Netdata®

CYBERSECURITY

Success story:

How to comprehensively secure over 6000 ATMs

Threat isolation
in 1 to 2 minutes

100% block
rate of penetration attempts

Immediate isolation
based on suspicious behavior

AI-driven automated
rules for legacy infrastructure

Netdata®

The challenge

A leading financial institution in Latin America operates as a regional conglomerate with a presence in the Colombian market and throughout Latam. Its infrastructure constitutes one of its most critical assets, supported by a network exceeding 6,000 ATMs and kiosks in the region, which serve as the primary physical and transactional contact point for millions of citizens. The relevance of this network is not limited solely to cash availability, but rather represents the entity's footprint across the national territory, demanding continuous and secure operability.

This massive regional network demands a unified and highly sophisticated cybersecurity model, capable of protecting critical data processing nodes in geographically dispersed environments with varying hardware specifications.

This organization faced the problem of having critical vulnerabilities in its physical infrastructure. The triggering incident occurred when malicious actors managed to breach an ATM and access its internal hardware, connecting unauthorized peripheral devices to attempt executing malicious actions. The previous security solution, based on traditional antivirus, proved to have limitations against custom devices and advanced threats that do not rely on known signatures.

The company attempted to deploy different solutions to protect its network of ATMs and kiosks, but several had limitations, failing to provide a comprehensive response to their security needs.

Netdata®

The process

The project began with a meticulous assessment of the entity's hardware diversity, which included more than 10 ATM models from different brands and kiosks that also allow cash transactions. The technical team identified between 60 and 70 specific components for each model (readers, printers, PCI chipsets) that had to be mapped to ensure their proper functioning under a restrictive security framework.

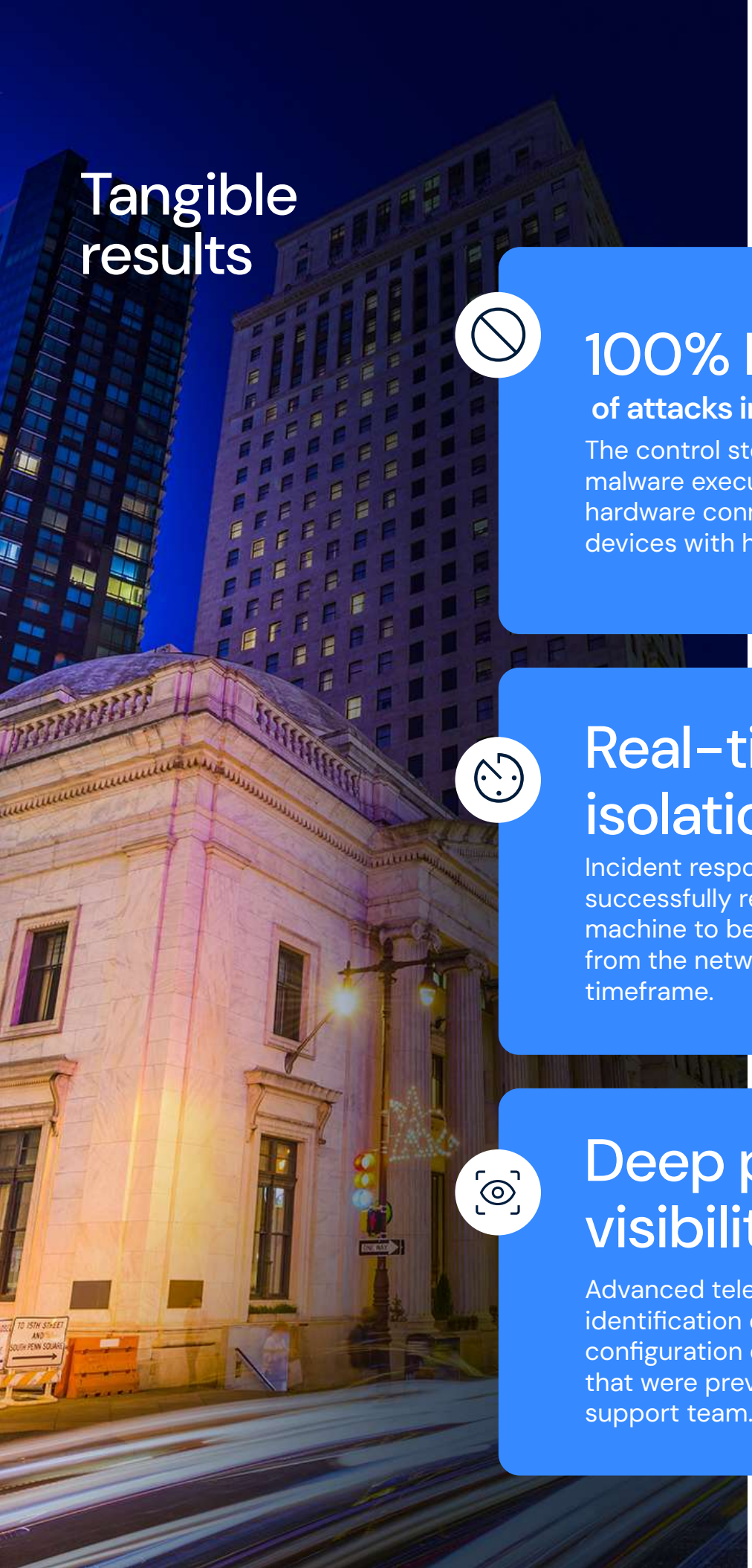
An initial "total lockdown" methodology was applied, progressively enabling only the logical processes and PCI connections essential for operation. This sanitization process made it possible to eliminate risks from unknown peripheral devices and ensure that each machine operated exclusively with its original parts.

Netdata®

The solution

An advanced protection architecture based on Cortex XDR was implemented, allowing centralized management of security and the local firewall for each ATM. The solution integrates:

- Behavior-based threat detection (MITRE tactics and techniques).
- Automated response for the immediate isolation of machines upon suspicion of compromise.
- Full control over peripheral and USB devices.



Netdata®

Tangible results

100% block rate

of attacks in penetration tests:

The control stopped all attempts of malware execution and unauthorized hardware connection, including devices with hidden class identifiers.

Real-time isolation:

Incident response time was successfully reduced, allowing a machine to be contained and isolated from the network within a 1 to 2-minute timeframe.

Deep process visibility:

Advanced telemetry now allows the identification of operational failures and configuration errors in the ATM software that were previously invisible to the support team.

Client testimonial

"We managed to elevate the protection of our critical infrastructure to the level of sophistication that today's market demands. We now have the certainty that every physical connection in our ATMs is monitored and that we can act on any anomaly remotely and automatically, without affecting our users' experience."

Cybersecurity Management.

Why Netdata?

ATM security cannot be solved with generic tools. This case confirms that the combination of detailed hardware mapping, along with automated response capabilities, transforms a vulnerable infrastructure into a resilient environment under total control.

Netdata understands the different types of critical infrastructures in ATMs. Having mapped the diversity of legacy hardware and internal components from multiple brands drastically reduces the time required for information gathering in new implementations, enabling an efficient transition toward restrictive security models without compromising business operations.

Beyond threat protection, it achieves an automated response capability that isolates suspicious machines in a matter of minutes and advanced telemetry that provides visibility into logical system errors, transforming cybersecurity into a diagnostic and preventive control tool for the entire financial network.

Netdata®

www.netdatanetworks.com