

Safeguarding 100 years of entertainment content with Veza

Industry

Multimedia & Entertainment

Size

3,500

Headquarters

Burbank, CA

Key Integrations

 Entra ID (Azure)



 AWS

 GitHub




 Jira

 Slack



Benefits

-  Centralized management of access permissions for hundreds of team members without slowing down development teams
-  Reduce costs by identifying underutilized software licenses

Challenges

-  Manual processes for understanding enterprise access
-  Multiple teams managing data in multiple systems
-  Finding a solution that does not slow down development teams or impact cloud workloads

Goals

-  Unified visibility of access permissions to data for all teams (security, engineering, IT teams)
-  Manage authorization policies without slowing down development processes and cloud workloads

A leading services company for over a century, Deluxe Media Inc. (Deluxe) provides localization, cinema, and distribution services to a global customer base of content creators, broadcasters, streaming platforms, and distributors. Customers rely on Deluxe’s experience and expertise to create, transform, localize, and distribute content. In return, they count on Deluxe to keep their content and data safe at all times.

“Our customer-first culture means that it’s every team’s responsibility to safeguard and protect our customer data.” says Sean Moore, Executive Vice President of Engineering at Deluxe.

Moore’s team focuses on delivering resilient and scalable software that enables Deluxe’s clients to succeed in the modern era of global entertainment and consumer engagement. “We take a proactive approach to ensure that we have robust authentication and access controls in place to keep our customer’s data secure,” says Moore.

Protecting data in a cloud environment calls for unified visibility

In the past, the data silos and disparate systems across Deluxe’s modern cloud environment made access control a cumbersome and inefficient task. To understand identity-to-data relationships across its cloud systems separate teams had to pull data and correlate reports for each application, making it time-consuming to achieve a unified and consistent visualization of who can take what action on what data.

“Our customers’ data and trust has always been paramount, and we wanted a solution for what is often a manual disjointed process,” says Moore.

That meant finding a centralized solution for security, engineering, and IT teams to validate authorization policies of data. At the same time, the company needed to be sure the new tool would not introduce new risks or impede business processes. ”

““ *We wanted control and visibility into our data security without impacting our processes and cloud workloads.*

Sean Moore • Executive Vice President of Engineering

Veza’s authorization platform for visibility and control over identity-to-data relationships

As Deluxe considered its options, Moore was drawn to Veza’s Authorization Platform because of the discoverability, visibility, and collaboration it enabled across the company’s teams.

A proof-of-concept made Veza’s benefits clear, including comprehensive visibility of access for all enterprise identities and data sources as well as the ability to query identities and privileged actions on any resource. Active, rule-based alerting and monitoring of authorization changes in the environment enable quick detection of changes and supports the company’s compliance efforts. “There wasn’t a lot of convincing needed once we started using the authorization platform,” Moore recalls.

“Veza gives my team and I complete visibility and control of our data so we can validate authorization policies based on least privilege standards and optimize fine-grained IAM controls in AWS.”

With support from the Veza team, Deluxe completed its deployment in a matter of weeks, including connecting to AWS, Github, and Azure AD.

““ *We are able to get insights into least privilege, cloud entitlements, and cloud misconfigurations by understanding the scope of authorization on data for any account.*

Jeff Cuneo • Head of Platform Engineering



This includes translating highly complex, system-specific authorization structures such as rows, groups, policies, and permissions into a common language of effective permissions.

“That makes it very simple for our teams to determine any misconfiguration or inappropriate access. For example, we are able to identify everyone in GitHub that has access to specific code repositories, and understand AWS user access down to the bucket level.”

Saved time and money with a single source of truth for enterprise-wide authorization

With less manual efforts to reduce risk to sensitive data, Deluxe has been able to scale its efforts to protect access to data across their entire cloud environment and secure engineering assets that are accessed by global teams.

Instead of having to pull data and correlate separate reports for each application, Deluxe’s security, engineering, and IT teams can now collaborate more easily with a single source of truth.

Deluxe uses Veza’s outbound integrations such as Slack and Jira to operationalize insights into well-defined business processes and workflows. “The Jira integration alerts our security teams so they can begin triaging the issue quickly. By using our existing enterprise apps, it makes providing evidence for audits at any point very easy,” says Cuneo.

The visibility and insights provided by Veza have also helped Deluxe identify licenses that weren’t being consumed by users or weren’t needed by teams. By retiring these licenses, the company has saved money while streamlining its IT portfolio to run its business more efficiently. “We can run our business more efficiently and ease strain and frustration by making it really easy to know who can and should take what action, on what data,” says Cuneo.

“Veza gives us a more effective way to determine who is allowed to access specific data, and under what circumstances,” Moore says. “It really brought the teams together and made us more efficient in our processes.”



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](#).