CISCO ADVANCED MALWARE PROTECTION CASE STUDY

Tennant Company

Introduction

This case study of Tennant Company 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."
>
> "We have gone from rebuilding ten to twelve devices per day to only two or three per month. This alongside with CWS has been a very effective solution to block threats."
>
> "AMP for endpoint provides full visibility 'outside' the corporate network and give us real-time telemetry on what is happening on all of our endpoints. The portal has key insight, in particular, the 'vulnerable applications' report, which helps to focus in on known problems."

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

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)
  - AMP for Email (AMP on Cisco ESA)
  - 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:
  - Prevent breaches
  - 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:
  - Palo Alto
  - FireEye
- Prevented/Detected/Defeated the following with AMP for Endpoints:
  - Advanced malware or advanced persistent threats (APTs)
  - Zero-day threats
  - Ransomware
  - Drive-by-attacks
- Reduced threat detection time by by more than 6 hours 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
  - Investigation speed and/or quality
  - Visibility into endpoints, vulnerabilities, and threats
  - Time to remediation

Company Profile

Company:
Tennant Company

Company Size:
Large Enterprise

Industry:
Industrial Manufacturing

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: Scott Shipley, IT Manager, Tennant Company

Validated Published: May. 22, 2017 TVID: 3E2-D10-7CA

Research by TechValidate