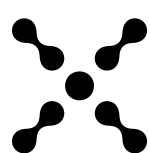


AI Doesn't ~~Replace~~ Fundamentals

Why cybersecurity
fundamentals still matter
in security operations



Axonius

AI Drives the Need for **Fundamentals** in Security Operations

INSIGHT 01

AI cannot fix bad telemetry; it only scales what you feed it.

INSIGHT 02

AI tools fail at correlation and need clean, normalized data.

INSIGHT 03

Knowing what you have and how it is exposed is the core need.

For decades, security automation was met with deep skepticism. Security and IT teams avoided automated response because the risk of accidentally taking down critical business systems far outweighed the benefits. When attack cycles were slower, teams had enough time to manually detect, test, and respond to threats. Today, the fear of AI-powered attacks operating at machine speed has shattered that time buffer, drastically lowering the risk barrier to automation.

Driven by this urgency, executive leadership teams across industries are urging security departments to deploy AI tools to accelerate threat detection and augment manual workflows.

Artificial intelligence acts as an amplifier of an organization's existing defensive posture, not a substitute for it.

Deploying machine learning models or autonomous agents on top of unverified endpoint coverage, unenrolled identity management, and fragmented asset inventories produces unreliable results and false confidence.

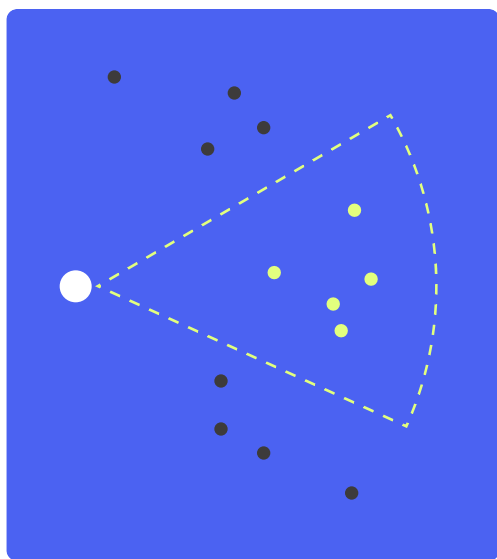
The primary bottleneck preventing security teams from realizing the operational benefits of artificial intelligence is not algorithmic sophistication, but control readiness. Organizations must prove that basic security fundamentals hold before automated intelligence can deliver trustworthy value.

Establishing Complete Visibility for AI

Artificial intelligence models construct their understanding of an environment primarily from the telemetry feeds supplied to them.

When visibility into specific network segments, cloud environments, or remote devices is missing, the underlying model develops an incomplete representation of normal behavior. Legacy inventory practices that rely on periodic manual audits or batch network scans are insufficient for real-time automated processing. Cloud instances, containerized workloads, and microservices are created and destroyed continuously, requiring dynamic, real-time data ingestion across every technical layer.

If a device or system is left out of your initial data feeds, AI tools cannot track its software, spot suspicious logins, or accurately judge its security risks. Gathering complete, well-organized data from every device, cloud service, and network connection is the essential first step before successfully deploying artificial intelligence.



Each tool only operates from its own limited point of view and formats data in its own way.

Unifying Fragmented Data to Prove Control Readiness

Even when data collection is thorough, security teams usually rely on dozens of different tools, and no single system sees the whole picture. Each tool only operates from its own limited point of view and formats data in its own way. For example, a cloud scanner, an endpoint agent, and a firewall might all monitor the same server, but they describe hostnames, IP addresses, and software versions differently. This fragmentation makes it much harder for AI to connect the dots and cross-reference events accurately.

Some organizations try to fix this by building internal AI models to translate and organize data from different systems on the fly. However, this DIY approach often fails because **generative AI makes educated guesses rather than following strict, exact rules**. When fed complex security data, these custom models can make subtle mapping errors, make up missing details, or unpredictably change data fields.

Building your own asset tracking tools also creates endless maintenance as vendor formats change. These fragile, home-grown tools require constant oversight to catch hidden errors and AI-generated fabrications. Ultimately, when your underlying data relies on AI guessing, you cannot reliably prove your security control readiness. True security posture requires clear proof; not just that an asset exists, but that every required security control on it is actively installed, properly configured, and working as expected.

In Practice with Western Union:



Control Readiness Demands Reconciled Ground Truth

As Western Union scaled its global operations across complex hybrid and ephemeral cloud environments, the challenge wasn't simply deploying security tools. Multiple systems already monitored endpoints, identities, and infrastructure across hundreds of countries. The real challenge was unifying those fragmented data streams and ensuring security controls automatically followed fast-moving, short-lived assets.

That coverage gap revealed a risk that basic monitoring could not address.

Western Union pushed asset coverage from 85% to a stable 99%, even across ephemeral cloud instances. Automated workflows eliminated 50% of manual operational effort and streamlined complex global compliance audits. The point wasn't simply that Western Union could track more assets.

It was that the enterprise established a single, automated source of truth, empowering teams to act on real-time intelligence and maintain global business trust.

Victor Ureña

Network Security
Engineer,
Western Union



"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".

TAKEAWAY

By replacing fragmented tool data with a continuously reconciled source of truth, Western Union achieved 99% asset coverage and cut manual security tasks by 50%.

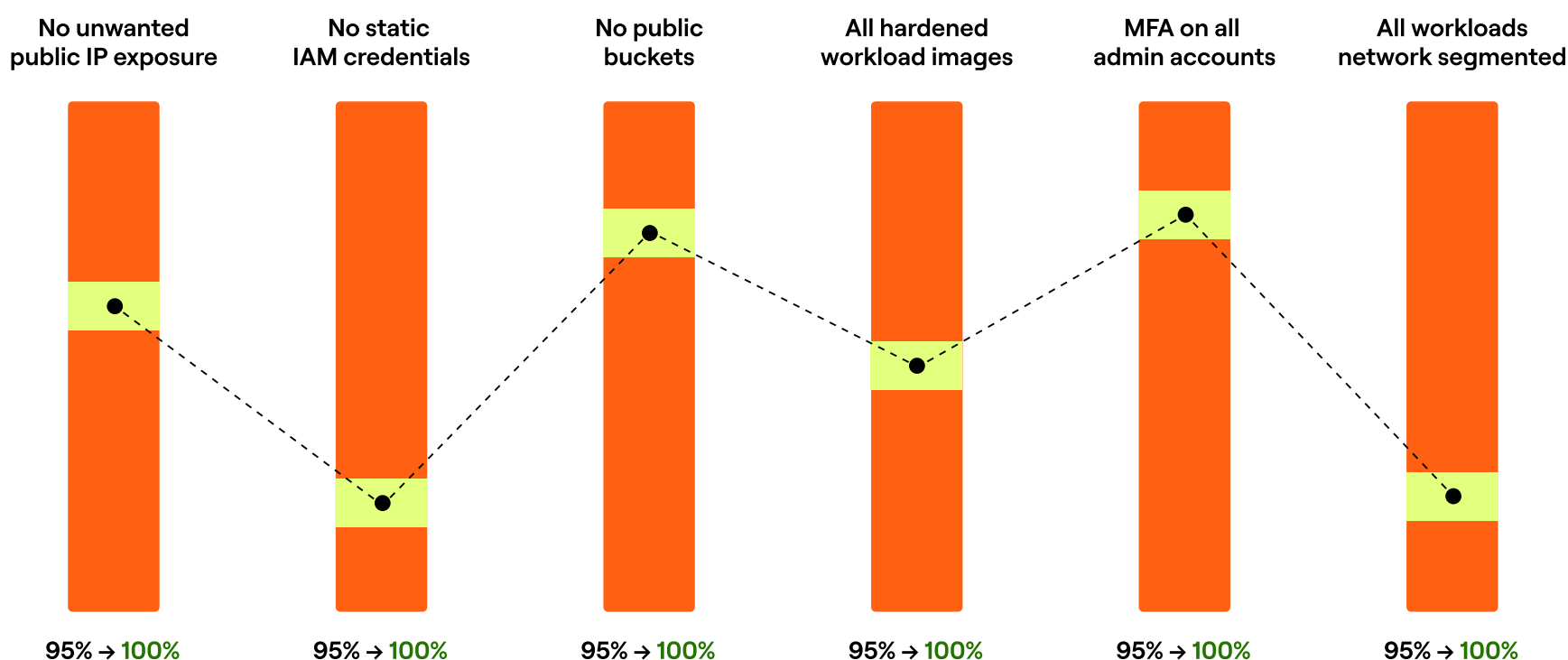
AI tools struggle to tell the difference between real security failures and normal daily activity, leading to false alarms and severe alert fatigue.

Continuously Reconciled Context and Asset Intelligence Pitfalls

Security-oriented AI tools evaluate control readiness by checking live data against defined rules, known as security invariants. When a company lacks a clear, up-to-date view across servers, virtual machines, and cloud containers, it cannot prove whether required security tools are actually active. This creates background noise that easily confuses automated systems.

Capturing the most accurate state of readiness ensures your data reflects true operational reality, proving that protective measures work as intended. Without continuously verifying these control invariants, AI tools struggle to tell the difference between real security failures and normal daily activity, leading to false alarms and severe alert fatigue.

Proving this readiness presents several practical challenges. Security teams often rely on outdated asset lists built from occasional network scans. These static lists fail to confirm whether security software is properly installed or running on fast-changing cloud systems.



Data scattered across separate security tools makes proving readiness even harder, as endpoint software, vulnerability scanners, and cloud platforms often show conflicting details for the same server. On top of that, unmanaged shadow infrastructure creates blind spots where control invariants cannot be tracked at all.

Lastly, failing to combine business context against asset data stops automated systems from evaluating control readiness against business impact. Without this connection, security teams cannot determine which compliance gaps pose the biggest risk or need immediate attention.

In Practice with the City of Los Angeles



Turning Organized Chaos into Automated Control

Security data at the City of Los Angeles lived in silos, with each of 40+ departments running its own tools and datasets, leaving the ISOC without a single view of what existed or whether it was protected and forcing analysts to piece things together in spreadsheets while investigations stretched into hours or days.

Axonius connected those existing data sources into one view, correlating users, accounts, and devices across Active Directory, cloud, and on-prem systems in real time, then turned that correlated foundation into action through hundreds of automated enforcement workflows across the city's EDR systems and custom scripts.

The result is visibility across 40+ departments and thousands of assets, investigation time cut from hours to minutes, stale accounts disabled and vulnerable endpoints flagged before they become incidents, and consistent audit reporting from a single source, showing that visibility was the missing piece and that connecting the data is what made the automation possible.

Joanne Scott

Senior Security
Analyst,
City of Los Angeles



"We rely on Axonius not just for visibility, but for automation...it's how we know our security stack is truly being deployed across the entire city."

TAKEAWAY

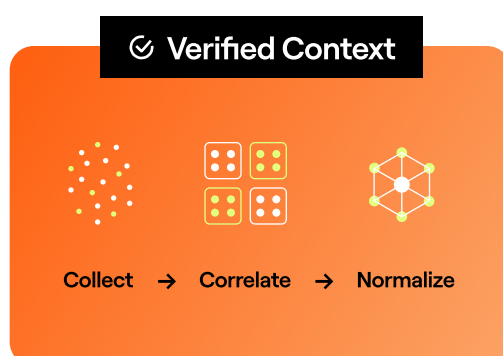
By connecting data from tools across 40+ departments into a single view, the City of Los Angeles **gained the visibility to automate enforcement citywide and cut investigation time from hours to minutes.**

Establishing a complete and standardized ground truth is not an extra burden, but the fundamental requirement for proving security control readiness in the age of artificial intelligence.

Building the Operational Maturity Model for AI Adoption

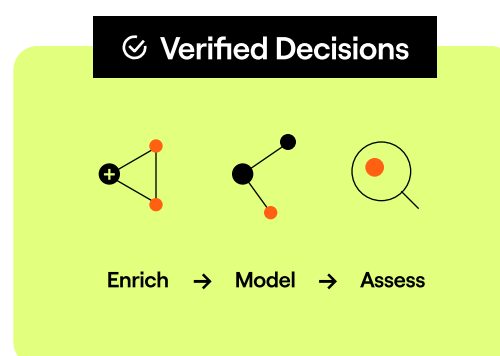
Achieving readiness for artificial intelligence requires a structural shift toward a continuously reconciled data layer that sits above the existing software stack. By ingesting telemetry directly from deployed security tools, this system converts fragmented data into an authoritative ground truth through six steps:

- **Collect:** Ingest telemetry continuously from existing endpoint platforms, network monitors, identity systems, and cloud management consoles.
- **Correlate:** Merge duplicate records from competing security tools into single, authoritative asset entities.
- **Normalize:** Standardize data fields so that attributes like operating systems, hostnames, and vulnerability severities carry identical meanings across all sources.
- **Enrich:** Attach organizational ownership, business criticality, and data sensitivity context directly to unified asset records.
- **Model:** Map dynamic relationships across the environment, linking users, infrastructure, software dependencies, and network pathways.
- **Assess:** Evaluate the modeled environment continuously against security baselines tailored to every asset class, including servers, cloud containers, and emerging artificial intelligence tools like agents and non-human identities.



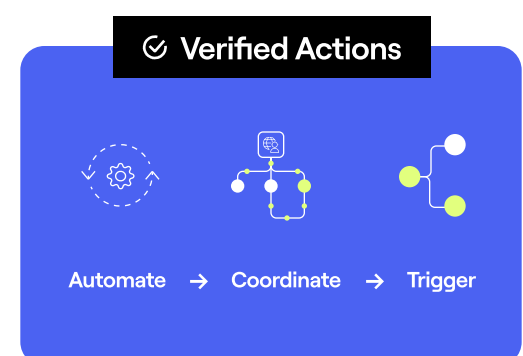
Dynamic Asset Source of Truth

- 1400+ API-based **adapters**
- **Continuous discovery** cycles
- A powerful **correlation** engine



Flexible Prioritization Engine

- Unify **asset, business, security context**
- Real-time **query** and **reporting**
- Smart **prioritization**



Multiple Mobilization Modes

- Complete view of **asset ownership**
- **Automation** where it makes sense
- **Integration** with existing ticketing / operations

Mastering these steps prepares security operations for the future. Maintaining a complete view of what assets exist and whether their required security controls are active creates the trustworthy baseline needed to power every downstream tool, from vulnerability scanners to automated response engines.

Downstream systems cannot accurately measure control readiness or take effective action when built on outdated or conflicting inputs. Establishing a complete and standardized ground truth is not an extra burden, but the fundamental requirement for proving security control readiness in the age of artificial intelligence.

Ten Questions to Ask Yourself

- ☐ **Is my asset inventory complete enough for AI?**
Can I account for every endpoint, cloud instance, container, and remote device?
 - ☐ **How current is my asset data?**
Periodic scans and manual audits, or continuous ingestion as workloads appear and disappear?
 - ☐ **What does control readiness look like for us, and can I prove it?**
For any asset, can I show each required control is installed, configured, and running?
 - ☐ **How much of my security data is fragmented across tools?**
How much of my security data is fragmented across tools?
 - ☐ **How are we relying on generative AI to normalize security data?**
If a model infers field mappings, how would I catch a silent error or fabricated attribute?
 - ☐ **Can we properly map the relationships between our assets?**
Do I know which users, dependencies, and network pathways connect to a given system?
 - ☐ **Are my security invariants continuously verified?**
Can tooling tell a real control failure from routine change, or does it surface as alert fatigue?
 - ☐ **How do I surface unmanaged infrastructure?**
What finds systems no one enrolled, and how long would one sit unnoticed?
 - ☐ **Is business context attached to my asset records?**
Do ownership, criticality, and data sensitivity sit alongside technical attributes?
 - ☐ **How are we using AI for security automation today, and how will that change in six months?**
Which workflows already depend on model output, and are the agents involved inventoried as assets?
- AI starts with asset intelligence. Learn more at axonius.com.