

CASE STUDY

Fortinet Helps a Large Educational Services Provider Boost Cybersecurity and Ensure Regulatory Compliance for Its School Districts

Established in 1967, the Board of Cooperative Educational Services of Nassau County (Nassau BOCES) is the largest BOCES in New York State. A state agency, Nassau BOCES serves 56 school districts. It aims to enhance public education and the opportunities available to students of all ages and abilities by providing innovative and cost-effective services. Nassau BOCES operates across more than three dozen locations, delivering approximately 100 different student and staff programs and services, including a network operations center (NOC) and managed technical services such as network rollouts, cloud migrations, and cybersecurity support.

The organization employs approximately 2,500 people and provides technical support to several hundred facilities across its school districts. Its technical staff includes 20 staff based in the NOC and an additional 150 engineers deployed at various sites across the state.

Drivers for Excellence

Nassau BOCES's prime operational driver is to meet its corporate mission. Sandeep Dhillon, Executive Manager at Nassau BOCES, explains: "Our North Star as an organization is to provide the very best technology options for our school districts at the lowest possible price points. Without sacrificing on quality and capability, we want to keep costs down for the districts so they can invest their budgets in delivering exceptional student experiences."

Regarding data privacy and security, Nassau BOCES also faces a significant external driver for excellence: New York EdLaw 2-d. In effect since 2020, the law requires that educational agencies and their contractors strengthen data privacy and security to better protect students' personally identifiable information (PII) and annual professional performance review data. "EdLaw 2-d has been a big change driver for us," says Dhillon. "It prompted us to review our security posture and make changes to ensure the highest levels of data protection."

One of the areas identified as ripe for improvement was the organization's firewalls. "We had in place devices that operated through ACLs [access control lists], which are not that effective and harder to support for east-west traffic monitoring and inspection," says Dhillon. "We wanted a more flexible and user-friendly alternative that would make it easy for our people to get into the firewall and understand why traffic is being blocked."



"The value was so much better than competing proposals; it piqued our interest. Then we started to look into the products, and we were blown away by their capabilities."

– Sandeep Dhillon, Executive Manager, Nassau BOCES

Details

Customer: Nassau BOCES

Industry: Education

Location: Nassau County, New York

Business Impact

- Significantly reduced the total cost of ownership for its school districts
- Enhanced its security capabilities and enabled compliance with New York EdLaw 2-d
- Enabled load balancing to support distributed, cloud-based working

In addition, Nassau BOCES hoped to find a system that would enable it to create rules and seamlessly integrate with the proliferation of cloud services in use since the onset of the COVID-19 pandemic. Dhillon adds: “The pandemic and the resulting move to remote working really shook up our district’s requirements. With workloads shifting from on-premises to the cloud, we needed to find a way to secure a distributed network perimeter.”

Reconnecting with Fortinet

To meet its regulatory compliance objectives, Nassau BOCES issued a request for proposal (RFP) to help evaluate the best companies to partner with. A Fortinet customer since the early 2000s, Nassau BOCES was inspired to look again at the company and its solutions due to its price-to-performance ratio. “The value was so much better than competing proposals; it piqued our interest,” recalls Dhillon. “Then we started to look into the products, and we were blown away by their capabilities.”

Today, Nassau BOCES offers its school district security and networking capabilities based on FortiGate Next-Generation Firewalls (NGFWs) for east-west traffic inspection and monitoring. In addition, the organization uses its FortiGate NGFWs to support its security operations center (SOC) and NOC by creating security baselines. Nassau BOCES also leverages integrations with FortiGate NGFWs and its security information and event management (SIEM) platform to better respond to malicious URLs and IP addresses. The FortiGate devices are supported by FortiManager for centralized control and management and FortiAnalyzer for security analytics and automation.

In addition, the organization uses the Fortinet Secure software-defined wide-area networking (SD-WAN) capability on its FortiGate NGFWs for load balancing WAN links to support higher demands on bandwidth during the post-COVID approach to distributed, cloud-based working. “We have a FortiGate NGFW in place locally at each building,” explains Dhillon. “We then use dynamic VPN [virtual private network] tunnels between buildings for legacy communication, effectively serving as a wide-area network. The approach is remarkably successful, and we can update everything centrally using the FortiManager.”

Because Nassau BOCES operates as a managed security services provider (MSSP) to its districts, it has also created separate administrative domains (ADOMs). Doing so enables the organization to centralize the management of Fortinet devices for the 28 school districts it directly supports. “Fortinet gives us the ability to port these 28 districts into our central FortiManager instance and then push out the needed FortiGuard artificial intelligence (AI)-powered Security Services and policies and updates to ensure their security posture is as strong as possible,” adds Dhillon. The approach also means that Nassau BOCES can help the districts it manages rapidly recover from outages.

Securing the Perimeter

In addition to the robust firewall rules that come with the FortiGate NGFWs, Nassau BOCES benefits from the FortiGuard Security Services ATP (advanced threat protection) Bundle. FortiGuard Security Services is optimized by AI and machine learning (ML) to create a proactive and automated security posture to detect and protect against rapidly evolving targeted threats. One service it uses includes an advanced intrusion prevention system (IPS). These include zero-day exploits, network intrusions, ransomware, cryptomalware, and known and previously unknown file-based attack tactics.

Fortinet’s products integrate seamlessly with one another and third-party systems, adding another benefit when it comes to increasing security. “The ability to create rules and integrations is not something we had prior to Fortinet,” says Dhillon. “Now we can integrate easily with our various enterprise platforms and automatically update our rules. This gives us much more control.”

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiAnalyzer
- FortiAuthenticator
- FortiManager

FortiGuard Security Services

- IPS

“Just for the price we were paying for software renewals, we have been able to buy two new pieces of hardware for our organization. And similar savings have been experienced by all the districts we work with. Fortinet is therefore helping us meet our central charter by helping us drive value for districts while delivering solutions that hit the mark every time.”

- Sandeep Dhillon, Executive Manager, Nassau BOCES

The organization also appreciates the high levels of integration between the FortiGate NGFWs and Microsoft Sentinel, its SIEM platform. “Fortinet enables us to automate a number of the processes linking the firewalls and our SIEM, saving our team a great deal of time and effort,” says Dhillon.

Segmenting the Network

When it comes to complying with EdLaw 2-d, the network segmentation capabilities of the FortiGate NGFWs have proved to be highly valuable. “This new law has given schools a whole new set of responsibilities in ensuring against PII data exfiltration and infection by malware. The FortiGate NGFWs have proved to be a huge benefit in this regard as they stop lateral movement across the network and provide the highest levels of intrusion prevention and anti-malware protection.” FortiAnalyzer will also help the organization ensure compliance with EdLaw 2-d by providing insights, such as information about the source of malware.

Fortinet further protects PII by enabling multi-factor authentication (MFA) when staff or students access financial systems using a VPN. And because the FortiGate NGFWs integrate with Microsoft and Google applications using Security Assertion Markup Language (SAML), Nassau BOCES can enable MFA with ease. The approach satisfies auditors and helps reduce the organization’s cybersecurity insurance premiums.

Moving forward, Nassau BOCES plans to build on this approach by using FortiAuthenticator to authenticate guests logging in to its networks. “Some of the districts cannot afford a true NAC [network access control] solution, so FortiAuthenticator provides an alternative. That said, we are also looking at deploying FortiNAC elsewhere on the network to restrict access to the network from unknown or outdated devices, which is an important security consideration for us.”

Supporting Distributed Working

The built-in SD-WAN capabilities provided by the FortiGate NGFWs came to the forefront during the pandemic. Using the Fortinet Secure SD-WAN capability, the organization was able to provide multiple broadband and multiprotocol label switching (MPLS) lines and use the FortiGate NGFWs to load balance during periods of peak demand. “The load balancing works flawlessly, and it saves money for our districts as we no longer need to maintain a redundant line as failover,” says Dhillon.

Dhillon believes that the Fortinet Secure SD-WAN solution will be deployed more fully and widely soon: “At present, we have one school using the full capabilities of the Fortinet Secure SD-WAN solution. However, I believe that when the time comes for other districts to look at their network setup, most will replace their existing MPLS networks in favor of broadband using the Fortinet Secure SD-WAN, given the lower cost and greater resilience of the approach.”

Price to Performance Is a Bright Spot

For Nassau BOCES, one of the most important benefits of working with Fortinet is the value it provides—both for the districts and BOCES itself. Driven by Fortinet’s application-specific integrated circuit (ASIC) architecture in every model, Fortinet is able to achieve a price-to-performance ratio other cybersecurity providers cannot offer. “Just for the price we were paying for software renewals, we have been able to buy two new pieces of hardware for our organization,” says Dhillon. “And similar savings have been experienced by all the districts we have worked with. Fortinet is therefore helping us meet our central charter by helping us drive value for districts while delivering solutions that hit the mark every time.”



www.fortinet.com