veza

Solution Brief

Non-Human Identity Management

Non-human identities (NHIs) are the largest and fastest growing part of your identity attack surface. Hackers are attacking NHIs because they know they can avoid human-focused security tools like MFA, so your security and compliance strategies must adapt to secure NHIs as first-class citizens.

17:1

Average ratio of non-human to human identities in the cloud

Learn more

Challenges in securing NHIs

Discovery

Most organizations know where some of their NHI accounts are, but have a blind spot for those that might have been created years ago, before any standardized processes were implemented.

Ownership

To secure or govern an NHI, you need a human owner who knows how it's used. Rotating credentials, doing access reviews, or even verifying that an NHI is still in use needs a person who understands where it fits in your technology stack.

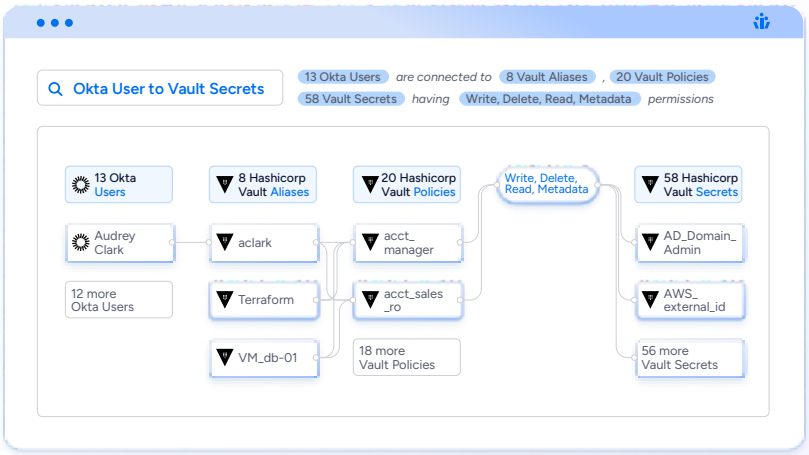
Rotating Secrets

Tools like secrets managers allow you to rotate credentials for NHIs, but what about all the NHI credentials that aren't in the secrets manager? How do you make sure you don't take on the security and compliance risk of expired keys?

Intelligent access for NHIs

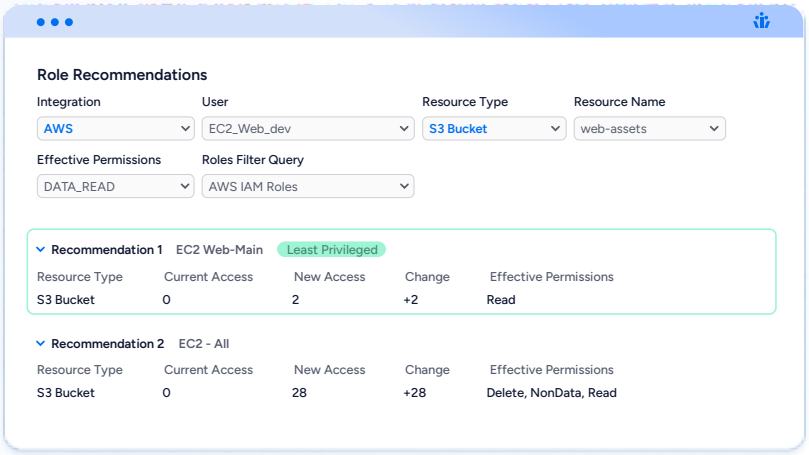
Discover NHIs across your stack

- Discover NHIs efficiently across on-prem, SaaS apps, custom apps, and cloud infrastructure.
- Import data from CMDBs (configuration management databases) or external spreadsheets to clearly label NHIs and assign human owners.
- Identify "shadow" NHIs not in your secrets manager and bring them in line with your security and governance policies.



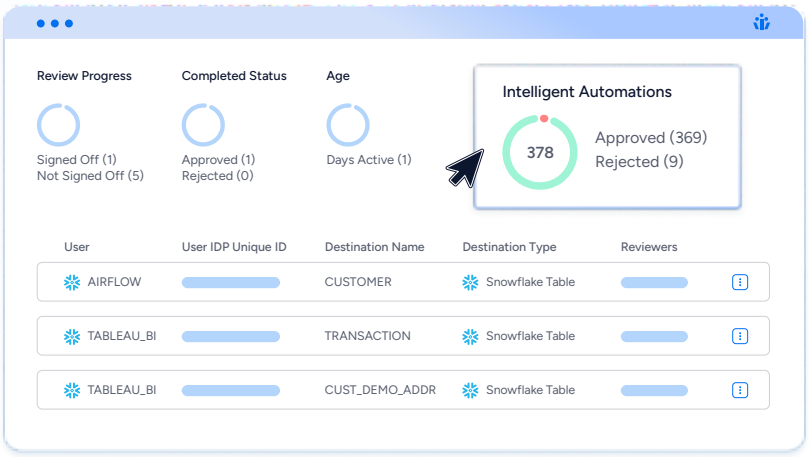
Least privilege for all identities

- Analyze permissions and activity of NHIs to identify and remove unneeded privileges, including admin permissions, without disrupting business-critical processes.
- Eliminate shadow NHIs by identifying and restricting the power to create and provision access to virtual machines, lambda functions, certificates, and secrets.
- Use access requests and role recommendations to create a single streamlined provisioning processes for both human and non-human identities that maintains least privilege.



One platform to govern humans & NHIs

- Run NHI Ownership Certification campaigns to ensure business need, correct ownership, and least privilege.
- Secure NHIs in local accounts, and manage human permissions to enforce a secure NHI Lifecycle.
- Enforce security policies like key rotation for NHIs, and provide useful context to access reviewers, like “Time last rotated” and “Time last used”.



250+ integrations

Veza provides 250+ out-of-the-box integrations that pull metadata from identity systems, cloud service providers, data systems, and on-prem applications to reveal the effective permissions to your most critical data.

Active Directory · AWS · Databricks · ElasticSearch · GCP · GitHub · Kubernetes · MongoDB · Okta · Oracle Cloud

PostgreSQL · ServiceNow · Snowflake · SQL Server · Workday · Salesforce · AWS KMS · Azure Key Vault · Google KMS · Azure

NHI use cases

Discover NHIs

Find and label which accounts are non-human across 250+ integrations

Assign human owners

Use Veza Tags to assign human owners to NHIs. Import ownership data from spreadsheets or other external sources.

Analyze permissions for least privilege

Understand permissions of NHI accounts/keys and right-size to business need

Ensure key rotation

Associate credentials with NHIs, and capture metadata from integrated systems, like “Time last rotated” and “Time last used”

Access Reviews

Assign reviews of all access to NHIs to their owners for certification. Identify and remove unneeded access.

Activity monitoring

Find dormant permissions to fix excess privilege in core platforms like Snowflake and AWS. Remove unused access.

Role recommendations

Optimize the NHI provisioning process to fix over-permissioning at the time of account creation. Eliminate “admin-level” permissions on NHIs where not needed.

The world’s most trusted companies use Veza

CROWDSTRIKE · snowflake · Blackstone · zoom · workday · Chipotle · Expedia · INTUIT · Edwards · Rakuten · dentsu · Capital One

“We needed to understand how users and service accounts have been entitled to specific data. Veza is the only tool I’ve seen that can show you both parts of the picture. One part is the people or accounts who are supposed to have access as part of a security group. And then there’s the flip side where you look at it from the data end and say, this is who also has access, and this is how that access was granted. It’s the clearest view I’ve ever seen for data access.”

Steven Guy / *Vice President, Security Solutions*

incomm

 | veza.com