CASE STUDY

Canadian School District Enhances Remote User Security and Drives Operational Efficiencies with Fortinet Single-Vendor SASE



Wellington Catholic District School Board (WCDSB) consists of 18 elementary schools, three secondary schools, and an alternative education program. The board meets the educational interests of more than 8,000 students across 26 sites in the city of Guelph and the county of Wellington in Ontario, Canada.

A Long-Standing Fortinet Shop

In 2017, the Ministry of Education in Ontario launched the "Broadband Access for All Students" initiative, with the goal of delivering one megabit per second of connectivity to every student across the province.

To meet this goal, WCDSB deployed Fortinet Secure SD-WAN (software-defined wide area network) across its 26 locations. As a result, the district could use broadband internet links instead of its legacy multiprotocol label switching (MPLS) connections, which were more expensive to run.

Peter VanDorp, Cybersecurity Analyst at Wellington Catholic District School Board, explains that this change led to an immediate benefit for end-users: "We no longer had to filter based on whether applications were using too much bandwidth. Thanks to Fortinet, we only need to block when there is a legitimate need, not because the network cannot handle it."

Today, the district uses almost entirely Fortinet Security Fabric solutions for its security and network infrastructure, including the FortiGate Next-Generation Firewalls (NGFWs), FortiSwitch secure Ethernet switches, FortiAP access points, FortiManager centralized management, FortiAnalyzer for logging and analytics, the FortiNAC network access control agent, and the FortiClient endpoint agent. The district also uses the FortiCamera surveillance system for physical security, and FortiVoice secure unified communications.

Meeting the Remote-Learning Security Imperative

In 2021, the Ministry of Education in Ontario created a reference architecture for schools within its jurisdiction to secure remote learning for staff and students as a result of the COVID-19 pandemic. Within that reference architecture was a recommendation to work with cloud-based secure access service edge (SASE) solutions.

VanDorp explains: "The aim of the reference architecture was to ensure that school districts could provide exactly the same level of protection for students and staff outside of schools as they are used to on school premises. That meant finding the right balance between locking down the network and ensuring that users could work and study freely."

"Fortinet came out on top. FortiSASE seamlessly integrates with our existing products while protecting our previous Fortinet investments. And, it was easy to extend FortiClient to FortiSASE, which freed us from needing to train our people on a new SASE solution. FortiSASE was really the next step in our network evolution."

Peter VanDorp
Cybersecurity Analyst
Wellington Catholic District School Board

Details

Customer: Wellington Catholic District School Board

Industry: Education

Location: Ontario, Canada

Business Impact

- 30% reduction in overall TCO through integration
- 2,000 hours saved annually in training with faster user onboarding

Offering remote learning capabilities on this scale was a significant challenge. "At that time, we had great security within the network perimeter, thanks to Fortinet Secure SD-WAN," says VanDorp. "But apart from providing VPN tunnels back to our FortiGate NGFWs for some of our office staff, we had no remote working capability at all."

As outlined in the ministry's reference architecture, SASE could provide a solution to this challenge. As a cloud-based solution, it can simplify the management and configuration of the security processes required for remote learning, including endpoint protection, extending antivirus across the distributed perimeter, and putting in place robust deep packet inspection (DPI) capabilities.

Other business drivers for moving to a SASE architecture included leveraging managed solutions to free internal resources from configuring and maintaining devices to focusing on security strategy, delivering a predictable pricing structure with lower and simplified budgeting, and increasing scale, control, and flexibility in security and networking.

Finding the Right SASE Solution

Following a review of leading SASE solution providers, the board selected Fortinet. VanDorp explains: "Fortinet came out on top. FortiSASE seamlessly integrates with our existing products while protecting our previous Fortinet investments. And, it was easy to extend FortiClient to FortiSASE, which freed us from needing to train our people on a new SASE solution. FortiSASE was really the next step in our network evolution."

Today, the company uses FortiSASE to enable consistent security policies and management on-premises and in the cloud. The solution delivers zero-trust network access (ZTNA) to school resources and protects internet access through a secure web gateway (SWG). Through the FortiSASE next-generation cloud access security broker (CASB), WCDSB can also control cloud applications to secure sensitive data and detect and remediate malware.

The Single-Vendor SASE Dividend

By selecting its installed security partner for its SASE evolution, the district has realized significant time savings. "There was a minimal learning curve for us with FortiSASE," comments VanDorp. "That meant we could deploy much faster, which saved us time and money." The district has unlocked a 30% reduction in overall total cost of ownership in part due to the smooth integration of FortiSASE, as well as savings in training time, which amount to 2,000 hours annually.

VanDorp adds: "By partnering with Fortinet, we deployed SASE while cutting costs. We essentially shifted our FortiClient investments into our new SASE capability."

Management Made Easy

Moving to FortiSASE has made it far easier for the board's IT team to manage the district's security and network infrastructure. As VanDorp explains: "FortiSASE delivers true single-pane-of-glass management, and we have found it easy to use. We can now deploy DPI with a single click of a button, which saves us time and effort."

Business Impact (cont.)

- Flexibility and security across on-premises and cloud systems
- Consistent security across schools, staff, and students, wherever their location

Solutions

- FortiSASE
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiGate Next-Generation Firewall
- FortiAP
- FortiClient EMS
- FortiManager
- FortiAnalyzer
- FortiNAC
- FortiCamera
- FortiVoice

"With the implementation of Single Sign-On in FortiSASE, most users do not even realize they are on a new system. That is the beauty of the product—it just works."

Peter VanDorp
Cybersecurity Analyst
Wellington Catholic District School Board

Being able to manage and address everything from a single location is particularly important for WCDSB as it only has a small team, and resources are tight. “In education, every dollar that we spend on technology is a dollar that is not going to the classroom for learning. That is always something that is back of mind,” VanDorp adds.

Delivering for Users

A core aim of this deployment was to ensure that staff and students have everything they need for secure, effective digital learning. VanDorp reports that the user experience has improved dramatically following the implementation of FortiSASE, so much so that the IT team regularly receives positive feedback from end-users.

“With the implementation of Single Sign-On in FortiSASE, most users do not even realize they are on a new system. That is the beauty of the product—it just works,” says VanDorp.

Next Steps

VanDorp explains that Fortinet has been highly flexible, working in close collaboration to ascertain the district’s needs and create a solution that meets these needs exactly.

Looking ahead, VanDorp hopes to further exploit the convergence of SD-WAN networking and cloud-delivered security that Fortinet can provide. He concludes: “We next want to extend ZTNA to cover all networked devices that could potentially pose a security risk.”

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

September 22, 2023 10:10 PM

2185804-0-0-EN