CYLANCE™



CASE STUDY INDUSTRIAL EQUIPMENT

B&R Enclosures Takes on Cybersecurity

INDUSTRY
Industrial Equipment

ENVIRONMENT
- 150 endpoints and 50 Windows servers protected by CylancePROTECT®

CHALLENGES
- Incumbent signature-based antivirus (AV) not effective
- Constant AV updates difficult to maintain for mobile workforce
- Unable to determine sources of ongoing ransomware attacks
- Malicious activity targeting endpoints

SOLUTION
- Deploy CylancePROTECT, leveraging artificial intelligence to detect and prevent malware, including ransomware, from executing in real time

B&R PROUDLY AUSTRALIAN

The Company

B&R Enclosures is a leading specialist in the design and manufacture of enclosures and cabinets for a wide variety of markets, including industrial, commercial, hazardous (IEC Ex certification), data/ICT, and residential in the Australasia region. B&R is the largest manufacturer of electrical and telecommunications enclosure solutions in Australia, turning over more than one million enclosures and accessories per year. The company has recently expanded into Asia and the Middle East.

The Situation

B&R Enclosures sustained two ransomware attacks. The most worrisome aspect of the attacks was the IT team's inability to determine how the attackers gained access to their systems. They only learned of the attacks when users complained they were unable to open files.

The company's Information Systems Manager, Ian van Haeringen, said they were quite fortunate — less than 1% of the company's files were affected. Considering the potential for harm, the infection was minor. The team was able to recover the files from backups and move on. Nonetheless, Ian said, "The attacks were disturbing." The ransomware attacks bypassed B&R's web gateway security and a signature-based AV solution. Ian added, "We searched through browser histories and were unable to identify the intrusion point."



150
ENDPOINTS
PROTECTED

According to Ian, "The first time we got hit with ransomware, I thought we were just unlucky. In the scheme of things, we are a private company — an SME with very little sensitive data. So, we did not consider ourselves a prime target. When the second attack occurred, I realized that we had to take this seriously."

The Process

In mid-2015, Ian and Systems Administrator James Vandenberg began looking to replace their endpoint security solution. James said, "A signature-based approach to endpoint security just did not make sense." James saw a live demonstration of CylancePROTECT and was very impressed with its ability to prevent all attack types before they could do harm. James paved the way for the management team to see a demonstration of CylancePROTECT.

Ian commented further, "We believe Cylance is the better approach to endpoint security over AV. One of the biggest reasons we selected CylancePROTECT was its ability to mitigate zero-day attacks."

After the ransomware attacks, B&R Enclosures re-evaluated its security posture, tightening down systems and putting a multi-layer defense-in-depth approach in place. The company also increased the urgency to secure their environment. This included deploying a next-generation firewall and CylancePROTECT. According to Ian, "CylancePROTECT is our second layer of defense, with the firewall as the first layer." The security team also significantly reduced employee access to certain systems and information, even for management. They also initiated a user education program.

James said, "Installation of CylancePROTECT was simple, probably one of the easiest products I have installed on an endpoint." He added that management is also easy. They do not have to worry about whether they are running the latest version on a server, because cloud-based CylancePROTECT automatically updates to the most current version. James added, "We just installed it, and it looks after itself."

Ian, James, and the rest of the IT team also like the fact that it protects laptops in the field, even when they are not connected to the network. B&R Enclosures had a fleet of 50 laptops using the previous AV solution which required special rules to keep signatures updated. According to James, "Updates were always an issue for us." Now their laptops are continuously protected both on and off the network with CylancePROTECT.

The Results

B&R Enclosures has not sustained a ransomware attack since installing CylancePROTECT. They are running in Auto Quarantine mode, and approximately a half dozen files are quarantined per month. James said, "It is usually users trying to do something they shouldn't. We check them out and most can be deleted." Because the IT team has reduced the volume of attacks, the number of new computer or server builds and associated man hours is also greatly reduced.

Ian is required to report a formal security metric to B&R's IT Steering Committee — the number of endpoints not protected. He said, "With the previous AV, there was always a reason why a certain percentage were not protected. With Cylance, we no longer have those issues. I cannot guarantee we will not be attacked, but CylancePROTECT is an important layer of our security-in-depth approach."

Ian reported, "CylancePROTECT works like we were told it would. With the way attackers and ransomware work, generally, signature-based AV is too slow. You have to wait for someone to find the problem, wait for them to look at it, work out a signature for it, and then get it back to you. We just expect CylancePROTECT to do that on the fly."

+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.

20170504-1028