CISCO AMP FOR ENDPOINTS CASE STUDY

Meso Scale Diagnostics

Introduction

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

> “Using AMP for endpoints has gotten us one step closer to our goal of single pane of glass monitoring for all of our security technologies, which has reduced the amount of time it takes to monitor and react to incidents. Investigations are also a lot quicker and easier.”
>
> “Easy to deploy and manage and we have been successful in protecting our endpoints completely.”
>
> “Not a single malware/virus infestation that has needed any remediation or re-imaging has occurred since adopting AMP for Endpoints.”

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
  - Needed a tool that interacts with other security tools such as Next Gen firewalls, web and email security appliances.
- Considered the following vendors before selecting Cisco AMP for Endpoints:
  - CrowdStrike
  - Carbon Black
  - McAfee
  - Symantec
  - 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:
  - Umbrella
  - Email Security
  - Threat Grid
  - NGFW (Next-Generation Firewall)
  - AnyConnect
  - Web Security (Ironport)
- Rates Cisco AMP for Endpoints on the following features:
  - Antivirus feature: blocking known malware: very satisfied
  - Exploit prevention feature: protecting against file-less malware: very satisfied
  - Threat detection and response feature: continuous file monitoring (file and device trajectory): very 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:
  - Realized better overall protection/prevention against file-less malware, ransomware, and other advanced threats
  - Improved security operations efficiency
- 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: 50% to 74%
  - Reduced costs and increased staff productivity by simplifying complex endpoint security management tasks: 50% to 74%
- 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
  - Understanding file trajectories and isolation requirements.
- 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

Company:
Meso-Scale Diagnostics

Company Size:
Medium Enterprise

Industry:
Pharmaceuticals

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: Vivek Mathur, Network and Security Architect, Meso-Scale Diagnostics

Research by TechValidate by SurveyMonkey

✓ Validated Published: Mar. 9, 2020 TVID: E62-C94-E04