Case Study: Medium Enterprise Banking Company

Introduction

This case study of a medium enterprise banking company is based on a June 2014 survey of Cisco Stealthwatch customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

> "By increasing visibility into our network we are able to correlate data between our network TAPs and Firewall information to generate a 'larger view' of whats really going on in the network and from where."

Challenges

- Purchased Cisco because it is differentiated from competitive products in the following areas:
  - Scalability up to 3 million flows per second
  - Flow analytics
  - Value for price
  - Customer support
  - IPv6 and Cisco ISE integration!!!!

Use Case

- Uses Stealthwatch with:
  - SIEM
  - Firewalls
  - Full-packet capture system
  - ISE
- 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:
  - Faster Incident response
  - Forensics
  - Monitors individual user activity & mobile devices
  - Continuous internal monitoring
  - Contextual & situational awareness
  - Meets auditing & compliance requirements
  - Cross-department collaboration
  - Integration with Cisco ISE
- Agrees that Stealthwatch's user/host-level information is critical for the following:
  - Security
  - Performance monitoring
  - Network troubleshooting
- Rated Stealthwatch's effectiveness in the following areas:
  - detecting DDoS: extremely effective
  - accelerating incident response and forensics: extremely effective
  - detecting advanced persistent threats: extremely effective
  - detecting insider threats / Suspicious behavior: extremely effective
  - detecting malware / zero-day attacks: extremely 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:
  - Arbor Networks
  - NetScout
  - Plixer
  - Orion which is currently in place.

Company Profile

The company 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.

Company Size:
Medium Enterprise

Industry:
Banking

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 Medium Enterprise Banking Company

Research by TechValidate by SurveyMonkey

Validated Published: Jan. 10, 2017 TVID: 391-B67-68B