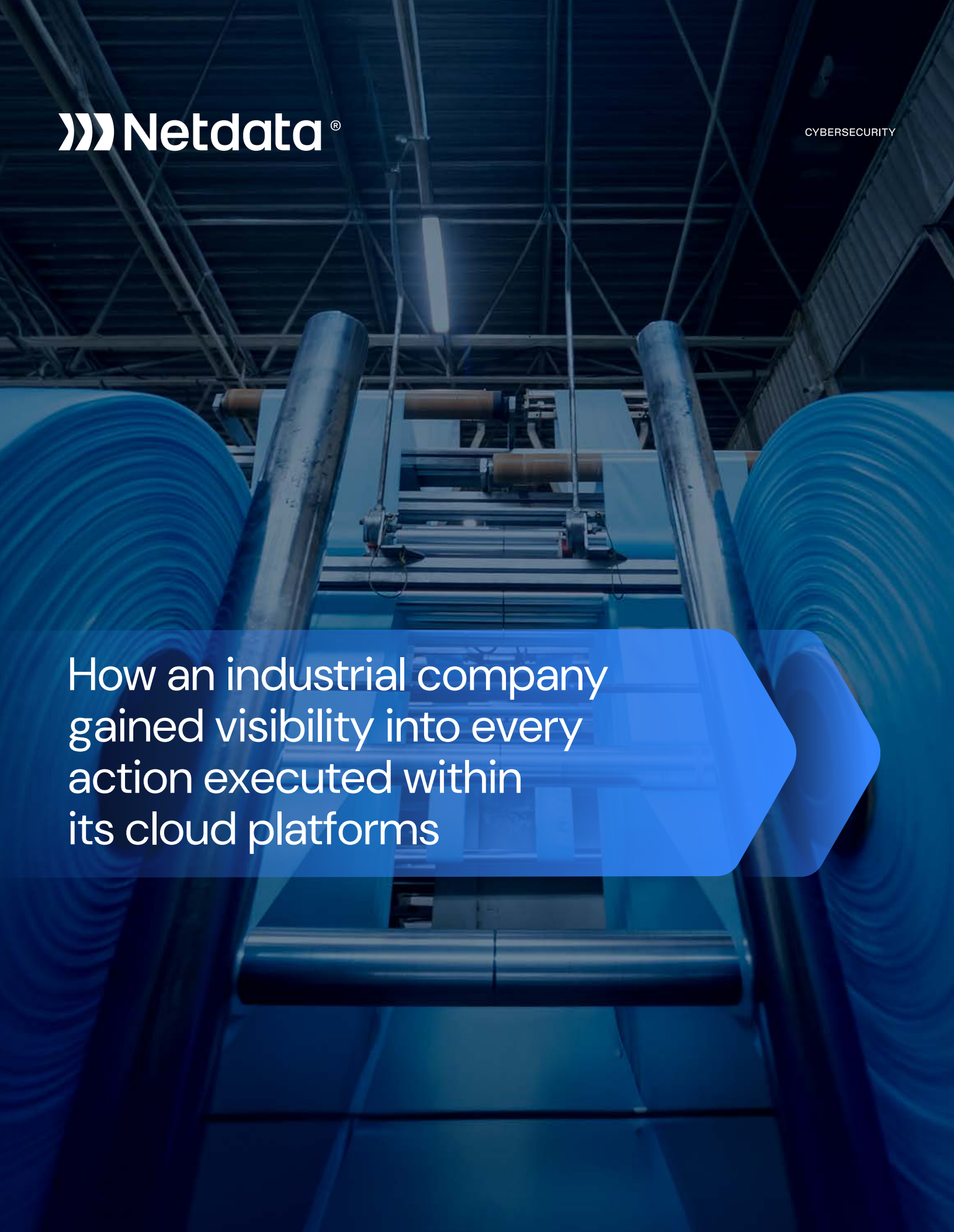
Netdata®

CYBERSECURITY



How an industrial company gained visibility into every action executed within its cloud platforms

Challenge

Having MFA does not mean knowing what happens inside the cloud.

Digital transformation has profoundly changed the way organizations manage their technology infrastructure.

In modern industrial environments, cloud platforms are no longer just complementary services: they support critical components of administration, security, operations, and technology integration.

For a major Latin American industrial organization, this created a growing challenge.

The company had mature authentication controls in place, including Single Sign-On and Multi-Factor Authentication. However, its team identified an important gap in its security posture:

access was protected, but the activities performed within cloud consoles had limited visibility.

Internal administrators, specialized teams, and external providers could access critical platforms and execute sensitive actions without a robust mechanism for detailed logging, operational evidence, or complete traceability.

Netdata®

Simple questions became difficult to answer:

Who changed this configuration?
What actions did an external provider perform?
What exactly happened within an administrative session?
Is there verifiable evidence of the operations performed?

In an environment where multiple cloud platforms are part of the technology ecosystem, this lack of visibility represents much more than a technical need: it creates governance, operational control, and investigation risks in the event of potential incidents.

The challenge did not end there

The existing technology architecture depended on a specific identity provider, creating additional restrictions for properly integrating the required auditing capabilities.

The project needed to solve visibility, auditing, identity, and architectural integration challenges simultaneously.

Netdata®

Solution

Building an observability layer over privileged cloud access.

To address the challenge, a specialized architecture focused on identity, auditing, and administrative cloud activity control was designed.

The solution combined:

Secure Cloud Access:

to strengthen control and supervision of access to critical cloud platforms.

Cyber Identity:

to support the identity model required by the technology environment.

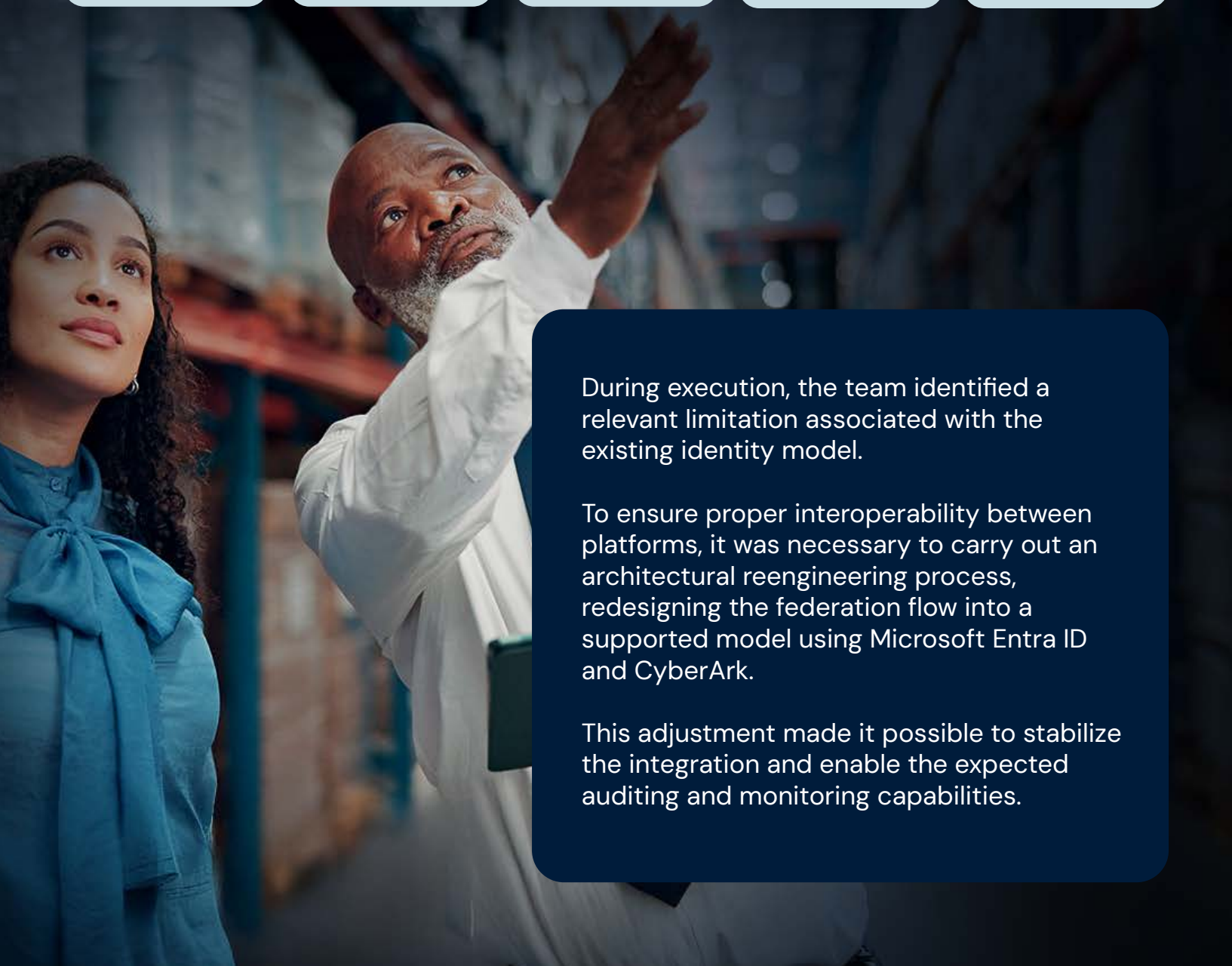
Secure Web Session:

to capture, record, and audit activities executed within web-based administrative.

Netdata®

The implementation was developed over approximately three months, following a structured methodology based on:

- Technical assessment and understanding of the environment
- Architectural design
- Configuration and integrations
- Functional testing
- Transition to production



During execution, the team identified a relevant limitation associated with the existing identity model.

To ensure proper interoperability between platforms, it was necessary to carry out an architectural reengineering process, redesigning the federation flow into a supported model using Microsoft Entra ID and CyberArk.

This adjustment made it possible to stabilize the integration and enable the expected auditing and monitoring capabilities.

Netdata®

Results

From authenticated access to complete evidence of administrative activity.

More than 10 critical platforms integrated under centralized auditing.

The organization initially integrated 10 cloud platforms into the new custody and monitoring model.

Subsequently, the continuous service model made it possible to expand the scope by adding six additional platforms, which gradually increased coverage throughout the protected area..

Detailed visibility into administrative sessions

The implementation delivered capabilities that were not previously available to the client:

- Recording of web-based administrative sessions
- Auditing of activities executed within cloud consoles
- Evidence of actions performed by administrators and third parties
- Operational traceability over changes and sensitive operations

The result was a paradigm shift: moving from knowing who accesses the environment to understanding what actually happens after access is granted.

Architecture optimized for secure integration
The reengineering based on Entra ID + CyberArk made it possible to overcome pre-existing design restrictions and establish an integration model aligned with the client's technological complexity.

Customer Success as a continuous operational capability.

The project evolved beyond a one-time implementation.

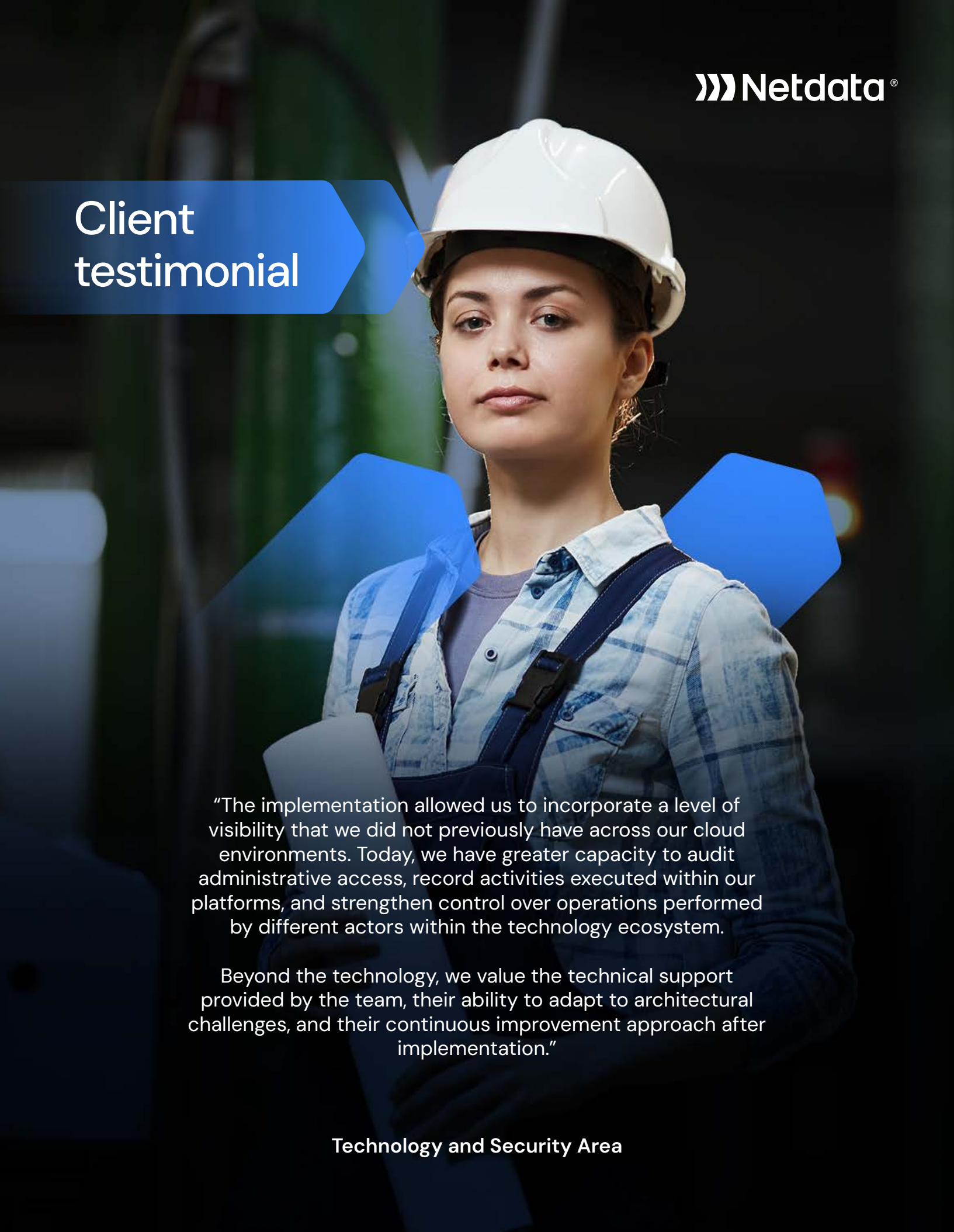
Afterward, the client adopted a continuous technical support model, where a dedicated engineer works weekly on:

- New integrations
- Technical recommendations
- Configuration optimization
- Evolution of the protected environment

This model helped maintain operational stability with a preventive approach, registering only two support tickets during the post-implementation stage.

Netdata®

Client testimonial



"The implementation allowed us to incorporate a level of visibility that we did not previously have across our cloud environments. Today, we have greater capacity to audit administrative access, record activities executed within our platforms, and strengthen control over operations performed by different actors within the technology ecosystem.

Beyond the technology, we value the technical support provided by the team, their ability to adapt to architectural challenges, and their continuous improvement approach after implementation."

Technology and Security Area

Conclusion

Modern cloud security is no longer limited to authenticating users.

Organizations need to answer a much more complex question: what actually happens inside their platforms once access has been authorized?

This case demonstrates how a strategy based on session auditing, privileged access governance, federated identity, and continuous technical support can transform an environment with partial visibility into an operating model based on traceability, evidence, and administrative control over critical cloud platforms.

The combination of Secure Cloud Access, Cyber Identity, and Secure Web Session strengthened not only access, but also the organization's ability to observe, record, and understand the activities executed within its technology environment.

Netdata understands the challenges associated with hybrid architectures, complex identity models, and constantly evolving cloud operations. Its experience integrating platforms, resolving architectural restrictions, and supporting the operational maturity of its clients makes it possible to accelerate complex implementations and turn cloud security into a continuous capability for governance and control.

Netdata®

www.netdatanetworks.com