ICT POWER.IT

Microsoft MVP Most Valuable Professional 2023

Microsoft

#POWERCON2023

Distribuire una soluzione Zero Trust con Microsoft Entra ID

Nicola Ferrini

Microsoft MVP

nicolaferrini

NicolaFerrini.it

nicolaferrini

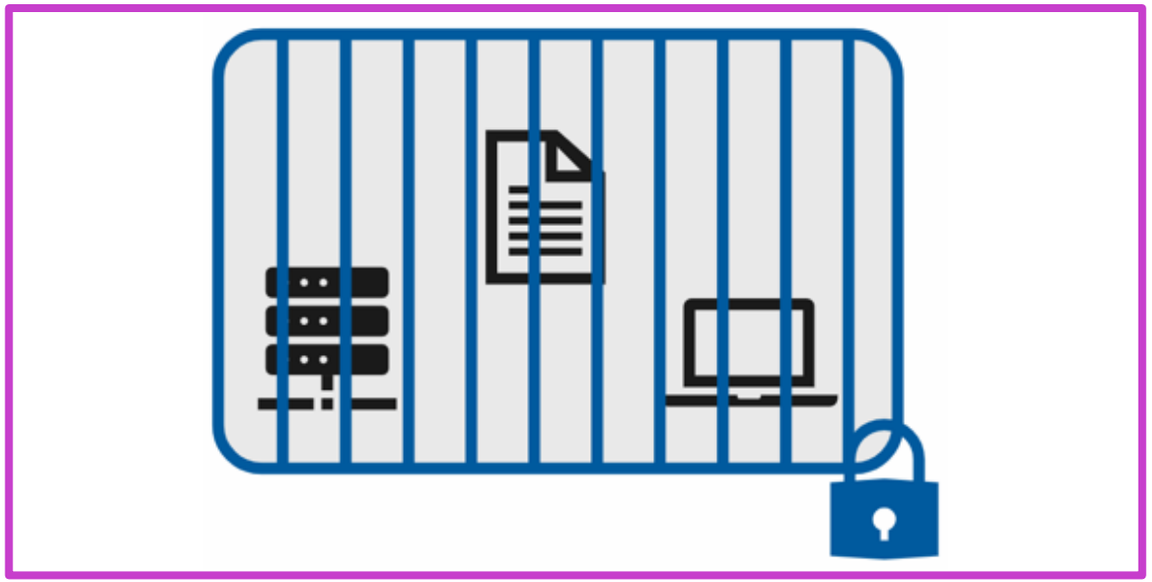
Source: Gartner

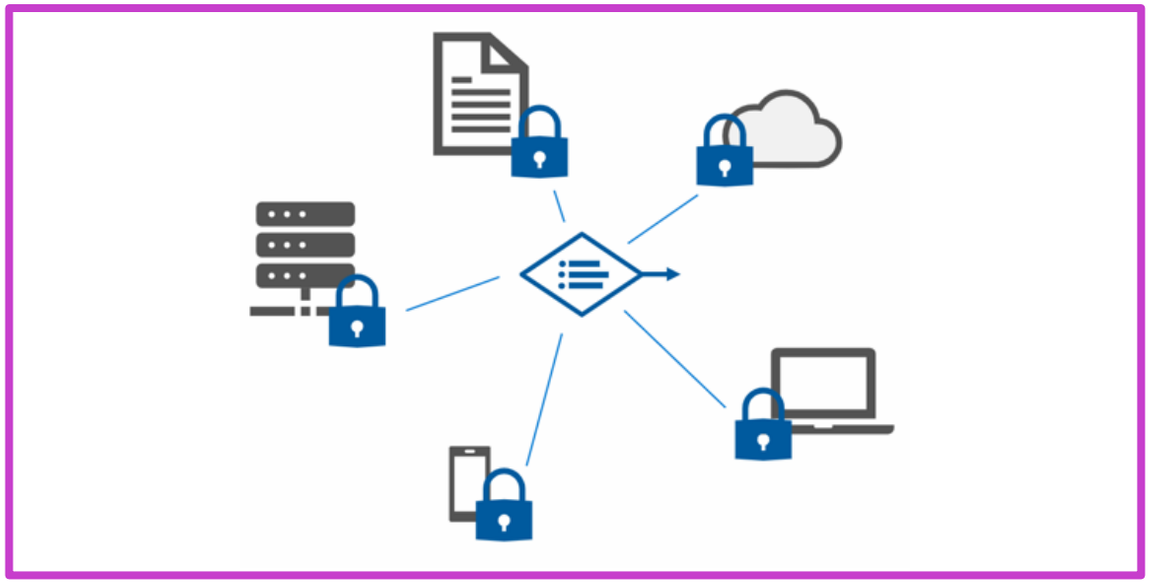
Microsoft named a Leader in 2023 Gartner® Magic Quadrant™ for Access Management for the 7th year

"Gartner® view of the market is focused on transformational technologies or approaches delivering on the future needs of end users."

[Microsoft is a Leader in 2023 Gartner Magic Quadrant for Access Management | Microsoft Security Blog]

Secure assets where they are with Zero Trust





- **Classic approach –** Restrict everything to a “secure” network
- **Zero Trust –** Protect assets anywhere with central policy

Il modello Zero Trust per la sicurezza delle infrastrutture informatiche - ICT Power

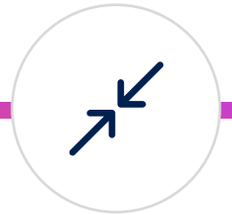
Microsoft Zero Trust Principles

Guidance for technical architecture

Verify explicitly

Always validate all available data points including

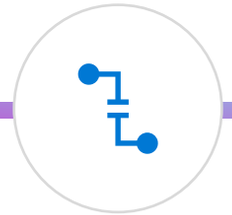
- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies



Use least privilege access

To help secure both data and productivity, limit user access using

- Just-in-time (JIT)
- Just-enough-access (JEA)
- Risk-based adaptive polices
- Data protection against out of

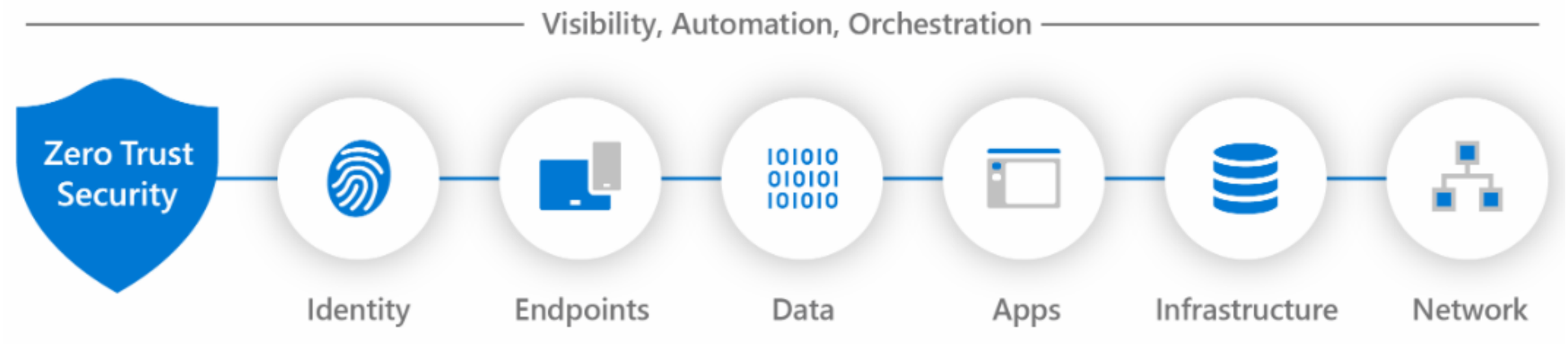


Assume breach

Minimize blast radius for breaches and prevent lateral movement by

- Segmenting access by network, user, devices, and app awareness
- Encrypting all sessions end to end
- Use analytics for threat detection, posture visibility and improving defenses

Deploying Zero Trust solutions



Secure identity with Zero Trust

Identities—whether they represent people, services, or IoT devices—define the Zero Trust control plane. When an identity attempts to access a resource, verify that identity with strong authentication, and ensure access is compliant and typical for that identity. Follow least privilege access principles.

Why use an identity?

To be able to prove what we are	Authentication
To get permission to do something	Authorization
To report on what was done	Auditing
To be able to (self) administer an identity	Administration

Authentication

- User sign-on experience
- Trusted source(s)
- Federative protocols
- Level of assurance

Authorization

- How and where are authorizations handled
- Can a user access the resource and what can they do when they access it?

Administration

- Single view management
- Application of business rules
- Automated requests, approvals, and access assignment
- Entitlement management

Auditing

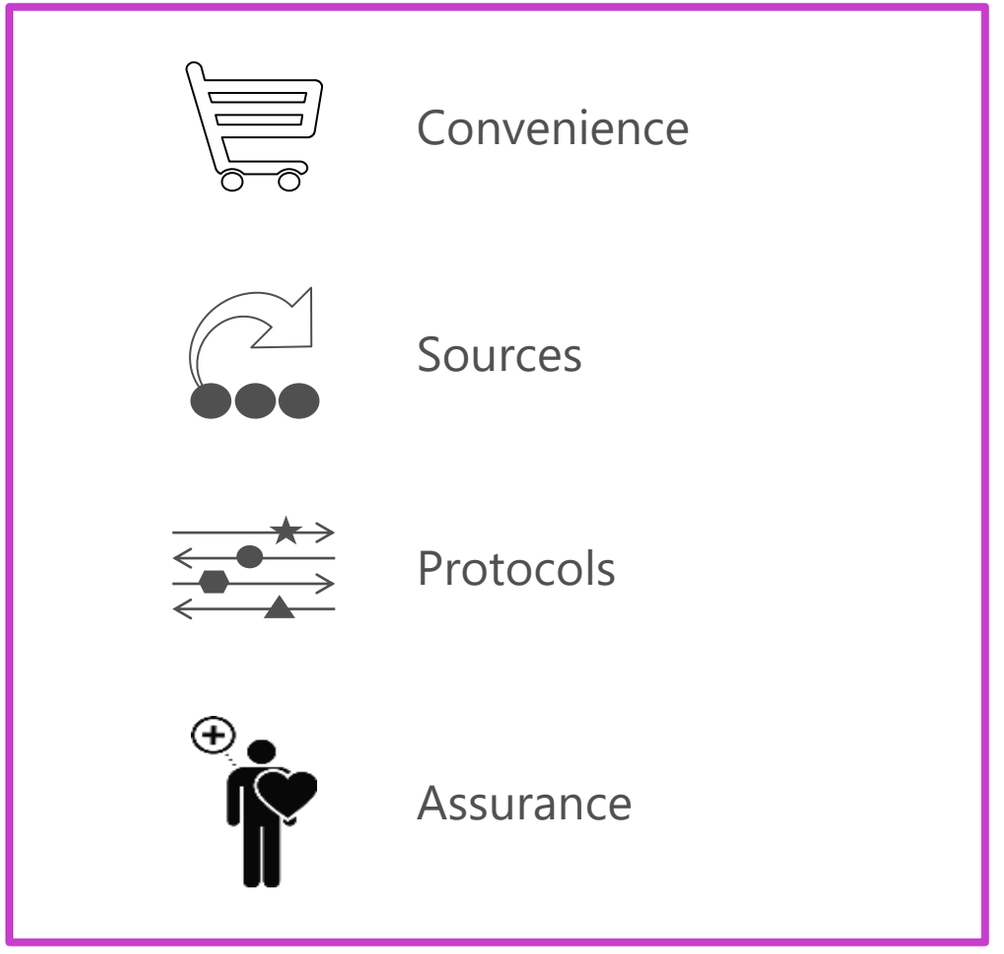
- Track who does what, when, where and how
- Focused alerting
- In-depth collated reporting
- Governance & compliance

Authentication

Validating the identity is who they proclaim to be while providing an appropriate level of validation and security throughout the authentication transaction.

Identity Authentication Provides

- Flexible, standards compliant, authentication that integrates across organizations
- Integration of disparate sources, applications, and protocols
- Employs many different industry standard methods of validation and assurance



Authorization

Covers what an identity can access and what are they allowed to do once they gain access.

Identity Authorization provides:

- Methods of assigning entitlement allowing for increased security and less administration
- Ability to manage policy control
- Simplify enforcement by standardizing on a common approach

Entitlement Type

Access Policies

Enforcement

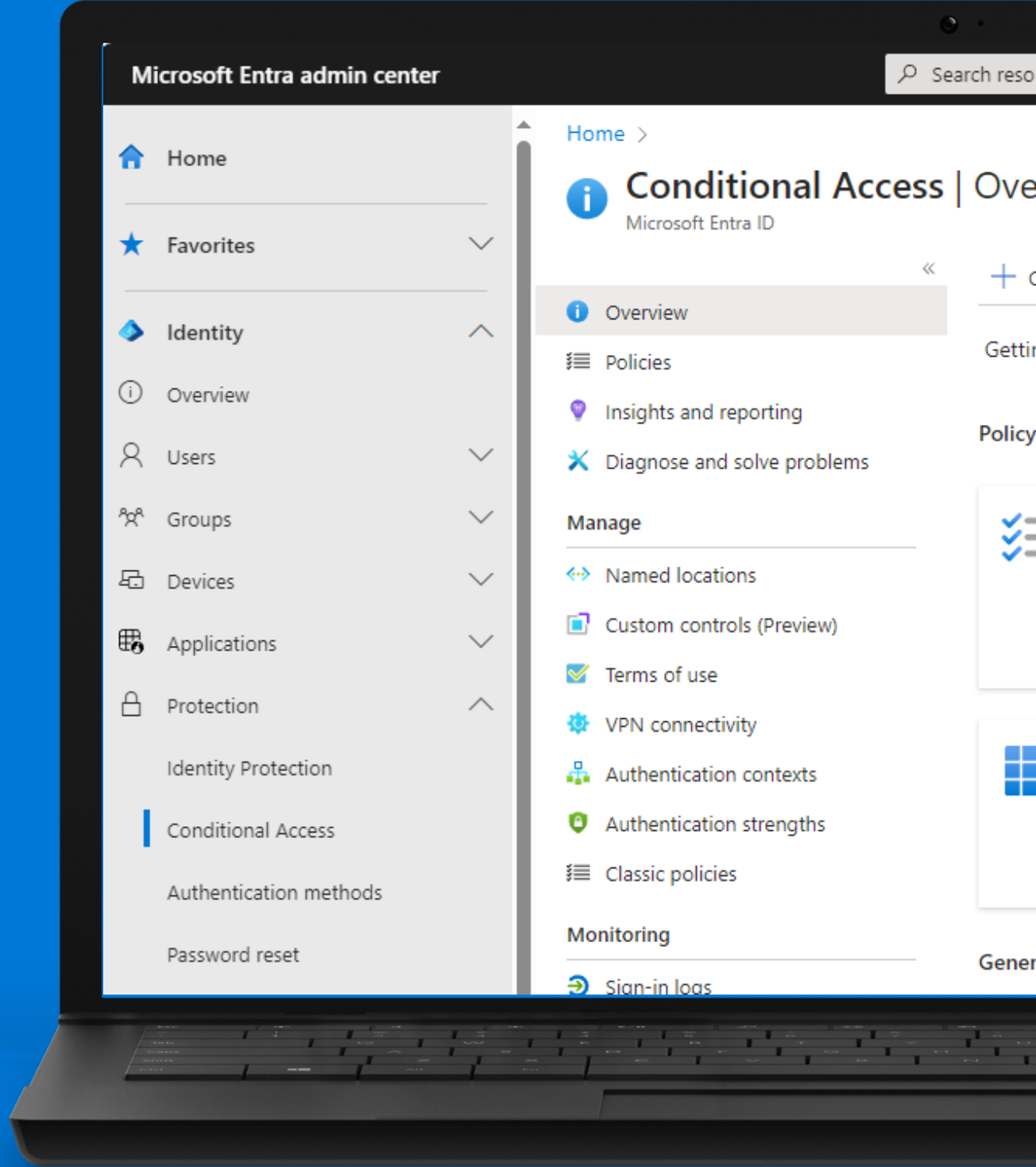
Common authorization approaches

Authorization type	Description
Access Control Lists (ACLs)	Explicit list of resource access. Very granular, hard to maintain.
Role-based access control (RBAC)	Grant access based on the users role.
Attribute-based access control (ABAC)	Grant access based on one or more attributes of the users current environment and identity.
Policy-based access control (PBAC)	Role and policy combined to determine user access.

Microsoft Entra ID can support any of these methods and others, based on your business and security goals.

- Creare ruoli personalizzati in Azure Role Based Access Control (RBAC) - ICT Power
- Introduzione a Azure attribute-based access control (Azure ABAC) - ICT Power
- Come implementare il Policy-Based Access Control (PBAC) in Microsoft Entra ID - ICT Power

DEMO


Microsoft Entra admin center
Search reso
Home
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Home
Conditional Access | Ove
Microsoft Entra ID
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies
Monitoring
Sign-in logs

Conclusions

- Connect to Microsoft Entra ID and federate with on-premises identity systems
- Integrate all your applications with Microsoft Entra ID
- Verify explicitly with strong authentication
- Use Conditional Access policies
- Secure privileged access with Privileged Identity Management
- Use passwordless authentication to reduce the risk of phishing and password attacks
- Manage entitlement

ICT POWER.IT

Microsoft MVP Most Valuable Professional 2023

Microsoft

Grazie

Nicola Ferrini
Microsoft MVP

nicolaferrini
NicolaFerrini.it
nicolaferrini