTECT demonstration, the company was prepared to evaluate the product immediately. Within 30 minutes, CylancePROTECT was deployed on their highest-priority endpoints.

Within the first 45 minutes, CylancePROTECT found more than 30 unique pieces of malware in a live environment, on an endpoint running both Symantec™ and Crowdstrike® endpoint solutions. These 30+ samples were completely missed by the existing products and only discovered by CylancePROTECT.

The company's technical evaluator was so impressed by the product that they tested it further by transferring a large number of archived malware samples – malware that had been previously used to compromise the company – to the evaluation system running CylancePROTECT.

CylancePROTECT immediately detected and blocked both the old samples as well as the existing malware without using any signatures, heuristics or behavioral analysis. CylancePROTECT did this all without needing any type of network connection.

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

CYLANCE™