CASE STUDY

Canadian Municipality Upgrades and Simplifies Its Cybersecurity Infrastructure with the Fortinet Security Fabric

With a population of over 8,000 people, the City of Kimberley was voted the best small town in British Columbia, Canada, in 2023 by CBC News readers. The municipality supports various services for residents, including operations, environment, emergency, bylaws and enforcement, and taxes and utilities. Its mission is to enhance the quality of life for inhabitants and visitors' experiences by providing community services and advocating for economic development.

To deliver on this commitment, the City of Kimberley must collect, store, and manage critical data such as population statistics, household information, land and property ownership details, tax and revenue records, and health and social services registers.

The city faced several cybersecurity challenges while dealing with this amount of information. The IT team became aware of the increasingly identifiable threats as nearby municipalities became the target of ransomware attacks and citizen record breaches. The technology they had didn't meet their needs, prompting the organization to look for an effective, comprehensive cybersecurity framework.

More Reliability and Uptime Across the Network

The main challenge for the City of Kimberley was to increase its overall data and network protection level. "We had to update our cybersecurity stance because the number of threats was ballooning around us," says Dave Hlady, manager of information technology. "Back then, we used an expensive firewall that didn't allow us to personalize the rules. We needed something that we could configure better."

This lack of set-up options meant higher vulnerability to attacks, problems in network performance and reliability, potential loss of data integrity and confidentiality, and critical compliance issues. Furthermore, the solution in place represented significant unreliability at the access point and firewall level because it would take a while to get support to fix any problem that arose. "I had to issue a ticket and wait an hour and a half for it to be solved. All that time, the firewall was down," Hlady says.

The licensing of the solution also became a burden. "I didn't have support contracts for most of my access points, so I just had to buy a few extra access points just to have on hand." At this point, the top priority was the need for a more comprehensive, cost-effective cybersecurity framework covering the entire digital attack surface from network infrastructure to endpoints and applications.

KIMBERLEY
BC • CANADA

"We chose the Fortinet Security Fabric for its cost-efficiency, but also, because it's a whole cybersecurity framework, I could envision having all my devices talking to each other, reducing the complexity of my infrastructure."

Dave Hlady
Manager of Information Technology,
City of Kimberley

Details

Customer: City of Kimberley

Industry: Government

Location: British Columbia, Canada

Business Impact

- Unified, coordinated, cost-effective cybersecurity posture
- Security compliance and implementation of best practices to protect critical data
- Identification and control of all applications on the network
- Detection and prevention of sophisticated threats

Enabling Higher Protection

The IT team launched looking for a significant upgrade to their existing solution. "We chose the Fortinet Security Fabric because of its cost-efficiency," Hlady says. "Since it's a whole cybersecurity framework, I could envision having all my devices talking to each other, my switches, firewalls, and access points becoming a single pane of glass, reducing the complexity of my infrastructure."

Central to the Fortinet Security Fabric deployment, the City of Kimberley rolled out the FortiGate Next-Generation Firewall (NGFW) across the network. It allowed Hlady's team to identify and control applications running on the network and detect and prevent sophisticated threats. The installation comprised various Ethernet switches, FortiSwitches, which support Layer 1 and 2 switching for centralized management, simplified the new platform deployment, and enhanced security. The goal was to provide the Municipality with robust network capabilities through a unified and coordinated security posture. Protection was complemented by an equal number of FortiAP wireless access points that provide secure, high-performance Wi-Fi connectivity.

Another critical element in the City of Kimberley's upgraded cybersecurity stance was enabling multi-factor authentication. "This became a necessity, not just a want. We needed to get municipal insurance and implement best practices, but I wanted something that could integrate into the security architecture," Hlady asserts.

In pursuit of this goal, the team implemented the FortiAuthenticator solution for all 50 on-site and remote workers. It allowed the municipality to centralize user identity management while offering single sign-on capabilities to reduce password fatigue. Also, it gave the IT team control access for visitors and temporary users with customizable access levels and expiration times. Furthermore, the IT team enabled two-factor authentication with the FortiToken mobile solution, so staff managers could generate one-time passwords to log in to the network.

Increasing Security Layers at the Endpoint Level

Across the 50 FortiAPs, the City of Kimberley also deployed the FortiEDR endpoint security solution to provide real-time monitoring, detection, and automated response to security threats. It features a centralized management console that provides visibility and control, simplifying the management of security policies and deploying response actions.

Fortinet's platform was also spread to all endpoints by deploying the FortiClient Endpoint Management Server in the city's zero-trust network access model. With this solution, the IT team defined dedicated policies for their devices to ensure that only authenticated and compliant devices and users can access sensitive resources. "If it's a laptop, users automatically get remote access set-up," Hlady says. "I also get to see all the endpoints and deal with vulnerabilities even if they have outdated software."

Another layer of security was added through the FortiDeceptor solution, allowing the IT team to deploy decoys to mimic real assets, such as servers and endpoints, to attract attackers. "I have many different lures such as SCADA, Windows, VoIP, and even a FortiGate lure to improve early detection. These are all assets that attackers might want to get into. In fact, there was an occasion when our FortiDeceptor detected a threat and promptly notified both me and my coordinator. Thanks to the solution, we could respond instantly to verify if the activity was legitimate."

The IT team monitors all network activity and collects the logs of all Fortinet devices with FortiAnalyzer. With this solution, they can leverage advanced reporting and forensic analytics and configure alerts and notifications for specific event thresholds to increase the speed of response.

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiAP
- FortiEDR
- FortiAnalyzer
- FortiClient EMS
- FortiAuthenticator
- FortiToken
- FortiDeceptor
- FortiRecorder
- FortiCamera

Services

- FortiGuard Managed Detection and Response (MDR)
- FortiGuard Incident Response (IR)

"Today, we only rely on one vendor for everything we need. I can call the Fortinet support team and talk to support staff within minutes without sending a ticket and dealing with significant downtimes."

Dave Hlady
Manager of Information Technology,
City of Kimberley

Comprehensive Framework with Full Connection

For the IT manager, however, one of the critical aspects of the Fortinet Security Fabric is the telemetry that allows all devices to "talk to each other." He says: "If the system identifies a vulnerability and one of my endpoints gets infected, I can set policies and shut it down immediately. And that's the FortiEDR talking to my FortiGate, and my FortiGate talking to my FortiSwitches."

"This communication and integration go along with the fabric's ease of configuration," Hlady asserts. "I find it very intuitive. I like the graphical user interface. Management-wise, the fabric is very good. If you get onto one appliance, say a FortiGate, you can jump on to FortiAuthenticator or FortiDeceptor. It's almost like a mirror on each device. You know right off the bat what you're looking for."

Coordinating different security components has led to a more robust and adaptive defense strategy for the City of Kimberley. The unified threat intelligence of FortiGate and FortiClient ensures that information about threats detected in one part of the network is shared across all security components, enabling a faster and more coordinated response.

Additionally, the municipality implemented FortiRecorder and FortiCamera, part of Fortinet's network video surveillance solution. They are designed to provide comprehensive video security and monitoring, integrating seamlessly with the Fortinet Security Fabric.

The Convenience of a Single Vendor

Overall, the Fortinet Security Fabric platform has significantly impacted the city of Kimberley's cybersecurity strategy and stance. "The difference is completely night and day. Before, we were relying on a firewall and a third-party antivirus that wasn't communicating together," Hlady explains. "We've gone from having nothing to having almost everything."

The deployment has also impacted every stakeholder within the municipality, especially at the C-level. "I have to say that our senior management is very happy," he says. Today, the City of Kimberley can collect, store, and manage critical inhabitant information more safely and continue supporting the community without fearing any data breach or cyberattack that can also endanger the welfare of its residents.

The IT manager asserts that fabric's integration also has enormous benefits in terms of support. "Today, we only rely on one vendor for everything we need. I can call the Fortinet support team and talk to support staff within minutes without sending a ticket and dealing with significant downtime. Fortinet also helps us sort out any issues with setting up new rules or policies, especially when they don't function as they should."

The municipality also leverages the FortiGuard Managed Detection and Response (MDR) Service. It offers the city 24x7 continuous monitoring of workstations and servers by Fortinet's MDR team using the FortiEDR platform. It helps the city offload security operations center efforts to the globally located FortiGuard MDR team. Also, the FortiGuard Incident Response (IR) Service allows the City of Kimberley to proactively prepare for an environmental incident or breach.

The next step in the municipality's cybersecurity journey is to enable Fortinet Secure SD-WAN on the FortiGate. "It seamlessly integrates with Fortinet's fabric with plenty of flexibility and cost-effectiveness through its broadband options," Hlady says. "This will certainly help us maintain a simplified network architecture." Lastly, Hlady and his team are planning to implement FortiExtender in the city's water PRV locations.

September 6, 2024 9:30AM / 2842160-0-0-EN