CYLANCE™



CASE STUDY AUTO GLASS

Safelite Takes on Cybersecurity

INDUSTRY
Auto Glass

ENVIRONMENT
- 6,000 endpoints protected by CylancePROTECT®

CHALLENGES
- Incumbent antivirus (AV) unable to protect endpoints
- Antivirus required significant labor investment to maintain

SOLUTION
- Deploy CylancePROTECT to safeguard endpoints from ransomware and other zero-day threats
- Simple and lightweight to manage with portable agent requiring only two updates per year
- Effective, continuous protection for endpoints operating both on and off the network

Safelite® AutoGlass

The Company

Safelite is a diversified services organization with 13,000 employees. As the largest auto glass repair and replacement provider in the U.S., Safelite fixes and replaces windshields through a network of more than 500 facilities in all 50 states. In addition, Safelite Group's Safelite Glass Corp. distributes materials and tools to other auto glass repair companies, and operates Safelite Solutions, which handles fleet and insurance claims processing.

The Situation

Matthew Coy, Safelite's Vice President of Information Technology, is responsible for overseeing all aspects of the company's IT infrastructure, including selecting, administering, and supporting technology products. The company handles personally identifiable information, including credit card information and insurance data collected from several sources, and must comply with insurance industry regulations and the Payment Card Industry Data Security Standard.

Safelite is the target of constant external attacks. The organization experienced ongoing security issues stemming from infected software, drive-bys and other malicious downloads. According to Matthew, "A lot of malware and email viruses were making it through the environment, all bypassing our email security and AV." Not only were the security controls ineffective, the previous AV platform required nearly 150 hours per week to manage.



Matthew knew Safelite needed to make a change, and fast. Having worked with Cylance at two previous companies, he was confident CylancePROTECT could significantly improve Safelite's endpoint security.

The Process

Matthew and his team quickly installed CylancePROTECT on a test group of 200 virtual endpoints, including Windows servers, desktops, and laptops. The Safelite environment is comprised entirely of virtual desktop infrastructures (VDIs). They operated CylancePROTECT in parallel with the incumbent AV system for several months to compare the results. Matthew said, "Cylance detected and stopped tens of thousands of events per day. Not one of them was noticed or acted upon by the existing AV system."

The members of Matthew's team were not familiar with CylancePROTECT and initially interpreted the high catch rate as an indication that the system was too sensitive and the resulting detections were not real. They believed the high number of vulnerabilities uncovered were false positives. According to Matthew, "I had high confidence that the catch rate was legitimate. The team just needed more time with the product to be convinced. The false positive rate for CylancePROTECT is effectively zero."

The team ultimately rolled out CylancePROTECT across 6,000 VDIs and 600 virtual Windows servers, including web, application, database, and email servers. Matthew noted that the Windows servers were particularly vulnerable from a security standpoint.

The Results

For Matthew, the low administration effort required to manage CylancePROTECT has resulted in significant cost savings for Safelite. He estimates that managing the incumbent AV product required 150 hours per week. This talent gap was largely filled by borrowing staff from other teams.

In the past, managing the AV product included a complex combination of monitoring, reporting, and maintaining a continuous server/agent connection. The agent required continuous updates of definition files to operate. In Safelite's environment of thousands of virtual endpoints, users are often not connected to the network or lack a viable connection. This caused the agents to fail on a regular basis, which in turn led to the continuous reinstallation of agents by the IT staff.

With CylancePROTECT, the agent is only updated every six months, and the portable agent runs entirely on the endpoint without cloud lookups. He stated, "The administrative effort for CylancePROTECT is effectively zero. It is administered by a junior-level staff member. I would venture to guess she spends less than 10 hours per month managing the operations of CylancePROTECT — install it once, and it just works."

Another important advantage of CylancePROTECT for Safelite is the way it manages agents. According to Matthew, "Competitive AV products manage multitudes of agents from a single host server. If the AV fails on the host server, all the endpoints it manages also lose protection. Cylance offers simple, clean endpoint protection – one instance on each endpoint for all device types including virtual servers, virtual endpoints, and physical devices. There is no danger of widespread failure."

Matthew stated, "CylancePROTECT is a simple and elegant product that works far better than competing solutions. It consumes no system resources, and is virtually effortless to administer."

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

CYLANCE™

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170322-0728