TAG

PLANNING THE MIGRATION OF ENTERPRISE IDENTITY GOVERNANCE TO THE VEZA PLATFORM

DR. EDWARD AMOROSO,
FOUNDER & CEO, TAG INFOSPHERE

MIKE TOWERS,
CHIEF SECURITY AND TRUST OFFICER, VEZA

veza®

PLANNING THE MIGRATION OF ENTERPRISE IDENTITY GOVERNANCE TO THE VEZA PLATFORM

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG INFOSPHERE[1]
MIKE TOWERS, CHIEF SECURITY AND TRUST OFFICER, VEZA[2]

ThisTAG Infosphere report explains how enterprise security teams can design and implement a plan to migrate from their existing identity ecosystem to an improved approach using Veza. A three-phase management model is introduced that can guide enterprise security management and practitioner teams toward a successful identity security deployment.

INTRODUCTION: WHAT IS THE STATE OF ENTERPRISE IDENTITY SECURITY TODAY?

Every modern enterprise information technology (IT) practitioner or manager understands the central role that identities play in organizing how data, resources, and systems can be accessed by humans and non-humans. This central role for identities stems from the dissolution of traditional perimeter networks, but it also emerges from the sprawling hybrid network complexity that has occurred for most organizations, usually guided by zero-trust design.

On the surface, the obligation to secure identities might seem simple – namely, that security policies should be put in place to govern who can access which types of data under what sets of circumstances. Identity and access management (IAM) vendors should be engaged to implement these policies, and enterprise teams should simply curate such operation to minimize costs through proper automation of IAM tasks and good business process design. In reality, however, the complexity associated

[1] *TAG Infosphere provides research and advisory in cybersecurity, artificial intelligence, and climate science/sustainability for enterprise teams, government agencies, public policy lawmakers, academic researchers, and commercial vendors. See* ***https://www.tag-infosphere.com****.*

[2] *Veza is the Identity Security company, helping organizations secure access across the enterprise. Veza's Access Platform goes beyond identity governance and administration (IGA) tools to visualize, monitor, and control entitlements so that organizations can stay compliant, achieve least privilege, and de-risk the breach. Founded in 2020, Veza is headquartered in California, and is funded by Accel, Bain Capital, Ballistic Ventures, Google Ventures (GV), Norwest Venture Partners, and True Ventures. See* ***https://www.veza.com****.*

with identity security has been almost unprecedented in cybersecurity, with identity governance and administration (IGA), and other tasks becoming too complex for manual support, but also complicated enough to make even proper automation tough. The result is that nearly every enterprise team today, especially in larger organizations, is struggling with their identity security approach.

In this report, we assume that the reader resonates with our claim that significant challenges exist in how their own enterprise manages access permissions, privileges, and other identity constructs for both human and non-human access – and that they have committed to select and migrate to a new identity security system. Our focus here is on how such migration would be planned and managed to the platform offered by identity security company *Veza* .

Specifically, we provide guidance on how such migration should occur and our perspective is from that of a platform insider from Veza (Mike Towers) and an external CISO practitioner (Ed Amoroso) working to better understand how this process can unfold. The objective is to help readers better understand how such migration can be done, since it is clear that virtually 100% of organizations, even smaller ones, are doing some form of identity security today.

It should go without saying that our assumption is that migration to Veza will provide good benefit to enterprise teams. It is not in-scope here to include marketing guidance on the platform, but readers interested in additional detail on the company, its value proposition, and specifics on the functionality inherent in the platform should directly **contact Veza** for such information.

OVERVIEW OF VEZA

Veza, an innovative identity cybersecurity startup, was founded in 2020 by Tarun Thakur, Maohua Lu, and Rob Whitcher . , T t he company's inception was driven by the founders' recognition of the critical need for enhanced security measures in the rapidly evolving area of identity and access management (IAM) – and in the provision of more advanced identity security for enterprise customers specifically.

Veza is headquartered in Los Altos, California, and has quickly gained attention for its unique approach to identity security . The core mission of Veza is to provide robust security solutions that simplify and secure the management of digital identities and access rights. This mission is particularly relevant as organizations increasingly rely on artificial intelligence, public cloud and SaaS services, and remote workforces, all of which introduce new security challenges.

Figure 1. Veza Founders: Tarun Thakur, CEO; Maohua Lu, CTO; Rob Whitcher, Chief Architect

The startup's flagship product is comprised of a comprehensive identity security platform. This platform leverages advanced technologies, including machine learning and artificial intelligence, to provide real-time insights and automated management of user identities and access controls. By doing so, Veza reduce the risk of data breaches and unauthorized access, which continue to be major concerns for businesses of all sizes.

One of the standout features of Veza's platform is its ability to integrate seamlessly with existing IT infrastructures. This includes compatibility with popular cloud service providers, on-premises systems, and hybrid environments. This flexibility ensures that organizations can adopt Veza's solutions without significant disruptions to their existing operations. This report, in fact, focuses on this integration aspect of the platform for practical identity security migration.

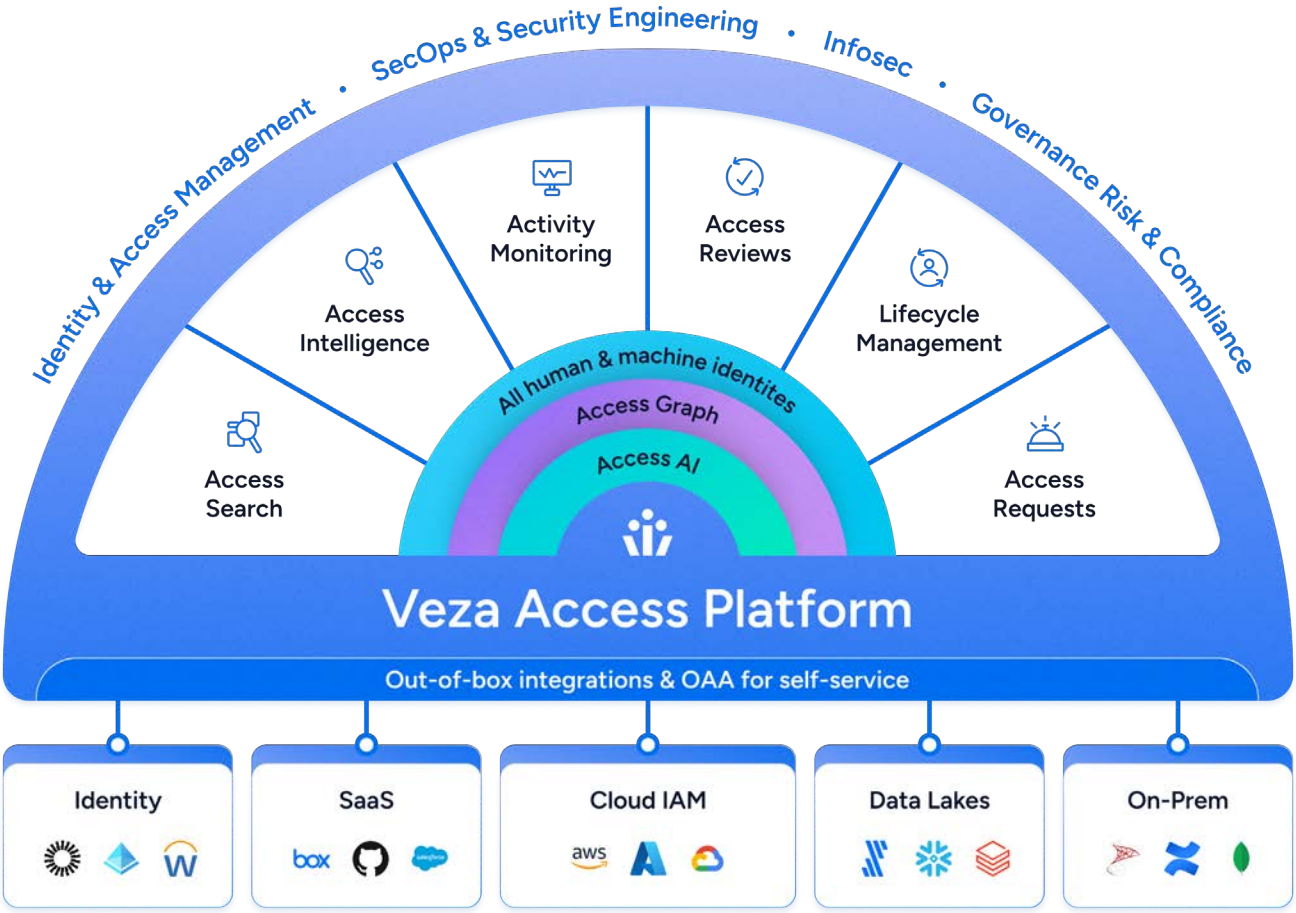

Figure 2. Veza Platform Architecture Overview

Key functions in the Veza platform include support for lifecycle management, access requests, access visibility, access intelligence, and access reviews. These capabilities are provided in the context of an API-rich approach to supporting an authorization graph for all human and machine identities. The result is an out-of-the-box integrations for SaaS, cloud, premise, and other self-service access control.

This overall approach to identity security emphasizes the principle of least privilege, which ensures that users only have the access necessary to perform their job functions. This minimizes the potential for insider threats and reduces the attack surface for external threats. The platform also provides detailed audit trails and reporting capabilities, enabling organizations to maintain compliance with industry regulations and standards.

Readers interested in additional details about the platform's core features and how it addresses specific pain points in the typical enterprise, usually rooted in deficiencies in least privilege support and complex identity governance and administration (IGA) should directly **contact Veza** for such detailed information.

PLANNING MIGRATION TO VEZA

The primary purpose of this report is to guide enterprise managers in the development of a practical plan that migrates their existing identity security scheme toward an improved IAM ecosystem that includes support from Veza. We understand that virtually no enterprise today represents a so-called greenfield in IAM – and we know that enterprise teams will want to preserve their IAM platform investment.

We address the migration approach here by introducing three management planning and implementation phases. Each of these phases is distinct, but experience dictates that interleaving between phases is common. That said, we explain the specific purpose, tasks, and expected outcomes in each phase with the hope that by following this three-phase planning model, managers can upgrade their identity governance to Veza with a minimum of friction.

It is worth noting the importance of involving key stakeholders from various departments across an organization in the planning process for migration to Veza. This typically include information technology (IT), security, human resources (HR), legal, and many other groups. The issue is simply that identity-related functions tend to sprawl across an organization and can touch virtually every aspect of an organization's day-to-day operations.

IMPLEMENTING MIGRATION TO VEZA

The three phases of migration to Veza include (1) an initial requirement gathering and planning phase, (2) a prioritization and initial transition phase, and (3) a full implementation and management phase. These are phases of work that will be guided by enterprise security leaders, but that will require day-to-day curation and guidance from team members working closely with identity and access management (IAM) related functions.

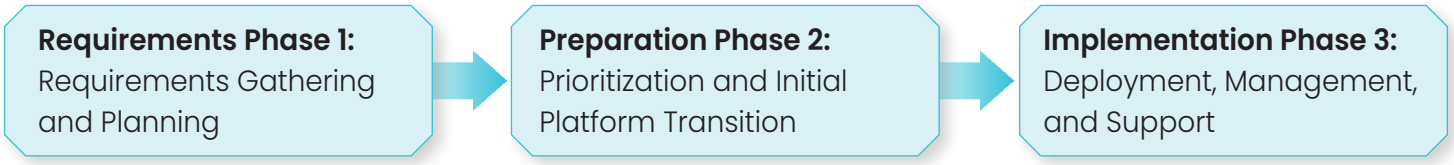

Figure 3. Recommended Three Phases of Migration to Veza

Note that the length of these stages can be contracted or expanded depending on the local circumstances. For teams who have a mature, flexible identity and access management and associated governance and administration ecosystem, the phases could be short weeks (perhaps even days), but the major of teams should set aside multiple weeks for each stage. There is no reason for this to take longer, but it is not inconceivable that the most complex environments might extend the length of the phases.

The overall goal of the three phases is to improve the ability for the team to capture and manage entitlements across the business in a more fine-grained manner. This must include all systems and identities with unified visibility, intelligence, and control of access permissions based on least privilege objectives. As will be shown, Veza supports this using access graphs that map identities, groups, roles, permissions, and other resources.

PHASE 1: REQUIREMENTS GATHERING AND PLANNING

For teams who are committed to make the transition to Veza, we recommend that the first step involve gathering all functional and compliance requirements that must be supported through the planned migration. Task owners, resource needs, and other program management information should be included. For many teams, this requirements task might have been part of an initial source selection and proposal evaluation process.

We would expect that the highest-level requirements should include focus on automated workflows, continuous monitoring, use of AI, and support for identity governance and administration (IGA) and privileged access management (PAM). Certainly, local priorities will introduce additional nuances to these broad objectives. The more detailed requirements should include the following functional areas central to deployment of the Veza platform:

During this Requirements Gathering and Planning phase, it is critical that migration teams begin by documenting the current state of the organization's identity security ecosystem, to help identify gaps and areas for improvement. This will help to ensure a smooth transition to the new system. We mention this also because far too many teams have insufficient documentation on their identity-related systems, so this must be rectified.

Account Related Functions
This area should include explicit requirements for how *user accounts* are created for target apps, including the required relationships for entities that can grant user access to groups, roles, permission sets, profiles, and teams. Requirements should be listed for how *user attributes are synchronized* across apps, including *one time and continuous synchronization* to keep local user details up to date.

Account-Related Functions	Description
User Accounts	Support for creating for target apps
Grant User Access	Access granting to groups, roles, permission
User Attribute Synchronization	Synchronization across apps
One Time and Continuous Synchronization	Support for keeping user details up-to-date

Figure 4. Recommended Account Related Requirements

Management Functions
This area should include *policy driven management of accounts* where business roles and hierarchical access profiles are used to support the need for flexible user-to-access modeling . A rules engine should be specified as a requirement to control provisioning by events and/or schedule. Such management control capability should be extensible to all identity source systems and targets.

As with most identity related functions, *full audit history* should be an absolute requirement, since audit, compliance, and regulatory activity will demand such log collection, management, and support. In addition, we recommend that a *dry-run capability* be included to allow managers to see what might happens before committing changes to production. Additional management functions will emerge based on the local environment.

Management Functions	Description
Policy Driven Management of Accounts	Manage business roles and hierarchical access profiles
User-to-Access Modeling	Provides useful relationship for use access policy management
Full Audit History	Required logs and audit records for compliance, assessment, and audit
Dry-Run Capability	Allows for review of action before committing change to production

Figure 5 . Recommended Management Functions

Integration Functions

One of the key functional requirements that should be defined during this first requirement gathering and planning phase involves determining which *major integrations* the Veza platform must support. Common applications and systems required for integration with Veza include Workday Enterprise Management, SAP Business Applications, Microsoft Active Directory (AD), Okta Identity Management, Snowflake AI Data Cloud, and others.

These applications are obviously well-known and occur commonly in most enterprise deployments. A challenge, however, for many teams is the so-called long tail of applications that also require integration, but that might not be as commonly used across industry. A key requirement here involves *custom integration and support* from Veza using their Open Authorization API (OAA) that allows for connector creation by local teams.

Integration Functions	Description
Major Integrations	Identification of the major applications (likely already integrated with Veza)
Custom Integration and Support	Smaller, local and proprietary applications requiring custom integration

Figure 6. Recommended Integration Functions

Access Review Support

An important use-case for Veza migration planning is how the enterprise seeks to use the platform in the context of access reviews . These can be done either by the *local security team* for the purpose of control validation, or by *third-party assessment teams* that might be part of an audit function, external regulatory review, customer requirements review, or other analysis of how the access ecosystem operates.

Access review coverage should include data, accounts, systems, and application that are hosted on premises, within public or private clouds, or available through a SaaS hosting arrangement. Reviewers must have visibility into actual permissions, they must have the ability to see actions that are permissible, and coverage must extend across both *user* and *non-human identities* and service accounts. The ability to review users by risk score is also a desirable feature.

Access Review Support	Description
Local Security Team Access Review	Support for access reviews by local team
External Assessor Access Review	Support for access reviews by external assessor
Access Review Coverage	Coverage of data, accounts, systems, and applications
User and Non-Human Identities	Extend to service accounts and other non-human use-cases

Figure 7. Recommended Access Review Support Requirements

Additional Requirements

The typical enterprise will likely include additional functional requirements in its migration planning to Veza. These might include capabilities such as support for natural language processing (NLP)-based queries or the option to implement self-servicing for manty of the identity governance and administrative tasks that are included in the Veza platform. Local teams should catalogue these requirements as part of this phase of migration planning.

It is also important to reference the need for stakeholder engagement and collaboration through the migration process to Veza. This might not be viewed so much as a functional requirement, but it is a management imperative and is best achieved through clear communication of migration objectives and frequent interaction across teams and departments to ensure buy-in and alignment.

PHASE 2: PRIORITIZATION AND INITIAL PLATFORM TRANSITION

The prioritization and initial platform transition phase can follow the requirements gathering and planning phase, perhaps with interleaving between the two sets of activities. The decision to prioritize initial deployment of Veza will be a local decision, and our experience is that some teams decide to start with the most urgent area of need to deal with existing gaps, whereas others decide to start with a less complex area in order to gain experience with the platform.

A key aspect of the prioritization stage should involve review of representative use-cases in order to understand how the initial transition will improve existing operation. Our recommendation is that these use-cases be categorized into three different groupings of identity security support: (1) *User Join Tasks,* (2) *User Move Tasks,* and (3) *User Leave Tasks.* These three stages are often referred to collectively as *joiner, mover, leaver (JML)*.

The *joiner stage* involves initial tasks required when new users are introduced to an environment. This demands review of so-called birthright user access for applications for any new employees, based primarily on least privilege demands and identity governance objectives. Support for least privilege, as readers will know, is a primary value proposition for enterprise teams migrating to Veza.

The *mover stage* involves the support, maintenance, and update functions required to adjust employees access and attributes across applications as such employees change jobs. This is a complex process in large environments where roles and privileges might not be clearly defined. The migration to Veza is designed specifically to help security teams and administrators take steps to clarity these attributes to support mover-stage requirements.

Finally, the *leaver stage* involves those tasks that are required, both for security and also for compliance, to disable and delete user accounts and remove access granting relationships whenever an employee leaves. Traditionally, this has been a lazy function, since teams worry about workflow breaking if an account is deleted. Veza is designed to ease this problem through integration with workflow (see Figure 8)..

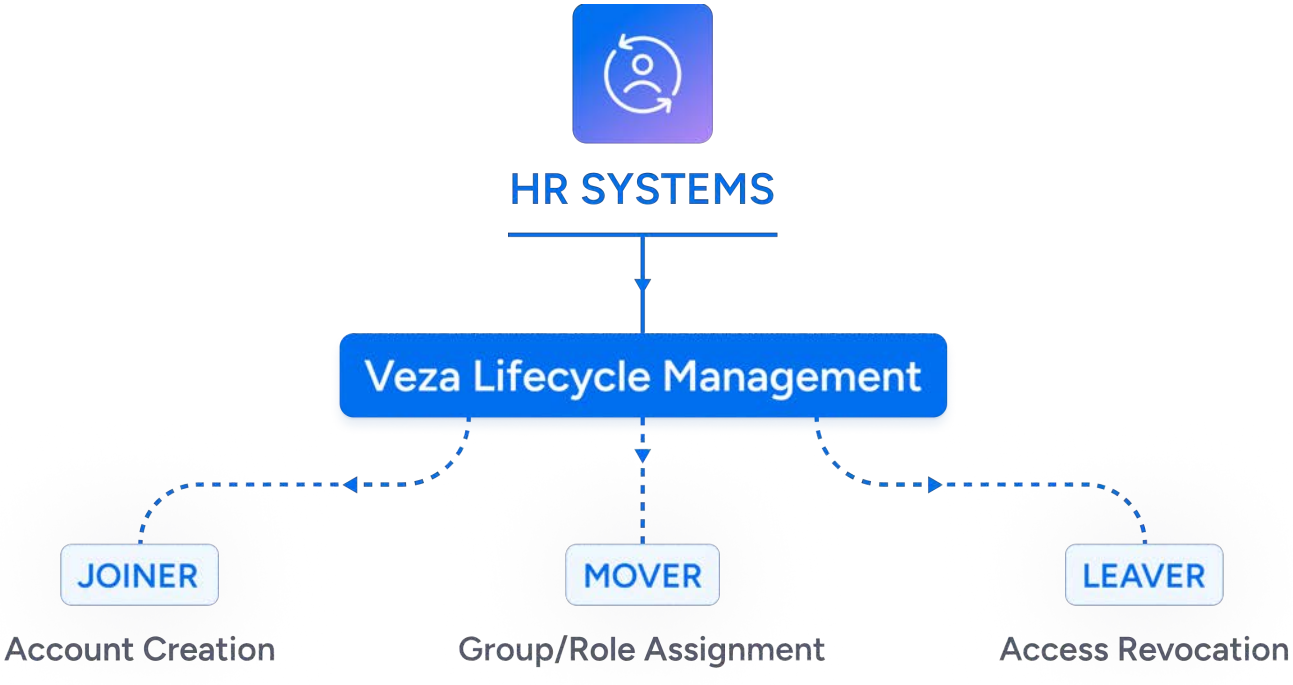

Figure 8. Veza IGA Support for Joiner, Mover, Leaver (JML)

Typical use-cases that are associated with this prioritization and initial platform phase include enterprise teams who have insufficient privileged access management (PAM), usually highlighting insider threats that benefit from poor visibility and weak support for least privilege. Once Veza is in place, these challenges wane and both threat and compliance-related issues for PAM are improved.

A second common use-case includes the transition from environments where cloud entitlement posture is scattered across various different tools or worse, not visible in any useful way, to a centralized view of how such entitlements have been issued. Early cloud infrastructure entitlement management (CIEM) solutions have begun to drive this approach, but the Veza solution provides unified visibility across hybrid cloud and SaaS applications.

PHASE 3: DEPLOYMENT, MANAGEMENT, AND SUPPORT

The third phase of migration to Veza involves the familiar tasks of platform deployment, ecosystem management, and support (including training) for the platform and program. This is obviously the target phase since it involves full operational capability, but too many teams jump into this phase without performing the important tasks listed above in the two prior phases. Skipping these initial tasks increases deployment risk and likely increases operating costs.

The Veza team has developed an extensive model and framework for how lifecycle management works in the context of IGA and least privilege deployment and use. The various inputs to the JML-process are shown and the output to applicable applications is also depicted in the diagram. We reproduce the Veza diagram here to guide our discussion of the four main steps involved in lifecycle management (see Figure 9).

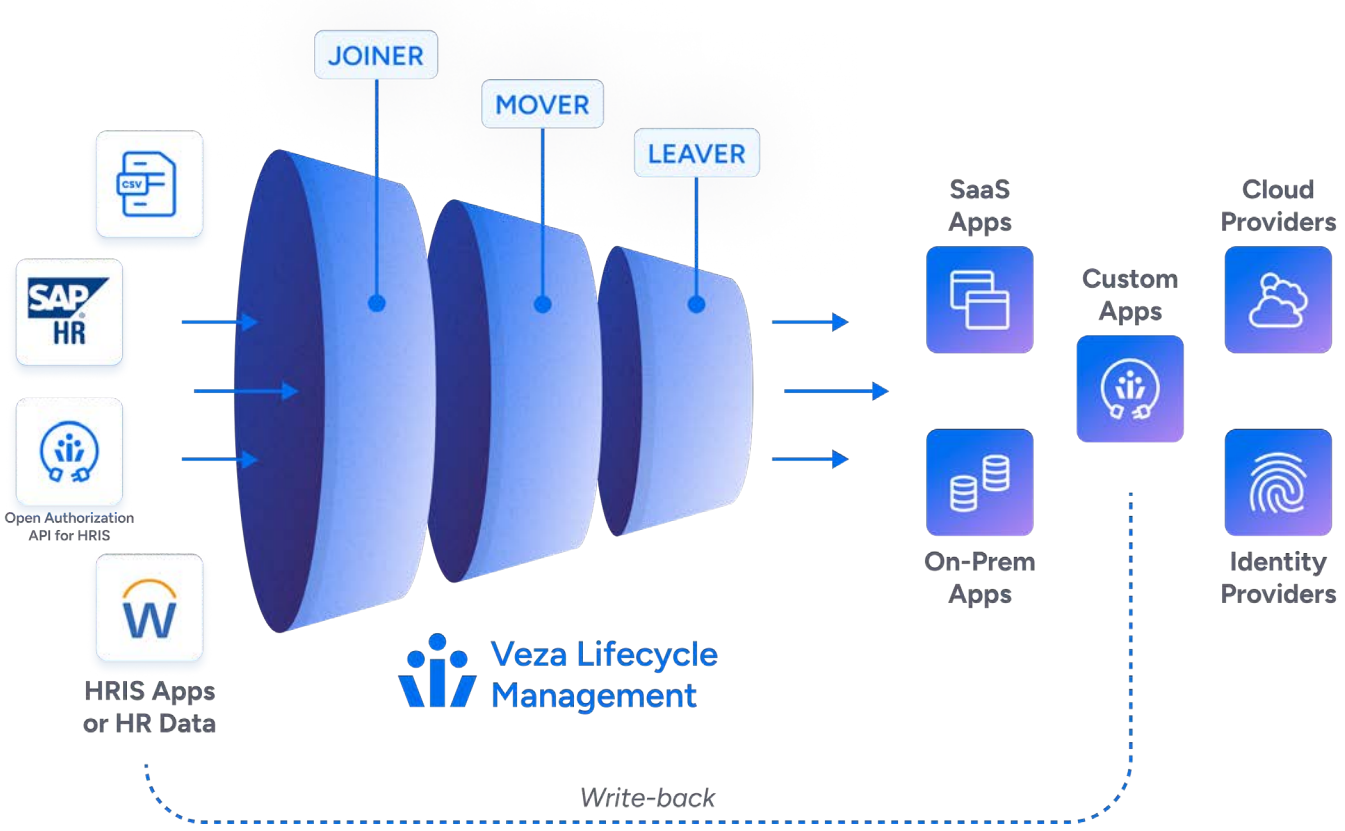

Figure 9. IGA and Privilege Lifecycle Management Overview

The recommended lifecycle to ensure correct and consistent access for users across all phases of deployment, support, and use include the following steps:

- **Automated Provision** – This involves the initial step of setting up new joiners with properly provision accounts using birthright policy for access to applications, services, and workloads.
- **Management of Accounts and Entitlements** – The management of accounts and entitlements is mostly focused on keeping things up to date as changes are made to roles, job, privileges, and user status.
- **Account Deactivation** – This is used when users leave the organization or make a significant change to their status. Removing accounts is essential to maintaining proper identity hygiene.
- **Application Support** – The need to maintain support for applications includes attribute write-back, policy versioning, auditing, and support to "dry-run" changes to review impact before commit.

ACTION PLAN

This document is intended to provide a management overview of the typical migration considerations involved in moving from an existing IGA and PAM deployment to a Veza implementation that changes the IGA function for processes such as JML and that introduces support for least privilege. Our hope is that this document helps to move the process from the early planning stage to an actual migration project.

Much more detailed migration documentation, resources, tools, and use-case examples are available from Veza for the technical team. This information can be used as the basis for a partnership between Veza and the migration team to address any local tailoring or other aspects of the migration that might demand more focused analysis and support. Our hope is that the migration process for your team goes smoothly and rapidly.

ABOUT TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.