Neohype reshapes its cybersecurity strategy with enhanced endpoint protection and a security-first culture

Neohype, 2025

kaspersky cybersecurity true to business

neohype.co

Customer engagement services supported by technology and automation

10+ million
Customer interactions per month

16,000+
Employees

A fast-growing service provider where trust is everything

Neohype is a Brazilian company specializing in customer services, BPO operations, technological automation, and cybersecurity support for major enterprises across the country. Founded in 2017, the company now serves more than 68 enterprise customers in the finance, telecoms, utilities, industrial, and healthcare sectors, managing over 10 million customer interactions each month with a workforce of approximately 16,000 employees.

Neohype operates in an environment where every interaction may involve sensitive personal or financial data, and where system availability is directly tied to service-level agreements and brand trust. As the company scaled rapidly, cybersecurity became not just an IT requirement, but a foundational business pillar.

In response, Neohype partnered with Kaspersky in 2017, initially focusing on enhancing endpoint protection and strengthening threat detection.

Embedding secure behavior across a highly distributed workforce

As a growing service provider handling millions of customer interactions each month, Neohype needed to secure its expanding infrastructure and the people behind it. With Kaspersky, the company unified advanced threat detection, real-time visibility and continuous security awareness into a single, company-wide strategy.

Turning security into an organization-wide responsibility

With Neohype's customer base and infrastructure expanding, so was the complexity of its attack surface, and managing 12,500 nodes meant that traditional, reactive approaches to security were no longer sufficient. Neohype's leadership also recognized that their security had to evolve from a purely technical function into an organization-wide mindset.

The company now faced two core challenges:

- Increasing exposure to phishing and social engineering attacks driven by human error
- A lack of a structured, scalable security awareness program to support long-term cultural change

Neohype needed a way to unify advanced threat detection with long-term behavioral change, without slowing down operations.

Technical impact

- Centralized visibility and control across 12,500 nodes
- Faster detection and response to advanced threats
- Improved resilience against zero-day attacks and exploitation attempts

Human impact

Through continuous training and behavioral reinforcement, Neohype achieved:

- High employee participation in awareness programs
- A reduction in phishing-related tickets
- An increase in employees identifying and reporting suspicious emails

Instead of treating users as the weakest link, Neohype turned them into an active layer of defense

45% to 60%

Reduction in click rates on phishing simulations within the first year following implementation

The solution path: from endpoint protection to a unified cybersecurity strategy

To gain real-time insight into threats across its growing infrastructure, Neohype implemented Kaspersky EDR Optimum. This enabled centralized monitoring across 12,500 nodes and real-time detection of malware, zero-day threats and exploitation attempts. This shift enabled Neohype's security team to move from reactive firefighting to proactive threat management.

Addressing the human layer of security with Kaspersky Security Awareness

While technical defenses improved, Neohype identified a recurring issue: human-related incidents, especially related to phishing and unsafe email behavior.

To address this, Neohype implemented the Kaspersky Automated Security Awareness Platform (Kaspersky ASAP), focusing on:

- Microlearning modules that fit into employees' workflows
- Realistic phishing simulations
- Continuous behavioral reinforcement
- Automated performance reporting and clear evolution metrics.

Rather than relying on one-off training sessions, Neohype adopted a continuous learning model designed to build habits, not just awareness.

Making awareness sustainable

To ensure long-term adoption, Kaspersky integrated the PROSCI ADKAR methodology into its awareness program for Neohype. This structured change-management approach aligns executives, managers and employees around shared responsibility for cybersecurity today and into the future, transforming security from a compliance requirement into a company-wide cultural initiative.

The results: from tools to transformation

Neohype's approach combined technology, behavior and methodology, enabling a shift from isolated security controls to a unified cybersecurity strategy.

Kaspersky
Automated Security
Awareness Platform

"When security stops being a campaign and becomes culture, risk decreases — and results follow."

Marcelo Mendes dos Santos

CISO, Neohype

Why this matters: business relevance

For Neohype, cybersecurity is not just about protection — it's about operational continuity, customer trust and scalability.

By aligning people, processes and technology, Neohype built a security framework that supports rapid business growth, reduces operational risk, protects sensitive customer interactions, and enables consistent service quality.

This unified approach allows Neohype to scale confidently while maintaining the performance standards its customers expect.

We transformed awareness into organizational culture: with Kaspersky ASAP, we reduced phishing, elevated user maturity, and strengthened our first line of defense — our people. By integrating continuous education, advanced detection and global threat intelligence, we built a human defense aligned with real-world threats.

Kaspersky Automated Security Awareness Platform

Learn more

Be aware. Stay safe.

www.kaspersky.com

#kaspersky
#truetobusiness