FinTech leader balances enforcing strict data governance and compliance while supporting collaboration for over 1,000 brand partners

Industry
FinTech

Size
6,000

Headquarters
Atlanta, GA

Key Integrations

AWS

SharePoint

Key Features

Access Graph

Rules & Alerts

Insights

Query Builder

Benefits

✅ New tool available to document the data exposure blast radius

✅ Replace excessive permissions in SharePoint Online

Challenges

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

⚠ Managing appropriate access for number of external users

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 • **VP, Security Solutions**

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.

> *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 • VP, Security Solutions

Veza connects the dots between identity and data

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."

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.

About InComm Payments

InComm Payments is a global leader in innovative payments technology. Leveraging dynamic technology and proven expertise, InComm Payments delivers enhanced end-to-end payment platforms and emerging financial technology solutions that help businesses grow across a wide range of industries including retail, healthcare, tolling & transit, incentives, mobile payments and financial services. By enabling omnichannel connections to an ever-expanding consumer base in an increasingly digital ecosystem, InComm Payments creates seamless and valuable commerce experiences across the globe. With more than 29 years of experience, over 500,000 points of distribution, 402 global patents and a presence in more than 30 countries, InComm Payments leads the payments industry from its headquarters in Atlanta, Ga. Learn more at www.InCommPayments.com.

About Veza

Veza is the identity security company. Identity and security teams use Veza to secure identity access across SaaS apps, on-prem apps, data systems, and cloud infrastructure. Veza solves the blind spots of traditional identity tools with its unique ability to ingest and organize permissions metadata in the Veza Access Graph. Global enterprises like Wynn Resorts, and Expedia trust Veza to visualize access permissions, monitor permissions activity, automate access reviews, and remediate privilege violations. Founded in 2020, Veza is headquartered in Los Gatos, California, and is funded by Accel, Bain Capital, Ballistic Ventures, GV, Norwest Venture Partners, and True Ventures. Visit us at veza.com and follow us on LinkedIn, Twitter, and YouTube.