



CISCO ADVANCED MALWARE PROTECTION CASE STUDY

# Abu Dhabi Gas Development Company Limited

## Introduction

This case study of Abu Dhabi Gas Development Company Limited is based on a March 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 Endpoints has successfully mitigated all ransomware attacks within the last 2 years of deployment. It has also provided increased visibility across all of the endpoints and also reduces my response time to incidents down to hours. ”

“AMP for Endpoints gives in a simple dashboard – without a lot of technical language – the threats, details, and actions that need to be taken. It also has the technical breakdown of threats and technologies for advanced users. It provides information about threats in a simple to understand manner.”

## Challenges

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

- Chose AMP for Endpoints for the following reasons:
  - Endpoint visibility into file activity and threats
  - Retrospective alerting to uncover stealthy attacks
  - Ability to quickly understand the threat and what it's trying to do
  - Simple, easy to use management interface

## Use Case

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

- Deployed the following in addition to AMP for Endpoints:
  - AMP for Networks (AMP on Cisco Firepower NGIPS)
  - AMP for Firewall (AMP on a Cisco ASA or NGFW Firewall)
  - AMP for Email (AMP on Cisco ESA)
  - Cisco Threat Grid

## Results

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

- Was able to do the following with AMP for Endpoints:
  - Improve security effectiveness
  - Prevent breaches
  - Detect threats faster
  - Increase visibility into potential threats
  - Remediate advanced malware
  - Accelerate incident response
- Evaluated the following company prior to signing up with AMP for Endpoints:
  - Palo Alto
- Prevented/Detected/Defeated the following with AMP for Endpoints:
  - Advanced malware or advanced persistent threats (APTs)
  - Ransomware
  - Malicious email attachments
- Experienced improvements in the following areas after deploying AMP for Endpoints:
  - Breach probability and business risk
  - Executive confidence in the security of the organization
  - Investigation speed and/or quality
  - Visibility into endpoints, vulnerabilities, and threats
  - Time to remediation

### Company Profile

Company:  
**Abu Dhabi Gas Development Company Limited**

Company Size:  
**Large Enterprise**

Industry:  
**Energy & Utilities**

### 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](#)

Source: Oluyemi Oshunkoya, Senior IT Architect, Abu Dhabi Gas Development Company Limited

Research by TechValidate

Validated Published: May. 22, 2017 TVID: DB7-CE2-603