CUSTOMER CASE STUDY

Protecting the future of learning at Universidad San Sebastián with Sophos

With more than 31,000 students and five campuses across Chile, Universidad San Sebastián (USS) faces the challenge of securing a vast and dynamic digital ecosystem — one that underpins learning, research, and innovation every day.

UNIVERSIDAD SAN SEBASTIAN

Industry
Higher education

Number of Users
4,200

Sophos Solutions

- Sophos Managed Detection and Response (MDR)
- Sophos Extended Detection and Response (XDR)
- Sophos Cloud Optix
- Sophos Phish Threat

SOPHOS

The university's digital ecosystem supports an immense volume of academic, administrative, and research activity, all of which must remain secure and uninterrupted. As its population and infrastructure expanded, so did its exposure to increasingly sophisticated cyberthreats.

Protecting a growing, distributed environment

As the University continued scaling its academic and administrative operations, its cybersecurity team faced an evolving threat landscape that exceeded the capabilities of its existing tools. While segmentation and zero trust improved defenses, the complexity of modern attacks demanded more than incremental measures — it required a unified, proactive approach.

"We needed to ensure operational continuity and protect the university's critical data in a constantly threatened digital environment," Mario Miranda, a cybersecurity analyst at USS, said.

The shift to remote work, increasingly strict legal requirements, and the university's broad user base amplified the urgency.

Endpoints quickly emerged as the most vulnerable point. With thousands of students and faculty connecting from personal devices, the risk of phishing, credential theft, and lateral movement grew significantly — creating a challenge for a team committed to keeping learning uninterrupted.

"The greatest security challenge [lies] in the protection of endpoint devices, as they are the most exposed link due to users with limited cybersecurity awareness," Miranda said. "They became the main entry point for attacks such as phishing."

While segmentation and zero trust improved defenses, these measures alone couldn't keep pace with increasingly sophisticated attacks. The university needed a unified, proactive approach that could anticipate threats and respond before they disrupted operations.

The team implemented network segmentation and stricter access policies, guided by a zero-trust approach, but the complexity of modern threats required a broader transformation. The university needed a centralized, proactive solution that could identify, analyze, and mitigate threats across thousands of devices and users.

Impact

- Delivered unified visibility and rapid threat response across all campuses, enabling the team to detect and contain attacks they previously couldn't see.
- Strengthened endpoint protection and reduced user-driven vulnerabilities, significantly lowering overall exposure to phishing and lateral movement.
- Streamlined security operations through a single, integrated platform, reducing manual workload and improving policy consistency across devices.
- Enhanced business continuity by preventing disruptions and allowing IT staff to redirect time toward strategic, value-adding initiatives.

SOPHOS

Unified, proactive security designed for scale

Recognizing that fragmented tools were limiting visibility and slowing response times, the team began evaluating platforms that could consolidate their defenses and scale with the institution.

"The concrete measure that emerged in the department was the search for and implementation of a unified and comprehensive security solution," Miranda said.

Their requirements centered on proactive threat prevention, a richer and more centralized data foundation, and the ability to customize workflows without overwhelming staff.

The goal was not simply to deploy new tools but to create a security posture resilient enough to anticipate threats, respond rapidly, and support the university's long-term strategic goals.

"The vision for IT and the company is to strengthen all security controls proactively and continuously," he said. "We aim to minimize risks through defense in depth, advanced technology, automation, and user awareness."

"The vision for IT and the company is to strengthen all security controls proactively and continuously," he said. "We aim to minimize risks through defense in depth, advanced technology, automation, and user awareness."

Mario Miranda, Cybersecurity Analyst, Universidad San Sebastian

Sophos MDR + XDR as the foundation for modern defense

USS selected Sophos MDR, complemented by Sophos XDR and additional Sophos tools such as Web Control and Peripheral Control, to modernize its security operations. For the first time, the cybersecurity team gained access to continuous, expert-led monitoring and response paired with deep, cross-environment visibility.

By partnering with Sophos MDR, USS gained continuous, expert-led threat detection and response — ensuring attacks are stopped before they disrupt learning. Sophos MDR and XDR transformed USS's security operations. For the first time, the team gained continuous, expert-led monitoring and deep visibility across thousands of endpoints — enabling faster detection and response to advanced threats that previously went unseen

"Sophos products were fundamental in materializing our vision," Miranda said. "MDR, combined with the flexibility of Sophos XDR, gave us visibility and reaction capacity against advanced threats that we did not have internally."

SOPHOS

Sophos Web Control strengthened browsing safety, while peripheral controls reduced exposure from physical entry points such as USB devices — areas that are often underestimated but essential for a university with diverse user behavior.

The native integration across Sophos tools helped the team move away from siloed detection and toward an ecosystem capable of identifying patterns, correlating signals, and initiating rapid response across endpoints and servers. This significantly raised the university's ability to prevent, contain, and remediate threats.

Stronger visibility, greater resilience, and improved efficiency

With Sophos in place, USS gained a real-time, granular view of its endpoint fleet and consistent security policies across every device.

"We now maintain detailed, real-time inventory with active, robust, and uniformly applied security policies," Miranda said. "This initiative has directly contributed to business efficiency by drastically reducing the risk of operational disruptions due to security incidents."

Operational continuity — critical for an institution serving tens of thousands of learners — improved measurably. Faster response times and automated protections reduced the workload on the internal team, freeing staff to focus on high-value projects that support the university's digital growth. The overall security posture became more coherent, predictable, and proactive.

By consolidating its defenses, USS strengthened its protection against cyberthreats and improved internal resource allocation, increased stability across campuses, and ensured a more resilient academic environment for students and faculty.

> "We now maintain detailed, real-time inventory with active, robust, and uniformly applied security policies."
>
> Mario Miranda, Cybersecurity Analyst, Universidad San Sebastian

Looking ahead

USS remains committed to advancing its cybersecurity maturity, with Sophos MDR and XDR serving as foundational components of its future strategy.

Miranda summarized the University's direction clearly: "Our objective is to strengthen all security controls proactively and continuously, minimizing risks as much as possible. With Sophos, we now have a unified and continuously evolving platform to stay protected against future threats."

With Sophos MDR and XDR as its foundation, USS is building a security posture that not only protects today's operations but empowers the university to embrace future innovation with confidence.

To get started with Sophos solutions today and find a solution that scales to your needs, speak to an expert today. Sophos.com

SOPHOS