veza | Customer Journey CHOICE HOTELS

Leveraging the Power of Authorization for Data Governance & Compliance

Choice Hotels Taps Veza for Securing Data in Its Evolving Multi-Cloud Environment

Industry
Hospitality

Organization Size
2,000 Employees

Headquarters
Rockville, MD

Veza features
Authorization Graph
Search
Insights
Violations
Workflows

Challenges
Modern cloud architecture using legacy access control model

Benefits
More optimal and secure fine grained controls in AWS IAM

Quick detection of changes that support compliance efforts and enhances audit readiness

Key Integrations

Okta

AWS

Custom Apps

Choice Hotels International is one of the largest hotel franchisors, currently operating more than 7,000 establishments worldwide, ranging from upscale hotels to extended-stay lodges. With 570,000 rooms in some 40 countries, the company collects massive amounts of data of both customers and franchisees, which it relies on to ensure smooth business operations and "get heads into beds."

Data is essential for tracking reservations and ensuring that guests end up in the right room at the right time. And the secure flow of data through payment systems, whether for guests or franchisees, is mission critical. "Data is our lifeblood. It's the key to understanding the marketplace and our customers," says Steven Cihak, Senior Director, Cloud Platform & Site Reliability.

With so much data and so many financial transactions traversing the globe, cybersecurity is a high priority. The company handles lots of personal information (PII) and payment data (PCI) that needs to be managed and protected, and there are data privacy rules like the General Data Protection Regulation (GDPR) that it needs to comply with for its European properties. And as a publicly traded company, Sarbanes–Oxley (SOX) compliance is another concern. "Ransomware is also a high priority, because if a hacker manages to get into an admin's account with elevated permissions and encrypt our reservation data, our business is dead in the water," notes Jason Simpson, VP of Engineering. Managing and securing vast data resources and complying with financial regulations and corporate governance mandates is a major challenge — one that grew exponentially as Choice Hotels moved its operations to the cloud.

Building a multi-cloud enterprise from the ground up

The company's journey to the cloud began in 2016, first by migrating to AWS to rebuild its central reservation system in a microservice architecture. "We were among the first to rebuild legacy systems from the 80's and 90's in a cloud-native way," says Cihak. Ever since, they've gone all in on cloud and now use services and tools from different providers.

However, their access controls are still those used in the legacy system. “We've got an old system using very modern technologies and permission sets. It’s a real challenge, so now we’re focusing on simplifying it and evolving into next-generation permissions.” That’s where Veza has been a big help.

> Veza’s permission graph lets us deeply understand the link between Okta and all our different AWS accounts, databases. We’d never seen anything like that, and being able to visualize it in 30 seconds is truly amazing.
>
> Jason Simpson • VP, Engineering

Getting the right data to the right people and the right applications

Identity and access management (IAM) in AWS can be a daunting task. Managing policies, users, and groups is very time-intensive, especially for a company with three distinct user groups — employees, franchisees, and guests. The company approached Veza to help expedite those activities and make it easier for engineers to track violations and changes. “We needed to lock down the various identities and permissions to ensure that only the right people got into the data and apps meant for them,” says Simpson.

The adoption of Okta helped integrate applications to a centralized user directory, authenticate users, and leverage existing groups and roles. But they still had problems authorizing access to resources while reusing legacy permission models without modifying them for the cloud. Managing fine-grained access controls became quite complex. There was a lot of cleanup to do regarding specific permissions to the ever-growing number of data stores in the cloud. The company had to create new roles and policies as cloud migration progressed and they moved into a microservice architecture. “User and entitlement management now extends across multiple systems. Because we’re so spread out, it was tricky to manage and hard to know who had access to what. Veza lets us understand it in a simple way. The first time we plugged Veza in, we knew we really needed it,” says Cihak.

Focusing on least privilege

Choice's InfoSec team uses Veza for data governance. "With Veza we can see all of our resources in a single pane of glass — who has access to them and whether or not they should," says Christopher Harris, cloud Platform Engineering Manager. Veza's inline deployment model only requires read-only permissions and doesn't call for any architectural modifications, so it didn't take long to integrate Veza and connect to Okta, AD, and AWS. According to Harris, the team was able to identify permission and privilege violations right out of the gate, noting that, within hours, they were writing tickets to clean up problems. "Veza has helped us standardize our access permissions and focus on least privilege."

> In two days we saw the extent to which we had permission sets that were not actually allocated to any role or user — permissions we could eliminate to clean up our system and make it easier to manage long term. It was fantastic.

Steven Cihak · Senior Director, Cloud Platform & Site Reliability

Key integrations

Choice's Veza implementation focuses on its cloud platform, its identity products, and its various cloud databases. Key integrations include Okta, AWS, and custom applications. The company gets deep visibility into the policies and permissions for accessing their Amazon Redshift databases and has gained a better idea of how to manage them in the future. "Veza shows us all of the permission sets we have and all the users and groups they're associated with. We can actually see who has access to which systems, all the way down to the table layer inside databases," says Cihak.

Veza: A critical tool for data governance and compliance

Upon implementing Veza's cloud-based data security platform, security teams were able to quickly identify challenges in Choice's environment. They found orphaned users and groups and policies that weren't attached to any entities. In short, lots of things to clean up. When policy violations are discovered, Veza helps accelerate remediation by automatically sending alerts to ServiceNow, thus giving Choice's security teams a heads-up regarding what needs to be fixed.

Veza gives Choice the power to report on any changes in their environment, streamlining their auditing and compliance efforts. “If you’re in the cloud, there’s probably plenty of things you’ve done that need to be fixed. Being able to put governance on top and keep things from sprawling out of control is something we love about Veza,” says Simpson.

> This is one of the most exciting tools I’ve ever seen, and I’ve been at it for 30 years. Out of the box, Veza has given us the ability to identify and fix aspects of our InfoSec environment that we didn’t have before.

Chris Harris • Platform Engineering Manager

What’s next?

“Our partnership with Veza has been fantastic. We’re very confident that not only are we going to get a lot out of the product, but we’re also going to help Veza set the direction for integrations they can add to make it easier to secure our cloud,” says Simpson. As for Choice Hotels, they’re looking to extend Veza to more teams and get to additional applications and eventually go deep into every database they have. The company is looking forward to leveraging the infrastructure permissions that Veza is now setting up around AWS security groups, which will give Choice even greater control over data security. “This is one of the most exciting tools I’ve ever seen, and I’ve been at it for 30 years. Out of the box, Veza has given us the ability to identify and fix aspects of our InfoSec environment that we didn’t have before,” concluded Harris.

Learn more about how Veza brings data security to your cybersecurity initiatives at www.veza.com

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.