

FIELD EFFECT CASE STUDY

Crossroads Children's Mental Health Centre **improves threat detection and protection by 100%.**

Case study **at a glance.**

Organization	Crossroads Children's Mental Health Centre (CCMHC)
Website	https://www.crossroadschildren.ca/
Industry	Healthcare
Need	Proactive IT and cyber security following a ransomware attack.
Solution	<ul style="list-style-type: none">• Field Effect Incident Response Services and Covalence threat detection and monitoring platform.• Fuelled Networks managed IT services, including cybersecurity, wireless networking, and cloud service packages.
Results	<ul style="list-style-type: none">• Improved threat detection and protection of endpoints, networks, and cloud services by 100% from one year ago.• Increased WiFi security for 2,000 CCMHC clients and guests visiting its facility each year.• Initiated security training series for employees, experiencing 95% improvement in user security awareness and safe computing behavior.• Retained Field Effect, deploying its Covalence monitoring platform.• Retained Field Effect partner Fuelled Networks for proactive IT support.

The **client**.

Crossroads Children's Mental Health Centre (CCMHC), a not-for-profit organization, provides Ottawa children under the age of twelve and their families a range of mental health services and support in the home, schools, and community.



Lynn LaHam, CPA and CGA, joined CCMHC in 2006 as Director of Finance and explains the organization's unique mission and success.

"We are a leader in our province and in our country and that's due to our child-centered, family-focused approach and our strong belief in early intervention. We continue to be on the leading edge in new services and treatments, research, and partnerships that will help make an impact in children's mental health," she says.

“We are held to a much higher standard for cyber security and data protection because of the confidential client data we manage.”

The **situation.**

For Lynn, the unknown is probably one of her biggest security concerns. And this rang clear one year ago when CCMHC became victim of a ransomware attack.

“Someone had gained access to our network, took data and asked for bitcoin in exchange for it back,” she explains. “The ransomware attack was a wake-up call. Prior to this, we had always accepted things at face value and we were not aware of the risks that could be targeting our organization and network. After the attack, we literally found holes in our system that we didn’t know we had.”

Fortunately, Lynn had started moving CCMHC’s operations to the cloud a few years ago so client and other confidential data was untouched by the attack. “The stolen data was mostly older documents that we had not prioritized to move to the cloud yet,” adds Lynn.

The **challenge.**

While Lynn’s primary role is ensuring CCMHC remains financially viable, she also manages all IT and security for the organization.

With 30 years of experience in financial management, mostly in technology and the for-profit sector, Lynn has also worn an IT hat for many of those years. This background has prepared her for today’s challenges, including a fast-changing threat landscape, increased data protection regulations from HIPAA to PHIPA, and an employee and client base of digitally-connected users.

“As a healthcare organization, we are held to a much higher standard for cyber security and data protection because of the confidential client data we manage. But the reality is for a not-for-profit of our size and the changing role of IT, we wouldn’t be able to keep pace with the continual training and expertise needed for a dedicated IT position so we depend on external support from IT service providers.”

“Someone had gained access to our network, took data and asked for bitcoin in exchange for it back.”

The **solution.**

Lynn took immediate steps to find out how the attack happened, remediate the damage, and put proactive measures in place.

She contacted Field Effect, a provider of threat detection, monitoring, and incident response solutions. “Within 24 hours, the Field Effect team had put its Covalence monitoring appliance on our network, and not only determined the cause of the attack but thoroughly evaluated our network health to identify any other vulnerabilities or potential risks,” says Lynn.

“Within 24 hours, the Field Effect team...not only determined the cause of the attack but thoroughly evaluated our network health to identify any other vulnerabilities or potential risks”

Field Effect’s forensics and analysis revealed that the attacker was able to access passwords shared online through CCMHC’s internal network. “We were able to identify that our password security was the major factor,” says Lynn. “It was amazing to see the level of detail from Field Effect’s services. We never had exposure to something like network forensics or threat monitoring.”

Lynn then retained Fuelled Networks, an Ottawa-based IT service company for six months. “After evaluating several other providers, I really liked Fuelled Networks’ high standards and approach. We knew these were the people we wanted to manage our ongoing IT operations.”



+



+



The results.

After the attack, there were a lot of learnings, new advantages, and significant improvements. She shares, “It was a very educational experience for us. You hear news of cyber attacks but you never think it will happen to you. It wasn’t until something went wrong that we found out how many holes we had.

Lynn retained both companies for long-term contracts. “My relationships with Field Effect and Fuelled Networks are the best outcomes from the cyber attack.”

Lynn estimates that CCMHC’s threat detection and protection have improved 100% from one year ago. She also has a layered IT and security defense in place through the ongoing work of both companies.

“We now operate a network that I can confidently say is secure and we have experienced professionals looking out for the best interests of our operations.”



100%

IMPROVEMENT IN
THREAT DETECTION



95%

INCREASE IN
USER EDUCATION

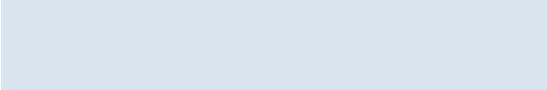


2k+

WIFI USERS
PROTECTED YEARLY

Field Effect’s real-time threat monitoring, vulnerability discovery, and analysis is in place across her devices, cloud services, and network. According to Lynn, Field Effect’s AROs process of threat alerts, recommendations, and observations give the Fuelled Network team additional visibility across CCMHC’s IT environment.

User education has increased by at least 95% and security has also improved for more than 2,000 clients and guests that visit CCMHC each year for daily walk-in clinics, meetings, and events, and use CCMHC WiFi. As part of CCMHC’s layered defense, Fuelled Networks took a three-stage approach to creating CCMHC’s new secure wireless network. This included setting up a secure authentication strategy for both corporate-owned and employee-owned devices, and a separate network for guest access with policies for granting and managing usage.



“Through the work of Field Effect and Fuelled Networks, we can provide a secure network for our team members, customers, and board. We have mitigated our risks with these two relationships and put preventive measures in place to ensure our operations are safe going forward. We have a total solution now as a result.”

Lynn LaHam, CPA, CGA
Director of Finance
Crossroads Children’s Mental Health Centre

LET'S TALK

It's time to get the expert support and tools to respond and remediate active threats, keep your business up and running, and build a better security defence.

Field Effect's Incident Response services, priced for SME budgets, are designed to identify, isolate, and resolve cyber security incidents quickly and thoroughly.

In the first 24 hours, we use our powerful Covalence threat detection and incident monitoring platform to assess your network health, perform an analysis to determine vulnerabilities or potential risks, and begin remediation.

We also add AROs — Actions Required, Recommendations, or Observations — that deliver threat alerts with understandable and actionable insights.

Through the intelligence of Covalence platform and our AROs, you can focus on the cyber security issues that matter. Find out more at sales@fieldeffect.com.

Contact our team today at sales@fieldeffect.com or call +1 (800) 299-8986.



Cyber security that keeps business moving.