McGill University Health Centre Fortifies Centre of Excellence with Trend Micro Connected Threat Defense Strategy

OVERVIEW
As a leading academic health science partnership, McGill University Health Centre (MUHC) was formed in 1997 through the merger of five hospitals in Montreal, Canada. The MUHC provides exceptional multidisciplinary patient-centric care and is committed to shaping the course of adult and pediatric medicine by assessing the latest in medical technology and training the next generation of medical professionals.

The MUHC developed a Center of Excellence (CoE) that focuses on four key missions: clinical care, research, teaching, and health technology assessment. With three main campuses and more than 20 specialized clinics and facilities, MUHC supports over 15,000 users, 12,000 devices, and 1,200 servers in two data centers. The MUHC manages more than 2.5 petabytes (PB) of data, plus 4 PB of archived data and supports a wide range of legacy and new systems, including Microsoft Windows and Office 365, Linux, and IBM systems.

CHALLENGES
With a widely distributed technology infrastructure, the MUHC IT security team’s main goals were to create a cybersecurity ecosystem for the CoE that reduced the risk of human error while unifying security across the entire organization. “As a Center of Excellence for Quebec, we play a major role in maintaining a secure IT environment to protect patient information, research data, and our networks,” said Hichem Motemem, director of information services at MUHC.

The IT security team wanted security for new and emerging technologies while ensuring legacy applications remain protected. It also sought to create a standardized security model that could be applied to other organizations within the province of Quebec. “The Ministry of Health looks to MUHC as a standard for other health care institutions in the province to deliver the highest levels of security,” said Motemem.
WHY TREND MICRO

While MUHC had been using Trend Micro solutions to protect its infrastructure for years, they were looking for additional solutions to help reduce security management costs while improving IT security efficiency and reporting for the CoE ecosystem.

After carefully evaluating the leading IT security solutions, Trend Micro was selected to protect the entire CoE ecosystem. “Trend Micro not only offers the best solutions for connected threat defense, but they collaborate closely with MUHC to customize solutions to meet our unique needs,” said Motemem.

SOLUTIONS

To ensure security across many facilities and users, MUHC uses a variety of Trend Micro solutions. With Trend Micro™ OfficeScan™ endpoint protection, the solution protects all endpoints and is integrated with other solutions to share information. OfficeScan was instrumental in protecting MUHC against the WannaCry ransomware attack in 2017 that impacted almost every IT facility in Quebec. “OfficeScan protected MUHC from WannaCry, and the Quebec Ministry turned to us to provide best practices to help other facilities avoid future attacks,” said Motemem.

To protect the organization’s 1,200 servers - including legacy servers which require virtual patching to ensure they’re up to date - MUHC relies on Trend Micro™ Deep Security™ solution. It uses Trend Micro™ Deep Discovery™ Analyzer and Trend Micro™ Deep Discovery™ Inspector to detect unknown threats and share this information throughout the security ecosystem.

MUHC uses Trend Micro™ Hosted Email Security™ solution to protect its Microsoft Office 365 environment and Trend Micro Control Manager™ centralized security management to unify all of its security solutions on a single, centralized console, automate security alerts, and simplify reporting required for management review. “Control Manager allows us to monitor our environment and quickly assess activity in one place, so it’s much more efficient than multiple security consoles,” said Carl Seguin, IT security analyst at MUHC.

RESULTS

With Trend Micro solutions delivering a truly connected security approach, the MUHC CoE delivers a cybersecurity ecosystem that unifies security across the entire organization. Trend Micro OfficeScan protects all endpoints, Trend Micro Control Manager provides centralized visibility to simplify management, and Trend Micro Deep Security keeps legacy servers protected.

Providing a preventative approach, Trend Micro Deep Discovery Analyzer and Deep Discovery Inspector detect 1,200 known threats monthly, plus dozens of previously unknown executable threats, and more than 100 URLs that were not known to be malicious. “Even though traditional security perimeters are fading away, Deep Discovery Analyzer and Inspector are keeping our environments secure,” said Seguin.

Trend Micro Hosted Email Security keeps the MUHC environment safe from socially engineered phishing attacks. “Hosted Email Security is a set-it-and-forget-it solution that effectively identifies more than 90 percent of our incoming emails, significantly reducing our email server’s workload,” said Seguin.

Today, MUHC’s CoE and Trend Micro provide a model for effective cybersecurity for all health care facilities across Quebec.

WHAT’S NEXT?

“We’re deploying a network access control (NAC) system and we’re interested in partnering with Trend Micro to develop a smart response solution that will provide additional visibility,” said Seguin.

MUHC also plans to offer Trend Micro solutions for user home computers and devices. “We want to strengthen our BYOD policies. By providing our user community with Trend Micro™ Internet Security for their home use, we’ll decrease infections coming from users by 30 - 40 percent,” said Motemem.