CISCO ADVANCED MALWARE PROTECTION CASE STUDY

HCL Technologies

Introduction

This case study of HCL Technologies is based on a March 2017 survey of Cisco Advanced Malware Protection customers by TechValidate, a 3rd-party research service.

"Deploying AMP for Endpoints alongside other AMP deployments has helped my organization uncover threats faster and improve overall security effectiveness."

"Organizations today are under the constant threat of cyber attack and security breaches happen every day. Given today's threat landscape, 'point-in-time' technologies, such as sandboxes or antivirus are only one part of a required solution since advanced malware can evade these defenses. Cisco AMP has provided the visibility, context, and control to not only prevent cyber attacks, but also rapidly detect, contain, and remediate advanced threats from they evaded front-line defenses and get inside."

"AMP detected 100% of exploits in testing, demonstrating its leadership in identifying the malicious software used to breach and compromise systems. AMP detected 99% of Web-based malware delivered via browsers and 98% of malware using e-mail to enter organizations. AMP detected malware employing every evasion technique tested, such as code designed to defeat sandbox and virtual machine based analysis and detection. AMP delivered faster time to detection than all other vendors."

Challenges

The business challenges that led the profiled company to evaluate and ultimately select Cisco Advanced Malware Protection:

- Chose AMP for Endpoints for the following reasons:
  - Superior protection from advanced threats and hackers
  - Rapid time to detection of threats
  - Endpoint visibility into file activity and threats
  - Ability to continuously monitor file behavior
  - Retrospective alerting to uncover stealthy attacks
  - Ability to quickly understand the threat and what it's trying to do
  - Simple, easy to use management interface

Use Case

The key features and functionalities of Cisco Advanced Malware Protection that the surveyed company uses:

- Deployed the following in addition to AMP for Endpoints:
  - AMP for Networks (AMP on Cisco Firepower NGIPS)
  - AMP for Firewall (AMP on a Cisco ASA or NGFW Firewall)
  - AMP for Web (AMP on Cisco WSA, AMP on Cisco CWS)
  - Cisco Threat Grid

Results

The surveyed company achieved the following results with Cisco Advanced Malware Protection:

- Was able to do the following with AMP for Endpoints:
  - Improve security effectiveness
  - Detect threats faster
  - Increase visibility into potential threats
  - Remediate advanced malware
  - Accelerate incident response
- Evaluated the following companies prior to signing up with AMP for Endpoints:
  - TrendMicro
  - Symantec
  - McAfee
- Prevented/Detected/Defeated the following with AMP for Endpoints:
  - Advanced malware or advanced persistent threats (APTs)
  - Zero-day threats
  - Drive-by-attacks
  - Malicious email attachments
  - File-less or memory-only malware
- Reduced threat detection time by by more than a month with AMP for Endpoints.
- Experienced improvements in the following areas after deploying AMP for Endpoints:
  - Mean time to detection of previously unseen and/or unknown threats
  - Breach probability and business risk
  - Organization's security posture
  - Executive confidence in the security of the organization
  - Investigation speed and/or quality
  - Visibility into endpoints, vulnerabilities, and threats
  - Time to remediation

Company Profile

Company:
HCL Technologies

Company Size:
Large Enterprise

Industry:
Computer Software

About Cisco Advanced Malware Protection

Get global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches with Cisco Advanced Malware Protection (AMP). But because you can't rely on prevention alone, AMP also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

Learn More:

Cisco

Cisco Advanced Malware Protection

Source: Karthikeyan NL, Senior Manager - IT Services, HCL Technologies

Research by TechValidate

Validated Published: May. 23, 2017 TVID: 287-EB5-82D