Secureworks

CASE STUDY

Managed Detection & Response powered by Red Cloak™

Overview

Firma FX is a global payments specialist with offices in Canada, Australia, New Zealand, and the UK. The company holds sensitive customer data, customer financial data and its own financial data all residing on-premises. The two major security concerns for the company are data exfiltration and loss of the ability to process payments, the core of their business. Firma is a global company with around 250 employees distributed across 3 continents. Up until choosing MDR, Firma had focused most of its security efforts on securing around 20 critical servers using Secureworks® agents. The company had also set up SYSLOG forwarding for four firewalls and a VPN service to the Secureworks Counter Threat Platform™. Firma has no dedicated security staff, but the four infrastructure admins are required to have foundational security knowledge.

FIRMA Foreign Exchange

Company: Firma FX
Industry: Financial
Location: CA/UK/AU/NZ
Employees: 250

Challenges

Firma was planning next steps to mature its security posture. The company had no dedicated security staff, and lacked the time and resources to gain genuine insight and visibility into the security side of their infrastructure. Initially, Firma planned to address this all in-house. They intended to procure a SIEM and hire a security manager to manage it. From there, they wanted to build a full team. Once Firma learned of MDR, it became clear this wasn't necessary.

Solution

Machine learning capabilities were a must-have for any potential solution, according to Mike Rue, Director of I.T. Infrastructure and Operations at Firma. Mike and his team of infrastructure admins could see the potential for machine learning and automation technologies to reduce the security workload. Security often requires looking for patterns, and when technology can do this for you, the productivity gains are clear.

Why Secureworks MDR stood out

Once Mike realized there was no need to build a team in-house, he decided to compare different solutions. Secureworks MDR stood out for one clear reason: the machine intelligence was paired with human expertise. Mike found Secureworks MDR to have a broader scope than other solutions. Two things were particularly appealing:

1. **Monthly threat hunts conducted by Secureworks experts.**
2. **Quarterly security-based line reviews conducted by Secureworks experts.**

"These two factors were huge in the decision," said Mike. "Other solutions didn't have the extra human element." The fact that MDR also includes an Incident Management Retainer was a bonus. The inclusion of IMR meant Firma could simplify and consolidate its security portfolio.

Securing the backing of executive leadership

After Mike decided Secureworks MDR made more sense than building a team in-house, he needed to convince executive leadership that it was the right choice. Fortunately, that proved easy. "I only had to make the case for a much cheaper solution," said Mike.

Firma's original plans involved hiring one full-time security employee, procuring a SIEM, and then using the full-time employee to set up and maintain the SIEM. From there, more staff would be hired. In the end, Mike realized none of this was necessary. So, what were the cost savings?

"For the current year, it saved us over half of what we were planning to spend on an in-house solution," said Mike. "It was pretty cut and dried."

Solution

Mike learned about MDR at a small lunch and learn-style event Secureworks held for IT and security leaders in Edmonton, Canada. Mike was already aware of the Red Cloak Threat Detection & Response security analytics software, and when he learned the new MDR service was built on that software, his interest was piqued. Through contact with Secureworks, Mike learned more about the full MDR package and realized there was no need to build a team in-house. "MDR pretty much met all our requirements," said Mike.

"For the current year, it saved us over half of what we were planning to spend on an in-house solution,"

Mike Rue
Director of I.T. Infrastructure and Operations at Firma.

Secureworks

Fast installation, rapid results

Installation of MDR took around three days at Firma. The fact Firma already had a few Secureworks agents deployed in the environment helped speed up the process. Installation meant expanding that deployment beyond a subset of devices, to the whole environment.

Once MDR was installed, Mike and his team of infrastructure admins spent time getting to know the software. Though they didn't plan to use the software themselves much, the team wanted to understand the decisions the software was making to establish trust. After a short while, they realized they could trust the software, and the Secureworks team, to do its job. According to Mike, the Secureworks team has been prompt and persistent when they've needed to get in touch. "I can't ask for better than that," Mike said.

One of the key immediate benefits was the ability to use the MDR dashboard to help illustrate how much data the security infrastructure processed. "Not long after it was installed, I demo'd the software to leadership to show them just how many alerts were being generated, how much data was going through our infrastructure and how much we were having to monitor in our environment," said Mike. "It helped them really understand what we were trying to achieve with the engagement of the platform."

The MDR dashboard makes it quick and easy to drill down into the details of alerts. With a couple of clicks you can identify which user or device generated the alert, for example. It proved so intuitive that Mike also presented to director-level leadership to help educate them about the organization's security workload and challenges.

'It's exceeded our expectations'

At the time of writing, MDR has been installed and running for over eight months at Firma. The decision to use MDR saved money, increased security productivity, and enabled Mike to help the rest of the organization understand the specifics of what the security function handles. The experience for Mike has been overwhelmingly positive. "I have trouble finding any faults, and new features mean it's constantly improving," said Mike. "It's one of the best decisions we've made in a long time."

"Not long after it was installed, I demo'd the software to leadership to show them just how many alerts were being generated, how much data was going through our infrastructure and how much we were having to monitor in our environment,"

Mike Rue
Director of I.T. Infrastructure and Operations at Firma.

About Secureworks
Secureworks® (NASDAQ: SCWX) a global cybersecurity leader, enables our customers and partners to outpace and outmaneuver adversaries with more precision, so they can rapidly adapt and respond to market forces to meet their business needs. With a unique combination of cloud-native, SaaS security platform and intelligence-driven security solutions, informed by 20+ years of threat intelligence and research, no other security platform is grounded and informed with this much real-world experience.
www.secureworks.com

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com