Case Study: Toronto 2015 Pan Am Games – Cisco Systems Canada, Inc.

Introduction

This case study of Cisco Systems Canada, Inc. is based on a August 2015 survey of Cisco Stealthwatch customers by TechValidate, a 3rd-party research service.

> "With over 150,000 user (BYOD) devices connected to the network during the Toronto 2015 PANAM Games we relied heavily on StealthWatch to help us understand what was happening on the network and where the threats were coming from. It helped us in many instances make the decision whether to simply notify a user or disconnect them from the network. With any multi-sports games or large event that is broadcast live time and high availability are critical."

> "Stealthwatch works well with Cisco NetFlow to give holistic picture of the network. It allows us to group and build out profiles that reduce the amount of raw analysis making it practical for a very small security team to get a handle on what is happening on a large network."

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
  - Malware/zero-day attacks
  - DDoS attacks
  - Network performance
  - Network segmentation
- Is able to secure the following with Stealthwatch:
  - Virtual infrastructure/private clouds
  - The data center
  - A BYOD environment

Results

- Reduced their network and security troubleshooting time by hours.
- 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
  - More visibility into mobile devices
- Found the following Stealthwatch capabilities to be the most beneficial:
  - Sophisticated security analytics/behavioral analysis
  - Context awareness (user, application, device data)
  - Flow stitching and deduplication
  - Detection of lateral movement (East-West Traffic)
- 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
  - Clearly report on organizational security to upper management

Company Profile

Company:
Cisco Systems Canada, Inc.

Company Size:
Global 500

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