Industry: Federal Government

## Customer

## Challenge

Federal organizations are particularly prone to cyber attacks, and have a great deal to lose in the event of an incident. As recently evidenced by the WikiLeaks scandal, perimeter security is no longer enough to protect federal agencies from increasingly sophisticated attacks. While required to comply with government initiatives such as FISMA/NIST and the CNCI, this federal organization's chief security architect wanted to go above and beyond simply adhering to standards to truly bolster his organization's security posture. With responsibility for securing more than 28,000 assets over 900 locations, he had his work cut out for him. "There is a difference between reacting and hunting," he said. "If you're reacting, you're done. We knew we had to go hunting, and that meant we had to do things differently."

## Solution

- StealthWatch Management Console
- StealthWatch Xe FlowCollector™

## Results

StealthWatch® has enabled this federal organization to:

- Increase network visibility and situational awareness
- Achieve an effective defense-in-depth security strategy
- Expedite incident response
- Go above and beyond compliance requirements to significantly bolster security
- Avoid becoming the victim of high-profile cyber attacks

# CASE STUDY:
# UNITED STATES FEDERAL GOVERNMENT

### Federal Organization Deploys StealthWatch to Improve Situational Awareness and Strengthen Network Security

## Introduction

This federal organization faces many unique challenges when it comes to security. It is a heavily targeted entity with tens of thousands of high-profile users who are widely distributed over hundreds of locations. Protecting confidential intellectual property for this type of environment requires more than just the bare minimum. Having been frequently attacked by both unfriendly nation-states and cyber criminals, with some of the attacks making headlines, this organization's chief security architect was determined to harden both the exterior and interior of this highly valuable government network.

## Overview

In light of increasingly sophisticated and high-profile cyber attacks, it became clear to this organization that implementing the minimum requirements to comply with federal regulations was no longer enough to adequately protect its critical assets. The organization therefore decided to move from a reactive to a proactive security strategy, going above and beyond traditional, perimeter-based security tools and embracing innovative solutions that would provide more comprehensive protection.

"How do we get better situational awareness of attacks within our target-rich environment?" asked the organization's chief security architect. "How do we stop reacting and start hunting?"

In order to improve its security posture, the organization implemented a defense-in-depth strategy consisting of a set of innovative, complementary security technologies, including Lancope®'s StealthWatch for behavioral-based network monitoring and anomaly detection. Overall, the organization wanted to increase its situational awareness and improve incident response. "We have a target-rich environment that has been (and will continue to be) attacked," said the chief security architect. "We need to detect these [attacks] sooner, and be able to rapidly investigate and respond."

Unifying security, network and application performance monitoring in a single platform, StealthWatch provides the in-depth network visibility and actionable insight needed to foster greater situational awareness and expedite incident response. By analyzing NetFlow™ and other flow data from existing routers and switches, StealthWatch empowers government organizations to troubleshoot a wide range

of issues across the entire network at a fraction of the cost of traditional solutions. According to this organization's chief security architect, NetFlow is far too often overlooked and underleveraged by the industry. Fully leveraging the power of NetFlow, StealthWatch enables federal organizations to quickly pinpoint the root cause of network problems down to the exact devices, applications and users involved.

> *"The stakes are very high for my organization. Reacting isn't working. We have to hunt."*

## StealthWatch Improves Federal Network Security

StealthWatch collects and analyzes flow data to create a baseline of normal network behavior and rapidly detect anomalous activities to significantly reduce the time between problem onset and resolution. The system's automated monitoring, baselining and alarming functionalities play an invaluable role in security operations. Not relying on signature updates, StealthWatch uncovers sophisticated, zero-day attacks that often bypass perimeter defenses, and also detects insider threats including policy violations, network misuse, device misconfigurations and data leakage.

Advanced security capabilities in StealthWatch streamline troubleshooting and dramatically improve protection, as well as boost compliance efforts and assist with network forensic analysis for security incident investigations. These capabilities include:

- **Comprehensive, Continuous Monitoring** of the entire network to enhance visibility
- **Behavioral-Based Anomaly Detection** for fast troubleshooting of internal and external threats without requiring signature updates to detect attacks
- **Application Awareness** to quickly pinpoint application problems
- **The Concern Index™** to automatically prioritize the top security issues facing an organization
- **Automatic Mitigation** to give IT administrators the option of quickly containing security problems
- **The Worm Tracker**, which visually graphs the spread of a worm or virus throughout the network to provide instant visibility into its scope and impact
- **Host Group Locking** to limit communication with sensitive systems
- **Identity Awareness** to pinpoint the exact users responsible for (or affected by) issues
- **Network Forensic Analysis** to enhance incident investigation

Above all, StealthWatch provides the additional "eyes and ears" sought by this organization to make continuous process improvements for securing its confidential assets. The system augments existing security deployments to achieve earlier detection and a more prompt and agile response to incidents.

> *"There is a difference between reacting and hunting. If you're reacting, you're done. We knew we had to go hunting, and that meant we had to do things differently."*

## StealthWatch Fills in the Gaps for Federal Networks

In addition to dramatically improving the security workflow, StealthWatch fills in the gaps left by other technologies to help federal organizations avoid damaging security incidents. StealthWatch takes federal agencies beyond bare-minimum compliance efforts to ensure continuously high levels of security.

"If they only wanted to do what everyone else is doing, they hired the wrong guy," added the chief security architect. "The stakes are very high for my organization. Reacting isn't working. We have to hunt."

> *"We have a target-rich environment that has been (and will continue to be) attacked. We need to detect these [attacks] sooner, and be able to rapidly investigate and respond."*

**To learn more or request a demo, contact sales@lancope.com.**

## About Lancope, Inc.

Lancope®, Inc. is a leading provider of flow-based monitoring to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem identification and resolution. Enterprises rely on Lancope to make better network decisions, respond faster to network problem areas and avoid costly outages and downtime — at a fraction of the cost of conventional network monitoring solutions.

## Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

U.S. Sales
+1.770.225.6500
888.419.1462

International Sales
+44 (0)560 344 8075

Website: www.lancope.com
E-mail: sales@lancope.com



CSV305102011