Insurance Leader Simplifies Security Management as Demands Multiply

EXECUTIVE SUMMARY

Customer Name: Insurance Corporation of British Columbia (ICBC)

Size: 5,000+ employees

Industry: Insurance

Location: Vancouver, BC (Headquarters), with approximately 80 locations across the province

"We needed a simpler and faster way to manage policy structure and keep all the rules in synch. Cisco Defense Orchestrator delivers great value at a reasonable price which made it an easy decision for us."

Stan Hembrough
Senior Technical Specialist, ICBC

Protection and peace of mind – when you're in the insurance business this is what customers expect, and leading providers deliver. Since 1973, the Insurance Corporation of British Columbia (ICBC), a Crown corporation established by the provincial government, has been committed to protection and peace of mind for drivers. The company provides universal auto insurance to more than three million vehicle owners and motorists along with driver licensing, vehicle licensing, and registration services.

Stan Hembrough, ICBC's Senior Technical Specialist, shares this dedication to protection and peace of mind. With more than 18 years of experience working on data and voice networks, Hembrough and his colleague Kirk Robinson are leading ICBC's Network Upgrade and Security Enhancement (NUSE) project with the aim of enhancing network and application performance while strengthening security. The project involves designing two new, parallel data center networks to support two data centers and 1,200 servers that will host about 130 different applications and platforms that the company's employees and customers rely on every day. Working closely with Cisco Professional Services, Hembrough and his team are using the Cisco VMDC data center design as the model for data center deployment as they build on their foundation of Cisco network and security solutions.

"We've used Cisco firewalls for 15 years and 99% of our network is Cisco equipment – routers, switches, and access points," said Hembrough. "We recently deployed dedicated Cisco intrusion detection and prevention systems to give us added protection behind the firewall where 90% of our apps and servers are, and to provide the multiple-gigabit per second performance we need to ensure our users can do what they need to do quickly."

When it came time to start migrating the company's applications to the new data center networks, they wanted a simpler and more affordable way to manage the rules to protect those applications. "In each data center we have a cluster of Cisco 5585X next-gen firewalls and by the time we are done with the project we expect that across the two clusters we'll have 50 firewall contexts which can be extremely time consuming and complex to manage," explains Hembrough.

With Cisco Defense Orchestrator™, ICBC can:
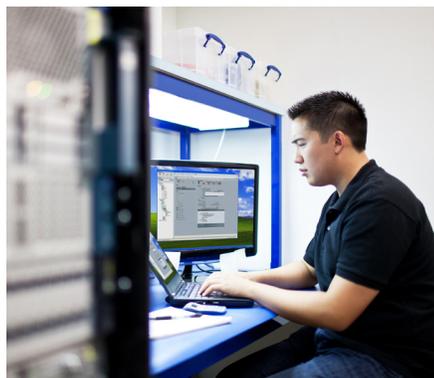
Save four to eight hours cleaning up and optimizing policies.

Centrally manage security policies from anywhere at any time.

Simplify audit and compliance with security policies.

"We needed a simpler and faster way to manage policy structure and keep all the rules in synch. Cisco Defense Orchestrator delivers great value at a reasonable price which made it an easy decision for us."

Cisco Defense Orchestrator is a cloud-based application that simplifies security policy management for network operations teams across Cisco security products while making security policy stronger. Policies can be applied based on groups of devices or conditions, also referred to as objects.

"Of course Cisco offers training, but Defense Orchestrator is so intuitive that we were able to jump right in," said Hembrough. "For instance, I can make a change in Defense Orchestrator or in the console of the firewall and either way the change is picked up and synched across."

Defense Orchestrator helps Hembrough and his colleagues work more efficiently as they cleanup and optimize policies. "As we migrate apps, we are making so many changes to policies that being able to make them quickly in one spot and keep everything in synch is a huge benefit," says Hembrough. "I know Cisco Defense Orchestrator is saving us time – at least four to eight hours a week. Even when we only had a dozen contexts, getting all the object groups aligned and together would take us half a day. Now it takes only 30 minutes which means we can easily do this every week."

Adding new applications is faster and easier as well. "Sometimes, when we add an application we have to add a new port across all 50 contexts," adds Hembrough. "This can take at least four hours when you have to do it one by one. But with Defense Orchestrator we can do this centrally and we're done in a fraction of the time."

Because Defense Orchestrator is accessed through a cloud-based portal, Hembrough and his team of six can work anytime anywhere, which has also increased productivity. Hembrough explains, "The design and implementation staff and the operational staff can all make changes at the same time – from wherever they are. This is important since most of us work remotely from home or some other location at least a couple of times a week, not to mention the peace of mind you get knowing you can have secure access from anywhere in the event of an emergency."

Accuracy is also increased. "Previously we stored all the configurations on a network share but you never knew if the configurations you were working on were up to date," says Hambrough. "To confirm we'd have to log in and check each firewall individually which could take hours. Now we can do this in seconds since Defense Orchestrator instantly shows if configurations are in synch and, if not, we can access the most recent configurations within a couple of clicks."

Hembrough used to rely on the app team to tell them the protocols and firewall rules required for a specific app but they couldn't validate that with certainty. This created "shadow" firewall rules that can create troubleshooting and compliance challenges. Defense Orchestrator keeps an active list headcount so Hembrough and his team can see if apps are being used and by whom and delete objects as needed to ensure accuracy.

Products and Services

- Cisco Defense Orchestrator™
- Cisco ASA 5505 and 5585-X Series firewalls
- Firepower 8350 and 8360 NGIPS appliances
- Firepower Management Center 4000
- Cisco AnyConnect
- Management tools: CDO, Ciscoworks (LAN and WLAN), DCNM
- Cisco routers: 800 to ASR1002 (approx. 100)
- Cisco switches: 2960 to Nexus 7010, including 1000V (approx.. 350)
- Cisco access points (approx. 400)

Looking ahead, Hembrough expects Defense Orchestrator will streamline audits and help ensure compliance with security policies. "As we conduct the migration we note the access required for each app," says Hembrough. "Down the road, when our IT security operations group does audits to ensure the app was implemented appropriately, they can easily find the object group and policies to verify configurations."

Guiding ICBC's Network Upgrade and Security Enhancement (NUSE) project through the last phase of migrating 130 apps and updating policies and rules is a big job, but Hembrough isn't daunted in the least. "Working with our Cisco team has been refreshing – they are very accessible and responsive," says Hembrough. "And the central view Cisco Defense Orchestrator provides is something we've never had before and unbelievably powerful. We can collaborate and work more efficiently to make sure rules and policies are in synch and configurations are clean. Even as the number of applications and contexts increases, Defense Orchestrator makes it easier to protect the business and our users."

For More Information

Contact cdosales@cisco.com