CYLANCE

CASE STUDY TRANSPORTATION

Bennett International Group Takes on Cybersecurity

INDUSTRY
Transportation
and Logistics

ENVIRONMENT
- Approximately 500 endpoints at 200 office, terminal, and warehouse locations throughout the U.S. and in strategic locations worldwide

CHALLENGES
- Securing information assets by preventing ransomware, zero-day malware, and advanced persistent threats
- Replacing existing AV products with a more robust and effective endpoint protection platform and endpoint detection and response solution
- Reducing the time and effort required to administer and manage endpoint defenses

SOLUTION
- Decommissioning the existing AV products
- Operationalizing CylancePROTECT® and CylanceOPTICS™ on all endpoint systems

BENNETT

The Company

Bennett International Group is a diversified, certified Women's Business Enterprise National Council (WBENC) transportation and logistics company that delivers integrated transportation and supply chain management solutions worldwide.

The Situation

As the IT administrator, Dustin Park leads a security operations center (SOC) team charged with preserving the availability and integrity of the data that fuels the company's trucking, warehousing, and logistics operations. Therefore, he was rightly concerned about the increasing prevalence of advanced malware capable of evading traditional perimeter defenses and defeating signature-based antivirus products. According to Park, "Ransomware changed the game for us. Now, we had to worry that a clerk might inadvertently open a weaponized attachment or fall victim to a phishing exploit. We needed a much more capable endpoint defense strategy."

After due consideration, Park selected a competing AV company's product that included an endpoint protection platform (EPP) and endpoint detection and response (EDR). However, Park soon discovered that these products were not as robust as he had hoped.

> "In the end, we chose CylancePROTECT and CylanceOPTICS because of their strong performance and the consummate level of skilled support and training we received from our Cylance systems engineer."
>
> **— Dustin Park, IT administrator**

The first clue came when an employee plugged a thumb drive into his web-isolated laptop and was promptly infected with CryptoLocker ransomware. "We'd been assured that the products we chose would prevent CryptoLocker from executing. As it turns out, they rely on the cloud to detect malicious hashes, so this particular strain slipped past our defenses. This was our first wake-up call that these products might not be as effective as we'd been led to believe."

The two applications also turned out to be much more difficult to manage than anticipated. According to Park, "We were never able to get the script whitelisting features to work properly. We also learned that the two products we purchased didn't play well together. I had to assign three members of my team full-time just to manage the products and the large volume of false positives they generated. Our end-users weren't happy either, complaining that the products made their systems sluggish and unresponsive. It was becoming increasingly clear that we needed to make a mid-course correction."

The Process

Park and his team resolved to replace the products that were failing with more capable EPP and EDR solutions. After meeting with several firms, he invited Cylance® and another vendor to face off in a one-month proof of concept (POC). Both companies' products would be configured in alert mode, exposed to a wide variety of advanced malware strains, and evaluated for detection accuracy, ease of configuration, efficient use of resources, and overall effectiveness. According to Park, "Both solutions performed well. In the end, we chose CylancePROTECT and CylanceOPTICS because of their strong performance and the consummate level of skilled support and training we received from our Cylance systems engineer."

Within days of completing the POC, CylancePROTECT's memory defense, script and device control, and macro prevention features had been enabled in full blocking mode. "We run the business on internally-developed applications, scripts, and macros, so whitelisting is extremely important to us. With CylancePROTECT, everything worked flawlessly."

In short order, Park and his team decommissioned their existing AV products and operationalized CylancePROTECT and CylanceOPTICS on all 500 endpoints. "We had to make some minor adjustments to the group policies we defined for the POC. Otherwise, the deployment was entirely glitch-free," said Park.

The Results

Bennett International hasn't experienced a single data breach or ransomware attack on any system operationalized with CylancePROTECT. The volume of security alerts has also plummeted to only a handful per day and Park's team is no longer contending with complaints from end-users about system performance issues. According to Park, "These operational improvements have allowed me to re-assign the three people I had managing our old AV products to more strategic threat hunting and incident response activities."

Park is particularly pleased with the seamless integration between CylanceOPTICS and CylancePROTECT. "CylanceOPTICS has proven to be an extremely capable EDR platform for us. We can see what applications are trying to do, create automated responses, and track suspect activity across all of our endpoints. In combination with CylancePROTECT, we now have the prevention, detection, and response capabilities we need to secure our business."

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

CYLANCE

20181029-1361