CASE STUDY

Canadian Community Health Center Achieves Reliable Phishing Defense and Network Security with the Fortinet Security Fabric

The East End Community Health Center is in eastern Toronto, Canada. Its mission is to ensure the well-being of everyone in the community, focusing on minority groups and individuals with lower income or education. The 70-member staff provides a comprehensive range of services, including clinical care, chiropody, and dietetics, and manages various groups that support the marginalized and isolated. Doctors strive for a compassionate environment where patients can access the care and assistance they need to lead healthier lives.

However, this noble mission faced escalating cybersecurity risks, particularly through sophisticated email phishing. Many attacks involved emails that mimicked real messages between staff and external contacts, making them harder to detect.

Seeing that this problem would worsen, East End decided to transition from a reactive to a more proactive cybersecurity approach. It started by relying on a mix of technologies and equipment from various vendors and faced significant budget constraints. A small IT team also meant that human resources were stretched thin, making it challenging to deal with significant threats coming in every day at full force.

Fragmented Security and Device Attrition

“Working with several vendors made securing and managing the network challenging,” says Chris Main, data management coordinator at East End Community Health Center. “We had to manage the various interfaces, tools, protocols, and reporting systems separately, risking email threats slipping through the cracks.” The center did not have a coherent and synchronized security posture in which integrated firewalls, intrusion detection systems, and email security could cover the gaps and avoid costly incidents.

East End’s firewalls and devices were also nearing the end of life, which posed significant security risks and increased the likelihood of system failures and downtime. This situation could severely impact the center’s ability to deliver essential healthcare services to the community. East End realized it had to make a critical decision to either continue patching up a fragmented system or migrate to a streamlined, unified framework on a reduced budget.

The health center chose the latter and immediately started looking for a comprehensive system to enhance its cybersecurity posture against email threats. In this search, Fortinet’s partner, Interware, introduced the team to Fortinet’s Security Fabric solutions. Main knew this was the way to go: “I immediately bought into the Fortinet Security Fabric concept, having everything integrated, with transparency and monitoring across devices. Fortinet aligned with our budget and met our security needs.”

East End
Community Health Centre

“It’s remarkable how much spam, phishing attempts, and other junk FortiMail filters out daily. It blocks over 80% of the unwanted emails we receive, making it an essential tool in our fight against email-based attacks.”

Chris Main
Data Management Coordinator
East End Community Health Center

Details

Customer: East End Community Health Center

Industry: Healthcare

Location: Ontario, Canada

Business Impact

- Improvement of personal health information (PHI) and electronic medical records (EMR) protection
- More secure operations for medical staff to deliver healthcare services by protecting the IT network

Adding Redundancy, Reliability, and Control

East End began deploying FortiGate Next-Generation Firewalls (NGFWs) to replace its existing system. Interware played a crucial role in ensuring a smooth implementation and operation by effortlessly transferring existing configurations and setting up new devices. FortiGates allowed the center to improve its cybersecurity posture through high-performance firewall capabilities, including additional antivirus, anti-malware, and email protection, while centralizing monitoring from a single dashboard.

With FortiGate NGFWs, East End could segment its network to protect sensitive data and reduce the risk of unauthorized access. "One network is set up for servers and critical systems, another for management and back-end access, and a third offers clinicians, doctors, nurses, and chiropodists access exclusively to the resources they need," says Main. To add redundancy, the health center deployed a backup FortiGate that automatically takes over when a data path fails.

East End further configured the NGFWs to require multi-factor authentication (MFA) for users connecting via VPN. This additional layer of security was possible by integrating the FortiToken Mobile solution, which enables a one-time passcode (OTP) on top of users' regular login credentials. This addition was essential for the center to meet its insurance security requirements to counter the increasing ransomware attacks. "A real bonus about FortiToken is that we can set it up easily on our end—for example, when someone gets a new phone. Instead of waiting for days or weeks for external support to help us, we can do it ourselves in just five minutes," adds Main.

To enhance the safety of standard switching functions, East End rolled out Fortinet Ethernet switches, FortiSwitch. Over 40 devices were connected to distribution panels that send the internet signal to every facility room. The organized and labeled setup simplifies troubleshooting by allowing quick identification of the port corresponding to any computer. East End complemented this approach with FortiAPs and set up a wireless network for every user group, operating similarly to a guest network. "The integration of both solutions gives the team transparency and the ability to monitor everything connected to our environment," Main says.

Higher Protection and Streamlined Operations

Phishing and ransomware, however, remained East End's biggest challenge. This situation prompted the rollout of the FortiMail solution, which East End integrated with FortiGate to create a more robust and cohesive security strategy that covers multiple email attack vectors. Both solutions can share threat intelligence, enabling more effective detection and protection against malicious activity across email and network traffic. "With FortiMail, we wanted to block unwanted emails without causing users to miss important communications," Main says.

East End can also fine-tune the hierarchical structure of the solution to tailor it to the center's needs. For example, it can still allow and prioritize individual email addresses to receive certain emails even from a blocked domain. "If one of our medical staff is sending emails from a country we've blocked, we do not need to unblock the entire domain to receive that email," shares Main.

"It's remarkable how much spam, phishing attempts, and other junk FortiMail filters out daily," Main says. "It blocks over 80% of the unwanted emails we receive, making it an essential tool in our fight against email-based attacks." The flexibility of

Business Impact (cont.)

- Achieved a unified cybersecurity stance despite budget constraints and a small staff
- Simplified configuration for new device access, saving valuable time

Solutions

- FortiGate Next-Generation Firewall
- FortiMail
- FortiToken
- FortiSwitch
- FortiAP

Services

- FortiCare Premium Support

"I immediately bought into the Fortinet Security Fabric concept, having everything integrated, with transparency and monitoring across devices. Fortinet aligned with our budget and met our security needs."

Chris Main
Data Management Coordinator
East End Community Health Center

FortiMail also allows the IT team to quickly access monitoring logs and efficiently locate and release emails when requested by staff members. To ensure the efficient and effective use of Fortinet solutions, East End also has the FortiCare Premium Support Service, which Interware manages.

When assessing the value of the current Fortinet solutions, Main says: “Knowing that we have Fortinet products working in conjunction and looking after our security needs makes me sleep better at night.” The management team fully understands the importance of the solutions, and users can focus on providing quality healthcare and ensuring positive outcomes for their patients. “For them, it’s simply expected that everything will be up and running smoothly when they arrive.”

Given the high level of integration that allows for a unified cybersecurity approach against email threats, East End will continue to build on its investment in Fortinet products, like the FortiAnalyzer. “It makes sense to continue with Fortinet and consider their solutions for any additional needs. We aim to create a cohesive networking and security environment, and the Fortinet Security Fabric solution aligns with our financial constraints. Their solutions are competitively priced and provide strong value compared to other options.”