Sophos Secures and Speeds Up Computers for **Large School District**, Saving Thousands of Labor-Hours for the IT Team

Based in the United States, this large school district serves over 25,000 students from elementary to high school, encompassing 55 schools and offers a wide spectrum of programs that include bilingual language immersion, hybrid learning, and expeditionary learning.

CUSTOMER-AT-A-GLANCE

Industry
K-12 Education

Number of Users
35,000 (students and staff)

Sophos Solutions
Sophos Intercept X Advanced with XDR
Sophos Email
Sophos Central

> *“We put Sophos on the machine and thought, ‘Really? Is this thing running?’ It was really fast.“*
>
> School District IT

Challenges

- Slow systems that dragged down staff productivity
- IT team spending half their days troubleshooting issues
- Former solution not removing viruses it found and not detecting others
- IT team always in reaction mode instead of being proactive about security posture

In this case study, Sophos spoke with their Senior Systems Administrator who has been with the district for more than 10 years and was part of the team that brought in Sophos about a decade ago. They work on the infrastructure team, overseen by the district’s Executive Director of IT, who also oversees the network, computer information systems (CIS) administration, and telecommunications teams—all of which consist of about 60 people. The district employs over 5,000 staff members.

What are the main pain points that drives a school district to consider Sophos?

The district’s previous antivirus solution was causing multiple problems with the health of their endpoints. Often it was not detecting viruses, and, when it did, it didn’t remove them. Aside from the solution not working as intended, it slowed down the endpoints.

“It would sit there and just chunk on the CPU and memory, making it difficult and slow to run normal Windows processes and programs like Microsoft Word and Excel. Staff members would call us all the time saying, 'Gosh, this is really slow, it's just dragging." As a consequence, this IT team spent about half their days hunting down and troubleshooting the slow systems.

What does the process of switching to Sophos look like?

As a first step, a request for proposal (RFQ) was put out to three vendors, including their existing security provider. They set up a test device to benchmark how fast the three products would perform and how they would handle various viruses and malware. Out of the three products they tested, they were most impressed with Sophos. "We put Sophos on the machine and thought, 'Really? Is this thing running?' It was really fast," they recalled. Processing speed was important to them. They were also impressed with how fast the Sophos endpoint solution recognized the test viruses and malware.

Once Sophos was selected, deploying Sophos Intercept X Advanced with XDR was straightforward and easy. The team put Sophos through Microsoft System Center Configuration Manager (SCCM) and deployed it to all of the machines within two months.

Rated number one in endpoint security by CRN, Gartner, AVTEST, and other independent third-party organizations, Sophos Intercept X Advanced with XDR provides automatic Endpoint Detection and Response (EDR) to pinpoint and prioritize potential threats on systems. It also includes Extended Detection and Response (XDR), which leverages data sources across other products for a more holistic view of the environment. Especially relevant for this customer is its robust anti-ransomware protection and automatic file recovery.

They also installed Sophos Email, which integrated well with their Microsoft 365 email client. They noted, "Sophos Email works very well at stopping viruses and malware links at the source instead of allowing them get into our mailbox." Sophos Email scans messages and attachments for sensitive data while authenticating senders and encrypting outgoing messages using a variety of industry-standard methods.

How has it been to manage and monitor thousands of Sophos licenses?

This school district deployed Sophos Intercept X Advanced with XDR on tens of thousands of devices. "It's been great," they shared. The team uses the cloud-based Sophos Central dashboard to simplify management of their current Sophos products. The platform enables them to easily monitor all the district's devices, and, if something high risk comes up, they get an email notification and can act on the issue immediately.

"Knock on wood, we've really not had a major incident since we started using Sophos," they pointed out. Even though ransomware attacks and other threats are fairly common occurrences in an environment where students tend to click on potentially malicious links, they have also seen a noticeable decrease in the volume of attacks that the team has had to deal with.

One attack that did occur early on in their deployment was detected and stopped by Sophos before it got deep into the environment. The district got hit with the CryptoLocker ransomware attack, which took center stage in 2013 to 2014 and utilized a Trojan to encrypt files on Windows computers and then demand payments to decrypt them. Fortunately the school district had Sophos in place. "Sophos Intercept X Advanced with XDR protected us from a lot of ransomware attempts that could have caused issues with our environment," they asserted.

What value does Sophos provide to long-term education customers?

Sophos has allowed their IT team to be proactive, rather than reactive, about their security posture. Thanks to Sophos, the team has been able to work on higher-level projects with the time they gained back from not having to "troubleshoot and fight with the old antivirus system." Timewise, they noticed a big change after deploying Sophos. "We probably gained back at least half of our day," they estimated.

They feel that the pricing of Sophos has been fair and comparable to other vendors in the space. As a school district, they have to watch their dollars closely— but believes Sophos has been very responsive to that need. With the money the team saved from switching to Sophos, they invested into other security projects that have improved their security posture.

Another thing they appreciated about Sophos is how their product requests and suggestions over the last several years have actually been added to the endpoint and email solutions. "That has given us a very positive outlook on our security posture," they concluded.

To find out more about Sophos solutions for education, visit sophos.com

SOPHOS