CASE STUDY

# How Ascenty Achieved a 50% Maturity Leap in Cyber Risk Management

Ascenty leverages Claroty xDome to secure 26 global data centers and bridge the IT/OT gap without disrupting critical SLA-backed tenant availability

## Overview

With a sprawling network of facilities across Latin America, it was hard for Ascenty to have a continual picture of their CPS assets. They couldn't use existing equipment or traditional IT security methods that would risk operational disruption, so the team sought out a purpose built solution for CPS protection. Ascenty selected Claroty xDome to automatically inventory assets, monitor network traffic in real time, and deliver contextualized insights that enable risk-based vulnerability prioritization, network segmentation, and the implementation of compensating security controls without affecting continuous operations. Ascenty saw fast results, achieving their asset visibility goals in just six weeks. The team also fully integrated xDome's CPS insights with their SIEM within six months. As a result, Ascenty achieved an estimated 50% improvement in its cybersecurity and cyber risk management maturity aligned with the NIST SP 800-82 framework, successfully transforming security into a strategic business capability that guarantees SLA-backed reliability for global cloud and enterprise customers.

## About Ascenty

Founded in 2010, Ascenty is Latin America's largest data center provider, with 40 facilities across Brazil, Mexico, Chile, and Colombia interconnected by a 4,000 km fiber-optic network. Backed by Brookfield Infrastructure Partners and Digital Realty, the company serves major cloud providers and clients across the financial, retail, industrial, and healthcare sectors.

## Challenges

Operating as the backbone for Latin America's digital economy, Ascenty recognized that physical resilience and digital security are inextricably linked. Securing their operational network presented several distinct hurdles:

**Gaps in Critical Asset Visibility:** To support the scale and complexity of its data center operations, Ascenty aimed to strengthen visibility across critical infrastructure assets through real-time automation, streamlining operations and minimizing manual reconciliation efforts.

**Fragile Legacy OT:** They were dealing with critical legacy equipment that could not simply be updated or subjected to intrusive IT scans without risking system faults or downtime.

**Supply Chain Trust:** As a carrier-neutral provider for major cloud companies and Tier-1 clients, Ascenty needed to provide concrete, defensible proof of their security posture to satisfy demanding tenant audits and secure high-value workloads.

**"In operational environments, security cannot be managed the same way as in traditional IT. We are often dealing with critical legacy equipment that cannot simply be updated. We need to understand the level of risk, the criticality of each asset, and which compensating controls can be applied without affecting operations."**

Rui Mella Junior, Information Security and IT Infrastructure Manager, Ascenty

## Solution

Ascenty deployed Claroty xDome to illuminate their operational environments and standardize security. The implementation delivered precise control over their infrastructure:

**Automated Discovery & Real-Time Monitoring:** Utilizing Claroty Edge, xDome automatically mapped Ascenty's complex BMS and power systems. This safe, active discovery approach provided fast results without sending a single disruptive ping to a critical controller, with passive discovery added for real-time traffic monitoring.

**Context-Driven Remediation Prioritization:** Moving beyond simple CVE lists, Claroty provided contextual insights into vulnerability severity, exploitability, and operational impact, allowing Ascenty to implement smart compensating controls for unpatchable assets.

**Bridging the Gap Between IT and OT:** Within six months, Ascenty fully integrated Claroty's CPS intelligence into its enterprise SIEM, providing critical context to existing SOC workflows, and centralizing alerting and remediation.

## Benefits

The transition from a manual, opaque environment to a continuously automated assurance model fundamentally shifted Ascenty's business posture.

**Added Operational Efficiency:** Ascenty eliminated the operational friction of manual asset reconciliation. Gaining automated visibility has helped facility teams more effectively allocate resources and ensure operational uptime. For the SOC team, automating reporting has freed analysts to focus on preventing attacks rather than manual log stitching.

**Ensured Trusted Partnerships:** Security transformed from a support function into a competitive advantage. By establishing a defensible "Single Source of Truth" for their CPS, Ascenty maintained demonstrable security controls that satisfy the most demanding global tenant audits. This confidence and trust is required as a supply chain provider for major technology players.

**Reduced Risk:** The goal of keeping operations running is more attainable with lower risk of an attack. Ascenty is better able to manage their risk today, driving an estimated 50% improvement in their cybersecurity and cyber risk management maturity.

**"The greatest value of the solution is the context it provides. Simply identifying a vulnerability is not enough. We need to understand its severity, operational impact, exploitability, and ultimately its impact on the business."**

Rui Mella Junior, Information Security and IT Infrastructure Manager, Ascenty

## Conclusion

Ascenty's journey with Claroty demonstrates that in data center environments where SLA-backed availability is paramount, cybersecurity must be fully integrated into the operational strategy. By achieving continuous asset visibility and contextualized risk analysis, Ascenty has protected its infrastructure against modern threats.

**"Today, security is no longer just a support function, it has become a strategic business capability. Our customers expect availability, reliability, and operational resilience. Without security maturity, recognized certifications, and demonstrable security controls, it is impossible to compete in this market."**

Rui Mella Junior, Information Security and IT Infrastructure Manager, Ascenty

**About Claroty**

Claroty empowers organizations to protect the mission-critical infrastructure that underpins modern life. The AI-powered Claroty Platform serves as the single source of operational truth, providing the deepest visibility and broadest protection across cyber-physical systems (CPS), leveraging five core solutions: asset inventory, exposure management, network protection, secure access, and threat detection. Claroty helps organizations operationalize CPS protection through a programmatic approach designed to reduce risk, maintain operational integrity, and meet compliance–whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.

CLAROTY