

# Leveraging Elevated Observability of Access Permissions to Quickly Identify Policy Violations



PayNearMe Protects Sensitive Financial Data and Streamlines Access Reviews with Veza

## Industry

Financial Services

## Headquarters

Santa Clara, CA

## Veza features

Authorization Graph

Rules and Alerts

Insights

User Access Reviews

Privileged Access Reviews

Cloud Entitlement Reviews

## Challenges

Keeping track of evolving data access permissions and IAM policies in AWS

Time consuming, manual and error-prone reviews in prep for compliance audits

## Benefits

Faster and accurate data security reviews

Understand and manage authorization to critical data stores within AWS

## Key Integrations



Okta



AWS

PayNearMe develops technology that drives better payment experiences for businesses and their customers. The company processes billions of dollars annually through a variety of payment types and channels, including credit and debit cards, ACH, cash, online portals, and mobile wallets. At its launch, the company processed payments through servers housed in co-located server farms. In 2009, as the cloud became more reliable, secure, and widely adopted, it migrated to AWS. “We’ve been working on a cloud-native approach since then, and Veza has really helped us take advantage of cloud architecture in a safe manner,” says Sean Todd, PayNearMe’s CISO.

PayNearMe strives to use the most secure and reliable technologies to tackle the biggest challenges in payments, one of which is securing the massive amounts of sensitive data it processes for bill-payers and the recipients of their payments. “Data is critical to our business,” says Todd. “We take the trust that merchants put in us very seriously when they give us their data, so security is a top priority.”

## Stringent security and compliance requirements

As the company’s client base grows, the volume of data that it handles has skyrocketed, as have the threats arising on the internet. “We’re seeing a lot more attacks from nation states, and lots of individual actors trying to get at our data, because it’s potentially of great value,” says Ziggy Brode, the company’s data security engineer. A key part of Brode’s job is formalizing governance policies based on data asset inventories, including a detailed accounting of who has access to which assets and under what conditions.

As a regulated money transmitter and PCI DSS (Payment Card Industry Data Security Standard) certified company, PayNearMe needs to follow strict regulations and ISO 27001 standards regarding the segregation and protection of resources. In addition, some of their larger clients impose proprietary security requirements. All of which requires lots of audits and access reviews.



As a payments company we need to audit our data asset inventories and access activities, both quarterly and annually. Veza lets us do it in a very timely and accurate manner.

Ziggy Brode · Data Security Engineer

## Elevating observability

PayNearMe's first objective was to get a handle on data security within AWS and streamline the access review processes. The key to controlling and protecting sensitive data is to have observability over data resources and access to them, including their associated permissions, all of which was lacking prior to PayNearMe's engagement with Veza. The dynamic nature of cloud architecture made identity and access management (IAM) more complex as the company's data resources continued to grow. Keeping track of changing data access permissions via Amazon Simple Query Service (SQS) became increasingly difficult as project assignments shifted from one team to another, month to month.

The painstaking process was time-consuming, expensive, and error prone. "We couldn't keep up with review cycles, couldn't be sure who should have access to what resources at any given time. Veza allows us to do a review in real time, so if access to critical resources changes, we're able to respond much faster than before," says Todd.

**Accumulating all the data we needed to comply with our audits was a real pain. Using Veza we can collate everything in a short amount of time, at a fraction of the price.**

Ziggy Brode · Data Security Engineer

## Key integrations

“We used to have just one cloud account, now we have dozens, constantly growing as we scale. Veza has been the key to integrating everything,” says Brode. The company uses Veza to analyze access to its Amazon Simple Storage Service (S3) buckets as well as other critical data stores, including Amazon Key Management Service (KMS) and Amazon DynamoDB. “At any point in time, we know who has access to those data sources and what kind of actions they can take on those resources. We’ve set up email notifications and integrated Slack to get real-time alerting should any permissions change and become insecure.”

## Policy violation insights mean faster, more accurate security reviews and audits

PayNearMe is using Veza to verify and enforce the principle of least privilege access within its AWS infrastructure. Instead of having to look at each IAM setting to understand specific permissions, Veza’s resource-centric reviews enable the company to globally monitor who has authorized access to critical data sources and how they can interact with them, all through a single pane of glass. “Veza’s connected graph visualization gives us a clear view of how a user might be accessing a resource. We can pinpoint and fix problems to remove any instances of inappropriate permissions,” observes Todd.

Veza continuously scans identity-to-data relationships querying for any deviations from corporate policies and their associated entities, which, if detected, are flagged and highlighted in Veza’s authorization graph and violations panel. These policy violation assessments allow PayNearMe to see where excessive privileges and permissions have been granted.

Brode notes that his team can now conduct data security reviews and audits quickly, more accurately, and with less need for human intervention. That’s because Veza provides pre-configured assessment templates that address entitlements, privileged access, misconfigurations, and other areas that might impact data security. By enabling his team to certify that the necessary controls are in place for their data stores, using Veza has led to a vast improvement in PayNearMe’s compliance efforts. “Data access reviews that used to take upwards of a week can now be done within minutes, which means we can do them much more frequently.”

## What's next?

“Veza helped us roll out the implementation, which only took just a day or so. Since then they’ve worked closely with us to ensure that our use cases are taken into account,” says Todd. Next up, the company is looking forward to using Veza as it expands its dynamic AWS infrastructure. Plans include adding a container-based architecture that will vastly increase the number of resources in its infrastructure. In the next phase, Brode and Todd are also looking to integrate Veza into the internal processes of its entire federated IAM environment to ensure that the insights Veza delivers are acted upon in order to keep the company always in compliance. “I sleep better knowing there’s an automated tool watching our systems. If one of our engineers makes a change in the middle of the night, I know I’ll have an alert waiting for me in the morning,” said Todd.

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