Case Study: Central Michigan University

Introduction

This case study of Central Michigan University is based on a December 2012 survey of Cisco Stealthwatch customers by TechValidate, a 3rd-party research service.

> "[Cisco] allowed us to gain visibility into our internal networks. It also allowed us to easily audit our secure zones to ensure certain types of traffic are not leaving those networks."

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 visibility of mobile devices
  - Increased flow collection, monitoring and analysis
  - Enhanced compliance posture

Use Case

- Primarily uses Stealthwatch by Cisco in the following ways:
  - Incident Response
  - Network Forensics
  - Security Forensics
  - Application performance monitoring
  - PCI compliance
  - HIPAA compliance
  - Network performance monitoring
- Used Stealthwatch to detect or prevent the following security threats:
  - Network malware or virus
  - Suspicious user behavior
  - External hacking attempt
  - Compromised host
  - Data loss/ exfiltration
  - Network reconnaissance
- 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

Organization Profile

Organization:
Central Michigan University

Industry:
Educational Institution

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

Results

- Chose Stealthwatch by Cisco for the following capabilities:
  - Behavior-based security monitoring
  - Real-time flow monitoring capabilities
  - Internal visibility
  - Forensics
  - Auditing and compliance requirements
  - Application Aware Network Performance Monitoring
- Selected Stealthwatch by Cisco over the following vendors:
  - Arbor Networks
  - Open source solution
- 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
  - Regulatory compliance
  - 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 25% to 49% by deploying Stealthwatch.
- Rated the following Stealthwatch by Cisco capabilities as compared to competing vendors:
  - Network Visibility: Much Better
  - Network Security: Better
  - Scalability: Better
  - Innovation: Better