mobile mentor

Entra Suite - An Introductory Guide

CONTENTS

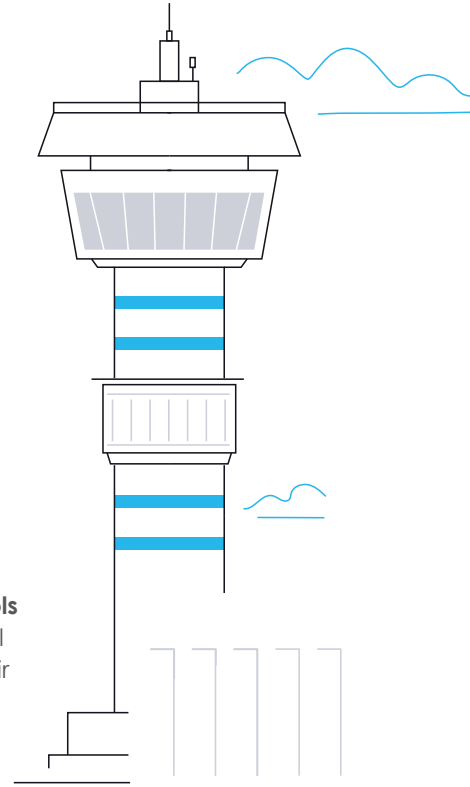
Entra Suite: Introduction

The Microsoft Entra Suite is your Zero Trust Control Tower, guiding every access decision with precision and confidence.

It doesn't just check IDs at the door, it orchestrates the entire journey. From verifying identities and enforcing least-privilege access to securing permissions across multi-cloud environments, Entra Suite makes **identity the core of your security strategy.**

Think of your IT environment like a busy airport. Dozens of systems, users, and applications are coming and going, each expecting seamless, secure access. Managing it all can feel chaotic without the right control system in place.

That's where Entra Suite shines. Instead of juggling a patchwork of tools, you get one unified platform that handles access across cloud and on-premises environments. **It's how forward-thinking businesses move from perimeter-first to identity-first security, and extend Conditional Access policies and identity controls out to all their applications.** Entra Suite extends the mature business's Conditional Access policies/identity controls down to all apps, further maturing / unifying their identity control plane.



What is the Entra Suite?

Think of Entra Suite not just as another security product, but as your friendly control tower for identity and access. It guards who you are (and who you're not), checks credentials in real time, and seamlessly reinforces zero trust security at every step. With one console to rule them all, you can manage cloud apps, on-premises apps and servers, conditional access, and hybrid setups without hunting for different dashboards or stitching together custom scripts.

It brings your ecosystem all together by:

- Evaluating **who** is requesting access
- Determining **what** they're accessing
- Enforcing **how** they access it, based on real-time risk signals
- Extending identity and access protection to on-premises applications, making hybrid environments **more secure** and manageable

Why the Entra Suite?

Think about the challenges your IT team potentially can encounter any day:

- Stolen credentials and unwanted logins putting your sensitive data at risk.
- Slow incident response because isolated systems can't share threat intelligence fast enough.
- Compliance gaps that leave you exposed to fines and legal trouble.
- An overly complex IT landscape where your security team spends more time triaging alerts than stopping attacks.
- Legacy systems or on-prem apps creating weak links that undermine your identity strategy. Identity security is only as strong as its weakest link, and when that link is an on-prem app or aging system, Entra Suite helps you close the gap with modern protections that extend beyond the cloud.

Fortunately, there's a better way.

When identity and access tools come together seamlessly, you strengthen security, speed up your workflows, and dramatically lower your risk.

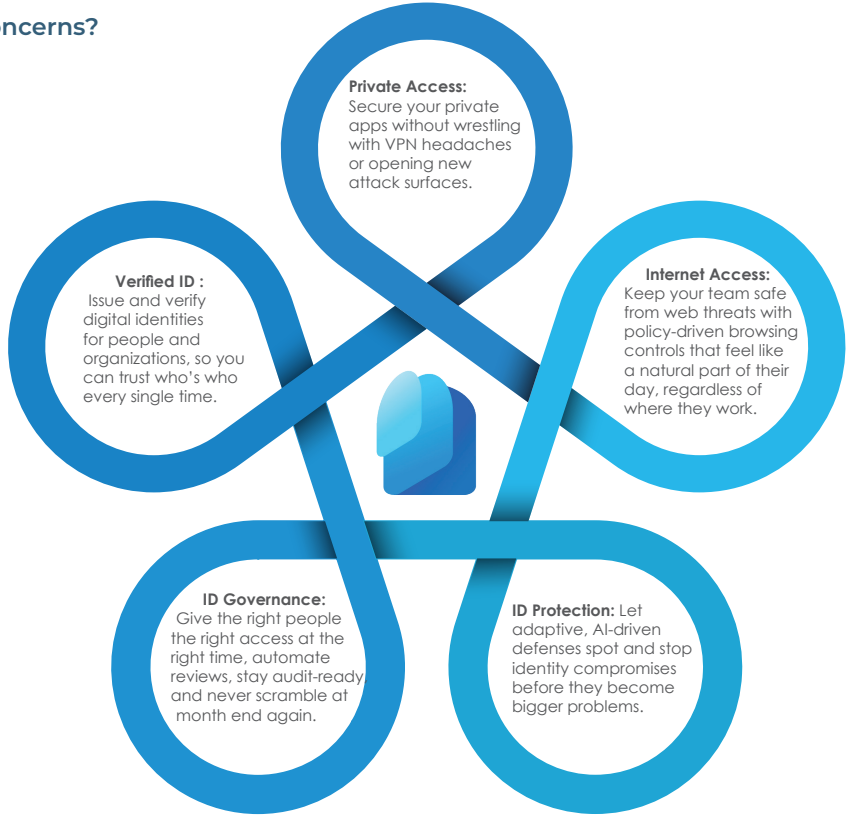
Entra Suite Solutions

How does the Entra Suite solve these concerns?

Microsoft Entra Suite addresses these challenges head-on by offering an integrated, intelligent platform with five core capabilities designed to fortify identity and access management

- **Private Access**
- **Internet Access**
- **ID Protection**
- **ID Governance**
- **Verified ID Premium**

By bringing all of these capabilities together, Entra Suite transforms a tangled web of tools into a smooth, proactive security posture, so you can focus on what really matters: empowering your people and protecting your business.



Private Access

Private Access works as an identity-first gatekeeper for your on-premises apps.

No code changes needed.

Continuing with the airport analogy: if your IT environment is a busy airport, **Private Access is like checking-in and receiving a boarding pass so the traveler can access the premium lounges, duty-free shops and departure gates.** It pre-screens users, checks risk signals, and grants secure access, quickly and efficiently. Here's how it simplifies and strengthens access:

Conditional Access Policies: Every request to your private resources is checked against the same smart policies you already use for cloud apps. That means you decide who gets in, when, and under what circumstances, down to the device health, location, or user risk level.

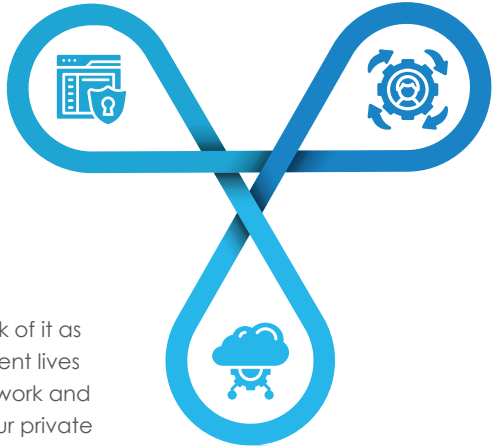
Real-Time Risk Assessment: Before a session even starts, Entra Suite evaluates signals from the user's identity, their device posture, and the specific application they're targeting. If something feels off, like a flagged device or unusual location, the system can block or step up authentication on the spot.

Network Aware Protections: Beyond identity, Private Access layers in network conditions to guard file shares, on-premises servers, and other internal apps. You control which IPs, protocols, or ports are allowed, so every resource has its own metaphorical moat.

How it Works

Behind the scenes, it all comes together through three light touch components:

Global Secure Access Agent: A small installation on user devices that enforces policies and gathers risk signals.



Entra's Private Access Service: The brains in the cloud that tie policies, risk assessments, and connectors into one smooth, invisible experience for your teams.

Private Network Connector: Think of it as the secure courier, This component lives in your datacenter or cloud network and brokers encrypted tunnels to your private apps.

In practice, your people click a link, Entra Suite quietly verifies identity and device health, then hands them a secure tunnel to access exactly what they need, and nothing more. No VPN clunkiness, no surprise "access denied" roadblocks, just secure, dependable access that keeps pace with modern work.

Internet Access

If Entra Private Access is like a boarding pass, then Entra Internet Access is your airport's public facilities as travelers leave the airport through baggage claim, car rental and general retail shops with all the one-way doors, scanners and hidden security cameras.

Entra Suite Internet Access acts like a secure escort through digital customs. Every website is scanned like a piece of luggage. Suspicious downloads get flagged like prohibited items. Risky behavior triggers secondary screening before it becomes a security incident.

Smart Web Content Filtering

Your people browse as usual, but under the hood Entra checks each site against a dynamic blocklist of known malicious or non compliant destinations. If a page is risky, it's stopped before it can load.

Custom "Safe Zones"

Need to whitelist specific corporate portals or partner sites? Admins can define approved endpoints so that critical resources always stay within reach, even if general web access is restricted.

Internet Access

Evolving Threat Intelligence

Speed Without Sacrifice

Private WAN

Evolving Threat Intelligence

By tapping into global security feeds, Entra Suite stays ahead of zero day attacks, phishing farms, and newly emerged malware, automatically updating filters so your team is always protected.

Speed Without Sacrifice

Instead of routing traffic through a slow VPN, Internet Access leverages a worldwide network of edge locations. Your users connect to the closest point of presence, keeping latency low and performance high.

Private WAN

For extra assurance, and under heavy use scenarios, traffic can flow through a private wide area network. That means no public internet hops and more predictable performance.

All of this ties back to one console and one set of policies, so your security team spends less time switching dashboards and more time proactively tuning defenses.

ID Protection

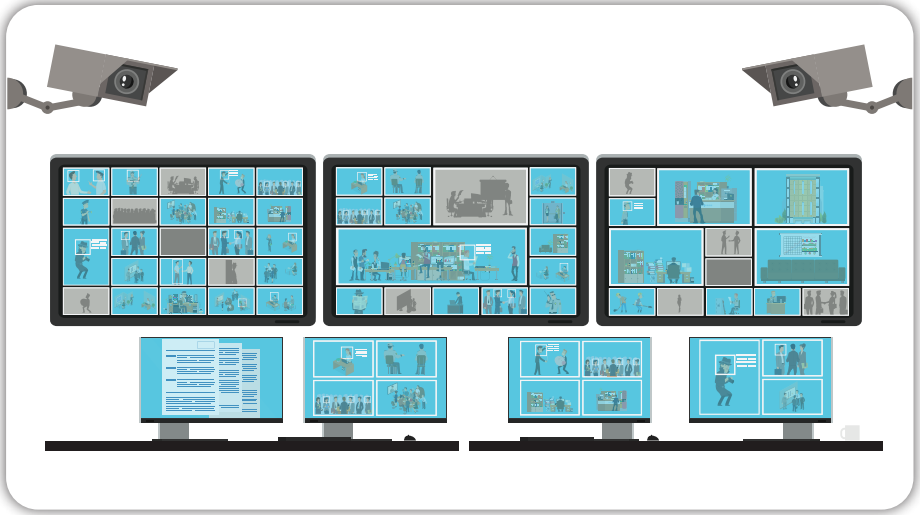
Using the airport analogy, ID Protection is the behavioral detection system at airport security, always watching for suspicious patterns before anything dangerous gets through.

Think of Entra ID Protection as your airport's undercover security intelligence unit. It's tracking behavior, monitoring anomalies, and quietly stepping in when something feels off.

Key features include:

AI Driven Threat Detection

Behind the scenes, machine learning models analyze login patterns and flag accounts showing signs of compromise, like logins from unusual locations or rapid password guessing attempts. When something looks off, the system can automatically block the session, force a password reset, or kick off an investigation, all without manual tinkering or delays.



ID Protection

Risk Based Conditional Access

Not all logins are created equal. ID Protection layers in adaptive controls so that access decisions adjust in real time. Is the user on a trusted device? Are they signing in from a familiar network? If they check all the right boxes, it's smooth sailing. If not, Entra Suite can require extra verification steps (think MFA or biometric checks) or simply deny access.

Continuous User Risk Assessment

Instead of a one-and-done login check, Entra Suite keeps monitoring account behavior over time. It builds a risk profile for each user, bumping up alerts if it spots suspicious patterns like logins at odd hours or credential stuffing. This way, you catch slowburn attacks that might otherwise slip through.

Under the hood, ID Protection weaves these capabilities into your existing workflows, so there's no heavy scripting or policy gymnastics. You get smart, automated defenses that learn and adapt, protecting identities without slowing your people down.

ID Governance

Think of ID Governance as the airport's gate and badge management office. It works to quietly orchestrate which staff, contractors, and vendors can access secure zones, maintenance hangars, or control towers.

ID Lifecycle Management in Entra:

Entitlement Management Made Simple

This solution is easy to set up and manage with no complex configurations or custom development needed. Admins and business owners can quickly choose from well-defined "access packages" that bundle the right mix of apps, groups, and permissions. With built-in self-service capabilities, users can request access independently, reducing delays and lightening the load on IT.

Review and Certification Workflows

This feature helps keep compliance officers happy by automating periodic reviews. They'll get neat, digestible lists of who can access what, and can approve or remove permissions with a click.

Time Bound Access

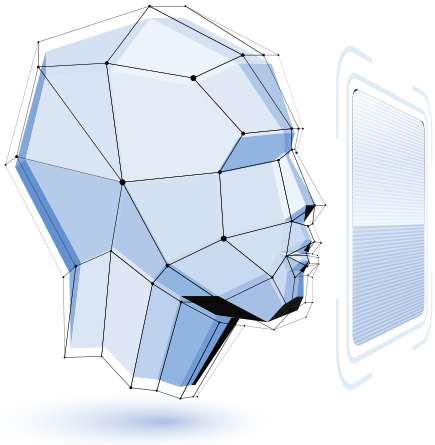
Need temporary rights for a contractor, auditor, or special project? Grant access for a fixed window, and watch Entra Suite automatically pull it back once the job's done. You get the agility of on demand access without the lingering "just in case" permissions.

Verified ID (Face Check)

Think of Verified ID as your airport's eGate system. Travelers approach the gate, scan their passport, and look into a camera. In seconds, the system checks their identity, confirms travel permissions, and, if everything aligns, grants access to the country. No manual checks, no paper forms, just a smooth, secure experience.

Here's how it maps:

- **Federated, Privacy Respecting Credentials**
  Instead of keeping user info in a central database, Verified ID uses secure, decentralized credentials. This lets you confirm someone's identity without storing their personal data, helping you stay compliant and reduce risk.
- **Autonomous, User Centric Issuance**
  Businesses or third-party issuers can create and issue custom credentials, like contractor passes or partner tokens, and users manage them in their own secure digital wallets. They choose what to share, keeping control in their hands.
- **Audit Ready Transparency**
  Every verification event is logged with cryptographic proof, so you have a tamper proof audit trail. When regulators or auditors come knocking, you can show exactly who verified what and when, instantly.



By weaving together federated credentials, seamless policy enforcement, and optional biometric checks, Verified ID Premium makes identity as easy as taking a selfie while giving you enterprise-grade trust and privacy.

Where to Begin

Implementing Microsoft Entra Suite involves a strategic, phased approach tailored to close security gaps and streamline identity and access management:

Benefits of the Entra Suite

The result of incorporating the Entra Suite into your IT strategy is three-fold:

1 **Unified Identity and Access Management**

Entra consolidates user identities across cloud and on-prem environments, ensuring seamless and secure access to apps and resources, reducing IT complexity.

2 **Advanced Security with Conditional Access**

Leverage AI-driven risk detection and adaptive policies to safeguard against identity-based attacks, only granting access when users meet specific security conditions.

3 **Streamlined User Experiences**

Enable passwordless authentication and self-service options, empowering users to securely access what they need without adding friction, boosting both security and productivity.

Are You Ready?

Are you already using the Entra Suite? If so, our team will give you the ability to embrace unified identity and access management, advanced security and access management. For a free consultation, reach out here.

Mobile Mentor is a global leader in the endpoint ecosystem and Microsoft's Partner of the Year in Modern Endpoint Management. Certified by Microsoft, Apple and Google, our engineers specialize in designs that balance endpoint security with employee experience for our clients. Check out our other whitepapers.