CASE STUDY

Enterprise-class Security That Municipalities Can Afford

In Western Canada, Alberta extends from prairies and deserts to some of the most iconic alpine vistas in the Rocky Mountains. More than half of the province's 4.3 million people live in either Calgary or Edmonton. The rest are distributed among a large number of small cities, towns, and villages.

The Alberta Urban Municipalities Association (AUMA) supports these dispersed municipalities by lobbying elected leaders on their behalf, and by providing services such as insurance and employee benefits. The association recently started offering managed cybersecurity services as well. An overhaul of its internal infrastructure revealed an opportunity to simultaneously build a new line of business and help its member-municipalities better protect their communities.

Fortinet Security Fabric Is a "No-brainer"

When Shaun Guthrie took over as senior director of information technology at the AUMA two years ago, one of his first actions was to launch a cyber threat vulnerability assessment. "We wanted to really understand which aspects of our technology infrastructure were vulnerable," he recalls. The results revealed a primary cause for concern: The company used core infrastructure systems from three different vendors.

"We had Fortinet firewalls, but then we had switching from another company and wireless access points from a third," Guthrie says. "We had very little visibility into security events across our network, which meant we did not even know what challenges we needed to solve." The organization's insurance and benefits services mean it has data that requires compliance with an assortment of regulations. "To ensure our security was effective, we needed to better understand the different types of data we had, where and how we were storing them, and how our security tools were working throughout the infrastructure."

The AUMA needed to upgrade its firewalls, and Guthrie decided to consolidate the organization's firewalls and security-driven networking with one vendor. He and his colleagues considered their options and settled on Fortinet security solutions, largely due to their tight integration. The team chose to move to a new managed service provider (MSP), as well. They selected an MSP with the experience to help remediate the issues that the threat risk assessment had revealed.

"Having three different platforms was challenging to manage," Guthrie says. "The platforms did not talk to one another, so if our legacy MSP had to change a configuration, they had to manage it across all those platforms. Moving to the Fortinet Security Fabric was a no-brainer."

"I sleep better at night because I know that if there is an incident, our systems will respond right away. Fortinet offers great technology at a great price, with great visibility across the whole security stack."

– Shaun Guthrie, Senior Director, IT, Alberta Urban Municipalities Association (AUMA)

Details

Customer: Alberta Urban Municipalities Association (AUMA)

Industry: Government

Location: Edmonton, Alberta, Canada

Business Impact

- Immediate threat response, vs. several hours in the legacy environment
- 43% lower costs for security infrastructure management services

Tightly Integrated Solutions Reduce Security Management Costs by 43%

The AUMA rolled out Security-Driven Networking, with a FortiGate firewall to secure the wide-area network (WAN) edge as well as the local-area network (LAN) edge, and with FortiSwitch secure access switches and FortiAP access points to provide secure wireless connectivity throughout its office. The new MSP manages the infrastructure; still, Guthrie immediately appreciated the benefits of working with a single vendor that seamlessly integrates all the core components together within the Fortinet Security Fabric platform.

"I am very impressed with the Fortinet Security Fabric," he says. "I have a small team. If we ever were to bring our security infrastructure back in-house, it would need to be easy to manage. That is a key reason why we selected the FortiGate next-generation firewall [NGFW]. And the ease-of-use benefit extends to the switches and access points. All those solutions share information, and the FortiGate gives us full visibility across our technology stack."

The management demands fell so significantly that Guthrie was able to negotiate reduced rates from the new MSP. "Now, they are able to manage our entire technology stack through one console," he says. "I made the case to them that it does not make sense to pay separately for management of the Wi-Fi, switches, and firewall. They agreed, and the AUMA recovered some of our operational expense.

Business Impact (contd.)

- Enterprise-grade managed security at an affordable price for Alberta municipalities of all sizes
- New line of business within IT that produces a new revenue stream: five figures in the first year of offering, followed by rapid expansion in years to come

Solutions

- FortiGate
- FortiSwitch
- FortiAP
- FortiSIEM
- FortiEDR

"Overall," Guthrie continues, "we have reduced our support costs by 43%. We've eliminated a switch and the Wi-Fi management device, as well as reducing the number of Wi-Fi access points because our newer devices have a stronger signal."

Streamlined and Automated Threat Response

The AUMA further strengthened its security infrastructure by adding security information and event management (SIEM) and endpoint detection and response (EDR) capabilities. "We wanted a SIEM to combine the threat information that our systems were gathering and turn it into actionable intelligence," Guthrie says. "That visibility would enable us to execute quickly in the event of an attack."

To access sophisticated SIEM capabilities without stretching staff resources too thin, the AUMA engaged Canadian Security-as-a-Service provider Stratejm to manage a cloud-based implementation of FortiSIEM. Information flows into FortiSIEM from not only the AUMA's Fortinet security solutions but also its server logs, network management tools, and logs from Azure and web servers.

"FortiSIEM correlates all this information against indicators of compromise," Guthrie explains. "There may be 16 million different events in our log files, but the SIEM will boil them down to four or five incidents. Our small staff can see right away if something critical changes or if there is odd behavior on the network. That means we, or our MSP, can tackle the threats as soon as they appear. If something happens, we will deal with it in hours, rather than the 120 days that pass in the typical company before a cybersecurity incident is even noticed."

The AUMA also recently replaced its legacy endpoint protection solutions with FortiEDR, which Stratejm will also manage. The cloud-based FortiEDR solution will protect endpoints both pre- and post-infection. Integration of FortiEDR with FortiSIEM will enable the endpoint security solution to automatically run playbooks that stop data breaches and tampering as soon as the SIEM detects them. Moreover, the Stratejm team will be able to see all the endpoint alerts on the SIEM.

"With FortiEDR and the Fortinet Security Fabric, our security infrastructure will automatically block and tackle," Guthrie says. "The AUMA has been very fortunate so far, but I believe an attack is not a question of 'if,' but 'when.' And if an attack happens in the middle of the night, no one on my team will have to wake up at 2 a.m. to remediate the situation on the endpoint."

The solution that FortiEDR is replacing did not offer automated response. "In our legacy environment, if our endpoint solution detected something, internal staff had to enter it on the MSP's help desk portal," Guthrie says. "The help desk would then pass it on to a technician, where it would go into his queue. Overall, it would take at least half a day for remediation efforts to begin, with a day or more until resolution. In contrast, if FortiEDR detects an issue, it will cut it off right away. The time to response is almost immediate. Also, because FortiEDR ties into the rest of the Fortinet Security Fabric, we will gain a better line of sight to our endpoints."

"In our legacy environment, if our endpoint solution detected something, it would take at least half a day for remediation efforts to begin. In contrast, if FortiEDR detects an issue, the time to response is almost immediate."

– Shaun Guthrie, Senior Director, IT, Alberta Urban Municipalities Association (AUMA)

Security Presents New Business Opportunity

The AUMA has been so pleased with FortiSIEM and FortiEDR that it partnered with Stratejm to extend a managed version of each solution as a service to its members. "The municipalities we serve, particularly the smaller towns and villages, may not be able to access enterprise-class security on their own," Guthrie says. "We want to give them access to the same type of actionable intelligence the AUMA now has, at a cost that is affordable to them. Stratejm makes that possible by achieving economies of scale in providing managed services to a number of our members."

FortiSIEM and FortiEDR were the right choice for this new service, Guthrie adds, in part because they are cloud-based. In addition, the multitenancy capabilities in FortiSIEM mean the solution can easily scale up as the AUMA and Stratejm add security customers.

Guthrie now runs the Managed Technology Services business unit of the AUMA. Through a revenue-sharing arrangement with Stratejm, the organization offers a vendor-neutral threat risk assessment, in addition to the managed FortiSIEM and FortiEDR services. The first pilot will launch within weeks.

"We are going to be providing additional value for our members, offering services they would never be able to get on their own," Guthrie says. "Fortinet was instrumental in making that happen." In addition, the new line of business will generate revenue while incurring minimal costs. "We earned $0 on this service last year because it didn't exist. This year, it will bring in five figures, and we expect the business to expand even more rapidly once we have proven the value of the business model. That's revenue we can use to the ongoing benefit of our members."

One of the aspects of this venture that Guthrie is most enthused about is the potential for AUMA members to share security-related information. "Unlike corporations, municipalities are usually not competing against one another," he says. "They tend to be looking to protect the greater good. If we can facilitate information sharing among the municipalities that choose to participate, the increased security intelligence will benefit all those communities. Seizing the power of our membership is, in fact, the foundation of our association. I even envision an opportunity, once we have proven its success in Alberta, by which we could provide this service to municipalities across all of Canada."

On behalf of both the AUMA and all its members, "I sleep better at night because I know that if there is an incident, our systems will respond right away," Guthrie concludes. "Fortinet offers great technology at a great price, with great visibility across the whole security stack."

March 30, 2021 12:26 PM
D:\Fortinet\Work\2021\0330\cs-alberta-urban-association
931998-0-0-EN