Brooks Running Gains Real-Time Asset Visibility to Support Secure Global Growth

How Brooks Running reduced flawed system builds by 90% while strengthening security operations at scale

BROOKS

Brooks Running creates market-leading performance running footwear, apparel, and accessories distributed worldwide. Since 1914, Brooks has been propelled by a never-ending curiosity with how humans move, pushing the limits of motion science, engineering, and technology to create gear that unlocks the power of energy and movement for everyone. Today, Brooks is a global performance running brand with more than 1,400 employees worldwide and operations spanning e-commerce, global distribution, data science, and digital experiences. Over the past decade of rapid growth, Brooks' technology environment has expanded significantly, requiring greater precision and visibility to ensure systems remain secure, reliable, and consistent at scale.

When Jon Hocut, Director of Information Security, introduced Axonius to the organization, the goal was simple: establish accurate visibility across Brooks' technology environment and eliminate operational friction caused by asset discrepancies and security agent gaps. In just months, Brooks achieved measurable improvements in security operations, including a 90% reduction in flawed system builds and significantly improved visibility across its infrastructure.

Results at a Glance

- 90% reduction in flawed system builds – Real-time visibility and accountability across teams reduced build errors within just a few months.
- 20% improvement in asset inventory accuracy – Automated reconciliation helped manage Brooks' infrastructure inventory.
- Faster issue resolution across multiple teams – Automated JIRA ticket creation allows teams to quickly identify and address security control gaps.
- Improved visibility across servers and security agents – The security team can now quickly determine whether discrepancies are caused by build issues, agent failures, or decommissioning gaps.
- Reduced operational friction across security and infrastructure teams – Multiple teams now work from a shared view of asset data instead of manually reconciling discrepancies.

"With Axonius, we can *finally tell the difference* between a build problem, an agent failure, or a decommission process that wasn't followed."

Jon Hocut – Director of Information Security

Securing Growth Across a Diverse Technology Environment

Brooks Running's success has always been rooted in product innovation, athlete insight, and deep trust with runners. As the company has grown globally, technology has become an increasingly critical enabler, supporting e-commerce, global operations, data science initiatives, and digital experiences for runners worldwide.

That evolution has resulted in a technology environment that spans modern cloud-native applications alongside long-standing systems that continue to support core business functions. Protecting this diverse ecosystem requires visibility, context, and a pragmatic approach to security modernization.

> "We've had very rapid growth over the past 10 years, said Jon Hocut, Director of Information Security. "Our environment includes highly modern, forward-thinking deployments alongside long-standing systems that support critical business operations."

The result is an environment that blends modern cloud-native applications with systems that have been running quietly in the background. Many of the older systems were never designed with today's security expectations in mind.

> "Some of these systems were deployed when Brooks had just one or two people in IT doing everything," Jon explained. "Securing those systems after the fact, without breaking production, is an extreme challenge."

This hybrid environment spans e-commerce platforms, data science initiatives, global operations, and legacy infrastructure that newer applications still depend on. For the security team, protecting this ecosystem requires both accountability at scale and careful preservation.

A Security Philosophy Grounded in Business Reality

Jon's approach to security is pragmatic, and deeply tied to business outcomes. Rather than pursuing security in isolation, his team focuses on managing risk in a way that enables the broader goals of the organization.

> "My job is to help the business manage risk," he said. "The best security outcome is whatever leads to the best business outcome."

That philosophy means making trade-offs.

In some cases, pursuing the most restrictive security posture could slow innovation or disrupt operations. Instead, Jon's team works to balance protection with productivity. Security, in this model, becomes a strategic partner rather than an obstacle.

And while the work often goes unnoticed when things are going well, Jon says that's simply the nature of the profession.

> "Security can be a thankless job," he said. "You have to be self-motivated and understand your own value."

Fortunately, Brooks' executive leadership understands the importance of the mission.

> "I'm lucky to have a very supportive senior executive staff here," Jon said. "They're happy that they don't have to think about security very often, that's exactly how it should work."

The Visibility Problem That Slowed Things Down

As Brooks scaled, maintaining consistent visibility across systems became increasingly complex, not because of a lack of investment, but because of the sheer pace and breadth of growth. Before implementing Axonius, Brooks' security team faced a problem common to many growing organizations: asset visibility that was constantly drifting out of sync. Servers and workstations were sometimes deployed without the full set of required security tools. Other systems were decommissioned without proper updates to inventory records.

The result was a steady stream of discrepancies across multiple systems. Several teams, including infrastructure, security engineering, and operations were spending significant time trying to reconcile those differences.

> "We were constantly chasing discrepancies," Jon said. "And it was burning time for four different teams."

The manual process for resolving those issues only made the situation worse. Every discrepancy required a support ticket. Those tickets often remained open for weeks, while new discrepancies continued to appear.

> "The number of tickets outstanding was steadily rising," Jon explained. "The resolutions were not keeping up with the creation of them."

Without reliable visibility, it became difficult to determine whether the problem was:

- A system built incorrectly
- A security agent failure
- Or a server that had been decommissioned improperly

Each group could point to a different root cause, and accountability remained unclear.

Progress stalled.

Why Brooks Turned to Axonius

Jon first encountered Axonius several years earlier. When a newly hired senior engineer, already familiar with the platform, recommended it again, the team decided to evaluate it through a proof of value.

The immediate goal was to reconcile several fundamental data points:

- Asset inventory
- Vulnerability management agents
- Endpoint detection agents
- Security tool coverage

If those numbers didn't align, the security team couldn't confidently say what systems were protected, or even what systems existed. Axonius provided a way to query systems in real time and compare multiple sources of data simultaneously. That capability quickly changed how Brooks approached the problem. Instead of investigating discrepancies one by one, the team could identify patterns.

They could distinguish between systems that had just been built, systems where agents had failed, and systems that had been decommissioned incorrectly.

> "With Axonius, we can query machines in real time," Jon said. "And we can tell the difference between a build problem, an agent failure, or a decommission process that wasn't followed."

This clarity allowed teams to address root causes instead of chasing symptoms.

"By surfacing these issues in near real time, we *reduced flawed system builds by 90%* in just a few months."

Jon Hocut – Director of Information Security

Turning Visibility Into Accountability

One of the biggest improvements came from making discrepancies visible immediately, and tying them directly to the teams responsible. Brooks integrated Axonius with JIRA, allowing the platform to automatically generate tickets when flaws were detected.

Jon jokingly refers to the system as a "**flaw finder**."

> But the impact is serious. "The manager of that department can quickly see which build caused the issue and talk directly to the person who built it," Jon explained. That level of transparency changed behavior across the organization.

For the first time, Brooks could measure how often systems were built incorrectly.

The team introduced a new metric:

- Number of builds per month vs. number of flawed builds.
- Within just a few months, the results were dramatic.

> "We've seen the number of flaws per build go down by 90%," Jon said.

What used to take months of ticket chasing now becomes an immediate correction.

Discovering What Was Really in the Environment

Another benefit of implementing Axonius was improving the accuracy of Brooks' asset inventory. The security team uncovered differences between the expected and actual number of servers.

> "We discovered about a 20% difference in our server inventory," Jon said. "And that's an area where I don't even want to be off by one."

The discovery also helped the team better distinguish between different system types, such as infrastructure appliances versus general-purpose servers. With more accurate asset classification, Brooks can prioritize security controls and risk management more effectively.

Supporting Global Operations and Privacy Compliance

Brooks operates globally, with employees and customers across multiple regions.

That footprint introduces an additional layer of security and compliance complexity.

Privacy regulations vary significantly across jurisdictions, from European privacy laws to Chinese regulations and U.S. state requirements such as California's privacy laws.

While Axonius is still relatively new in Brooks' environment, the platform is already helping the security team ensure systems comply with the company's own internal policies.

> "We use Axonius to help us stay compliant with our own policies," Jon explained.

Maintaining internal standards consistently across global systems is often the first step toward broader regulatory readiness.

"If you're *constantly trying to reconcile* your asset inventory with your vulnerability and endpoint agents, a tool like Axonius can help you get your arms around that problem."

Jon Hocut – Director of Information Security

A Foundation for Future Security Innovation

Although Brooks has only been using Axonius for several months, the platform has already become a core component of the organization's security operations. What began as an effort to reconcile asset counts has evolved into a system for identifying flaws, improving processes, and increasing accountability across teams.

> Jon sees significant potential to expand how Brooks uses the platform in the future. "Axonius has quickly become a foundational part of how we approach visibility and accountability, helping us bring clarity to a complex environment. " he said.

The team is exploring additional use cases that could further automate security operations and strengthen visibility across the environment. For organizations facing similar challenges, Jon's advice is straightforward.

> "If you're constantly trying to reconcile your asset inventory with your vulnerability agents and your endpoint agents, and you're always wondering why machines aren't checking in, a tool like Axonius can help you get your arms around that problem."

Security Leadership: Protecting the Business While Enabling Growth

For Jon, security is not just about protecting infrastructure. It's about helping Brooks continue to grow without unnecessary risk. His role, and his team's mission, is to quietly ensure the business can operate confidently.

When that happens successfully, most employees never notice.

And that's exactly the point.

Get Started

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

Request a demo

Speak with sales

Get started