CYLANCE

**CASE STUDY** CONSUMER GOODS

# Consumer Goods Company Takes on Cybersecurity

**INDUSTRY**
Consumer Goods

**ENVIRONMENT**
- Over 3,000 endpoints on three continents

**CHALLENGES**
- Prevent ransomware attacks that eluded the incumbent antivirus
- Prevent zero-day exploits and advanced persistent threats
- Reduce the time and effort required to administer and manage endpoint defenses

**SOLUTION**
- Decommission incumbent antivirus and operationalize CylancePROTECT® on all endpoint systems

## The Company

A privately-held consumer goods company with offices, factories, and distribution facilities throughout the U.S., Europe, and the Middle East.

## The Situation

The company's CISO resolved to replace their incumbent antivirus software with a more capable solution after several of the firm's satellite offices became infected with a relatively primitive form of ransomware. Although the attacks were eventually contained, the CISO worried that a more sophisticated ransomware strain could cripple the company's ability to manufacture and ship products through its far-flung network of wholesalers and distributors. The CFO was concerned that even a short disruption could seriously impair the firm's ability to meet its quarterly revenue targets. The person responsible for maintaining the company's existing antivirus solution also weighed in, citing the challenges and time constraints caused by the constant stream of signature updates that had to be pushed out regularly to keep it up to date. According to the CISO, "We needed an endpoint security solution that would proactively prevent zero-day and advanced persistent attacks while sharply reducing our administrative overhead." He quickly assembled a cross-functional team comprised of representatives from the U.S., Europe, and the Middle East to identify and evaluate a candidate solution.

"CylancePROTECT is exactly what we needed," said the CISO. "It's extremely effective, easy to manage, and transparent to our end-users. We couldn't be more pleased."

3,000
ENDPOINTS PROTECTED

## The Process

Multiple products were considered before Cylance® and two competing solutions were invited to compete in a one-month proof of concept (POC). The evaluation would focus on three key decision criteria:

**Administration and Management Simplicity**
This would include the initial time and effort involved in product training and implementation, along with any ongoing requirements for signature and/or model updates.

**Detection Accuracy**
The team would track each solution's false positive rate and overall effectiveness in identifying and blocking malware.

**Performance and Usability**
The team would measure the CPU and memory resources consumed by each solution and their potential impact on user experience.

Once the POC was underway, it soon became apparent that CylancePROTECT was the superior solution. "CylancePROTECT detected malware that the other products completely missed and with virtually zero false positives," said the CISO. Previously, the firm had struggled to maintain the necessary heartbeat connection between its 3,000 systems and the antivirus server required by their existing solution. In contrast, "CylancePROTECT didn't require any updates or even an Internet connection to maintain its effectiveness. Once the agent was installed, CylancePROTECT went quietly about its business with minimal impact on system resources."

## The Results

At the conclusion of the POC, the team selected CylancePROTECT as the company's new endpoint security solution. "Based on our experience working with CylancePROTECT, we felt confident we'd be able to handle the implementation ourselves," said the CISO. "It took us only four weeks to decommission the existing AV solution and operationalize CylancePROTECT on all of our endpoints." Much of that time was spent cleaning systems that had previously been infected with malware and potentially unwanted programs.

Despite these successes, it took some time for the security team to fully appreciate the benefits of its new AI-powered security posture. "Our antivirus administrator had become so accustomed to rolling out signatures, he found it hard to believe that updates were no longer necessary," says the CISO. "For the first few months, he contacted Cylance support whenever the press reported a new strain of malware to make sure we were still protected. The answer was always an unqualified, 'Yes!'"

Since then, the company has not experienced a single ransomware attack or malware infection. "CylancePROTECT is exactly what we needed," said the CISO. "It's extremely effective, easy to manage, and transparent to our end-users. We couldn't be more pleased."

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

CYLANCE



20190222-0130