ICT POWER.IT

Microsoft MVP Most Valuable Professional

Microsoft

#POWERCON2022

Secure Identities and Access to Azure AD

Nicola Ferrini

Microsoft MVP – Cloud and Datacenter Management

/nicolaferrini.it

@nicolaferrini

/nicolaferrini

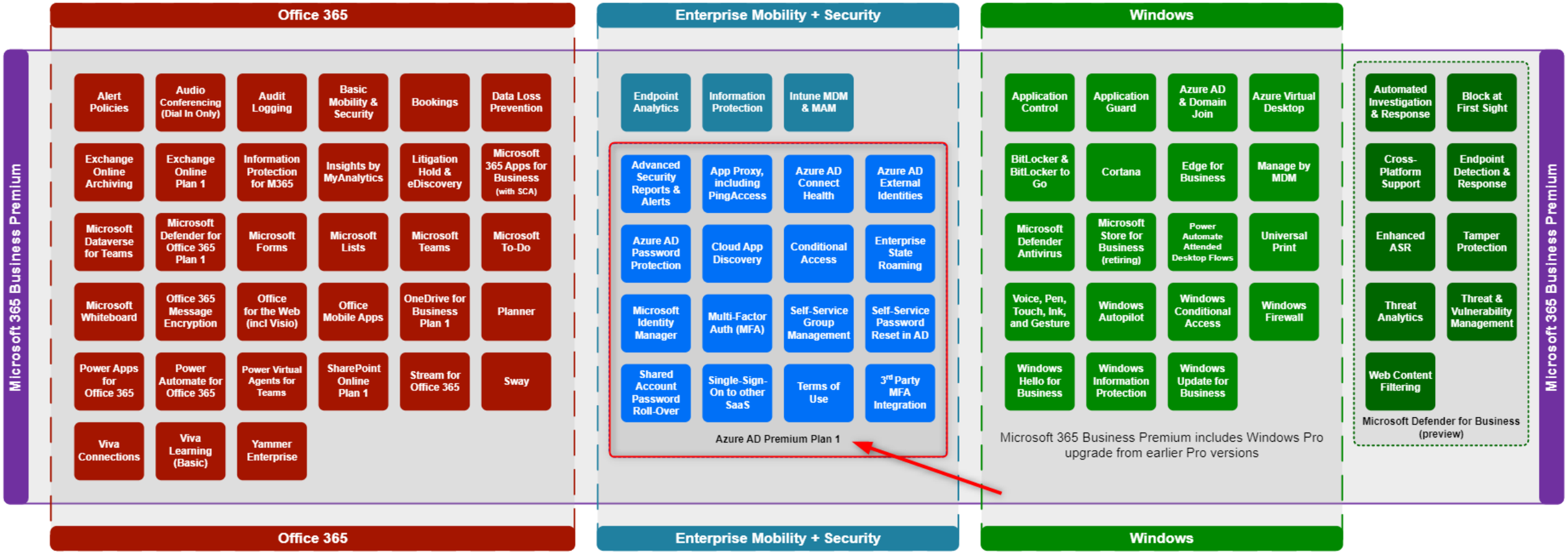
Agenda

- Identity Fundamentals
- Secure Identities & Access
- Multi-factor Authentication
- Passwordless Authentication
- Conditional Access

Microsoft 365 Business Premium

January 2022

m365maps.com



Azure AD Integration Scenarios

Cloud Identity

Azure Active Directory

Azure Active Directory

Independent cloud identities.

Synchronized Identity

Azure Active Directory

Azure AD Connect sync

Azure AD Connect cloud sync

Active Directory

Single identity, enabling a same or single sign-on experience with Password Hash Sync or Pass-through Authentication*.

Federated Identity

Azure Active Directory

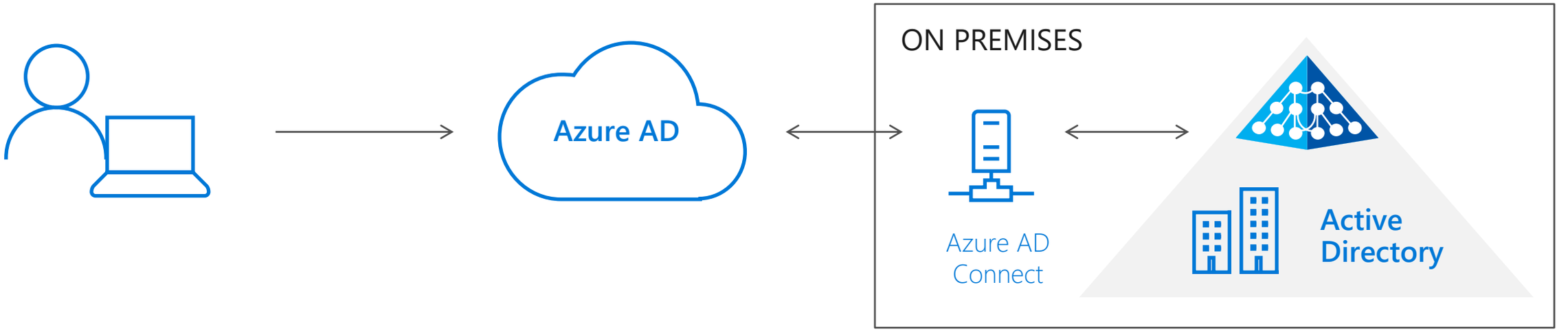
Azure AD Connect sync (cloud sync)

Federation

Active Directory

Single federated identity, enabling single-sign-on experience and on-premises multi-factor authentication options

Password Hash Sync



Great user experience

- Same passwords for cloud-based and on-premises apps
- Disaster recovery option incase other authentication methods are unavailable

Secure and compliant

- Only non-reversible hashes are stored in the cloud
- Leaked credential report available
- Integrated with Smart Lockout, Identity Protection and Conditional Access

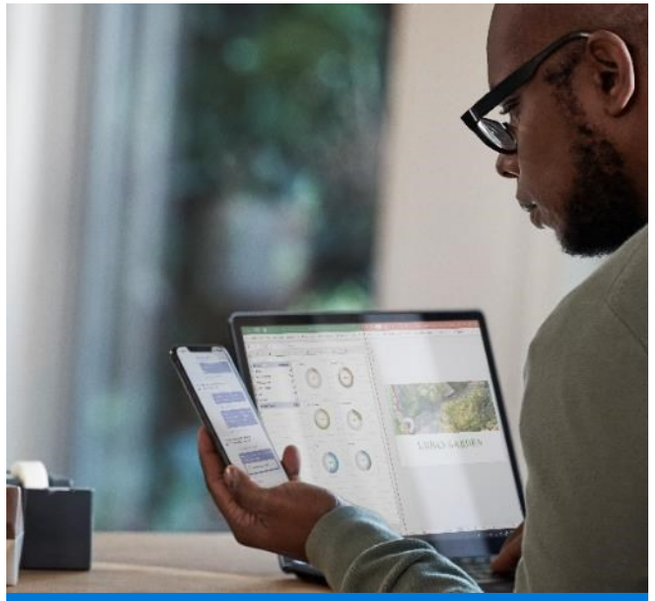
Easy to deploy & administer

- No on-premises agent needed
- Small on-premises footprint

Multi-Factor Authentication (MFA) overview

Multi-Factor Authentication

Verify user identities with strong authentication to establish trust



We support a broad range of multi-factor authentication options

Push Notification

SMS, Voice

Soft Tokens OTP

Hard Tokens OTP

Including passwordless technology

Microsoft Authenticator

Windows Hello

FIDO2 Security key

Biometrics

Multi-factor authentication prevents 99.9% of identity attacks

Azure MFA – Available versions of MFA vs. licensing

Feature	Azure AD Free - Security defaults	Azure AD Free - Azure AD Global Administrators	Office 365 Business Premium, E3, or E5	Azure AD Premium P1 or P2
Protect Azure AD tenant admin accounts with MFA	•	• (Azure AD Global Administrator accounts only)	•	•
Mobile app as a second factor	•	•	•	•
Phone call as a second factor		•	•	•
SMS as a second factor		•	•	•
Admin control over verification methods		•	•	•
Fraud alert				•
MFA Reports				•
Custom greetings for phone calls				•
Custom caller ID for phone calls				•
Trusted IPs				•
Remember MFA for trusted devices		•	•	•
MFA for on-premises applications				•

Azure AD Security defaults

Azure AD Security Defaults

Things to consider!

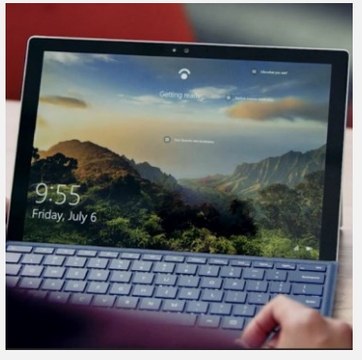
- **Authentication methods**
  - MFA only available using the authenticator app
- **Break-glass Accounts**
  - Security defaults apply to all accounts. You won't be able to deploy break glass accounts that won't be expected to perform MFA
- **Conditional Access**
  - Can't be combined with Security Defaults
  - Enabling Conditional Access policies prevents you from enabling Security Defaults
  - All these defaults can be achieved using Conditional Access
- **Blocking Legacy Authentication**
  - First need to understand if there are users that have apps using legacy auth
  - Need to make sure you are using at least Office 2013 (with registry change*) and above
  - Modern authentication needs to be enabled in the Office 365 tenant and Skype for Business Online (tenants created before August 2017 only)
  - Exchange Hybrid configurations may need to be updated to support Modern Auth

Ridurre i rischi di attacchi utilizzando Azure AD Security Defaults - ICT Power

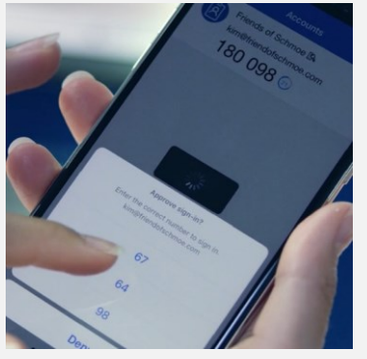
Passwordless Authentication

Changing the game with passwordless

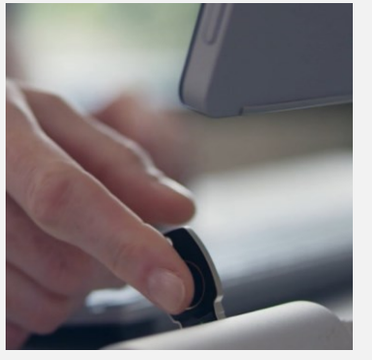
Make sign-in even more seamless and secure



Windows Hello



Microsoft Authenticator



FIDO2 Security Keys

Microsoft Authenticator

Overview

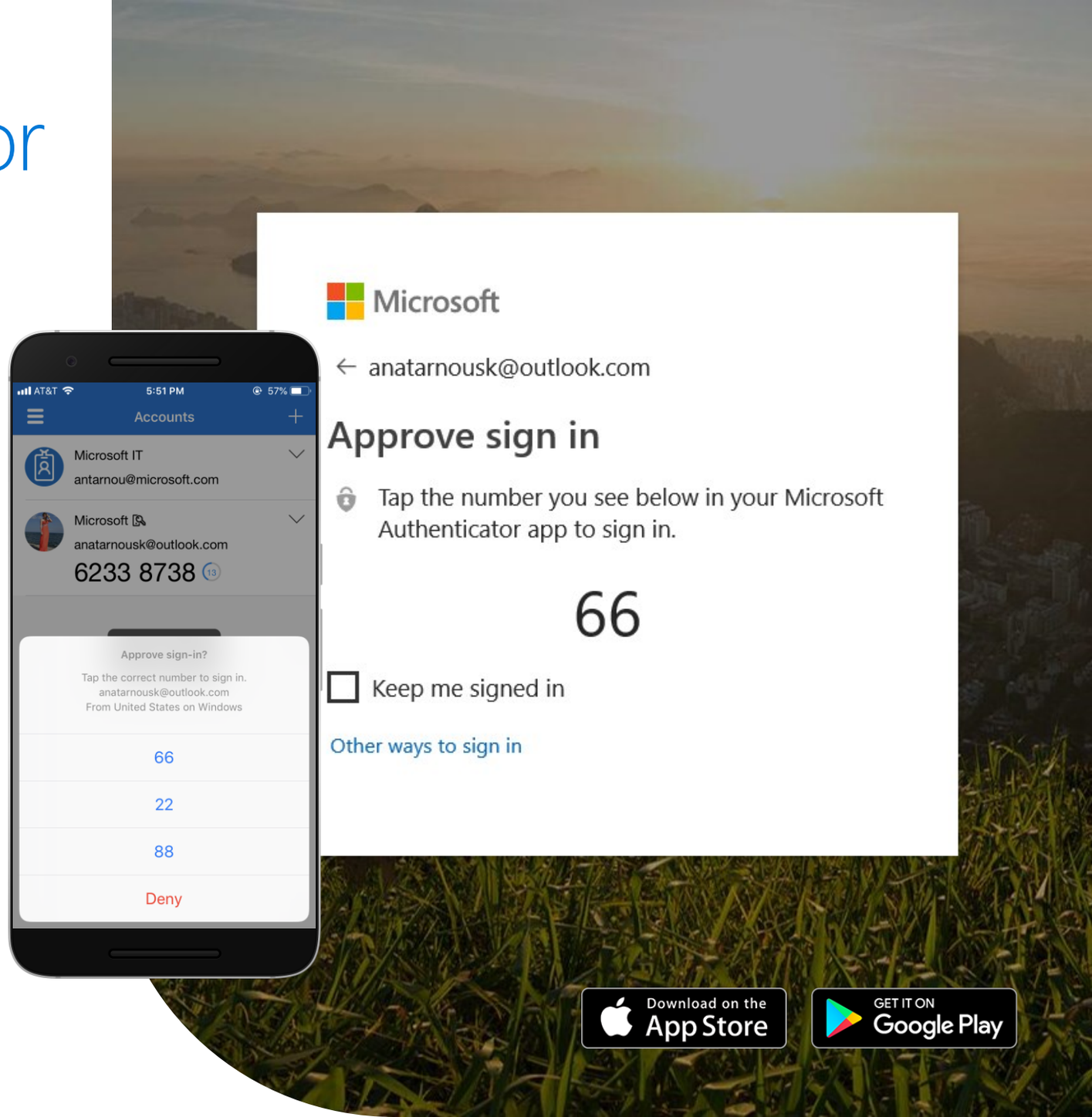
- Standards based MFA
- Supports TOTP, Push Approvals, Biometrics + Number Match

Windows 10

- Passwordless authentication – i.e. device registration in OOBE, Windows Hello provisioning

Mobile

- SSO to native mobile apps

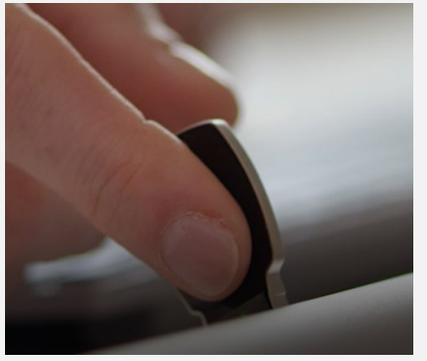


Passwordless with FIDO2 security keys

Microsoft Intelligent Security Association

Choose from additional form factors to meet business needs

USB/NFC Key



USB Biometric Key

NFC & BLE

yubico Trust the Net.

TRUSTKEY SOLUTIONS

HID

FEITIAN WE BUILD SECURITY

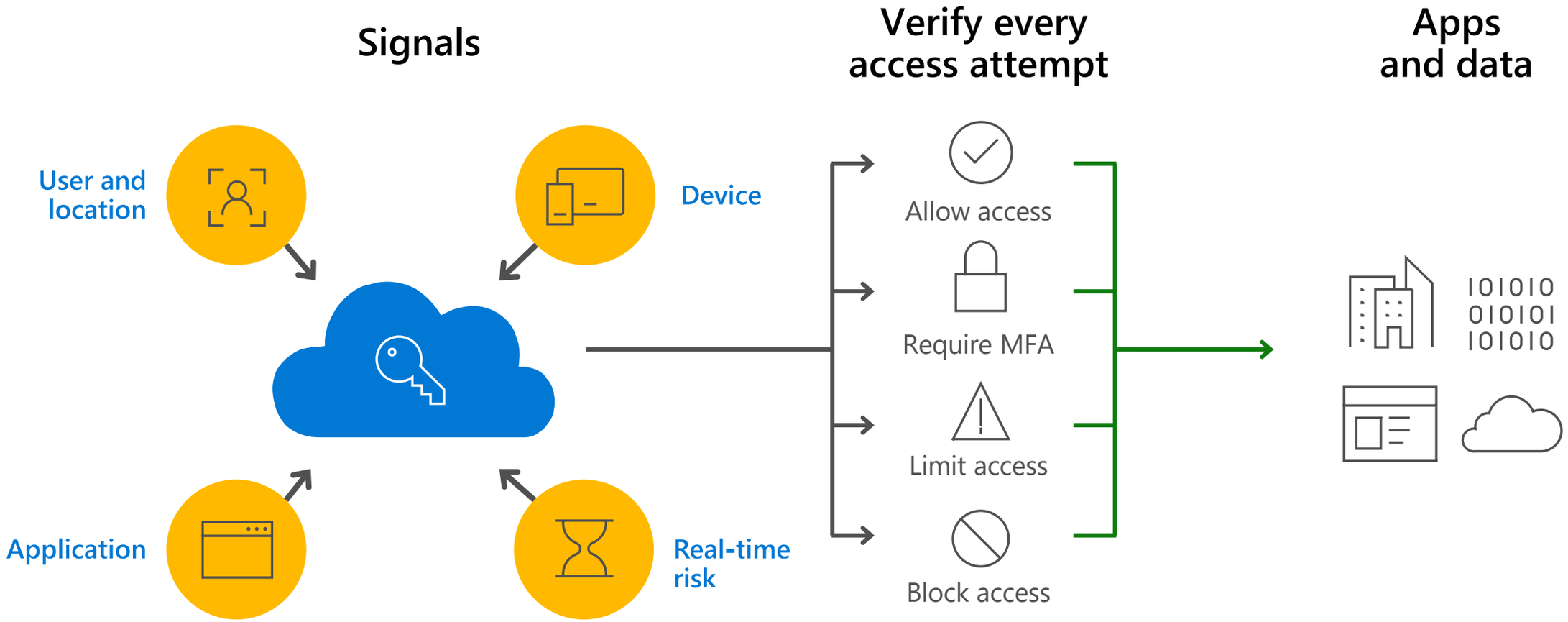
ensurity

AUTHENTREND

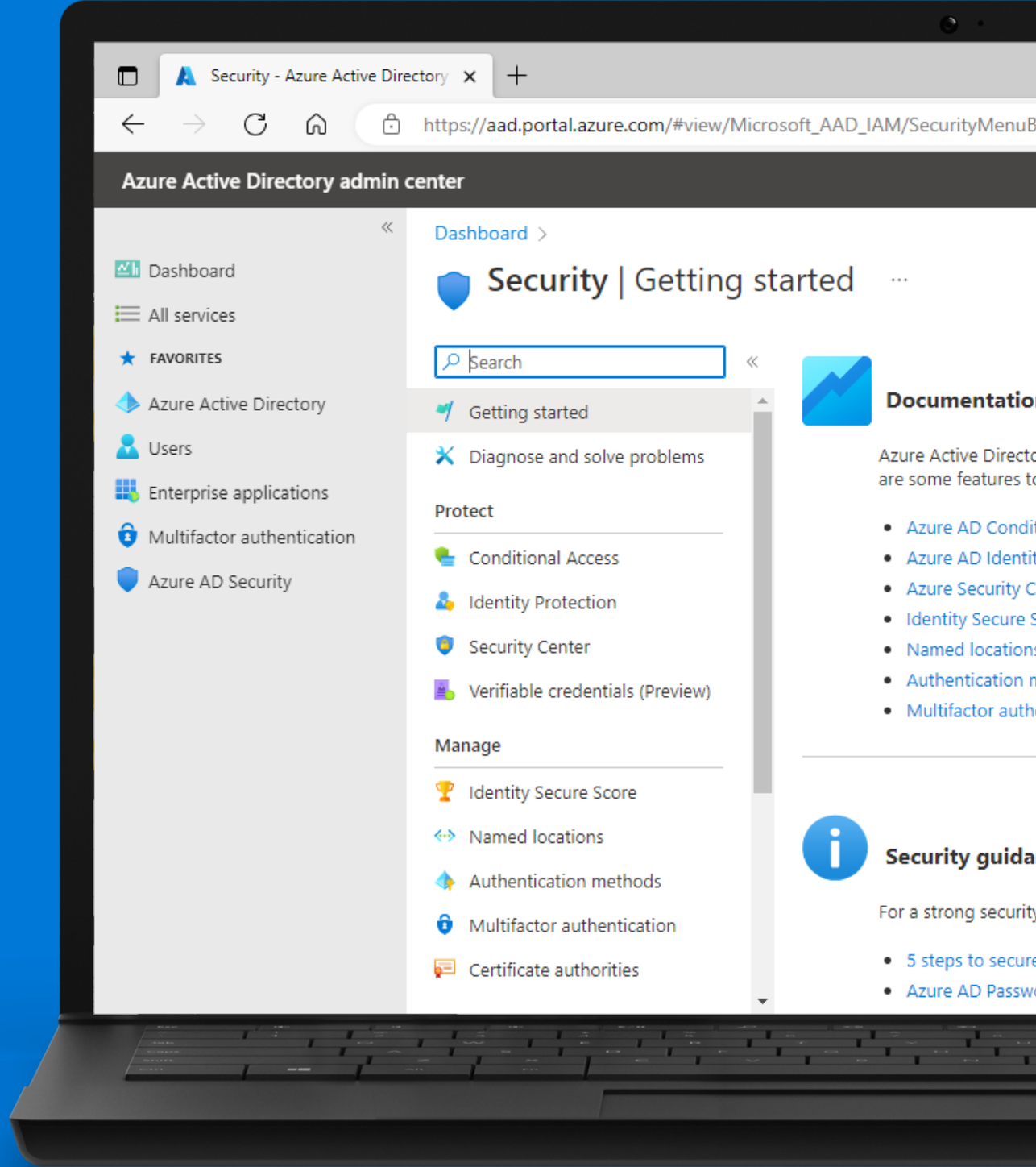
Conditional Access overview

Conditional Access – general overview

Enforce strong protection policies and risk assessment to grant access to employees and partners



DEMO


Security - Azure Active Directory
https://aad.portal.azure.com/#view/Microsoft_AAD_IAM/SecurityMenuB
Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Multifactor authentication
Azure AD Security
Dashboard
Security | Getting started
Search
Getting started
Diagnose and solve problems
Protect
Conditional Access
Identity Protection
Security Center
Verifiable credentials (Preview)
Manage
Identity Secure Score
Named locations
Authentication methods
Multifactor authentication
Certificate authorities
Documentatio
Azure Active Directo
are some features t
Azure AD Condit
Azure AD Identit
Azure Security C
Identity Secure S
Named location
Authentication m
Multifactor auth
Security guida
For a strong security
5 steps to secure
Azure AD Passwo

ICTPOWER.IT

Microsoft MVP Most Valuable Professional

Microsoft

Grazie

/nicolaferrini.it

@nicolaferrini

/nicolaferrini