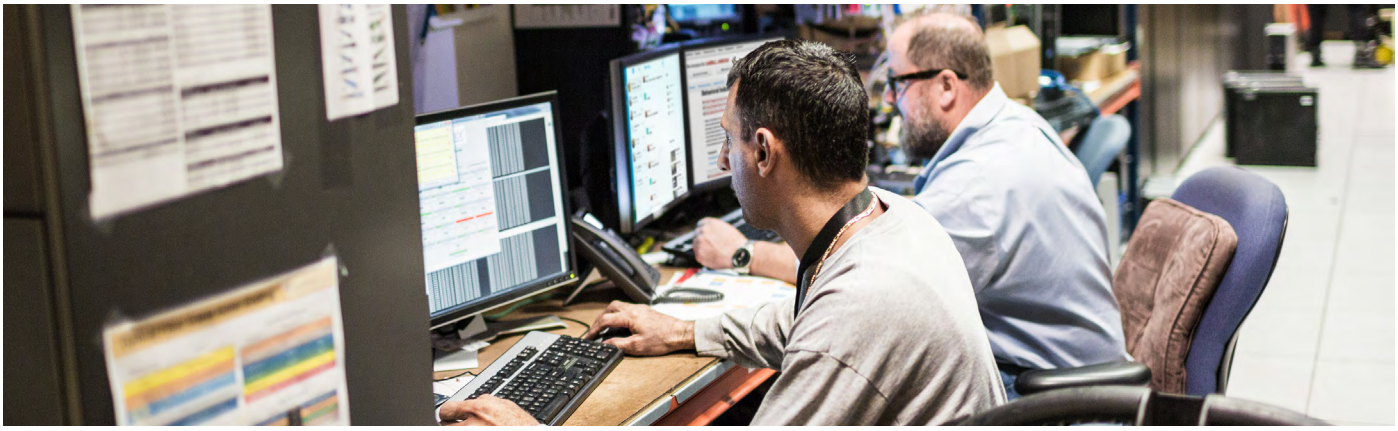
Case Study

Shawmut Strengthens Security and Simplifies Management



EXECUTIVE SUMMARY

Customer Name: Shawmut Design and Construction

Size: More than 1000 employees

Industry: Construction

Location: Boston, Mass., United States (Headquarters), with branch offices across the country

"Cisco Defense Orchestrator was able to automate the process of identifing any duplicate, unused, or inconsistent objects, and made it very easy to combine and remove objects. This saved us days of manual, frustrating work and significantly lowered the risk of accidentally removing valid objects."

Chris Ryan
Network Manager, Shawmut

Shawmut Design and Construction doesn't like surprises – not when it comes to construction projects, and not when it comes to security. They're all about being proactive.

As an employee-owned company, Shawmut has created a culture of ownership, proactive solution-making, and forward thinking. For this reason, the US$1.2 billion national construction management firm has established a reputation for completing extremely complex and logistically challenging projects for an array of high-profile clients. The company is also known for building lasting partnerships with their customers (80 percent of their business comes from repeat clients) and their vendors (the Shawmut-Cisco relationship dates back to the early 2000s).

Ongoing expansion and changes in how the company works continuously challenge Shawmut's IT team to evaluate new operational techniques and applications to support their business. Protecting business operations and valuable data, including the company's intellectual property, is a priority. Aging hardware had to be upgraded with the latest security controls to meet the ongoing threats Shawmut faces on a daily basis. The ultimate solution would need to simplify how the IT team managed security across the organization, providing the company with the controls to proactively protect the business without requiring IT to hire more resources.

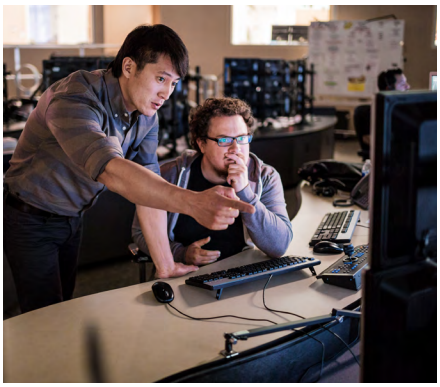
Shawmut's IT staff engaged with Cisco to evaluate what was currently in place and to learn more about the Cisco® portfolio of security solutions.

The existing Cisco ASA 5500 Series firewalls installed in the company's Boston and Westborough, Massachusetts data centers had reached the end of their lifespan and had to be replaced. Shawmut modernized its infrastructure with Cisco ASA 5500-X Series next-generation firewalls set up in high availability active-passive mode for each of their data centers.

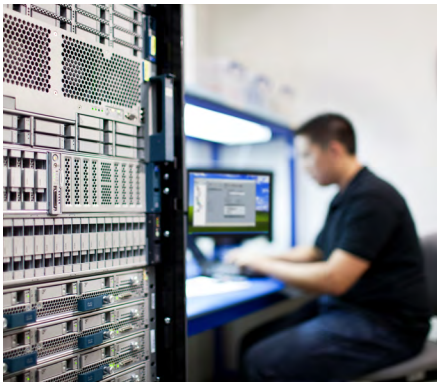
In addition to the upgrade in hardware, Network Manager, Chris Ryan, knew it was equally critical to ensure that the base configuration and policy structure were optimized and consistently moving forward as well.

With Cisco Defense Orchestrator, Shawmut can:

- Automatically discover policies and create consistent structure



- Centrally manage security policies across devices



- Improve security posture and simplify troubleshooting

"After years of policy changes to support business requests and new applications, we needed to find a way to simplify the policy structure in place today," Chris explains. "A simple and consistent policy design could help streamline the approach to troubleshooting and strengthen our overall security posture."

The first step was to gain awareness of the current policy structure holistically across the ASA devices. Chris and his team looked to Cisco Defense Orchestrator as the platform to help discover the current policies in place.

Defense Orchestrator simplifies security policy management across Cisco security products. It helps the network operations team orchestrate and manage policies consistently from one spot to keep the organization protected from the latest threats. Policies can be applied based on groups of devices or conditions, also referred to as objects.

Because Defense Orchestrator is a cloud-based application, Chris and his team had an account from Cisco within 24 hours and were able to onboard their legacy ASA firewall appliances within minutes. Upon onboarding, the Shawmut IT team was able to quickly identify common issues such as:

Duplicate Objects

These are objects that have a different naming scheme, but the same content within that object. As an example, imagine the client had one object called "Web Proxy Server" and another object called "Content Server," but all details in the object match completely. In Defense Orchestrator, the client would be able to choose a name to keep and merge the objects together to reduce the number of objects within the configuration.

Unused Objects

These are objects that are not currently used within the ASA configuration, which can create troubleshooting and compliance challenges. A very common example is when clients use Cisco Adaptive Security Device Manager to manage ASA configuration. By default, the Device Manager will create objects called "DM-Inline," which have no real value to the client's configuration. Using Defense Orchestrator, they can now make a decision to delete the unused objects in their environment for a cleaner configuration.

Inconsistent Objects

These are objects with the same name across ASA platforms, but with different content across devices. This is not only a troubleshooting nuisance, but can also be a potential vulnerability. An example of this could be "country block lists" where the client is looking to block certain countries within their objects and expect that all ASA next generation firewalls are blocking the same list. Defense Orchestrator can help a client identify whether there are inconsistencies and allow them to merge all objects to help ensure a consistent object across platforms.

With Defense Orchestrator, the team can to quickly discover these issues, and also remediate the problems within minutes.

For More Information

Contact cdosales@cisco.com

Products and Services

- Cisco Defense Orchestrator
- Cisco ASA 5500-X Series with FirePOWER Services

"Cisco Defense Orchestrator was able to automate the process of identifing any duplicate, unused, or inconsistent objects, and made it very easy to combine and remove objects," Chris reports. "This saved us days of manual, frustrating work and significantly lowered the risk of accidentally removing valid objects."

Having quickly stabilized the policy structure, Shawmut can now use Defense Orchestrator to proactively manage their security policies. Changes made to policy now take place centrally, and Chris can help ensure consistency moving forward.

"As we continue to evaluate our security needs and potentially expand the portfolio of Cisco solutions we use, Defense Orchestrator has provided us with a centralized and consistent way to manage security policy across our environment," adds Chris.

Defense Orchestrator works with Cisco firewalls, next-generation firewalls and OpenDNS. Policy changes are easily orchestrated across dozens or thousands of devices in a single pane of glass.

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**.

C36-738171-00 11/16