veza | Customer Journey incomm

InComm extends a culture of data governance and compliance to the cloud

A global FinTech leader supports collaboration while maintaining strict data security

Industry
FinTech

Organization Size
6,000 Employees

Headquarters
Atlanta, GA; operating in 30+ countries

Veza features
Authorization Graph
Query Builder
Insights
Rules & Alerts

Challenges
Lack of visibility into how access to SharePoint data was being granted

Managing appropriate access for number of external users

Benefits
New tool available to document the data exposure blast radius

Replace excessive permissions in SharePoint Online

Key Integrations

AWS
Azure AD
SharePoint

A FinTech industry leader for a quarter-century, InComm Payments manages prepaid card transactions for more than 1,000 brand partners around the world, including retailers, gift card issuers, toll and transit agencies, and other customers across in-store, online, and mobile channels.

> **We're the premier provider in prepaid and payment solutions and technologies. "We're the company behind the scenes connecting merchants with customers for this kind of transaction."**
>
> Steven Guy • Vice President of Security Solutions at InComm

Given the highly regulated nature of InComm's core business, the company has built a culture of compliance throughout its organization—not just for sensitive data falling under specific mandates and standards, but for all of the information in its environment.

As InComm began its journey to the cloud, it needed a way to maintain full visibility and insight into identity, access, and permissions across its evolving hybrid environment. This proved especially challenging given the complexity of the SharePoint permissions model, which encompasses multiple levels of default and customizable permissions, the ability of individual users to share data within each other, and the inheritance of each site's permissions to all of the pages, lists, and document libraries within it. "As we moved our SharePoint content from on-prem file shares up to SharePoint Online, a lot of those legacy controls went with it," says Guy. "We didn't have a good solution to identify how access was being allotted to who, for what SharePoint data, both on-prem and in the cloud."

Cloud migration calls for a new level of data access visibility and insight

To support its business, InComm needs to be able to deliver trusted data to the right users at the right time to harness its full value. Its business personnel need to share corporate data in a collaborative environment, while the organization needs to have confidence that the proper controls are in place to keep it secure. From a zero trust perspective, this means enforcing least privileged access and maintaining complete visibility into authorization across all data. In order to meet these requirements for the data moving to SharePoint Online—and the subsequent phases of its cloud migration—InComm needed to formalize the access management strategy across its hybrid environment.

While identity governance administration (IGA) tools offered a way to manage identities, groups, roles, and entitlements at the application or infrastructure level, they couldn't provide an accurate view of data permissions.

> We needed to understand how users and service accounts have been given access to specific data, and what level of access and authorization they've been given. Are they going through security groups? Are they coming through roles? To align to our identity and access management (IAM) standards, we needed to enforce role-based access controls to this data instead of potentially having it granted individually to each SharePoint Online drive or site.

Steven Guy • Vice President of Security Solutions at InComm

Veza connects the dots between identity and data

To formalize data governance for its evolving hybrid environment, InComm had to make sure proper controls were in place to manage different access levels for each data system in their environment, with a focus on SharePoint. This required a way to link authorization information from Azure AD with permissions structures across SharePoint and other data repositories. Veza brought this information together within a single control plane to identify the effective permissions resulting from the combined effect of all groups, roles, authorization policies, privileges, and local users that connect to data repositories. Now, InComm can understand and control enterprise-wide authorization for any identity into any data system, simplifying the management of audits, privileged access, and entitlement reviews.

> Veza is the only tool I've seen that can show you both parts of the picture. One part is the people or accounts who are supposed to have access as part of a security group. And then there's the flip side where you look at it from the data end and say, this is who also has access, and this is how that access was granted. It's the clearest view I've ever seen.

Steven Guy • Vice President of Security Solutions at InComm

InComm Payments' implementation of Veza has helped the company streamline and enhance its adoption of SharePoint and AWS. Veza worked closely with InComm Payments to deploy the solution, taking a collaborative engineering approach to ensure that the solution met the company's needs. "It's definitely been one of the best partnerships I've ever experienced," says Guy. "I've worked with a lot of vendors and been on customer advisory boards, and it's rare to give feedback and see it actually implemented so quickly. That's been very refreshing."

By integrating SharePoint into Veza, InComm has gained complete visibility into all the user and service accounts that can access sensitive SharePoint Online drives and sites. Veza's Authorization Graph allows the company to map Identity-to data relationships from Azure AD into SharePoint. With this information, the company can formalize stringent security controls in alignment with zero trust principles. "Understanding how data is being accessed is a critical part of applying the principle of least privileged access," says Guy. "It enables a role mapping process where we replace unique, individually allocated levels of access by putting people and service accounts into roles."

InComm Payments can also more easily identify over-privileged accounts resulting from the collaborative nature of its business.

> **Veza has enabled us to look for guest users who have been assigned excessive permissions for SharePoint libraries, lockdown access to sensitive information, and reduce the attack surface that can expose us to data leaks.**

Steven Guy • Vice President of Security Solutions at InComm

As Incomm Payments deployed Veza, its security operations team identified how the tool could be super helpful during an incident response by providing a fast and clear way to understand the blast radius of a potential user compromise; guiding containment and remediation actions. “We can quickly pivot into an identity-centric search and say: this person has access to this sensitive data. What else does he have access to? If the credentials were stolen, what could the attacker do with them? In just a few clicks, we can see all the applications, AWS resources, and data he can also access via single sign-on (SSO),” says Guy.

Looking ahead

“We look at Veza as a very long-term partnership,” says Guy. “We’ll be extending the solution to on-prem SQL and on-prem AD, and start getting better access modeling across cloud and on-prem applications. We’ll also integrate with additional cloud repositories to minimize the risk of exposure. We’ll just keep expanding our scope with Veza’s API feature sets, working toward a single pane of glass for total access visibility across not just one application or one side or one cloud location, but everything.”

If you’re interested in learning more about how Veza can work alongside many more enterprise data stores, see our integrations page at https://www.veza.com/platform/integrations.

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 multi-cloud 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.