Auction Company Makes Network Access Safer, Faster

Customer Case Study

EXECUTIVE SUMMARY

Ritchie Bros. Auctioneers

Auctions

Headquarters near Vancouver, Canada; 40+ Sites Worldwide

1300 Employees

Challenge

- Prevent network outages and protect sensitive information
- Provide great experience for employees and customers
- Minimize workload for small IT team

Solution

- Upgraded to Cisco Integrated Services Routers (ISR) G2 with two connections: Internet and WAN
- Switched from on-premises web security solution to Cisco Cloud Web Security
- Strengthened security using Cisco firewall solutions and Cisco AnyConnect Secure Mobility Solution

Results

- Blocked access to malicious websites based on reputation scores
- Improved WAN performance by moving web traffic to Internet
- Enabled departments to create web-usage reports without help from IT team

Ritchie Bros. Auctioneers uses integrated services routers for Internet and WAN access, cloud web security, and firewall.

Challenge

As the world's largest industrial auctioneer, Ritchie Bros. Auctioneers conducts hundreds of live, unreserved public auctions of used heavy equipment and trucks every year. Auctions take place at more than 40 auction sites in North America, Europe, the Middle East, Asia, and Australia. More than half of bidders participate online, at www.rbauction.com.

The company works hard to keep the network fast and free of infections. Malware can prevent customers from bidding online and can expose sensitive information. "We need to give customers confidence that online bidding is safe and secure," says Dragan Milojević, senior network security specialist for Ritchie Bros. "Their first experience has to be good."

A common source of infections is when employees or customers unknowingly click links to malicious websites. Ritchie Bros. had tried using a web-filtering application at the head office. "The trouble was that routing web traffic from all 40 sites to one location slowed down critical business applications," says Milojević. Routing all web traffic through Canada also meant that customers at auction sites around the world could only use Canadian search engines.

Ritchie Bros. decided to give each auction site its own Internet connection for web traffic. But the company wanted to centrally control web security for all auction sites.

Solution

Ritchie Bros. Auctioneers met its goals for performance and security using Cisco® Intelligent WAN (IWAN) and complementary Cisco security solutions. Now employees and customers at the auction sites can securely access the network using any device.

 © 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

"With our old web security solution, our IT team had to spend time generating weekly reports. But with Cisco Cloud Web Security, any authorized employee who needs a report can just go to an online portal to generate it without our help."

Dragan Milojević
Senior Network Security Specialist
Ritchie Bros. Auctioneers

The auction sites only need one piece of equipment: a Cisco Integrated Services Router Generation 2 (ISR G2). "Cisco is the only vendor that can support the routers in all of our worldwide offices," says Milojević. The Cisco ISR G2 supports two connections: Internet and Multiprotocol Label Switching (MPLS) WAN. Ritchie Bros. uses the Internet connection for web traffic, and the MPLS connection for everything else.

Cisco IWAN helps to make the business even more secure, in two ways. First, web requests from every auction site are now sent directly to Cisco Cloud Web Security. They no longer have to travel over the MPLS WAN, so they don't slow down any of the company's business applications. "We evaluated three web security solutions, and Cisco Cloud Web Security gives us the best protection because of its large threat database," Milojević says. SenderBase is the world's largest email and web traffic monitoring network. Hundreds of analysts and automated systems research emerging threats 24 hours a day by monitoring more than one-third of the world's email and web traffic.

Second, Cisco IWAN also provides Cisco IOS® Firewall services. "Each location only needs one device, the Cisco ISR G2, for connecting to Cloud Web Security, the Internet, our MPLS network, and for firewall services," says Milojević. "This saves space, power, cooling, and management costs." The company's head offices in Canada and Europe use Cisco ASA Next-Generation Firewalls for secure Internet access.

Ritchie Bros. also takes advantage of other Cisco security solutions. Mobile employees can securely connect to the company network from anywhere, with any device, using Cisco AnyConnect® Secure Mobility Client. They just download the free application to their personal smartphone or tablet. When a Canadian employee travels to Germany and wants to access a corporate application, for instance, the smartphone app connects to the company's closest VPN hub. Then it opens a secure connection to the employee's home office.

And before any mobile device can even connect to the network, the network verifies that the device meets security requirements and that the person using the device is authorized. The technology that makes it possible is Cisco Identity Services Engine (ISE), integrated with the MaaS360 mobile device manager (MDM) from Fiberlink, a Cisco partner.

Results

Secure Web Access Protects Business

Now when a Ritchie Bros. Auctioneers employee or visitor tries to visit a website with a low reputation score, Cisco Cloud Web Security blocks the request. That means the company can confidently offer guest Wi-Fi access at all auction sites. Customers like being able to connect with their phones or tablets to browse the web and check email. They can also bid online for items at other auction sites, increasing sales. At one auction site, as many as 500 people have connected over Wi-Fi at the same time.

 © 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Each location only needs one device, the Cisco ISR G2, for connecting to Cloud Web Security, the Internet, our MPLS network, and for firewall services. This saves space, power, cooling, and management costs."

Dragan Milojević
Senior Network Security Specialist
Ritchie Bros. Auctioneers

Detailed Reports, with No Effort from IT Team

"With our old web security solution, our IT team had to spend time generating weekly reports," Milojević says. "But with Cisco Cloud Web Security, any authorized employee who needs a report can just go to an online portal to generate it without our help."

For example, the Human Resources team can now confirm that employees are complying with company web use policy. That includes visiting only allowed social networking sites.

"A central reporting tool for our network infrastructure saves a lot of time compared to going to different applications and websites," Milojević says. Just three IT staff members are able to provide network support for all 1300 employees. Cisco helped Ritchie Bros. integrate Cisco Cloud Web Security with Microsoft Active Directory. This lets the IT team see if a particular employee is slowing network performance by downloading very large files in a short period of time, for example.

Foundation for Bring-Your-Own-Device

Ritchie Bros. has introduced a bring-your-own-device (BYOD) policy. The IT team uses the mobile device manager to provision and manage company-owned iPads and iPhones. Workers in the auction yards can use iPhones and iPads to check in equipment, for example.

When employees go to any auction site, their devices connect automatically. "The employee doesn't have to take any action," says Milojević. Employees can also connect securely to the company network from airports, coffee shops, and other public Wi-Fi hotspots. The Cisco AnyConnect application on their device establishes the secure connection automatically.

Next Steps

To simplify network management, Ritchie Bros. is adopting Cisco Unified Access. Whether people connect over wired, wireless, or VPN, the company will have one network, one access policy, and one management tool. The company already uses Cisco ISE to consistently apply access policies. "Cisco ISE maintains a single database of all TrustSec tags and related access policies for all users, says Milojević. "Policy enforcement is simpler when it's centralized."

The company will add more Cisco wireless access points as more people bring more mobile devices to auction sites. The IT team plans to use the same architecture for its Europe and Asia Pacific auction sites.

 © 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

PRODUCT LIST

Switching and Routing

Cisco Catalyst 4503-E and 3650 Switch at head office

Cisco 4451-X Integrated Services Router at head office

Cisco 2911 Integrated Services Router at auction sites

Security

Cisco TrustSec

Cisco ASA 5545-CX Next-Generation Firewall

Cisco ASA 5525-X for secure VPN access

Cisco Cloud Web Security

Cisco Prime Infrastructure

Cisco Identity Services Engine

Cisco AnyConnect Secure Mobility Client

Wireless

Cisco Aironet® Wireless Access Points 3700, 2600, and 1140

Cisco 5760 Wireless Controller for head office

Cisco 5508 Wireless Controller for auction sites

Cisco Prime Infrastructure

Data Center

Cisco Wide Area Application Services (WAAS) for traffic between data centers

For More Information

Learn more about Cisco Intelligent WAN: www.cisco.com/go/iwan.

Learn more about Cisco ISR G2 Routers: www.cisco.com/go/isrg2.

Learn more about Cisco Identity Services Engine: www.cisco.com/go/ise.

Learn more about Cisco AnyConnect: www.cisco.com/go/anyconnect.

Learn more about Cisco Cloud Web Security: www.cisco.com/go/cloudwebsecurity.

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**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

C36-731168-00 04/14