



Marcil Lavallée chooses Covalence as preferred solution.

Case study at a glance

Company

Marcil Lavallée

Website

marcil-lavallee.ca

Industry

Accounting

Business Need

Powerful, easy-to-manage threat monitoring and analysis for a small IT team.

Solution

Field Effect's Covalence® threat monitoring, detection, and response platform.

Results

Gained a more powerful, manageable, and cost-effective threat detection and monitoring solution than available options.

Realized significant time savings each week with the improved ability to quickly identify and respond to threat alerts.

Reduced number of tools in technology stack, minimizing system impact and improving performance by nearly 40-50% on certain servers.

The Company



As one of the largest, independent French speaking accounting firms in Canada, Marcil Lavallée provides a full line of audit, bookkeeping, tax, and consulting services for healthcare, education, not-for-profit organizations, small and medium-sized businesses, and more. With 100 employees and offices in Ottawa and Gatineau, the firm has continued to experience steady growth.

Information technology veteran Keith Chabot joined the firm 16 years ago as Marcil Lavallée's IT Director, responsible for the security of the firm. Among everything else in his busy role, his small team is ultimately tasked with keeping Marcil Lavallée's 100 onsite and remote users secure as well as ensuring proprietary information and sensitive client data remains private and safe.

If you ask Keith, he will tell you the firm's success lies in its impeccable approach to customer service. And that is easy to see as Marcil Lavallée recently celebrated 35 years in business.

Keith has seen a lot of change and innovation, but a few things have remained constant. "Our focus on customer service and cyber security are key differentiators," he explains. "We take a true interest in helping clients meet their challenges — beyond servicing their accounting needs — and cyber security is always central to our approach."

Marcil Lavallée



The Challenge



The key challenge as a smaller business is finding ways to defend our network against new threat vectors and potential risks with limited resources.

As a small IT team for a firm that manages, shares, and stores confidential financial data on a daily basis, Keith can't afford cyber security surprises. He needs a continual view across his network.

The reality though, he doesn't have the resources for a security operations center to provide 24/7 monitoring, but still requires the same, strong capabilities and functionalities.

"The key challenge as a smaller business is finding ways to defend our network against new threat vectors and potential risks with limited resources," says Keith. "My top concern isn't what I can see today, but what I may be missing. When it comes to putting the best defense in place, I need complete visibility. I never want to worry about what I may not be seeing."

Adding more challenge and risk, while the company's workforce had always been nearly 50% remote, now nearly all employees were accessing the Marcil Lavallée network from home locations.

Keith needed to ensure his security tool stack was robust and easy to manage, but also provided full insight to the daily system and user activity across his endpoints, network, and cloud infrastructure.

The Solution

To solve for his monitoring needs, Keith initially considered a range of options, including security information and event management (SIEM) solutions. As he explains, "I was concerned a SIEM would require a lot of my time to manage and would be costly, but at the time, I thought the log consolidation of events would help me see what's happening in my network."

Keith quickly changed his mind after seeing a demo of Field Effect's Covalence threat detection and monitoring solution. After evaluating other monitoring solutions, he chose Covalence. Covalence provides complete detection and monitoring from one platform for his cloud infrastructure and services, endpoint devices, and network.

While log-based SIEMs can be powerful monitoring tools, the reality is, the process, data volume, configuration, and maintenance needed for effective detection and monitoring results can be expensive and costly to maintain.

As Keith discovered, Covalence provides a more powerful, manageable, and cost-effective threat detection alternative. Covalence gathers data-rich security telemetry from a customer's network, endpoints, and cloud sources, and applies both machine learning as well as humanled analytics to identify active threats, risks, and vulnerabilities that may exist in the IT environment — an approach that also continually improves the security posture.



As a lean IT team, we don't have the time to analyze and extract our own information from the multitude of threat alerts and vectors. Using Covalence and its AROs, the data is easy to digest and share, and that saves me time.

"I'm getting better features and functionality than a SIEM without the management and maintenance costs," he adds. "Using Covalence, I gain a very easy to use, end-to-end solution for threat monitoring, vulnerability discovery, and analysis."

According to Keith, Covalence not only provided full monitoring coverage, the platform was the best at consolidating security information. This saved time and provided very accurate detail.

"Covalence's uniqueness is really in its alerting and reporting capabilities. The depth of alerting and analytics are impressive. It's able to tie in so many sources of security information across my entire IT environment and provide reports that are simple to understand and well explained," he says.

Unlike other monitoring platforms, Covalence and its AROs process consolidate security events into simple and actionable reporting, providing three types of alerts — a required Action, Recommendation, and Observation. This results in focused alerting with reports that provide clear, practical information with specific remediation steps to protect the entire IT environment. Each ARO is checked by Field Effect's cyber analysts and guides priority, response time, and activities needed to better protect networks.

"As a lean IT team, we don't have the time to analyze and extract our own information from the multitude of threat alerts and vectors. Using Covalence and its AROs, the data is easy to digest and share, and that saves me time," Keith adds. "I can share the reports directly with our executives to ensure they're informed, but also demonstrate the value I'm bringing to our IT function," Keith explains.

The Results

For Keith, Covalence provides exactly what he was looking for. "Covalence solves for detection and monitoring in a completely different and more effective way than any of the tools I have used or evaluated," he shares.

Prior to Covalence, Keith says the effort to efficiently gather this type of detail across his multiple data sources and take action was a long, arduous process. "The best outcome from the Covalence deployment is having all of the information readily available," he says.

"I now have a bird's eye view of all the systems, services, and user activity across my network. I can see when and from where employees are logging into our Office 365 services, and all other activity happening in our IT environment," he explains. "Whether it's my local infrastructure, a remote worker, or out in the cloud, I have complete peace of mind that Covalence is checking everything and will catch any potential risk or compromise attempts."

Covalence has also helped him streamline his technology stack and reduce resource consumption. Prior to deploying Covalence, Keith was using an endpoint protection solution that was not only generating a volume of alerts that required time to investigate but also consumed a lot of his system resources.

After uninstalling this and deploying Covalence's endpoint agents, which only consume about 2% CPU, he was able to resolve some previous high CPU usage issues with the previous solution.

"Covalence is so lightweight and powerful, it has become a core tool in my solutions stack," Keith adds. Keith estimates that he is working more efficiently each week by reducing his threat alerting volume through focused monitoring. This has simplified the task of analyzing alerts, prioritizing remediation, and resolving any issues.

100%

IMPROVEMENT IN
THREAT DETECTION

Less Tools

REDUCED TOOLS IN
TECHNOLOGY STACK

50%

BETTER SYSTEM PERFORMANCE,
LESS IMPACT

“


I have not only
gained an amazing
monitoring,
detection, and
response solution,

but a team of cyber experts by my
side analyzing my data and helping
me stay ahead of the risks and
improve the security of my network.

Keith Chabot

IT Director

Marcil Lavallée



It's time to get the visibility you need to prevent cyber attacks and secure your business.

Covalence makes it easy to understand, prioritize, and act on cyber threats and risks to your operations. It's purpose-built to continually monitor your network 24/7 in real time and identify any changes or unusual activity that may put you at risk.

Providing a powerful, continual view into networks, Covalence delivers advanced analytics and alerting across cloud infrastructures, traditional on-premise networks, and endpoint devices, with understandable and actionable insights.

Designed to reduce cyber security complexity and costs, you gain an end-to-end threat monitoring, detection, and response system to measure, manage, and reduce the cyber risks to your networks and infrastructure.

Through the intelligence of the Covalence platform and our AROs, you can focus on the cyber security issues that matter.

About Field Effect

Field Effect believes that businesses of all sizes deserve powerful cyber security solutions to protect them. Our threat monitoring, detection, and response platform, along with our training and compliance products and services are the result of years of research and development by the brightest talents in the cyber security industry. Our solutions are purpose-built for SMBs and deliver sophisticated, easy-to-use and manage technology with actionable insights to keep you safe from cyber threats.

Contact our team today.

Contact us
letschat@fieleffect.com

Canada and the United States
[+1 \(800\) 299-8986](tel:+18002998986)

United Kingdom
[+44 \(0\) 800 086 9176](tel:+4408000869176)

Australia
[+61 1800 431418](tel:+611800431418)