Enterprise Identity Maturity Model – Website Copy

Level 1 – Legacy Identity Hygiene

At this stage, organizations are shoring up the basics—locking down obvious entry points that attackers frequently exploit. Even in 2026, weak passwords, shared accounts, and dormant identities remain common drivers of breaches. Foundational hygiene dramatically reduces risk and sets the stage for more advanced controls.

What this level includes:

- Multi-factor authentication (MFA) enabled for all users
- Strong, unique passwords and elimination of shared accounts
- Removal of dormant and unused accounts (high-risk for takeover)
- Waiting rooms, lobbies, and restricted meeting sharing to prevent unauthorized joiners

Risks addressed:

- Prevents basic account takeover (still the #1 root cause of breaches)
- Reduces unauthorized meeting attendance—a growing vector for AI-based impersonation attacks () [Enterprise...2026-01-30 | PowerPoint]
- Minimizes internal misuse or accidental exposure via forgotten accounts

Level 2 – Secure Application & Cross-Tenant Identity

As organizations modernize their digital ecosystem, applications and cloud services must authenticate to *each other*—not just to users. This level secures identity flows across SaaS apps, partners, and collaboration platforms to eliminate weak, inconsistent login experiences.

What this level includes:

- Seamless SSO across applications through federation
- Strong app-to-app authentication using SAML or OIDC
- Automated provisioning and de-provisioning via SCIM

Risks addressed:

- Eliminates password sprawl and inconsistent login behavior
- Reduces unauthorized third-party access across interconnected apps
- Shrinks attack surface created when external partners, contractors, or shadow IT tools plug into collaboration platforms () [Enterprise...2026-01-30 | PowerPoint]

Level 3 – Passkeys & Zero Trust

AI-enabled phishing and impersonation have made passwords obsolete. At this stage, organizations shift to phishing-resistant, passwordless authentication and enforce contextual access rules based on risk. This is where you meaningfully reduce AI-driven account takeover.

What this level includes:

- Passwordless authentication for all users
- Hardware secure keys or device-based passkeys for admins and high-risk roles
- Conditional Access policies using device posture, geography, and real-time risk signals

Risks addressed:

- Prevents credential theft even against AI-generated phishing (a rapidly growing attack vector)
- Blocks unauthorized access from risky devices, unmanaged endpoints, or suspicious locations
- Stops attackers from leveraging deepfaked IT staff to socially engineer MFA resets (documented in multiple real-world incidents—Retool, etc.) () [Enterprise...2026-01-30 | PowerPoint]

Level 4 – AI-Resilient Identity Security

This level recognizes that identity is no longer static. AI-driven attacks bypass traditional MFA, mimic executives, and blend into normal communication patterns. Enterprises begin using continuous, behavioural identity assurance and deep security integration across platforms.

What this level includes:

- Behavioural and continuous authentication
- Privileged Access Management with isolated admin accounts and secure keys
- AI-driven anomaly detection in collaboration platforms
- Integrated XDR/EDR with SIEM/SOAR for real-time identity correlation

Risks addressed:

- Detects impersonation even after login—where deepfake attacks typically strike () [Enterprise...2026-01-30 | PowerPoint]
- Limits blast radius if an attacker compromises an admin or high-privilege identity
- Provides automated detection of unusual meeting behavior, suspicious file-sharing, and abnormal communication patterns

- Strengthens response to emerging AI voice/video impersonation threats that bypass legacy controls

Level 5 – AI Agent Governance (2026+)

By 2026, AI agents—bots, copilots, automated assistants, synthetic avatars—will access sensitive systems just like human users. This level governs *nonhuman identities* and protects collaboration sessions from advanced AI impersonation and synthetic media attacks.

What this level includes:

- Verified, secure identities for all AI agents
- Inline protections against prompt injection and data leakage
- Cryptographic meeting-join verification for sensitive calls
- Integrated deepfake detection during collaboration sessions

Risks addressed:

- Prevents rogue AI agents, shadow agents, and unauthorized automation from accessing enterprise data
- Stops deepfaked executives, avatars, or agents from joining meetings unnoticed
- Shields sensitive workflows (finance, R\&D, legal) from real-time impersonation attacks, which have already led to multimillion-dollar fraud incidents () [Enterprise...2026-01-30 | PowerPoint]

Top 5 Identity Priorities for 2026

These are the highest-impact steps organizations can take right now to harden collaboration, reduce AI-driven impersonation risk, and modernize identity security.

- Deploy phishing-resistant passkeys enterprise-wide
- Enable continuous, risk-based authentication
- Implement Privileged Access Management (PAM) for all administrators
- Govern AI agent identities and nonhuman access
- Integrate real-time deepfake detection into critical workflows