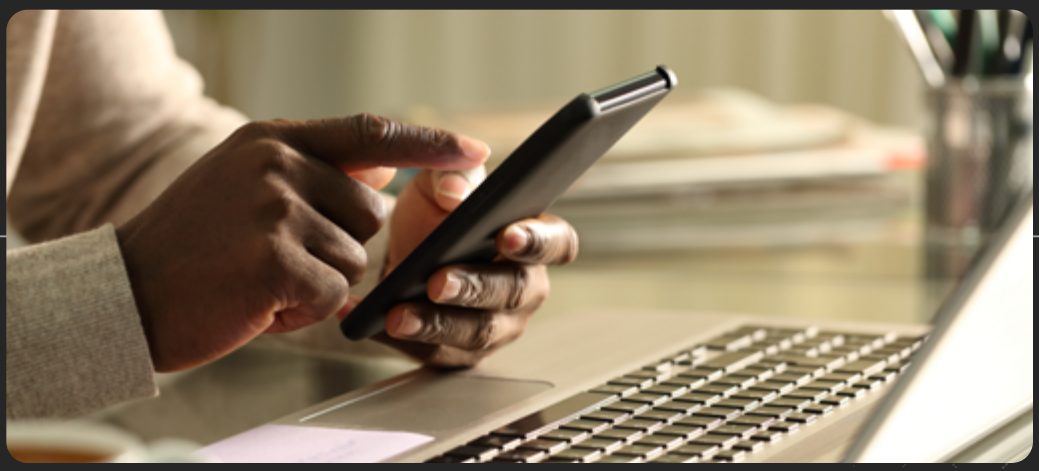
Lumen Technologies Builds Security "At Telecom Scale" with Axonius

From fragmented inventory to a living, risk-based view of 1.1M+ assets and faster action when zero-days hit



LUMEN®

Lumen Technologies is a global telecommunications and technology company operating critical infrastructure across a massive, distributed environment. When Geoff Krahn joined as Director of Product and Platform Security, his mandate was simple to say and hard to execute: help Lumen understand what it owns, what it's responsible for, and what's exposed, across dozens of systems, business units, and technology generations.

Axonius became a foundational layer in that journey, first to establish a trusted "known universe," and then to power faster response, risk-based remediation, and scalable reporting for executives, the board, and customers.

> "Lumen has been around in some form for nearly a century, and we *struggled to tell* what was ours versus our customers'."

Geoff Krahn – Director of Product and Platform Security

The Scale Problem No One Escapes in a 100+ Year Company

Telecom isn't just "large IT." It's infrastructure, uptime expectations, and a constant collision between legacy systems and modern cloud-native architectures. Lumen is also a company that has existed "in some form for nearly a century," which means the environment is deep, wide, and full of history.

Geoff didn't inherit a blank slate. He inherited complexity, spread across operational reality and organizational structure.

> "Lumen has been around in some form for nearly a century, and we struggled to tell what was ours versus our customers'." - Geoff Krahn
>
> "We were constantly in incident response calls with no idea who owned what." - Geoff Krahn

Geoff's team spans offensive security, vulnerability management, asset management, security engineering, and product security architecture. In many enterprises, those functions can become siloed by necessity. At Lumen, Geoff's emphasis was the opposite: build a system where each function reinforces the others.

> "Having a great team is the only way it is possible. My leaders of those functions are amazing and collaborate seamlessly." - Geoff Krahn
>
> "CyberSecurity Asset Management defines the scope for the downstream services, which in turn provide feedback... improving our systems. These feedback loops allow for continuous improvement and sustainability." - Geoff Krahn

But even with strong leadership and strong people, the foundational blocker remained: they couldn't confidently answer basic questions at enterprise scale.

The Breaking Point: When Security Can't Say "Out of Scope"

Many business units can define scope. **Security cannot.**

That's where the pain shows up in the most practical way, when leadership asks a "simple" question.

> "Security control coverage was a real struggle. Security is the only department that can't say out of scope. Answering simple CISO questions like what is the percentage of all servers have EDR was extremely difficult, creating trust issues with leadership." - Geoff Krahn

Lumen had **40+ independent inventory systems**, each with varying degrees of completeness and maturity. The result wasn't just operational friction. It was a structural risk: when incidents occur, the organization can't move fast if it can't route responsibility fast. They needed a way to bring disparate signals into one view, without pretending the environment was smaller or simpler than it is.

Why Axonius: Establish the "Known Universe" First

Geoff introduced Axonius initially to answer coverage questions, assurance, licensing requirements, and investment planning around controls.

But what Axonius unlocked wasn't just reporting. It was a credible baseline: a living inventory built from many sources, continuously compared and reconciled.

> "That has been the real magic. With the ability to ingest data from so many different sources, including all our security and infrastructure tools, and compare them to several different inventory systems, we have been able to paint a much better picture of known." - Geoff Krahn

In a complex organization, "knowing what you have" isn't a one-time project. It becomes an operating model. Once you can define what's real, you can start defining what's managed, and what's missing.

> "Now business units have a better picture of what is within their scope of responsibility, what has been deployed in a compliant manner, and what is secure vs insecure. Once things are known they can become managed, and managed systems are cared for and remain patched and secured." - Geoff Krahn

From 17,000 Assets to 500,000 – And Then the Real Number

The first major impact was sheer visibility growth. What started as a view of 17,000 assets quickly expanded beyond what the organization expected.

Within months, Lumen grew from 17,000 discovered assets to 500,000 devices identified and categorized. And as the program matured, Geoff's updated number is even more telling:

> "I think we are up to 1.1M devices now," - Geoff Krahn

This wasn't just "more inventory." It was an organizational wake-up call.

> "It has really been an eye-opener for the organization as a whole how large our responsibilities are. Being able to quantify it and highlight gaps in controls has allowed us to gain the leadership support and funding we need and take a risk-based approach on which areas we shore up first." - Geoff Krahn

Geoff notes the company is now spending **10x** what it was when he was hired, momentum tied directly to leadership seeing the real scope and the real gaps.

The Shift: Visibility Becomes an Action System

Asset visibility is foundational, but Geoff's objective wasn't to build a prettier spreadsheet. It was to build a mechanism for execution, where accurate scope drives downstream action, and downstream outcomes improve scope.

That's where Lumen's approach becomes more than "inventory modernization." It becomes a model for how large enterprises sustain security improvements over time.

Geoff describes moving toward a world where systems stay in sync, sources of truth are clarified, and automation reduces the friction of keeping everything aligned.

> "This has set the stage for Action Center to support the automation of now keeping these systems in sync with each other and defining sources of truth." - Geoff Krahn

The Application Posture Dashboard: Turning the CMDB into Security Context

One of the most meaningful outcomes of this program wasn't simply asset counts. It was the ability to assess **applications**, what they run on, how they're covered, and what risk looks like in context.

Lumen develops and runs thousands of internal applications. That means the security question isn't only "is the server patched?" It's also: what does this server support, who owns the application, and what risk does it represent?

The **Application Posture Dashboard** became a major win because it ties together relationships and security signals in a way architects and auditors can actually use.

> "The Application Posture Dashboard is a fantastic example of the partnership between our IT Asset Management, ServiceNow and DevOps teams. It allows Security Architects and Auditors to quickly evaluate the security posture of an application… leveraging the relationships from the CMDB that Axonius brings in and correlates control coverage, vulnerabilities, risk scoring, EOL and other key metrics." - Geoff Krahn

And Geoff's next step shows where this is going: connect application posture to business impact.

> "We plan to take it a step further and roll those applications up to the products Lumen provides its customers to track cybersecurity risk to revenue." - Geoff Krahn

That's the difference between "security metrics" and executive relevance, risk expressed in the language of products and revenue.

"This has set the stage for Action Center to support *the automation* of now keeping these systems in sync with each other and defining sources of truth."

Geoff Krahn – Director of Product and Platform Security

Zero-Day Response: Minutes Matter, and So Does Ownership

In modern vulnerability response, speed is constrained by two things: knowing exposure and routing action. Lumen uses Axonius to compress both.

When a new zero-day vulnerability emerges, Geoff's team can quickly determine affected systems, exposure status, and ownership, and then drive response workflows without delay.

> "Being able to get near instantaneous information on how many assets are susceptible to a 0 day vuln, who owns them, are they externally exposed, etc., is pivotal to timely response and communication." - Geoff Krahn

This is where "inventory" turns into incident readiness. It's not enough to know "how many boxes." You need to know which ones matter most and who is accountable. And Lumen is already pushing further, automating the communication loop and accelerating response through conversational interfaces.

> "We are using these foundational capabilities in Axonius to drive automated alert notification for leadership and engineers to effectively respond to 0 day threats. We're automating most of the zero-day response using a chatbot that sits on top of Axonius." - Geoff Krahn

Growing Beyond Inventory: Exposure Management as the Next Maturity Step

Once Lumen had confidence in "what exists," the next challenge was prioritization: not just scanning and producing noise, but reducing risk efficiently at scale.

That's where Exposure Management entered the picture, helping Lumen evolve vulnerability management from volume to value.

> "While knowing what you have is step 1 in NIST and any other security framework, being able to quantify and track how vulnerable what you have is critical. Exposure Management... will allow us to evolve vulnerability management beyond scan and spam to intelligent risk-based requests driven by remediation actions that will deliver the most risk reduction." - Geoff Krahn

This matters in telecom scale environments because the "scan everything and patch everything immediately" mindset collapses under its own weight. Risk-based action is the only sustainable model. Geoff also described Axonius as a true partner in this evolution, one that understands what enterprise scale really means.

> "Axonius has been the best partner for aggregated data. They understand what it means to handle complex, distributed systems at our scale." - Geoff Krahn

Extending the Value to Customers: Managed Services and Real-Time Trust

Lumen's story isn't only about internal security maturity. It's also about how visibility and reporting translate into customer outcomes, especially as Lumen brings managed service feeds into Axonius to strengthen transparency and compliance reporting.

> "Leveraging the capabilities of Axonius for asset discovery and the ability to report patching compliance has improved the fidelity and efficiencies of the managed services groups managing devices on behalf of our customers. Our customers have commented and benefited from improved reporting and dashboards that improve trust in service delivery and adherence to SLAs." - Geoff Krahn

That's a powerful shift: security visibility isn't just defense, it becomes a service differentiator.

When Visibility Rewrites the Executive Conversation

For Geoff, the most significant impact wasn't a single dashboard. It was the way trusted visibility changed leadership decisions. One example: end-of-life visibility and risk clarity contributed to a major infrastructure decision.

> "The visibility Axonius was able to shed on the End of Life issues we had with our systems directly contributed to the decision to migrate the majority of our infrastructure to the cloud, reducing overall risk by 40%." - Geoff Krahn

That's what "security as an enabler" looks like in practice: visibility creates executive confidence, which unlocks modernization at the scale required to reduce risk materially.

Geoff also notes Axonius became part of how Lumen communicates to the board, turning security from opinions into measurable operational truth.

> "The board now relies on Axonius-generated reports for asset coverage, EDR status, and compliance insights. We were immature in our security journey. Axonius gave us a way to mature, it's part of how we evolve." - Geoff Krahn

Key outcomes include:

- Growth from 17,000 to 500,000 discovered assets, and now ~1.1M devices in scope
- Faster, more confident zero-day response, with automated alerting and chatbot-driven workflows
- Stronger application posture visibility, connecting CMDB relationships to control coverage, vulnerabilities, EOL, and risk scoring
- More mature, risk-based vulnerability operations, moving beyond "scan and spam"
- Improved executive and board reporting, and a cloud migration decision tied to EOL visibility that reduced risk by 40%
- Expanded value into managed services, improving customer transparency, reporting trust, and SLA adherence
- Increased organizational investment (now 10x compared to when Geoff was hired), enabled by quantifiable scope and control gaps

Geoff's Advice to Other Large Enterprises

For organizations staring at the same problem, many tools, many inventories, and no unified truth, Geoff's guidance is direct: treat it as a journey, start with a definable slice, and keep raising fidelity.

> "Start small, continually define the problem and acceptable fidelity levels, constantly communicate this is a long, challenging but extremely worthwhile journey...and before you know it you will go from 17,000 to 1.1M assets." - Geoff Krahn

"Axonius has been the best partner for *aggregated data*. They understand what it means to handle complex, distributed systems at our scale."

Geoff Krahn – Director of Product and Platform Security

Get Started

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

Request a demo

Speak with sales

Get started