CYLANCE

CASE STUDY HIGHER EDUCATION

University of Delaware Takes on Cybersecurity

INDUSTRY
Higher Education

ENVIRONMENT

- 2,500 endpoints protected by CylancePROTECT®
- Windows and Mac laptops and desktops
- Web application and Windows email servers

CHALLENGES

- Block zero-day attacks
- Stop unknown malware
- Secure endpoints with restricted data or personally identifiable information

SOLUTION

- Deploy CylancePROTECT on endpoints used to handle personally identifiable information.

UNIVERSITY OF DELAWARE®

The Customer

One of the oldest universities in the United States, the University of Delaware traces its roots to 1743. Today, it is the largest university in the state of Delaware with 23,000 students, 4,300 employees, and the first study abroad program in the U.S. The university's faculty includes internationally known authors, scientists, and artists, and the school's campuses have state-of-the-art facilities that provide students with research-intensive, technologically advanced resources with a global impact. The school is also enriched by distinguished guest speakers, NCAA Division I intercollegiate athletics, 300-plus engaged student organizations, concerts, and other arts and cultural activities. UD's thriving study-abroad program and expanding international partnerships further enhance students' education as global citizens.

The Situation

Faced with the threat of zero-day attacks and a desire to secure student and employee personally identifiable information (PII), the university's IT staff was not satisfied with their existing signature-based cybersecurity solution. As with many organizations, the school's IT leadership was concerned about protecting the machines of people handling financial information from threats like malware that would exfiltrate PII and harm students and employees if that information was stolen.

> “When we have an infection and we walk over to the machine, we ask ourselves, ‘Why didn’t this machine have Cylance on it?’”
>
> *— Ben Miller, Manager of Technical Security, University of Delaware*

4,300
EMPLOYEES

2,500
ENDPOINTS
PROTECTED

Ben Miller, the school’s Manager of Technical Security set out to find a solution that could stop zero-day attacks and block unknown malware. Ben and Craig Prettyman, an IT Systems support consultant, spoke with and tested a number of vendors, but didn’t find any that provided the security they were looking for, or that fit well into their environment.

The Process

Fortunately, when Ben and Craig looked at Cylance®, they found a solution that not only fit well into their existing environment, but also was able to stop zero-day attacks and block unknown malware, all while running silently in the background on the endpoints that were used to process restricted data and PII. “CylancePROTECT basically did what we wanted it to do, and we were fairly happy with it,” said Ben Miller. “With flexible rollout options, we were able to meet our goal of securing our most critical endpoints. This allowed us to protect groups like HR, finance, and student data first, which would have been the most difficult and costly to recover from following a breach.”

The university’s IT team tested CylancePROTECT on a few systems by pitting the endpoints against a large number of malware samples. They were pleased to see that CylancePROTECT stopped the malware from running while having very little impact on the endpoints. “The console gave us very responsive feedback on what was going on at the endpoints,” said Craig Prettyman, “and it was nice having the ability to delegate zones to different people.”

Following the successful tests, the university originally deployed CylancePROTECT on 1,000 endpoints, and later increased that number to 2,500. The IT team initially deployed the solution in detect mode to ensure there were no issues, then once they found nothing needed to be remediated, set CylancePROTECT to full block mode to auto quarantine any potential threats.

The university is using CylancePROTECT in conjunction with McAfee. Thanks to Cylance’s ability to integrate with existing solutions, McAfee searches when files attempt to write to an endpoint’s disk, and CylancePROTECT blocks all attempts to execute. Cylance technology blocks the potentially unwanted programs and coupon installers that get by McAfee.

The Results

“CylancePROTECT works, and we’re comfortable knowing that it works,” Ben said. “Before Cylance, we had systems become infected with ransomware, but since installing CylancePROTECT, we have not had a single machine fall victim to it.”

“CylancePROTECT also stops a great deal of adware,” Craig commented. “We’ve instituted additional training for users, and their behavior has improved, but we’re still seeing a lot of adware coupon installers and risk of data exfiltration. We are confident, however, that CylancePROTECT can stop those threats because it protects against the unknown and doesn’t have to wait for something to be seen as a threat before stopping it from executing.”

The university has not had to re-image a single endpoint that has been protected by CylancePROTECT. This has allowed them to spend the time they once dedicated to re-imaging machines to other, more critical projects. UD’s IT team has a high confidence level that the systems they have in block mode using CylancePROTECT are well protected. “There have been no breaches, and no compromises,” Ben said.

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

©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.