CISCO AMP FOR ENDPOINTS CASE STUDY

Perry Spencer Communications

Introduction

This case study of Perry-Spencer Communications is based on a January 2020 survey of Cisco AMP for Endpoints customers by TechValidate, a 3rd-party research service.

> "We had had two ransomware attacks before we implemented AMP for Endpoints and haven't had another one since. It works very well, is a great solution, and uses less resources than other endpoint security tools that we evaluated."

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
- Considered the following vendors before selecting Cisco AMP for Endpoints:
  - CrowdStrike
  - Carbon Black

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
  - NGFW (Next-Generation Firewall)
- 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: extremely satisfied
  - Multi-platform/OS support: extremely 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:
  - Realized better overall protection/prevention against file-less malware, ransomware, and other advanced threats
- Experienced the following after implementing Cisco AMP for Endpoints:
  - Reduced security risks: greater than 75%
  - Improved security operations efficiency: greater than 75%
  - Improved threat detection and remediation speed and quality: greater than 75%
  - Improved incident response speed and effectiveness: greater than 75%
  - Reduced costs and increased staff productivity by simplifying complex endpoint security management tasks: greater than 75%
- Cisco AMP for Endpoints helped their security team to better protect their environment from:
  - Ransomware
  - Cryptomining
- Their confidence in protecting their endpoints against malware and other threats has very 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

Company:
Perry-Spencer Communications

Company Size:
Small Business

Industry:
Professional Services

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