CYLANCE™

CASE STUDY ENERGY SERVICES

Cape plc Takes on Cybersecurity

INDUSTRY
Energy Services

ENVIRONMENT
2500 endpoints protected by CylancePROTECT®

CHALLENGES
- Existing AV solution unable to offer protection from zero-day threats
- Ongoing ransomware attacks
- Limited resources make it difficult to manage a complex security system while remediating ongoing infections

SOLUTION
- Deploy CylancePROTECT to prevent zero-day threats, including ransomware, from successfully compromising company laptops and servers
- Use proactive protection to greatly reduce time invested in remediation efforts and free up security, infrastructure, and service delivery resources

cape Excellence delivered

The Company

Cape is an international leader in the provision of critical industrial services principally to the energy and natural resources sectors. The company's multi-disciplinary service offering includes the traditional services of access, insulation, coatings and mechanical, and a range of specialist services including oil and gas storage tanks, heat exchanger replacement and refurbishment, and environmental services. Cape's 16,400 people deliver safe, reliable, and intelligent solutions both on and offshore. International coverage extends across the U.K., Middle East, and Asia Pacific.

The Situation

As Head of Information Security and Compliance, Dave Smith oversees a team responsible for securing the organization's facilities across the U.K., as well as locations spanning the Middle East, Asia Pacific, and CIS.

Although the company had a market-leading antivirus solution in place, Dave had evidence that the endpoints were not protected from zero-day threats. In particular, they were experiencing ransomware attacks from drive-bys, browser vulnerabilities, and malicious content in email. When Cape was first experiencing localized ransomware attacks, the IT teams were spending a fair amount of time re-imaging affected machines and restoring file shares, which was time consuming. Not to mention, this significantly reduced productivity for the concerned employees. The logistics associated with Cape's remote locations meant a three-day turnaround to re-image a machine.

Cape was already considering finding a better way to secure their environment against such attacks and while they were managing the situation, it wasn't improving. When Cape was hit by a sizable ransomware attack, the urgency to find a solution increased.

The Process

Dave had begun a search for a solution capable of handling zero-day threats and ransomware. He had spoken with several major, leading security vendors and found their products to be overly complex to deploy and lacking protection for machines disconnected from the corporate WAN. During discussions with a leading global IT analyst firm, it was suggested Cape consider Cylance®.

According to Dave, "What initially attracted us to Cylance was the fact there was no investment in infrastructure, it protects endpoints on and off network across numerous remote sites with a small agent, and provides a path to rapid deployment." He further stated, "With a small security team, prevention is the best form of defense for us. We'd rather prevent an infection than have to encounter it and then remediate."

The Results

The Cape security team initially intended to run a proof of concept to test the efficacy of CylancePROTECT with a small number of machines. They soon determined there was no downside to rolling it out to all 2,500 machines globally.

During the proof of concept, the Cape team presented the ransomware that had infected their machines to CylancePROTECT. The team learned that if CylancePROTECT was in place, it would have prevented the ransomware attack. That attack took down their U.K. files shares for four hours, equating to roughly £40,000GBP or $50,100US in lost productivity.

CylancePROTECT operates transparently alongside Cape's incumbent AV system, which continues to run like a filter but requires many custom rules. CylancePROTECT continuously blocks unwanted programs, script control attempts, and other exploits, including ransomware that has slipped passed the incumbent AV system. Cape, however, plans to discontinue use of their legacy AV when the contract expires.

"Since installing CylancePROTECT, we have seen zero incidents of ransomware and zero-days, and experienced zero down time from endpoint security incidents, which is pretty impressive," Dave said. He added, "Cylance makes my life much easier!"

16,400
EMPLOYEES

2,500
ENDPOINTS
PROTECTED

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

CYLANCE™

20170519-1152