

A graphic featuring a blue shield with a keyhole, surrounded by a network of glowing blue nodes and lines, set against a dark blue background with faint binary code.

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?

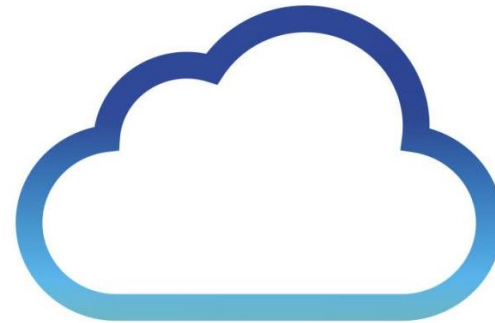
Obiettivi di oggi

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

What is the Cloud?

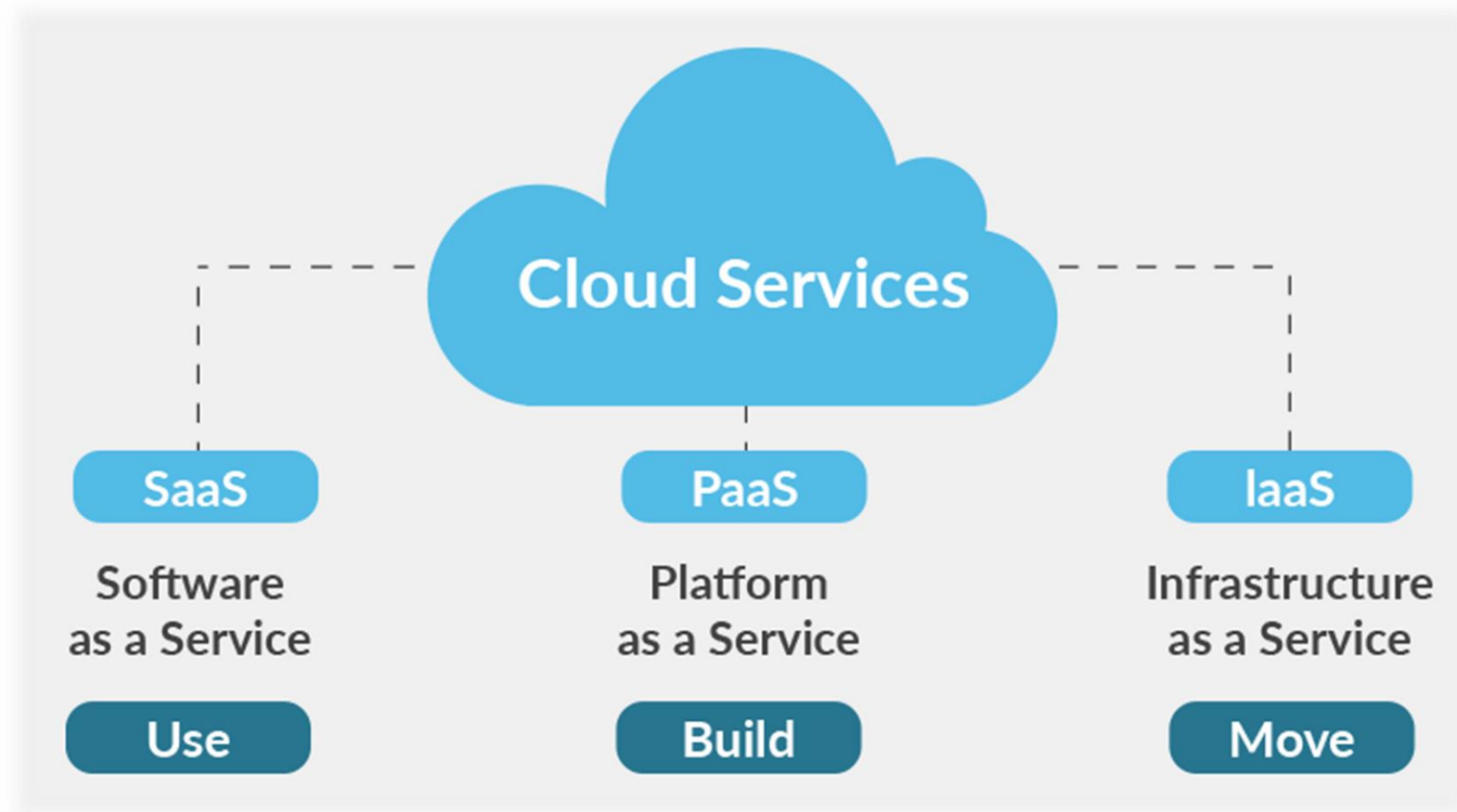


There is no cloud
It's just someone else's computer

**The ability to rent computing
resources on demand**

Il concetto di responsabilità condivisa

Cloud Computing Services



Lo shared responsibility Model



Modello di responsabilità condivisa

Responsabilità	SaaS	PaaS	IaaS	Locale	
Informazioni e dati	Cliente	Cliente	Cliente	Cliente	RESPONSABILITÀ MANTENUTA SEMPRE DAL CLIENTE
Dispositivi (dispositivi mobili e PC)	Cliente	Cliente	Cliente	Cliente	
Account e identità	Cliente	Cliente	Cliente	Cliente	
Infrastruttura di identità e directory	Microsoft	Microsoft	Cliente	Cliente	RESPONSABILITÀ VARIABILE IN BASE AL TIPO DI SERVIZIO
Applicazioni	Microsoft	Microsoft	Cliente	Cliente	
Controlli di rete	Microsoft	Microsoft	Cliente	Cliente	
Sistema operativo	Microsoft	Microsoft	Cliente	Cliente	TRASFERIMENTO DI RESPONSABILITÀ AL PROVIDER DI SERVIZI CLOUD
Host fisici	Microsoft	Microsoft	Microsoft	Cliente	
Rete fisica	Microsoft	Microsoft	Microsoft	Cliente	
Data center fisico	Microsoft	Microsoft	Microsoft	Cliente	

■ Microsoft ■ Cliente



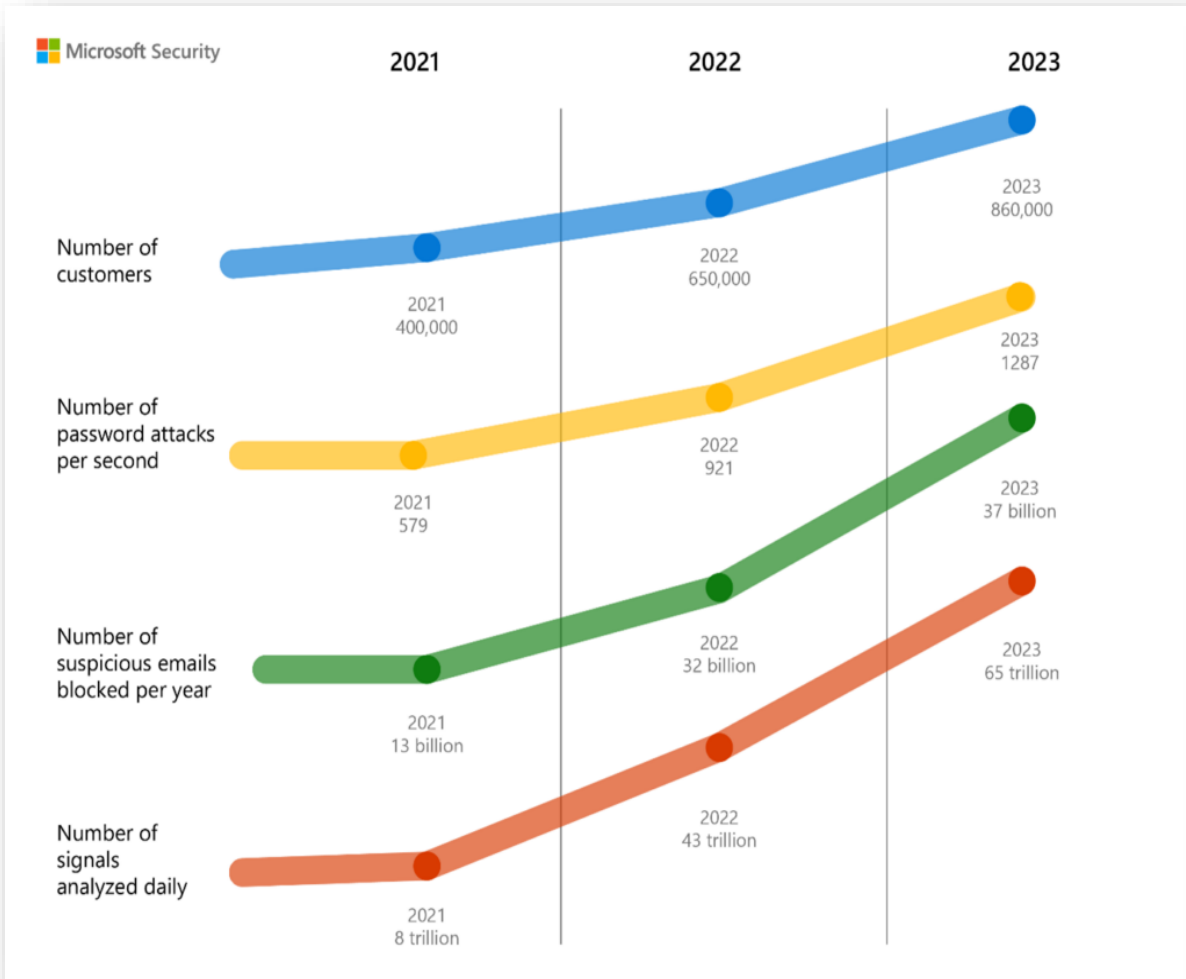
Microsoft 365, rappresenta una soluzione SAAS completa di strumenti di produttività basati su cloud sviluppati da Microsoft.

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



Microsoft Security

\$4.35 M

The average cost of a data breach reached an all-time high of USD 4.35 million in 2022.

Since September 2021, the number of password attacks rose from

579 → 1,287 per second

65 trillion signals

Analyzed daily by Microsoft to better understand and protect against digital threats and cybercriminal activity

70 billion

Email and identity threat attacks blocked by Microsoft last year alone

2.75 million

Site registrations successfully blocked by Microsoft to get ahead of criminal actors that planned to use them to engage in global cybercrime

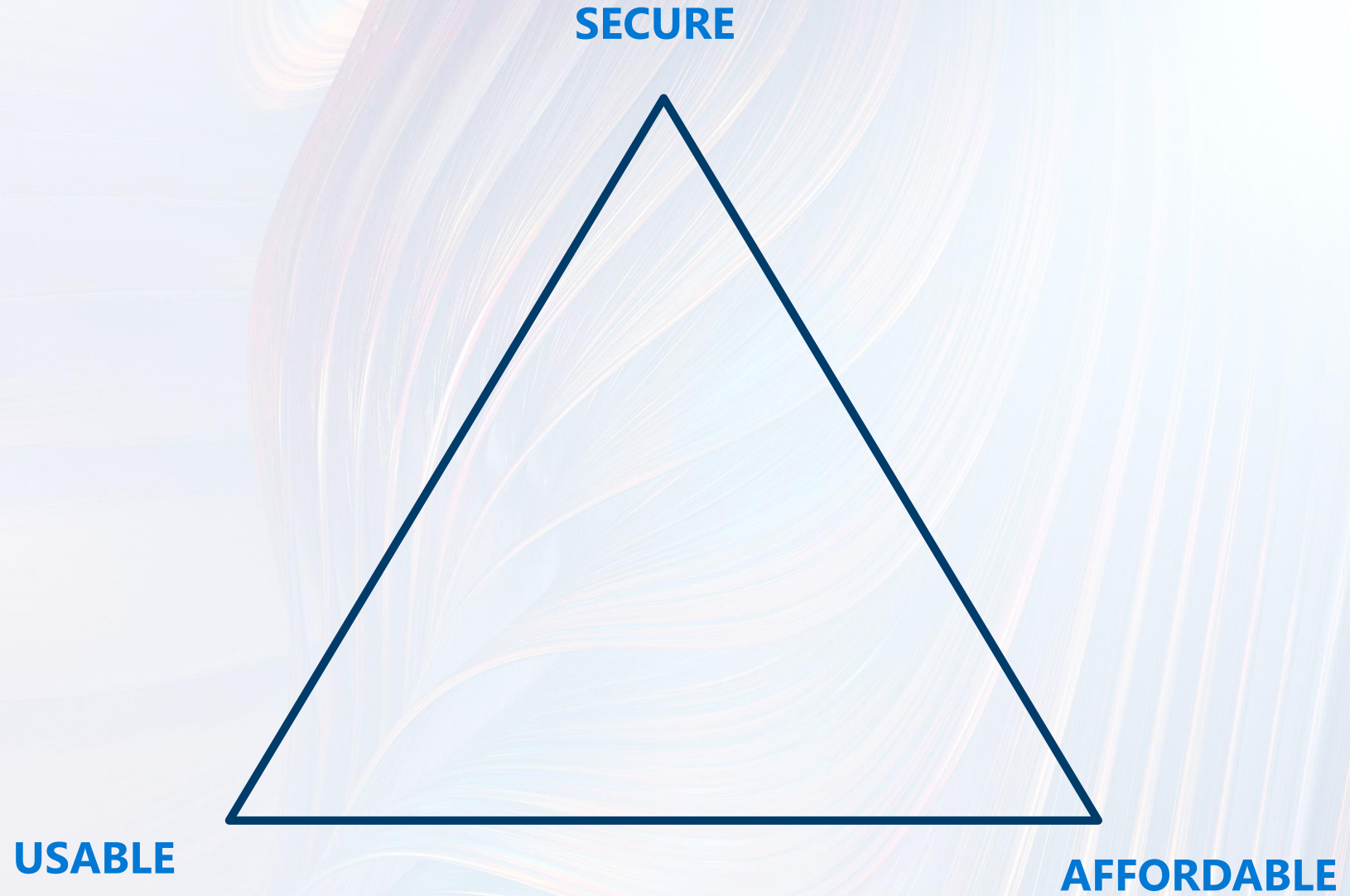
60% cost savings

When customers invest in Microsoft end-to-end security rather than multiple point solutions

Security Challenges



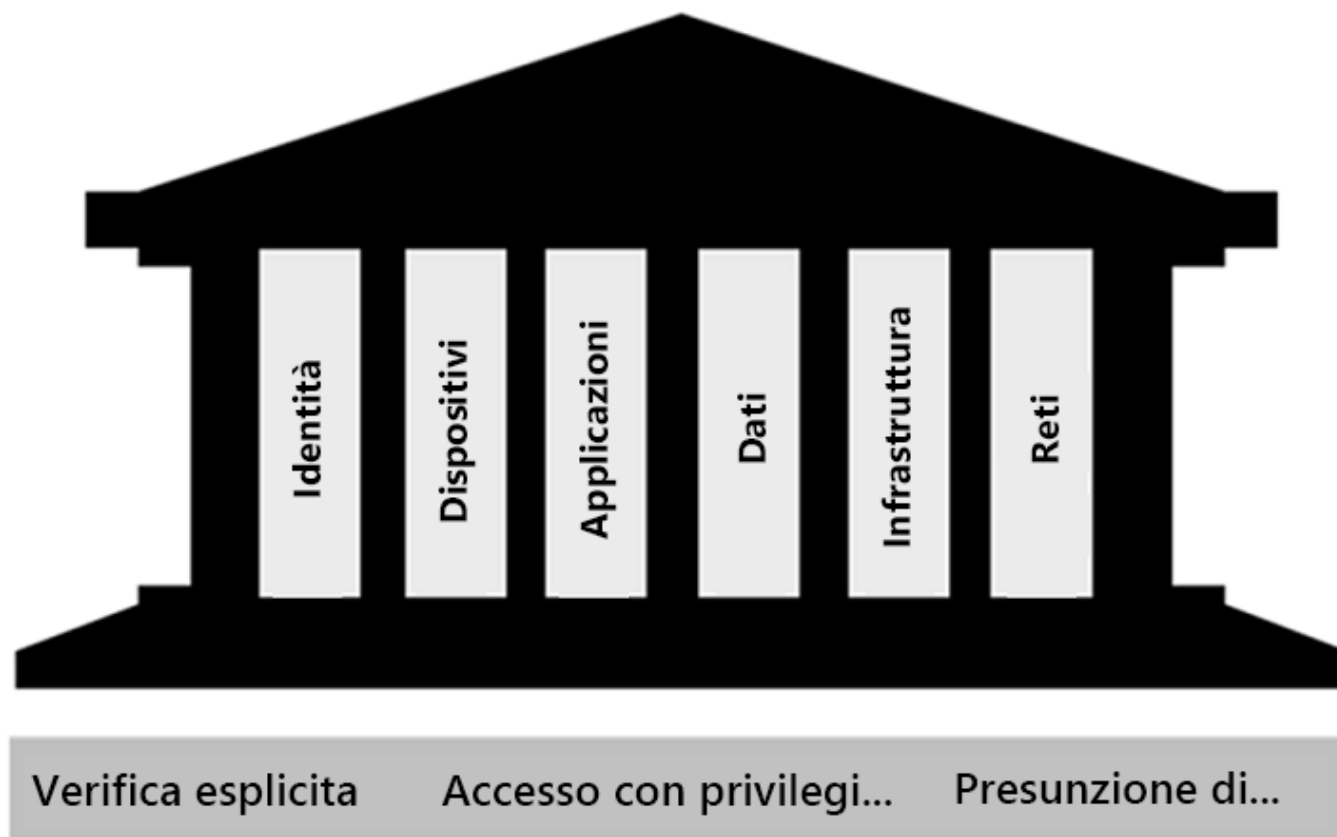
Security Dilemma



Approccio alla soluzione

Zero trust architecture

Metodologia Zero Trust
"Non fidarti di nessuno, verifica tutto"



Zero trust architecture

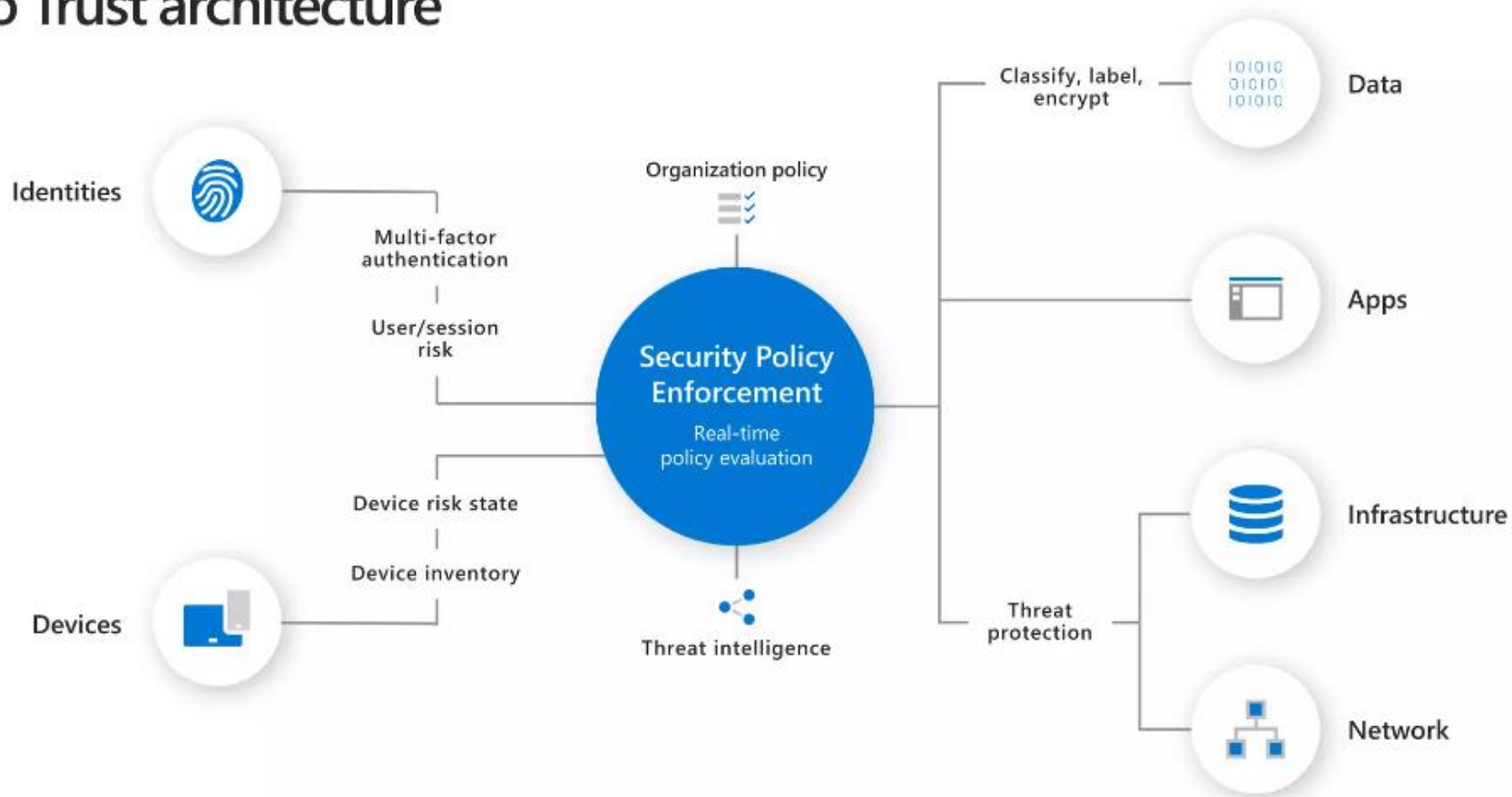
Il modello Zero Trust presuppone che tutto sia in una rete aperta e non attendibile, anche le risorse protette dai firewall della rete aziendale. Il modello Zero Trust opera sul principio "**nulla è attendibile, verifica tutto**".

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

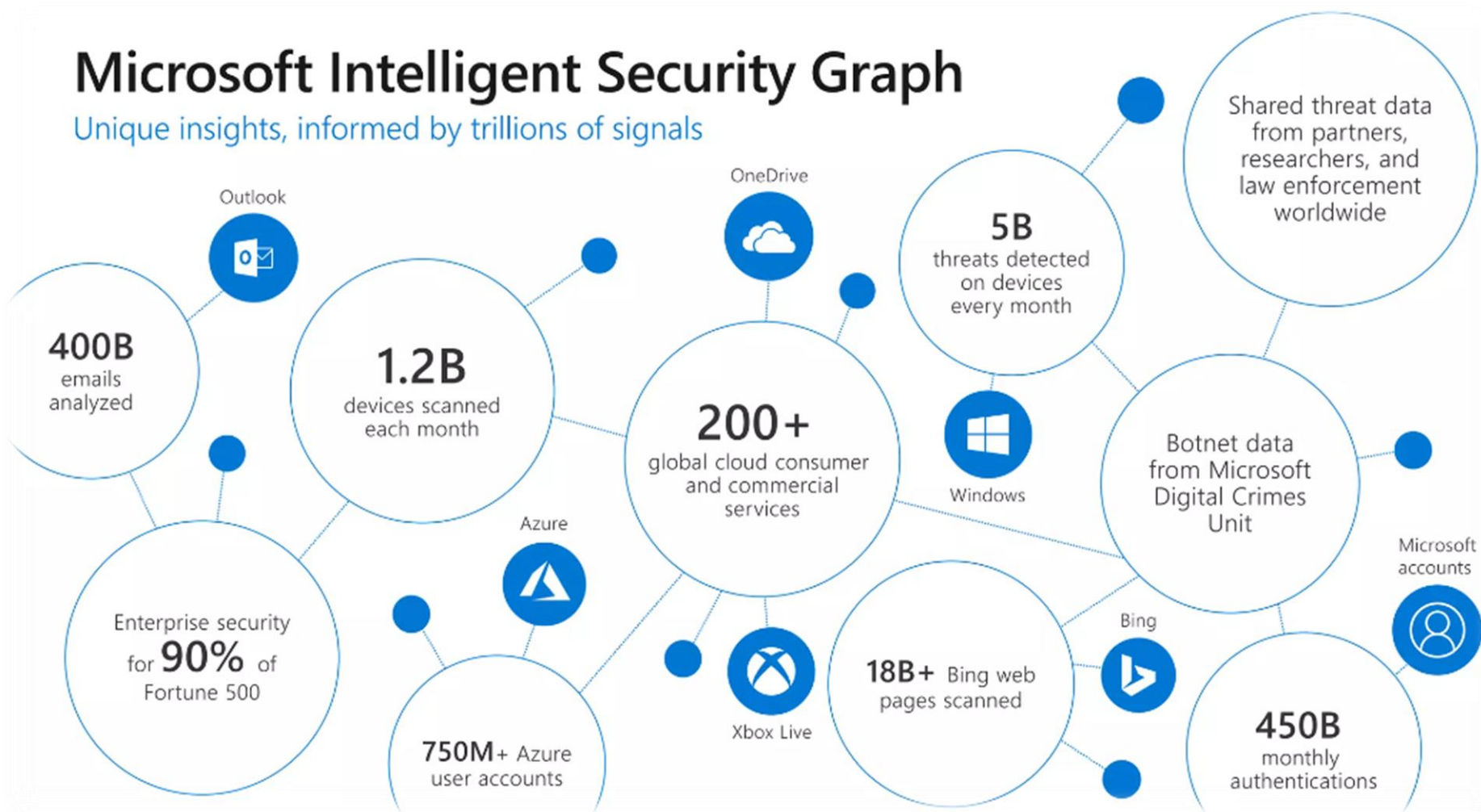
Zero Trust architecture



Perché Microsoft?

Microsoft Intelligent Security Graph

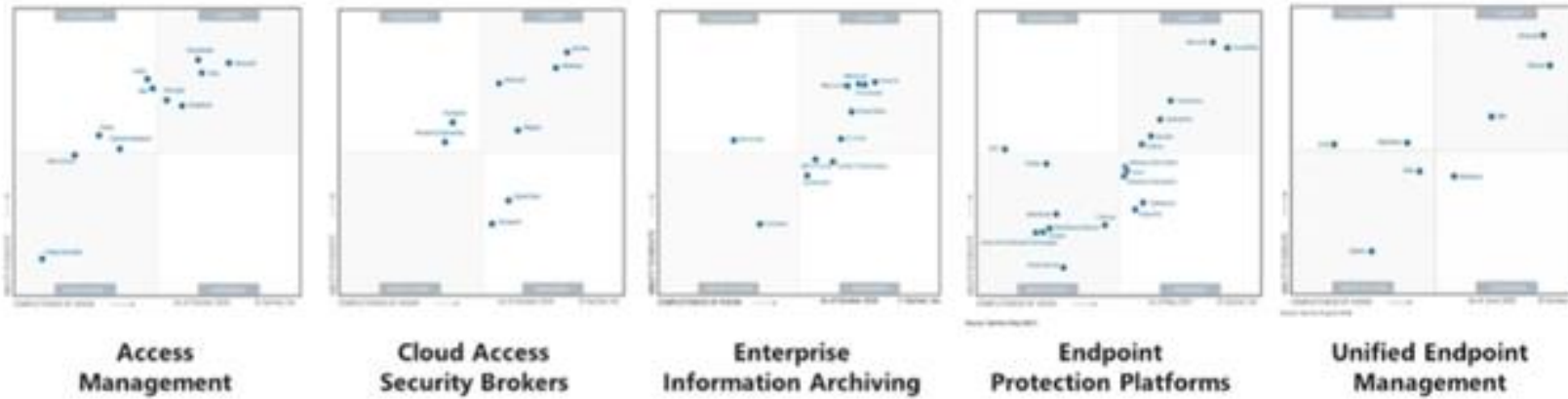
Unique insights, informed by trillions of signals



Perché Microsoft?

Gartner

Microsoft Security — a Leader in Gartner Magic Quadrant reports



"Gartner Magic Quadrant for Access Management," by Michael Kelley, Abbyday Datta, Henrique Pereira, 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 Hoch, Jeff Vogel, October 2020
"Gartner Magic Quadrant for Endpoint Protection Platforms," by Paul Walker, Rob Smith, Praveek Bhargava, Mark Harris, Peter Fendrick, May 2021
"Gartner Magic Quadrant for Unified Endpoint Management," by Dan Wilson, Rich Doherty, Rob Smith, Chris Ska, Manjunath Shet, August 2020
These graphics were published by Gartner, Inc. as part of larger research documents and should be included in the context of the entire document. 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 the 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 US and internationally, and is used herein with permission. All rights reserved.

Perché Microsoft?

FORRESTER

FORRESTER®

Microsoft Security — a Leader in 7 Forrester Wave reports



1. The Forrester Wave™ Security Analytics Platforms, Q4 2020. Joseph Bartlamship, Claire O'Malley, December 2020.
2. The Forrester Wave™ Enterprise Email Security Q2 2021. Joseph Bartlamship, Claire O'Malley, April 2021.
3. The Forrester Wave™ Enterprise Detection And Response, Q1 2020. Josh Zelen, 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 2019. Andrew Resnik, November 2019.
6. The Forrester Wave™ Unstructured Data Security Platforms, Q2 2021. Heidi Shey, May 2021.
7. The Forrester Wave™ Cloud Security Gateways, Q2 2021. Andrius Cisar, May 2021.

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and judgments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Delivering device security across platforms



Endpoints and servers¹



macOS

Mobile devices²



iOS

Virtual desktops



Azure Virtual Desktop

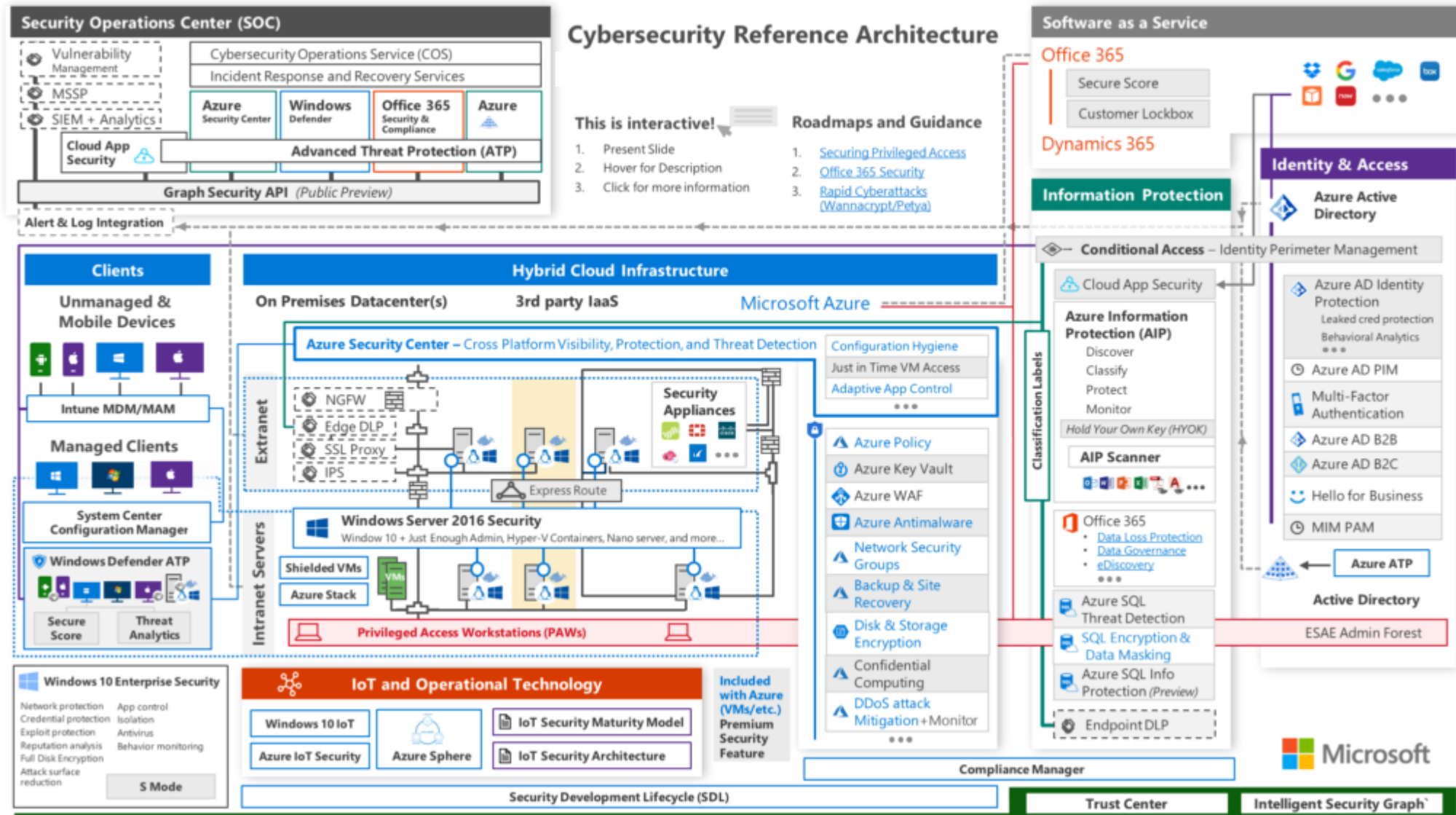


Windows 365

¹Add-on for server support is [now available](#).

²iOS and Android security without Intune for MDB standalone now GA. Intune Plan 1 is included in Microsoft 365 Business Premium. See [Documentation](#) for detail.

IT security stack Microsoft





Ok, ma dove comincio?

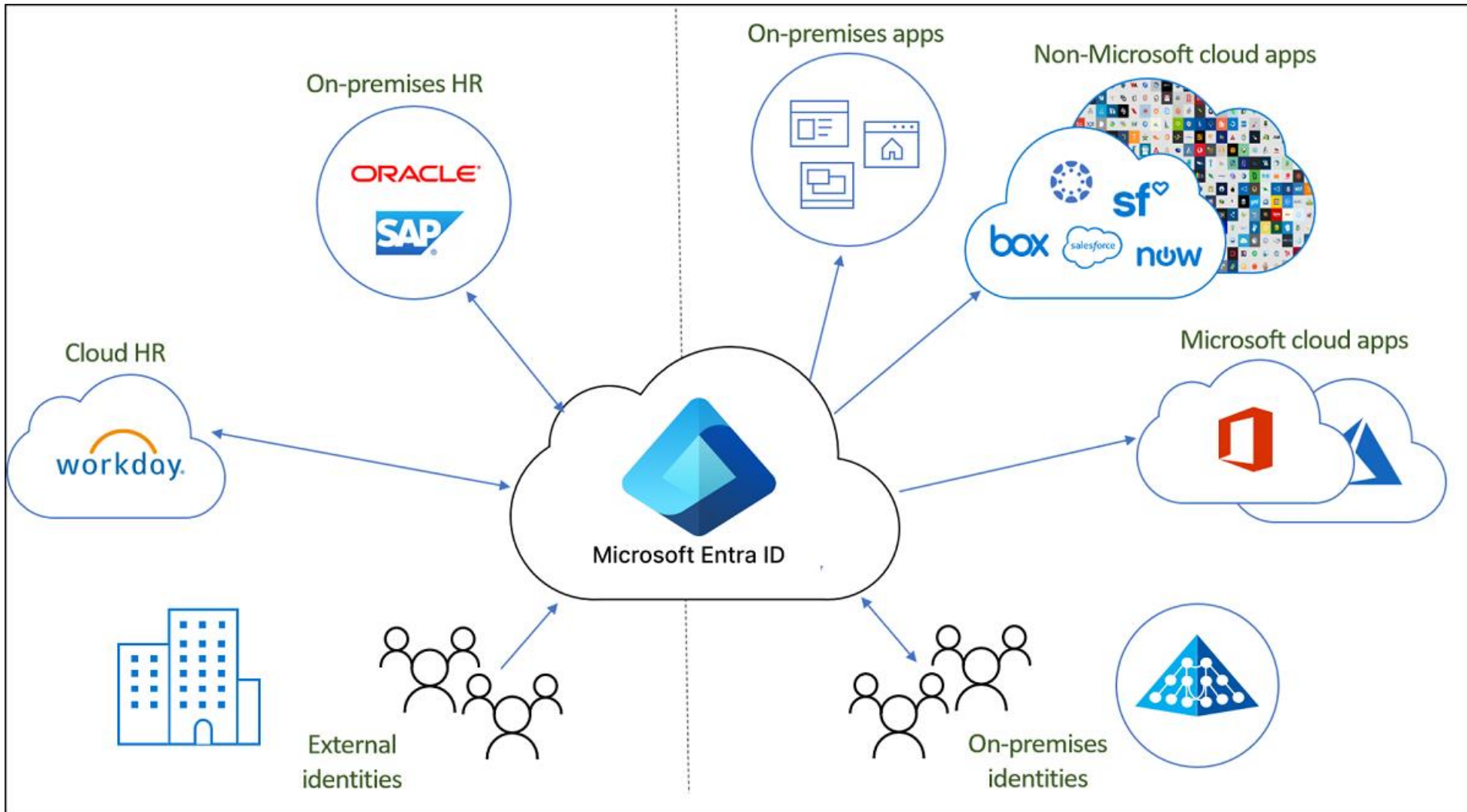




Identity is at the center of security



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

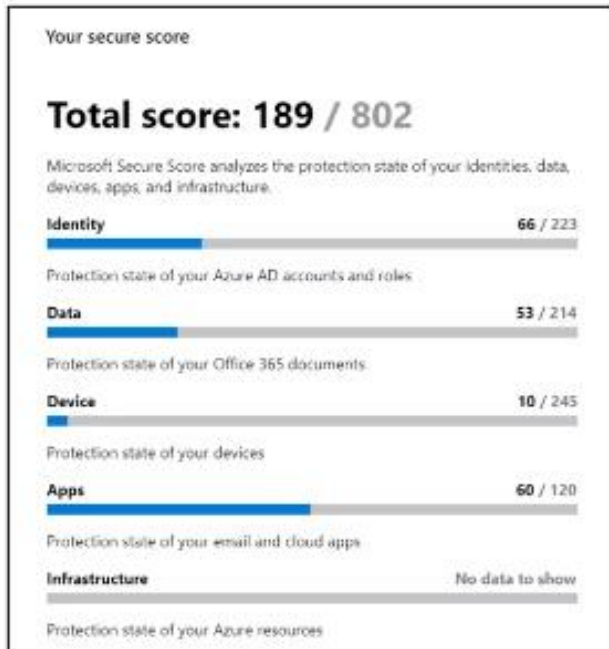
Source:

statista 



I primi passi...

I primi 3 step fondamentali



Sfrutta il secure score per definire la tua security baseline

 BSC

t.cornelliadm@bsg.it

Approve sign in request

 Open your Authenticator app, and enter the number shown to sign in.

69

No numbers in your app? Make sure to upgrade to the latest version.

Don't ask again for 7 days

Usa un modello di autenticazione moderno

Name *

Block legacy authentication

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

All cloud apps

Network **NEW** ⓘ

Not configured

Conditions ⓘ

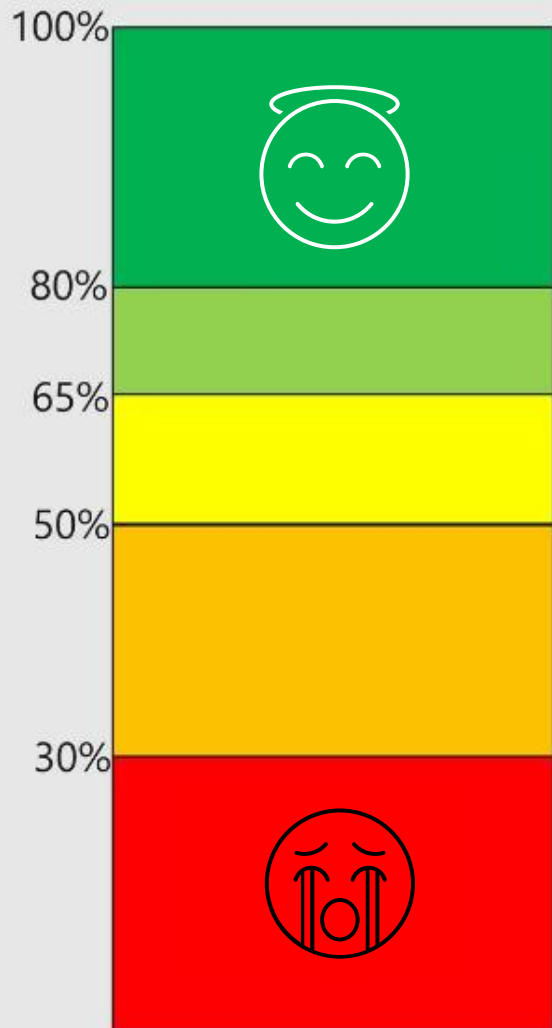
1 condition selected

Enable policy

Report-only **On** Off

Usa l'accesso condizionale per sicurezza e agilità

IT secure score



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

Your secure score Include ▾

- Planned score**
Show projected score when planned actions are completed
- Current license score**
Show score that can be achieved with your current Microsoft license
- Achievable score**
Show score that can be achieved with your Microsoft licenses and current risk acceptance

50%
0%

02/04 02/09 02/14 02/19 02/24 03/01 03/06 03/11 03/16 03/21 03/26 04/01 04/10 04/15 04/20 04/25 05/03

Breakdown points by: Category ▾

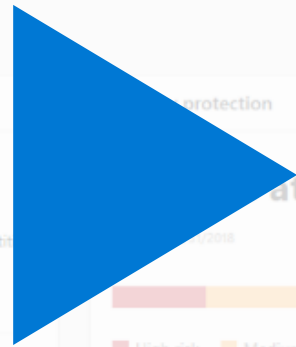
Identity 10.71%

Apps 25%

■ Points achieved ■ Opportunity ■ Achievable score

II secure score

Demo



Secure score

Hunting

Classification

Policies

Permissions

More resources

Intro Next steps Give feedback

Welcome to the Microsoft 365 security center, the new home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure. Learn more about the Microsoft 365 security center

Next Close

Prevent

Microsoft Secure Score

Overall score: 407 / 707

This score reflects the collective security state of your identities, data, devices, apps, and infrastructure.

Updated 04/18/2019

Category	Score	Total
Identity	207	223
Data	107	219
Device	68	245
Apps	20	20
Infrastructure	No data to show	

Device protection

At risk

High risk Medium risk Low risk

View all users

Device compliance

35% noncompliant

Intune device compliance status

Noncompliant In grace period Compliant Not evaluated

View details

Cloud App Security - OAuth apps

248 privileged apps

Apps that users gave permissions to. Discovered by Cloud App Security

Updated 6:20 pm today

High Medium Low

App	Permission level
Boomerang	High
Yesware email tracking	High
Jira for Outlook	High
Pickit Free Images	Medium
officeatwork Template Chooser	Medium
MyScript Math Sample	Medium

Devices with active malware

1 unresolved malware

Intune-managed devices with active, unresolved malware

Updated 02/11/2019










Active Malware No Active Malware

DLP policy matches

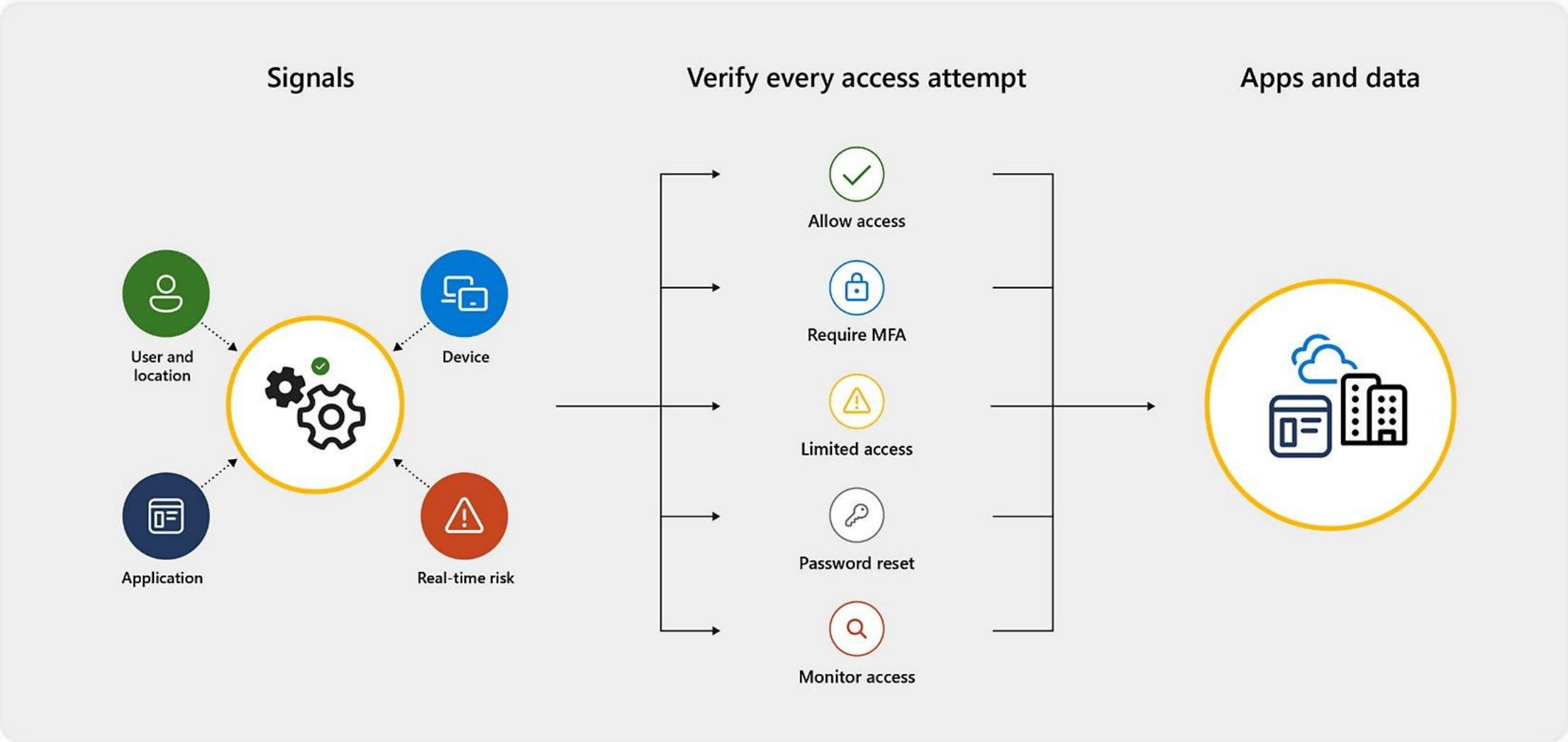
3/20 3/21 3/22 3/23 3/24 3/25 3/26

PCI Data Security Standard (PCI DSS)
U.S. Health Insurance Portability and Accountability Act (HIPAA)

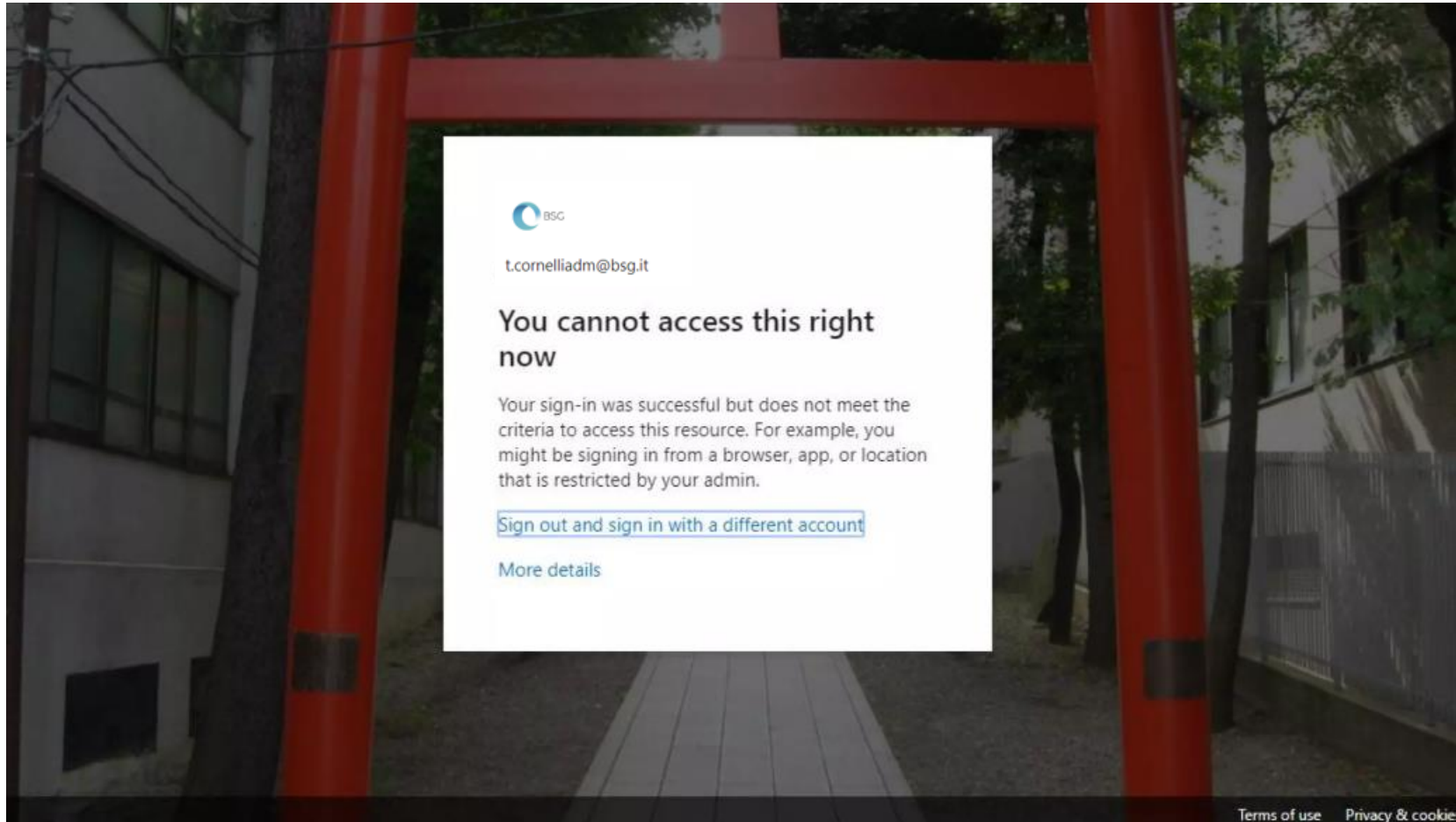
Autenticazione sicura

Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456			
qwerty	SMS	Authenticator (Push Notifications)	Authenticator (Phone Sign-in)
password			
iloveyou	Voice	Software Tokens OTP	Window Hello
Password1			
		Hardware Tokens OTP (Preview)	

Accesso condizionale



Accesso condizionale





JIT & JEA is the way to go

JIT & JEA

JIT > JUST IN TIME

JEA > JUST ENOUGH ACCESS

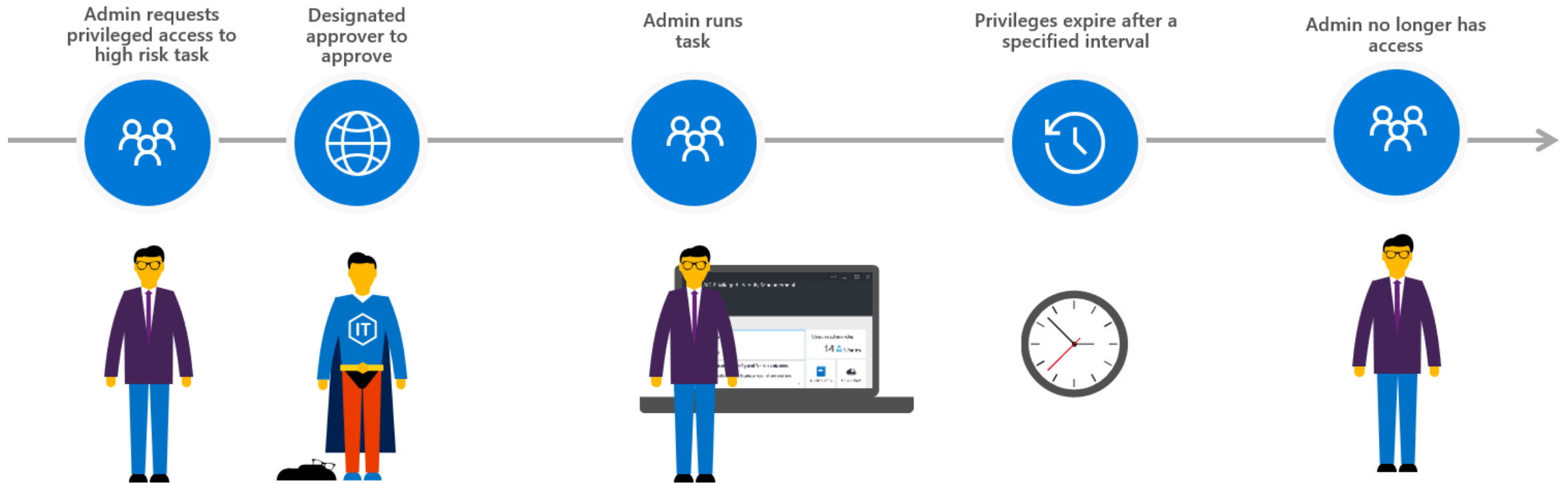


Discover and monitor

It is common for access to critical resources to go undetected. Ensure you know who has access to what, and receive notifications when new assignments are granted to accounts in your organization.

[Discover](#)

AZURE PIM





8 M365 Security Fast tips

Fast Tips

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.

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 scansati 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.

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.

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.

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



Exchange



Teams



OneDrive



SharePoint



Outlook



Word



Excel



PowerPoint



Publisher



Access



Intune



Azure Information Protection



Defender



Conditional Access



Windows Virtual Desktop

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

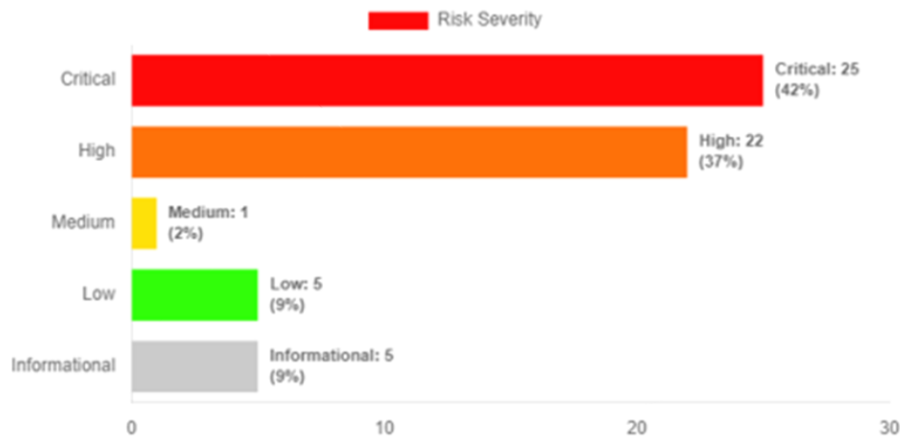


Richiedi un security assessment del tuo ambiente M365

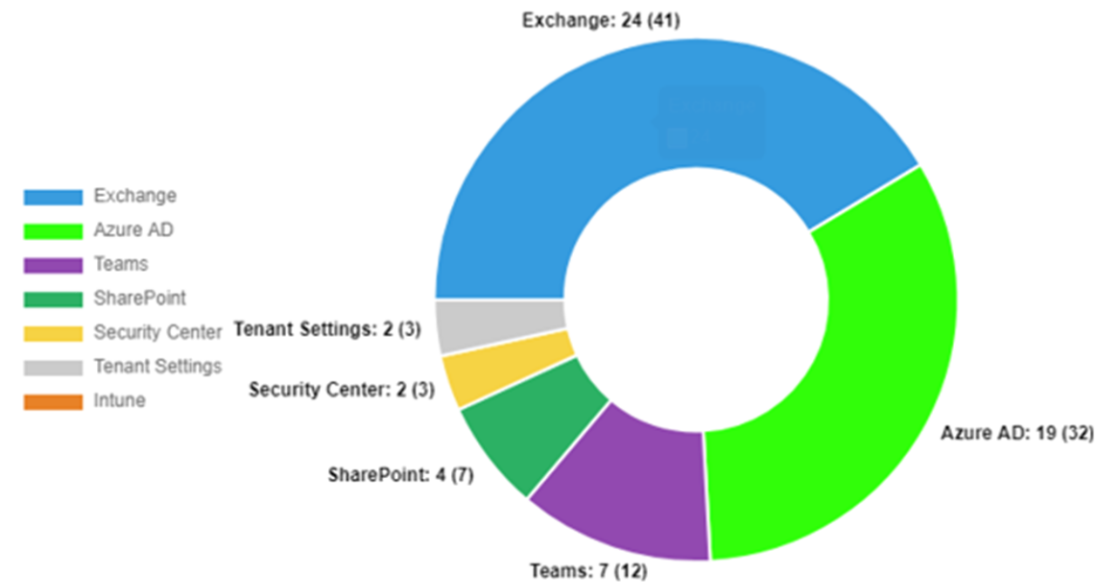


Dalle analisi effettuate e dalle informazioni condivise con i referenti del cliente è evidente la consapevolezza e la volontà di proteggere il tenant M365. Il secure score si attesta al 43,24% rientrando nella media delle aziende dello stesso sizing. Nelle slide successive verranno delineate le opportunità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

