CYLANCE

CyberSight Takes on
Cybersecurity

INDUSTRY
Higher Education

ENVIRONMENT
- 6,000 university endpoints

CHALLENGES
- High user account turnover
- Large walk-in user base
- Bring Your Own Device (BYOD) connectivity

SOLUTION
- Upgraded to CylancePROTECT® to protect infrastructure and identify system vulnerabilities

CyberSight

The Organization

CyberSight is a company dedicated to helping businesses build and maintain world class security solutions and strategies for their infrastructure. They use a three-tiered approach providing assessment services, market-leading security solutions, and security monitoring/alerting services to their customers.

By assessing the specific requirements and vulnerabilities of a given business, CyberSight can offer the most effective solution to meet their exact needs and to dramatically strengthen their security posture. CyberSight enables customers to achieve the best possible security posture by providing support throughout the process, from understanding the current risks, delivering the best possible solutions, to offering proactive managed and monitored services.

Cybersight was in contact with the University of Hull and reviewing security options when the esteemed educational institution suffered a data breach.

The Situation

John Hosegood of CyberSight was working with David Jarvis, Head of Architecture at University of Hull, on securing the organization's infrastructure. David described to John the challenging technical environment he manages. The university is exposed to numerous cyberthreats due to

the open nature of its infrastructure. Every year thousands of students enroll or graduate, leading to considerable turnover in user accounts. The university also allows visitors on their corporate network and permits BYOD connectivity. Each additional account, device, or endpoint connecting to university infrastructure increases the overall attack surface of the organization.

David and John began the process of finding the right security solution for the university. The pair attended numerous product demonstrations, carefully weighing the pros and cons of each offering. The CylancePROTECT demo left a favorable impression on the duo.

"People can deploy it (CylancePROTECT) quickly and easily, and there aren't any complaints," John observed. "Quite often, people find that running something which does not require loads of updates, in some instances, actually improves the end-user's experience. Which is awesome compared to working with legacy AVs."

Before a final decision was reached, the university suffered an automated cyberattack. The attackers distributed trojans, keyloggers, and Cryptolockers throughout the environment. Containing and eliminating the threats was a costly and time-consuming exercise. Fortunately, the encrypted files were recoverable. Locked files were restored using backup snapshots of the data, via third-party software. The lengthy recovery experience proved both exhausting and demoralizing for David and his team.

With the cleanup and recovery in full swing, David reached out to John once again. It was time to bring Cylance to the University of Hull.

The Process

The initial Cylance® rollout was limited to 200 endpoints. The results were startling with CylancePROTECT detecting over 500 threats while running in audit mode. Each threat was classified as high, medium, or low risk. This classification system helped David and his team devise a strategy for tackling the dangers already lurking in the environment. David shifted his focus to infostealers, droppers, and trojans. AdWare, which comprised many of the reports, was a secondary concern to be addressed as more resources became available.

Armed with a plan, a process, and the right tool for the job, David's team rolled CylancePROTECT out to the larger environment. During the rollout, CylancePROTECT scanned million of files and made over 3,300 detections. Three weeks after the initial test run, over 6,000 university endpoints were running in full-protect mode.

The Results

There have been no reported security breaches at the University of Hull since the installation of CylancePROTECT. The reporting capabilities of CylancePROTECT have helped highlight threat demographics and attack vectors within the environment. Gap analysis tools have assisted the university with identifying at-risk assets and fingerprinting devices. David has used this information to set up security zones and allocate security resources to areas with the greatest need.

Information provided by CylancePROTECT also holds long-term value for assisting with budgeting decisions, justifying policy changes, and tracking the health of various systems. Auditors frequently request information from David's department. CylancePROTECT has made the retrieval of relevant security information considerably easier.

CyberSight proved instrumental in bringing Cylance and the University of Hull together. The result is a safer, more secure campus for thousands of users.

CyberSight is dedicated to keeping their client's information secure by delivering measurable results. Their commitment to effective solutions makes them a valued partner of Cylance.