Canadian Healthcare Provider Needs to Protect Rapidly Changing Network

Hamilton Health Sciences turns to Cisco TrustSec to protect its Borderless Network with tightly integrated access controls.

EXECUTIVE SUMMARY

- Healthcare: a family of six unique hospitals and a cancer centre
- Headquartered in Hamilton, Ontario, Canada
- 9500 users, including 1000 physicians

CHALLENGE

- Merger growth equals success, but also mismatched network confusion
- Added demands on network due to complex medical equipment, robust healthcare apps, and more remote users
- Increased network vulnerability from more open environment, sophisticated viruses, and social networking use

SOLUTION

- Hamilton Access Security Program for more focused, integrated security strategy
- Cisco end-to-end security technology, with device access controls, perimeter security

RESULTS

- Devices secured and isolated, providing end-to-end safeguarding of sensitive data
- User security levels established for more open network protection, especially with social media use
- PHIPA compliant

Challenge

As the largest employer in Hamilton, Ontario, Canada, Hamilton Health Sciences (HHS) has built a reputation as an innovative healthcare provider, including six unique hospitals and a cancer centre, serving the 2.3 million residents of Hamilton and Central South and Central West Ontario, Canada. HHS offers the services of acute care facilities, a respected physicians group, a pediatric hospital, long-term care, rehab group, an ambulatory surgery center, plus senior housing, a continued care retirement community, and a healthcare foundation.

Through a series of mergers, HHS grew in size and stature but also found itself with a disparate infrastructure of technologies that was the result of acquisitions over time and that was in need of reorganization and updating. As Hamilton's IT team looked for a solution to standardize its network, it turned to CompuCom to create a network utility model in concert with Cisco. The three partners built on and refreshed the model over nearly a dozen years.

As HHS added resource-intensive medical equipment on the network, the growth of remote users taxed security controls, and more sophisticated viruses threatened network devices. As a result, a more focused, integrated security strategy was needed. HHS again turned to CompuCom and Cisco, putting together the Hamilton Access Security (HAS) Program, based on the Cisco TrustSec® platform, to safeguard its increasingly open environment, including the demand for social networking capabilities, against growing vulnerabilities. The program is designed to provide real-time end-to-end security.

HHS became one of the first hospital groups to use the Cisco end-to-end security technology, utilizing device access controls and perimeter security to lock down its environment while providing secure access to a wide array of users, including staff, physicians, vendors, and other health providers. The solution also needed to protect the growing collection of individual devices, including medical equipment known to be more susceptible to breach issues, such as computed tomography (CT) and magnetic resonance imaging (MRI) machines, lab equipment, and other devices regulated by the U.S. Food and Drug Administration and Health Canada.

The HHS team also required the new security environment to be compliant with the Personal Health Information Protection Act (PHIPA), protecting 7700 endpoints, in addition to the network, with 10,000 staff and physicians accessing the network at any given time. As HHS looked to the future, the team needed to address the requirement for more virtual devices to be part of its more open environment, especially as it explored a Bring Your Own PC (BYOPC) program for physicians, in addition to iPads, iPhones, and tablets. And, the system needed to meet user demand for social networking capabilities, necessitating protection in multiple scenarios.

Solution

In assembling the components of its HAS Program, HHS, along with Cisco and CompuCom, put at its core the Cisco® Network Admission Control (NAC) appliance to authenticate any user accessing the network at any time, using any device and from any location. Key to the program's success was the utilization of the NAC's monitoring capabilities to identify software used by HHS, as well as wireless access software from handhelds, laptops, and carts on wheels (COWs). The new HHS environment also included voice over IP (VoIP) used by its wireless phone system over the network, plus the technologies of the newer Blackberrys and iPhones.

The Cisco NAC is used as part of its endpoint security solution, assessing the safety of any device or user entering the network.

"The Cisco TrustSec solution gives us peace of mind due to its ability to secure devices, isolating them as needed," says Mark Farrow, CIO, Hamilton Health Sciences. "This gives us tremendous control and flexibility to implement a BYOPC Program for our physicians, and to securely allow an array of devices onto the network. As a truly integrated solution, I trust that it is secure from end to end."

> "Healthcare is becoming more and more like banking. We expect systems to be up and running 24x7 in an increasingly more dangerous world, particularly on the Internet. The days of hoping an antivirus would catch everything is gone. We need layers of protection, especially to address wireless and mobility needs, as well as the challenges they bring. TrustSec gives us that security."
>
> **— Mark Farrow, CIO, Hamilton Health Sciences**

Results

A key benefit for HHS is the cohesive integration with tight endpoint protection, because the Cisco security components are designed to work together with the existing Cisco environment. HHS also uses Trend Micro antivirus software on its servers, plus Cisco virtual firewalls, Cisco Virtually Routing and Forwarding (VRF) technology, and the Cisco Intrusion Detection System (IDS) to prevent distributed denial of service (DDOS) attacks. As a result, HHS has eliminated major virus outbreaks. The Cisco monitoring tools enable the HHS IT team members to watch traffic across the network, alerting them to address any issues before the network can be compromised versus after the fact.

Farrow also notes that one key to the success of the HAS Program is the ability for the IT team to provide various levels of role-based user and device security as the HHS environment becomes more open. Adding social media to the mix, while also using sensitive medical equipment, brings increased pressure to an environment that cannot afford outages.

PRODUCT LIST
TrustSec • Cisco Network Admission Control (NAC)
Routing and Switching • Cisco Catalyst® 6500
Security and VPN • Cisco Adaptive Security Appliance (ASA)
Wireless • Cisco Wireless
Management • Cisco LAN Management Solution (LMS), Cisco Security Manager (CSM)

"Healthcare is becoming more and more like banking," says Farrow. "We expect systems to be up and running 24x7 in an increasingly more dangerous world, particularly on the Internet. The days of hoping an antivirus would catch everything is gone. We need layers of protection, especially to address wireless and mobility needs, as well as the challenges they bring. TrustSec gives us that security."

Through the Cisco TrustSec solution, HHS has become one of more advanced hospitals in terms of securely managing its network and enacting controls, protecting sensitive patient information, and focusing on best-in-class patient care. The team now is working with other hospitals in the area, advising them how to utilize components to protect their own network.

By extending the HAS Program to other healthcare providers as a software as a service (SaaS) solution, HHS is enabling many smaller hospitals, which otherwise could not afford such systems and may have limited IT staff, to protect themselves and their patient data. The program started as a test with one hospital that needed help and has since grown to include three healthcare providers.

"Our goal at Hamilton Health Sciences is to provide better healthcare to any patients anywhere," says Farrow. "It's a win-win for all of us if we can help our fellow healthcare providers be part of the solution."

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.**

Printed in USA C36-682665-00 08/11