

A modern office interior with a curved ceiling, perforated walls, and contemporary furniture. The scene is dimly lit, with a focus on the architectural details and the text overlay.

Neohype reconfigura su estrategia de ciberseguridad con mayor protección para sus endpoints y con la seguridad como pilar cultural

Neohype, 2025

Servicios de atención al cliente que se apoyan en la tecnología y la automatización

Más de
10 millones

de interacciones con
clientes al mes

Más de
16 000

Empleados

Un proveedor de servicios en rápido crecimiento donde la confianza lo es todo

Neohype es una empresa brasileña que se especializa en servicios de atención al cliente, operaciones de BPO, automatización tecnológica y soporte en ciberseguridad para grandes empresas de todo el país. Fundada en 2017, la empresa hoy tiene más de 68 grandes clientes en los sectores de finanzas, telecomunicaciones, servicios públicos, industrial y salud. Gestiona más de 10 millones de interacciones con clientes al mes y ostenta una fuerza laboral de aproximadamente 16 000 empleados.

Neohype opera en un entorno en el que cada interacción puede involucrar información financiera o personal confidencial, y en el que la disponibilidad de los sistemas repercute de forma directa en los acuerdos de nivel de servicio y confianza en la marca. Cuando la empresa comenzó su veloz expansión, la ciberseguridad pasó de ser un mero requisito del área de sistemas a un verdadero pilar comercial.

En consecuencia, en 2017, Neohype forjó una alianza con Kaspersky. Inicialmente, la relación se centró en reforzar la protección de los endpoints y en mejorar la detección de amenazas.

k

Lograr que una fuerza
laboral ultradispersa
se comporte con
seguridad

Como proveedor de servicios en pleno crecimiento, Neohype necesitaba proteger su infraestructura y a las personas detrás de ella para atender millones de interacciones con clientes cada mes. Con Kaspersky, Neohype creó e implementó una estrategia única y para toda la empresa que combina detección de amenazas de avanzada, visibilidad en tiempo real y concientización permanente en seguridad.

Hacer de la seguridad una responsabilidad corporativa compartida

A medida que la base de clientes y la infraestructura de Neohype se expandían, también se complejizaba su superficie de ataque. Administrar 12 500 nodos suponía repensar la seguridad: la mirada reactiva tradicional ya no bastaba. Los directivos de Neohype también reconocieron que la seguridad debía pasar de una mera función técnica a una actitud adoptada por toda la organización.

Ahora la empresa se enfrentaba a dos grandes desafíos:

- El aumento en la exposición a ataques de phishing y de ingeniería social facilitados por el error humano
- La falta de un programa de concientización en seguridad escalable y estructurado, que condujera a un cambio cultural de largo plazo

Neohype necesitaba un modo de unificar la detección de amenazas de avanzada con un cambio en el comportamiento perdurable, y todo sin ralentizar las operaciones.



Impacto técnico

- Visibilidad y control centralizados para 12 500 nodos
- Detección y respuesta más rápidas frente a amenazas avanzadas
- Mayor resistencia contra ataques de día cero e intentos de aprovechamiento



Impacto humano

Mediante capacitaciones continuas y refuerzos del comportamiento, Neohype logró lo siguiente:

- Amplia participación del personal en los programas de concientización
- Reducción en los casos de soporte vinculados al phishing
- Aumento en la cantidad de empleados que identificaban y denunciaban correos sospechosos

En lugar de tratar a los usuarios como el eslabón más débil, Neohype los convirtió en una barrera activa.

De 45 % a 60 %

Reducción en la tasa de clics en casos de phishing simulados en el primer año de implementación

El camino a la solución: de la protección de endpoints a una estrategia de ciberseguridad unificada

Para conocer en tiempo real las amenazas que afectaban a su creciente infraestructura, Neohype implementó **Kaspersky EDR Optimum**. Con esta solución, lograron supervisar de forma central sus 12 500 nodos y detectar malware, amenazas de día cero e intentos de aprovechamiento en tiempo real. El cambio permitió que el equipo de seguridad de Neohype dejara de "apagar fuegos" según se iban encendiendo y pasara a administrar proactivamente las amenazas.

Abordar el factor humano de la seguridad con Kaspersky Security Awareness

Si bien las defensas técnicas mejoraron, Neohype detectó un problema recurrente: los incidentes provocados por errores humanos, en especial los relacionados con el phishing y el uso indebido del correo electrónico.

Para hacer frente a esta situación, Neohype implementó **Kaspersky Automated Security Awareness Platform (Kaspersky ASAP)**, con un énfasis en lo siguiente:

- Micromódulos de aprendizaje que el personal podía incorporar en su día de trabajo
- Simulaciones de phishing realistas
- Refuerzos del comportamiento permanentes
- Generación automatizada de informes de rendimiento y métricas de evolución claras

En lugar de sesiones de capacitación aisladas, Neohype adoptó un modelo de aprendizaje continuo, diseñado para inculcar hábitos, no solo conciencia.

Por una concientización sostenible

Para asegurar la adopción a largo plazo, Kaspersky integró la metodología ADKAR de Prosci en el programa de concientización de Neohype. Este enfoque estructurado de administración de cambios pone a ejecutivos, gerentes y empleados en un mismo plano, en el que todos son responsables de la ciberseguridad, hoy y en el futuro. Así, la seguridad deja de ser un requisito normativo y se convierte en una iniciativa cultural compartida por toda la empresa.

Los resultados: de las herramientas a la transformación

El enfoque de Neohype combinó la tecnología, el comportamiento y la metodología, y les permitió pasar de controles de seguridad aislados a una estrategia de ciberseguridad unificada.



Kaspersky
Automated Security
Awareness Platform

"Cuando la seguridad deja de ser una campaña y se transforma en una cultura, el riesgo disminuye y aparecen los resultados".



**Marcelo Mendes
dos Santos**

CISO de Neohype

Por qué esto es importante: relevancia comercial

Para Neohype, la ciberseguridad va más allá de la protección: **implica continuidad operacional, escalabilidad y confianza comercial.**

Al alinear a las personas con las tecnologías y los procesos, Neohype construyó un marco de seguridad que les permite crecer rápidamente, reducir el riesgo operacional, proteger las interacciones confidenciales con los clientes y brindar un servicio de calidad coherente.

Con este enfoque unificado, Neohype puede crecer con confianza y mantener los estándares de rendimiento que esperan sus clientes.

Hicimos de la concientización una cultura empresarial: con Kaspersky ASAP, redujimos los casos de phishing, aumentamos la madurez de los usuarios y reforzamos nuestra primera línea de defensa: el personal. Al integrar la educación continua con inteligencia de amenazas global y capacidades de detección avanzadas, creamos una barrera humana que está a la altura de las amenazas del mundo real.



Kaspersky Automated Security Awareness Platform

Más
información

Preste atención.
Manténgase a salvo.

latam.kaspersky.com

© 2026, AO Kaspersky Lab.
Las marcas registradas y las marcas de servicio
pertenecen a sus respectivos propietarios.

#kaspersky
#truetobusiness