CYLANCE

CASE STUDY MILITARY

USO Takes on Cybersecurity

INDUSTRY
Non-profit
service organization

ENVIRONMENT
- Approximately 1,300 endpoints in over 200 locations throughout 14 countries, safeguarded by CylancePROTECT®

CHALLENGES
- Securing a wide variety of devices: kiosks, desktops, BYODs, and custom infrastructure
- Migrating to threat prevention and away from signature-based AV detection
- Protecting the USO infrastructure "from the edge"
- Monitoring a complex environment in real time
- Securing an environment with a large walk-in user base

SOLUTION
- Upgrade AV software to CylancePROTECT

The Company

The United Service Organizations Inc (USO) has provided moral and material support for uniformed soldiers of the United States since 1941. Their mission is to keep service members connected to family, home, and country. Pursuing this goal has driven the organization to expand into fourteen countries and maintain a presence on all seven continents. Today, the USO is found in over 200 locations, including airports, military bases, and un-staffed service sites in active combat zones.

The Situation

The global nature of their user base has led the USO to develop a complex IT environment. In addition to traditional network infrastructure the USO regionally deploys standalone kiosks for service member use and recently released a mobile app.

Vice President of Information Technology for the USO, Eli Hertz, realizes that each new advancement increases the overall attack surface of the organization. As USO technology evolves, Eli is committed to upholding two primary security goals:

1. Protecting information of donors who fund the organization
2. Protecting information of the servicemembers and families using USO services

200
LOCATIONS
WORLDWIDE

In 2014, Eli watched the Home Depot hack unfold in the news. Attackers used the credentials of a third-party vendor to compromise the retailer's systems. Over 7,500 point of sale terminals were infiltrated, resulting in the theft of 56 million credit card numbers. Knowing similar losses could prove catastrophic for the USO, Eli and his team began an intense analysis of their organization's vulnerabilities.

Like Home Depot, the USO works with outside vendors and supports a large walk-in user base. Eli also considered other obscure ways for threats to enter USO systems. Numerous possibilities came to mind, including the remote computer kiosks, smart panels used for room scheduling, and on-site wireless access points. Convinced that endpoint security was vital to the USO, Eli took a "protect from the edge" approach to finding a solution.

The Process

The USO acquired test licenses from Cylance® to evaluate CylancePROTECT®. For several months, the organization ran CylancePROTECT side-by-side with its existing security software. During this period, Eli and his team examined several key factors:

- Is CylancePROTECT easy to manage?
- How much control and/or configuration does CylancePROTECT allow?
- What sort of information does CylancePROTECT provide admins about the environment?
- How does CylancePROTECT perform?

The test rollout followed a cautious, three-phase process which allowed technicians to verify performance at each step. Described by Eli as a "walk-jog-run" approach, the first phase limited CylancePROTECT to providing alerts without taking further action. Once the USO had a feel for what CylancePROTECT could detect, they slowly phased in blocking and quarantining the reported threats.

As the testing period drew to a close, Eli was impressed with the results. The Cylance dashboard offered an easy and intuitive way to manage endpoint security. The roll-up view made it easier to evaluate and examine the complex security environment. The low CPU utilization of the security agents made it accessible to a wide range of hardware. Incidents of false positives were minimal, numbering only one or two cases throughout several months.

The Results

The USO does a monthly review of their security posture that includes analyzing information from the Cylance dashboard. The informative layout of the dashboard has greatly simplified the monitoring of their globally distributed architecture. Endpoints are easily managed through the detailed device reports, configurable policies, and customizable alerts.

Perhaps the most important benefit of CylancePROTECT was expressed by Eli when we asked about his new workflow.

"From a CIO perspective, I'm sleeping a little bit easier, I'll tell you that!" he said.

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

CYLANCE

20180109-0030