# Αρχιτεκτονική Αυθεντικοποίησης & Ταυτοποίησης για Εταιρεία 350 Ατόμων

Για την ασφάλεια ταυτοποίησης και πρόσβασης στο πληροφοριακό περιβάλλον της εταιρείας, υιοθετείται μια ενοποιημένη αρχιτεκτονική που βασίζεται σε τεχνολογίες της Microsoft, αξιοποιώντας πλήρως το Microsoft Entra ID Premium P1 (και P2 για διαχειριστές), σε συνδυασμό με άλλες πλατφόρμες του οικοσυστήματος Microsoft 365.

## Microsoft Entra ID (Premium P1 / P2)

Η βασική πλατφόρμα ταυτοποίησης και αυθεντικοποίησης για όλους τους υπαλλήλους.  
- Έκδοση: Microsoft Entra ID Premium P1 για όλους τους χρήστες, Premium P2 για διαχειριστές.  
- Υποστηρίζει Single Sign-On (SSO), MFA και συγχρονισμό με on-prem Active Directory μέσω Azure AD Connect.

## Microsoft Authenticator App

Χρησιμοποιείται ως βασική μέθοδος πολυπαραγοντικής αυθεντικοποίησης (MFA) για όλους τους χρήστες.

## Conditional Access Policies (Entra ID Premium P1)

Εφαρμόζονται πολιτικές ελέγχου πρόσβασης με βάση τοποθεσία, συσκευή, ρόλο χρήστη. Υποχρεωτική ενεργοποίηση MFA για πρόσβαση εκτός εταιρικού δικτύου ή από μη συμμορφωμένες συσκευές.

## Microsoft Intune (Microsoft Endpoint Manager)

- Έκδοση: Microsoft Intune Plan 1  
- Χρησιμοποιείται για διαχείριση εταιρικών συσκευών (Windows, macOS, Android, iOS).  
- Ενσωματωμένο με Entra ID για συμμόρφωση πολιτικών Conditional Access.

## RBAC (Role-Based Access Control)

Χρησιμοποιείται στο Microsoft Azure και στο Microsoft 365 Admin Center για καθορισμό ρόλων και δικαιωμάτων πρόσβασης σε cloud πόρους σύμφωνα με την αρχή ελάχιστου δικαιώματος (least privilege).

## Microsoft Defender for Cloud

- Έκδοση: Microsoft Defender for Cloud Plan 2  
- Παρέχει ασφάλεια και συμμόρφωση για workloads σε Azure, Microsoft 365 και hybrid περιβάλλοντα.

## Microsoft Information Protection (MIP)

- Έκδοση: Συμπεριλαμβάνεται στο Microsoft Purview Information Protection  
- Χρησιμοποιείται για ταξινόμηση, labeling και προστασία ευαίσθητων δεδομένων με εφαρμογή πολιτικών DLP.

## Session Lifetime Policies (Conditional Access)

Καθορίζονται πολιτικές διάρκειας συνεδρίας ανάλογα με ρόλο, ευαισθησία της εφαρμογής και συσκευή.

## Entra ID Protection (P2)

- Έκδοση: Microsoft Entra ID Premium P2  
- Παρέχει risk-based conditional access, ανάλυση μη φυσιολογικής συμπεριφοράς και αυτοματοποιημένη απόκριση.

## Privileged Identity Management (PIM)

- Έκδοση: Microsoft Entra ID P2 (Admin μόνο)  
- Παρέχει προσωρινή ανάθεση δικαιωμάτων διαχειριστή με αιτιολόγηση, έγκριση και MFA.

## Συμπέρασμα

Η παραπάνω αρχιτεκτονική εφαρμόζει αρχές Zero Trust Security και ανταποκρίνεται πλήρως στις απαιτήσεις GDPR, εταιρικής πολιτικής ασφαλείας και προστασίας cloud περιβάλλοντος Microsoft 365 & Azure. Παρέχει ισχυρή, ευέλικτη και κλιμακώσιμη ταυτοποίηση/αυθεντικοποίηση για εταιρικό περιβάλλον 350 ατόμων, με σαφή διαχωρισμό ρόλων και ενσωμάτωση μηχανισμών προστασίας τόσο για χρήστες όσο και για διαχειριστές.