CASE STUDY

# Pennsylvania School District Improves Network Visibility and Control Through the Fortinet Security Fabric

East Stroudsburg Area School District is a 216-square-mile public school district located in northeast Pennsylvania's Poconos region. The district comprises six elementary schools, two middle schools, two high schools, and one cyber academy. In addition, East Stroudsburg's footprint includes four non-instructional facilities, including maintenance garages for its bus fleet. The district has enrolled 6,500 students who are served by a staff of 1,200 people.

Brian Borosh is the director of technology at East Stroudsburg Area School District. "As with any school, we face a wide range of threats to our network and IT infrastructure," says Borosh. "Back in 2015, our challenges chiefly concerned preventing unauthorized devices connecting to our network—something that happens a lot in schools—and improving network visibility. That was when we initially brought Fortinet on board."

In this first stage of its partnership with Fortinet, the East Stroudsburg Area School District deployed the FortiNAC[1] network access control solution, which further increased its network visibility and enabled its IT team to immediately remove unauthorized devices from the network. Next, the district added FortiGate Next-Generation Firewalls (NGFWs), which seamlessly integrated with FortiNAC, for enhanced edge security and network visibility. The NGFWs were augmented by FortiAnalyzer, which provides additional network intelligence and insights.

## Addressing the Evolving Threat Landscape

However, in the years since 2015, the threat landscape has continued to evolve, and so have the district's security needs. Borosh explains: "Our main goal is to stop attackers from penetrating the network, in whatever form that takes. Ransomware is one priority, given the increasing use of this attack method; but we also come up against a lot of denial-of-service (DoS) attempts, often orchestrated by our own students hoping for a day off from lessons. The education sector is unique in that its biggest security challenge is quite often the insider threat."

David Cooper, network analyst at East Stroudsburg Area School District, adds: "Zero-day threats have become particularly challenging, such as new 'browser in a browser' phishing spoofs. Cyber criminals are more sophisticated than ever, and we need a security system that can shut down threats that are entirely new and for which there are no known signatures or profiles."

## Building on the Fortinet Security Fabric

Based on its excellent experience with Fortinet products and support since 2015, the district expanded its Fortinet Security Fabric footprint in 2020 and 2021 with two new products and one product refresh. The two new products, which are now operational, are FortiEDR for endpoint detection and response, and FortiSIEM

EAST STROUDSBURG AREA SCHOOL DISTRICT

*"Security alerts happen all the time, and in order for me to do anything else with my day, I need to have information at my fingertips. Fortinet's solutions provide me with just that."*

– David Cooper, Network Analyst, East Stroudsburg Area School District

## Details

**Customer:** East Stroudsburg Area School District

**Industry:** Education

**Location:** East Stroudsburg, PA

**Endpoints:** 1,500

## Business Impact

- Enhanced visibility and threat response to stop bad actors before they cause damage
- Data aggregation and in-depth analysis to better identify and remediate suspicious network activity

for security information and event management. The product refresh was for its FortiGate NGFW; the district doubled its devices to enable redundancy and upgraded to to the current version.

The district uses FortiEDR to drive real-time visibility, analysis, and threat protection and remediation for faculty devices and student workstations, helping it keep pace with the evolving threat landscape. Meanwhile, the district uses FortiSIEM to analyze data from across its network and devices to better spot suspicious activity and data exfiltration. FortiSIEM was deployed with the help of the Fortinet Professional Services team, which helped the district's IT team integrate and configure the system for optimal performance.

## High Responsive Threat Mitigation

Since deploying FortiEDR to 1,500 staff endpoints and lab computers, East Stroudsburg Area School District's IT team has been impressed with the speed and responsiveness of the system. "I am always on the lookout for bad actors coming onto the network, and FortiEDR helps me immensely in this work," says Cooper. "Recently, an attacker compromised one of our devices and the FortiEDR picked up on it immediately, automatically stopping the compromise at the source. That has been our experience ever since deploying the system: as soon as a student or employee clicks on a bad link, or downloads something risky, the FortiEDR catches it immediately and its automatic remediation means our network is never at risk." FortiEDR has also been instrumental in helping the district rapidly detect students attempting to launch DoS attacks and lock them out from the network.

Meanwhile, the district notes significant benefits from FortiSIEM, particularly when it comes to identifying and stopping data exfiltration. Cooper explains: "FortiSIEM allows us to conduct in-depth research and analysis of traffic history, which it ingests from our Active Directory servers, our FortiGate NGFWs, and our core switches. Armed with this data, we can see exactly where data flows, allowing us to identify suspicious activity. Soon we will also integrate data from the FortiNAC, which will provide a complete picture of everything that happens on our network. Fortinet has therefore enabled a new level of visibility and understanding, which greatly enhances our security posture."

The district's IT team has found that the ability to go back and review historic network traffic is a key benefit of FortiSIEM. The solution automatically combines data from multiple sources, which reduces the time it takes for the team to resolve potential security issues. Prior to FortiSIEM, time-consuming tasks like manually unifying datasets fell on few shoulders in the relatively small IT team of 16 people. As Cooper explains: "Security alerts happen all the time, and in order for me to do anything else with my day, I need to have information at my fingertips. Fortinet's solutions provide me with just that."

## Complete Interoperability for Seamless Infrastructure Management

While individually the district's new systems are delivering significant benefits, the whole is greater than the sum of its parts. Having deployed six Fortinet products (also including FortiToken, which the district uses for one-time password access authentication), the district is leveraging an interoperable Security Fabric that employs one user interface for all systems and which it can manage through a single pane of glass.

### Business Impact (contd.)

- Reduction in manual security processes and time savings for the district's small IT team
- Seamless security system interoperability for enhanced automation and easier infrastructure management

### Solutions

- FortiGate Next-Generation Firewalls
- FortiAnalyzer
- FortiToken
- FortiNAC
- FortiSIEM
- FortiEDR

*"There are so many directions we could potentially take with Fortinet. Its product catalog is second to none across security, networking, and telephony. We do not know exactly where we will go next, but suffice it to say that we consider Fortinet a partner for the long term."*

– Brian Borosh, Director of Technology, East Stroudsburg Area School District

Borosh comments: “It is too difficult to manage firewalls, endpoint detection and response tools, and SIEM solutions when they are all from different vendors. Fortinet unifies our network security system, which makes it far simpler to manage. It also means that we have just one place to go for new products or for issue resolution. The interoperability benefits of the Security Fabric are such that we fully intend to bring more Fortinet products into our network in the years ahead.”

The district also appreciates the levels of automation that is enabled through the Security Fabric. “Interoperability drives better security,” says Borosh. “For instance, the FortiEDR can automatically alert the FortiNAC through a FortiGate NGFW when a bad actor is on the network, and the FortiNAC can then knock them off the network while we investigate. The Fabric gives us much greater visibility and responsiveness than we had in the past.”

## A Strong Partnership for the Future

Over the years, Borosh and his team have come to regard Fortinet as a true partner, rather than just a technology vendor. In addition to service support, the district uses Fortinet Professional Services to help optimize its systems. As Borosh explains: “Fortinet obviously has an in-depth knowledge of its products, and we like to leverage that understanding. We have found its teams’ expertise invaluable in ensuring we get the most out of our investments in terms of functionality.”

Looking ahead, East Stroudsburg Area School District plans to broaden its use of Fortinet products. Its plans start with leveraging the VPN (virtual private network) capabilities of the FortiGate NGFWs to a greater degree. The district had experimented with the functionality at the onset of the COVID-19 pandemic when it needed to support remote learning and teaching at scale. In addition, the district is considering using Fortinet for email security and user identity authentication.

Borosh concludes: “There are so many directions we could potentially take with Fortinet. Its product catalog is second to none across security, networking, and telephony. We do not know exactly where we will go next, but suffice it to say that we consider Fortinet a partner for the long term.”





May 21, 2022 4:37 AM
1609763-0-0-EN