Located in Montgomery County in the state of New York, the Greater Amsterdam School District (GASD) comprises four elementary schools, one middle school, and one high school. The district’s IT department supports approximately 700 staff members and up to 4,000 students.

Holding the Line

Cybercriminals have K–12 organizations set firmly in their sights, with schools among the most frequently targeted organizations in the United States today. As a public sector institution with tight budgets and a small IT team, GASD has to hold the line against attackers—and it’s a significant challenge.

Eric Scholl, Chief Security Officer (CSO) at GASD explains: “We have a small IT department, and we have to cope with a barrage of cyberattacks. We also have to ensure that we are up to date with our compliance, which presents another significant challenge.”

In 2020, the compliance burden increased with the introduction of New York State Education Law 2-d, which mandates that educational institutions’ technologies, safeguards, and processes align with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (the NIST Cybersecurity Framework).

GASD used the introduction of this law as an opportunity to overhaul its network and security systems. “We realized that we had a lot of security gaps,” says Scholl, “and we needed to better integrate our systems. At the time, we were using equipment from a range of different vendors, which added unnecessary complexity.”

Selecting as Network Transformation Partner

GASD has been a Fortinet customer since 2016, when they installed FortiGate Next-Generation Firewalls (NGFWs) to protect its network edge.

“When it came time to refresh our network and security systems, Fortinet was the obvious choice,” says Scholl. “Our experience with the FortiGate NGFWs has been great, and we were impressed by the level of integration enabled by the broader Fortinet Security Fabric as well as Fortinet’s competitive pricing. Importantly, Fortinet could also provide the level of security required to access federal government and state funding and deliver against the NIST Cybersecurity Framework.”

Financing the Network Transformation

To help finance the project, GASD secured grants from the COVID-19 Elementary and Secondary School Emergency Relief Fund and ARP funding. The district also secured support from the Federal Communication Commission’s (FCC) E-Rate program.
Finally, GASD's network overhaul benefitted from nearly $1 million in funding from the FCC's Emergency Connectivity Fund (ECF), a $7.171 billion program aimed at helping schools and libraries provide tools and services to support remote learning.

Closing Critical Security Gaps

As well as upgrading its FortiGate NGFWs, the district started by implementing FortiMail, Fortinet's email security solution, to protect staff and student Gmail accounts. Next, the district implemented FortiXDR (extended detection and response) to protect 1,000 endpoints, including servers and laptops, with automated detection, investigation, and remediation tools. It further enhanced this capability through the FortiClient Fabric Agent, which provides greater endpoint information, visibility, and control.

GASD has achieved further protection through the implementation of FortiAuthenticator, which enables seamless and secure two-factor authentication across the organization in conjunction with FortiToken one-time password (OTP) generators. With FortiToken, a password is used along with a physical or mobile application-based token according to user preference.

GASD also optimizes its Security Fabric with FortiAnalyzer, which provides Security Fabric analytics and automation.

Building Out the District's Defenses

Another significant element of GASD's security transformation is the use of FortiGuard Security Services, a suite of services that delivers artificial intelligence (AI)- and machine language (ML)-powered protection across the Security Fabric. GASD has implemented the FortiGuard Unified Threat Protection (UTP) Bundle, with a particular focus on its deep packet inspection (DPI) capabilities, URL filtering, Domain Name System (DNS) filtering, antivirus, inline sandbox, and intrusion prevention system (IPS) services.

The district's security transformation will continue with the rollout of FortiSIEM (security information and event management) and FortiNAC (network access control) in the months ahead. "We are already using the network access control features of the FortiGate NGFWs," explains Scholl, "so we have seen what Fortinet can deliver in terms of streamlined management and improved visibility. We cannot wait to unlock the benefits of the full FortiNAC solution."

Refreshing and Extending the Network

One significant element of GASD's network transformation has already been completed with the deployment of 1,200 Linksys HomeWRK for Education devices. Secured by Fortinet, these devices provide students with reliable and secure internet connectivity for schoolwork, leveraging multiple cellular carrier networks to deliver the best connection available. Linksys HomeWRK extends FortiGuard enterprise-grade security services, including content filtering to the home. And IT teams can easily roll out the plug-and-play solution to students for home connections in minutes with zero-touch provisioning.

Now, the district is focused on completing the rollout of its new wired and wireless network based on FortiSwitch and FortiAP (access point) devices. Already, GASD has implemented 10 FortiSwitch devices in its core network. Next, the district plans to finish deployment of FortiSwitch and FortiAP at the local-area network (LAN) edges.

Business Impact (cont.)

- Significantly improved security posture and reduced operational risk
- Improved access to cyber insurance
- Secured internet connection at home for disadvantaged students
- Support with federal funding applications

Products and Solutions

- FortiGate Next-Generation Firewall
- FortiMail
- FortiAuthenticator
- FortiSwitch
- FortiAP
- FortiNAC
- FortiSIEM
- FortiClient
- FortiAnalyzer
- FortiXDR
- Linksys HomeWRK for Education

FortiGuard Security Services

- URL filtering
- DNS filtering
- Antivirus
- Inline sandbox
- Intrusion Prevention System
- Deep packet inspection
Increased Visibility, Control, and Protection

One of the key benefits of GASD’s new systems is that they enable a holistic approach to security. “I appreciate the entire Security Fabric, as it is part of a coherent, interconnected ecosystem, which enables us to see real-time intelligence and provide defense in depth against those who would seek to do my staff and students harm,” says Scholl.

Utilizing the Fortinet Security Fabric, the district has reduced its attack surface significantly through increased visibility across all facets of its IT and operational technology (OT) infrastructure. Scholl explains: “The design of the FortiGate NGFW, with its ability to offload work to tailor-made ASICs, provides us with visibility into 100% of our network traffic without a hit to performance.

“Current figures are that over 80% of internet traffic is encrypted via SSL/HTTPS, which means if you are just doing standard certificate inspection, you are in fact missing 80% of the threats coming into your network. Utilizing DPI on the FortiGate NGFW, we can decrypt and scan that 80% of SSL/HTTPS traffic to ensure there are no threats coming into our network—all this with a minimal hit to performance compared to other vendors’ solutions.”

In addition to the overarching benefits of integration, individual products are helping boost security at GASD in specific ways. For instance, FortiMail has provided better content filters and as a result has all but stopped phishing emails from getting through. “Just looking at today alone, by 10 a.m. FortiMail has flagged 13,511 spam messages and 20 confirmed viruses. That is incredible performance,” adds Scholl. GASD uses FortiMail in the gateway operation mode with a FortiGuard Enterprise Advanced Threat Protection (ATP) Bundle, which allows full control of multiple email security features.

FortiAuthenticator is also providing a significant security boost. Scholl explains: “When a teacher had a district-owned laptop stolen by a student, we were able to use the FortiAuthenticator Client for Windows to determine who had taken the device.”

When the student made a logon attempt, FortiAuthenticator sent a push notification to the teacher’s FortiToken phone app. Scholl was then able to use the FortiAuthenticator logs to determine the Internet Protocol (IP) address of the device and then identify which FortiAP was used during the logon attempt.

“I then used security camera footage to check who was in the area of the FortiAP when the logon attempt was made and who was using the laptop,” says Scholl. “We then gathered these students together and let them know the repercussions of theft and how it would affect their lives if they were caught. The student returned the laptop to the teacher within 30 minutes.”

Supporting Cyber Insurance

As a result of its enhanced cyber defenses, GASD is now both compliant with New York State Education Law 2-d and also better able to secure cyber insurance. FortiAuthenticator has been a key capability in this regard. Scholl explains: “In the past, we relied on staff and students inputting the data required to set up password resets and two-factor authentication, which often they would not do. With FortiAuthenticator, all we need to do is provide them with a FortiToken.”

The data loss prevention (DLP) feature of the FortiGuard Security Services has also helped from a cyber-insurance perspective. As Scholl explains, DLP is a significant challenge for K–12 environments, because education is largely predicated on sharing. DPI is another feature that provides the IT team visibility into everything going in and out of the network, allowing them to take appropriate action. One of the features it uses is virtual private network (VPN) blocking to stop students from using personal VPN workarounds.

Scholl continues: “We can only get the best cyber insurance if we can prove we have the highest levels of security. Thanks to Fortinet, we can do just that. Recently, a neighboring school district came under a heavy DoS attack and the network fell
down as a result. We came under the same attack, but our FortiGate NGFWs simply quarantined the IP addresses that were attacking us, and we were able to keep our network up and running.”

Intuitive, Convenient Installation and Management

Scholl has also been impressed with the ease with which he has been able to set up and manage Fortinet’s equipment. “The FortiSwitches are a great example. They are integrated into the Fortinet Security Fabric via FortiLink. With this integration, we can manage everything through the FortiGate NGFW interface. This provides us with a single-pane-of-glass view into the network and further increases visibility and control of users and devices. Building up our network could not be easier. Installing a new FortiSwitch is just a matter of plugging it in and connecting some cables—everything else is programmed and ready to go.”

Scholl says that simplicity and ease of use are hallmarks of all Fortinet devices. “Whatever the product, Fortinet outperforms the market in terms of ease of management. We are able to install devices rapidly and start benefitting from day one. I spend just 45 minutes on FortiAnalyzer, FortiMail, and the FortiGate NGFWs, checking that everything is running well. Before Fortinet, the same effort would have taken up most of my morning.”

The Benefits of True Partnership

GASD also recognizes that the strong relationship with Fortinet has been a significant benefit. “The support from Fortinet is outstanding,” Scholl says. “For instance, when we were deploying FortiXDR, Fortinet provided an engineer to sit with me one day a week for a couple of months to fine-tune the system and reduce false positives. They are always ready to go the extra mile.”

Fortinet’s approach to partnering with GASD extends beyond the technology itself. Fortinet helped GASD during the application process for the ECF funding round. As a result of this grant, GASD was able to fund the entirety of its Linksys HomeWRK for Education rollout.

Supporting Inclusive Education

With the 1,200 Linksys HomeWRK for Education devices in place, GASD is now able to support approximately a third of its student population with home connectivity. This is a significant achievement as it means that students can work effectively from home regardless of their socio-economic background.

As Scholl explains: “Some of the families who send their children to our schools cannot afford fast internet connections at home. Thanks to the ECF funding that Fortinet helped us secure, and the excellent capabilities of the Linksys devices, these students can now work from anywhere.”

The devices have proved to be beneficial to students in a number of other ways. “One student was hit by a car when walking to school,” explains Scholl. “Fortunately, we had just received the shipment of hotspots, and we were able to provide the student with internet access so the student could remotely and securely connect their district Chromebook and not fall behind on their work.”

With the security provided by Fortinet, GASD is also able to comply with relevant regulations when enabling home working for students. “We could enable content filtering on all the devices, which was great from a compliance perspective,” says Scholl. The solution helps schools meet the Children’s Internet Protection Act (CIPA) compliance requirements, for example. “And with the security from Fortinet, students can work without having to worry about having their identity stolen or falling victim to other types of cybercrime.”
Looking Ahead

Once the district is completely up and running on the Fortinet Security Fabric, it intends to fully embrace zero-trust network access (ZTNA). The district is already experiencing early benefits. As Scholl explains: “Through ZTNA, we have been able to isolate our HVAC and OT network and eliminate IPsec and SSL VPN needs for our vendors. With FortiClient EMS, we are able to ... enable connectivity based on device and user identity for our vendors. Furthermore, we are able to enforce vulnerability scans on the vendor devices that are attempting to connect via ZTNA as well as ensure they have antivirus enabled and updated. These features allow us to further reduce our attack surface to outside and inside threats.”

Combined with FortISIEM, Scholl hopes the FortiNAC will bring new levels of automation to the security function, helping its small team keep on top of their challenges. “We are always understaffed, so any way in which we can save time through automation is welcome,” Scholl concludes. “Fortinet has delivered unprecedented levels of automation to enable us to achieve the same levels of protection that once would have required an entire security team to achieve.”