Netdata®

CYBERSECURITY

Success story

How a Financial Institution Turned Thousands of Security Events into Actionable Decisions

An AI-driven architecture, automation, and a specialized SOC service helped modernize security operations, reduce operational workload, and turn telemetry into useful intelligence for decision-making.

Netdata®

Results

2.911 cases managed

Continuous operation in a highly regulated environment.

9,000 endpoints under monitoring

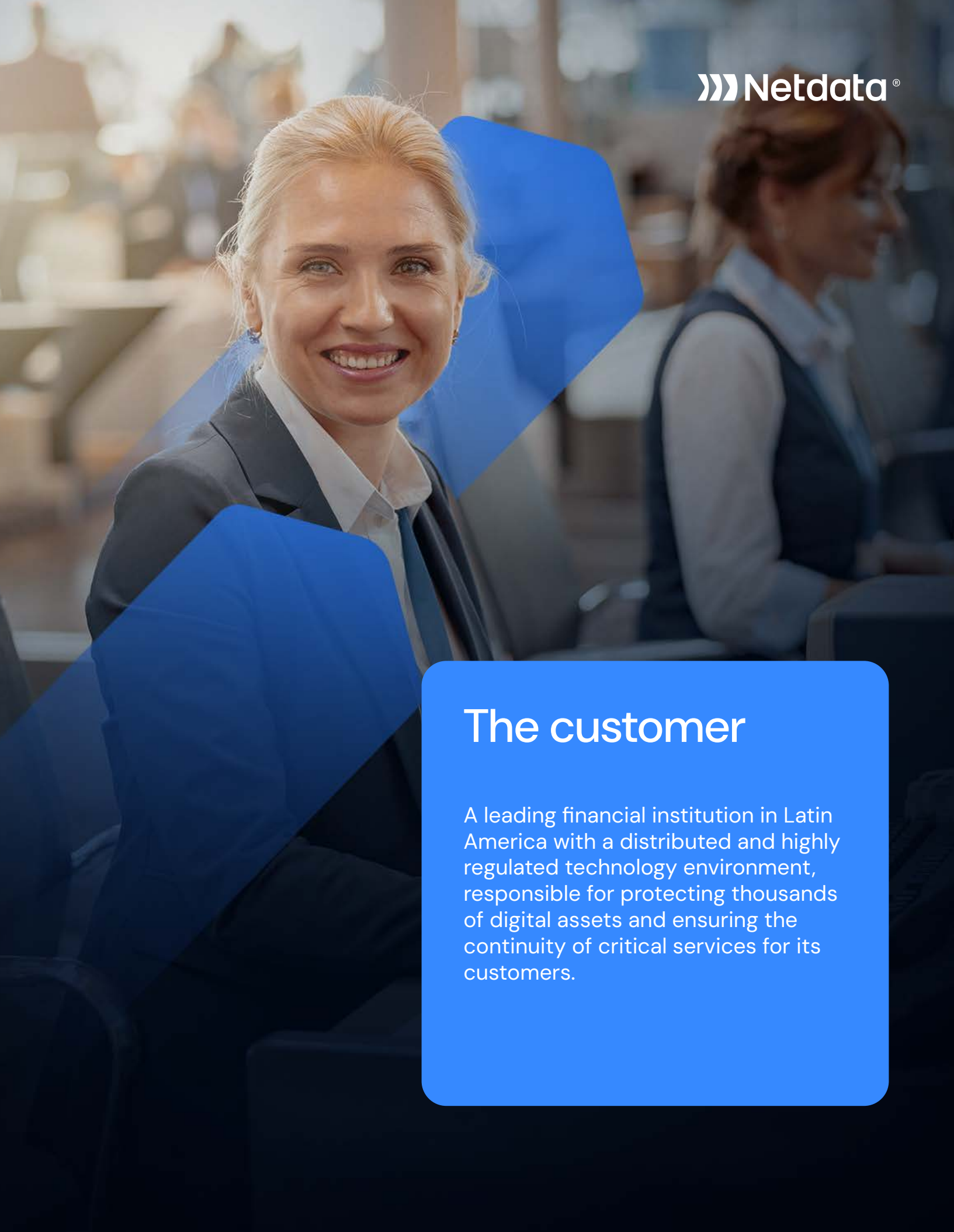
Continuous protection across the bank's infrastructure.

25 telemetry sources integrated

Unified visibility across endpoints, network, firewalls, and cloud services.

907 cases resolved without customer intervention

Higher operational efficiency and less workload for the internal team.



Netdata®

The customer

A leading financial institution in Latin America with a distributed and highly regulated technology environment, responsible for protecting thousands of digital assets and ensuring the continuity of critical services for its customers.

The challenge

The problem was not the lack of information. It was turning that information into decisions.

Financial institutions generate thousands of security events from endpoints, firewalls, network infrastructure, cloud platforms, and critical applications. However, having more information does not always mean having better response capacity.

Before the project, the organization's Security Operations Center operated with legacy technologies and isolated tools. This made it difficult to correlate events and build a single view for investigation.

Each platform provided useful information, but analysts had to spend a lot of time manually connecting data from different vendors, investigating false positives, and performing repetitive tasks that delayed the response to real threats.

As telemetry volume increased, operational complexity also increased. The challenge was no longer to receive more alerts.

The real challenge was to reduce noise, prioritize what represented real risk, and give analysts the right information to make faster and better decisions.

The organization also needed to strengthen its capabilities to respond to new cybersecurity and data protection requirements.

The solution

Unify data, automate processes, and strengthen decision-making.

To address this challenge, the organization implemented a modern architecture based on Cortex XSIAM, supported by the specialized Sentria service, Cyber Threat Intelligence (CTI), and Brand Protection.

The solution helped centralize SOC operations in one platform, able to correlate information from different technologies and automate processes that previously required manual work.

Netdata®

The project included:

25 telemetry sources
integrated from endpoints, network infrastructure, firewalls, and cloud services.

9.000 endpoints
included in the monitoring model.

Sentria
service with **24x7 coverage** and a specialized engineering team.

Advanced automation,
artificial intelligence, and continuous threat hunting.

Beyond technology, the project also improved the operating model.

During the first stages, there were differences between the customer's expectations and the standard service model. Instead of keeping a rigid approach, the team performed a new discovery process, adjusted processes, improved automations, and adapted the service to the real needs of the bank.

This consultative approach turned the implementation into a continuous improvement relationship.

Results

From managing alerts to managing decisions.

The SOC transformation quickly started to show results in daily operations.

2.911 cases managed

During the first months of operation, **2,911 cases** were managed, maintaining operational continuity in a complex financial environment.

2.238 cases closed

The SOC resolved most of the investigated events, keeping a continuous response and follow-up process.

907 cases resolved without customer intervention

Thanks to the managed **Sentria** model, many investigations were fully resolved by the specialized team, allowing the internal team to focus on strategic activities instead of repetitive operational tasks.

Less operational workload for the SOC

Intelligent event correlation, together with continuous rule and automation optimization, helped reduce unnecessary escalations and improve the quality of investigations.

Unified visibility across the environment

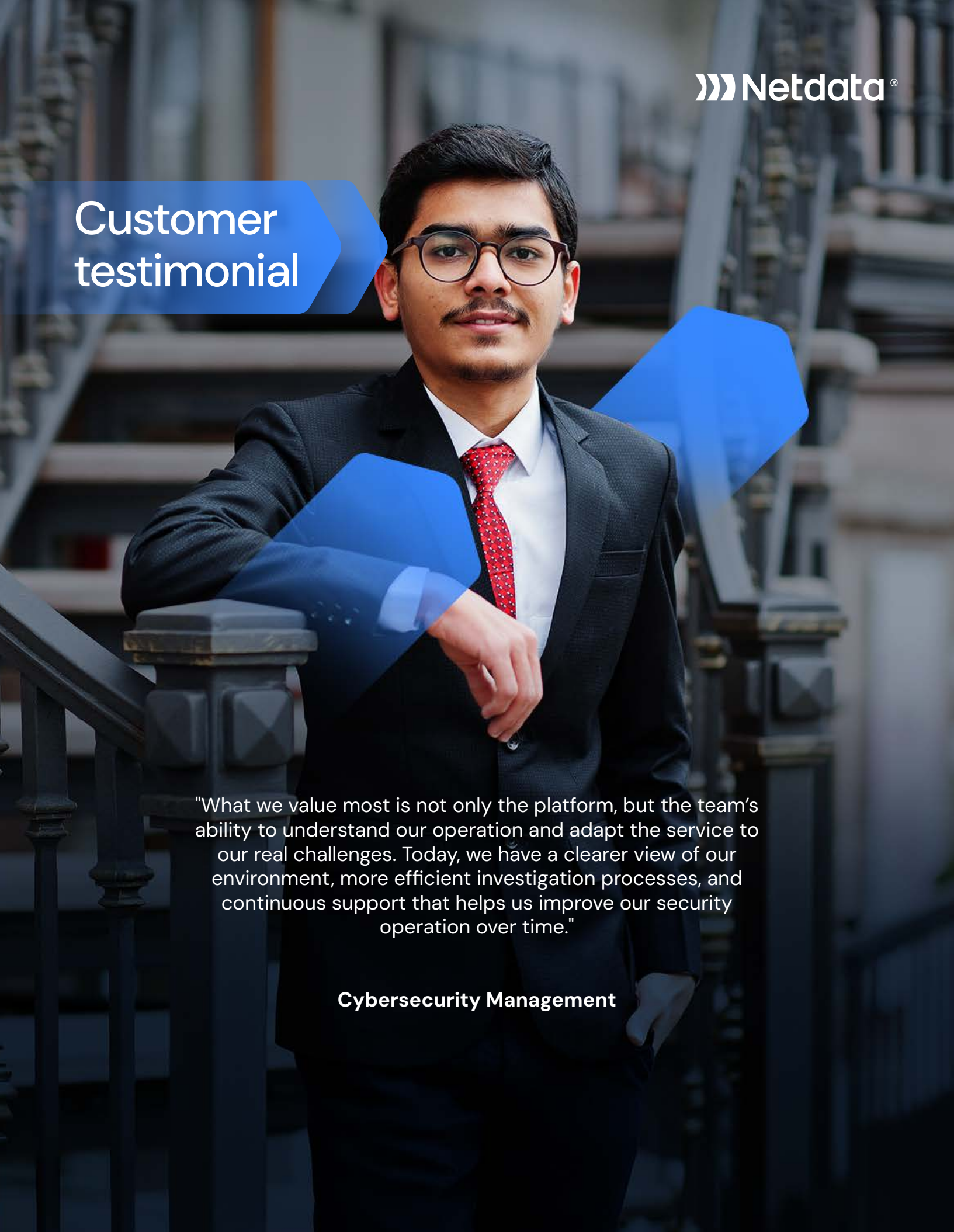
The integration of **25 telemetry sources** provided a centralized view of the technology ecosystem, making threat detection, threat hunting, and incident investigation more effective and contextualized.

Continuous evolution

The service evolved beyond traditional monitoring. Today, it includes continuous alert optimization, new integrations, automation improvements, and technical recommendations that strengthen the customer's security posture over time.

Netdata®

Customer testimonial



"What we value most is not only the platform, but the team's ability to understand our operation and adapt the service to our real challenges. Today, we have a clearer view of our environment, more efficient investigation processes, and continuous support that helps us improve our security operation over time."

Cybersecurity Management

Conclusion

Security Operations Centers can no longer measure success only by the number of alerts they process.

Their real value is the ability to turn large volumes of information into timely decisions that protect the business.

This case shows how the combination of **Cortex XSIAM, Sentria**, artificial intelligence, automation, and a specialized team helped transform a reactive SOC into an operation focused on prioritization, investigation, and intelligent response.

More than implementing a platform, the organization adopted a continuous improvement model that allows it to integrate new data sources, optimize detection capabilities, and strengthen resilience against an evolving threat landscape.

At Netdata, we understand that SOC transformation does not depend only on technology. It depends on combining experience, operational knowledge, and specialized services to help organizations make better decisions when it matters most.

Netdata®

www.netdatanetworks.com