CUSTOMER CASE STUDY

Protegiendo el futuro del aprendizaje en la Universidad San Sebastián con Sophos

Con más de 31.000 estudiantes y cinco campus en todo Chile, la Universidad San Sebastián (USS) enfrenta el desafío de proteger un ecosistema digital amplio y dinámico, que sustenta el aprendizaje, la investigación y la innovación todos los días.

UNIVERSIDAD SAN SEBASTIAN

Industria
Educación superior

Número de usuarios
4,200

Soluciones de Sophos

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

SOPHOS

El ecosistema digital de la universidad respalda un enorme volumen de actividades académicas, administrativas y de investigación, todas las cuales deben mantenerse seguras y sin interrupciones. A medida que su población e infraestructura crecieron, también lo hizo su exposición a ciberamenazas cada vez más sofisticadas.

Protección de un entorno en crecimiento y distribuido

A medida que la universidad continuó ampliando sus operaciones académicas y administrativas, su equipo de ciberseguridad se enfrentó a un panorama de amenazas en constante evolución que superaba las capacidades de las herramientas existentes. Si bien la segmentación y el enfoque de zero trust mejoraron las defensas, la complejidad de los ataques modernos exigía algo más que medidas incrementales: requería un enfoque unificado y proactivo.

“Necesitábamos garantizar la continuidad operativa y proteger los datos críticos de la universidad en un entorno digital constantemente amenazado”, señaló Mario Miranda, analista de ciberseguridad de la USS.

El cambio al trabajo remoto, los requisitos legales cada vez más estrictos y la amplia base de usuarios de la universidad incrementaron la urgencia.

Los endpoints se convirtieron rápidamente en el punto más vulnerable. Con miles de estudiantes y docentes conectándose desde dispositivos personales, el riesgo de phishing, robo de credenciales y movimiento lateral aumentó de forma significativa, lo que representó un desafío para un equipo comprometido con mantener el aprendizaje sin interrupciones.

“El mayor desafío de seguridad radica en la protección de los dispositivos endpoint, ya que son el eslabón más expuesto debido a usuarios con un nivel limitado de conciencia en ciberseguridad”, explicó Miranda. “Se convirtieron en el principal punto de entrada para ataques como el phishing”.

Si bien la segmentación y el enfoque de zero trust mejoraron las defensas, estas medidas por sí solas no lograban seguir el ritmo de ataques cada vez más sofisticados. La universidad necesitaba un enfoque unificado y proactivo que pudiera anticipar las amenazas y responder antes de que interrumpieran las operaciones.

El equipo implementó segmentación de red y políticas de acceso más estrictas, guiadas por un enfoque de zero trust, pero la complejidad de las amenazas modernas requería una transformación más amplia. La universidad necesitaba una solución centralizada y proactiva que pudiera identificar, analizar y mitigar amenazas en miles de dispositivos y usuarios.

Impacto

- Se logró una visibilidad unificada y una respuesta rápida ante amenazas en todos los campus, lo que permitió al equipo detectar y contener ataques que antes no podía ver.
- Se fortaleció la protección de endpoints y se redujeron las vulnerabilidades derivadas del comportamiento de los usuarios, disminuyendo significativamente la exposición general al phishing y al movimiento lateral.
- Se optimizaron las operaciones de seguridad mediante una única plataforma integrada, reduciendo la carga de trabajo manual y mejorando la consistencia de las políticas en todos los dispositivos.
- Se reforzó la continuidad operativa al evitar interrupciones y permitir que el personal de TI redirigiera su tiempo hacia iniciativas estratégicas de mayor valor.

Seguridad unificada y proactiva diseñada para escalar

Al reconocer que las herramientas fragmentadas limitaban la visibilidad y ralentizaban los tiempos de respuesta, el equipo comenzó a evaluar plataformas capaces de consolidar sus defensas y escalar junto con la institución.

"La medida concreta que surgió en el departamento fue la búsqueda e implementación de una solución de seguridad unificada e integral", indicó Miranda.

Los requisitos se centraron en la prevención proactiva de amenazas, una base de datos más rica y centralizada, y la capacidad de personalizar flujos de trabajo sin sobrecargar al equipo.

El objetivo no era simplemente implementar nuevas herramientas, sino crear una postura de seguridad lo suficientemente resiliente como para anticipar amenazas, responder con rapidez y respaldar los objetivos estratégicos a largo plazo de la universidad.

"La visión para TI y para la institución es fortalecer todos los controles de seguridad de forma proactiva y continua", explicó. "Buscamos minimizar los riesgos mediante defensa en profundidad, tecnología avanzada, automatización y concientización de los usuarios".

> "La medida concreta que surgió en el departamento fue la búsqueda e implementación de una solución de seguridad unificada e integral"
>
> Mario Miranda, Cybersecurity Analyst, Universidad San Sebastián

Sophos MDR + XDR como base de una defensa moderna

La USS seleccionó Sophos MDR, complementado con Sophos XDR y otras herramientas de Sophos como Web Control y Peripheral Control, para modernizar sus operaciones de seguridad. Por primera vez, el equipo de ciberseguridad obtuvo acceso a monitoreo y respuesta continuos, liderados por expertos, junto con una visibilidad profunda en todos los entornos.

Al asociarse con Sophos MDR, la USS obtuvo detección y respuesta ante amenazas de forma continua y guiada por expertos, lo que garantiza que los ataques se detengan antes de interrumpir el aprendizaje. Sophos MDR y XDR transformaron las operaciones de seguridad de la universidad. Por primera vez, el equipo contó con monitoreo continuo y visibilidad profunda en miles de endpoints, lo que permitió una detección y respuesta más rápidas frente a amenazas avanzadas que antes pasaban desapercibidas.

"Los productos de Sophos fueron fundamentales para materializar nuestra visión", afirmó Miranda. "MDR, combinado con la flexibilidad de Sophos XDR, nos brindó visibilidad y capacidad de reacción frente a amenazas avanzadas que no teníamos internamente".

Sophos Web Control reforzó la seguridad de la navegación, mientras que los controles de periféricos redujeron la exposición derivada de puntos de entrada físicos como dispositivos USB —áreas que a menudo se subestiman, pero que son esenciales para una universidad con comportamientos de usuario diversos.

La integración nativa entre las herramientas de Sophos ayudó al equipo a dejar atrás la detección aislada y avanzar hacia un ecosistema capaz de identificar patrones, correlacionar señales e iniciar respuestas rápidas en endpoints y servidores. Esto incrementó significativamente la capacidad de la universidad para prevenir, contener y remediar amenazas.

Mayor visibilidad, mayor resiliencia y mejor eficiencia

Con Sophos implementado, la USS obtuvo una visión granular y en tiempo real de su parque de endpoints, junto con políticas de seguridad coherentes en todos los dispositivos.

"Ahora mantenemos un inventario detallado y en tiempo real, con políticas de seguridad activas, robustas y aplicadas de forma uniforme", explicó Miranda. "Esta iniciativa ha contribuido directamente a la eficiencia operativa al reducir drásticamente el riesgo de interrupciones debido a incidentes de seguridad".

La continuidad operativa —crítica para una institución que atiende a decenas de miles de estudiantes— mejoró de forma tangible. Los tiempos de respuesta más rápidos y las protecciones automatizadas redujeron la carga de trabajo del equipo interno, lo que permitió al personal enfocarse en proyectos de alto valor que respaldan el crecimiento digital de la universidad. La postura de seguridad general se volvió más coherente, predecible y proactiva.

Al consolidar sus defensas, la USS fortaleció su protección frente a ciberamenazas, optimizó la asignación de recursos internos, aumentó la estabilidad entre campus y garantizó un entorno académico más resiliente para estudiantes y docentes.

"Ahora mantenemos un inventario detallado y en tiempo real, con políticas de seguridad activas, robustas y aplicadas de forma uniforme."

Mario Miranda, Cybersecurity Analyst, Universidad San Sebastián

Mirando hacia el futuro

La USS mantiene su compromiso de seguir avanzando en su madurez en ciberseguridad, con Sophos MDR y XDR como componentes fundamentales de su estrategia futura.

Miranda resumió con claridad la dirección de la universidad: “Nuestro objetivo es fortalecer todos los controles de seguridad de manera proactiva y continua, minimizando los riesgos al máximo. Con Sophos, ahora contamos con una plataforma unificada y en constante evolución para mantenernos protegidos frente a las amenazas futuras”.

Con Sophos MDR y XDR como base, la USS está construyendo una postura de seguridad que no solo protege las operaciones actuales, sino que también permite a la universidad adoptar la innovación futura con confianza.

Para comenzar hoy mismo con las soluciones de Sophos y encontrar una opción que escale según sus necesidades, hable con un experto hoy mismo.

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

SOPHOS