Case Study: Large Enterprise Professional Services Company

Introduction

This case study of a large enterprise professional services company is based on a August 2015 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.

> "We were able to increase our visibility into all of our remote offices by adding a single flow sensor in each location. We can now monitor network performance and security events using one platform. We typically use StealthWatch to remediate events generated from within Stealthwatch and also from our IDS. The ability to search on a name or IP address allows us to identify and locate the source of an issue very quickly."
>
> "The design and implementation of the solution fits perfectly within my firm. The ability to monitor performance and security using deep packet inspection and netflow within the same product helps us respond quickly to events on the network. The platform is very stable and the ability to keep data for a year is critical when trying to research an event."

Challenges

- Stealthwatch has helped improve the following:
  - Real-time threat detection
  - Incident response
  - Forensic investigations
  - Overall security posture
  - Network troubleshooting

Use Case

- Stealthwatch has helped with:
  - Insider threats
  - APTs
  - Malware/zero-day attacks
  - DDoS attacks
  - Compliance
  - Network performance
  - Network segmentation
- Is able to secure the following with Stealthwatch:
  - Virtual infrastructure/private clouds
  - The data center
  - Remote locations

Results

- Reduced their network and security troubleshooting time by days.
- Stealthwatch System has helped their organization achieve the following:
  - Greater network visibility
  - Heightened threat intelligence
  - Enhanced visibility in the data center
  - Improved user identity awareness
  - Increased application awareness
- Found the following Stealthwatch capabilities to be the most beneficial:
  - Sophisticated security analytics/behavioral analysis
  - Context awareness (user, application, device data)
  - Detection of lateral movement (East-West Traffic)
  - Scalability
  - Long-term flow storage
- Compared to other security vendors, Cisco is:
  - Effective at detecting attacks
  - Innovative
  - Supportive of its customers
- Stealthwatch enables the company to:
  - Better manage security with limited staff/resources
  - Accelerate threat detection and mitigation
  - Speed up incident response
  - Reduce enterprise risk
  - Gain pervasive network visibility
  - Foster cross-team collaboration within the IT department

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:
Large Enterprise

Industry:
Professional Services

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 Large Enterprise Professional Services Company

Research by TechValidate by SurveyMonkey

Validated Published: Jan. 10, 2017 TVID: A76-7E4-0DA