CYLANCE

CASE STUDY EDUCATION/RESEARCH

The Australian Museum Takes on Cybersecurity

INDUSTRY
Education, Natural History and Scientific Research

ENVIRONMENT
400 endpoints protected by CylancePROTECT®

CHALLENGES

- Antivirus systems unable to prevent malware attacks
- Securing vast amounts of sensitive historic research data

SOLUTION

- Deploy CylancePROTECT to prevent malware from executing on endpoints

AUSTRALIAN MUSEUM

The Company

The Australian Museum is the oldest museum in Australia, with an international reputation in the fields of natural history and scientific research. It was first conceived and developed along the contemporary European model of an encyclopedic warehouse of cultural and natural history, and features collections of vertebrate and invertebrate zoology, as well as mineralogy, paleontology, and anthropology. Apart from exhibitions, the museum is also involved in indigenous studies research and community programs.

The Situation

Founded in 1827, the museum has amassed a collection of more than 18 million objects. This includes a valuable physical bank of biological and cultural information preserved and made available to researchers in Australia and abroad. More than 60 scientists conduct research on and maintain detailed databases of the collection, and collaborate with other scientists around the world.

Michael Brady, the museum's Manager of ICT, oversees the Information and Communications Technology or ICT unit, which has responsibility for managing the museum's point of sales terminals, enterprise resource planning (ERP) systems, and Office365 for collaboration and business productivity. They also maintain and secure endpoint systems and staff the help desk.

“CylancePROTECT is an extremely **good value** for a solution based on predictive modeling versus signature-based AV.”

— Michael Brady, Manager of ICT

400

ENDPOINTS PROTECTED

In addition to supporting the museum’s business systems, the team manages the systems used by the scientists, including custom programs they have built to analyze, share, and maintain databases of information, such as details about the collection, research, and intellectual property. According to Michael, “Probably one of our biggest challenges is keeping the scientists’ systems protected, up-to-date, and operational as they evolve.”

The Process

The museum’s ICT team had evidence of malware bypassing its AV systems. They were using a cloud-based filtering service and found that malicious emails were circumventing security controls, so they began a search for a more effective endpoint security solution.

To test the efficacy of CylancePROTECT, the ICT team initiated a proof of concept (POC) by installing the artificial intelligence based endpoint security on 100 machines and had it run in parallel with the existing AV. During the month-long test period, CylancePROTECT scanned 19 million files. Michael told Cylance, “From that POC, we discovered that CylancePROTECT had picked up an enormous amount of dormant material that had not executed, but was on our file shares. CylancePROTECT quarantined a couple hundred different pieces of executables or software. We then embarked on a process of analyzing the quarantined files using tools within CylancePROTECT to make a decision on whether to have them remain in quarantine or release them as safe.”

The Results

The museum uses a multi-layered approach to security. They outsource protection of servers and their firewall to an MSSP, and manage endpoint security themselves with CylancePROTECT. Since installing CylancePROTECT, they have not seen any viruses execute. The team uses the Cylance dashboard to monitor how many of the PCs are collecting and quarantining malware, and what types of malware are attempting to breach their proactive defenses. They use this information to regularly update CylancePROTECT on the types of threats the museum is experiencing.

The ICT team was also concerned with managing internal threats. “We have a constant stream of new staff arriving with research and information on USBs so we have CylancePROTECT set to automatically scan those USBs. We can see from our dashboard which files are quarantined from those devices,” said Michael. “With CylancePROTECT as part of our multi-layered approach, we believe we are secure.”

According to Michael, “CylancePROTECT is an extremely good value for a solution based on predictive modeling versus signature-based AV. Artificial intelligence is exactly where we need to be going with defense because we need to be one step in front of the attackers and anticipate their next move. It doesn’t matter how they write the malicious code — predictive modeling flags the attacks for us, and that is an advantage to us.”

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

CYLANCE™