Sentria® By Netdata

Sentria

Caso de éxito

El punto ciego que ningún agente puede cubrir: cómo un hospital de alta complejidad incorporó su equipamiento médico al SOC

MTTD 10 min y MTTR 120 min en toda la telemetría

Equipamiento médico incorporado al SOC

De soporte reactivo 5x8 a proactivo 24/7

Reducción del costo de la póliza de ciberseguro

Desafío

El sector salud concentra dos condiciones que rara vez coinciden: información altamente sensible y una operación que no admite interrupciones. A eso se suma una restricción estructural, la presencia de equipamiento médico de alto costo y larga vida útil que no fue diseñado para convivir con las herramientas de seguridad actuales. Es un contexto que exige resolver la protección sin la opción de renovar el parque tecnológico.

Una institución hospitalaria de alta complejidad —más de 500 camas, cerca de un centenar destinadas a cuidados críticos, 2.700 endpoints— operaba con antivirus tradicional y firewalls UTM de generación anterior. La protección existía, pero funcionaba en silos: no había correlación ni colaboración entre la telemetría de red y la de endpoints, de modo que ninguna fuente podía validar ni enriquecer a la otra. La visibilidad sobre la infraestructura era parcial por diseño.

El punto ciego crítico estaba en el IoMT. Resonadores magnéticos, electrocardiógrafos y otros dispositivos médicos no admiten agentes de seguridad, y buena parte de ese equipamiento opera sobre sistemas operativos fuera de soporte. Son activos conectados a la red, indispensables para la operación clínica y, hasta entonces, invisibles para el SOC.

El modelo de soporte era reactivo y en ventana 5x8, dependiente de tickets levantados manualmente. Un hospital opera 24/7; su esquema de respuesta, no. Esa asimetría no es un problema solo operativo: la indisponibilidad de sistemas en urgencias y pabellón impide la atención y se convierte en un riesgo directo sobre la vida del paciente, además de una exposición reputacional y regulatoria bajo marcos como HIPAA.

El impacto financiero de una indisponibilidad prolongada, calculado sobre el volumen de exámenes y procedimientos que la institución realiza, alcanza cifras millonarias en cuestión de días.

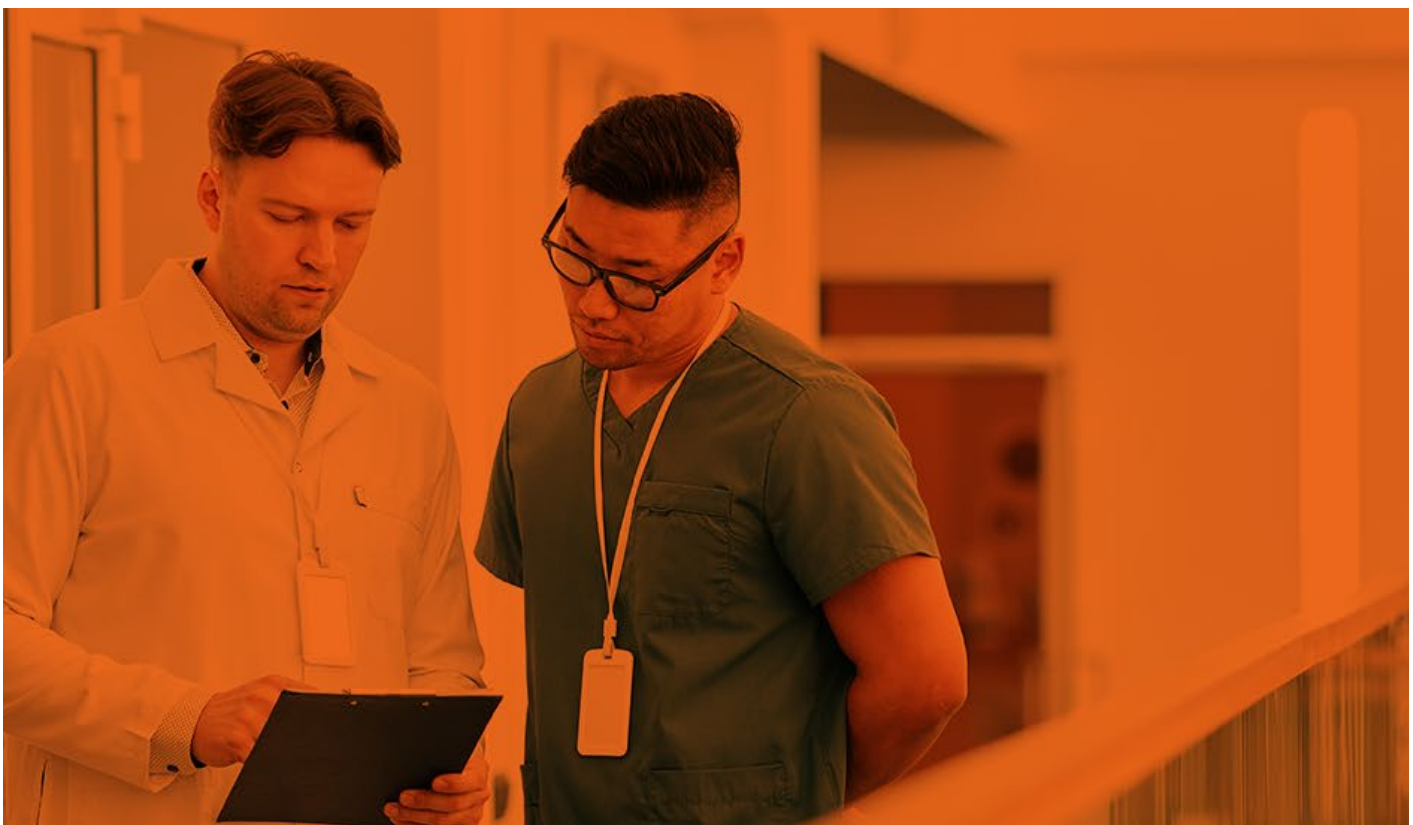
Proceso

La decisión no partió de cero. Tres años previos de servicio MDR sobre endpoints habían dejado evidencia concreta de que el proveedor cumplía su promesa de valor. La conversación no fue si adoptar una plataforma nueva, sino si esa misma experiencia podía replicarse sobre el resto de la infraestructura.

El obstáculo era financiero, no técnico: quedaba tiempo vigente del contrato anterior, de cinco años. Se aplicó un modelo de retoma que reconoció la inversión previa del cliente y descontó el valor del tiempo remanente del costo de la nueva solución. Ese reconocimiento fue el factor decisivo para concretar la mejora tecnológica.

La implementación fue calificada como sencilla y se apoyó en tres frentes. La migración de Cortex a XSIAM se ejecutó de forma transparente para la operación. Se activó licenciamiento IoMT sobre la plataforma de firewalls de Palo Alto Networks en alta disponibilidad, lo que permitió visibilizar el equipamiento médico sin instalar agente alguno sobre él. Y se desplegaron playbooks de automatización que reemplazaron el flujo de tickets manuales por acciones correctivas autónomas, como el bloqueo de tráfico malicioso.

Con la telemetría de red y de endpoints integrada en una sola plataforma, la homologación de tiempos de detección y respuesta dejó de aplicarse solo a endpoints para extenderse a toda la plataforma tecnológica.



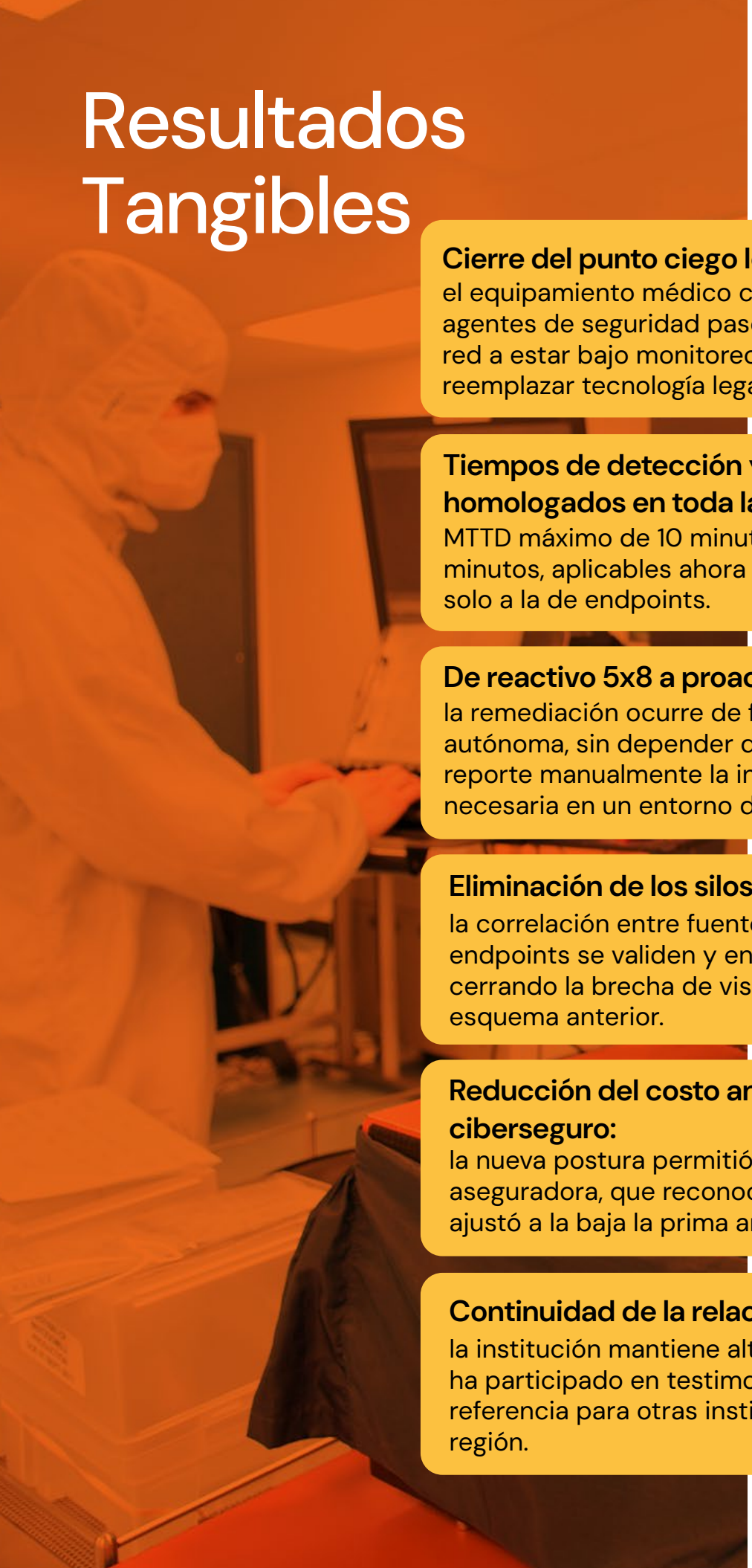
Sentria

Solución

Se implementó SENTRIA Powered by XSIAM, servicio gestionado de ciberdefensa sobre 2.700 endpoints y telemetría multifuente. La solución integra:

- Integración de la telemetría de red y de endpoints en una plataforma única, eliminando la operación en silos.
- MTTD máximo de 10 minutos y MTTR máximo de 120 minutos homologados en toda la plataforma tecnológica, no solo sobre endpoints.
- Visibilidad IoMT mediante licenciamiento sobre la plataforma de firewalls en alta disponibilidad, incorporando al monitoreo los dispositivos médicos que no admiten agente.
- Playbooks de automatización que ejecutan acciones correctivas de forma autónoma, eliminando la dependencia del reporte manual por tickets.
- Operación proactiva 24/7 en reemplazo del esquema reactivo 5x8, con remediación inmediata sin necesidad de que el hospital reporte la incidencia.

Resultados Tangibles



Sentria

Cierre del punto ciego IoMT:
el equipamiento médico crítico que no admite agentes de seguridad pasó de estar a ciegas para la red a estar bajo monitoreo continuo, sin necesidad de reemplazar tecnología legacy.

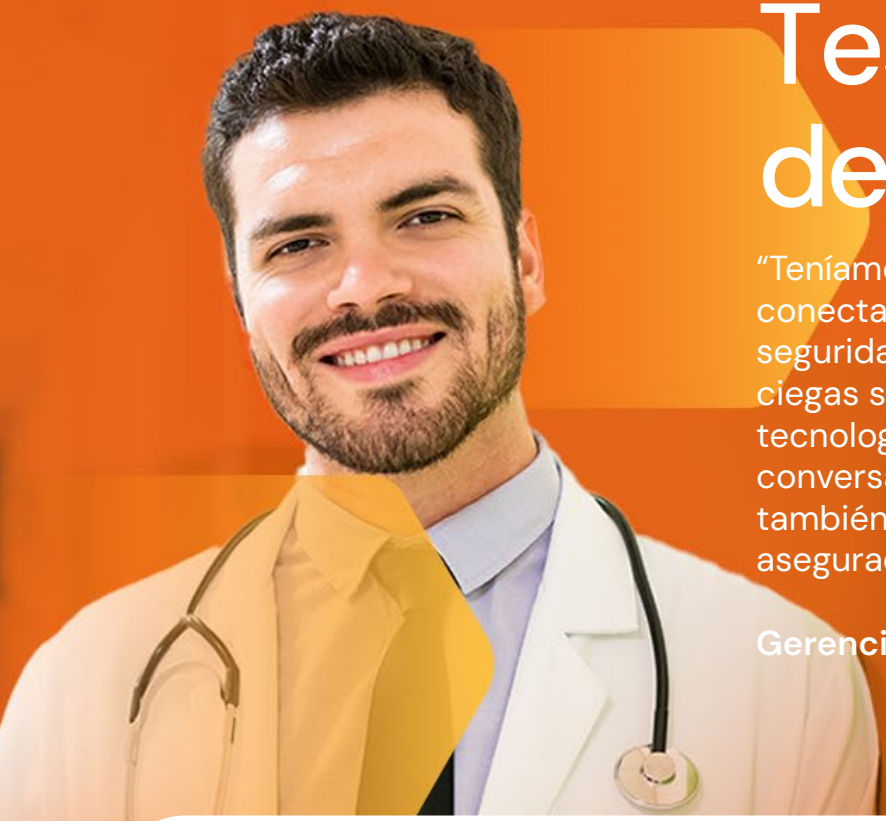
Tiempos de detección y respuesta homologados en toda la plataforma:
MTTD máximo de 10 minutos y MTTR máximo de 120 minutos, aplicables ahora a la telemetría de red y no solo a la de endpoints.

De reactivo 5x8 a proactivo 24/7:
la remediación ocurre de forma inmediata y autónoma, sin depender de que el hospital detecte y reporte manualmente la incidencia, condición necesaria en un entorno de operación continua.

Eliminación de los silos de telemetría:
la correlación entre fuentes permite que red y endpoints se validen y enriquezcan mutuamente, cerrando la brecha de visibilidad que dejaba el esquema anterior.

Reducción del costo anual de la póliza de ciberseguro:
la nueva postura permitió solicitar una reevaluación a la aseguradora, que reconoció un menor nivel de riesgo y ajustó a la baja la prima anual.

Continuidad de la relación y rol de referencia:
la institución mantiene alta satisfacción con el servicio, ha participado en testimonios públicos y actúa como referencia para otras instituciones de salud de la región.



Testimonio del Cliente

"Teníamos equipos médicos críticos conectados a la red que ningún agente de seguridad podía proteger. Dejar de operar a ciegas sobre ellos, y hacerlo sin reemplazar tecnología, cambió por completo nuestra conversación de riesgo: internamente y también con nuestra aseguradora"

Gerencia de Tecnología.

Conclusión

La discusión de ciberseguridad en salud suele quedarse en cobertura de endpoints. Este caso marca el límite de ese enfoque: mientras el equipamiento médico permanezca fuera del alcance del SOC y la telemetría de red no se correlacione con la de endpoints, la visibilidad real no mejora por más licencias que se agreguen.

La vía de solución tampoco pasó por reemplazar tecnología legacy, un desembolso que ninguna institución de salud puede justificar, sino por incorporar esos activos al monitoreo desde la capa de red, donde sí es posible observarlos. Esa distinción es la que vuelve alcanzable la protección integral en entornos hospitalarios.

Netdata ejecuta esta clase de transición sobre infraestructura hospitalaria en producción, sin interrumpir la operación clínica, reconociendo la inversión previa del cliente mediant modelos de retoma y comprometiendo métricas de detección y respuesta sobre todas las fuentes integradas.

Sentria By Netdata