Netdata®

CYBERSECURITY

Caso de éxito

Cómo una entidad financiera transformó miles de eventos de seguridad en decisiones accionables.

Una arquitectura impulsada por IA, automatización y un SOC especializado permitió modernizar las operaciones de seguridad, reducir la carga operativa y convertir la telemetría en inteligencia para la toma de decisiones.

Netdata®

Resultados

2.911 casos gestionados

Operación continua sobre un entorno altamente regulado.

9.000 endpoints bajo monitoreo

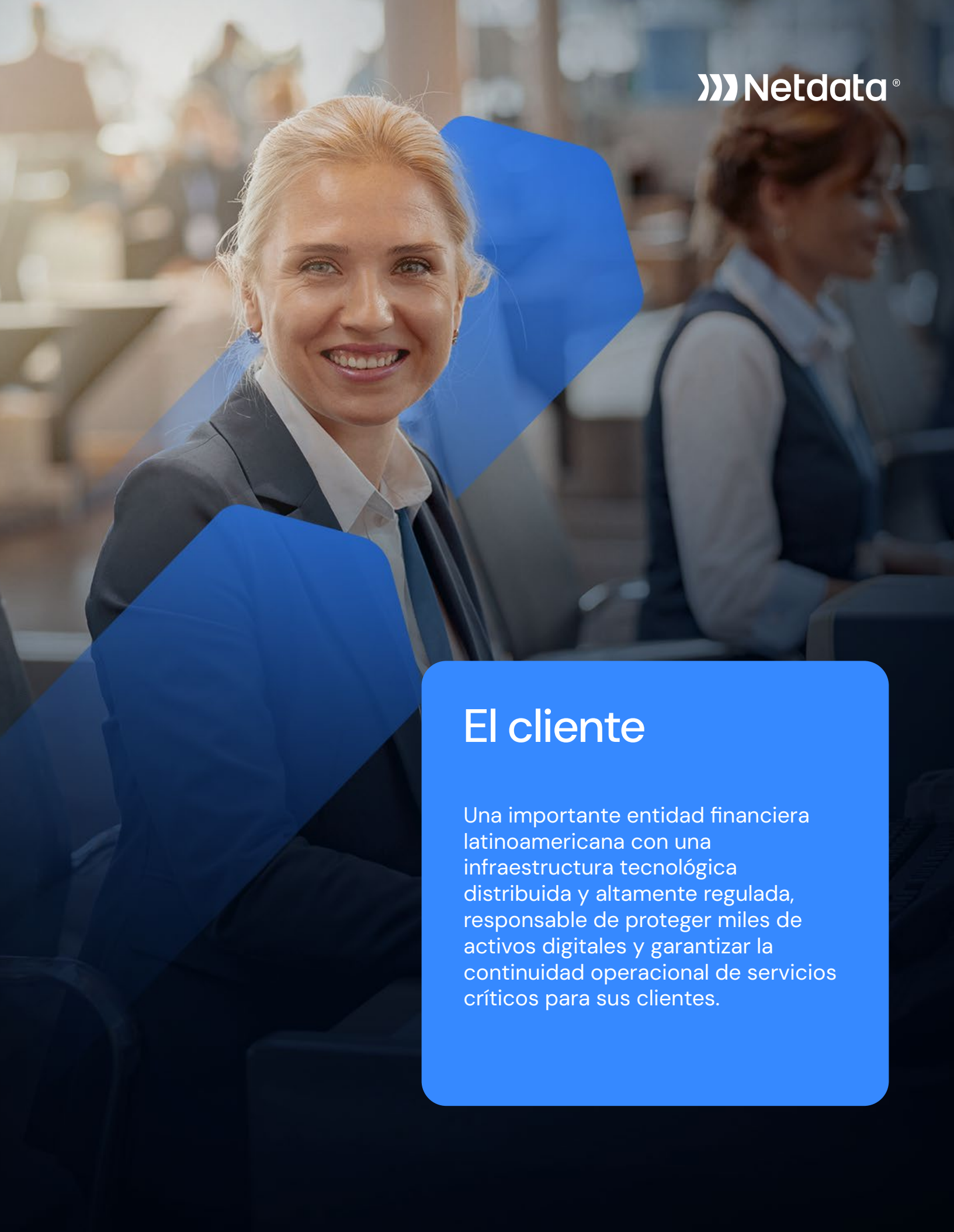
Protección continua sobre la infraestructura del banco.

25 fuentes de telemetría integradas

Visibilidad unificada sobre endpoints, red, firewalls y servicios cloud.

907 casos resueltos sin intervención del cliente

Mayor eficiencia operativa y menor carga para el equipo interno.



Netdata®

El cliente

Una importante entidad financiera latinoamericana con una infraestructura tecnológica distribuida y altamente regulada, responsable de proteger miles de activos digitales y garantizar la continuidad operacional de servicios críticos para sus clientes.

El desafio

**El problema no era la falta de información.
Era transformar esa información en decisiones.**

Las instituciones financieras generan millones de eventos de seguridad provenientes de endpoints, firewalls, infraestructura de red, plataformas cloud y aplicaciones críticas.
Sin embargo, disponer de más información no necesariamente significa tener mayor capacidad para responder.

Antes del proyecto, el Centro de Operaciones de Seguridad (SOC) de la organización operaba sobre un conjunto de tecnologías heredadas y herramientas aisladas que dificultaban la correlación de eventos y la construcción de un contexto único para la investigación.

Cada plataforma entregaba información relevante, pero los analistas debían invertir una cantidad considerable de tiempo relacionando manualmente datos provenientes de distintos fabricantes, investigando falsos positivos y ejecutando tareas repetitivas que retrasaban la respuesta frente a amenazas reales.

A medida que el volumen de telemetría aumentaba, también lo hacía la complejidad operativa.

El desafío ya no consistía en recibir más alertas.

El verdadero reto era reducir el ruido, priorizar aquello que realmente representaba un riesgo y entregar a los analistas la información necesaria para tomar decisiones con mayor velocidad y precisión.

Además, la organización debía fortalecer sus capacidades para responder a los nuevos requerimientos asociados a la Ley Marco de Ciberseguridad y la Ley de Protección de Datos, incorporando un modelo más moderno de detección y respuesta.

La solución

Unificar datos, automatizar procesos y fortalecer la toma de decisiones.

Para responder a este desafío, la organización implementó una arquitectura moderna basada en Cortex XSIAM, acompañada por el servicio especializado Sentria, inteligencia de amenazas (CTI) y Brand Protection.

La solución permitió consolidar la operación del SOC en una plataforma capaz de correlacionar información proveniente de múltiples tecnologías y automatizar procesos que anteriormente dependían de intervención manual. El proyecto incorporó:

Netdata®

25 fuentes de telemetría integradas provenientes de endpoints, infraestructura de red, firewalls y servicios cloud.

9.000 endpoints incorporados al modelo de monitoreo.

Servicio Sentria con cobertura 24x7 y un equipo especializado de ingeniería.

Capacidades avanzadas de automatización, inteligencia artificial y threat hunting continuo.

Más allá de la implementación tecnológica, el proyecto representó una evolución del modelo operativo.

Durante las primeras etapas surgieron diferencias entre las expectativas del cliente y el modelo estándar del servicio. En lugar de mantener un enfoque rígido, el equipo realizó un nuevo proceso de descubrimiento, redefinió procesos, ajustó automatizaciones y adaptó el servicio a la realidad operacional del banco.

Ese enfoque consultivo permitió convertir una implementación tecnológica en una relación de mejora continua.

Resultados

De administrar alertas a gestionar decisiones.
La transformación del SOC comenzó a reflejarse rápidamente en la operación diaria.

2.911 casos gestionados
Durante los primeros meses de operación se gestionaron 2.911 casos, manteniendo continuidad operacional sobre un entorno financiero de alta complejidad.

2.238 casos cerrados
El SOC logró resolver la mayor parte de los eventos investigados, manteniendo un flujo continuo de respuesta y seguimiento.

907 casos resueltos sin intervención del cliente
Gracias al modelo gestionado de Sentria, una parte importante de las investigaciones fue resuelta completamente por el equipo especializado, permitiendo que el personal interno concentrara sus esfuerzos en actividades estratégicas y no en tareas operativas repetitivas.

Menor carga operativa para el SOC
La correlación inteligente de eventos, junto con la optimización continua de reglas y automatizaciones, permitió disminuir el volumen de escalamientos innecesarios y mejorar la calidad de las investigaciones.

Visibilidad unificada sobre el entorno
La integración de 25 fuentes de telemetría entregó una visión centralizada del ecosistema tecnológico, facilitando la detección de amenazas, las actividades de threat hunting y la investigación de incidentes con mayor contexto.

Evolución continua
El servicio evolucionó más allá del monitoreo tradicional. Actualmente incorpora optimización permanente de alertas, nuevas integraciones, automatizaciones y recomendaciones técnicas que fortalecen continuamente la postura de seguridad del cliente.

Netdata®

Testimonio del Cliente

"Lo que más valoramos no fue únicamente la plataforma, sino la capacidad del equipo para comprender nuestra operación y adaptar el servicio a nuestros desafíos reales. Hoy contamos con una visión mucho más clara de nuestro entorno, procesos de investigación más eficientes y un acompañamiento permanente que nos permite evolucionar continuamente nuestra operación de seguridad."

Gerencia de Ciberseguridad

Conclusión

Los Centros de Operaciones de Seguridad ya no pueden medir su éxito por la cantidad de alertas que procesan.

Su verdadero valor está en la capacidad de convertir grandes volúmenes de información en decisiones oportunas para proteger el negocio.

Este caso demuestra cómo la combinación de Cortex XSIAM, Sentria, inteligencia artificial, automatización y un equipo especializado permitió transformar un SOC basado en procesos reactivos en una operación orientada a la priorización, la investigación y la respuesta inteligente.

Más allá de implementar una plataforma, la organización adoptó un modelo de mejora continua que hoy le permite integrar nuevas fuentes de información, optimizar permanentemente sus capacidades de detección y fortalecer su resiliencia frente a un panorama de amenazas en constante evolución.
En Netdata entendemos que la transformación de un SOC no depende únicamente de la tecnología. Depende de combinar experiencia, conocimiento operativo y servicios especializados para ayudar a las organizaciones a tomar mejores decisiones cuando más importa.

Netdata®

www.netdatanetworks.com