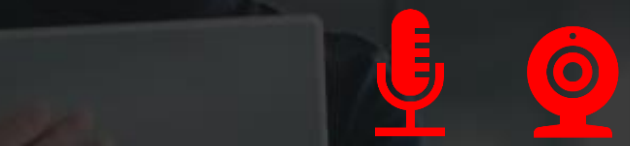
RESOLVE

by ErgonGroup

PRIMA DI INIZIARE



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

RESOLVE

/ Digital

DIRETTA LIVE

Cybersecurity multilivello con Microsoft 365

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

RESOL/E

/ CHI SIAMO

SPEAKER

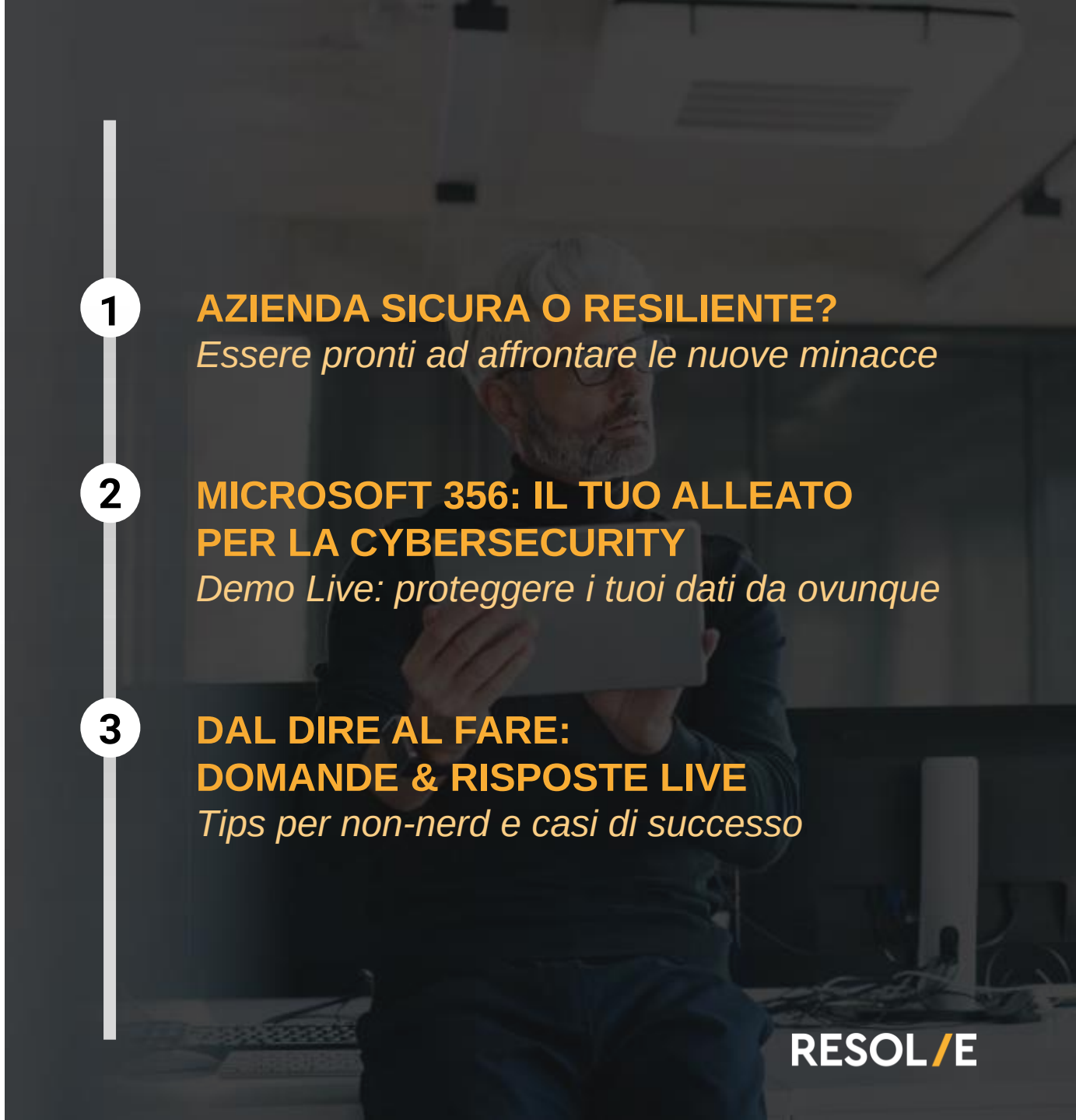
MICHELE RUBERTI

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**.

RESOL/E

/ 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

RESOL/E

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)

Fonti: Forbes: *Alarming Cybersecurity Stats: What You Need To Know For 2021* di Chuck Brooks; CSO: *Top cybersecurity facts, figures and statistics* di Josh Fruhlinger; Comparitech: *300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends* di Andra Zaharia; IBM Security: *Cost of a Data Breach Report 2020* Verizon: *Data Breach Investigations Report 2020*

RESOL/E

/ 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.

RESOL/E

/ 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

RESOL/E

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

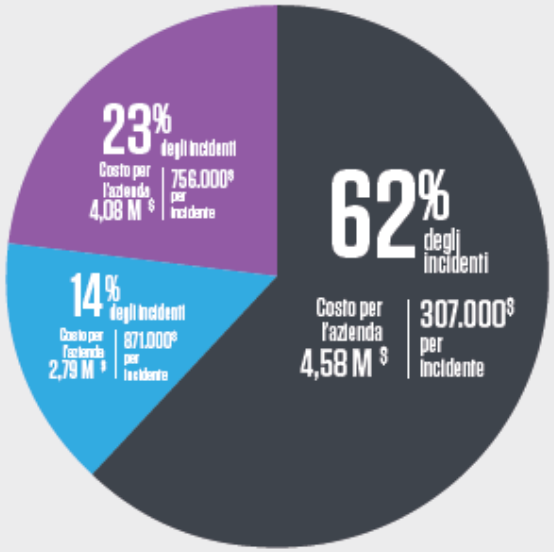
Tempo medio necessario per contenere un incidente di origine interna

Dal 2018, il costo delle minacce interne è cresciuto del

31%

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

47%



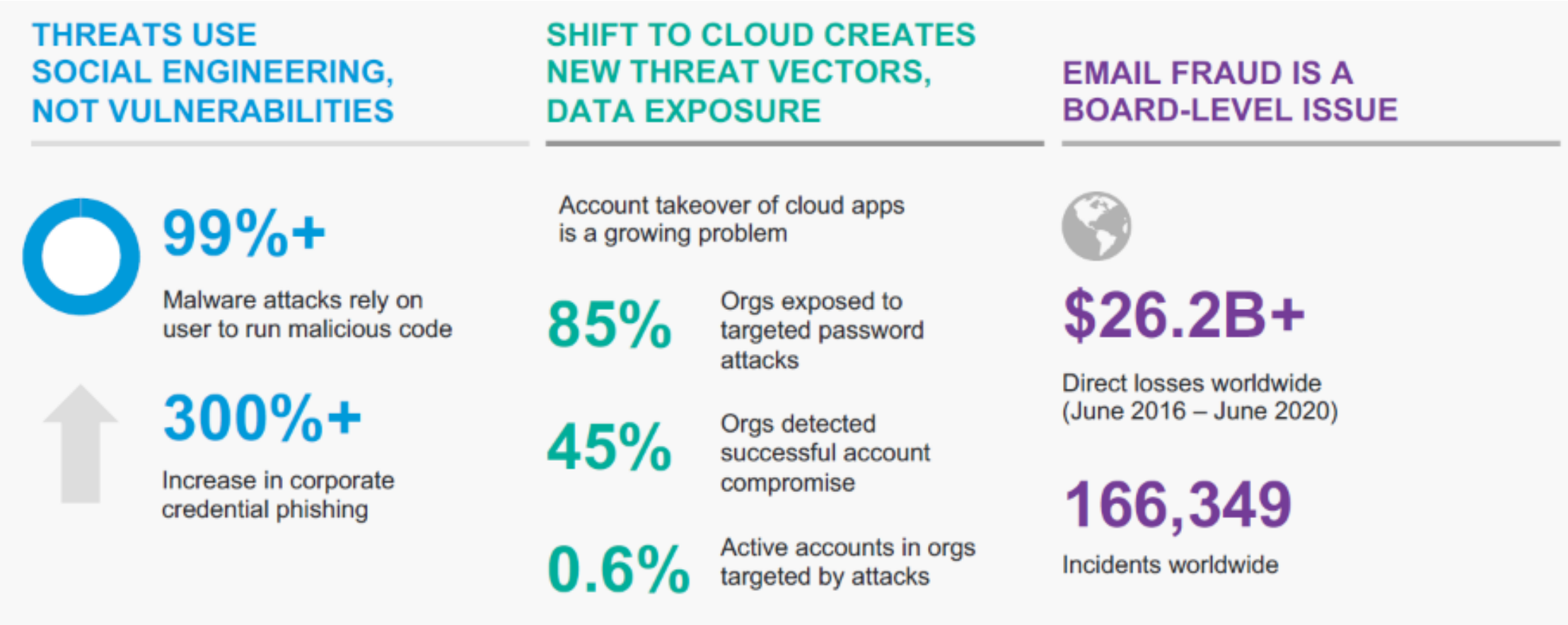
- Collaboratori interni negligenti
- Utenti interni malintenzionati
- Furto delle credenziali di accesso

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

RESOLVE

/ Persone, non infrastrutture

Il nuovo bersaglio degli «hacker»

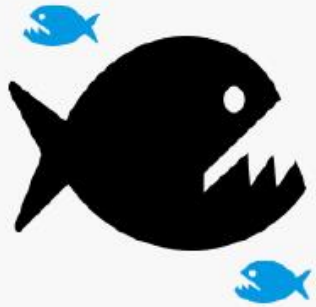


RESOL/E

/ Panorama delle minacce

Cosa può accadere in 30 giorni a una PMI?

129 email attacks



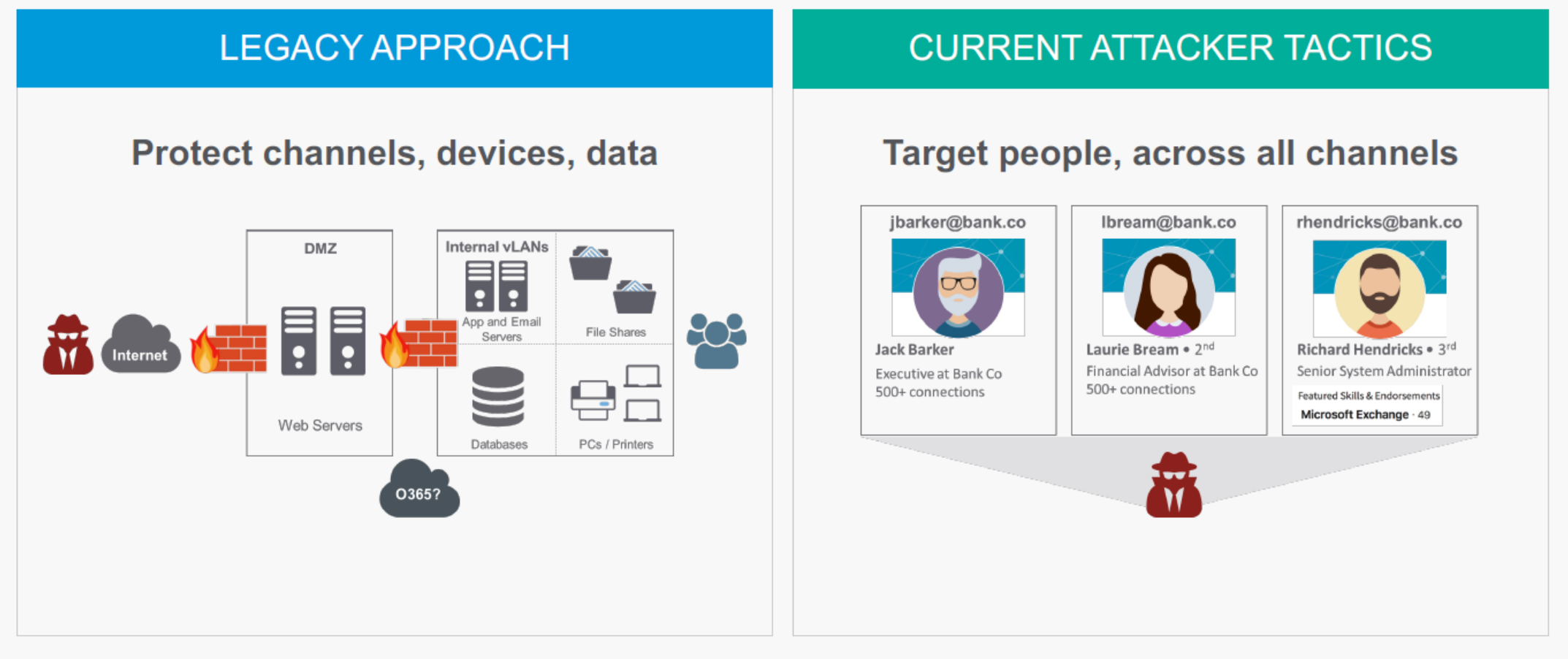
57 phishing attacks

73 malicious attachments*

* Including 2 previously unknown threats

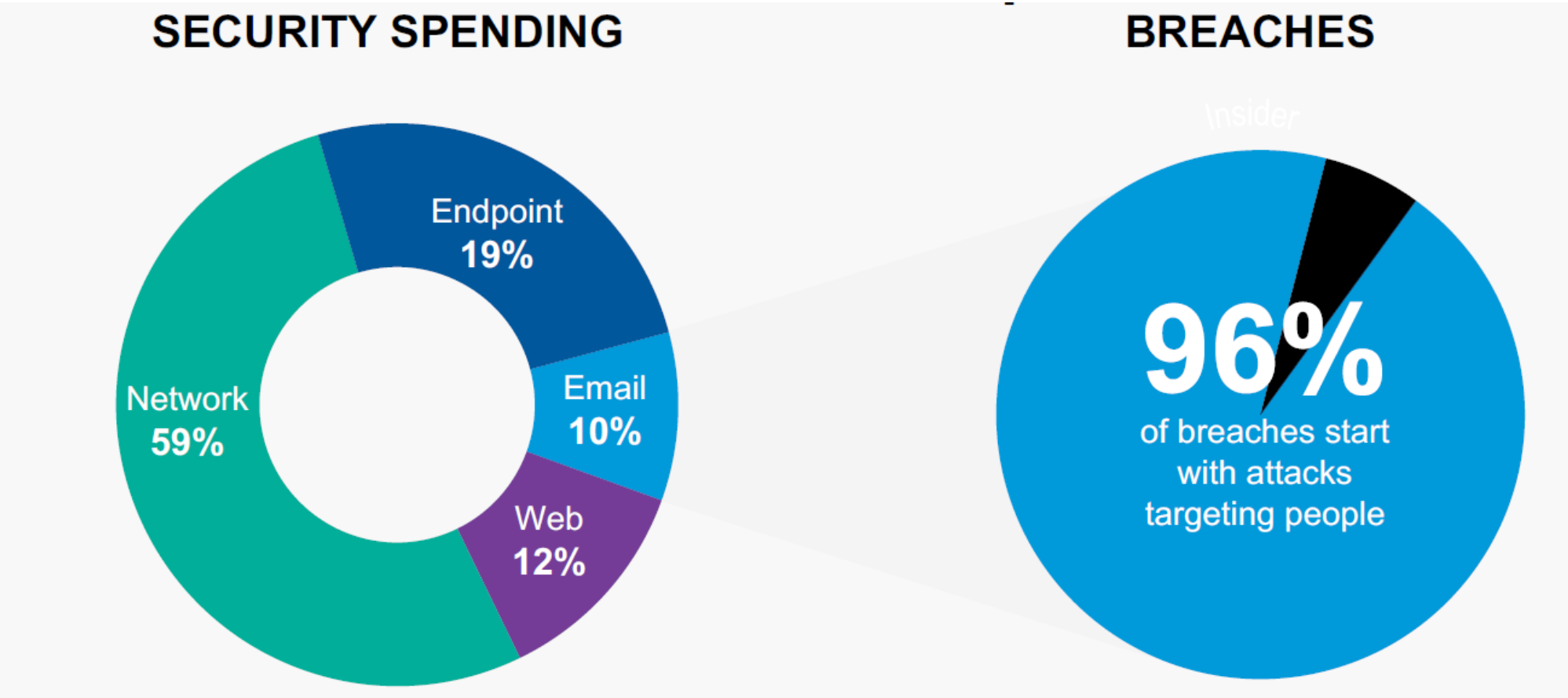
RESOL/E

/ Strategia difensiva deve competere con le tattiche degli attaccanti



RESOL/E

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



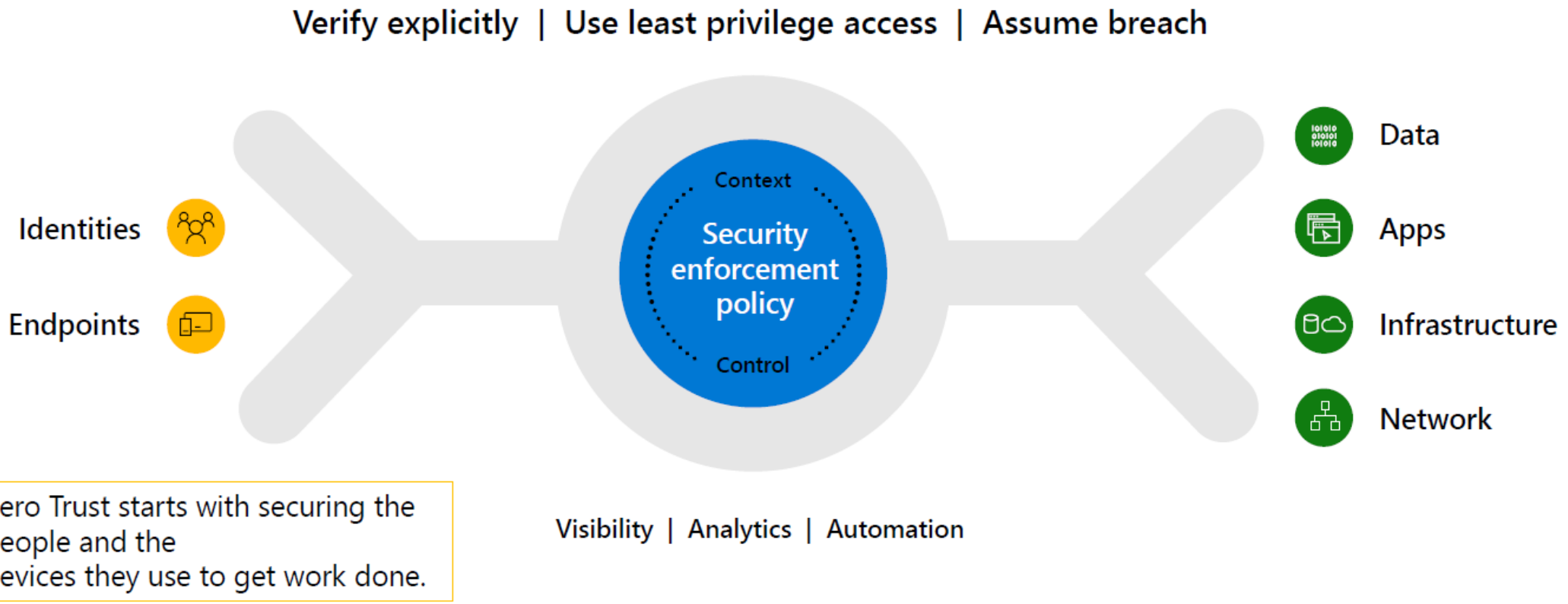
RESOL/E

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



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

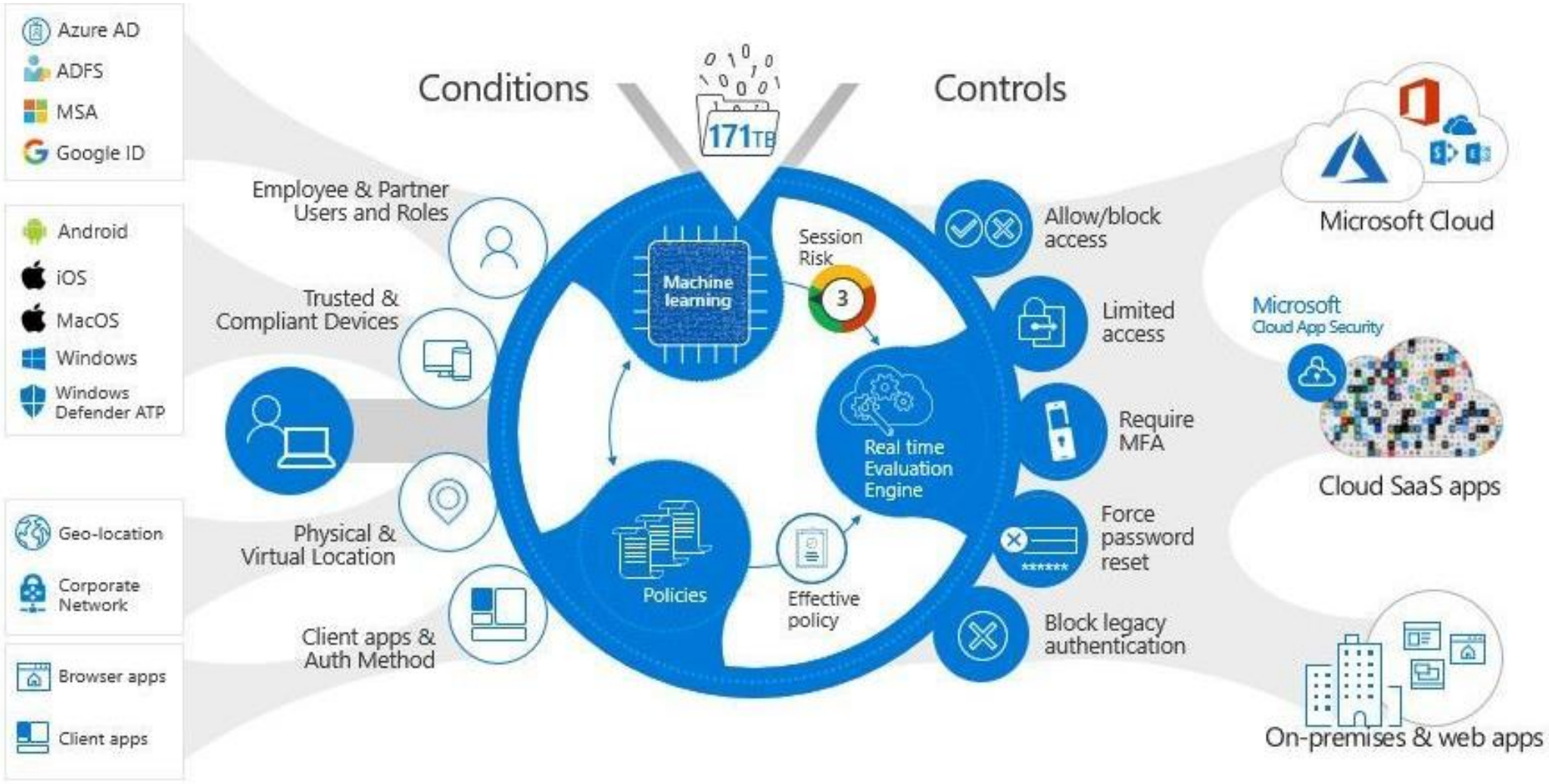
RESOLVE

01. Proteggiamo le identità

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

Identity

Microsoft 365
Business Premium



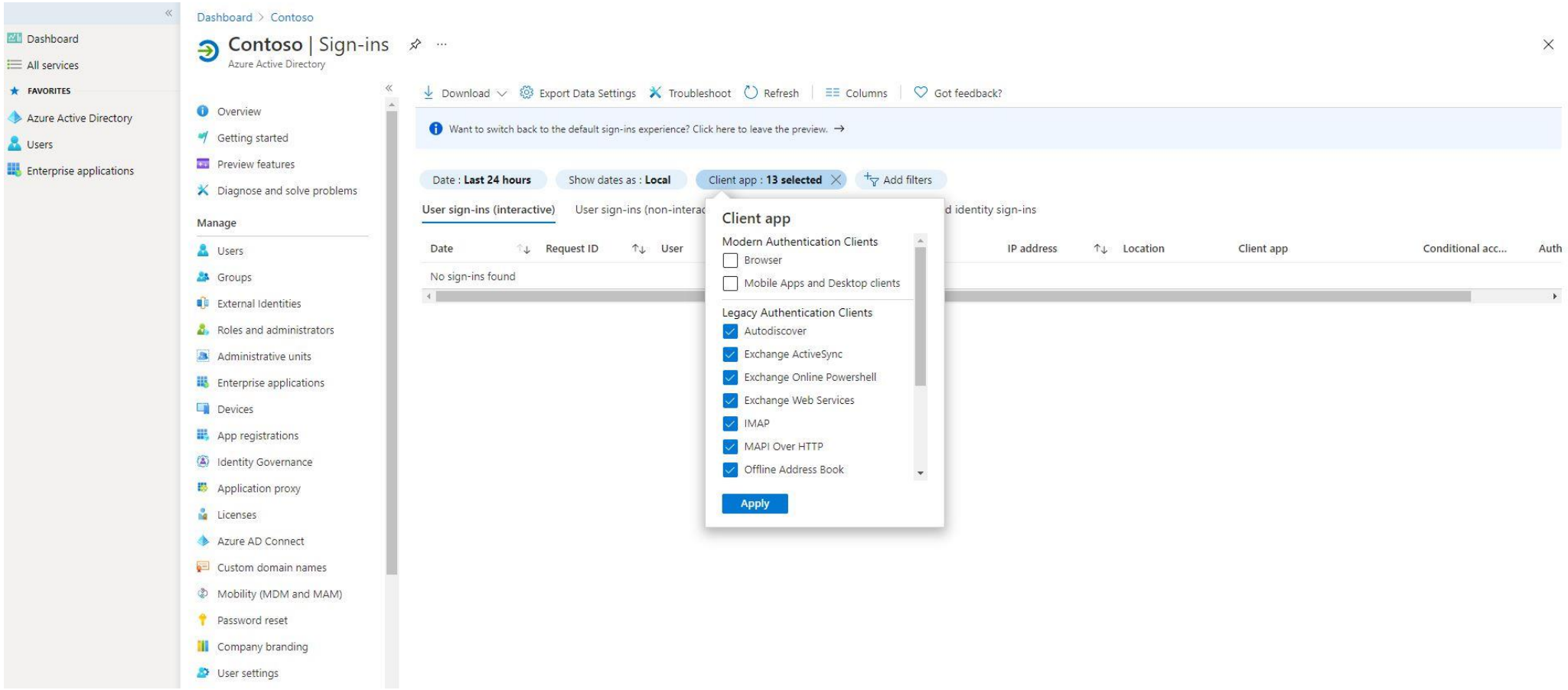
RESOLVE

01. Proteggiamo le identità

Disabilitazione protocolly Legacy

Identity

Microsoft 365
Business Premium



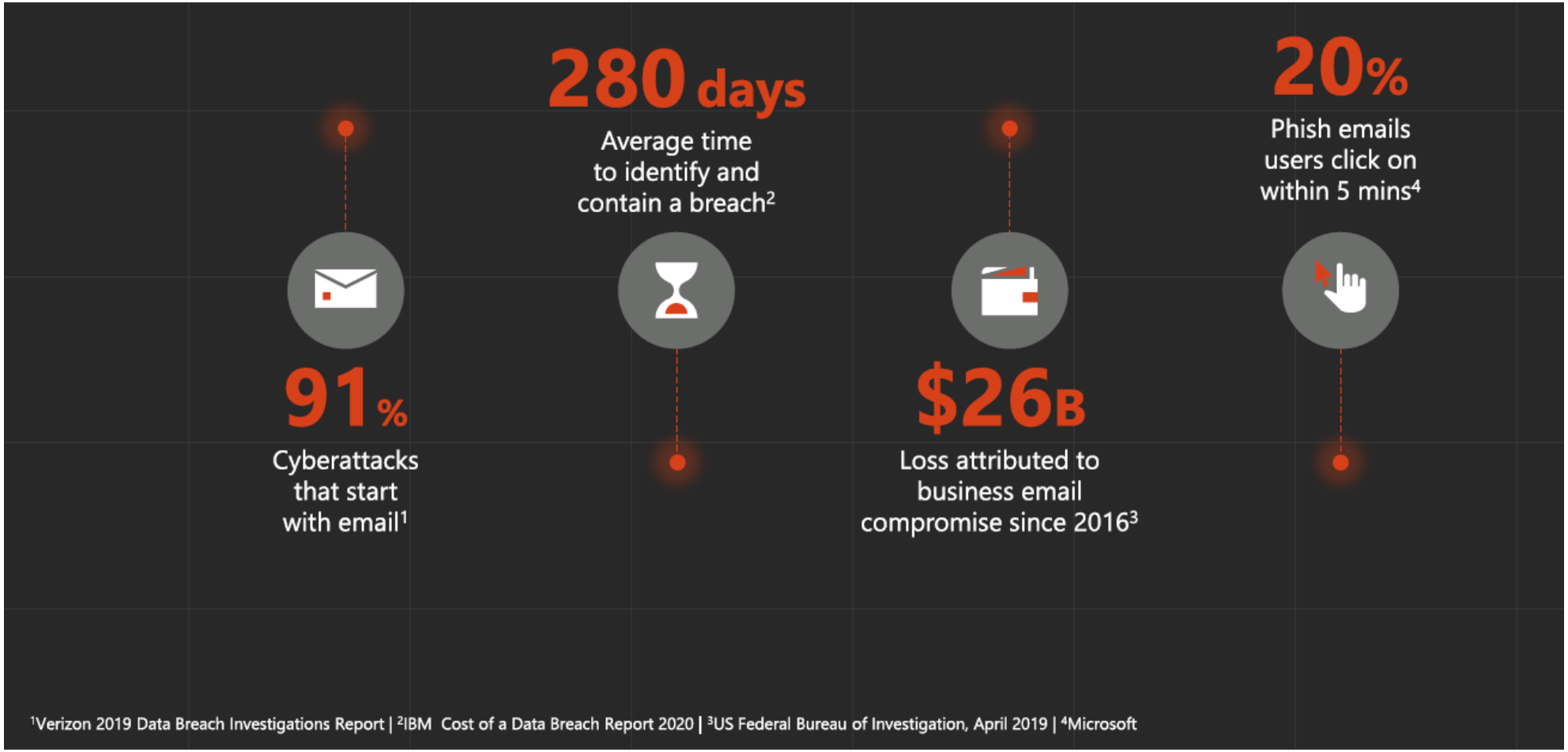
RESOLVE

01. Proteggiamo le identità

Evitiamo il phishing con i safe links

Identity

Microsoft 365
Business Premium



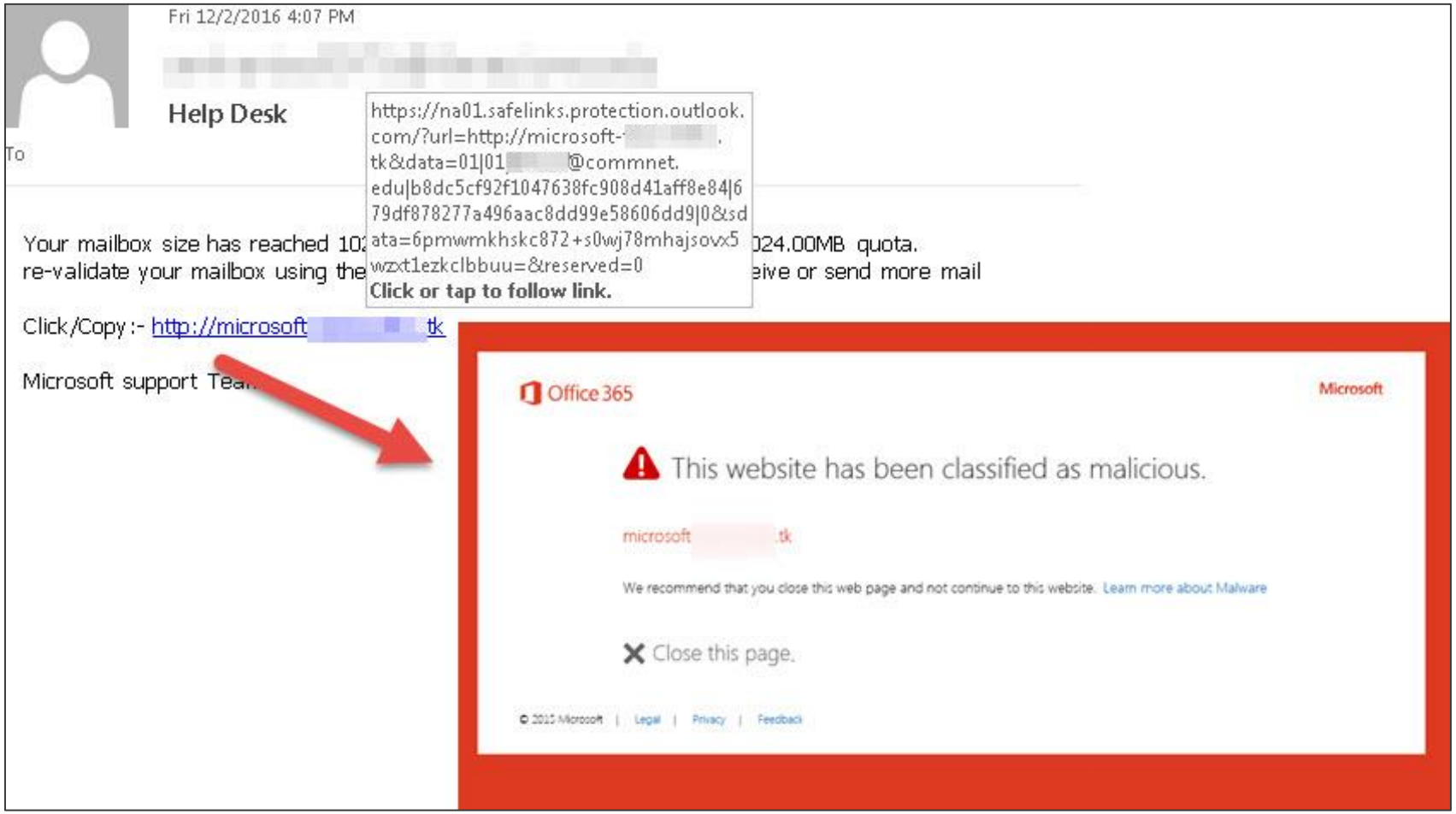
RESOLVE

01. Proteggiamo le identità

Evitiamo il phishing con i safe links

Identity

Microsoft 365
Business Premium



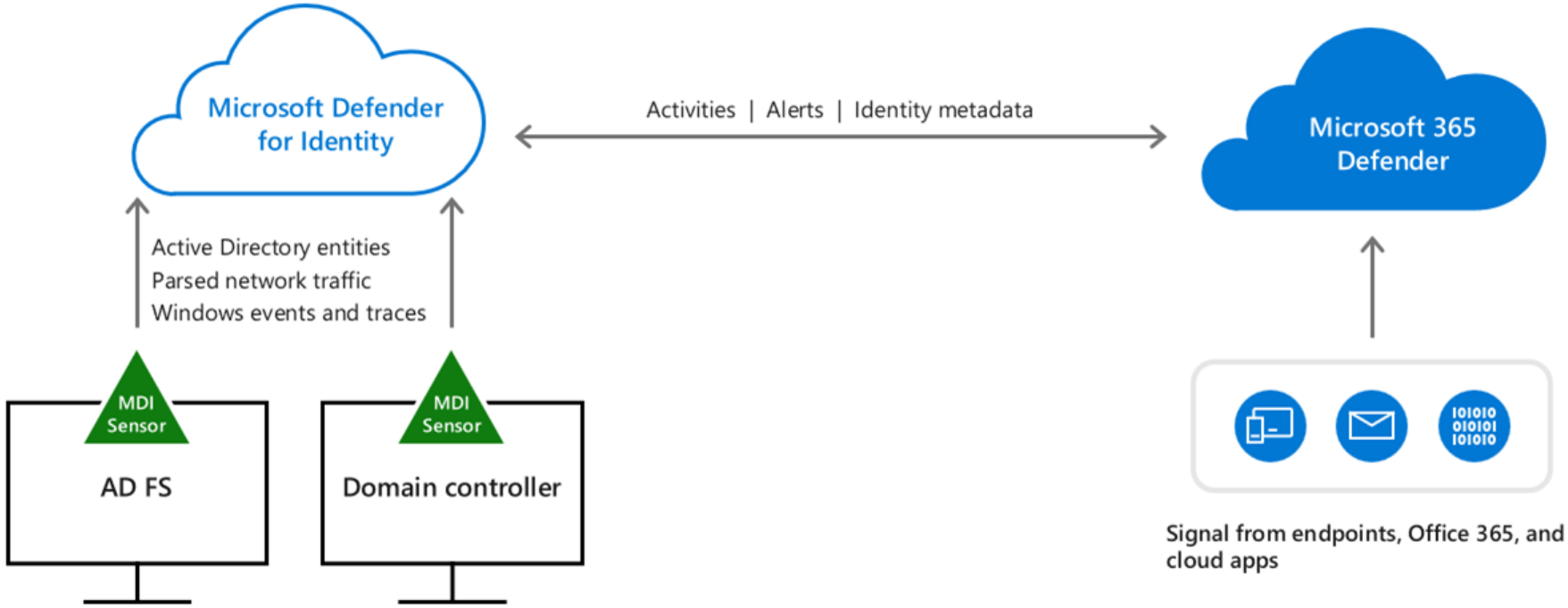
RESOLVE

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

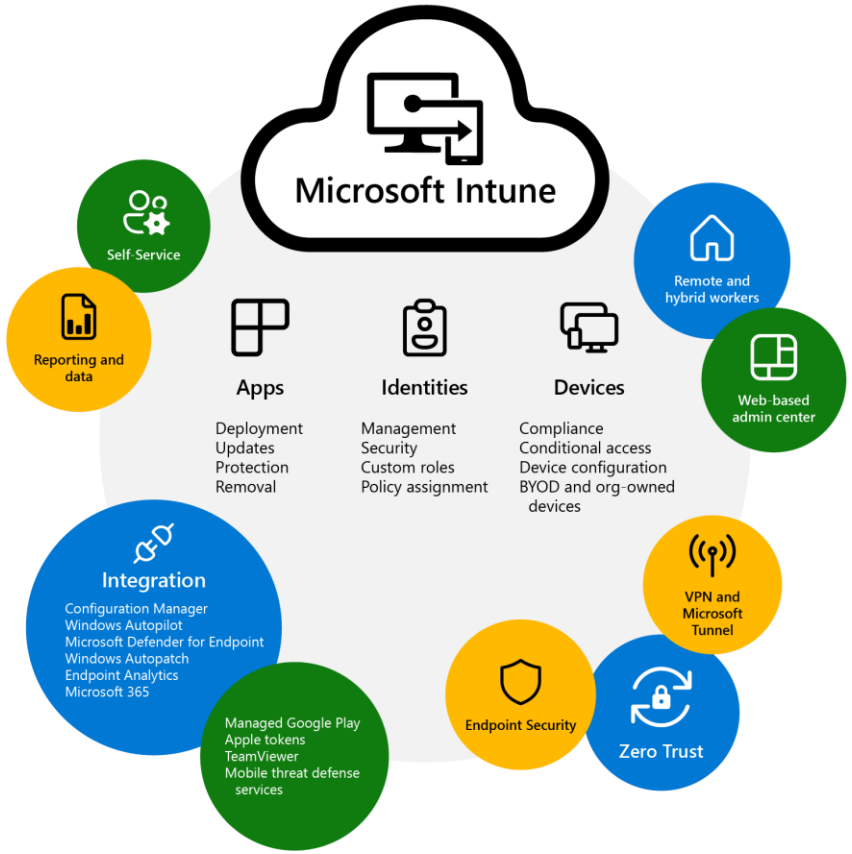
Identify suspicious activities and advanced cyber attacks

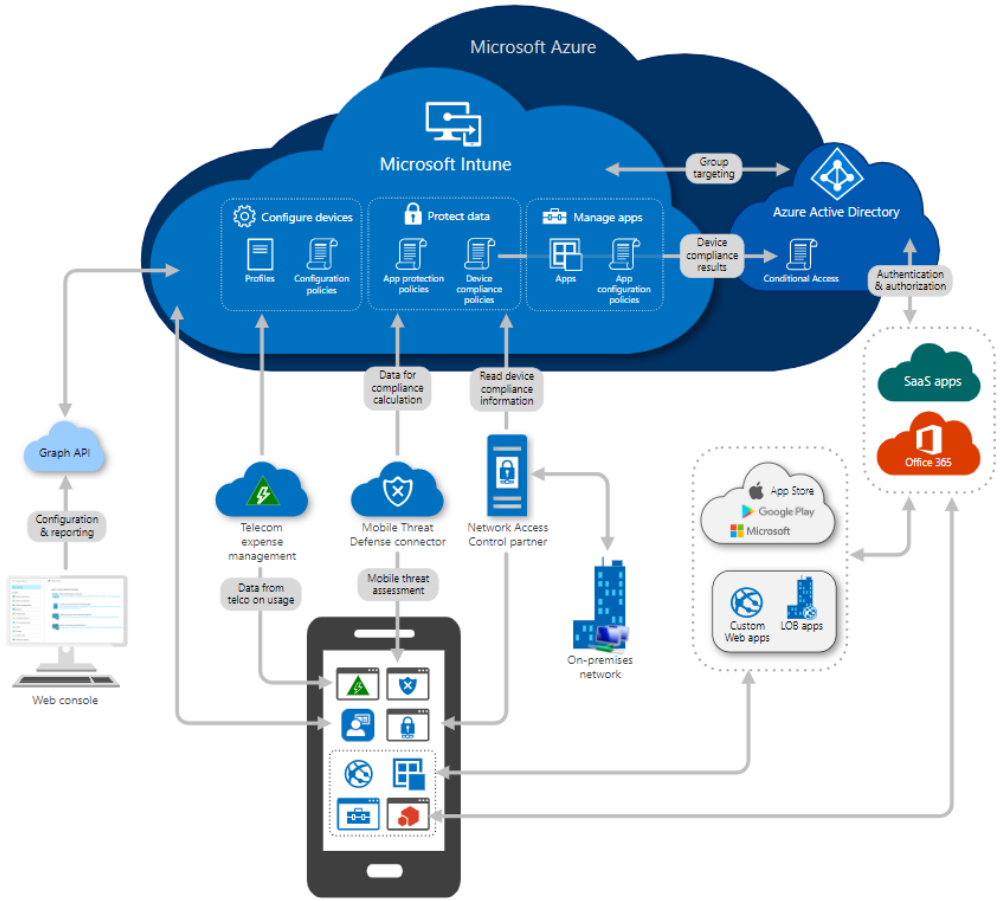
02. Gestiamo gli endpoint

Gestione dei dispositivi (PC, Tablet, Smartphone)

Endpoints

Microsoft 365
Business Premium





RESOLVE

02. Gestiamo gli endpoint

Microsoft Defender for Endpoint

Endpoints

Microsoft 365
Business Premium

An industry leader in endpoint security

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

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

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

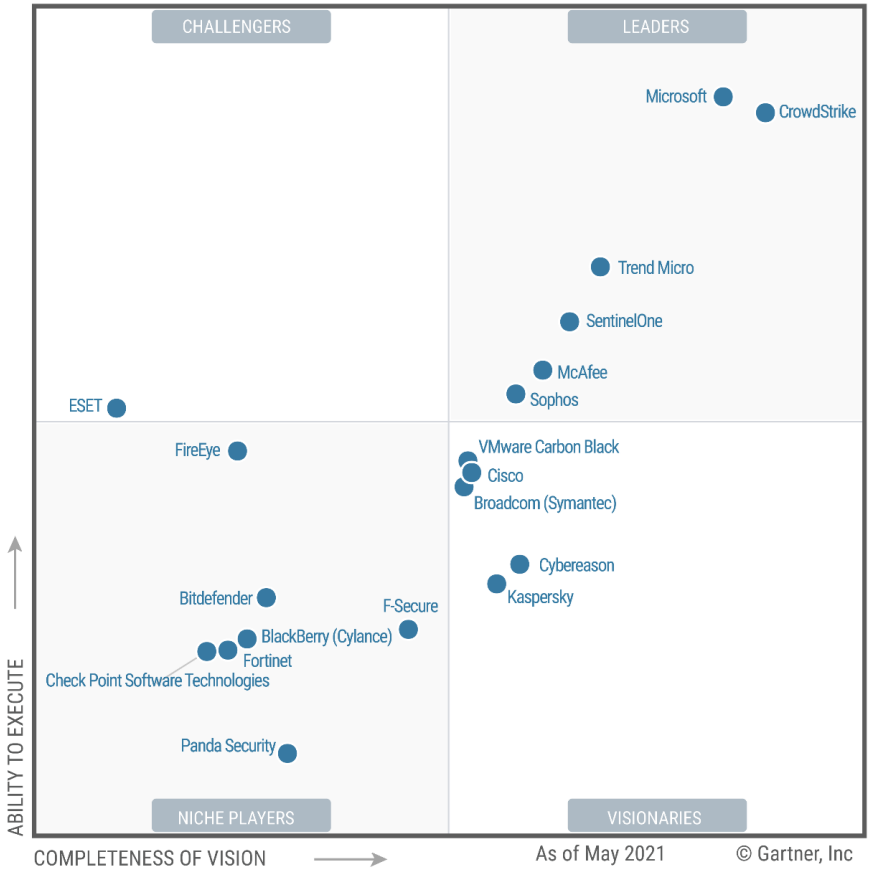
Forrester names Microsoft a Leader in 2020 Enterprise Detection and Response Wave.

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)

RESOLVE

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.

RESOLVE

03. Proteggiamo gli endpoint

Microsoft Defender for Endpoint

Endpoints

Microsoft 365
Business Premium

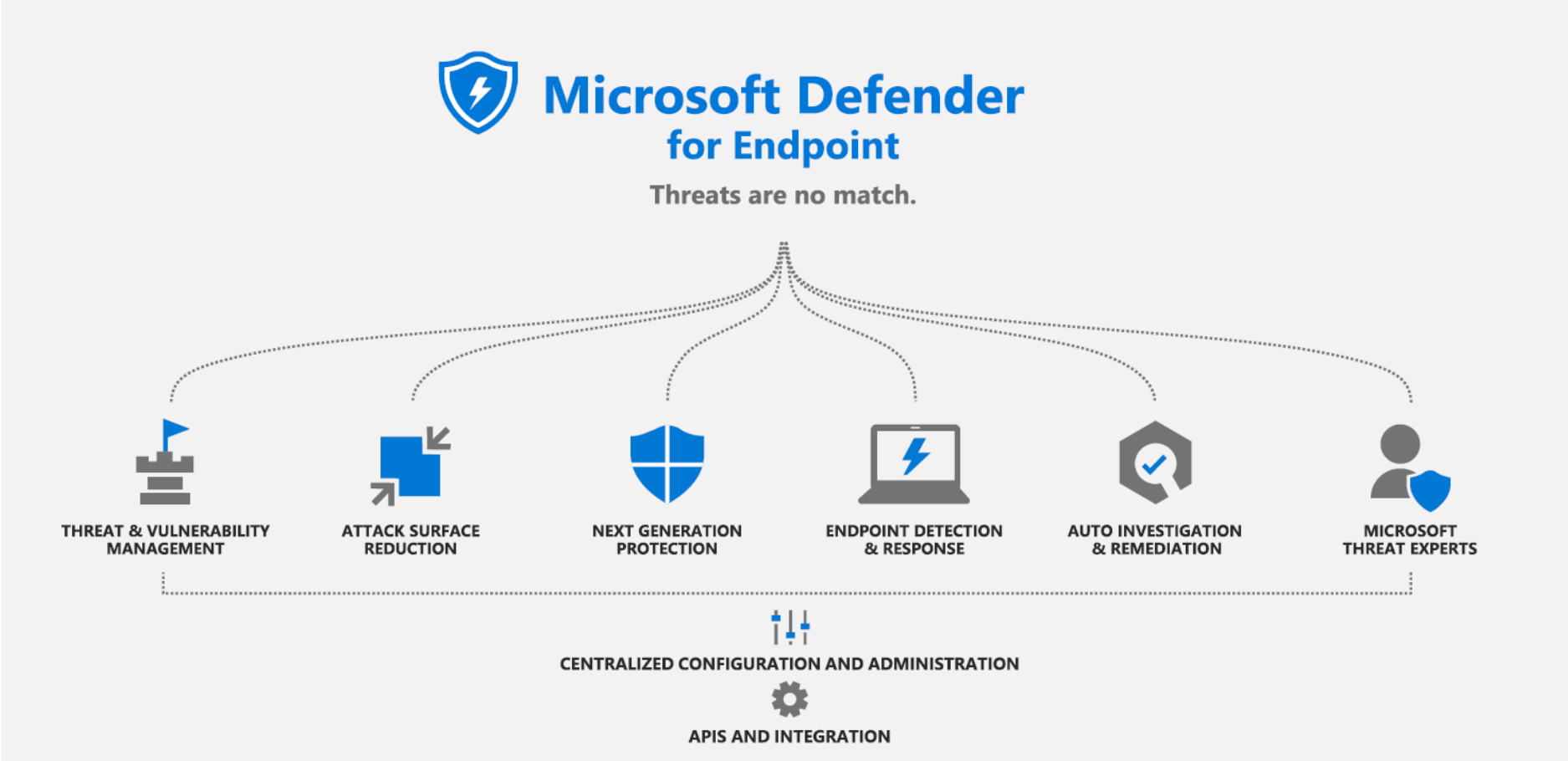
RESOLVE

03. Proteggiamo gli endpoint

Microsoft Defender for Endpoint

Endpoints

Microsoft 365
Business Premium



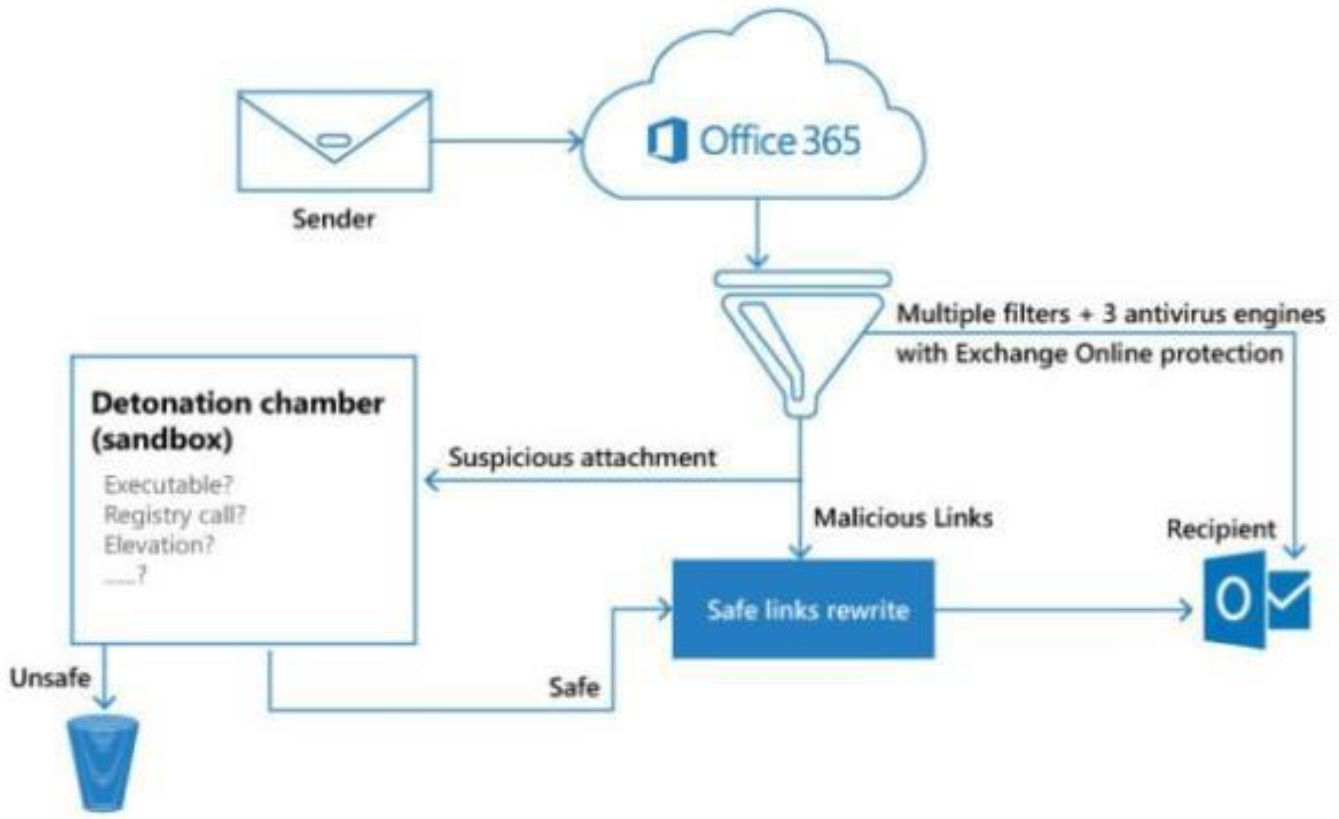
RESOLVE

03. Proteggiamo gli endpoint

Microsoft Defender for Office 365 – Safe attachment

Endpoints

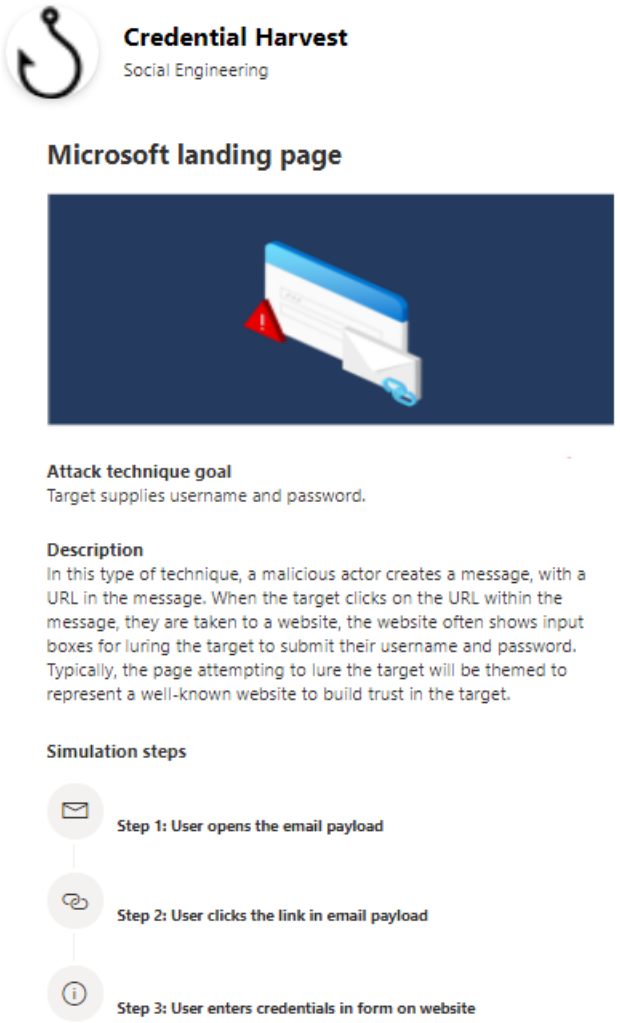
Microsoft 365
Business Premium



RESOLVE

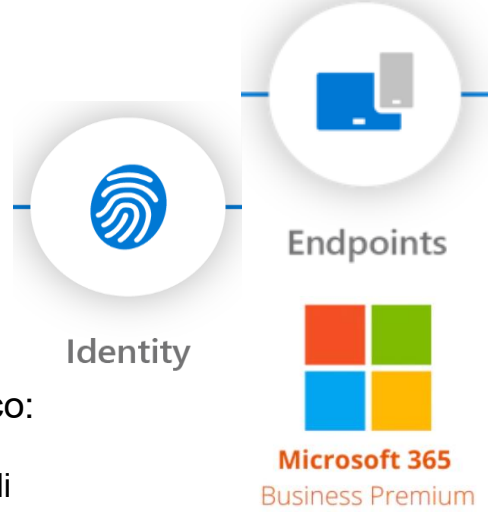
04. Modifichiamo i comportamenti

Microsoft Defender for Office 365 P2 – Simulazione attacchi



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

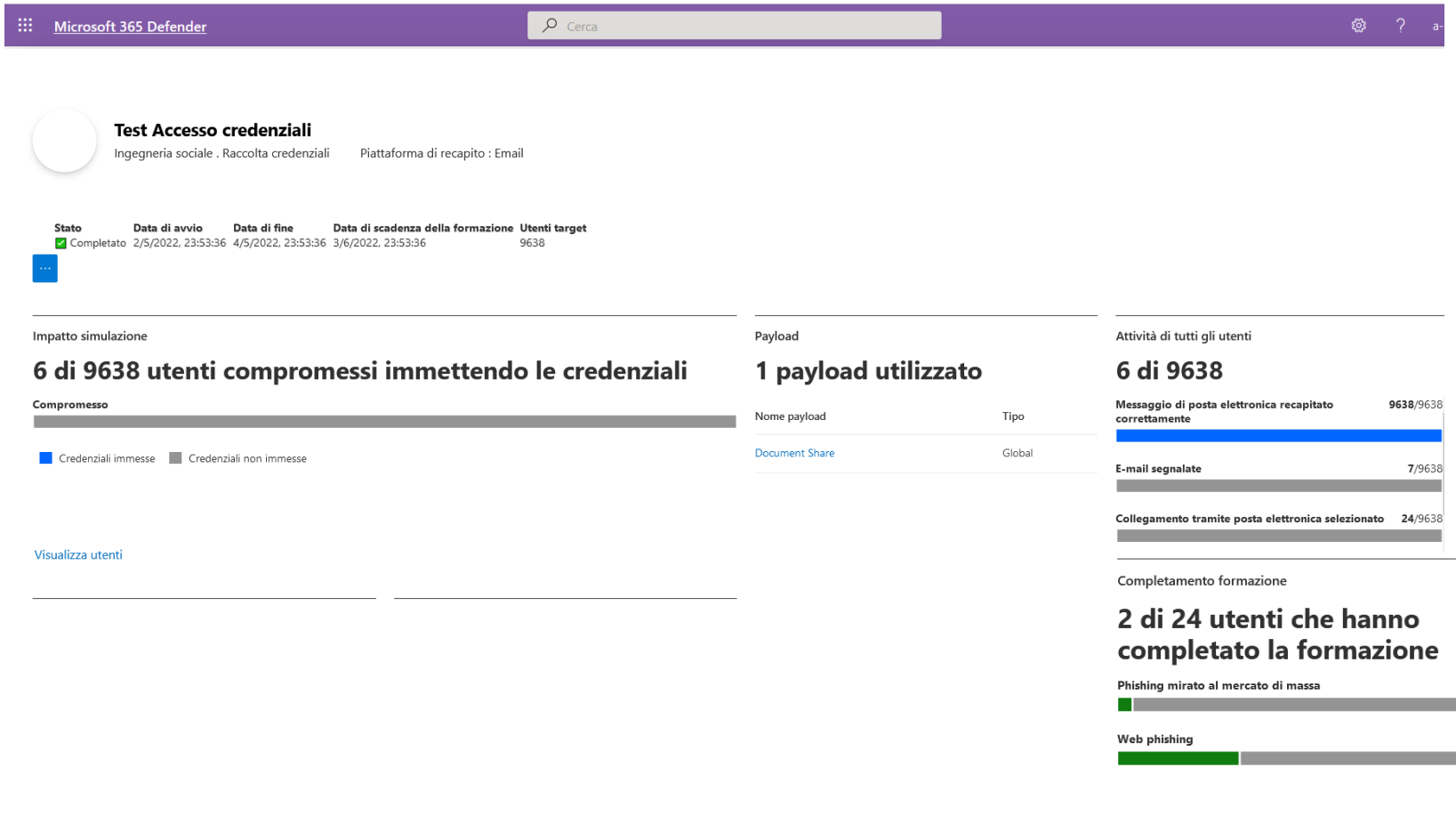
- **Raccolta delle credenziali**: tenta di raccogliere le credenziali portando gli utenti a un sito Web dall'aspetto noto con caselle di input per inviare un nome utente e una password.
- **Allegato malware**: aggiunge un allegato dannoso a un messaggio. Quando l'utente apre l'allegato, viene eseguito 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.

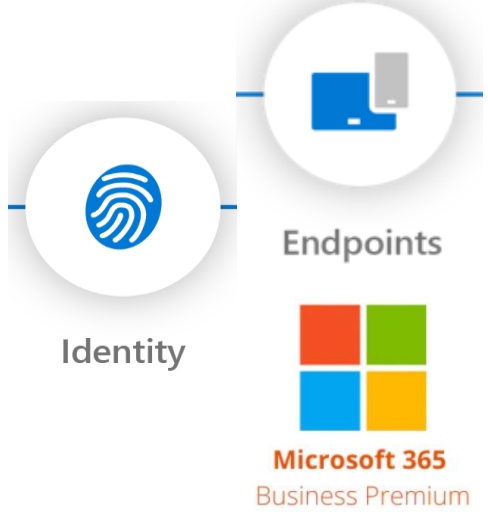


RESOLVE

04. Modifichiamo i comportamenti

Microsoft Defender for Office 365 P2 – Simulazione attacchi





RESOLVE

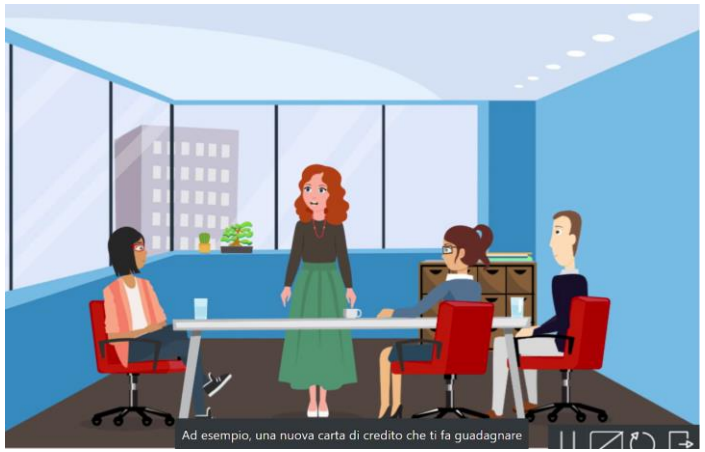
04. Modifichiamo i comportamenti

Microsoft Defender for Office 365 P2 – Simulazione attacchi

Endpoints

Identity

Microsoft 365
Business Premium



RESOLVE

05. Proteggiamo i dati

Introduzione ad Azure Information Protection

Microsoft 365
Business Premium

RESOL/E

05. Proteggiamo i dati

Introduzione ad Azure Information Protection

Microsoft 365
Business Premium

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

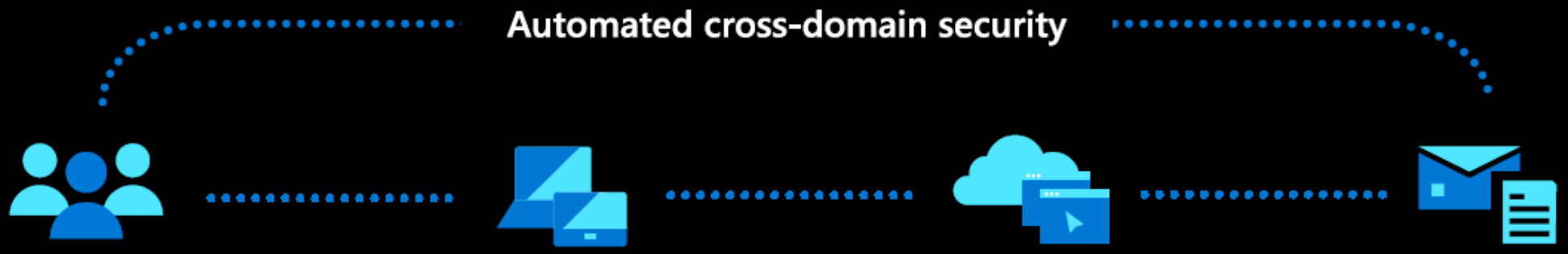
Apply flexible protection actions, such as encryption, access restrictions and visual markings.

Monitor and remediate

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

RESOLVE

Microsoft 365 Defender



Identities

Microsoft Defender for Identity

Formerly Azure Advanced Threat Protection

Endpoints

Microsoft Defender for Endpoint

Formerly Microsoft Defender Advanced Threat Protection

Cloud Apps

Microsoft Defender for Cloud Apps

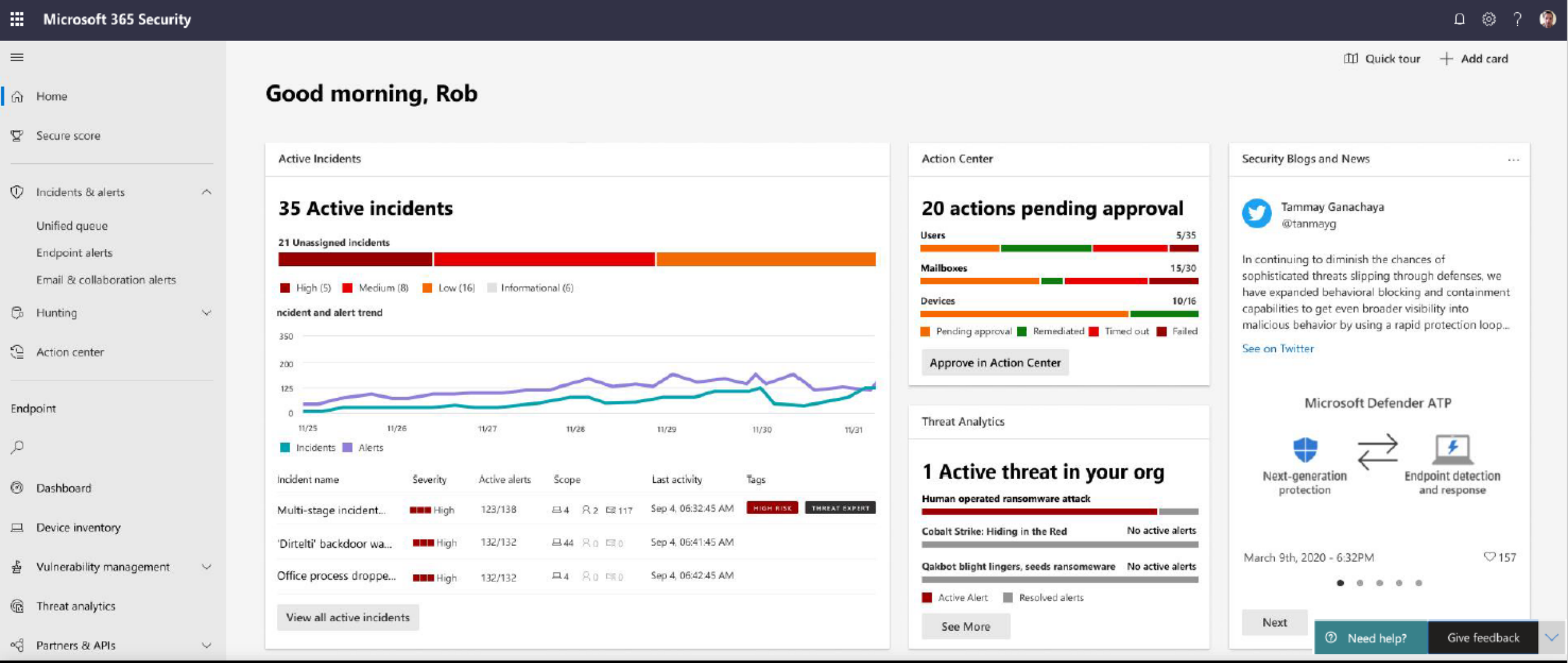
Formerly Microsoft Cloud App Security

User Data

Microsoft Defender for Office 365

Formerly Office 365 Advanced Threat Protection

RESOLVE



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

/2

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

/3

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

/4

Dimissione dell'ambiente on-prem

CYBERSECURITY MULTILIVELLO CON MS365

/ DOMANDE

Chiedete in chat le vostre curiosità

RESOL/E

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

RESOLVE

by ErgonGroup