CISCO AMP FOR ENDPOINTS CASE STUDY

NHS Management

Introduction

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

> "Cisco AMP for Endpoints has dramatically increased our response time to threats. Reduced time spent on security operations and increased endpoint visibility."

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 vendors before selecting Cisco AMP for Endpoints:
  - Carbon Black
  - Sophos
  - TrendMicro
  - Palo Alto Networks

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
  - Umbrella
  - Email Security
  - Threat Grid
  - Stealthwatch
  - NGFW (Next-Generation Firewall)
  - AnyConnect
  - ISE (Identity Services Engine)
- Rates Cisco AMP for Endpoints on the following features:
  - Antivirus feature: blocking known malware: very 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: 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
  - Improved security operations efficiency
  - Experienced faster and more accurate threat detection and remediation
  - 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: 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: less than 10%
- 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 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 up to 12 hours after implementing Cisco AMP for Endpoints.

Company Profile

Company:
NHS Management

Company Size:
Large Enterprise

Industry:
Healthcare

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: Cole Twobears, IT Architect, NHS Management

Validated Published: Mar. 11, 2020 TVID: 143-20B-E93

Research by TechValidate by SurveyMonkey