

Case Study: Westinghouse Electric

Introduction

This case study of Westinghouse Electric Company, LLC is based on a December 2012 survey of Cisco Stealthwatch customers by TechValidate, a 3rd-party research service.



“Cisco’s solution has provided us with better visibility into network activity across our global enterprise. The near real-time data reporting and alerting capabilities enable our team to detect and respond quicker to security incidents as they occur.”

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
 - Improved forensic analysis
 - Increased correlation of user identity and activity
 - Increased flow collection, monitoring and analysis
 - Enhanced compliance posture

Company Profile

Company:
Westinghouse Electric Company, LLC

Company Size:
Large Enterprise

Industry:
Energy & Utilities

Use Case

- Primarily uses Stealthwatch in the following ways:
 - Incident Response
 - Network Forensics
 - Security Forensics
 - NIST compliance
 - Network performance monitoring
- Used Stealthwatch to detect or prevent the following security threats:
 - Advanced persistent threats
 - Network malware or virus
 - Compromised host
 - Data loss / exfiltration
 - Command and control traffic / botnets
 - Network reconnaissance
- Is doing the following with Stealthwatch deployment:
 - Monitoring a large, globally distributed network
 - Monitoring traffic within a data center, physical and virtual

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 for the following capabilities:
 - Behavior-based security monitoring
 - Real-time flow monitoring capabilities
 - Internal visibility
 - Forensics
 - Advanced Persistent Threats (APTs)
 - Scalability
 - Identity awareness
- Selected Stealthwatch over the following vendors:
 - Q1 Labs / IBM
 - Fluke / Visual Network systems
- Meets enterprise requirements by utilizing the following Stealthwatch by Cisco benefits:
 - Scalability and flexibility
 - Real-time threat detection and correlation with user identity data
 - Enterprise-wide visibility into network activity
 - Deployment and support simplicity
 - Forensic analysis
- Reduced the time it took to mitigate a security incident by 25% to 49% by deploying Stealthwatch.
- Rated the following Stealthwatch capabilities as compared to competing vendors:
 - Network Security: Much Better
 - Network Visibility: Much Better
 - Innovation: Better
 - Scalability: Better