Seymour Public Schools

CASE STUDY

Small-Town System Gains Big Value in Fight Against Cyberthreats With Security Lifecycle Review and Security Operating Platform From Palo Alto Networks

"With the Palo Alto Networks Security Lifecycle Review, we suddenly could see how big a target we really were. It was clear we needed to take action. You can't see something like that and not act."

Rob Dyer | Director of Technology | *Seymour Public Schools*

INDUSTRY
K–12 Education

CHALLENGE
Strengthen security against growing cyberthreats to the schools and town with limited resources and tightening budgets

ANSWER
Palo Alto Networks® Security Lifecycle Review to identify vulnerabilities on the network and provide direction for addressing them; Palo Alto Networks Security Operating Platform with two virtual instances of the next-generation firewall to prevent successful cyberattacks for the schools and town

SUBSCRIPTIONS
Threat Prevention, URL Filtering (PAN-DB), WildFire® malware prevention service

APPLIANCES
PA-3020 (1)

RESULTS
- Protects against 43,000+ previously undetected vulnerabilities revealed on the network
- Prevents successful cyberattacks automatically
- Increases employee productivity through selective content filtering
- Improves bandwidth utilization by 25%
- Delivers strong ROI for organizations with tight budgets

Customer Overview
Seymour Public Schools serves the community of Seymour, Connecticut, with two elementary schools, a middle school and a high school. Incorporated in 1850, Seymour is a town of approximately 16,500 residents, located in the southwestern portion of the state. Seymour Public Schools educates 2,200 students with a strong academic emphasis on college preparation.

Summary
Seymour Public Schools, in Seymour, Connecticut, is focused on preparing its students for college and successful careers. It could not allow cyberthreats to disrupt the education process or expose private information to cybercriminals. However, the schools did not have a true picture of how vulnerable they actually were. When its legacy firewalls were due for upgrading, Seymour consulted with trusted IT adviser and Palo Alto Networks partner Digital BackOffice, who recommended a Palo Alto Networks Security Lifecycle Review. By installing a Palo Alto Networks Next-Generation Firewall behind Seymour's legacy firewall and tracking activity, the SLR showed that more than 43,000 vulnerabilities were slipping past the legacy firewall. Armed with this insight, the school system and town of Seymour collaborated to share infrastructure and free funds to enable the purchase of the Palo Alto Networks Security Operating Platform, convinced that a next-generation approach to security was the most effective way to protect their respective data and users. The result was a dramatic reduction in vulnerabilities and strong intelligence-based prevention of successful cyberattacks, which drove higher employee productivity while improving bandwidth utilization, saving both organizations money.

Addressing Growing Cyberthreats to Schools and Towns
Seymour Public Schools serves a relatively small, close-knit community in rural Connecticut. Yet, it is an organization that thinks big. Fortunate to have a superb teaching staff, students complete their years of primary education well-prepared to take on the rigors of college and pursue successful careers. In fact, in annual testing over the past few years, Seymour Public Schools has ranked highest in the state – and many of its students head off to the best universities in the country.

Naturally, the caliber of its teachers and hard work of the students produce such results. However, the teachers and students also have reliable, secure access to a wide range of digital tools and applications that enhance the education process, thanks to an innovative IT department led by Rob Dyer, director of technology.

Dyer has done much to improve the efficiency and reliability of the network on which the schools rely for effective administration, classroom management, and student research and collaboration. That's really saying something, given an economic climate in which limited state funding has squeezed school budgets tighter and tighter. Not surprisingly, his work caught the eye of the town of Seymour's first selectman, Kurt Miller, who approached Dyer about sharing IT resources to help the town also improve efficiency.

Using grant money, Dyer worked with Miller – whose position is equivalent to mayor – to merge the school system and town networks so they could share the same infrastructure. However, the question of security then came up. The legacy Cisco® ASA firewalls used by both the school system and

"The Palo Alto Networks platform has brought us a secure, efficient infrastructure that enables our employees to be more effective and productive, and through our resource-sharing approach, with very small net impact on our budget. If you compare how far we've come to our actual cost, it's been worth every penny."

Kurt Miller | First Selectman | *Town of Seymour, Connecticut*

town were due to be replaced. Cognizant that schools and towns are just as susceptible to cyberattacks as large enterprises, Dyer wanted to know how vulnerable Seymour truly was. So, he approached his trusted technology adviser, Digital BackOffice – a Palo Alto Networks partner.

Security Lifecycle Review Shines Light on Vulnerabilities

Digital BackOffice recommended conducting a Palo Alto Networks Security Lifecycle Review, which reveals potential network risks that could affect security. The SLR involved installing a Palo Alto Networks Next-Generation Firewall in passive mode behind the Cisco ASA to gather traffic data for about one week, and then report on the findings.

Dyer remarks, "We understood anything that showed up on the SLR was activity that snuck by the ASA. What we saw was very eye-opening."

The SLR showed that Seymour had 252 applications in use on its network – 18 above the industry average – and some not authorized by IT. Of greater concern, 57 of those applications were high-risk, meaning they could introduce or mask malicious activity, transfer files outside the network, or establish inappropriate communication with outside parties. But most alarming of all, the SLR detected more than 43,000 threats on the network, including vulnerability exploits, known and unknown malware, and outbound command-and-control activity. The threats were coming from all over the world – Russia, North Korea, China, Europe, the Middle East and even the United States itself.

"With the Security Lifecycle Review, we suddenly could see how big a target we really were," says Dyer. "It was clear we needed to take action. You can't see something like that and not act."

Miller adds, "The report was written in such a way that a lay person could read it and see there was a problem. You didn't need an IT degree to understand it. We had voter registration, student records, school and town employee records all at risk. We simply had to find a way to fund the next-generation firewall and stop those attacks."

Gaining Control Over Cyberthreats

Dyer had done his due diligence researching next-generation firewalls and knew what he was looking for. Namely, he wanted an integrated approach to security that was cloud-connected to stay current with definitions and updates and enable real-time threat prevention. The Palo Alto Networks Security Operating Platform met those criteria and more.

"I liked the fact that Palo Alto Networks developed their operating environment from scratch," notes Dyer. "That was important to me because it meant there wouldn't be any latent exploits from some older environment being adapted for the next generation. I could see that a lot of the major players were building off of what Palo Alto Networks was doing, which told me they were the real innovators and that everyone else was playing catch-up. The WildFire cloud service, in particular, stood out for me."

Dyer and his team deployed the Palo Alto Networks Next-Generation Firewall and configured it with two virtual instances, enabling the school system and town to share the same device while keeping their traffic separated. This not only saved money for both organizations but also simplified administration for Dyer. Most importantly, the next-generation firewall went to work immediately preventing successful cyberthreats that could disrupt the everyday work of educating students and running the town.

"As soon as we installed the Palo Alto Networks Next-Generation Firewall, we were able to identify computers infected with malware trying to ping outside sites hundreds of times a day," reports Dyer. "We could then reimage those machines, which freed up bandwidth and prevented our 2,500-plus machines from turning into a botnet going out and trying to hack other organizations."

He continues, "There's an expression I learned years ago: 'think globally, act locally.' That's what we're trying to do here by being responsible in securing our environment and not letting it affect others. If everyone did that, we'd have a lot less malicious activity going around the internet."

Improved Productivity, Increased Bandwidth Utilization

In addition to increased visibility, the Palo Alto Networks Security Operating Platform brought Seymour much-needed content filtering, which its previous security implementation did not provide, as well as the ability to automatically block a whole host of applications that would never be used legitimately by the school system or town. Shutting down categories that were unnecessary for work resulted in a noticeable increase in employee productivity. Limiting access to questionable content also reduced the risk of someone getting hit by a "drive-by download" of malicious code from a poorly secured website.

"We're realizing some major benefits from the Palo Alto Networks platform," Dyer points out. "For one thing, we've lessened the threats affecting us, which allows our IT staff to do other things instead of spending time on remediation.

> "Our next-generation firewall is tagging things that our antivirus software is not picking up. Using Traps, and tying that into our firewall and the WildFire service, we have the opportunity to prevent threats from getting through at the endpoints, using dynamic protection that traditional antivirus approaches simply can't match."
>
> **Rob Dyer** | Director of Technology | *Seymour Public Schools*

We've also increased our bandwidth utilization by about 25 percent, so we avoid needing to upgrade our internet because it's loaded with malicious traffic, saving us money."

The value that the Palo Alto Networks platform has brought to Seymour Public Schools and the town of Seymour has prompted Dyer to now look at endpoint protection. The effectiveness of the next-generation firewall exposed how much is slipping through the endpoints and getting caught on the network. Dyer sees the opportunity to stop threats at the endpoint using Traps™ advanced endpoint protection.

"Our next-generation firewall is tagging things that our antivirus software is not picking up," Dyer says. "Using Traps, and tying that into our firewall and the WildFire service, we have the opportunity to prevent threats from getting through at the endpoints, using dynamic protection that traditional antivirus approaches simply can't match."

As with any major IT investment, organizations like Seymour Public Schools must always weigh cost and benefits. Through consolidation and cooperation, Dyer and Miller found a way to use resource sharing to gain efficiencies that enabled these important investments even with a very tight budget.

Dyer comments, "If you truly value your data, you do a security review like we did and find out just how vulnerable your infrastructure is. That clear evidence makes it much easier to convince stakeholders to make the necessary investment. But, you still have to find the money. By merging infrastructure for our two organizations, we reduced the cost burden substantially within our individual budgets."

Miller adds, "The Palo Alto Networks platform has brought us a secure, efficient infrastructure that enables our employees to be more effective and productive, and through our resource-sharing approach, with very small net impact on our budget. If you compare how far we've come to our actual cost, it's been worth every penny."