Western Union Achieves Global Security Visibility and Automation with Axonius

Western Union is one of the world's leading financial services companies, enabling individuals and businesses to send and receive money quickly and securely. With operations in over 200 countries and territories and hundreds of thousands of agent locations worldwide, Western Union processes millions of transactions each day. Protecting customer trust and maintaining compliance with international standards is a core part of its business mission.

Industry: Financial Services

Number of employees: 9,000

Key challenges:

- Fragmented data across multiple tools
- Limited visibility into assets, especially ephemeral devices in AWS
- Manual ticketing and reporting processes consuming valuable engineering hours
- Difficulty correlating users, devices, and entitlements across systems

Solutions: Western Union first deployed Axonius over five years ago with a focus on cyber hygiene: ensuring antivirus coverage, monitoring vulnerabilities, and feeding asset data into Splunk. Today, Western Union uses 38 Axonius adapters to aggregate, normalize, and correlate data from across the enterprise.

Results:

- 99% asset visibility across global operations, including ephemeral AWS instances
- Automated workflows reduced asset management effort by 50%
- Expanded visibility from workstations to servers, networks, certificates, and beyond
- Accelerated compliance reporting for audits, SOC reviews, and M&A activity

"Western Union is like a playground for engineers. Axonius is one of the *best tools we have*."

Douglas Salazar – Engineering Operations Manager, Western Union

Moving Money, Managing Trust

For Western Union's cybersecurity engineering operations team, visibility is more than a metric, it's the foundation for protecting a global enterprise.

> "How do you protect something you can't see?" said Douglas Salazar, Engineering Operations Manager at Western Union.

Together with colleague Victor Ureña, Douglas manages engineering operations across global IT infrastructure that spans traditional data centers, AWS, Oracle, and Google Cloud. Their mission: deliver reliable, real-time visibility to every user, device, and security control across the company. Douglas and Victor aren't just managing cybersecurity operations; they're protecting the backbone of a financial services giant that moves money across hundreds of countries daily. For them, visibility isn't just a metric, it's a requirement.

The High Stakes of Global Visibility

Western Union's IT estate is as complex as its global reach. With multiple data centers, hybrid cloud environments, and hundreds of thousands of endpoints, visibility gaps were inevitable. When Douglas joined Western Union, agent security coverage was ~85% reported via Axonius. With help of Axonius team we tune the queries, and we reached a +90 coverage. Tickets to the support team to install security agents were submitted manually, adding hours of overhead. After Axonius implemented the Service Now automation we were able to create all the tickets needed with no effort. This makes our compliance to Jump to 98%.

Audit preparation means pulling data from multiple sources, now with Axonius we simplified the process as we have all the data in a single location.

> "I came from a company where we used Excel because there was no single pane of glass," Douglas recalled. "At Western Union, AXONIUS provided a smarter way to see all assets, correlate them, and make decisions quickly".

Challenges

The cybersecurity team faces several challenges common to large, global organizations:

Fragmented visibility: Data lives across many tools, each with a partial view. AVM tools show endpoints, but not users. Other tools focus on vulnerabilities, identities or other security controls. No single source ties everything together.

Ephemeral cloud assets: In cloud environments, new machines spin up by the hour and disappear just as fast. Without full visibility, there is no reliable way to ensure security agents and controls are consistently applied.

Manual effort: Without automation, even basic workflows consume valuable engineering time. Ticket creation, coverage validation, and reporting are repetitive and resource intensive.

Compliance:
- With PCI, SOC, and audits for multiple countries recurring regularly, the team needs to demonstrate coverage.
- Validation of EUC policy compliance, by validating endpoints encryption and security controls across a large, distributed environment.

M&A complexity: Integrating newly acquired environments requires fast discovery and validation of security posture, a process that can take months without a unified view.

⋇ Axonius

Consequences

The implications of these challenges are clear. Without a comprehensive source of truth, the team risks:

- **Slower response times** when investigating incidents, resolving access issues or even answering daily management enquiries.
- **Slower audit evidence collection**.
- **Operational inefficiency**, where engineers are tied up in manual tasks rather than strategic projects like Zero Trust or M&A integrations.

> As Douglas emphasized, "We are not just a cost center, we are a value provider. Our role is to keep the company secure and resilient, and we need better visibility to do that effectively".

Solutions

Western Union selected Axonius as its cybersecurity asset intelligence platform, beginning with a focus on cyber hygiene and gradually expanding into technology teams as the source of truth.

Step One: Establish cyber hygiene

The initial scope focused on ensuring antivirus, vulnerability and log collection agents coverage across workstations and servers.

Step Two: Expand visibility enterprise-wide

Over time, the deployment scaled to 38 adapters connected to Axonius spanning:

- Workstations, servers, and networks
- AWS and other cloud infrastructure
- Certificates and encryption status
- Local user accounts
- Security tools including CrowdStrike, Active Directory, and Netskope

Step Three: Automate workflows

ServiceNow integration replaced manual ticketing. Automated actions now validate controls, trigger policy enforcement, and update asset inventories in real time.

Step Four: Address ephemeral cloud environment devices

With a stable compliance in 99% we decided to enforce the policies to other devices. This caused our compliance to fall again to 92%. Working with Axonius and the cloud security team, the engineers-built scripts to ensure ephemeral cloud machines had security agents attached in a matter of hours. This brought coverage up to 99%, even for instances that lived only minutes or hours.

> "The only way to gain visibility into these devices is through Axonius," Victor said. "Now we can see them closer to real time, apply controls.

Step Five: Enable cross-team adoption

Today, multiple teams beyond security, including network, compliance, and operations, rely on Axonius as their trusted source of asset intelligence.

A Single Source of Truth for Global Enterprise

With Axonius, Western Union has transformed its cybersecurity operations:

- **99% Asset Coverage** across all environments, including ephemeral cloud instances.
- **50% Reduction in manual workload**. Victor now spends half his time on strategic projects instead of manual asset management.
- **Faster audits** with automated dashboards supporting PCI, SOC, and specific compliance and regulation from different countries.
- **M&A agility**, rapidly discovering and securing assets in newly acquired or integrated environments.
- **Cross-team collaboration**, with Axonius serving as a single pane of glass for multiple teams beyond Cybersecurity.

"Axonius isn't just security, *it's visibility* for the whole enterprise."

Victor Ureña – Network Security Engineer, Western Union

Axonius

Visibility as a Business Enabler

For Western Union, visibility isn't just about data, it's about trust. Every endpoint, cloud instance, and digital connection represents a customer depending on them to move money safely across the world. By adopting Axonius, Western Union didn't just modernize cybersecurity; they redefined what operational clarity means for a global enterprise.

With one source of truth uniting IT, security, and compliance, the team now moves faster, audits easier, and collaborates better. Manual work has given way to automation, freeing engineers to focus on innovation instead of maintenance. Coverage gaps that once required hours of troubleshooting now close themselves in real time.

In an environment where every second counts, Axonius helps Western Union stay ahead, not just reacting to threats, but continuously improving the way they secure, support, and serve millions of people around the world.

> "It's not just about security, it's about enabling better ways for the business to function." - Douglas Salazar, Engineering Operations Manager, Western Union

Western Union's story proves that visibility isn't a destination. It's a continuous advantage, one that empowers people, accelerates progress, and strengthens the trust that moves the world.

"Axonius isn't just a security tool, *it's our source of truth*. If someone calls with a server issue, I can paste the name into Axonius and instantly see its configuration, location, and policies. That kind of visibility is invaluable".

Victor Ureña – Network Security Engineer, Western Union

Get Started

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

Request a demo

Speak with sales

Get started