WHITE PAPER

REIMAGINING ACCESS: THE BUSINESS VALUE OF PASSWORDLESS AUTHENTICATION AT SCALE

Abstract

Identity has become the primary attack surface in Australian enterprises. As cloud adoption accelerates, hybrid work stabilises, and SaaS ecosystems expand, authentication now sits at the centre of operational resilience and regulatory accountability.

Credential compromise remains one of the most common drivers of security incidents. In Australia, ransomware groups and financially motivated threat actors continue to exploit phishing infrastructure, password reuse, and session token theft to gain initial access. While Multi-factor authentication (MFA) has improved control maturity, many implementations still rely on reusable secrets leaving them vulnerable to adversary-in-the-middle techniques.

Passwordless authentication represents a structural evolution in identity assurance. By replacing shared secrets with device-bound cryptographic proof, organisations can reduce attacker scalability, lower credential management overhead, and strengthen defensibility under regulatory and board scrutiny.

This whitepaper outlines why password-based authentication is misaligned with the modern threat landscape, examines the operational and financial impact of credential compromise in the Australian context, and demonstrates how passwordless authentication changes the risk equation at enterprise scale.

themissinglink®
An Infosys company

Infosys
Navigate your next

The Industry Problem: Identity as the Primary Attack Vector

Credential Compromise in the Australian Context

Australian organisations continue to face elevated identity-driven risk. The Australian Cyber Security Centre Annual Cyber Threat Report 2024–25 identifies credential harvesting and account compromise as common initial access vectors across both public and private sectors.[1]

Globally, the Verizon 2025 Data Breach Investigations Report confirms that stolen credentials remain one of the most prevalent breach patterns.[2] Microsoft's Digital Defense Report 2025 similarly identifies password spray, token replay, and phishing proxy infrastructure as sustained attack methods.[3]

A typical identity-driven attacks now follow a predictable progression:

- Credentials harvested via phishing or breach reuse
- MFA intercepted through proxy infrastructure
- Session tokens replayed
- Privilege escalation within Microsoft 365 or cloud control planes
- Lateral movement and data exfiltration

The attack surface has shifted from the network perimeter to the identity control plane.

For Australian CISOs, this shift carries regulatory and disclosure implications. Under the Notifiable Data Breaches scheme, credential-driven compromise involving personal information can trigger mandatory reporting obligations. For APRA-regulated entities, CPS 234 requires demonstrable control effectiveness and regular validation of security controls.

The Structural Weakness of Password-based Authentication

Passwords operate on a shared secret model. It is the design, rather than user behaviour, that creates persistent risk.

In a shared secret system, the same credential must be known by both the user and the verifying service. That credential must be stored, transmitted, compared at each authentication attempt, and reused over time.

Even when protected through hashing and modern cryptographic storage techniques, password databases remain high-value targets. Once compromised, they provide material for offline cracking or credential reuse attacks across other services.

More fundamentally, passwords are phishable by design. If a user can enter a password into a legitimate domain, they can be persuaded to enter it into a convincing replica. No awareness program or rotation policy can fully mitigate that exposure because the weakness lies in the authentication model itself.

As long as authentication depends on reusable knowledge, it remains susceptible to harvesting and replay at scale.

The Limitations of Traditional MFA

Multi-factor authentication has been a critical maturity step. However, there is a meaningful distinction between MFA-enabled and phishing-resistant authentication.

Many enterprise MFA deployments remain vulnerable to:

- Push fatigue attacks
- SMS interception
- Adversary-in-the-middle phishing
- Session cookie replay

Regulatory and standards bodies increasingly emphasise on phishing-resistant methods rather than one-time-password-based approaches.[4] [5]

For Australian enterprises operating in financial services, insurance, healthcare, and critical infrastructure, this distinction is material. Insurers assess identity control maturity when underwriting cyber policies. Boards increasingly ask whether authentication is resistant to phishing, not simply whether MFA is enabled.

Traditional MFA reduces risk. It does not eliminate shared secret exposure.

Business and Operational Consequences

Credential compromise extends beyond technical control failure. It creates financial exposure, regulatory risk, and operational disruption.

Account takeover enables fraud, invoice manipulation, and unauthorised fund transfer. Compromised identities frequently provide access to personal information, intellectual property, or commercially sensitive data, potentially triggering mandatory reporting under the Notifiable Data Breaches scheme.

Administrative account compromise further increases impact. Access to Microsoft 365, Azure, and SaaS control planes allows attackers to alter configurations, establish persistence, and weaken defensive controls before detection.

The financial impact is measurable. The IBM Cost of a Data Breach Report 2025 continues to show that compromised credentials are among the most expensive initial access vectors.[6] Gartner similarly identifies credential management and password resets as a recurring operational cost in large enterprises. [9]

At scale, password-dependent authentication embeds ongoing support overhead into the identity model while increasing the likelihood and severity of breach events.

The Architectural Shift: Passwordless Authentication

Passwordless authentication removes the shared secret from the authentication process. Instead of verifying knowledge of a password, systems verify possession of a private cryptographic key bound to a trusted device.

In a passwordless model:

- The private key remains securely stored in hardware such as a TPM or secure enclave
- The identity provider stores only a corresponding public key
- Authentication occurs via cryptographic challenge-response
- Credentials are domain-bound and cannot be replayed
- There is no credential to intercept

Even if an attacker proxies traffic, there is no password to harvest or replay.

This represents a structural shift in trust validation rather than incremental hardening.

Comparative Risk Model

Password-based authentication enables attacker scale. Passwordless authentication disrupts it.

Under password-based models:

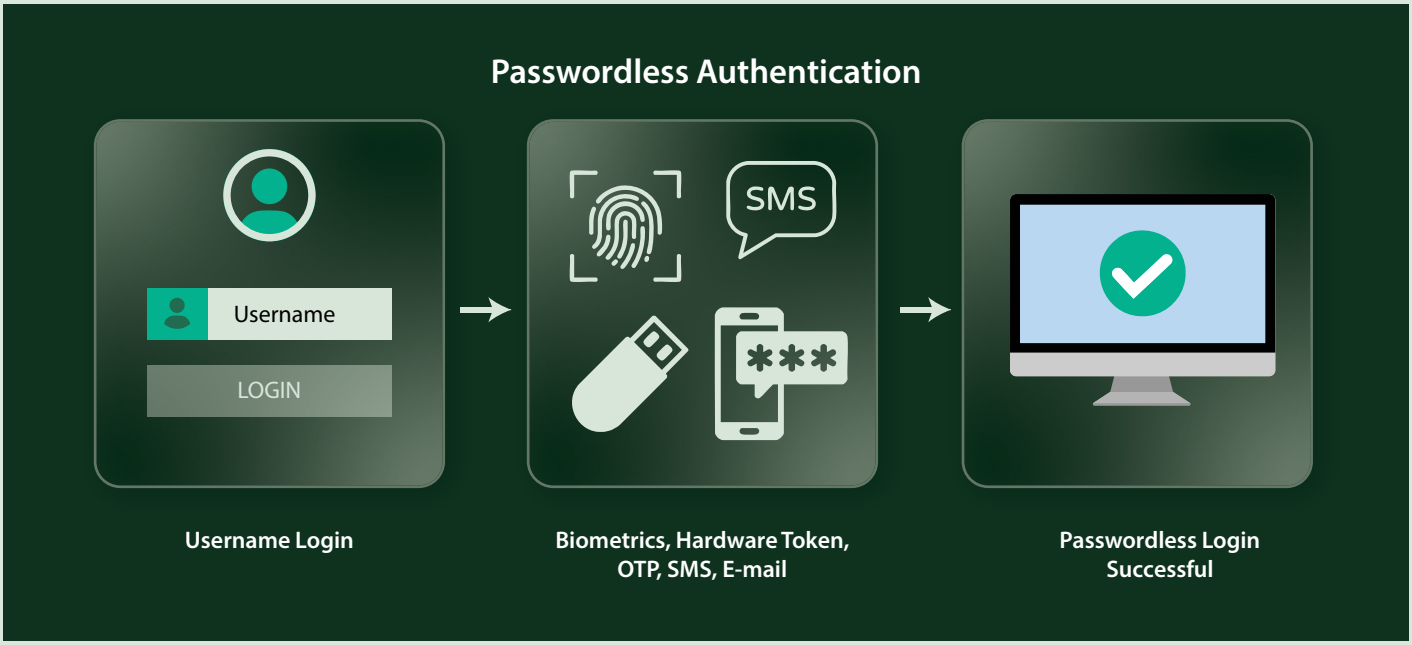
- Password spray scales across thousands of accounts
- Credential stuffing leverages breached datasets
- Phishing infrastructure industrialises harvesting

Under passwordless models:

- There is no password to spray
- There is no reusable credential to stuff
- There is no secret to replay

Attackers must pivot to endpoint compromise or physical device theft. This increases operational complexity and reduces the scalability of identity-based intrusion.

Recommendation: Enterprise Architecture Model



Implementation Realities

Passwordless transformation requires executive sponsorship and structured governance. It affects identity lifecycle management, endpoint trust, and access policy design.

Enterprise leaders must address:

- Device registration and trust governance
- Recovery and break-glass account controls
- BYOD and endpoint management alignment
- Legacy application compatibility
- Workforce change management

Where password-based methods must temporarily coexist with phishing-resistant controls, a defined transition plan is essential. The objective should be the progressive reduction of reusable credentials across the estate.

Successful adoption depends on disciplined rollout, clear ownership, and measurable milestones.

Best Practices for Passwordless Authentication at Scale

Passwordless transformation is an architectural and governance shift. The following practices support measurable risk reduction and sustainable adoption.

Prioritise privileged and high-risk identities
Administrative and executive accounts should transition first. Protecting these identities delivers immediate impact and demonstrates control maturity to boards and regulators.

Eliminate password fallback wherever feasible
Fallback mechanisms preserve shared secret exposure. Where legacy constraints require temporary coexistence, define a clear decommissioning roadmap and track reduction in password-based authentication.

Align with recognised phishing-resistant standards
Adoption should align with FIDO2 and WebAuthn standards to ensure domain-bound, device-based cryptographic authentication. This strengthens defensibility during audits and regulatory reviews.

Integrate device trust with identity policy
Passwordless authentication shifts assurance to the device. Integration with endpoint management, TPM validation, and conditional access policies ensures authentication strength, and reflects device posture and contextual risk.

Design secure recovery processes
Account recovery must not reintroduce shared secret weaknesses. Break-glass accounts should be tightly governed, monitored, and excluded from standard workflows.

Define measurable success criteria and track impact
Passwordless initiatives should link directly to measurable business outcomes. Success should be assessed through observable changes in identity risk and operational overhead.

Key indicators include:

- Monthly password reset volume and associated helpdesk cost
- Credential compromise incident frequency
- Fallback authentication rate
- Passwordless adoption coverage across workforce and privileged identities
- Reduction in reusable privileged credentials
- Authentication friction metrics, including time-to-authenticate and failure rate

Monitoring these indicators enables evidence-based reporting to boards, insurers, and regulators. It demonstrates that authentication risk exposure is being structurally reduced rather than incrementally improved.

Strategic Implications for Australian CISOs

Passwordless transformation requires executive sponsorship and structured governance. It affects identity lifecycle management, endpoint trust, and access policy design.

Enterprise leaders must address:

- Device registration and trust governance
- Recovery and break-glass account controls
- BYOD and endpoint management alignment
- Legacy application compatibility

Workforce Change Management

Where password-based methods must temporarily coexist with phishing-resistant controls, a defined transition plan is essential. The objective should be the progressive reduction of reusable credentials across the estate.

Successful adoption depends on disciplined rollout, clear ownership, and measurable milestones.

Passwordless authentication directly affects:

- Notifiable Data Breaches obligations
- APRA CPS 234 control effectiveness expectations
- Cyber insurance underwriting scrutiny
- Board-level cyber risk oversight

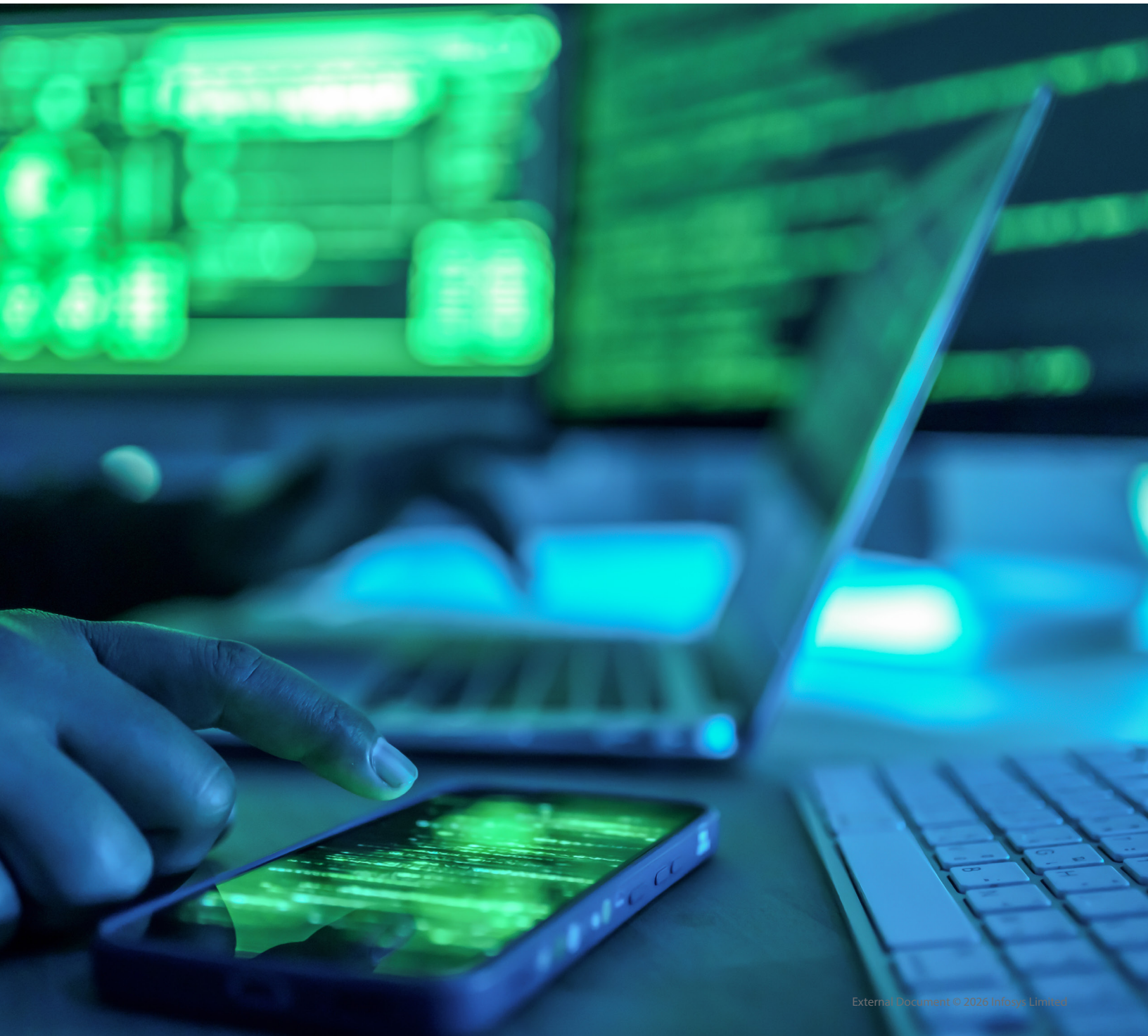
Boards are asking whether identity controls are resistant to phishing. The presence of MFA alone no longer answers that question. The issue is whether reusable secrets remain embedded in the authentication architecture.

In regulated environments, continued reliance on shared secret authentication is a governance choice. When phishing-resistant alternatives are available, organisations must consider whether maintaining reusable credentials aligns with their defined risk appetite.

Identity assurance is shifting from knowledge-based verification to cryptographic proof at the enterprise level. Organisations that treat this transition as a structural control evolution will be better positioned to demonstrate measurable risk reduction.

Those that retain reusable credentials as a foundational control may increasingly find that the exposure is structural rather than technical.

Treating passwordless authentication as a strategic control transformation will be better positioned to demonstrate measurable risk reduction to regulators, insurers, and boards.



References

1. Australian Cyber Security Centre. (2025). Annual Cyber Threat Report 2024–25.
2. Verizon. (2025). 2025 Data Breach Investigations Report (DBIR).
3. Microsoft. (2025). Microsoft Digital Defense Report 2025.
4. Cybersecurity and Infrastructure Security Agency (CISA). (2024). Implementing Phishing-Resistant MFA.
5. National Institute of Standards and Technology (NIST). (2024). Digital Identity Guidelines (SP 800-63-4 draft updates).
6. IBM Security. (2025). Cost of a Data Breach Report 2025.
7. Australian Prudential Regulation Authority (APRA). CPS 234 Information Security.
8. FIDO Alliance. (2024). Passkey Adoption and FIDO Authentication Trends.
9. Gartner. (2024). Reducing Password-Related Support Costs Through Passwordless Authentication.

About the Author

Ruchit Deshpande

Security Solutions Director, The Missing Link

Ruchit is a seasoned cybersecurity leader with over 15 years of experience spanning Security Architecture, Engineering, and Project Management. He has successfully led complex cyber-uplift programs, security assessments, and enterprise-wide implementation initiatives across diverse industry sectors.

Ruchit is recognised for his ability to translate technical depth into strategic insight and is adept at presenting to Board members and C-suite stakeholders. His expertise is backed by an extensive portfolio of certifications, including CyberArk Guardian, CDE, CISSP, SANS GCIH, Fortinet NSE 4 & 7, CCNA, ZCCA-IA, ZCDS-IA, and FCSA.

Contact The Missing Link

E-mail: contactus@themissinglink.com.au

Website: www.themissinglink.com.au