Microsoft Entra Suite Identity & Access Accelerator

4-Week Interactive Workshop

Bring clarity, control and automation to identity and access across your Microsoft Entra estate without disrupting end users or overloading your teams. This 4-week workshop gives your security and IT stakeholders a clear view of what you already have in Microsoft Entra, how it works together, and where a phased, low-friction roadmap can reduce risk and manual effort.

Business challenge

Many organizations have enabled basic Entra capabilities but still struggle with:

- Access sprawl and inconsistent policies across apps, networks, and admin roles.
- Manual joiner–mover–leaver processes and scattered approvals.
- Limited use of risk-based controls, ZTNA and SWG features already available in Entra Suite.

The result is higher audit effort, hidden privilege exposure and missed value from existing Entra investments.

What this workshop delivers

A structured, 4-week engagement (3–4 x 1.5-hour sessions per week) that:

- Educates stakeholders on Microsoft Entra ID, ID Governance, ID Protection, Private Access, Internet Access, and Verified ID as one integrated platform.
- Uses guided discussions, polls and optional tenant walk-throughs to surface patterns with minimal disruption and no formal “audit”.
- Produces neutral, documented recommendations, 1–2 standard high-level reference architectures and a phased roadmap from quick wins to advanced governance and network access.

Who should attend

- Security leadership (CISO, security architects, SOC leads).
- Identity and access teams (Entra/Azure AD owners, IAM engineers).
- Network and infrastructure leads exploring ZTNA and SWG options.
- Application owners for key SaaS and line-of-business apps.

Workshop structure (4 weeks)

Week	Focus	What customers get
Week 1 – Foundations & Signals	Entra product family overview, Entra ID, Conditional Access, Identity Protection, and how signals drive access decisions.	Shared mental model of Entra Suite, initial view of how current apps and users map to Entra capabilities.
Week 2 – Governance & Privileged Access	Entra ID Governance (entitlement management, access reviews, lifecycle workflows) and PIM in the context of least privilege.	Identified opportunities to replace manual approvals and reviews with Entra-native automation.
Week 3 – Network Access & Verification	Entra Private Access (ZTNA), Entra Internet Access (identity-centric SWG), and Entra Verified ID (including Face Check scenarios).	Candidate use cases for VPN reduction, safer SaaS/internet access, and high-assurance identity verification.
Week 4 – Patterns, Architectures & Roadmap	Synthesis of observations, standard reference architectures and a phased roadmap.	Neutral summary of strengths and gaps, 1-2 high-level reference architecture options and a quick wins → maturity roadmap with clear, optional next steps.

Key outcomes for your organization

By the end of the engagement, you receive:

- **Current-state overview –** Concise description of how identities, apps and networks are protected today using Entra capabilities, focusing on patterns rather than scores.
- **Strengths & gap summary –** Clear articulation of where Entra is already strong and where automation or policy improvements could reduce risk and manual work.
- **Standardized reference architectures –** 1-2 Microsoft-aligned high level architecture options showing how Entra ID, Governance, Protection, Private Access, Internet Access and Verified ID can be combined for your environment.
- **Phased roadmap –** A high-level, pragmatic, low-disruption plan that starts with configuration-based quick wins and advances toward more mature governance and network access patterns.
- **Optional next-step engagements –** Clearly defined, non-obligatory implementation phases (e.g., Conditional Access optimization, Governance pilot, Private/Internet Access pilot, Verified ID use case deployment).