



Unified Identity Security Platform

Identity Protection at the
Speed of AI with Silverfort



What it is:

A solution to unify identity protection across every authentication

Security Leaders



Identity Teams



Risk Leaders



Address fragmented identity controls through unified visibility and runtime protection.

Why it matters

Identity controls remain fragmented across legacy, cloud, human, machine and AI identities, limiting visibility and creating inconsistent enforcement. Gaps in legacy protection and reactive detection may allow risky access and lateral movement before action is taken. Unified visibility and controls applied at authentication runtime enable organisations to understand exposures, strengthen access decisions and protect identities consistently.

What it does: Strengthen control across every identity

Gain unified visibility

Understand identity risks and authentication activity.

Enforce runtime controls

Prevent risky access before it escalates.

Extend protection

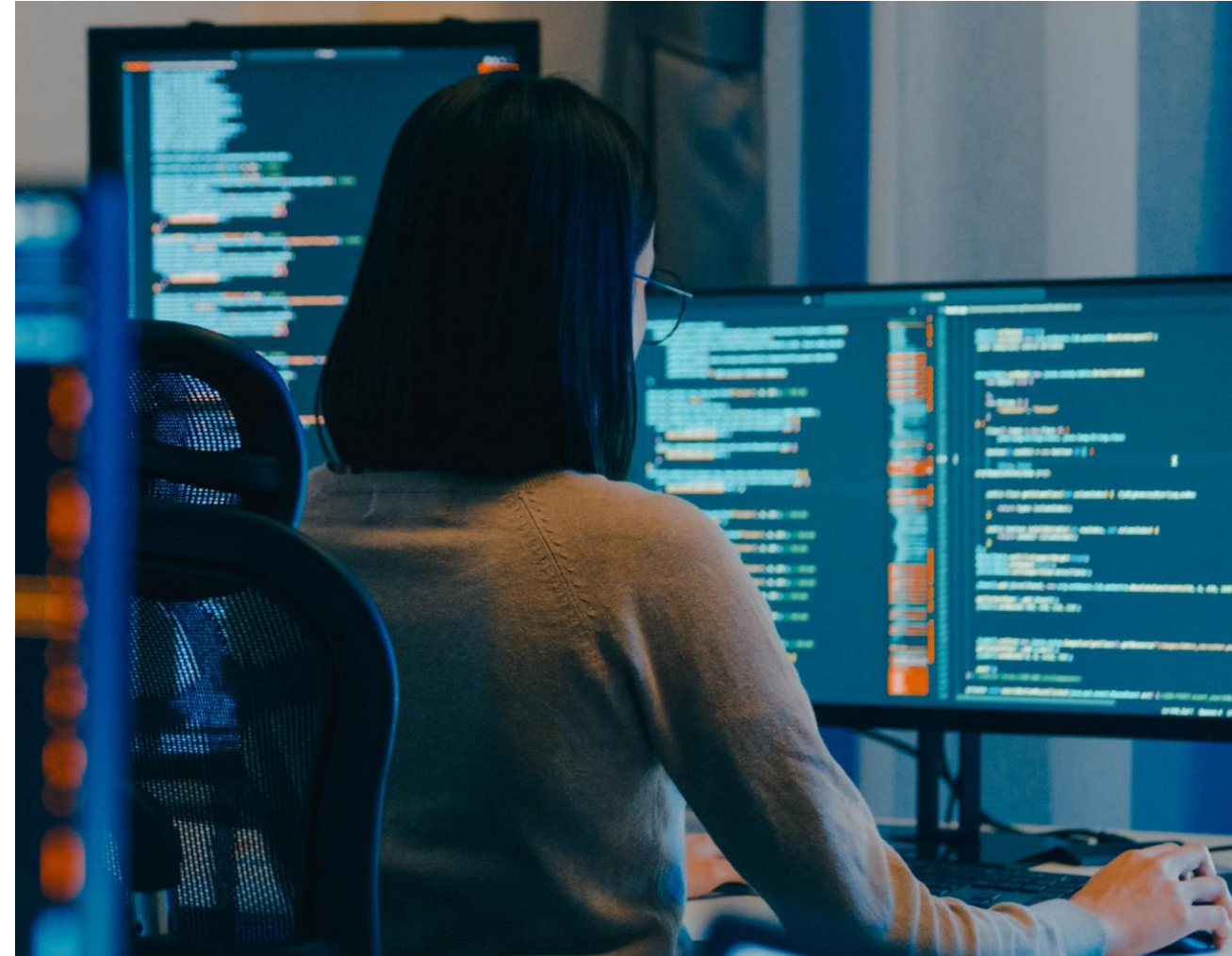
Secure legacy, privileged and non-human identities.

Operationalise policies

Maintain consistent control across environments.

Benefits

- Prioritised remediation of identity exposures
- Consistent protection across legacy and cloud environments
- Continuous control through monitoring and optimisation



How it works

Input

The organisation identifies its identities, authentication environments, exposures and priority use cases.

Action

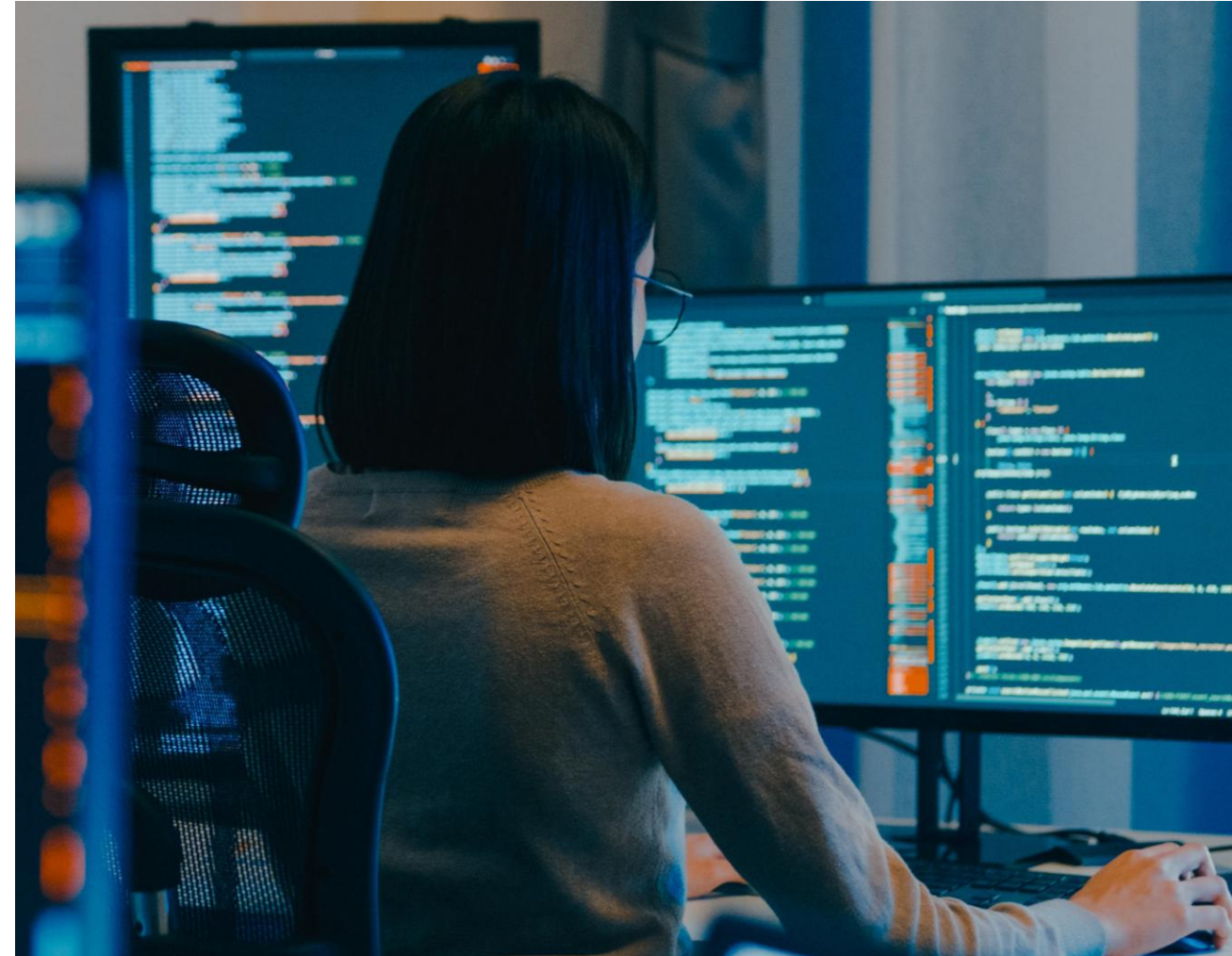
Identity risks are assessed, runtime policies are designed and controls are deployed, tested and tuned.

Output

The organisation receives consolidated visibility, risk insights and consistently enforced authentication controls.

Impact

Address risky access earlier while maintaining identity protection across legacy and cloud environments.



Strengthen identity protection across your environment

See how unified visibility and runtime controls help protect human, machine and AI identities.

Consider a consultation if your organisation is:

- Assessing identity and Active Directory risks
- Extending MFA to legacy systems and protocols
- Strengthening privileged and non-human identity protection

Book a consultation to identify and prioritise your identity protection opportunities.



Hu Tsun Hao

Associate Director, Cyber,
KPMG in Singapore

tsunhaohu@kpmg.com.sg

Our Joint Offering: Operationalise Identity Protection

A joint offering that combines identity visibility and runtime enforcement with assessment, implementation, policy design and sustained operations.

SILVERFORT

Technology and runtime controls

- 1 Identity discovery, graph and risk insights
- 2 Runtime Access Protection across AD and cloud
- 3 Universal MFA and Authentication Firewall
- 4 Protection for privileged and non-human identities
- 5 ITDR, ISPM, Access Intelligence and AI Agent Security

KPMG

Advisory, implementation and operations

- ✓ Identity security and AD risk assessment
- ✓ Target architecture and deployment planning
- ✓ Use-case and policy prioritisation
- ✓ Control testing, tuning and rollout governance
- ✓ Operating model, training and managed support

JOINT OFFERINGS

01

Identity risk assessment

Discover exposures and prioritise remediation.

02

Implementation & integration

Deploy, connect and configure the platform.

03

Policy operationalisation

Design, test and phase runtime controls.

04

Managed optimisation

Monitor outcomes and continuously tune coverage.



© 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.

Document Classification: KPMG Public



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