Peruvian University shifts from a reactive to a proactive approach to security with Sophos Intercept X Advanced.

Located in Lima, Peru, the Universidad del Pacífico offers undergraduate, graduate, and post-graduate degree programs in law, engineering, business, information sciences, marketing, languages, and finance. It also has an extensive international training and research program. Founded in 1962 by a group of business leaders and the Jesuit religious community, the university seeks to expand its role as a key contributor to the educational, economic, and social development of Peru.

CUSTOMER-AT-A-GLANCE

Universidad del Pacífico (Perú)

Industry
Education

Website
www.up.edu.pe

Number of Users
3,800

Sophos Solutions
Sophos Intercept X Advanced
Sophos Intercept X Advanced for Server

Challenges

- Protecting all users and endpoints, including mobile devices, across campus
- Detecting and blocking ransomware and zero-day threats
- Elevating security by seamlessly integrating advanced endpoint protection with existing solutions
- Finding a solution that works automatically and transparently, without disrupting processes and activities essential to higher education
- Prioritizing alerts and enabling better, more accurate investigations
- Simplifying and centralizing security management

When faced with a changing threat environment, what steps can an educational institution take to modernize its security?

For many years, IT Director Ugo Ojeda and this team at the Universidad del Pacífico were satisfied with their endpoint solution, which largely centered around signature-based antivirus and device inventory management – until the institution started getting hit with ransomware attacks.

"Our solution did a great job for a while, but times change. When we were directly impacted by ransomware, we knew it was time to modernize our defenses in order to combat these new threats," relates Ojeda. He explains that his vision was to implement a solution that provided a more comprehensive defense, was easy to manage, and worked automatically and transparently so as not to disrupt the activities of the diverse user population, which includes students, faculty, and administrative staff. He and his team also felt the university's existing endpoint product was doing a good job overall, so they needed a solution that would interoperate with it.

Ojeda oversees 42 employees, but only a handful are dedicated to information security. With the volume of alerts mounting and the inability of the current solution to counteract advanced malware and other threats, the security team was clearly overwhelmed. Ojeda was particularly concerned about never-before-seen threats. Because the existing antivirus is signature-based, it was unable to identify and block malware associated with a ransomware attack that targeted one of the organization's servers. This event added fuel to the fire and prompted Ojeda to look for another more robust and advanced solution to reinforce his endpoint security defenses.

'The Sophos Central platform is accessible from anywhere and this has greatly simplified things for us.'

Ugo Ojeda
IT Director
Universidad del Pacífico

'Sophos is the only brand with a mature suite of products, the functionality we need to meet our requirements, and the same high level of service and support that we have come to expect from our vendors.'

Ugo Ojeda
IT Director
Universidad del Pacífico

What technologies does Sophos Intercept X Advanced rely on to help combat ransomware and zero-day threats?

Ojeda and his team performed a market analysis and sought the assistance of their trusted technology partner, Yachay Telecommunications, to help them find the optimal technology that would secure all types of endpoints – laptops, servers, and mobile devices – for all types of users across the entire campus, from offices to computer labs.

A Sophos Platinum Partner for three years, Yachay provides a broad spectrum of IT services, from network connectivity to security to telephony. Yachay serves multiple industry sectors, including healthcare, government, energy, manufacturing, and education. Yachay has had many years of experience supporting customers in the education market and understands their particular technology requirements and budgetary constraints. Having worked with the university for nearly five years, the Sophos managed service provider was well acquainted with Universidad del Pacífico's technology environment and understood exactly what was needed to boost its security posture and better protect its users and devices. Yachay recommended Sophos Intercept X Advanced for both devices and servers.

Universidad del Pacífico acquired 2,800 licenses of Sophos Intercept X Advanced and 250 licenses of Sophos Intercept X Advanced for Server. For Ojeda, Sophos took the university's security infrastructure to a new level. With capabilities far beyond traditional antivirus, these solutions provide next-generation endpoint protection that detects never-before-seen malware with deep learning – a form of artificial intelligence. It also stops ransomware with CryptoGuard technology, which blocks encryption attempts on hard drives, USB devices, and network shares. Furthermore, Sophos Intercept X Advanced halts attacks in progress by blocking the exploits and techniques attackers typically use to propagate malware, steal credentials, and avoid detection. The server version of the product leverages the same technologies as the endpoint version and is purpose-built to protect the university's critical applications and workloads from hacking attempts and data loss.

'With Sophos, we can do everything we need to do on a daily basis to secure the organization.'

Ugo Ojeda
IT Director
Universidad del Pacífico

"Sophos Intercept X Advanced was exactly what we were looking for. Our current endpoint solution was purely reactive, unable to detect and mitigate zero-day threats. Sophos Intercept X Advanced, on the other hand, uses a signatureless approach, so we are confident that we are now well protected against both known and unknown malware," explains Ojeda.

Another key differentiator for Ojeda is the fact that Sophos technology is based on an open architecture. It is complementary to other security technologies, allowing for easy and seamless integration. Ojeda and his team were able to quickly deploy Sophos Intercept X Advanced and enable it to run concurrently and transparently in tandem with their existing endpoint product – all without impacting user productivity.

How has EDR and centralized management changed the mindset of the security team and improved their effectiveness?

Intercept X Advanced also provides intelligent endpoint detection and response (EDR) capabilities, replicating tasks that would normally be performed by skilled analysts. The solution leverages machine learning to automatically detect and prioritize potential threats and analyze malware down to code-level details for more fruitful investigations. Ojeda's team also has access to on-demand threat intelligence curated by SophosLabs, which receives and processes more than 400,000 previously unseen malware samples daily. All of this has significantly lightened the workload for Ojeda and his team and enables them to focus on what's most important from a security perspective.

Ojeda and his team have also gained operational efficiency in other ways. Deployment and management from the cloud-based Sophos Central management platform, with its intuitive dashboard, are straightforward and easier than ever, saving an enormous amount of time and effort. Other solutions the team had implemented in the past required laborious, time-consuming on-premises installations at every single location.

Sophos Central expands visibility into the computing infrastructure, with details into potential vulnerabilities across all devices and all users.

"Our previous solution lacked a 360-degree view into our environment, and this prevented us from performing a proper forensic analysis that would have prevented new infections. Sophos has changed all that," notes Ojeda. "We can do everything we need to do on a daily basis to secure the organization, and then, when the occasion arises, we can perform effective troubleshooting."

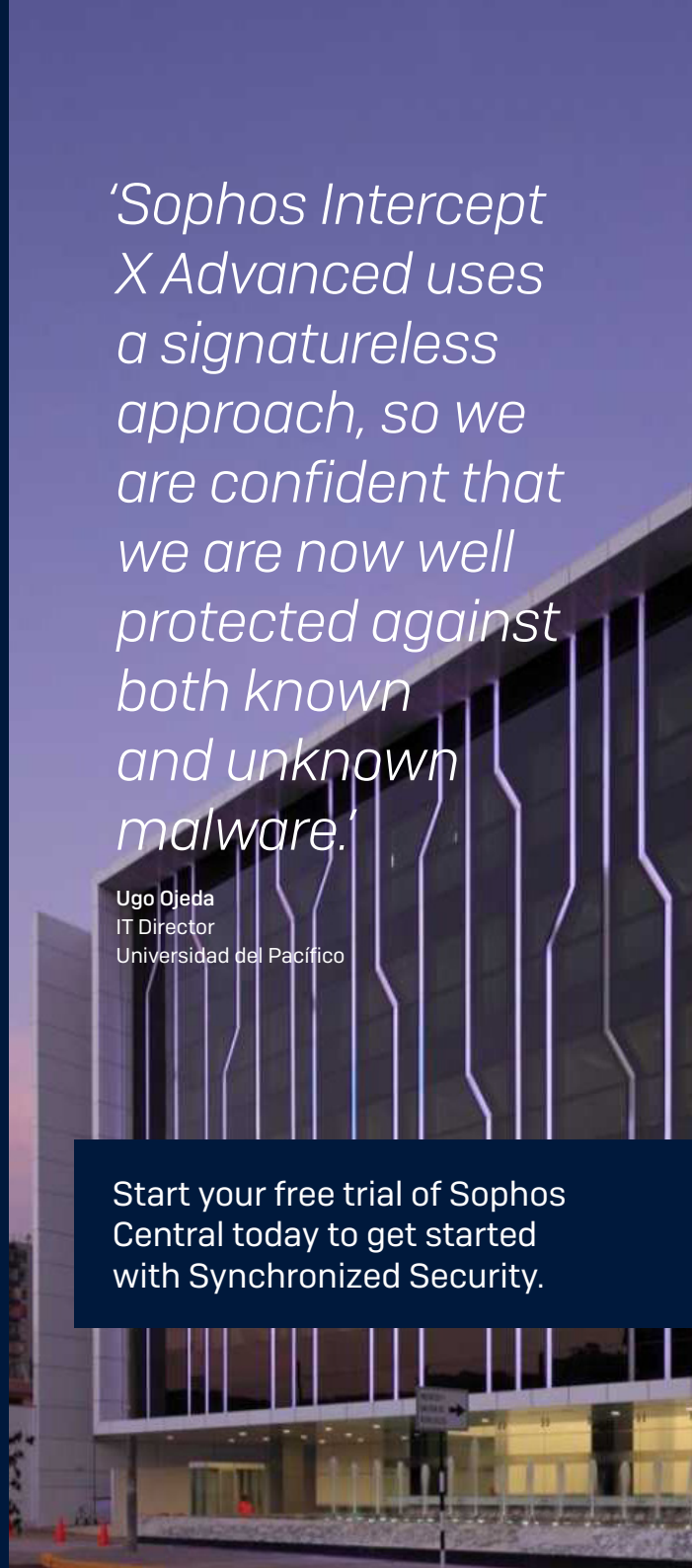
All these capabilities allow the team to take a proactive rather than reactive approach to minimizing security risks. And, thanks to Sophos, they are no longer dedicating all their precious time to security.

"Because it's in the cloud, the Sophos Central platform is accessible from anywhere, and this has greatly simplified things for us," says Ojeda. "My team is now much more effective and efficient. They spend less time chasing alerts. When security events do occur, they take action and resolve incidents much faster. Now they can turn their attention to other activities and responsibilities, like collaborating on technology initiatives that foster the university's success and growth."

Ojeda also appreciates the flexibility and support of the Sophos team every step of the way. With limited funds available to them, universities and other educational institutions often have to make the most of what they have. Not only did the Sophos open architecture accommodate integration with Universidad del Pacífico's current endpoint solution, the pricing fit perfectly within the organization's budget parameters.

"Sophos is the only brand with a mature suite of products, the functionality we need to meet our requirements, and the high level of service and support we have come to expect from our vendors," concludes Ojeda.

SOPHOS



'Sophos Intercept X Advanced uses a signatureless approach, so we are confident that we are now well protected against both known and unknown malware.'

Ugo Ojeda
IT Director
Universidad del Pacífico

Start your free trial of Sophos Central today to get started with Synchronized Security.