Case Study: State & Local Government

Introduction

This case study of a state & local government is based on a June 2014 survey of Cisco Stealthwatch customers by TechValidate, a 3rd-party research service. The profiled organization asked to have their name blinded to protect their confidentiality.

> "Cisco provides the network visibility to help my staff see cyber threats data flow trends and improve our network troubleshooting."

Challenges

- Purchased Cisco because it is differentiated from competitive products in the following areas:
  - Advanced behavioral detection
  - Flow analytics

Use Case

- Uses Stealthwatch with:
  - Firewalls
  - IDS / IPS
- Is doing the following with Stealthwatch by Cisco deployment:
  - Monitoring a centralized network with a large number of satellite or retail locations
  - Monitoring traffic within a data center, physical and virtual

Results

- The following are the greatest benefits of the internal visibility provided by Cisco Stealthwatch:
  - Earliest detection of advanced threats (APTs, malware, etc.)
  - Faster Incident response
  - Forensics
  - Monitors individual user activity & mobile devices
  - Continuous internal monitoring
  - Contextual & situational awareness
- Agrees that Stealthwatch's user/host-level information is critical for the following:
  - Security
  - Performance monitoring
  - Forensics
  - Network troubleshooting
- Rated Stealthwatch's effectiveness in the following areas:
  - detecting DDoS: effective
  - accelerating incident response and forensics: effective
  - detecting advanced persistent threats: extremely effective
  - detecting insider threats / Suspicious behavior: extremely effective
  - detecting malware / zero-day attacks: effective
- Rated how critical Cisco Stealthwatch is for the following:
  - Monitoring visibility: very critical
  - Improving security: very critical
  - Managing cyber security: very critical
  - Responding to cyber threats : very critical
- Selected Stealthwatch by Cisco over the following vendors:
  - Riverbed Cascade / Mazu Networks
  - NetScout
  - Fluke / Visual Network systems
  - Open source solution

Organization Profile

The organization featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Organization Size:
State & Local

Industry:
Government

About Cisco Stealthwatch

With Stealthwatch, organizations can improve both network security and performance, and avoid the high costs associated with downtime, security breaches and other issues.

Learn More:

Cisco

Cisco Stealthwatch

Source: TechValidate Survey of a State & Local Government

Validated Published: Jan. 10, 2017 TVID: 1D5-264-B1A

Research by TechValidate by SurveyMonkey