

RESOL/E

by ErgonGroup

PRIMA DI INIZIARE



Controlla che l'audio del tuo microfono
e la videocamera siano disattivati



/ Digital

DIRETTA LIVE

Cybersecurity multilivello con Microsoft 365

MER 07/12 | 17:00-18:00

RESOL/E



/ CHI SIAMO

SPEAKER

MICHELE RUBERTI

Digital Director & Co-founder @RESOLVE

Direttore Tecnologico della linea Digital di Resolve, Michele è da sempre un appassionato di **innovazione digitale**. Microsoft Certified Solutions Associate, Solution Expert, IT Professional, Technology Specialist e Microsoft Certified Trainer: da più di vent'anni, supporta le aziende nelle sfide tecnologiche che il mercato propone. Gli ambiti in cui opera sono molteplici ma attualmente le sue aree di riferimento fanno capo ad **Active Directory, SharePoint, Microsoft 365, Azure, EMS, Business Intelligence e Virtualizzazione**.

/ AGENDA

1

AZIENDA SICURA O RESILIENTE?

Essere pronti ad affrontare le nuove minacce

2

MICROSOFT 356: IL TUO ALLEATO PER LA CYBERSECURITY

Demo Live: proteggere i tuoi dati da ovunque

3

DAL DIRE AL FARE: DOMANDE & RISPOSTE LIVE

Tips per non-nerd e casi di successo

01. AZIENDA SICURA O RESILIENTE?

TRA NUOVE MINACCE E NUOVE SOLUZIONI

/ Le aziende sono pronte?

Qualche numero

80%

IT SENIOR

ritiene che **la propria azienda non sia adeguatamente protetta contro gli attacchi informatici**, nonostante l'aumento degli investimenti nella sicurezza IT

5%

CARTELLE

sono dotate di una protezione appropriata. Un dato gravissimo se confrontato agli **11 milioni di file** a cui ciascun utente ha mediamente accesso

57%

AZIENDE

ha effettuato una valutazione dei rischi per la sicurezza dei dati nel 2020 e il 77% delle aziende non ha definito un piano di risposta in caso di incidenti di sicurezza IT

93%

SANITARI

ha segnalato almeno una violazione della sicurezza IT negli ultimi tre anni (il che significa che i nostri dati sensibili sono esposti a intrusioni da parte di hacker)

/ Da dove arrivano le minacce?

+47%

INCIDENTI DI
SICUREZZA
ORIGINATI DA
**MINACCE
INTERNE**

Con minaccia interna intendiamo **qualsiasi persona autorizzata ad accedere a informazioni o sistemi critici e che abusa di tale accesso, intenzionalmente o accidentalmente**, esponendo l'azienda a perdite di dati, problematiche legali, perdite finanziari, danni alla reputazione e altro ancora.

/ Da dove arrivano le minacce?

+47%

INCIDENTI DI
SICUREZZA
ORIGINATI DA
**MINACCE
INTERNE**

Con minaccia interna intendiamo **qualsiasi persona autorizzata ad accedere a informazioni o sistemi critici e che abusa di tale accesso, intenzionalmente o accidentalmente**, esponendo l'azienda a perdite di dati, problematiche legali, perdite finanziari, danni alla reputazione e altro ancora.



Le persone sono il nuovo perimetro della rete aziendale.

Questo impone un **ripensamento della gestione delle minacce** che permetta di garantire la produttività e valutare il rischio aziendale con una soluzione di sicurezza efficace partendo da una prospettiva diversa, dall'interno verso l'esterno.

/ Digital Workplace

I nuovi criteri: «always on», «da remoto» e nuove dinamiche

L'evoluzione del lavoro ha creato nuove sfide per la Cybersecurity.

Le aziende sono sotto pressione per preservare la loro produttività e la Business Continuity, rispettando al contempo le normative sulla protezione dei dati e proteggendosi dalle minacce interne.



Dipendenti



Collaboratori e consulenti indipendenti



Collaboratori terzi



Partner della supply chain



Fornitori di servizi

L'era del flusso e della trasformazione

Tutti sono ora nel settore della tecnologia



Gli strumenti di sicurezza convenzionali non hanno tenuto il passo



Professionisti della sicurezza da soli non possono colmare il divario



I requisiti normativi e i costi sono in aumento



PRINCIPALI RISULTATI

Nel 2020, il costo annuale medio delle minacce interne è stato di

11,45 milioni\$



77 GIORNI

Tempo medio necessario per contenere un incidente di origine interna

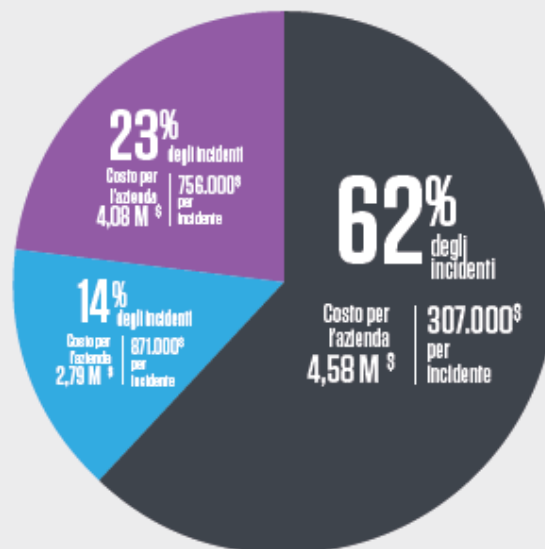
Dal 2018, il costo delle minacce interne è cresciuto del

31%



Dal 2018, gli incidenti di cybersecurity di origine interna sono aumentati del

47%



Collaboratori interni negligenti



Utenti interni malintenzionati



Furto delle credenziali di accesso

Fonte: Report 2020 sul costo delle minacce interne del Ponemon Institute

/ Persone, non infrastrutture

Il nuovo bersaglio degli «hacker»

THREATS USE SOCIAL ENGINEERING, NOT VULNERABILITIES



99%+

Malware attacks rely on user to run malicious code



300%+

Increase in corporate credential phishing

SHIFT TO CLOUD CREATES NEW THREAT VECTORS, DATA EXPOSURE

Account takeover of cloud apps is a growing problem

85%

Orgs exposed to targeted password attacks

45%

Orgs detected successful account compromise

0.6%

Active accounts in orgs targeted by attacks

EMAIL FRAUD IS A BOARD-LEVEL ISSUE



\$26.2B+

Direct losses worldwide
(June 2016 – June 2020)

166,349

Incidents worldwide

/ Panorama delle minacce

Cosa può accadere in 30 giorni a una PMI?



129 email attacks



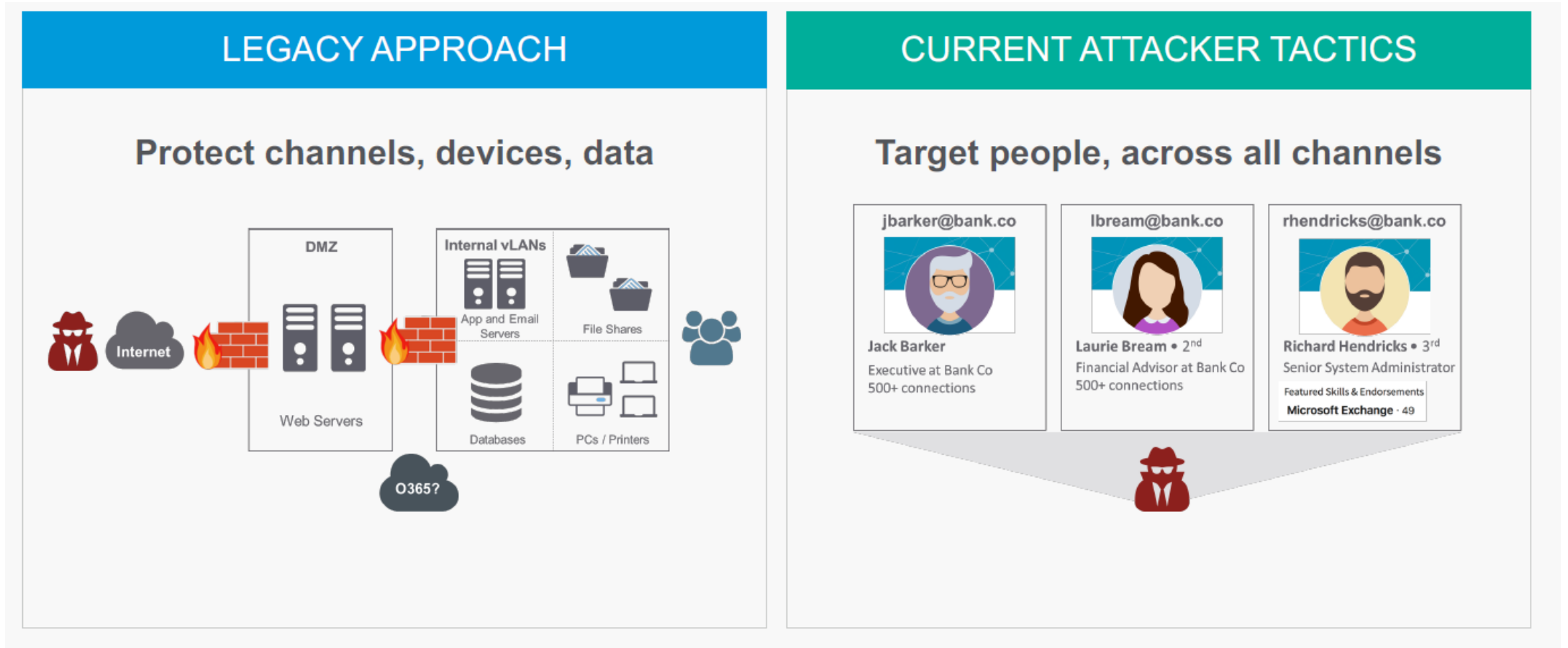
57 phishing attacks



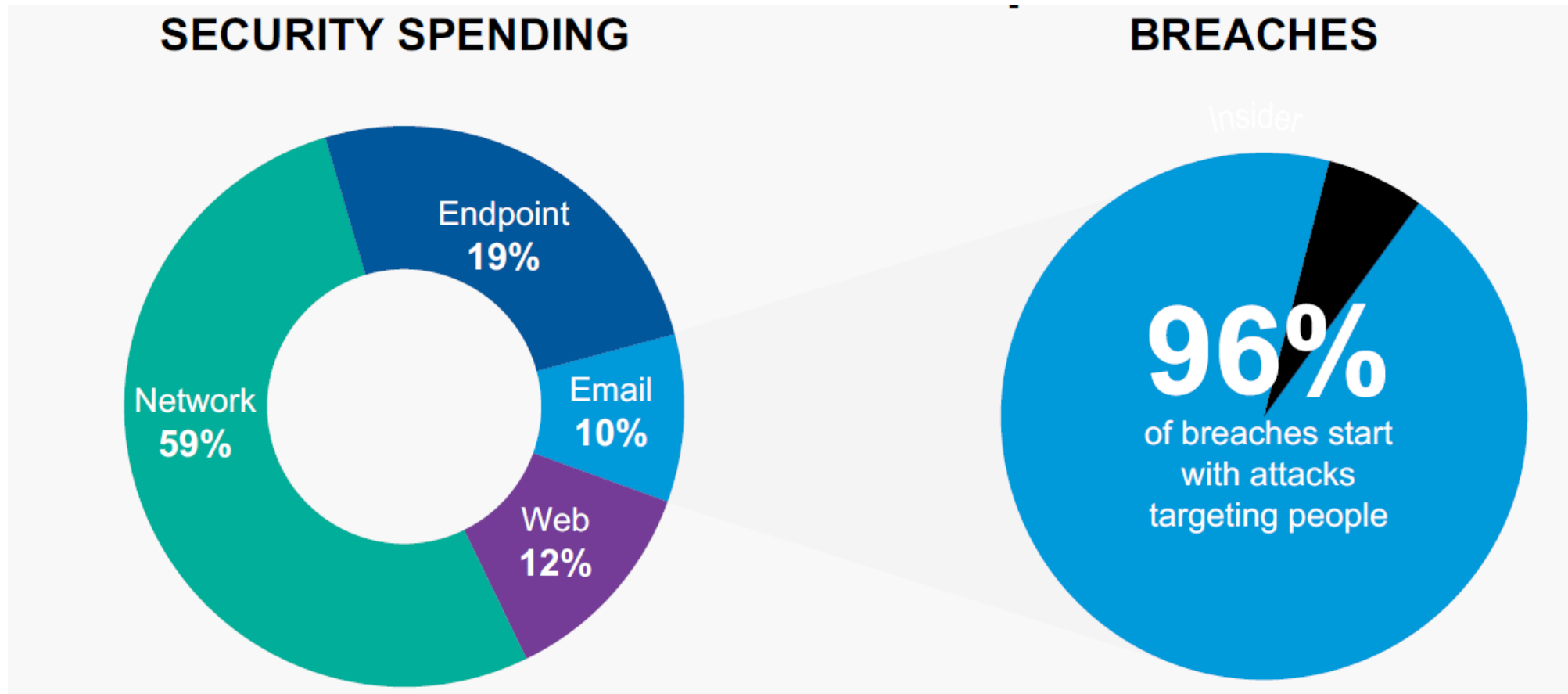
73 malicious attachments*

* Including 2 previously unknown threats

/ Strategia difensiva deve competere con le tattiche degli attaccanti



/ Le aziende non si concentrano sulle persone, gli attaccanti sì



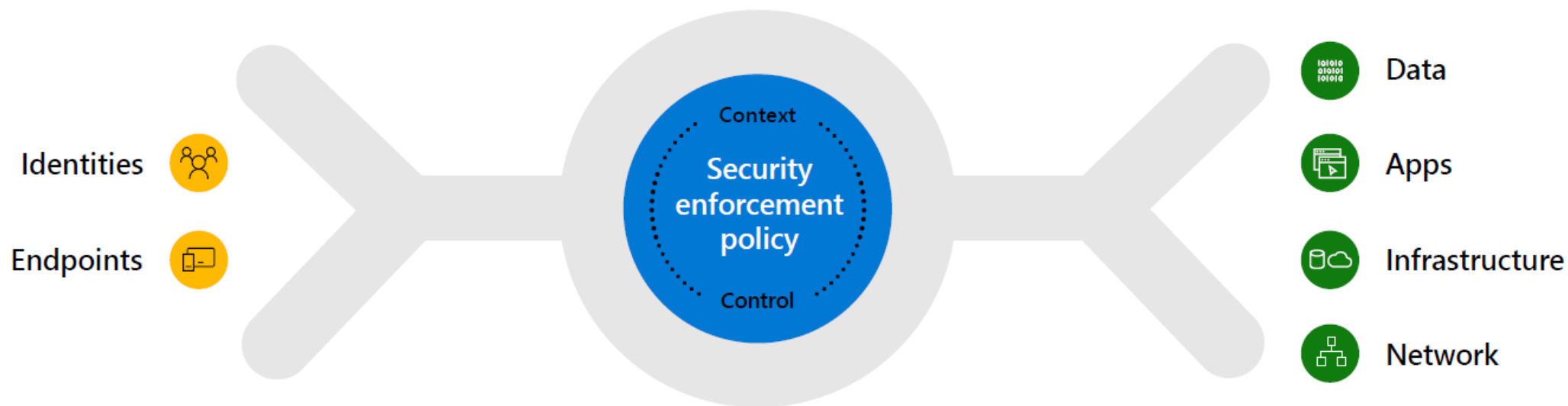
02. DAL DIRE AL FARE

5 DIGITAL TIPS PER NON-NERD

Secure your organization with Zero Trust

Increase security assurances for your critical business assets

Verify explicitly | Use least privilege access | Assume breach



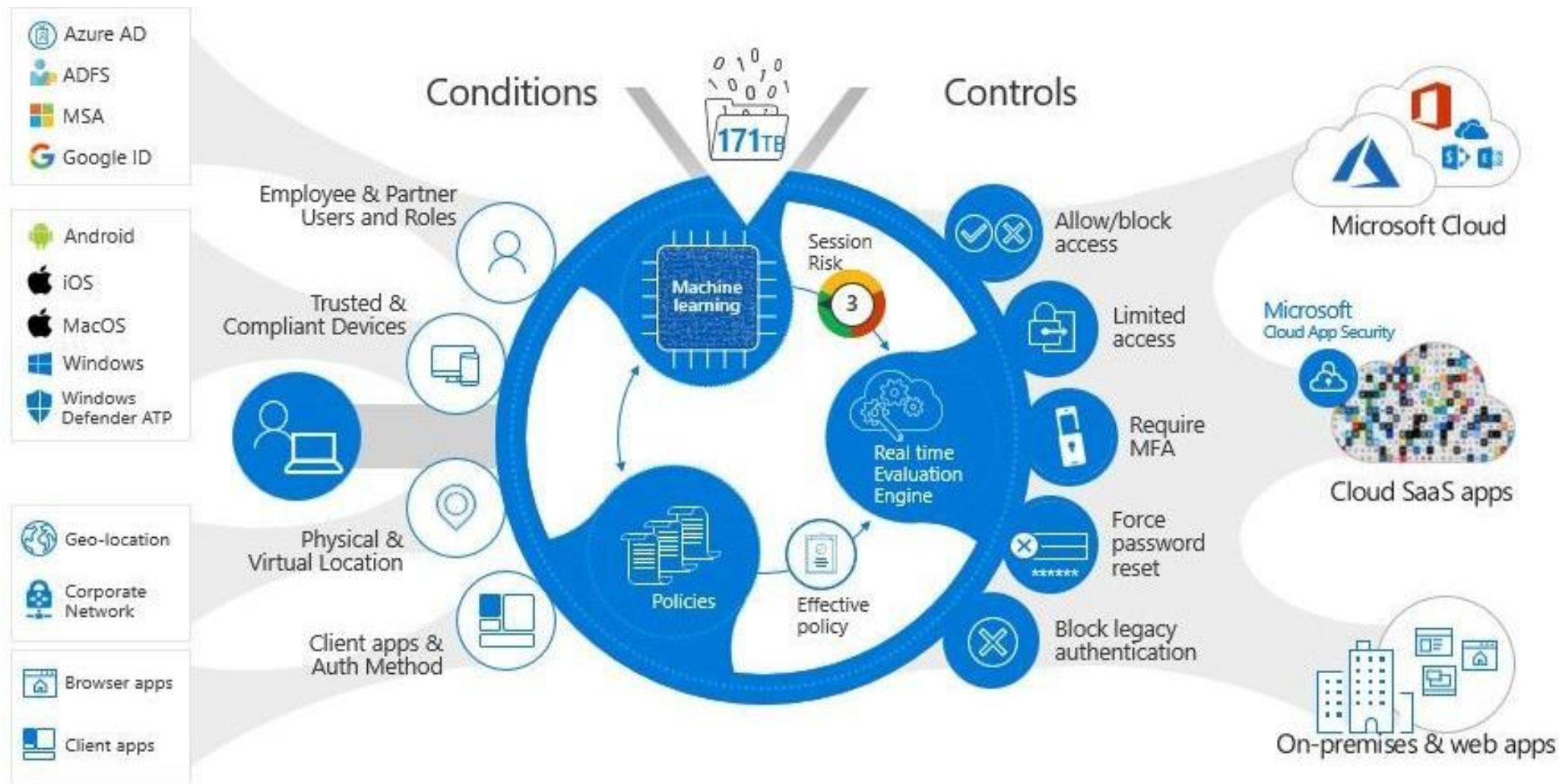
Zero Trust starts with securing the people and the devices they use to get work done.

Visibility | Analytics | Automation

01.

Proteggiamo le identità

Attivazione Multi Factor Authentication in modalità intelligente e su tutte le applicazioni aziendali (conditional access)



Identity



Microsoft 365
Business Premium



RESOL/E

01.

Proteggiamo le identità

Disabilitazione protocolly Legacy



Identity



Microsoft 365
Business Premium

Dashboard > Contoso

Contoso | Sign-ins

Overview

Getting started

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Licenses

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

Company branding

User settings

Date: Last 24 hours Show dates as: Local Client app: 13 selected Add filters

User sign-ins (interactive) User sign-ins (non-interactive) and identity sign-ins

No sign-ins found

Client app

Modern Authentication Clients

- ☐ Browser
- ☐ Mobile Apps and Desktop clients

Legacy Authentication Clients

- ☒ Autodiscover
- ☒ Exchange ActiveSync
- ☒ Exchange Online Powershell
- ☒ Exchange Web Services
- ☒ IMAP
- ☒ MAPI Over HTTP
- ☒ Offline Address Book

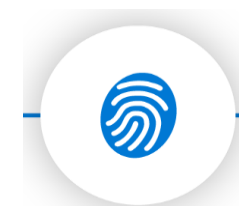
Apply

Date	Request ID	User	IP address	Location	Client app	Conditional acc...	Auth
------	------------	------	------------	----------	------------	--------------------	------

01.

Proteggiamo le identità

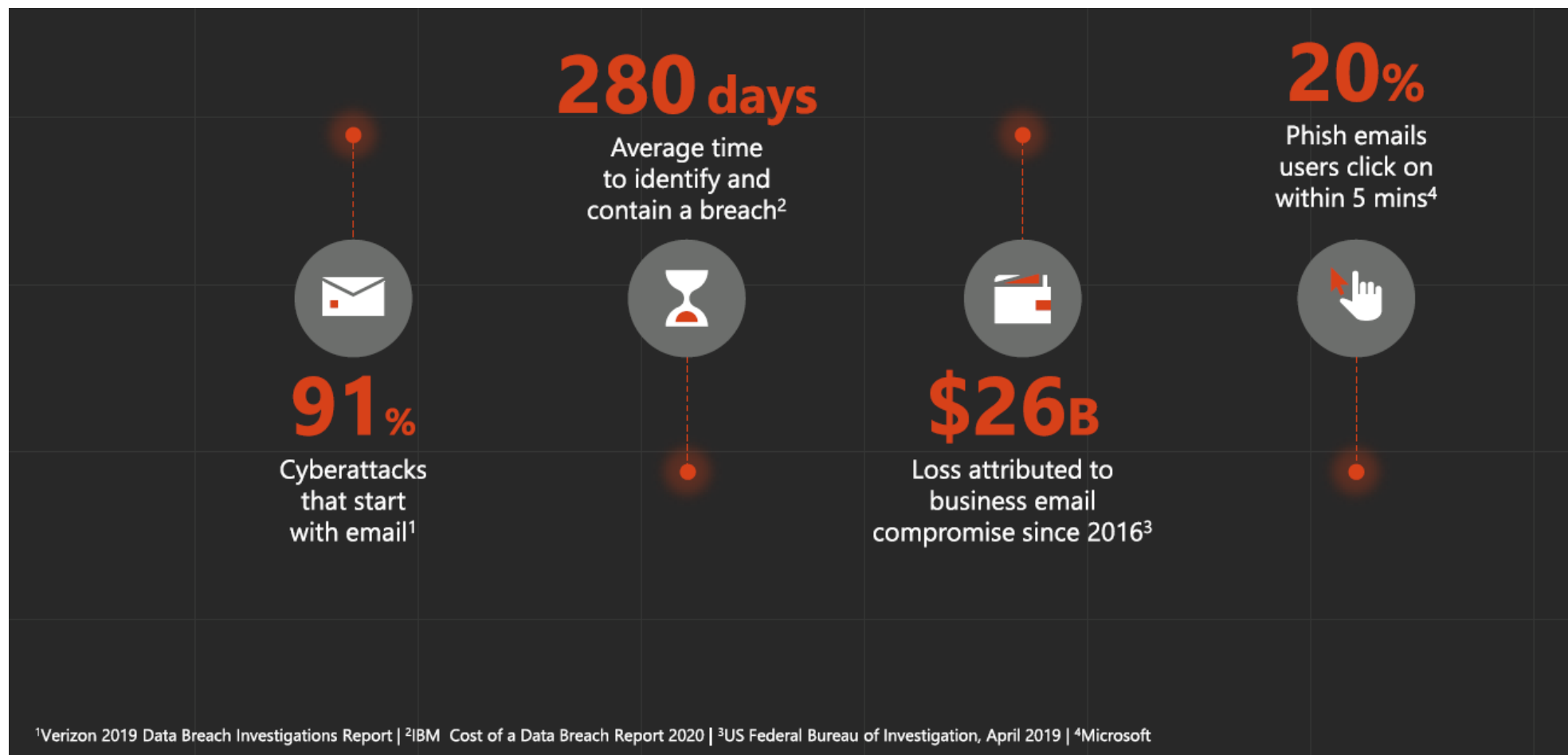
Evitiamo il phishing con i safe links



Identity



Microsoft 365
Business Premium



01.

Proteggiamo le identità

Evitiamo il phishing con i safe links



Identity



Microsoft 365
Business Premium

Fri 12/2/2016 4:07 PM

 **Help Desk**

To: [Redacted]

https://na01.safelinks.protection.outlook.com/?url=http://microsoft-
tk&data=01|01|
edu|b8dc5cf92f1047638fc908d41aff8e84|6
79df878277a496aac8dd99e58606dd9|0&sd
ata=6pmwmkhskc872+s0wj78mhajsov5
wzxtlezkclbbuu=8&reserved=0
Click or tap to follow link.

Your mailbox size has reached 1024.00MB quota.
re-validate your mailbox using the
Click/Copy :- [http://microsoft-
tk](http://microsoft-
tk)

Microsoft support Team



Office 365

Microsoft

 This website has been classified as malicious.

microsoft-
tk

We recommend that you close this web page and not continue to this website. [Learn more about Malware](#)

✕ Close this page.

© 2015 Microsoft | [Legal](#) | [Privacy](#) | [Feedback](#)

01.

Proteggiamo le identità

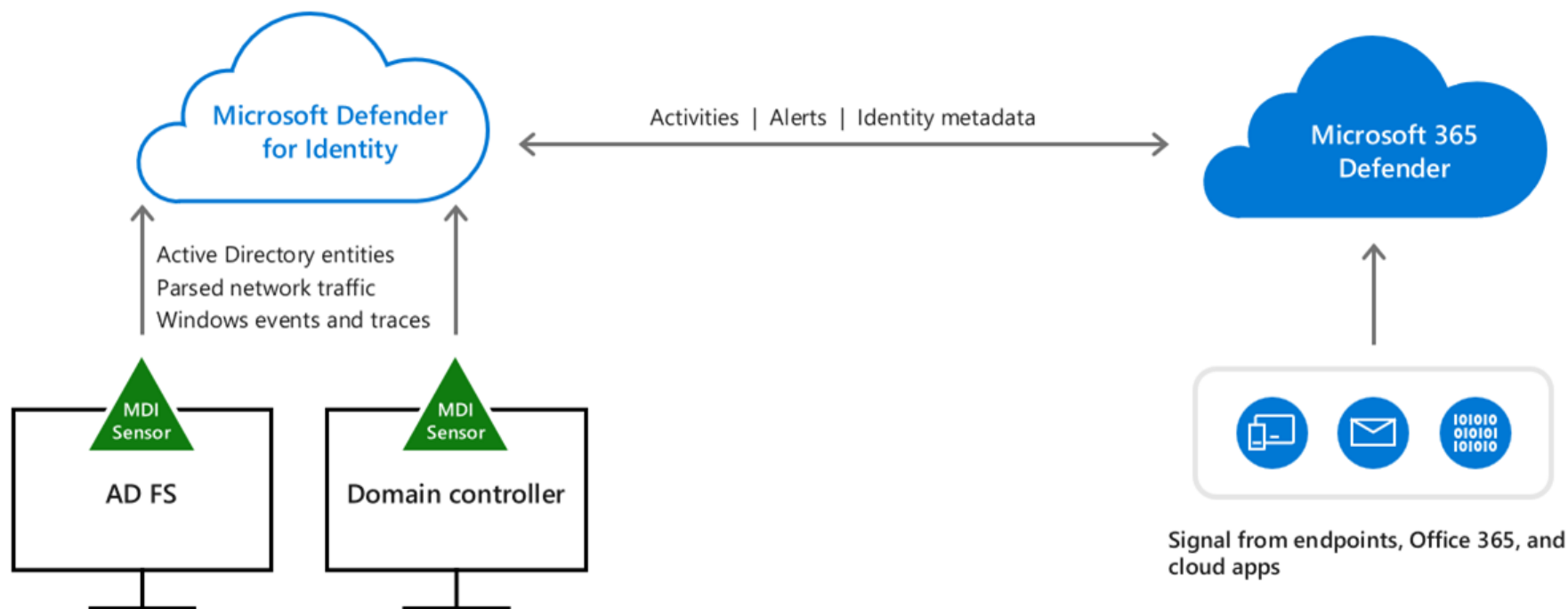
Introduciamo Microsoft Defender for Identity



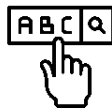
Identity



Microsoft 365
Business Premium



Monitor and profile user behavior and activities



Identify compromised credentials



Detect lateral movements



Reduce the attack surface and protect user identities

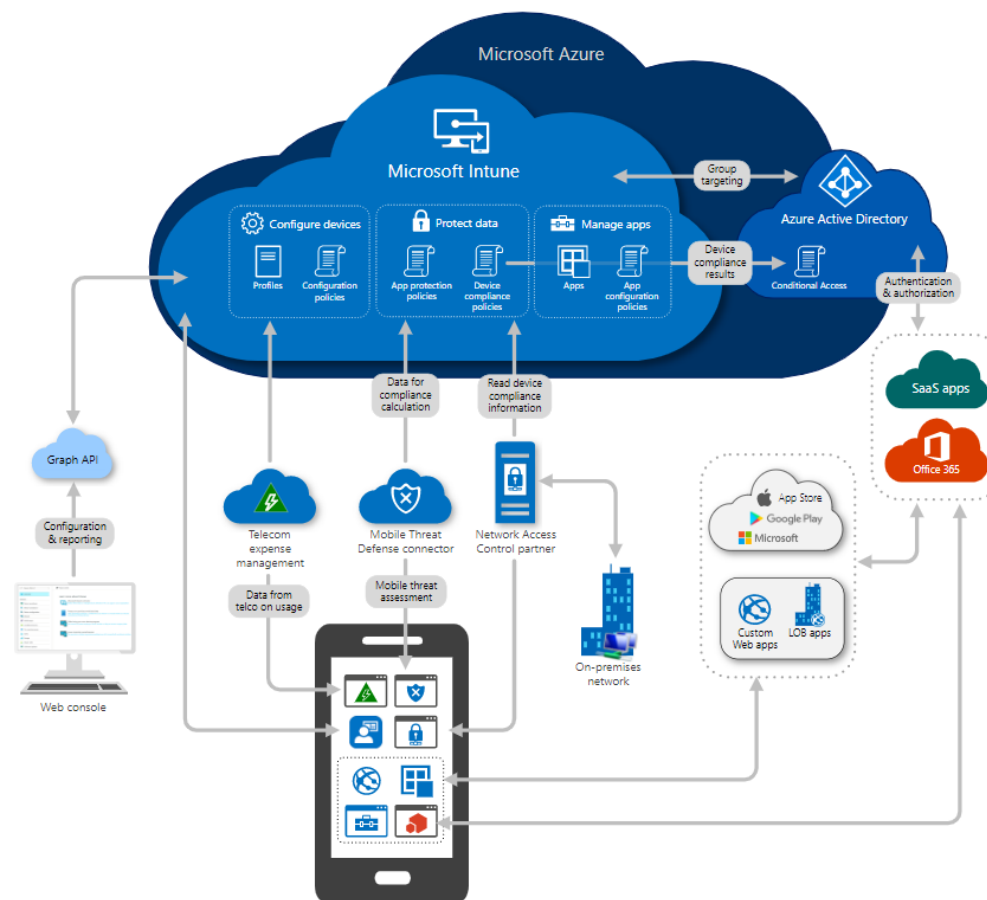
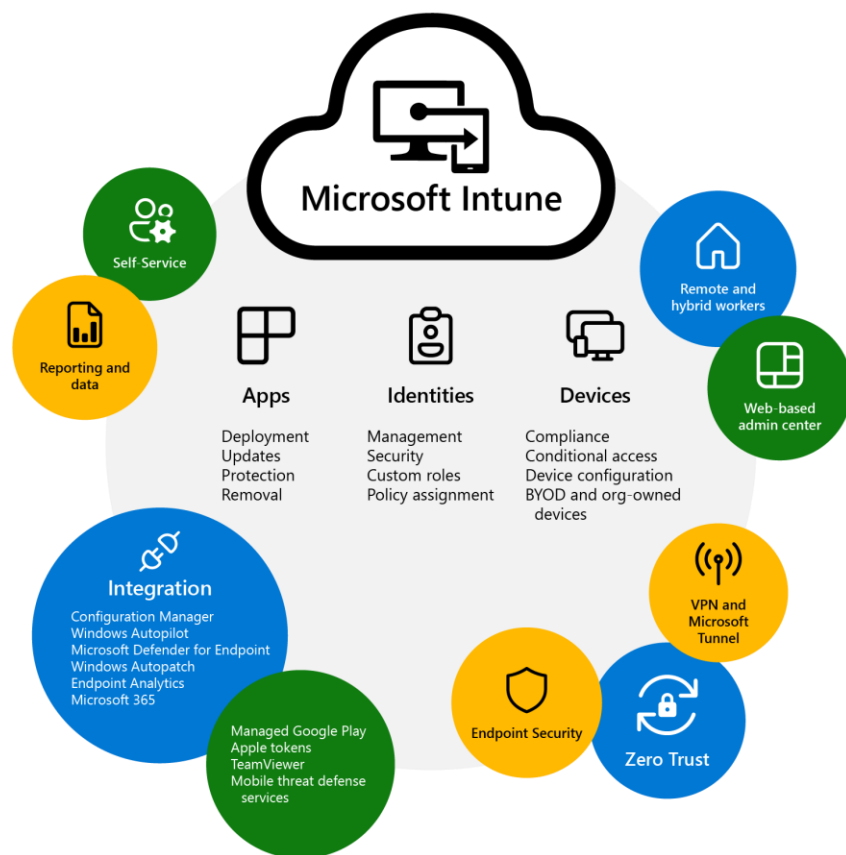


Identify suspicious activities and advanced cyber attacks

RECODE

02. Gestiamo gli endpoint

Gestione dei dispositivi (PC, Tablet, Smartphone)



Endpoints



02. Gestiamo gli endpoint

Microsoft Defender for Endpoint

An industry leader in endpoint security

Gartner

Gartner names Microsoft a **Leader** in 2021 Endpoint Protection Platforms Magic Quadrant.

MITRE ATT&CK

Microsoft **leads in real-world detection** in MITRE ATT&CK evaluation.

FORRESTER

Forrester names Microsoft a **Leader** in 2021 Endpoint Security Software as a Service Wave.



Microsoft Defender for Endpoint awarded a **perfect 5-star rating** by SC Media in 2020 Endpoint Security Review

FORRESTER

Forrester names Microsoft a **Leader** in 2020 Enterprise Detection and Response Wave.



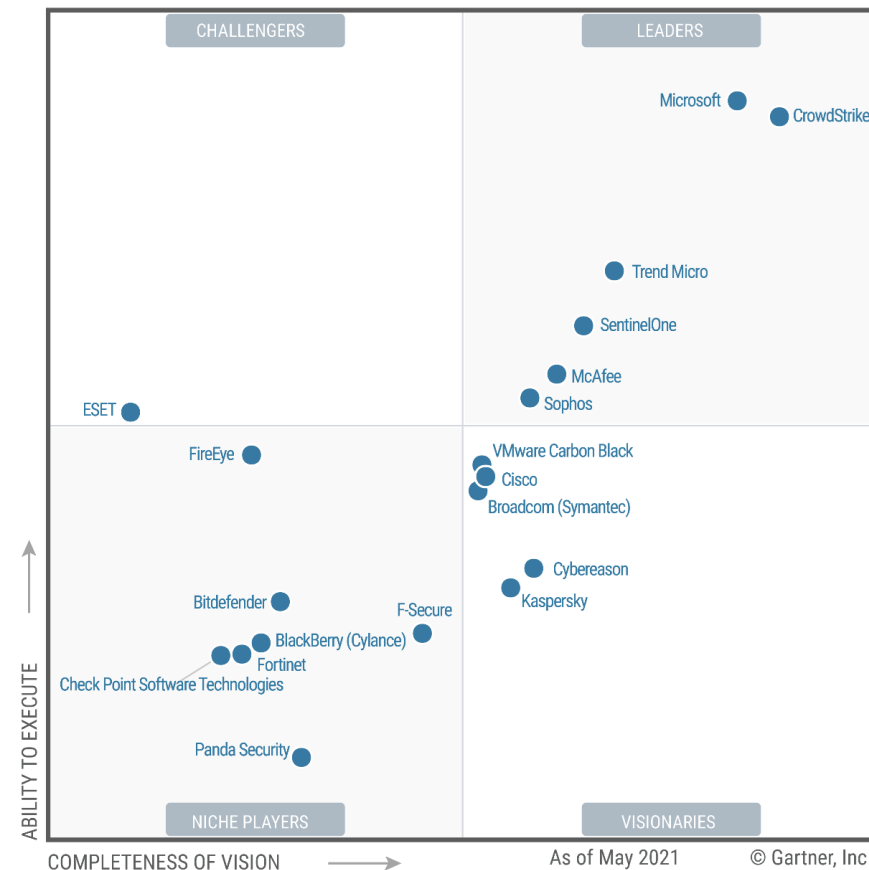
Microsoft won six security awards with Cyber Defense Magazine at RSAC 2021:

- ✓ Best Product Hardware Security
- ✓ Market Leader Endpoint Security
- ✓ Editor's Choice Extended Detection and Response (XDR)
- ✓ Most Innovative Malware Detection
- ✓ Cutting Edge Email Security



Our antimalware capabilities consistently achieve **high scores** in independent tests.

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)



Endpoints



Microsoft 365
Business Premium

03.

Proteggiamo gli endpoint

Microsoft Defender for Endpoint



Endpoints



Microsoft 365
Business Premium



Agentless, basato sul cloud

Nessuna distribuzione o infrastruttura aggiuntiva. Nessun ritardo o problema di compatibilità degli aggiornamenti. Sempre aggiornato.



Ottica senza pari

Basato sulla conoscenza più approfondita del settore delle minacce e dei segnali condivisi tra dispositivi, identità e informazioni.



Sicurezza automatizzata

Porta la tua sicurezza a un nuovo livello passando dall'avviso alla correzione in pochi minuti, su larga scala.

03. Proteggiamo gli endpoint

Microsoft Defender for Endpoint



Endpoints



Microsoft 365
Business Premium

Delivering endpoint security across platforms



Windows macOS

Endpoints and servers

Android iOS

Mobile device OS

Windows 365
Azure Virtual Desktop

Virtual desktops

Cisco Juniper Networks HP Enterprise
Palo Alto Networks

Network devices

03. Proteggiamo gli endpoint

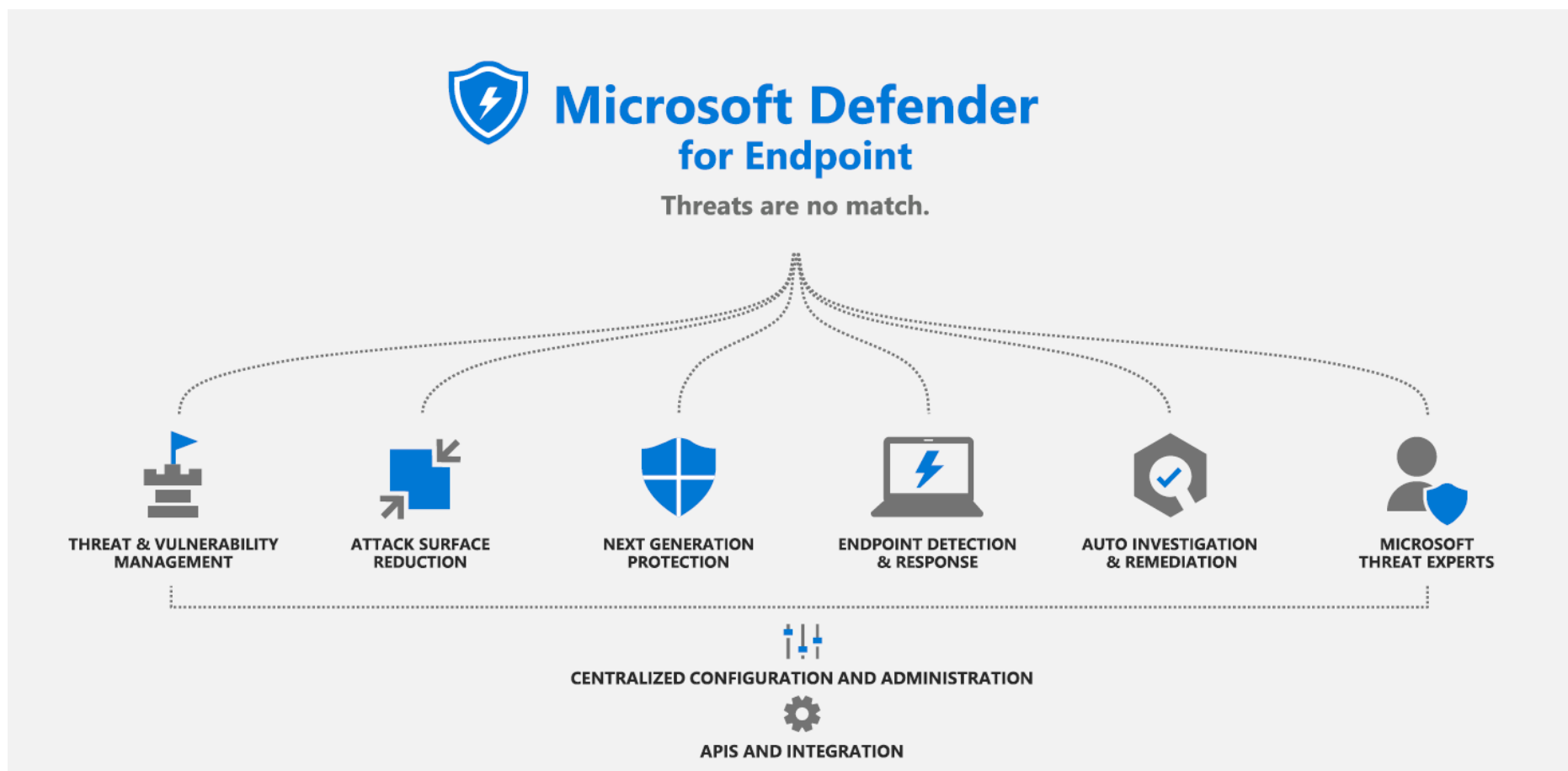
Microsoft Defender for Endpoint



Endpoints

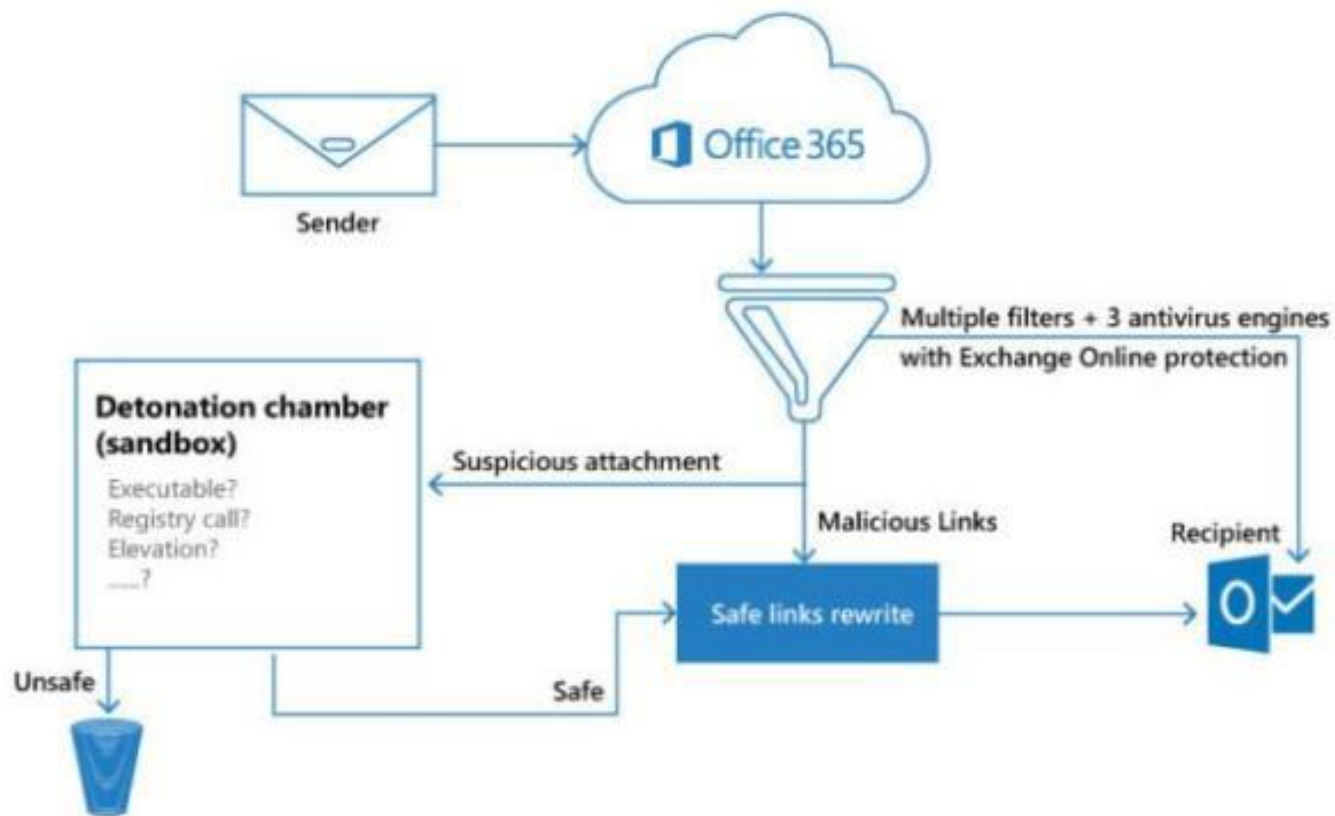


Microsoft 365
Business Premium



03. Proteggiamo gli endpoint

Microsoft Defender for Office 365 – Safe attachment



Endpoints



Microsoft 365
Business Premium

04.

Modifichiamo i comportamenti

Microsoft Defender for Office 365 P2 – Simulazione attacchi



Credential Harvest

Social Engineering

Microsoft landing page



Attack technique goal

Target supplies username and password.

Description

In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a website, the website often shows input boxes for luring the target to submit their username and password. Typically, the page attempting to lure the target will be themed to represent a well-known website to build trust in the target.

Simulation steps



Step 1: User opens the email payload



Step 2: User clicks the link in email payload



Step 3: User enters credentials in form on website

Le simulazioni di attacchi aiutano a valutare la vulnerabilità della tua azienda agli attacchi. Ci sono diverse tipologie di simulazione d'attacco:

- **Raccolta delle credenziali:** tenta di raccogliere le credenziali portando gli utenti a un sito Web dall'aspetto noto con caselle di input per inviare un nome utente e una password.
- **Allegato malware:** aggiunge un allegato dannoso a un messaggio. Quando l'utente apre l'allegato, viene eseguito un codice arbitrario che aiuterà l'attaccante a compromettere il dispositivo del bersaglio.
- **Link in allegato:** un tipo di ibrido di raccolta delle credenziali. Un utente malintenzionato inserisce un URL in un allegato di posta elettronica. L'URL all'interno dell'allegato segue la stessa tecnica della raccolta delle credenziali.
- **Collegamento a malware:** esegue del codice arbitrario da un file ospitato su un noto servizio di condivisione file. Il messaggio inviato all'utente conterrà un collegamento a questo file dannoso. L'apertura del file aiuterà l'attaccante a compromettere il dispositivo del bersaglio.
- **URL drive-by:** l'URL dannoso nel messaggio porta l'utente a un sito Web dall'aspetto familiare che esegue e/o installa codice sul dispositivo dell'utente in modo invisibile all'utente.



Identity



Endpoints



Microsoft 365
Business Premium

04.

Modifichiamo i comportamenti

Microsoft Defender for Office 365 P2 – Simulazione attacchi



Test Accesso credenziali

Ingegneria sociale - Raccolta credenziali Piattaforma di recapito : Email

Stato	Data di avvio	Data di fine	Data di scadenza della formazione	Utenti target
Completato	2/5/2022, 23:53:36	4/5/2022, 23:53:36	3/6/2022, 23:53:36	9638

Impatto simulazione

6 di 9638 utenti compromessi immettendo le credenziali

Compromesso



■ Credenziali immesse ■ Credenziali non immesse

[Visualizza utenti](#)

Payload

1 payload utilizzato

Nome payload

Tipo

[Document Share](#)

Global

Attività di tutti gli utenti

6 di 9638

Messaggio di posta elettronica recapitato correttamente 9638/9638



E-mail segnalate 7/9638



Collegamento tramite posta elettronica selezionato 24/9638



Completamento formazione

2 di 24 utenti che hanno completato la formazione

Phishing mirato al mercato di massa 1/24



Web phishing 2/6



Azioni consigliate

11 Azioni di miglioramento

Classi...	Azione di miglioramento	Impatto Secure Score
1	Require MFA for administrativ...	50
2	Turn on sign-in risk policy	30
3	Turn on user risk policy	30
4	Esige all users complete...	30



Identity



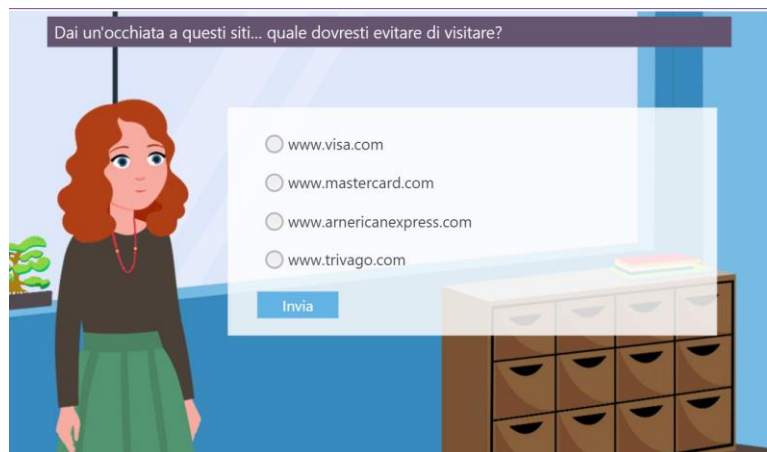
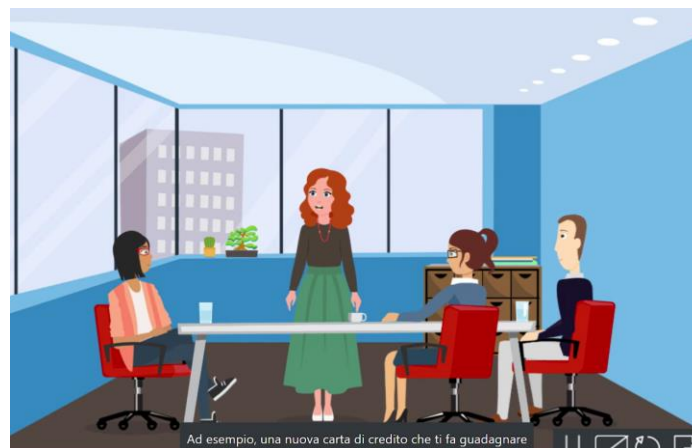
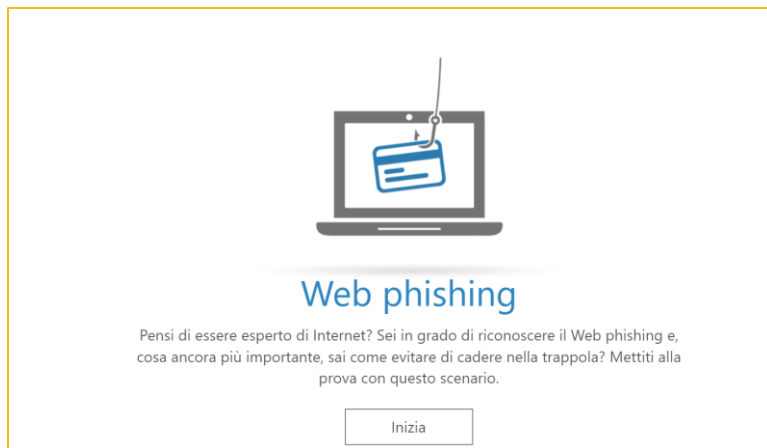
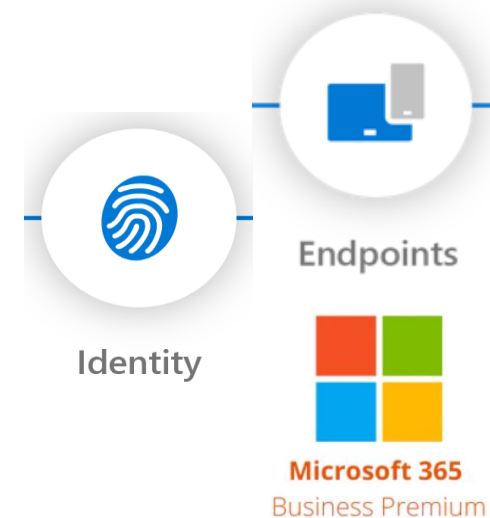
Endpoints



Microsoft 365
Business Premium

04. Modifichiamo i comportamenti

Microsoft Defender for Office 365 P2 – Simulazione attacchi



05. Proteggiamo i dati

Introduzione ad Azure Information Protection



05.

Proteggiamo i dati

Introduzione ad Azure Information Protection



Discover

Detect sensitive data across a variety of locations, based on the rules you define.



Classify and label

Classify sensitive data and apply labels to documents and emails – automatically or manually.



Protect and control sharing

Apply flexible protection actions, such as encryption, access restrictions and visual markings.

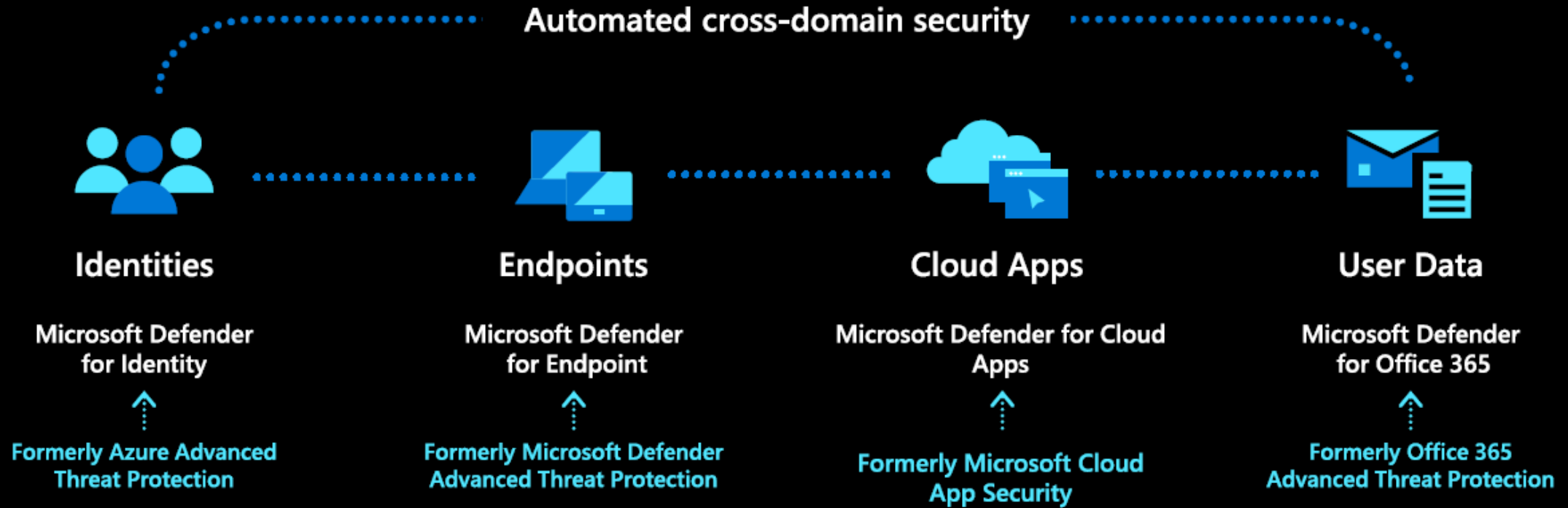


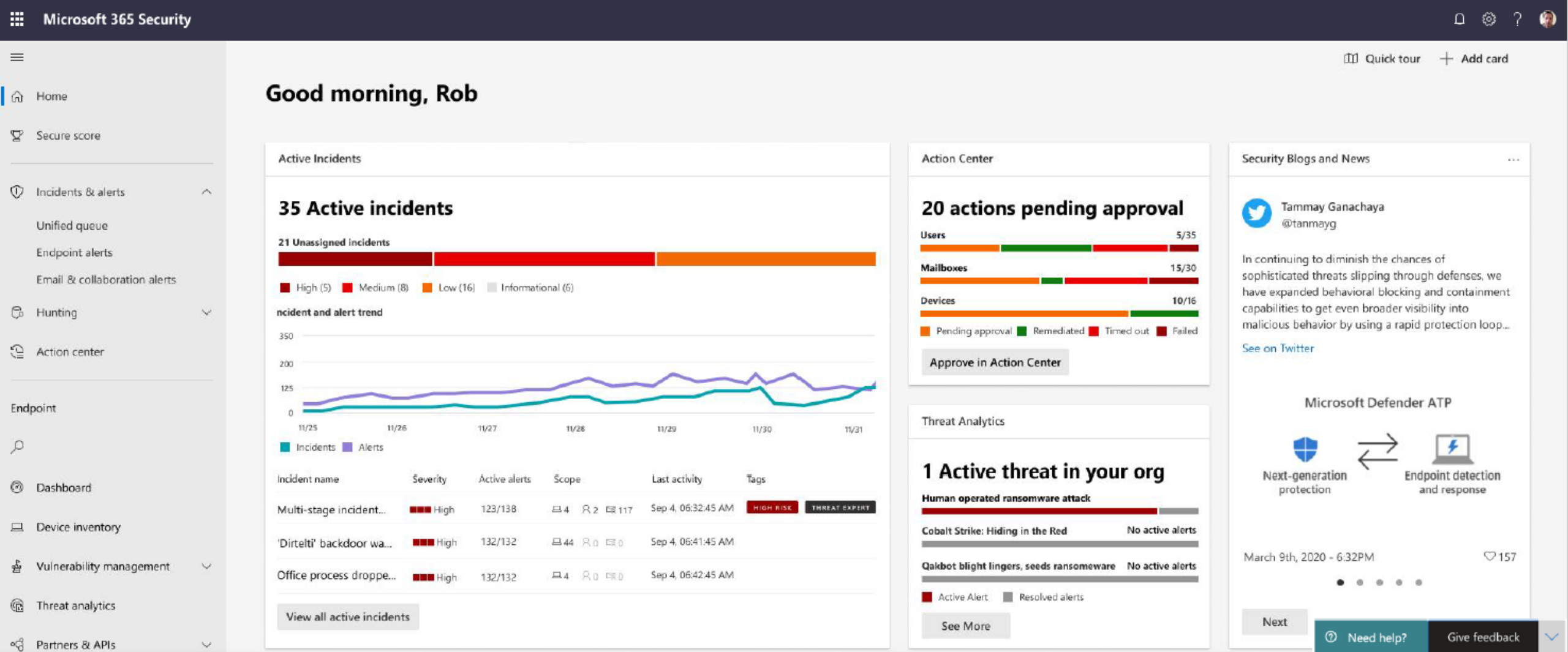
Monitor and remediate

See what's happening with your sensitive data to gain more control over it.



Microsoft 365 Defender





Microsoft 365 Defender Unified Portal

- Microsoft 365 E5 license or any individual product E5 license
- Use Microsoft 365 Defender even if you only have one E5 product, expand over time to get cross-product value

Microsoft 365 Defender Dashboard

- My organization's overall security state
- What's the next highest priority SOC work item

03. MS365 PER LA CYBERSECURITY

**DEMO LIVE:
PROTEGGERE I DATI
DA OVUNQUE**

03. DAL DIRE AL FARE

CASO DI SUCCESSO

/ PMI cliente

/1

**Migrazione della posta
e attivazione nuove
funzionalità di
collaboration**

/3

**Migrazione dati su SharePoint
Online, e degli altri workload su
soluzioni SaaS o VM in azure.
Attivazione defender for Endpoint**

/2

**Onboarding di tutti i dispositivi
su Intune, attivazione
conditional access e regole
safe-links, safe-attachment**

/4

**Dimissione dell'ambiente
on-prem**

CYBERSECURITY MULTILIVELLO CON MS365

/ DOMANDE

Chiedete in chat le vostre curiosità

CYBERSECURITY MULTILIVELLO CON MS365

/ CONTATTI

Resolve è la divisione consulenza di ErgonGroup

CONTATTI

✉ info@resolve-consulenza.it

🌐 www.resolve-consulenza.it

☎ +39 049 636 5600

Sede legale

Viale Dell'Industria, 21
35129 – Padova (PD)

Sedi operative

Friuli Venezia Giulia, Veneto,
Lombardia, Toscana, Marche

RESOL/E

by ErgonGroup