Global Bank Builds Foundation for Highly Secure BYOD

Financial services company standardizes network, improves security.

Enables the customer to focus less effort on network upgrades and more effort on strategic, added-value tasks.

Challenges

- Accelerate Cisco IOS Software standardization in the face of frequent M&A activities
- Implement coherent security policy to enable more granular controls of approved, suspect, and rogue devices
- Prohibit noncompliant devices from accessing critical applications
- Help ensure segmentation of development and production systems

For one European financial services company, securing the network is both a high priority and a considerable challenge.

Several years ago, as the organization set out to implement a bring-your-own-device (BYOD) policy, it became clear that IT teams lacked the ability to detect and identify rogue devices on the network. The principal barrier was a lack of standardization. The company had so many build variations across its global infrastructure, many of them running different versions of Cisco IOS® Software, that IT teams were unable to create a coherent policy to comply with the latest regulations around security.

To complicate matters, the company is often enmeshed in merger and acquisition (M&A) activity. Each time it acquires another financial institution, it inherits new plant infrastructure, policies, and procedures and moves further from IOS standardization. To achieve a higher level of security, the company needed to find a more efficient, scalable way to integrate a wide range of endpoints into a fast-growing network of heterogeneous devices.

Case Study | Financial Services Company

Size: 100,000+ | Location: Global | Industry: Financial Services

Cisco worked with the bank to design and implement a solution that would unroll in two phases. In phase one, the focus was on IOS standardization. Led by Cisco® Compliance Management and Configuration Service (CMCS), this phase involved a major software image management (SWIM) action to deploy a single standard of IOS on a massive scale. CMCS combines Cisco expertise, intellectual property, and best-in-class software automation to simplify the whole range of configuration management, up to and including the design, implementation, and maintenance of custom organizational standards. Together, these capabilities help the company develop reporting and validation against its internal security policies, in compliance with the Sarbanes-Oxley Act, the Payment Card Industry Data Security Standard (PCI DSS), and other regulatory standards.

Solutions

- Gain Cisco expertise, intellectual property, and best-in-class software
- Upgrade thousands of network elements via successive two-hour change windows
- Apply automation technology to manage compliance for wired and wireless connectivity
- Enforce network policies and protect critical applications with intelligent, scalable access control

After an intensive discovery process, the Cisco team began upgrading approximately 9000 network elements in 2-hour change windows, moving at such a rapid pace that the customer's service desk scrambled to keep up. That level of efficiency was possible, in part, because the Cisco team proactively identified issues within the infrastructure prior to deployment. For example, some legacy switches only contained enough flash memory to hold a single image. During an upgrade, these devices ran the risk of causing a chain reaction affecting every device on the network. Cisco Compliance Management and Configuration Service generated a report showing which devices demanded remediation before an upgrade could take place, helping to ensure that the SWIM action could proceed with minimal disruption. Meanwhile, the customer was able to use the CMCS portal to view and approve all of these activities, thus maintaining a sense of ownership and control throughout the process.

By standardizing IOS devices, the company is establishing a solid foundation for comprehensive device management. Phase two of the implementation, now under way, builds on that foundation with the deployment of Cisco Identity Services Engine (ISE). ISE is a security policy management and control platform that applies automation technology to comply with PCI DSS by achieving granular insight into the full range of devices operated by employees, contractors, and guests on the corporate network.

The ISE solution builds a "ring of steel" around critical data center applications and other information assets, allowing the IT team to quickly survey the current state of the BYOD environment and arrive at a single version of the truth. Intelligent monitoring technology plays an especially critical role in these efforts, proactively identifying rogue devices for quick investigation and remediation. ISE paves the way for a massive deployment of Cisco TrustSec® technology across wired and wireless LAN access points, including 4000 access switches. The TrustSec solution bolsters the company's security posture by simplifying the provisioning and management of access to the network, including the enforcement of policy across the entire network. As part of an aggressive security overhaul, ISE will eventually be integrated with Sourcefire® Advanced Malware Protection and Lancope StealthWatch, a platform providing in-depth network intelligence that includes application awareness and real-time monitoring of Dynamic Host Configuration Protocol (DHCP).

Results

- Offered a high-performance tool set deployed by an experienced team to surpass customer expectations
- Upgraded an average of 600 network elements every week
- Shifted IT focus from network upgrades to more strategic, added-value tasks

Cisco Compliance Management and Configuration Service enables companies to perform complex SWIM actions in a fraction of the time and at a much lower cost. Unlike change management solutions that require companies to wrestle with learning, administering, and maintaining software tools, CMCS offers the compelling combination of a unique, high-performance tool set deployed by a deeply experienced team. A fully documented API makes it possible to integrate the Cisco solution into the company's work flow ticketing systems, while a Cisco service manager actively applies his or her subject-matter expertise, informed by the latest best practices, to maximize the value of the solution.

Due to this unique combination of technology and expertise, CMCS has been able to implement IOS standardization across thousands of the organization's devices with a stunning level of fidelity and minimal risk. The Cisco team upgrades an average of 600 network elements every week, with a success rate of more than 98.5 percent. This activity occurs within 2-hour change windows rather than the 4-hour standard. Throughout the entire process, Cisco has never needed to dispatch an engineer to recover infrastructure on the customer site.

The company's IT leadership freely acknowledges that these capabilities were simply beyond their reach until Cisco came into the picture. The CMCS team has achieved a level of speed and accuracy that the customer did not even realize was possible, and IT teams are thrilled with the ongoing service delivery effort that includes proactive support, automation, scripting, testing, and validation. Perhaps most important, the Cisco service offering, which was performed up to the highest standards using leading-edge tools, makes it possible for the customer to focus less effort on network upgrades and more effort on strategic, added-value tasks.

Products & Services

- Cisco Identity Services Engine
- Cisco Mobility Services Engine
- Cisco 5500 Series Wireless Controller
- Cisco TrustSec technology
- Cisco Compliance Management and Configuration Service
- Cisco Catalyst Switches

Next Steps

The Cisco team has completed approximately 60 percent of the necessary network upgrades. Meanwhile, the Cisco ISE implementation continues to ramp up, with predeployment teams gaining a clear understanding of the customer's environment to optimize the rollout of a solution that will enable a highly secure approach to BYOD for 30,000 users at more than 80 sites. Throughout the process, other members of the Cisco service team will work to maintain the highest levels of compliance across a massive global network, ultimately helping this bank continue its long tradition of market leadership.

More Information

- To find out more about Cisco Identity Services Engine, visit www.cisco.com/go/ise.
- To find out more about Cisco TrustSec, please visit www.cisco.com/go/trustsec.
- To find out more about Cisco Compliance Management and Configuration Service, visit www.cisco.com/go/cmcs.

Americas Headquarters
Cisco Systems Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at **www.cisco.com/go/offices**.