Netdata®

CYBERSECURITY

Caso de éxito

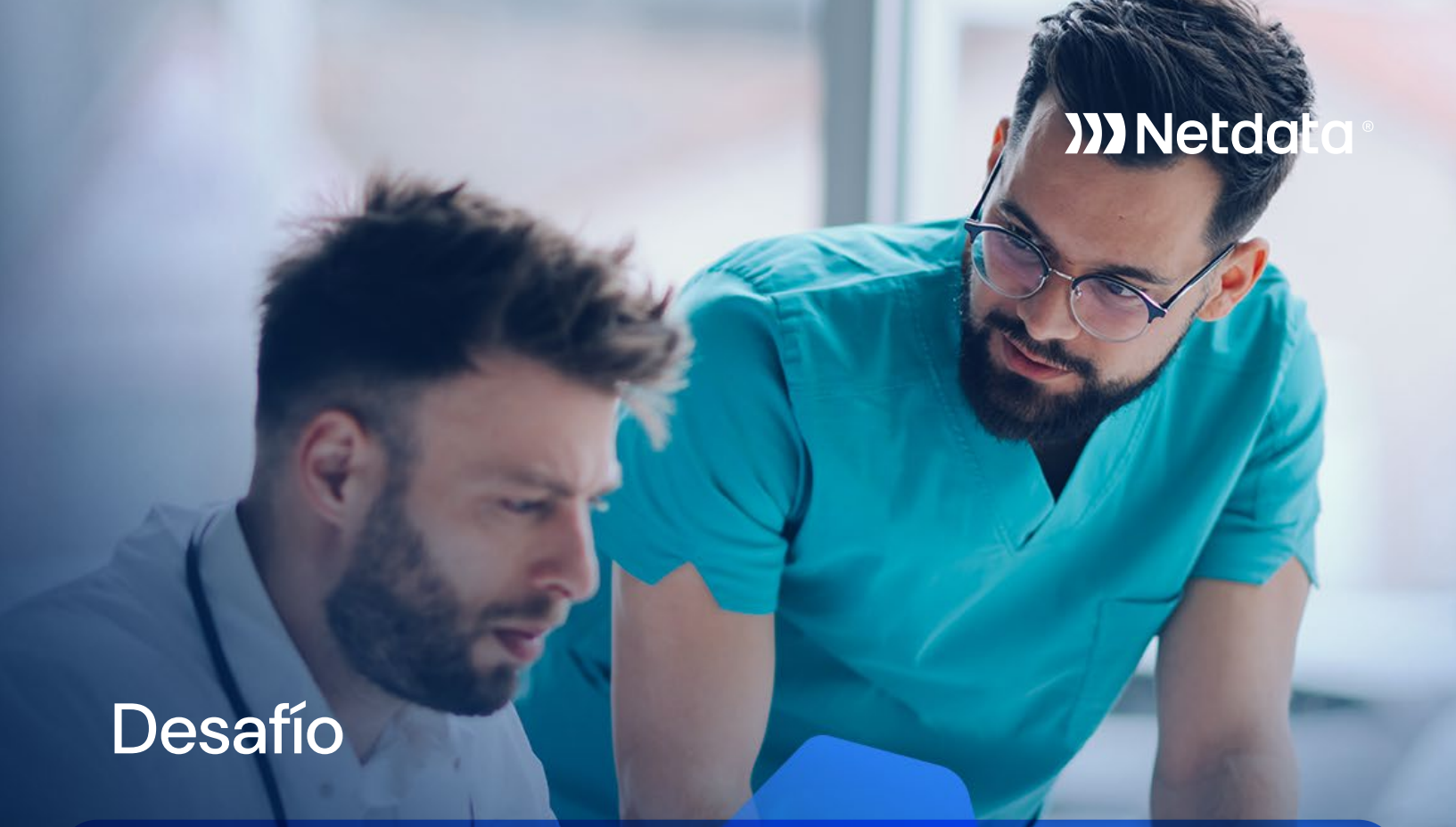
Cómo un hospital pediátrico aseguró más de 250 endpoints

Detección y visibilidad cercanas al 100%

MTTD de 10 minutos comprometido por SLA

MTTR de 120 minutos comprometido por SLA

TTV (time to value) en menos de 3 meses



Desafío

Una institución de salud latinoamericana especializada en atención pediátrica opera con una infraestructura tecnológica de la que depende por completo la disponibilidad de sus sistemas clínicos y administrativos. En el sector salud, la interrupción de un servicio no representa únicamente una pérdida operativa: compromete la atención de pacientes, el acceso a historias clínicas y la continuidad de procesos médicos que no admiten pausas.

La institución ya había sido víctima de un ataque de ransomware, experiencia que marcó un punto de quiebre y generó un cambio cultural hacia la priorización de la ciberseguridad. A esto se suma un contexto de industria adverso: el sector salud es uno de los más atacados a nivel global, con un volumen creciente de intentos dirigidos a instituciones con infraestructura crítica y datos altamente sensibles.

Su esquema de protección se apoyaba en un antivirus tradicional, cuya capacidad de detección y visibilidad no superaba el 50% en evaluaciones del MITRE ATTACK®. Además, no contaba con un aliado que comprometiera tiempos de detección y respuesta. La institución tampoco había establecido una estrategia que le permitiera medir cuánto tiempo tomaba detectar un incidente y cuánto demoraba su resolución.

La restricción más determinante era la capacidad operativa: solo tres personas tienen a cargo la gestión de toda la infraestructura tecnológica del hospital. Sostener una operación de ciberseguridad 24/7 con ese equipo era inviable, por lo que la institución necesitaba un aliado estratégico capaz de asumir la capa de ciberseguridad mediante un centro de operaciones de seguridad (SOC).

Proceso

La alianza junto a Netdata comenzó por la capa perimetral, con la gestión de firewalls. La experiencia positiva con la tecnología de Palo Alto Networks y el desempeño sostenido de esa primera etapa abrieron la conversación hacia un modelo más amplio: pasar de la administración de productos puntuales a un servicio gestionado de seguridad.

La decisión se definió por la propuesta de un servicio llave en mano. A diferencia de un modelo tradicional y reactivo, enfocado principalmente en instalar y configurar la tecnología para luego dejar su operación en manos del cliente, Sentria propuso un enfoque proactivo y continuo. El servicio incorporó capacidades como cacería de amenazas, monitoreo permanente y gestión activa de la seguridad, junto con objetivos claros, SLAs, SLOs y KPIs orientados a medir la protección del negocio y fortalecer su capacidad de ciberresiliencia, no solo a la instalación de una herramienta.

La implementación tomó aproximadamente un mes. El proceso consistió en reemplazar las herramientas tradicionales por una solución XDR, apalancando su capacidad de despliegue masivo sobre un parque inicial de 200 endpoints que posteriormente creció a 250. En paralelo se estableció una línea base de comportamiento, necesaria para que la analítica integrada comprendiera los patrones de uso de usuarios y entidades y pudiera detectar anomalías reales.

El onboarding incluyó un triage para identificar y priorizar los activos críticos de la institución. Durante la fase inicial, el equipo técnico de Netdata acompañó los ajustes y la creación de excepciones en las políticas, evitando el bloqueo de procesos legítimos del negocio mientras la herramienta aprendía el entorno operativo. La continuidad de las funciones clínicas y administrativas se mantuvo en todo momento.

Netdata®

Solución

Se implementó el servicio gestionado de seguridad **SENTRIA**, que combina tecnología XDR con la operación continua de un SOC. La solución integra:

- Monitoreo y respuesta gestionada sobre 250 endpoints, con tiempo máximo de detección (MTTD) de 10 minutos y tiempo máximo de resolución (MTTR) de 120 minutos comprometidos por SLA.
- Reemplazo del antivirus tradicional por XDR, con analítica de comportamiento de usuarios y entidades sobre una línea base propia del entorno.
- Triage y priorización de activos críticos, con acompañamiento para el ajuste de políticas sin interrumpir procesos del negocio.
- Cacería de amenazas e inteligencia proactiva como parte de la estrategia de ciberdefensa.
- Tableros de visualización que permiten a la institución evidenciar el comportamiento de las amenazas y justificar la inversión ante la dirección.

Resultados Tangibles

Detección, visibilidad y prevención cercanas al 100%:

la cobertura pasó de aproximadamente 50% con la tecnología anterior a un nivel cercano al total del entorno, eliminando puntos ciegos en la infraestructura hospitalaria.

Tiempos de respuesta comprometidos y medibles:

la institución pasó de no tener referencia alguna a operar con un MTTD de 10 minutos y un MTTR de 120 minutos definidos contractualmente.

Retorno de valor en menos de un trimestre:

sobre una implementación de un mes, el cliente percibió los beneficios del servicio en menos de tres meses, indicador clave para justificar la inversión realizada.

Descarga operativa del equipo interno:

las tres personas responsables de toda la infraestructura tecnológica delegaron la operación de ciberseguridad al SOC, liberando capacidad para proyectos propios del negocio.

Tendencia decreciente en intentos de ataque:

los tableros muestran una disminución sostenida de los intentos diarios a lo largo del tiempo, patrón observado también en otros clientes y explicado por el desistimiento de los atacantes frente a una defensa efectiva.

Testimonio del Cliente

“Pasamos de no saber cuánto tardábamos en detectar un incidente a tener tiempos comprometidos y medibles. Con un equipo de tres personas a cargo de toda la tecnología del hospital, contar con un SOC que responde por nosotros nos permitió bajar la carga operativa y concentrarnos en lo que sostiene la atención de nuestros pacientes.”

Gerencia de Tecnología.

Conclusión

En salud, la ciberseguridad no se mide en licencias instaladas sino en continuidad de la atención. Este caso confirma que una institución con equipo reducido puede alcanzar un nivel de protección de grado empresarial cuando delega la operación en un servicio gestionado con objetivos, SLAs y métricas claras.

Netdata conoce las restricciones reales del sector salud: equipos de TI pequeños, sistemas que no admiten interrupciones y antecedentes de ransomware que exigen resultados demostrables desde el primer trimestre. La metodología de onboarding con triage de activos críticos y ajuste progresivo de políticas permite migrar desde herramientas tradicionales hacia XDR en aproximadamente un mes, sin detener la operación clínica.

La confianza construida se refleja en la renovación anual del contrato, en la decisión de la institución de avanzar hacia un modelo Enterprise o NG-SOC, con integración de múltiples fuentes de telemetría, playbooks de automatización y capacidades potenciadas por inteligencia artificial, así como en la recomendación del servicio a otros centros de salud y organizaciones del ecosistema..

Netdata®

www.netdatanetworks.com