CISCO AMP FOR ENDPOINTS CASE STUDY

Fortune 500 Industrial Manufacturing Company

Introduction

This case study of a Fortune 500 industrial manufacturing company is based on a January 2020 survey of Cisco AMP for Endpoints customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

> “Cisco AMP for Endpoints has been a solid product offering. It is a robust EPP solution that provided all of the appropriate protections for our assets when we originally bought the tool, but has also continued to add advanced features and transform into more of a complete EDR tool too.”
>
> “The level of increased visibility of what was actually happening on our endpoints was astounding – the latest buzz is that the endpoint is the new perimeter. Seeing instances of Outlook launching Word, which then launched Powershell, which then ran a exact malicious command, (which AMP for Endpoints blocked!), gives us insight into what types of exposure we have, and a view of the efficacy of other aspects of our security program like our patching posture, config management, and also hammers home the efficacy of soft solutions like security awareness for the users.”

Challenges

The business challenges that led the profiled company to evaluate and ultimately select Cisco AMP for Endpoints:

- Invested in Cisco AMP for Endpoints because they:
  - Needed to protect against advanced threats
  - Needed to improve security operations efficiency
  - Wanted to increase threat detection and remediation speed and accuracy
  - Needed to be able to respond to incidents faster
  - Needed tools to enhance their threat hunting capabilities
- Considered the following vendor before selecting Cisco AMP for Endpoints:
  - Cylance

Use Case

The key features and functionalities of Cisco AMP for Endpoints that the surveyed company uses:

- Other Cisco Security products used in addition to Cisco AMP for Endpoints:
  - Threat Response
  - Threat Grid
  - AnyConnect
  - ISE (Identity Services Engine)
- Rates Cisco AMP for Endpoints on the following features:
  - Antivirus feature: blocking known malware: extremely satisfied
  - Exploit prevention feature: protecting against file-less malware: extremely satisfied
  - Threat detection and response feature: continuous file monitoring (file and device trajectory): extremely satisfied
  - Threat intelligence: ability to understand unknown threats to their environment: very satisfied
  - Multi-platform/OS support: very satisfied

Results

The surveyed company achieved the following results with Cisco AMP for Endpoints:

- Most prominent benefits realized from their investment in Cisco AMP for Endpoints:
  - Experienced faster, more effective incident response
  - Enhanced threat hunting capabilities
- Experienced the following after implementing Cisco AMP for Endpoints:
  - Reduced security risks: greater than 75%
  - Improved security operations efficiency: 50% to 74%
  - Improved threat detection and remediation speed and quality: greater than 75%
  - Improved incident response speed and effectiveness: greater than 75%
- Cisco AMP for Endpoints helped their security team to better protect their environment from:
  - Zero-day threats
  - Ransomware
  - Cryptomining
  - File-less malware
  - Drive-by-attacks
- Their confidence in protecting their endpoints against malware and other threats has significantly improved now that they have Cisco AMP for Endpoints as part of their security strategy.
- Reduced their time to detection of threats by more than a week after implementing Cisco AMP for Endpoints.

Company Profile

The company featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Company Size:
Fortune 500

Industry:
Industrial Manufacturing

About Cisco AMP for Endpoints

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 AMP for Endpoints

Source: TechValidate survey of a Fortune 500 Industrial Manufacturing Company

Research by TechValidate

✓ Validated Published: Mar. 10, 2020 TVID: 4C3-AC2-D9E