CUSTOMER CASE STUDY

El Hospital Provincial de Castellón refuerza su ciberseguridad con Sophos

- El centro sanitario despliega Sophos MDR, Sophos Managed Risk, Sophos XGS Firewall, Sophos NDR y conectores para proteger más de 700 puestos de trabajo, 1.000 usuarios y 100 servidores.
- La implementación permite una monitorización 24/7 con detección y respuesta gestionadas ante la amenaza creciente del ransomware en hospitales.
- La colaboración tripartita entre el Hospital, TWT-TS y Sophos facilita la continuidad operativa en un entorno que no puede interrumpirse.

GENERALITAT VALENCIANA

Consorci Hospitalari Provincial de Castelló

Customer Name
Hospital Provincial de Castellón Strengthens Cybersecurity with Sophos

SOPHOS

Madrid, 08 de enero de 2026. – Sophos, líder mundial en soluciones de seguridad innovadoras para combatir los ciberataques, ha anunciaso hoy que el Consorcio Hospitalario Provincial de Castellón ha completado la implementación de un ecosistema integral de soluciones de ciberseguridad de Sophos para proteger su infraestructura crítica y datos sensibles y garantizar la continuidad asistencial.

El proyecto, desarrollado en colaboración con el partner tecnológico TWT-TS, incluye soluciones de detección y respuesta gestionadas (Sophos MDR), gestión de vulnerabilidades (Sophos Managed Risk), firewall de próxima generación (Sophos XGS Firewall), detección de intrusiones en red (Sophos NDR) y conectores de integración.

Plataforma unificada para recursos limitados

Cuando el equipo de TI asumió la gestión del departamento tecnológico del hospital, se encontró ante una situación de ciberseguridad con redes sin segmentar, ausencia de firewall perimetral y de sistemas de detección de intrusiones y con falta de personal especializado en gestión de ciber-amenazas.

Esta realidad coincide con los resultados del informe State of Ransomware 2025 de Sophos, que identifica las vulnerabilidades sin parchear (33% de los ataques) y la falta de recursos especializados para monitorizar los sistemas en el momento del ataque (42% de las víctimas) como las principales causas de compromiso en el sector sanitario.

Como explica **Carlos García, Director TIC del Consorcio Hospitalario Provincial de Castellón** *"al asumir la gestión del departamento de TI, la ciberseguridad no era una prioridad. Teníamos que cambiar esa situación abordando todo de la forma más rápida posible sin detener el servicio, en un momento en que otros centros sanitarios españoles estaban sufriendo una oleada de ataques de ransomware".*

La complejidad de gestionar múltiples fabricantes y consolas de seguridad resultaba inviable para el tamaño del hospital. TWT-TS, el partner de Sophos encargado de la implementación, diseñó una estrategia basada en la unificación de la plataforma de seguridad para maximizar la protección con los recursos disponibles.

El despliegue se ejecutó por fases priorizando activos críticos: primero servidores con acceso a datos sensibles y el firewall perimetral, seguido de áreas asistenciales como urgencias, UCIs, laboratorio y radiología. La implementación completa del porfolio se completó en cerca de tres meses, minimizando interrupciones mediante horarios de tarde y una estrecha coordinación con el personal sanitario. Actualmente, el hospital se encuentra en pleno proceso de renovación de toda la infraestructura de red, políticas, configuraciones y segmentación.

> "La mejor solución era optar por una plataforma capaz de unificar consolas, productos y estrategias, para que todo fuera más sencillo de controlar. Si además esa propia solución la gestionaba la misma Sophos, se acortaban enormemente los plazos", señala
>
> **César Benítez**
>
> Responsable de Desarrollo de Negocio de Ciberseguridad en TWT-TS.

Protección multicapa

En un sector donde el tiempo de inactividad afecta directamente a la atención al paciente, la prevención sigue siendo el objetivo final. El ecosistema desplegado proporciona así protección en múltiples capas de la infraestructura hospitalaria: el servicio MDR de Sophos ofrece threat hunting y respuesta gestionada 24/7/365, mientras que la solución Managed Risk permite identificar y priorizar vulnerabilidades críticas en función del contexto específico del hospital.

Por su parte, la sonda NDR monitoriza entornos legacy y equipamiento médico que no puede protegerse con agentes tradicionales, como sistemas TAC, máquinas de radiología y otros dispositivos especializados.

Visibilidad, tranquilidad y protección continua

Desde la implementación, el hospital ha obtenido una completa visibilidad de su postura de seguridad a través de la consola centralizada Sophos Central. En los tres primeros meses de operación, el sistema procesó cerca de 1 millón de detecciones potenciales de amenazas, de las cuales aproximadamente 50.000 fueron escaladas y correlacionadas por los algoritmos de inteligencia artificial. El equipo de MDR de Sophos ha intervenido activamente en una ocasión, deteniendo con éxito un intento de ejecución de código malicioso sin requerir acción por parte del Hospital.

El proyecto ha permitido al hospital cumplir con su obligación de proteger datos médicos sensibles de aproximadamente 1.000 pacientes mientras mantiene la continuidad operativa de 100 servidores y más de 700 puestos de trabajo para que los servicios críticos no se interrumpan.

Como concluye Carlos García, *"aunque hubiéramos tenido los recursos, no somos una empresa tan grande como para cubrir un servicio 24/7 con ese nivel de especialización. Sophos MDR nos ofrece la tranquilidad de que gente mucho más preparada está vigilando el entorno de manera continua".*

Durante los últimos doce meses, Sophos X-Ops ha descubierto 88 grupos de ciber-amenazas distintos atacando a organizaciones sanitarias en todo el mundo, siendo GOLD FEATHER (Qilin), GOLD IONIC (INC Ransom) y GOLD HUBBARD (RansomHub) los más destacados. Los casos gestionados por Sophos Incident Response y MDR revelan la explotación de vulnerabilidades como vector principal, además de los ataques de phishing, ingeniería social, fuerza bruta, descargas no autorizadas y credenciales robadas.

"La potencia del servicio MDR no reside únicamente en la capacidad de respuesta, sino en su habilidad para analizar automáticamente millones de eventos y filtrar aquellos que realmente representan amenazas genuinas, reduciendo drásticamente la carga operativa del equipo de TI del Hospital. Toda esta actividad queda documentada en informes mensuales que resumen las detecciones filtradas por tipo de amenaza y dispositivo afectado",

César Benítez

Responsable de Desarrollo de Negocio de Ciberseguridad en TWT-TS.

Acerca de TWT-TS

TWT-TS es una empresa tecnológica especializada en infraestructura, redes y ciberseguridad, con amplia experiencia apoyando a organizaciones críticas en la protección de sus sistemas. Es Partner Platinum de Sophos y cuenta con un alto nivel de experiencia en el ecosistema de seguridad de Sophos. Además, TWT-TS cuenta con la certificación ENS (Esquema Nacional de Seguridad) de nivel medio, lo que le permite ejecutar proyectos alineados con los requisitos regulatorios en los sectores público y sanitario.

Acerca de Sophos

Sophos es una empresa líder en ciberseguridad que protege a más de 600.000 organizaciones en todo el mundo mediante una plataforma impulsada por inteligencia artificial y servicios especializados. Sophos acompaña a las organizaciones estén donde estén en su camino hacia la madurez en ciberseguridad y evoluciona con ellas para hacer frente a los ciberataques. Sus soluciones combinan aprendizaje automático, automatización e inteligencia de amenazas en tiempo real con la experiencia humana del equipo Sophos X-Ops, ofreciendo una vigilancia, detección y respuesta ante amenazas avanzada y 24/7.

Sophos proporciona un servicio líder de detección y respuesta gestionada (MDR), junto con un completo portafolio de tecnologías de ciberseguridad que abarca protección de endpoints, redes, correo electrónico y entornos en la nube, así como detección y respuesta extendida (XDR), detección y respuesta ante amenazas de identidad (ITDR) y soluciones SIEM de nueva generación. Además, Sophos ofrece servicios de asesoría expertos que ayudan a las organizaciones a reducir proactivamente el riesgo y a responder con mayor rapidez, contando con la visibilidad y escalabilidad necesarias para adelantarse a las amenazas en constante evolución.

Sophos opera a través de un ecosistema global de partners, que incluye proveedores de servicios gestionados (MSP), proveedores de servicios de seguridad gestionada (MSSP), distribuidores, resellers, integraciones en marketplaces y socios especializados en gestión de riesgos cibernéticos, ofreciendo a las organizaciones la flexibilidad de elegir relaciones de confianza para proteger su negocio. La sede central de Sophos se encuentra en Oxford, Reino Unido. Más información en https://www.sophos.com/es-es.

Para obtener más información:
TEAM Lewis
Nina Janmaat
nina.janmaat@teamlewis.com
Tel: 91 926 62 82

To learn more visit www.sophos.com/es-es

SOPHOS