InComm Payments
From Fragmented Data to Confident Decisions

How InComm Built a Data-Driven Security Program with Axonius

InComm Payments™

Customer: InComm Payments – Global financial services and prepaid payments provider operating in 30+ countries

Industry: Financial Services

Number of Employees: 1,001-5,000

Solutions:

- Mitigate Threat Exposure
- Manage & Optimize Assets

Products:

- Cyber Assets

Building Security on a Foundation of Trustworthy Data

InComm Payments operates at the intersection of financial services, healthcare, and global payments infrastructure, an environment where regulatory pressure is constant, systems evolve rapidly, and data risk is always present.

When Luis Valenzuela joined InComm nearly five years ago, the security organization faced a familiar but dangerous reality: fragmented asset data, inconsistent ownership records, and limited ability to confidently scope compliance or prioritize remediation. Security teams were working hard, but without a reliable source of truth, every major initiative required manual investigation, cross-team coordination, and repeated validation.

By adopting Axonius as its cybersecurity asset intelligence platform, InComm established a unified, continuously updated view of its global asset landscape, enabling smarter security decisions, faster compliance workflows, and more effective deployment of protection controls.

As a result:

- InComm improved security project execution efficiency by 40–60%, significantly reducing the time and resources required to track and remediate gaps.
- Asset visibility accuracy improved by an estimated 20%, closing blind spots that often include cloud, containerized, and short-lived production systems.

Today, Axonius serves as the operational data backbone for cybersecurity, IT operations, compliance, and data protection initiatives across the enterprise, enabling teams to shift from reactive troubleshooting to proactive risk management.

A Global Business with Hidden Technical Complexity

Most consumers have never heard of InComm Payments, but they interact with its technology every day.

> "InComm isn't known by name, but most of the gift cards used around the world come from us," said Luis. "We operate in financial services, prepaid cards, healthcare HSA cards, and globally across more than 30 countries."

Behind those transactions is an ecosystem of applications, payment systems, databases, cloud workloads, partner integrations, and regulatory boundaries that shift by geography and industry. For security and data protection leaders, that complexity translates into a critical operational challenge: knowing exactly what systems exist, what data they process, and which controls are in place.

When Luis joined the organization, part of his initial role was helping stabilize and complete security initiatives that had stalled due to lack of visibility.

> "We had compliance gaps, audit findings, and projects that were started but never fully finished. Before we could fix anything, we had to understand what we actually had and where it lived."

Why Visibility Is the Prerequisite for Risk Reduction

For Luis, cybersecurity is fundamentally about informed decision-making, not just technical controls.

> "Security is not only about tools or hacking. It's about relationships, negotiation, and helping the business reduce risk to an acceptable level. But you can't negotiate risk if you don't have reliable data."

Like many enterprises, InComm had multiple systems that each provided partial views of the environment: network tools, endpoint platforms, cloud consoles, CMDB records, and vulnerability scanners. None of them alone provided a complete or consistent asset picture.

As a result, answering basic operational questions often required manual effort:

- Which systems fall under PCI versus healthcare compliance?
- Which environments are production versus staging?
- Who owns each asset?
- Are security controls actually deployed, or just assumed?

Without centralized asset intelligence, security teams were spending valuable time validating assumptions instead of closing gaps.

"I found Axonius to be *the most useful tool* for knowing what assets we have, where they are, and what compliance scope they fall under, PCI, HIPAA, customer contracts, everything."

Luis Valenzuela – Head of Data Governance, Data Protection & DLP

Why Axonius Became the Foundation of the Security Program

InComm became an early adopter of Axonius when Luis was managing security project delivery and compliance remediation efforts.

> "I found Axonius to be the most useful tool for knowing what assets we have, where they are, and what compliance scope they fall under, PCI, HIPAA, customer contracts, everything."

By aggregating and correlating data from more than 50 integrated sources, Axonius allowed teams to:

- Identify all systems regardless of management domain
- Normalize ownership and business context
- Track control coverage across asset types
- Monitor remediation progress over time

> "It gave me a fast way to understand our true scope and track improvement week over week when we were rolling out security controls."

Instead of chasing spreadsheets and reconciling inconsistent reports, teams now worked from a continuously updated, unified asset dataset.

Turning Asset Data into Operational Intelligence

Once Axonius became trusted as the authoritative asset source, its role expanded beyond cybersecurity.

> "We started using it to identify software versions, contract mismatches, unused licenses we were still paying for. It started supporting IT operations and even financial decisions."

Because asset records were enriched with software, ownership, and environment data, teams could now analyze:

- Which systems were running unsupported software
- Where licensing exceeded actual usage
- Which assets should be decommissioned but weren't

> "The value started showing up in places we didn't originally plan for."

Axonius evolved from a security visibility tool into a shared operational intelligence platform across multiple teams.

Breaking the Elephant into Edible Pieces: Endpoint Protection at Scale

One of the clearest examples of Axonius' operational impact came during InComm's enterprise endpoint protection rollout.

Coverage was high, but not complete, and the remaining gaps were difficult to explain.

> "We were close, but we still had assets missing protection and no clear reason why. Teams were overwhelmed because the problem was too big and ownership wasn't always clear."

Using Axonius' filtering and query capabilities, Luis broke the population into actionable segments:

- Systems that had agents installed but dropped off
- Servers that never had agents deployed
- Workstations stuck in staging environments
- Assets with connectivity or configuration issues

> "All of that data helped us break a big elephant into edible pieces."

Each team could now focus on fixing the specific failure modes relevant to their systems, accelerating remediation and preventing recurrence.

> "We saw between *40% and 60% improvement* in how efficiently we used time and resources when managing security projects."

Luis Valenzuela – Head of Data Governance, Data Protection & DLP

Using Axonius to Augment and Validate the CMDB

As confidence in Axonius data grew, it became a validation layer for InComm's CMDB.

> "There were things our CMDB couldn't do that Axonius was doing better. So we used Axonius to identify gaps and clean up ServiceNow."

Instead of debating which system was correct, teams used Axonius to identify:

- Assets missing from the CMDB
- Incorrect ownership assignments
- Misclassified environments

> "We could troubleshoot why assets weren't visible and close the gap between the two systems."

This created a continuous improvement loop, where asset intelligence strengthened CMDB accuracy, and CMDB context further enriched asset intelligence.

Shrinking Compliance Scope Instead of Expanding Work

InComm operates under multiple regulatory frameworks across finance, healthcare, and international markets.

> "We have audits every year, often multiple at the same time. PCI, healthcare, international regulations, all with overlapping and conflicting scopes."

Using Axonius tags and metadata, teams classify assets by compliance domain and regulatory requirements.

This enables targeted compliance workflows:

- Identify in-scope systems
- Validate required controls
- Isolate only the true gaps
- Route remediation to responsible teams

> "We don't waste time fixing systems that are already compliant, and we avoid double work across frameworks."

Because overlapping systems are already validated, new audits often start with a reduced remediation scope.

> "It helps us focus effort where it actually matters instead of spreading resources thin."

Enabling Data Protection Strategy Through Asset Intelligence

As Head of Data Governance and Data Protection, Luis depends on asset intelligence to deploy and operate data security tooling effectively.

> "When I roll out a DSPM or data classification tool, I need to know exactly which database servers are production and which contain sensitive data."

Axonius provides that targeting capability.

> "I can get a full count of all databases across operating systems and environments, then decide where to start. That's how I know I'm not missing something critical."

This ensures that data protection investments align with actual data exposure — not assumptions.

Quantifiable Business Impact

While many security outcomes are difficult to measure, InComm quantified improvements in operational efficiency.

> "We saw between 40% and 60% improvement in how efficiently we used time and resources when managing security projects."

Asset accuracy also improved substantially.

> "I'd estimate Axonius closes about a 20% visibility gap compared to what we'd have otherwise, and that 20% can include critical cloud and production systems."

In highly dynamic environments, those blind spots often represent the highest risk.

Why Luis Recommends Axonius to Other Security Leaders

When peers ask about asset management, Luis is direct.

> "You can't protect what you don't know you have. And Axonius gives you that visibility better than anything else I've seen."

Beyond coverage, usability matters.

> "It's easy to query, easy to build dashboards, and non-technical teams can use it without scripting or complex analytics."

That accessibility allows security, IT, compliance, and business teams to operate from shared, trusted data.

From Visibility to Confidence

For InComm Payments, Axonius is not simply an asset inventory.

It is the data foundation that enables:

- Control deployment
- Compliance readiness
- CMDB integrity
- Data protection strategy
- Executive risk reporting

And most importantly, it allows teams to act with confidence rather than assumption.

> "When I focus on the top 20% of assets that matter most, I know I'm not blind to the rest of the environment. That confidence changes how we operate."

Get Started

Discover what's achievable with a product demo, or talk to an Axonius representative.

Request a demo

Speak with sales

Get started