



IAM & Non-Human Identity (NHI)



What it is:

Secure access across human and non-human identities

SecOps & Identity Teams



IT Operations & Engineering Teams



Risk, Compliance, & Governance Teams



Gain continuous assurance through visibility into human and non-human access.

Why it matters

Traditional identity tools focus on directory roles and groups, while actual permissions extend across applications, cloud services, databases and code repositories.

Non-human identities and AI agents create additional, often invisible access paths. Without resource-level visibility, organisations cannot understand what identities can do, assess their potential blast radius or confidently govern access.

What it does:

Gain clarity and control over enterprise access

Trace permission paths

Understand how access is granted across identities, policies and resources.

Quantify blast radius

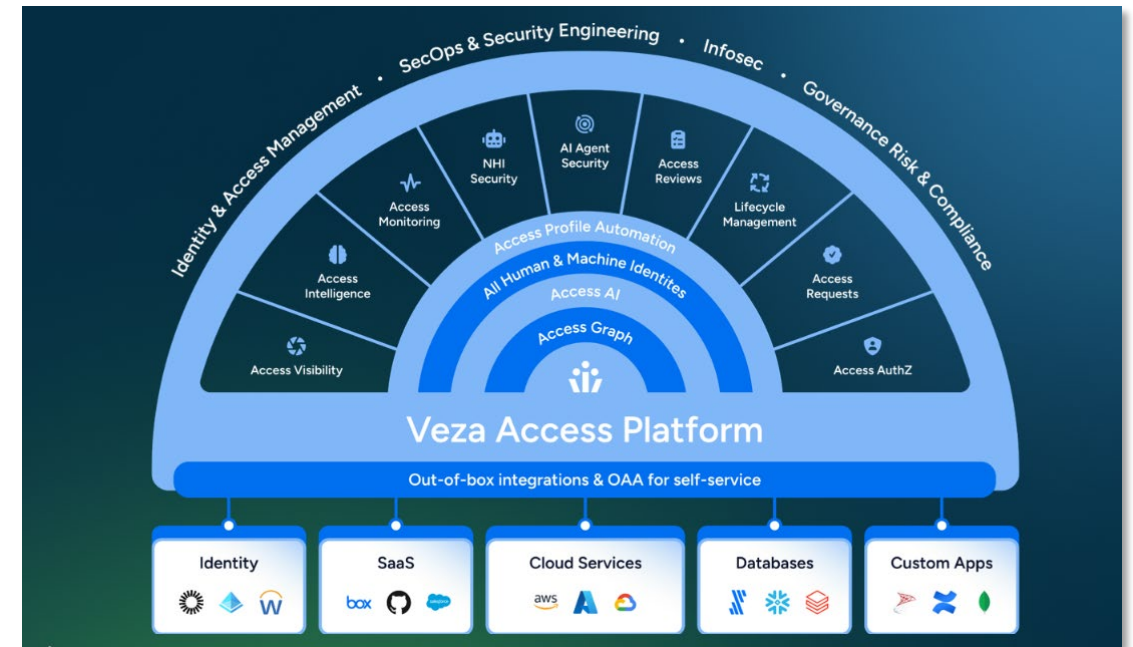
Identify where excessive access creates security and business risk.

Reveal effective permissions

Make decisions based on actual access rather than roles or groups.

Benefits

- Minimise exposure from hidden and unmanaged access
- Improve governance decisions with resource-level evidence
- Support confident adoption of AI agents and machine identities



How it does it: Demo

Input

Access data from enterprise applications, cloud platforms, databases, code repositories and identity systems.

Action

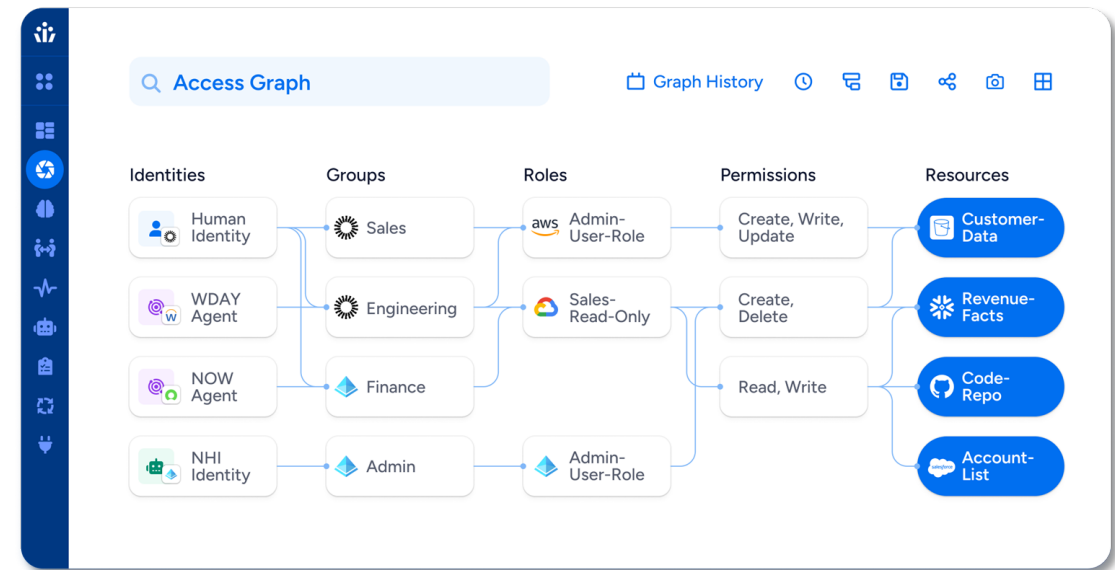
The solution maps relationships between identities, permissions, policies and resources to reveal effective access and hidden access paths.

Output

Security and governance teams gain a unified view of who can access what, what actions can be performed and where risks exist

Impact

Organisations can reduce blind spots, prioritise access risks and make more informed governance decisions based on actual permissions rather than assumptions.



Explore your organisation's true access landscape

Discover how resource-level visibility can strengthen access governance across human, machine and AI identities.

Consider a discussion if your organisation is:

- Reviewing access beyond directory roles and groups
- Securing non-human identities and service accounts
- Deploying AI agents with appropriate governance

Request a consultation to identify and prioritise access risks across digital identities.



Mayuresh Dhavale

**Director, Cyber,
KPMG in Singapore**

mdhavale@kpmg.com.sg



KPMG Services Pte. Ltd.

© 2026 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

General disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Document Classification: KPMG Public