



Sint-Paulusschool secures teachers and students learning with digital devices with Sophos Firewall and synchronised security

Sint-Paulusschool is a large school in the Belgian province of West Flanders, with more than 6,000 pupils and 1,000 staff members, spread across six campuses. The teachers of the school already work with a personal laptop and soon most pupils will also receive their own device as part of the 'Digisprong', an initiative of the Flemish government. To provide a secure environment and ensure that its small IT team can handle the extra work, the school switched to a Sophos Firewall with Central Endpoint Management. It not only meets the requirements but also offers the benefits of synchronised security.

CUSTOMER-AT-A-GLANCE



Sint-Paulusschool
Waregem (West Flanders) – Belgium

Industry
Education

Number of Users
6,000 pupils and 1,000 staff members

Sophos Solutions
Sophos Firewall
Sophos Central Endpoint Protection
Sophos Synchronised Security

“Pupils can be very curious and there is always a risk that they will click on phishing that in turn infects their device with malware. Synchronised security ensures that we can resolve most incidents without manual intervention.”

Pieter-Jan Lamont, IT coordinator at Sint-Paulusschool

Sint-Paulusschool is a school group with six campuses in Waregem, Anzegem and Avelgem. Pupils can choose from a wide variety of studies, such as Language & Culture, Science & Technology, Art & Creation, Economics & Organisation, etc. As in most Flemish schools, digitalisation is rapidly advancing in educational activities. Although good teaching is about more than just digital tools, it is impossible to imagine the classroom without computers. It is therefore an ongoing challenge for the IT team to prevent problems and malfunctions, and to solve the same problems when they do occur.

Digisprong: the digitalisation of education

The VTI campus in Waregem alone has about 700 desktop computers that students use almost constantly. Soon, these fixed digital classrooms will largely make way for personalised laptops. Most teachers already have a laptop at their disposal and in the upcoming school years all students will also use a laptop device that they can take home after school. This is possible thanks to the Digisprong, a programme that aims to digitalise education in Flanders. The Flemish government has invested 375 million euros to give children starting from the fifth grade access to a personal laptop.

These additional devices also bring new challenges, which is why part of the government's investment is meant for the development of a future-proof and secure ICT environment for schools. Because Sint-Paulusschool was already using Sophos for antivirus protection, the school decided to extend its licenses to more devices and install a new Sophos Firewall in combination with Central Endpoint Management. “Our main challenge is making sure that we can keep everything running at all times. Watching over each individual device would be an impossible task for our team. That's why the synchronised security options from Sophos really appealed to us”, says Pieter-Jan Lamont, IT coordinator at Sint-Paulusschool.



“We hope that we can handle the influx of additional IT devices, but we are confident that we have taken the right measures to guarantee a secure and high-performance network for our teachers and students.”

Pieter-Jan Lamont, IT coordinator at Sint-Paulusschool

Security with a heartbeat

The previous firewall of Sint-Paulusschool was not able to support the transition to a digital-first environment. So they upgraded to a next-gen Sophos XG Firewall. This not only gives the school's ICT team a different interface and better performance, but also provides a system with fully automated protection. Sophos Security Heartbeat is a feature that allows endpoints and firewalls to communicate their health status with each other. “Children can be very curious and there is always a risk that they will click on phishing that in turn infects their device with malware. Synchronised Security ensures that we can resolve most incidents without manual intervention”, says Lamont.

The constant, centralised communication between endpoints and firewalls allows for the creation of automatic policies. If malware is detected by the antivirus protection, the infected endpoint immediately isolates itself from the network and blocks all communication with other devices. The endpoint will then automatically attempt to tackle the problem and reconnect to the network once the problem is resolved. The IT manager can then choose to investigate what went wrong, but by that time the danger has passed thanks to the rapid troubleshooting. Manually, this process would take several hours, but now they can do the job in only eight seconds, ensuring that teachers and students are not affected by the disruption.

An interesting fact: the IT team of Sint-Paulusschool took care of the complete implementation of the security solutions. “We do have a lot of expertise in-house, so we try to limit the number of partners. During webinars we often hear Sophos claim that their firewalls are easy to install. We can only agree: everything is extremely secure by default and it is not difficult to adjust the configuration. For urgent questions, we can also count on our other partner, Telenet. But our own team can handle the configuration itself”, says Lamont.

Schools become a target for hackers

“We are doing everything we can to prevent a cyberattack at Sint-Paulusschool. With the Sophos Firewall, we feel we are on the right track. At least 99% of all incidents are resolved without manual intervention by our team”, says Lamont. Although cyberattacks seem to be more associated with enterprises, schools are also targets and need to take the right security measures. “We have heard stories from other schools and universities that have fallen victim to a cyberattack. Hackers are targeting schools for the same reason they attack hospitals. Schools store sensitive data, including personally identifying information (PII) and we need to take care to process this information in a secure way.”

In a modern school like Sint-Paulusschool, access control is also becoming increasingly complex as different profiles want to connect to the network. Some teachers need sufficient rights to browse through websites they want to use in the

classroom. The students also need the ability to work with certain resources, but don't need as high an access level as their teacher. And finally, the administrative staff has to manage sensitive data about staff and pupils. To make sure that each of these profiles has secure and flawless access to the content they need, the IT team can use the security system to create policies for different users. This way, a student does not have the same privileges as a teacher and the school's data is restricted to the people who need to work with the information.

For Sint-Paulusschool, the 'Digisprong' and the implementation of a more secure environment have been a giant leap into the future of education. “We hope that we can handle the influx of additional IT devices, but we are confident that we have taken the right measures to guarantee a secure and high-performance network for our teachers and students”, concludes Lamont.

