BSG

Microsoft 365 Security per SMB’s

Tommaso Cornelli – Partner BSG

Grazie a:

ASSEPRIM
FEDERAZIONE NAZIONALE SERVIZI PROFESSIONALI PER LE IMPRESE

Chi sono?

Tommaso Cornelli

CTO @ BSG

t.cornelli@bsg.it

Di cosa mi occupo:
Direzione practice servizi Cloud e Modern Work in BSG

Technical Advisory e presale progetti IAAS-PAAS-SAAS (Azure, AWS)
Technical Advisory e presale progetti M365 (AAD, EXO, SPO, Teams, PP)
Technical Advisory e presale progetti security MWP

Di cosa parleremo oggi?

Obiettivi di oggi

Approfondiremo insieme il concetto di responsabilità condivisa nel rapporto con i cloud provider e esploreremo le funzionalità di Microsoft Defender di Microsoft 365 con l'obiettivo di fornirti gli strumenti necessari a mettere in sicurezza il patrimonio più importante della tua azienda... I dati!

Cloud Services definition

BSG

What is the Cloud?

Cloud Computing Services

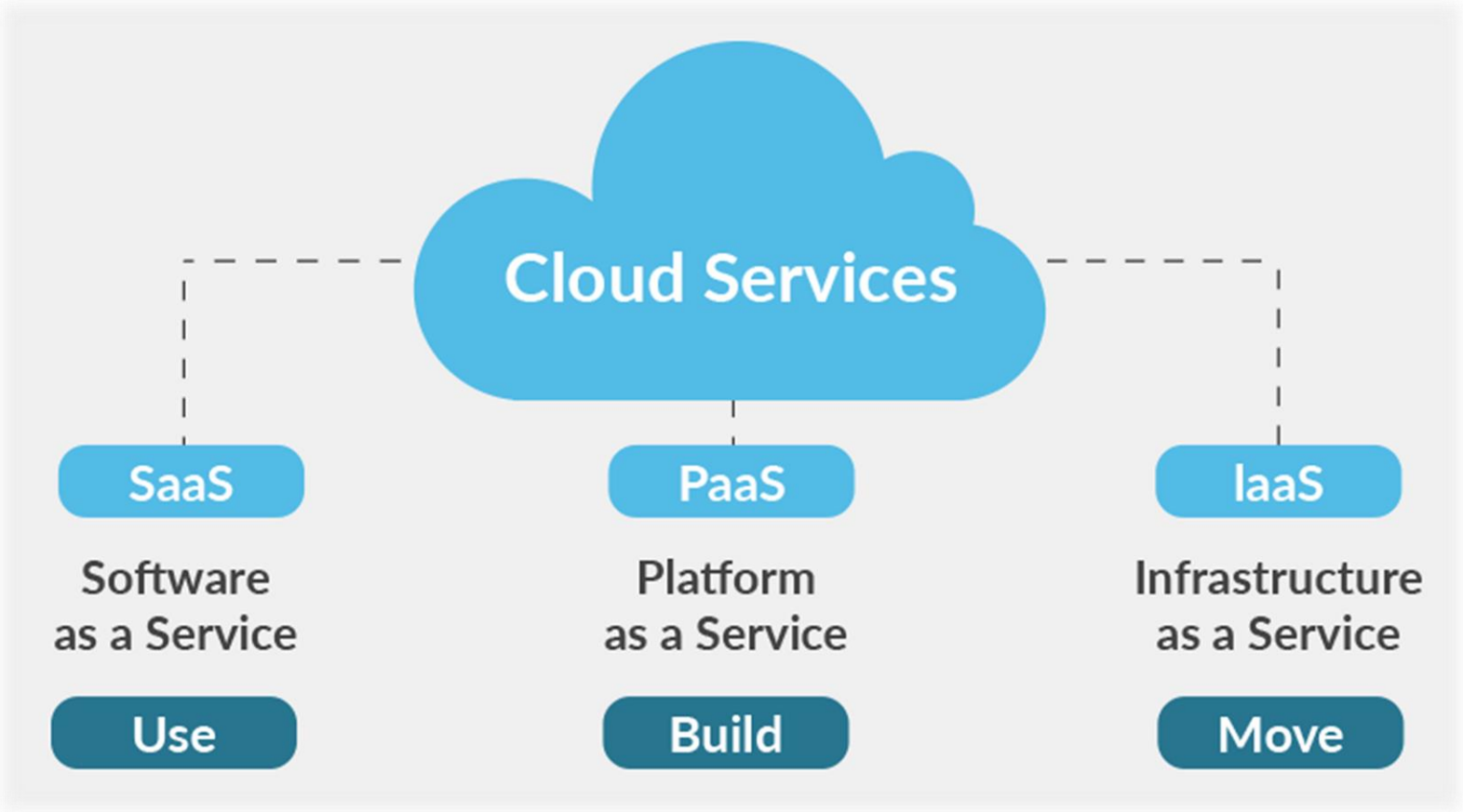
Cloud services definition

BSG

The ability to rent computing resources on demand

Il concetto di responsabilità condivisa

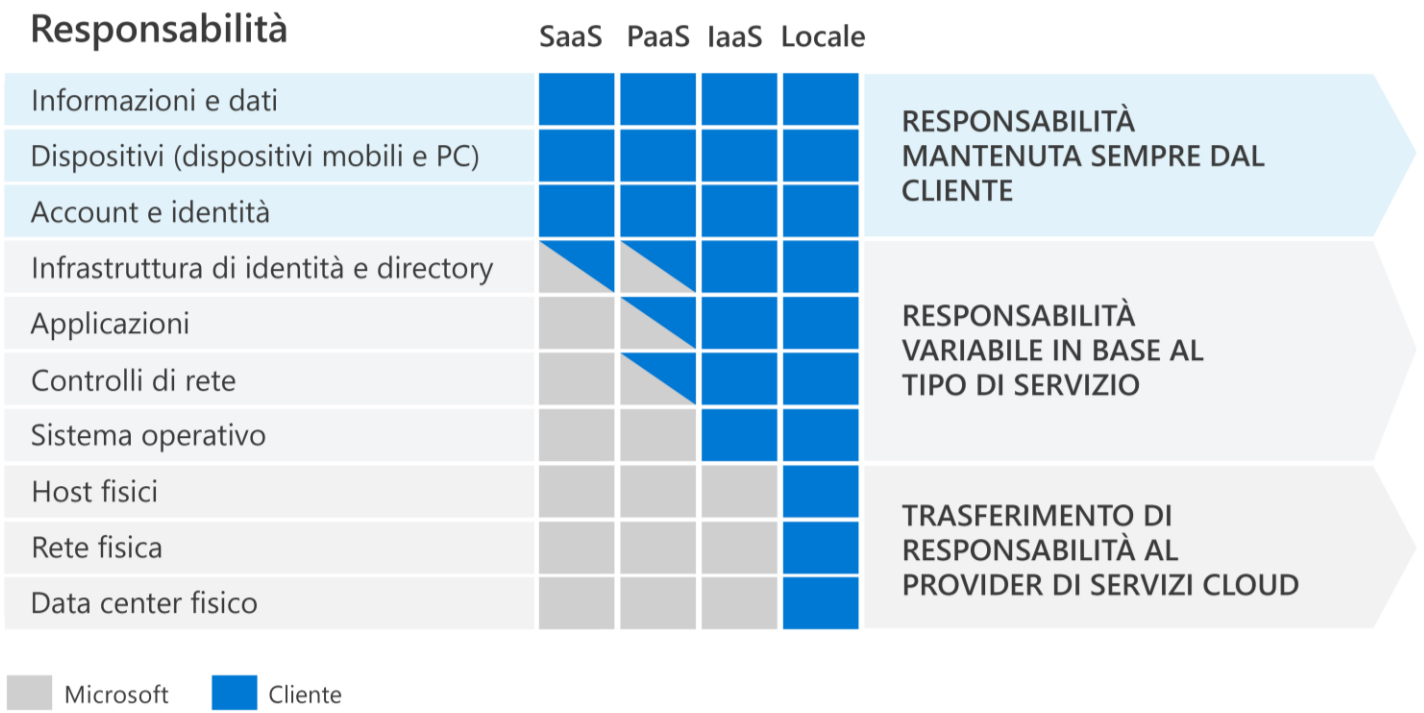
Cloud Computing Services



Lo shared responsibility Model

BSG

Modello di responsabilità condivisa



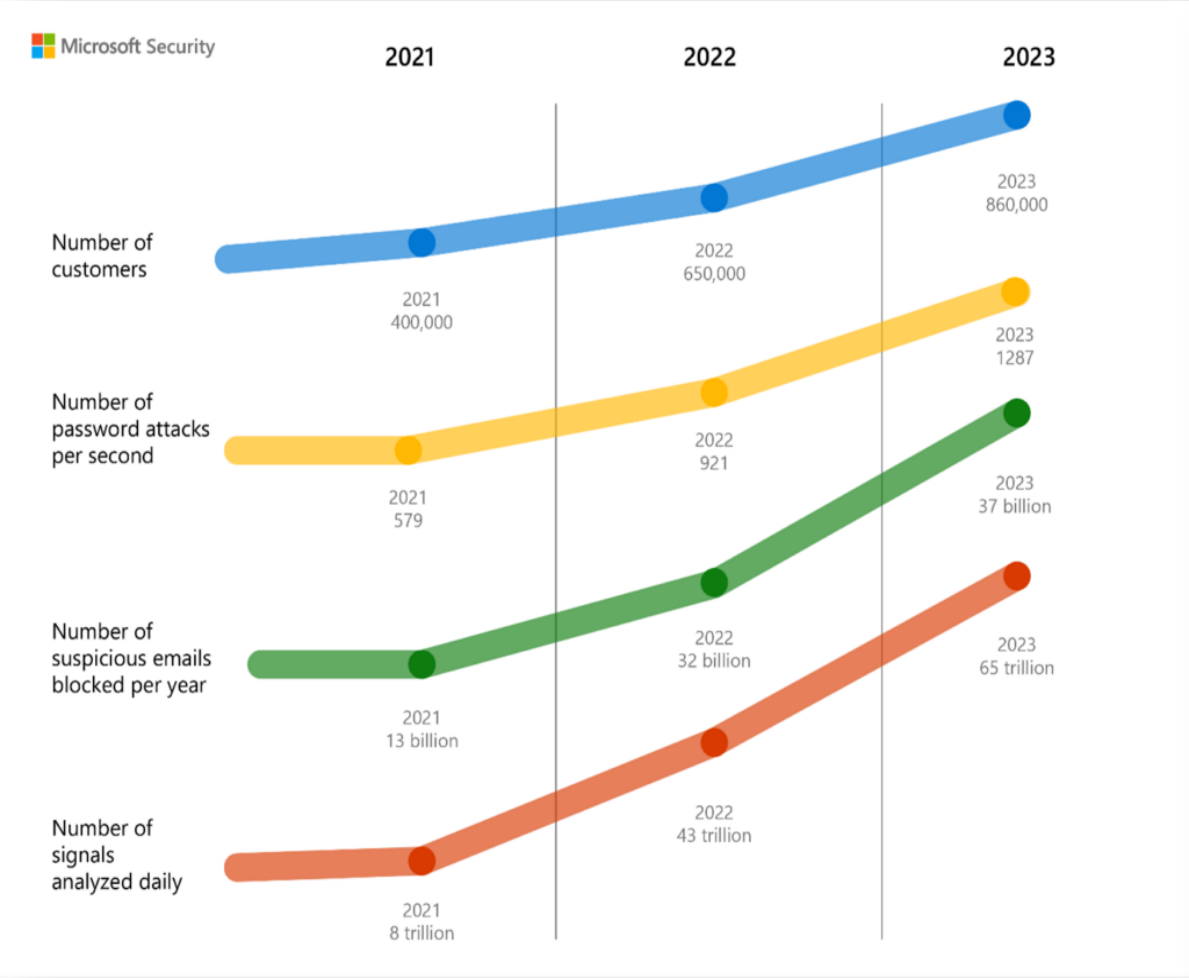
BSG

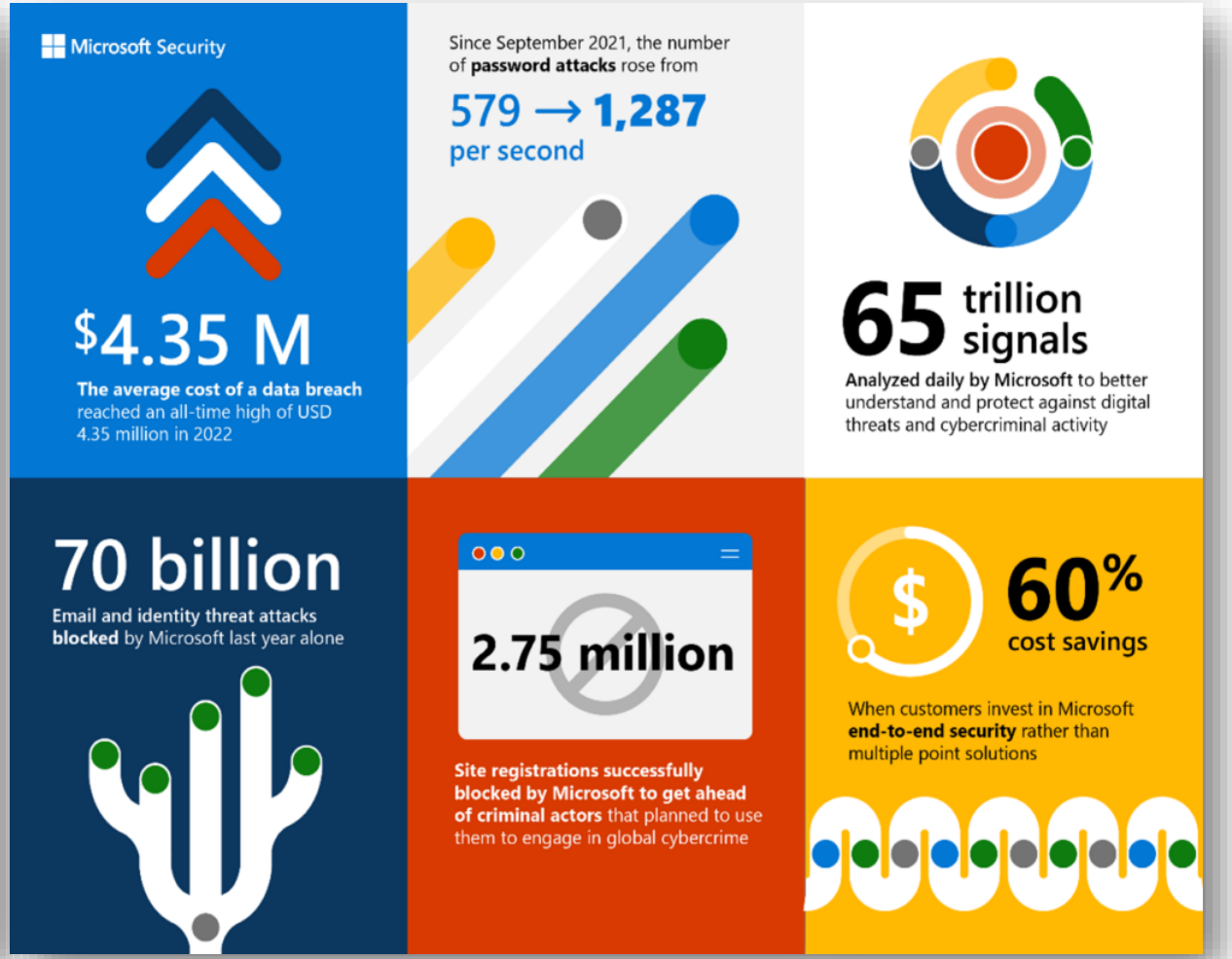
Microsoft 365, rappresenta una soluzione SAAS completa di strumenti di produttività basati su cloud sviluppati da Microsoft.

Questa suite si è evoluta offrendo il passaggio da un pacchetto software installabile tramite CD a un servizio dinamico e agile ospitato sul cloud.

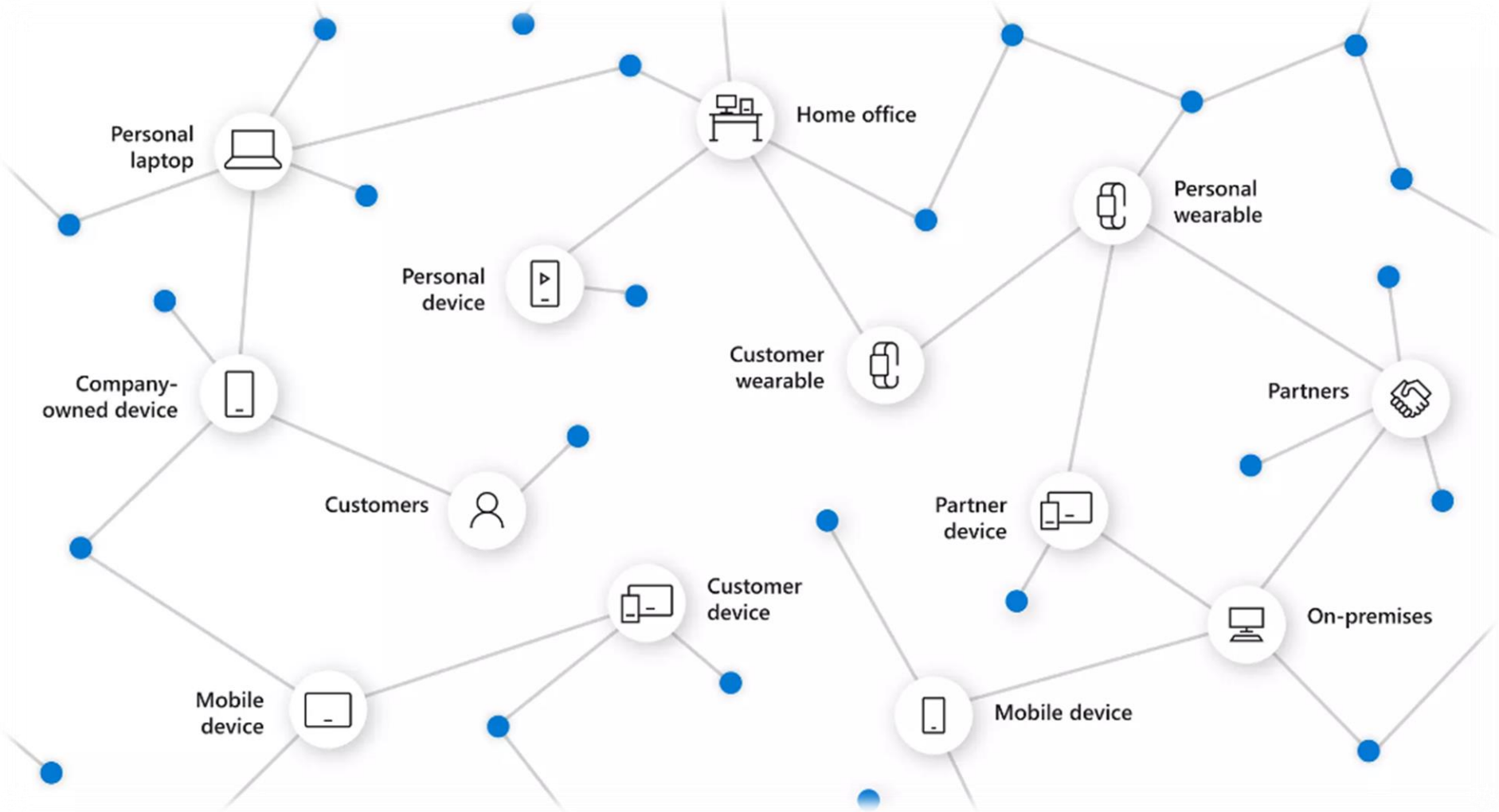
E quindi la security del tenant è un mio problema?

Security Challenges

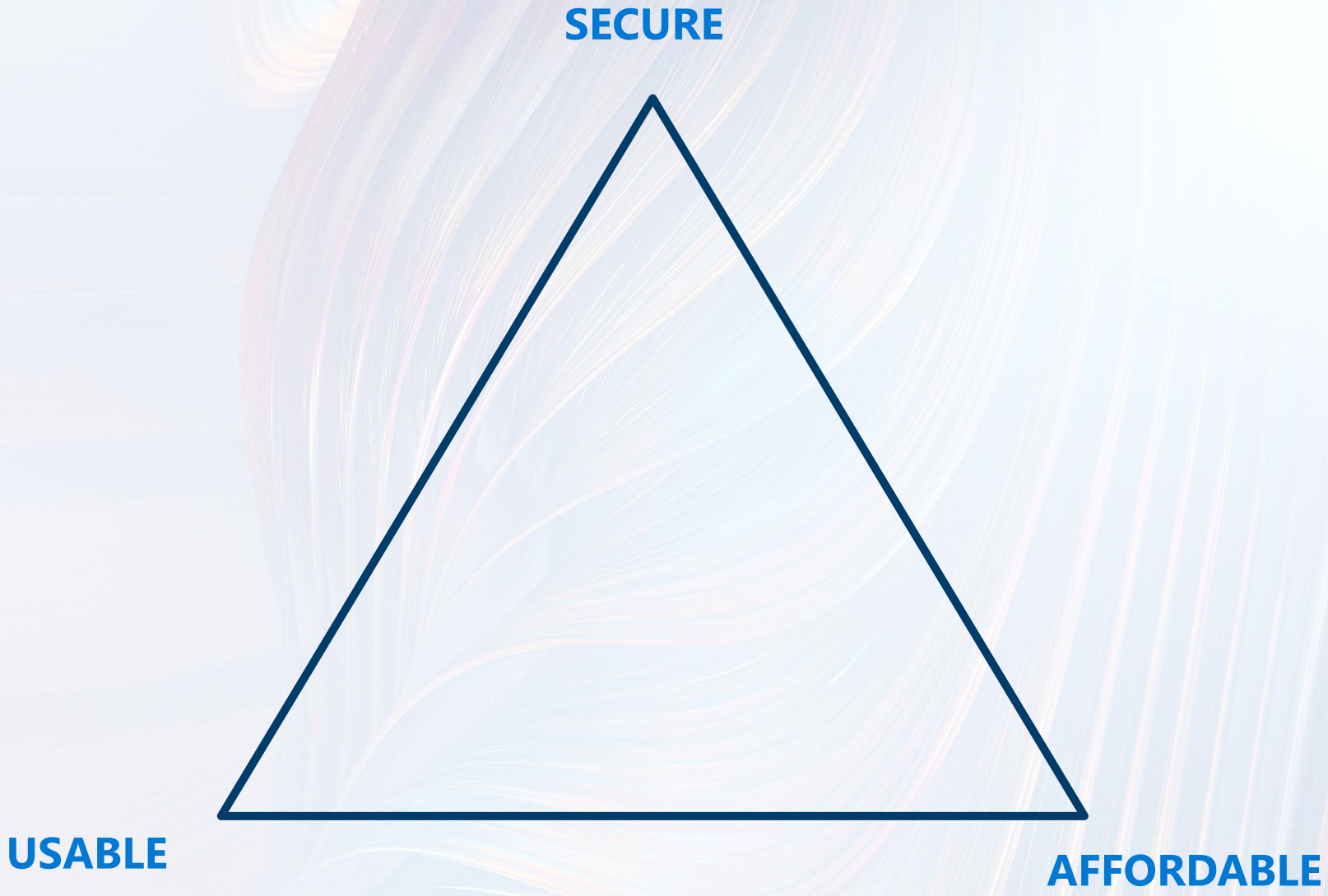




Security Challenges



Security Dilemma



Approccio alla soluzione

Zero trust architecture

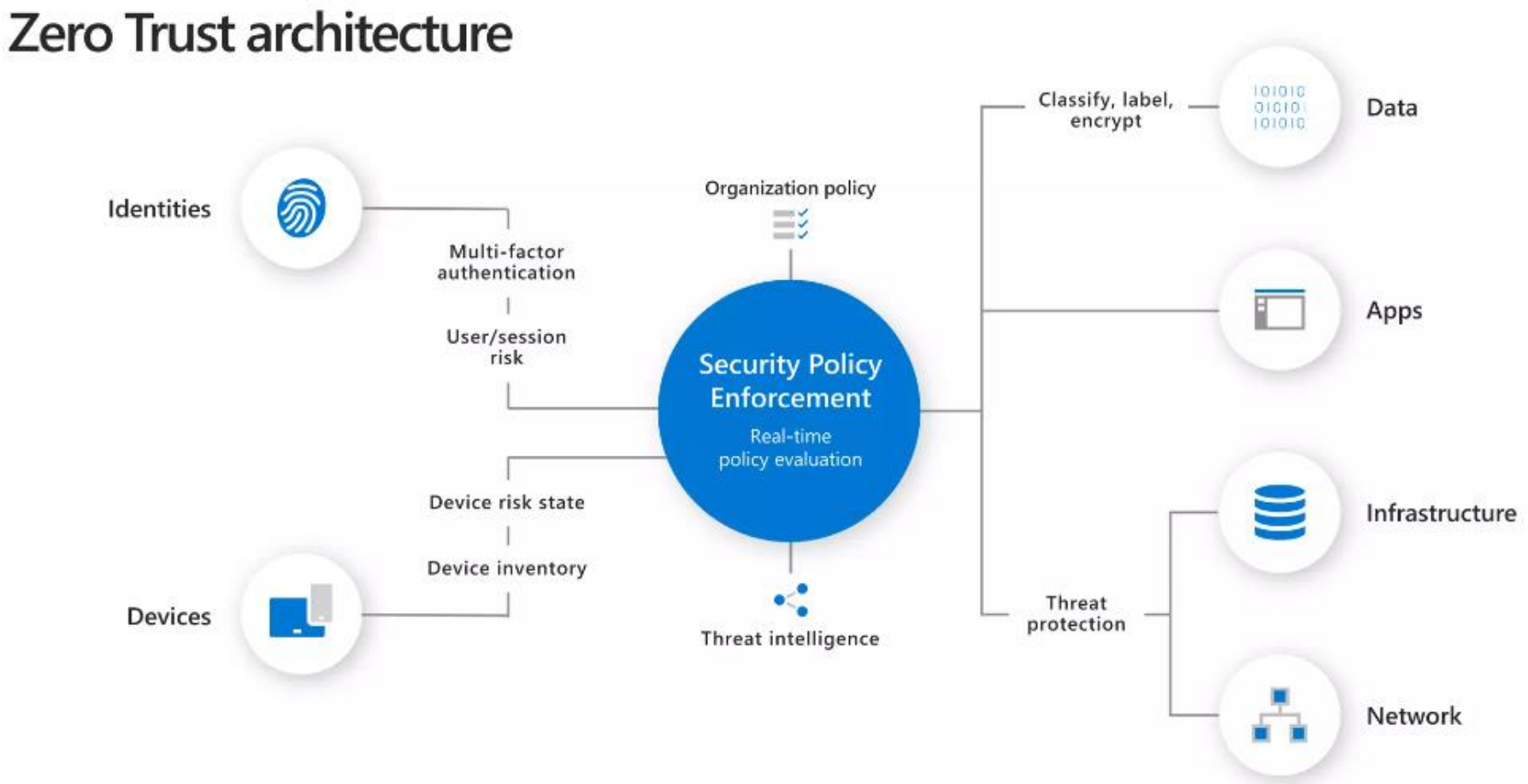
Zero trust architecture

Il modello Zero Trust presuppone che tutto sia in una rete aperta e non attendibile, anche le risorse protette dai firewall della rete aziendale. Il modello Zero Trust opera sul principio "**nulla è attendibile, verifica tutto"**.

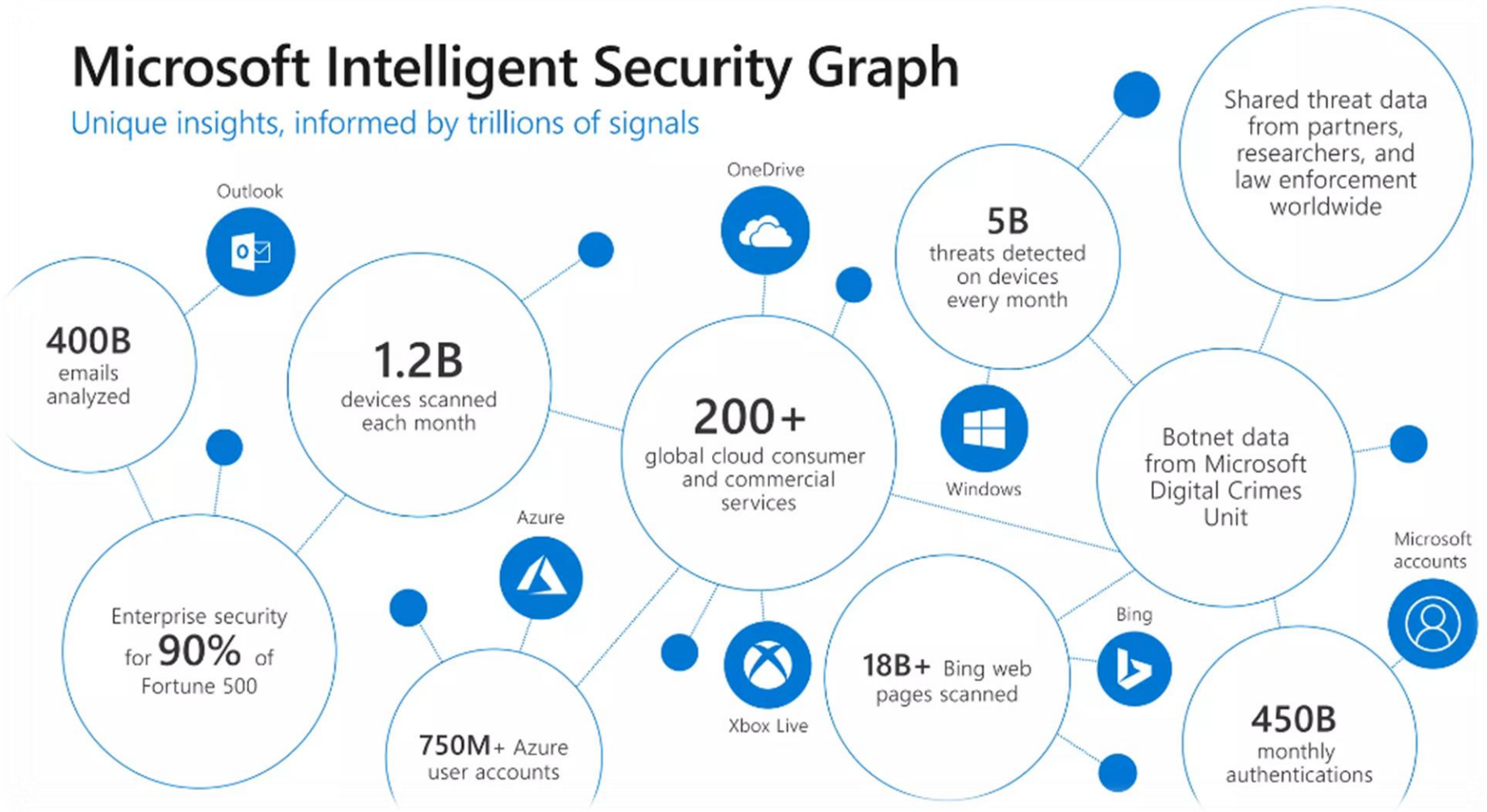
Il fatto che gli utenti malintenzionati riescano ad aggirare i controlli di accesso convenzionali ha messo fine a qualsiasi illusione sul fatto che le strategie di sicurezza tradizionali siano sufficienti. Il fatto di non considerare più attendibile l'integrità della rete aziendale rafforza la sicurezza.

In pratica, questo significa non dare più per scontato che una password sia sufficiente per convalidare un utente, ma prevedere l'aggiunta dell'autenticazione a più fattori per implementare controlli aggiuntivi. Invece di concedere l'accesso a tutti i dispositivi nella rete aziendale, agli utenti viene consentito l'accesso solo alle applicazioni o ai dati specifici necessari.

Zero trust architecture per Microsoft



Perché Microsoft?

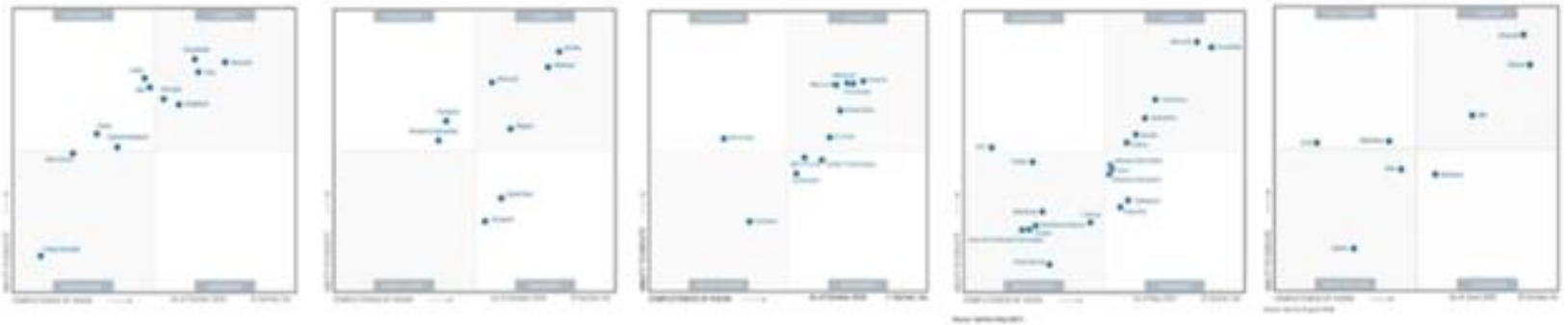


Perché Microsoft?

Gartner
Magic Quadrant

Gartner

Microsoft Security — a Leader in Gartner Magic Quadrant reports



Access Management | Cloud Access Security Brokers | Enterprise Information Archiving | Endpoint Protection Platforms | Unified Endpoint Management

"Gartner "Magic Quadrant for Access Management," by Michael Kelley, Abhyuday Data, Henrique, Toronto, November 2020
"Gartner "Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020
"Gartner "Magic Quadrant for Enterprise Information Archiving," by Michael Hoech, Jeff Vogel, October 2020
"Gartner "Magic Quadrant for Endpoint Protection Platforms," by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021
"Gartner "Magic Quadrant for Unified Endpoint Management," by Dan Wilson, Rich Doherty, Rob Smith, Chris Silva, Manjunath Bhat, August 2020

These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

Perché Microsoft?

FORRESTER

FORRESTER®

Microsoft Security — a Leader in 7 Forrester Wave reports

Security Analytics Platform | Enterprise Email Security | Enterprise Detection & Response | Endpoint Security Software as a Service | Unified Endpoint Management | Unstructured Data Security Platforms | Cloud Security Gateways

1. The Forrester Wave™: Security Analytics Platforms, Q4 2020, Joseph Blankenship, Claire O'Malley, December 2020
2. The Forrester Wave™: Enterprise Email Security, Q2 2021, Joseph Blankenship, Claire O'Malley, April 2021
3. The Forrester Wave™: Enterprise Detection And Response, Q1 2020, Josh Zelonis, March 2020
4. The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021, Chris Sherman, May 2021
5. The Forrester Wave™: Unified Endpoint Management, Q4 2018, Andrew Hewitt, November 2018
6. The Forrester Wave™: Unstructured Data Security Platforms, Q2 2021, Heidi Shey, May 2021
7. The Forrester Wave™: Cloud Security Gateways, Q2 2021, Andras Cser, May 2021

Delivering device security across platforms

Endpoints and servers[1]

Windows

macOS

Mobile devices[2]

iOS

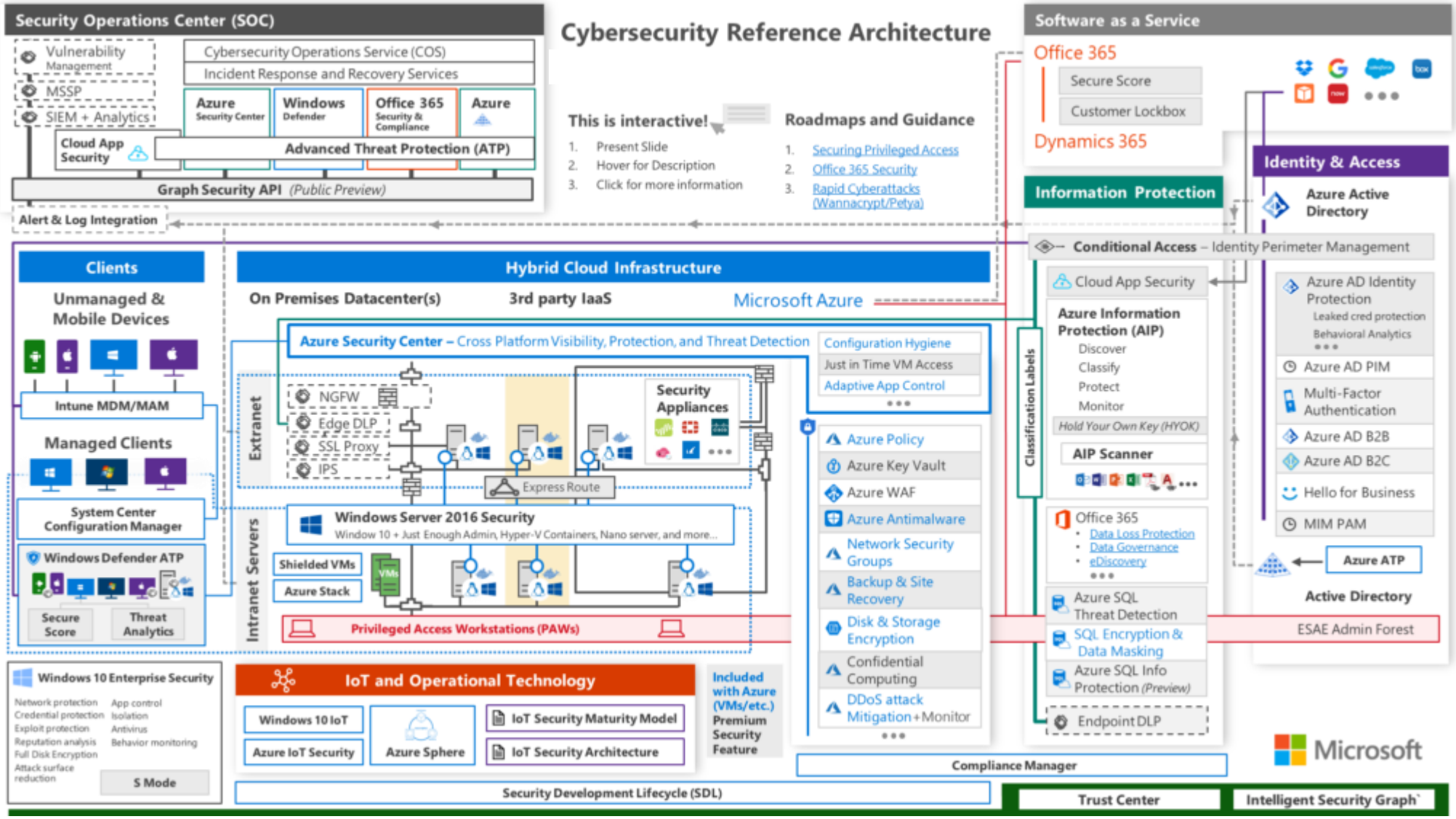
Virtual desktops

Azure Virtual Desktop

Windows 365

[1]Add-on for server support is now available.
[2]iOS and Android security without Intune for MDB standalone now GA. Intune Plan 1 is included in Microsoft 365 Business Premium. See Documentation for detail.

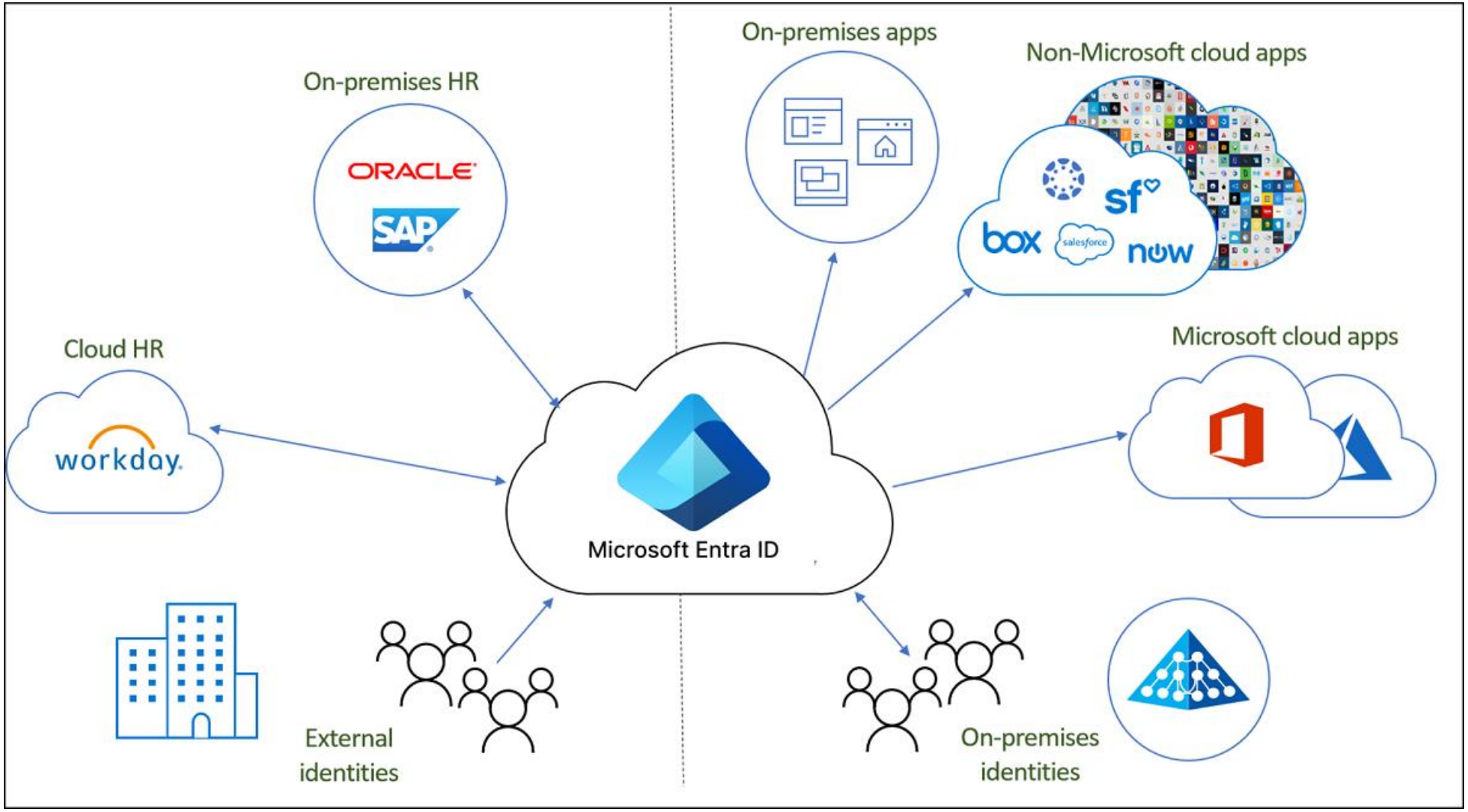
Il security stack Microsoft



Ok, ma dove comincio?


Identity is at the center of security

Identity is at the center of security



>353

Millioni

Di account compromessi nel 2023

>99.7%

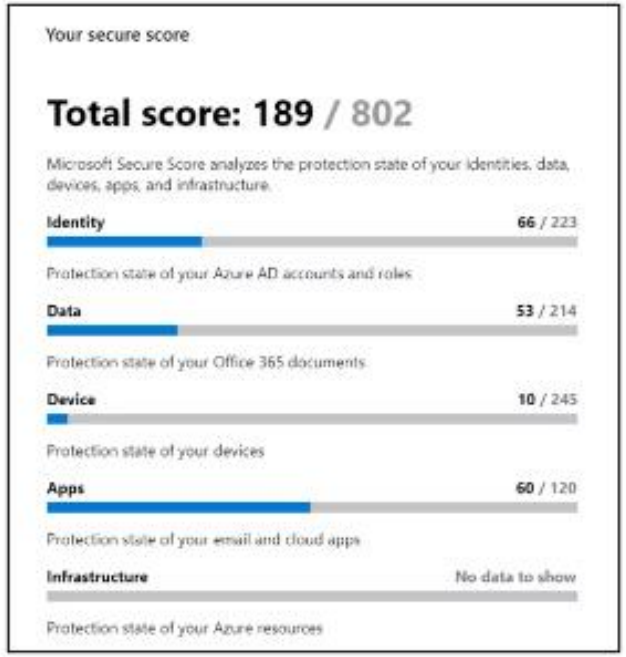
Degli account compromessi nel 2023

Non avevano MFA attivo

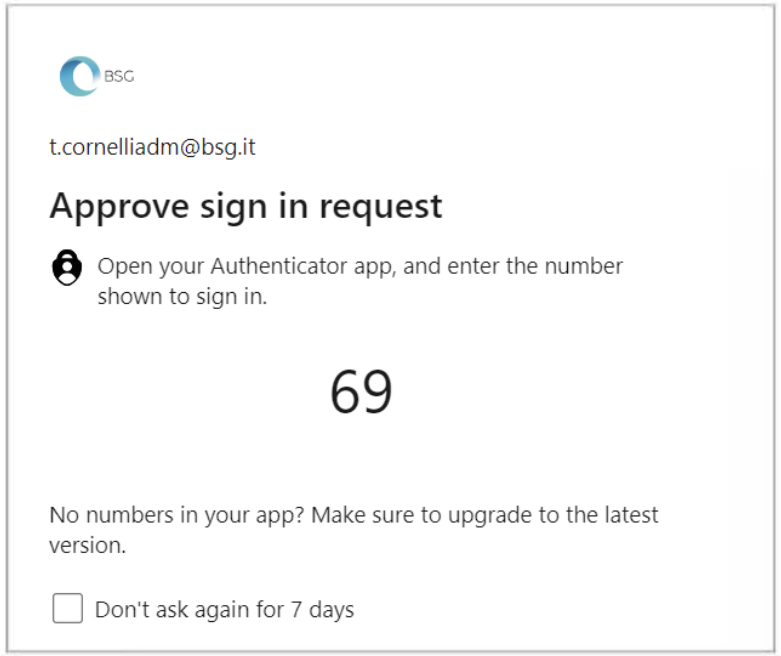
Source: statista

I primi passi...

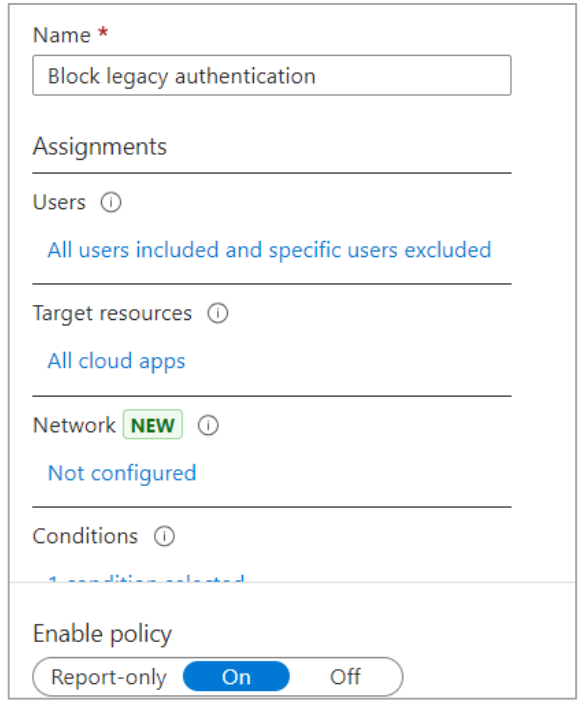
I primi 3 step fondamentali



Sfrutta il secure score per definire la tua security baseline



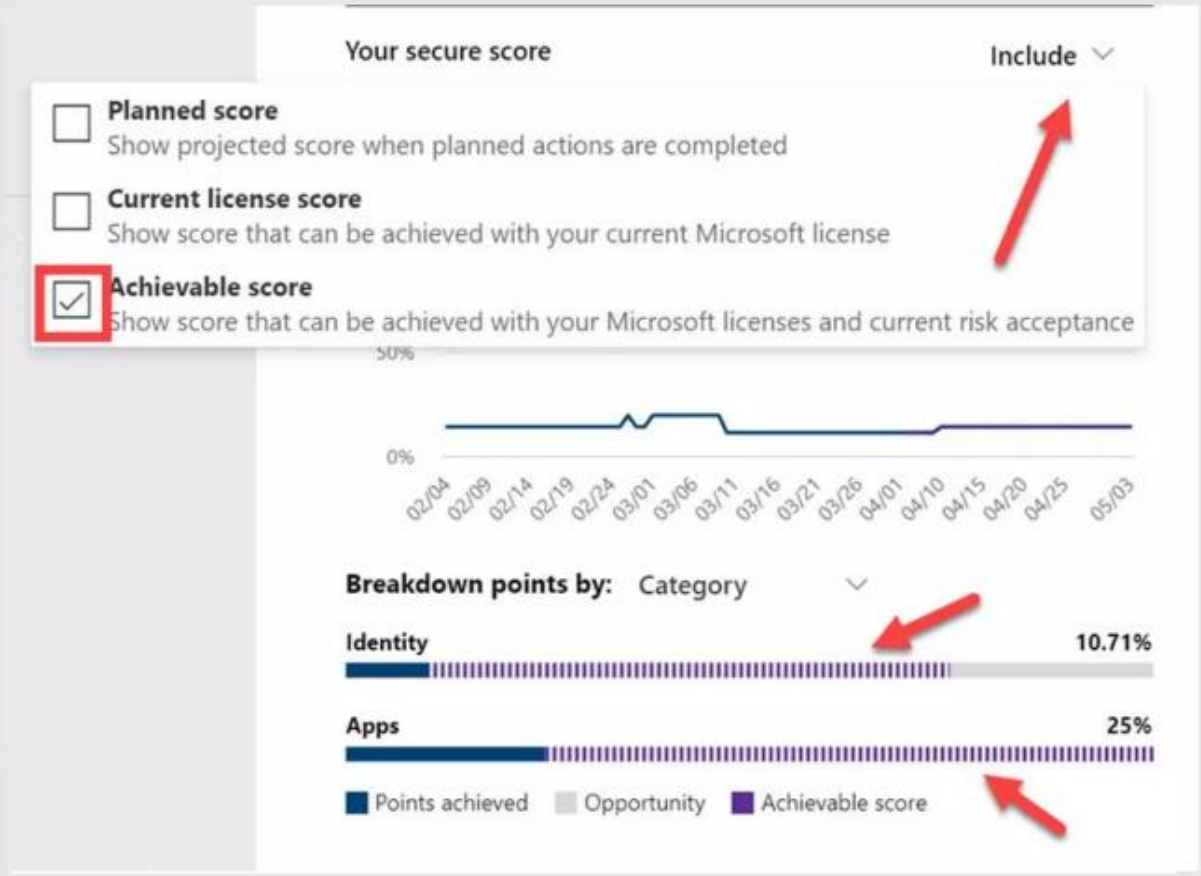
Usa un modello di autenticazione moderno



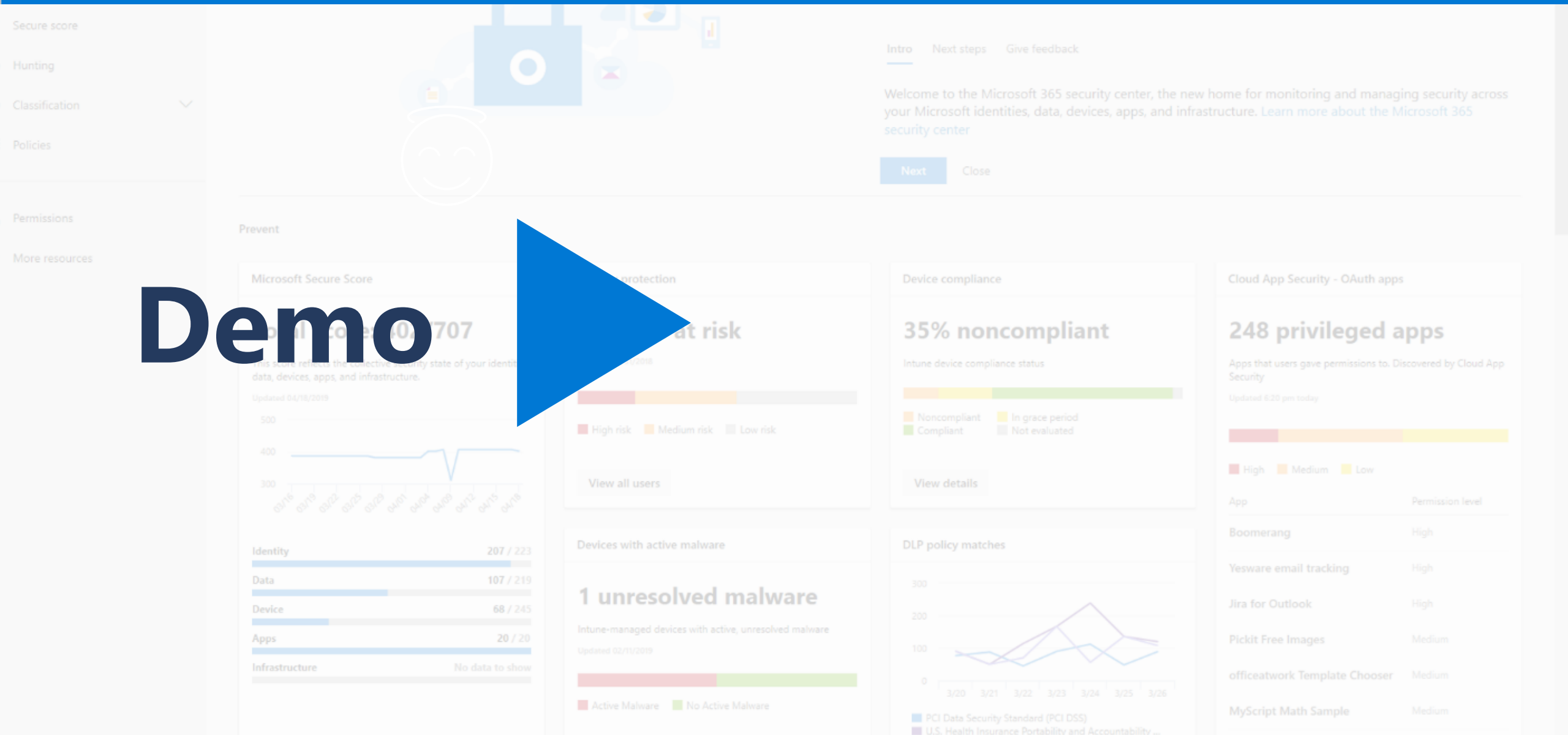
Usa l'accesso condizionale per sicurezza e agilità

Il secure score

https://security.microsoft.com/exposure-secure-score

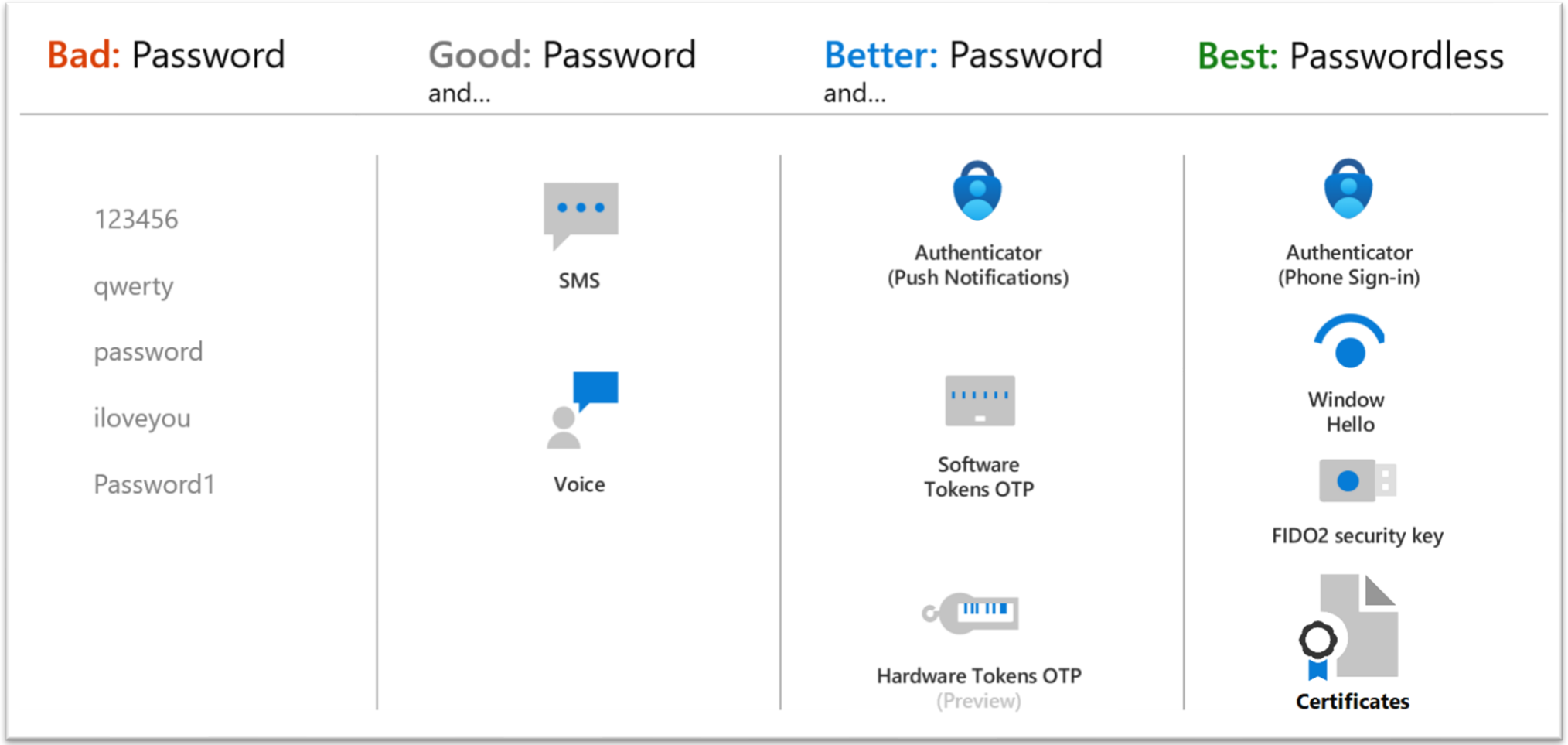


Il secure score

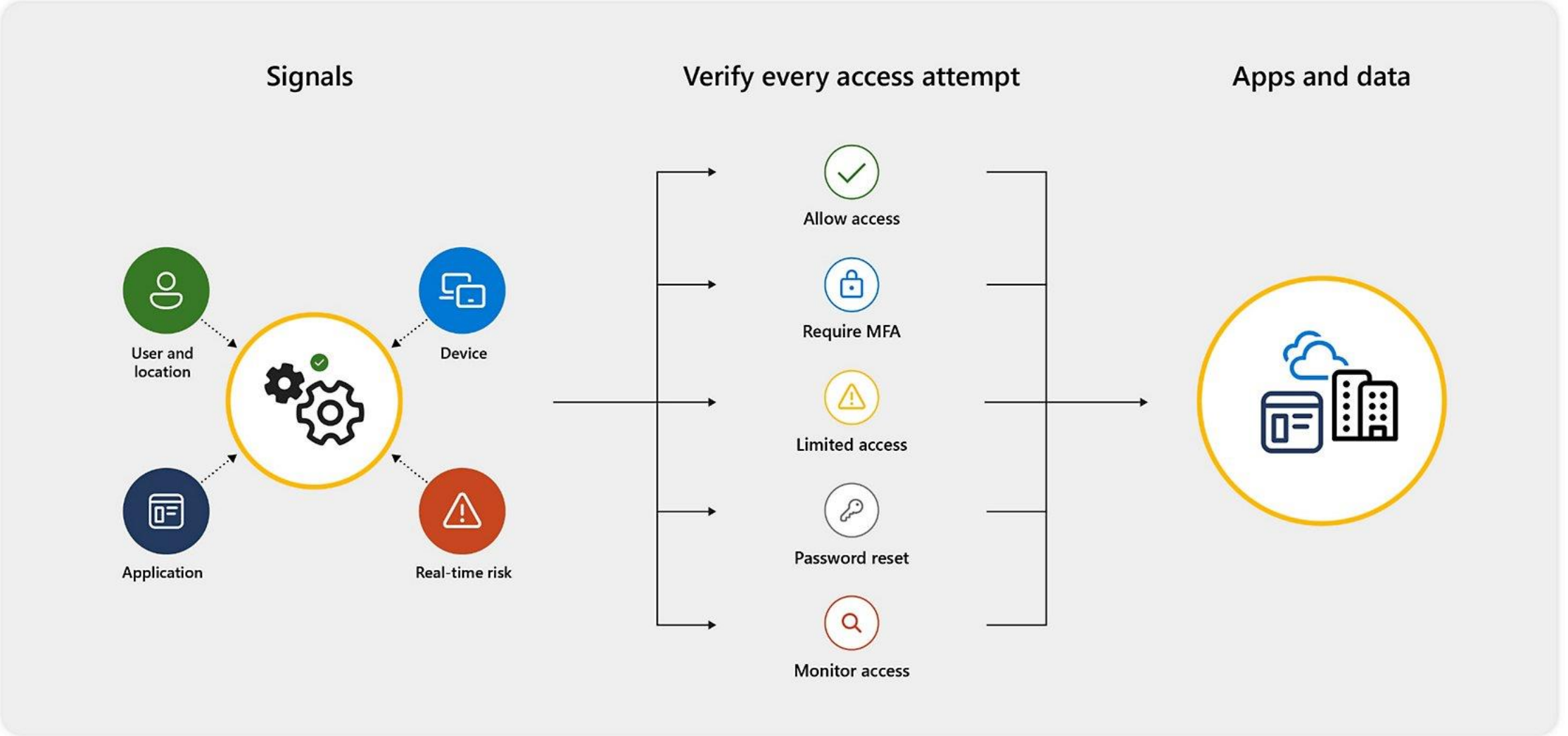


Demo

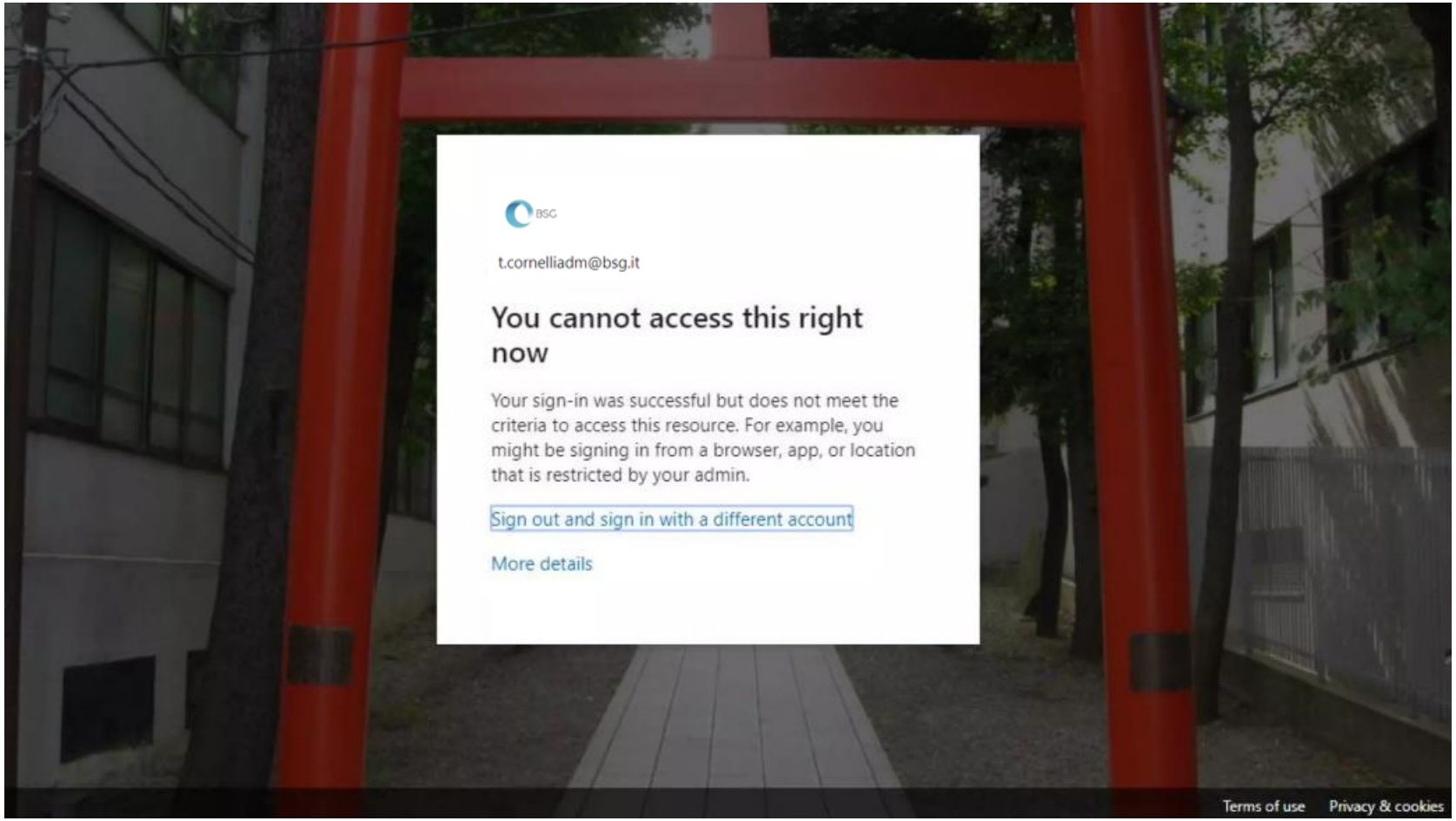
Autenticazione sicura



Accesso condizionale



Accesso condizionale



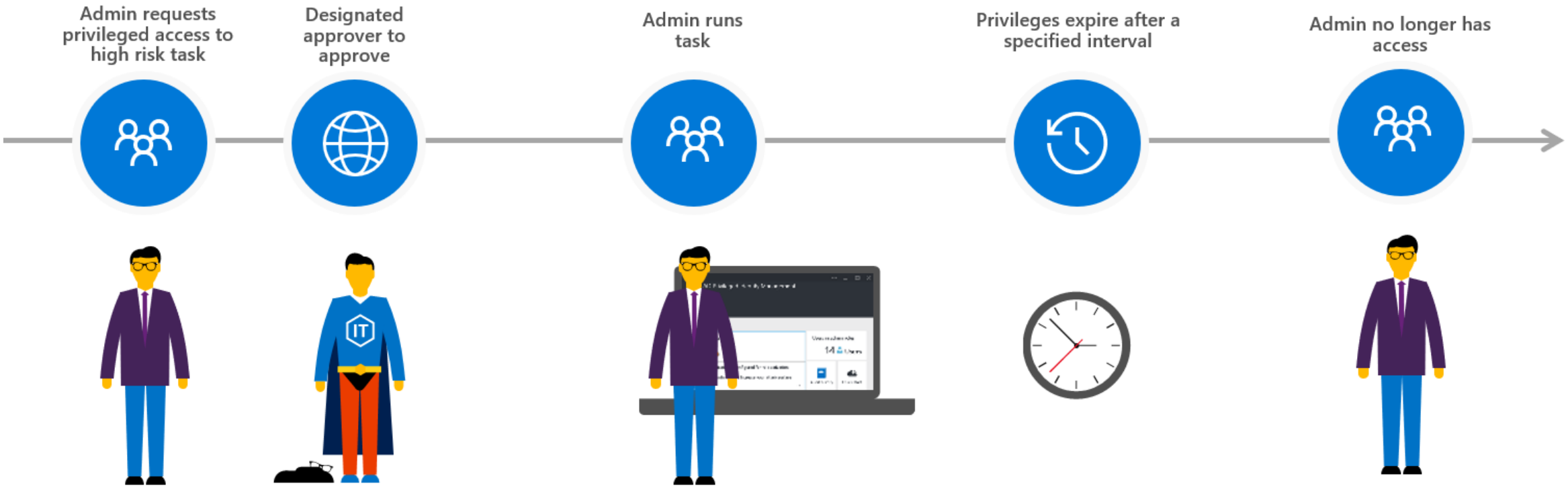
JIT & JEA is the way to go

JIT & JEA

JIT > JUST IN TIME

JEA > JUST ENOUGH ACCESS

AZURE PIM


Admin requests privileged access to high risk task
Designated approver to approve
Admin runs task
Privileges expire after a specified interval
Admin no longer has access
IT

8 M365 Security Fast tips

Fast Tips

1

Utilizza account amministratore dedicati

Gli account amministrativi di Microsoft 365 hanno privilegi elevati, che li rendono obiettivi più attraenti per i criminali informatici. Gli amministratori devono utilizzare questi account esclusivamente per eseguire attività amministrative e utilizzare account utente standard separati per attività quotidiane non amministrative; riducendo il vettore di attacco in caso di compromissione degli account.

2

Disattiva l'inoltro automatico

È possibile disattivare l'inoltro automatico per le e-mail utilizzando le regole di trasporto della posta. Ciò impedisce all'utente e/o a un criminale informatico di inoltrare automaticamente tutte le e-mail a un indirizzo esterno, proteggendo i dati organizzativi.

Fast Tips

Utilizza la protezione avanzata dalle minacce

Advanced Threat Protection o ATP è una funzionalità che aiuta a proteggere gli utenti da allegati e-mail dannosi, come ransomware e virus. Tutti gli allegati vengono scansionati ed detonati nell'ambiente "sandbox" di Microsoft per determinare se esegue azioni dannose. Se i file sono considerati sicuri, vengono riallegati al messaggio e recapitati nella casella di posta del destinatario.

Utilizza i safe link

La funzione "Collegamenti sicuri" fornisce la scansione degli URL e la riscrittura dei messaggi di posta elettronica in entrata nel flusso di posta, nonché la verifica dell'URL al momento del clic. Funziona con collegamenti nei messaggi di posta elettronica e in altre posizioni, come teams e SharePoint.

Tips

5

Abilita l’auditing delle caselle di posta

Il controllo delle cassette postali consente agli amministratori di tenere traccia delle azioni eseguite dagli utenti nelle proprie cassette postali e in quelle di altri utenti. Questa funzionalità è automaticamente attiva per i clienti che si sono iscritti dopo gennaio 2019. Tuttavia, per coloro che l'hanno acquisita dopo tale data, gli amministratori devono verificare se il controllo è abilitato.

6

Utilizza il controllo degli accessi basato sui ruoli (RBAC)

Questa funzionalità garantisce agli amministratori la possibilità di assegnare ruoli agli utenti, consentendo o negando loro di eseguire azioni specifiche. Ad esempio, un amministratore della fatturazione può accedere alla fatturazione solo all'interno di Microsoft 365. Ciò impedisce agli amministratori globali di concedere più autorizzazioni del necessario ad altri utenti.

Tips

Disabilita la condivisione di SharePoint e OneDrive

Per impostazione predefinita, gli utenti di Microsoft 365 possono condividere documenti e file all'esterno dell'organizzazione. La revisione e la modifica delle policy consente agli amministratori di disabilitare la condivisione su siti specifici, riducendo il rischio di fughe di dati.

Utilizza avvisi e-mail

Questa funzionalità invia avvisi per attività sospette o anomale, ad esempio l'eliminazione di volumi elevati di dati dai siti di SharePoint. Una volta ricevuto l'avviso, l'amministratore può indagare e agire se necessario.

Ma il budget?

Microsoft 365 Business Premium

20,60 € utente/mese

(Pagamento annuale – rinnovo automatico)[1]

Il prezzo non include l'IVA

Acquista ora

Microsoft 365 Business

Secure identity

- Self service password reset
- Multi factor authentication

Secure devices

- Device management for Windows and mobile devices
- Device management for iOS and Android

Secure apps

- Restrict paste to personal apps and storage
- Save only to OneDrive for Business

Secure email

- Protect from external threats with Advanced Threat Protection
- Control data access with DLP, archiving, IRM, and encryption

Secure documents

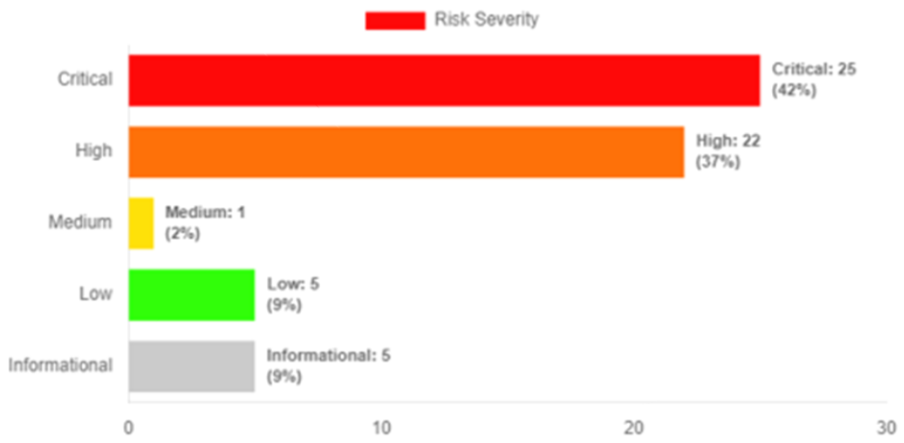
- Classification and labels
- Encryption
- Tracking
- Revoke access

Non devi fare tutto da solo

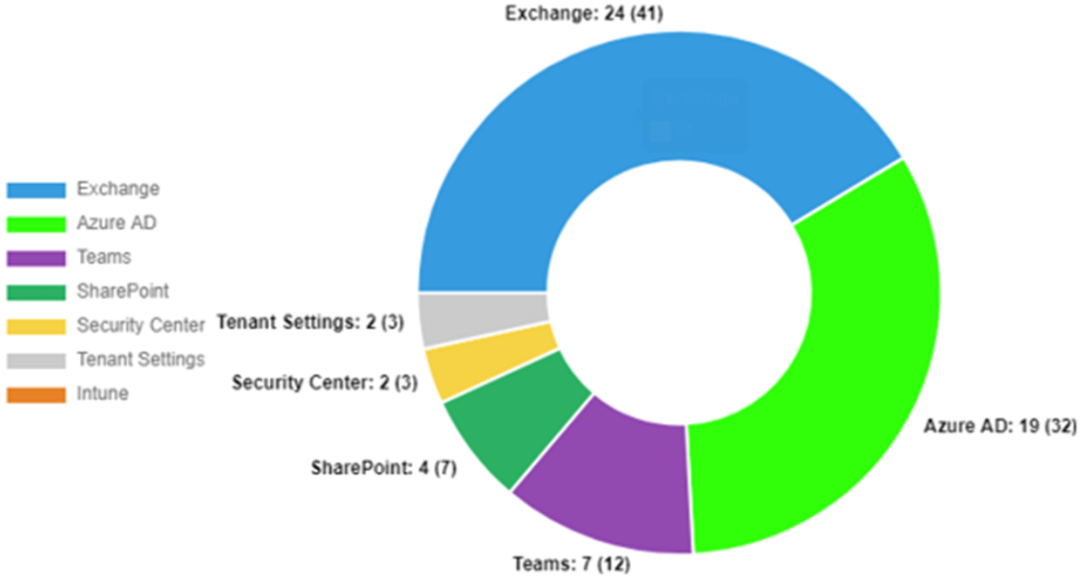
Richiedi un security assessment del tuo ambiente M365

Dalle analisi effettuate e dalle informazioni condivise con i referenti del cliente è evidente la consapevolezza e la volontà di proteggere il tenant M365. Il secure score si attesta al 43,24% rientrando nella media delle aziende dello stesso sizing. Nelle slide successive verranno delineate le opportunità di miglioramento individuate e implementabili sul breve, medio e lungo termine.

Risk Severity



Risk Distribution



Grazie!

Non esitare a contattarmi: t.cornelli@bsg.it

Business Solutions Srl - Viale Jenner, 51 - 20158 Milano