

Saudi Arabia National Guard

Introduction

This case study of Saudi Arabia National Guard (SANG) is based on an April 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.”

“AMP for Endpoint increased endpoint visibility by 90%, detected 90% more threats, and reduced incident response time to less than a day.”

“AMP for Endpoints is awesome APT for endpoints!”

Challenges

The business challenges that led the profiled organization to evaluate and ultimately select Cisco Advanced Malware Protection:

- Chose AMP for Endpoints for the following reasons:
 - Superior protection from advanced threats and hackers
 - Endpoint visibility into file activity and threats
 - Ability to continuously monitor file behavior
 - Simple, easy to use management interface

Use Case

The key features and functionalities of Cisco Advanced Malware Protection that the surveyed organization uses:

- Deployed the following in addition to AMP for Endpoints:
 - AMP for Networks (AMP on Cisco Firepower NGIPS)
 - Cisco Threat Grid

Results

The surveyed organization achieved the following results with Cisco Advanced Malware Protection:

- Was able to do the following with AMP for Endpoints:
 - Improve security effectiveness
 - Prevent breaches
 - Increase visibility into potential threats
- Evaluated the following company prior to signing up with AMP for Endpoints:
 - TrendMicro
- Prevented/Detected/Defeated the following with AMP for Endpoints:
 - Advanced malware or advanced persistent threats (APTs)
 - Zero-day threats
 - Ransomware
 - Malicious email attachments
- Reduced threat detection time by by more than an hour 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
 - Executive confidence in the security of the organization
 - Visibility into endpoints, vulnerabilities, and threats
 - Fewer false alerts
 - Time to remediation

Organization Profile

Organization:
Saudi Arabia National Guard (SANG)

Organization Size:
Federal

Industry:
Government

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](#)