Case Study: Medium Enterprise Pharmaceuticals Company

Introduction

This case study of a medium enterprise pharmaceuticals company is based on a December 2012 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 lacked visibility into what was happening on the network previously. The intelligence that Cisco gives us is immeasurably valuable in terms of security response, forensics, and knowledge of what is happening on the network."

Challenges

- Solved the following operational challenges with Stealthwatch by Cisco:
  - Reduced mean-time-to-know (MTTK) root cause of network or security incidents
  - Enhanced network security posture
  - Increased efficiency in the identification of security threats
  - Improved forensic analysis
  - Increased correlation of user identity and activity
  - Increased flow collection, monitoring and analysis

Use Case

- Primarily uses Stealthwatch by Cisco in the following ways:
  - Incident Response
  - Network Forensics
  - Security Forensics
- Used Stealthwatch to detect or prevent the following security threats:
  - Network malware or virus
  - Suspicious user behavior
  - Compromised host
- Is doing the following with Stealthwatch by Cisco deployment:
  - Monitoring a large, globally distributed network

Results

- Chose Stealthwatch by Cisco for the following capabilities:
  - Behavior-based security monitoring
  - Internal visibility
  - Forensics
  - Identity awareness
  - Application Aware Network Performance Monitoring
  - IPv6 monitoring
- Selected Stealthwatch by Cisco over the following vendors:
  - Riverbed Cascade / Mazu Networks
  - Plixer
- Meets enterprise requirements by utilizing the following Stealthwatch by Cisco benefits:
  - Scalability and flexibility
  - Real-time threat detection and correlation with user identity data
  - Improved incident response and threat management
  - Enterprise-wide visibility into network activity
  - Deployment and support simplicity
  - Enterprise-wide user monitoring
  - Forensic analysis
- Reduced the time it took to mitigate a security incident by > 75% by deploying Stealthwatch.
- Rated the following Stealthwatch by Cisco capabilities as compared to competing vendors:
  - Network Security: Better
  - Scalability: Better
  - Network Visibility: Better
  - Innovation: Much Better

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:
Pharmaceuticals

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