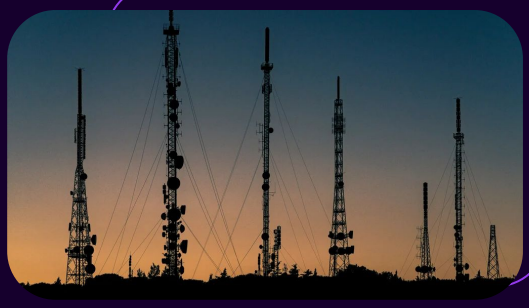
veza | Customer Journey ATN International

ATN International enables people around the world to connect to data

A telecommunications company unlocks the value of data while keeping it secure with Veza



Industry
Telecommunications

Organization Size
2,500 Employees

Headquarters
Beverly, MA

Veza features
Query Builder
Workflows
Insights
Tags

Challenges
Lack of standardized access policies

Time intensive and error prone access certification process

Benefits
Single pane of glass for enterprise data authorization

Enhanced compliance posture

Key Integrations

Okta
Snowflake
Azure
AWS

As a global telecommunications holding company, ATN International focuses on providing underserved communities in rural America, the Caribbean, Australia and many other locations with access to internet, broadband, television, and mobile services. Data analytics plays a key role in this mission.

> **Data is critical at ATN. What's key isn't just the information we bring from our network, customers, and business operations, but also information about the communities and markets in the areas we serve, and how it all blends together. That helps us understand what our customers really want, what's important to them, and how we can deliver that value.**
>
> Kevin Fournier • Vice President of Data Analytics and Integration, ATN International

In recent years, an ongoing digital transformation has brought new requirements for securing users and data, along with a Snowflake data warehouse reshaping its data ecosystem. With data living everywhere, the company needed to be able to enforce strict governance and control across its complex data ecosystem. "Cybersecurity has been a huge focus for us," says Ben Doyle, CIO of ATN international.

> **We've been deploying innovative security solutions like Okta for IAM and multifactor authentication, Zscaler to support zero trust, and ServiceNow to manage and organize our security operations. What's been missing through that journey is a focus on data security.**
>
> Ben Doyle • CIO, ATN International

Rapid growth brings challenges around data access and compliance across systems

As a holdings company, much of ATN's growth comes through M&A. To support its data-driven business strategy, ATN needs to be able to blend the content from acquired telecommunications companies into a common data environment, including subscriber, account, network, billing, and marketing information.

This includes reconciling a diverse mix of data access policies developed organically over the course of decades to meet the specific needs of various distributed markets. "Our data access model has grown organically over twenty-plus years," says Fournier. "One of our biggest challenges is trying to modernize that into a modern, scalable architecture that lives in the cloud." To reduce the risk of privilege abuse and data breaches for sensitive customer and business information, ATN needs to maintain strict governance over data policies and permissions wherever data resides.

> Some of our key initiatives around cybersecurity over the last year have been around zero trust for data privacy. As we provide a single platform across our different operating companies and markets, it's critical to know that our sensitive customer and business information is secure, just not internally across those different markets, but also externally for the customer-facing applications we support.

Kevin Fournier • Vice President of Data Analytics and Integration, ATN

Beyond the cybersecurity implications of data access, ATN also needed to ensure compliance with numerous domestic and international regulations from the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), to Bermuda's Personal Information Protection Act (PIPA) and the Cayman Islands Data Protection Law, to rules governing Customer Proprietary Network Information (CPNI) for telecommunications companies. These mandates include requirements for companies to understand and prove who has access to sensitive data, and to enforce the principle of least privileged access.

As ATN migrated on-prem data to the cloud, the complexity of its security model and policies grew significantly. "It's not just admins with local access or direct access to reporting technology anymore; you're now opening up to developers and engineers and front-end applications, as well as casual users like myself and other managers. So you have a whole other security infrastructure that needs to go on top of that," explains Fournier.

> And you need a single pane of glass to be able to monitor and support and control it all. You need a way to understand: who has delete access? Who has write access? Who has global admin privileges? Do they all really need it? If we have sixteen different Snowflake admins, something's wrong.

Kevin Fournier • Vice President of Data Analytics and Integration, ATN

Veza helps ATN gain centralized visibility into identity and access across the data ecosystem

To build data security, governance, privacy, and compliance into its complex ecosystem, ATN needed a data security platform that could link user identities, roles, and groups in Active Directory and Okta to the data stored in its Snowflake data warehouse and elsewhere across AWS, Azure, and on-prem resources.

As the industry's first cloud data security platform rooted in authorization, Veza offered a way for ATN to confidently answer questions about who can and should take what action on what data. The Veza platform provides a single control plane to understand and control enterprise-wide authorization for any enterprise identity to any enterprise resource, including data systems, applications, and cloud services. "Veza gives us a single view of our data environment and how it connects to Okta, our identity provider," says Doyle. In addition to Okta, ATN has integrated Veza with Azure and Snowflake and AWS in the cloud. "Having an integrated view also means that we can see the whole security schema at once, helping us understand where there are gaps," says Fournier. "If a user suddenly doesn't have access to Tableau, we can see why without having to spend all day tracking it down."

As part of its risk management and regulatory compliance strategy, ATN performs regular access reviews, typically a complex and time-consuming process. "Before Veza, we had no way to connect identity and data," says Doyle.

> **Veza reporting and analytics tools make it simple for us to visually walk through our identity and data environments and identify employee access down to individual tables. This saves us an enormous amount of time, and it helps us achieve the strongest compliance posture possible. From a cybersecurity standpoint, that's very important to our business.**

Ben Doyle • CIO of ATN

ATN has also taken advantage of Veza's extensive Authorization Graph to make information about data access more easily consumable by a broader range of personas. "Our compliance team has access, our IT security team has access, our internal audit team has access," says Doyle. "It's allowed us to democratize and make transparent our data environment in ways that were never possible before."

Looking ahead

With a centralized data security platform across its entire hybrid cloud environment, ATN will now be able to extend visibility to cloud identity and data systems like Okta and Snowflake, Cloud IAM (AWS IAM), and its thousands of on-prem SQL databases, helping it support governance, privacy, and zero trust consistently wherever data resides. This capability will be critical to ensure that M&A activity doesn't bring unintended consequences such as cross-company access to customer PII, which can jeopardize regulatory compliance and certification. Moving forward, ATN will use Veza as part of its due diligence process for new acquisitions to understand their data environment and mitigate any potential risks they may present.

> So much of security is about access to applications and databases and servers, but data security is critically important. Most hackers aren't really after your application—they're after the data in that application. Having an ability to tie identity to data access and data security is really a game changer for us.

Ben Doyle • CIO, ATN

Interested in learning more about how to utilize Veza for the data security needs of your organization? Visit us at www.veza.com/platform.

About Veza

Veza is the data security platform powered by authorization. Our platform is purpose-built for multi-cloud environments to help you use and share your data more safely. Veza makes it easy to dynamically visualize, understand and control who can and should take what action on what data. We organize authorization metadata across identity providers, data systems, cloud service providers, and applications — all to address the toughest data security challenges of the modern era. Founded in 2020, the company is remote-first and funded by top-tier venture capital firms including Accel Partners, Google Ventures, Norwest Venture Partners, and True Ventures. To learn more, please visit us at veza.com.