

RESOL/E

by ErgonGroup

PRIMA DI INIZIARE



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

 Microsoft
Solutions Partner
Business Applications

 Microsoft
Solutions Partner
Data & AI
Azure

 Microsoft
Solutions Partner
Infrastructure
Azure

 Microsoft
Solutions Partner
Digital & App Innovation
Azure

 Microsoft
Solutions Partner
Modern Work

RESOL/E

/ RESOLVE

Siamo parte di ErgonGroup:

Nata nel 2006 come “**società del sapere**”, con gli anni e l’esperienza **ErgonGroup** ha sviluppato un know-how sempre più esteso in risposta alle esigenze di **persone, aziende, enti e istituzioni** che necessitano di crescere colmando gap, acquisendo tecnologie, sviluppando eccellenze individuali, di team e di organizzazione.

Oggi ci presentiamo come una **Holding che conta 3 brand**: Resolve SB Srl, Upskill by ErgonGroup Srl, JObros Srl.

Upskill, Società **specializzata nella formazione e nei servizi formativi**. Grazie alla storia, all’esperienza e alla forza di ErgonGroup, da oltre 15 anni Upskill accompagna aziende, persone e istituzioni nello sviluppo di percorsi di alta **formazione manageriale**, fianco a fianco in tutte le fasi del processo formativo.

JObros, **Agenzia per il lavoro non convenzionale**. JObros accompagna persone e imprese nella loro crescita: affianca gli **HR** nella selezione, inserimento e creazione di talenti in azienda e supporta le **persone** nell’orientamento, nella ricerca del lavoro e nei percorsi di carriera.

Resolve nasce per colmare il gap tra il “dire” e il “fare”, affiancando imprenditori e manager, del settore pubblico e privato, nel delineare strategie e calarle in azienda e nel territorio, in modo semplice, tecnologico e sostenibile.

Dal 2023 è **Società Benefit**, a conferma dell’impegno sostanziale verso il mercato, le persone e i territori in cui opera.

RESOL/E

Consulenza strategica,
digitalizzazione e sostenibilità

UPSKILL

Formazione per le imprese
e le persone

JObros

Agenzia per il lavoro
non convenzionale

ergonGROUP
Più competenti. Più intelligenti. Più veloci.

Microsoft
Solutions Partner
Business Applications

Microsoft
Solutions Partner
Data & AI
Azure

Microsoft
Solutions Partner
Infrastructure
Azure

Microsoft
Solutions Partner
Digital & App Innovation
Azure

Microsoft
Solutions Partner
Modern Work

RESOL/E



/ CHI SIAMO

SPEAKER

VINCENZO PAGANO

System Architect di @RESOLVE

System Architect di Resolve, Vincenzo si occupa di gestire progetti e infrastrutture IT principalmente su tecnologie Microsoft. Grande appassionato di Cloud Computing e di trasformazione digitale, affianca le aziende nel **sfruttare al meglio il potenziale del cloud per migliorare l'efficienza, la sicurezza, la scalabilità e l'innovazione.**

 **Microsoft**
Solutions Partner
Business Applications

 **Microsoft**
Solutions Partner
Data & AI
Azure

 **Microsoft**
Solutions Partner
Infrastructure
Azure

 **Microsoft**
Solutions Partner
Digital & App Innovation
Azure

 **Microsoft**
Solutions Partner
Modern Work

RESOL/E

/ AGENDA

1

MICROSOFT DEFENDER FOR SERVER

- *Protezione Multi-Cloud e On-Premises*
- *Gestione e Reporting Centralizzati*
- *Miglioramento della Postura di Sicurezza*
- *Rilevamento Intelligente delle Minacce*

2

MICROSOFT DEFENDER FOR IDENTITY

- *Integrazione con Microsoft Defender XDR*
- *Prevenzione delle Violazioni*
- *Integrazione con Servizi di Gestione delle Identità*
- *Valutazione della Postura di Sicurezza*

3

Q&A LIVE

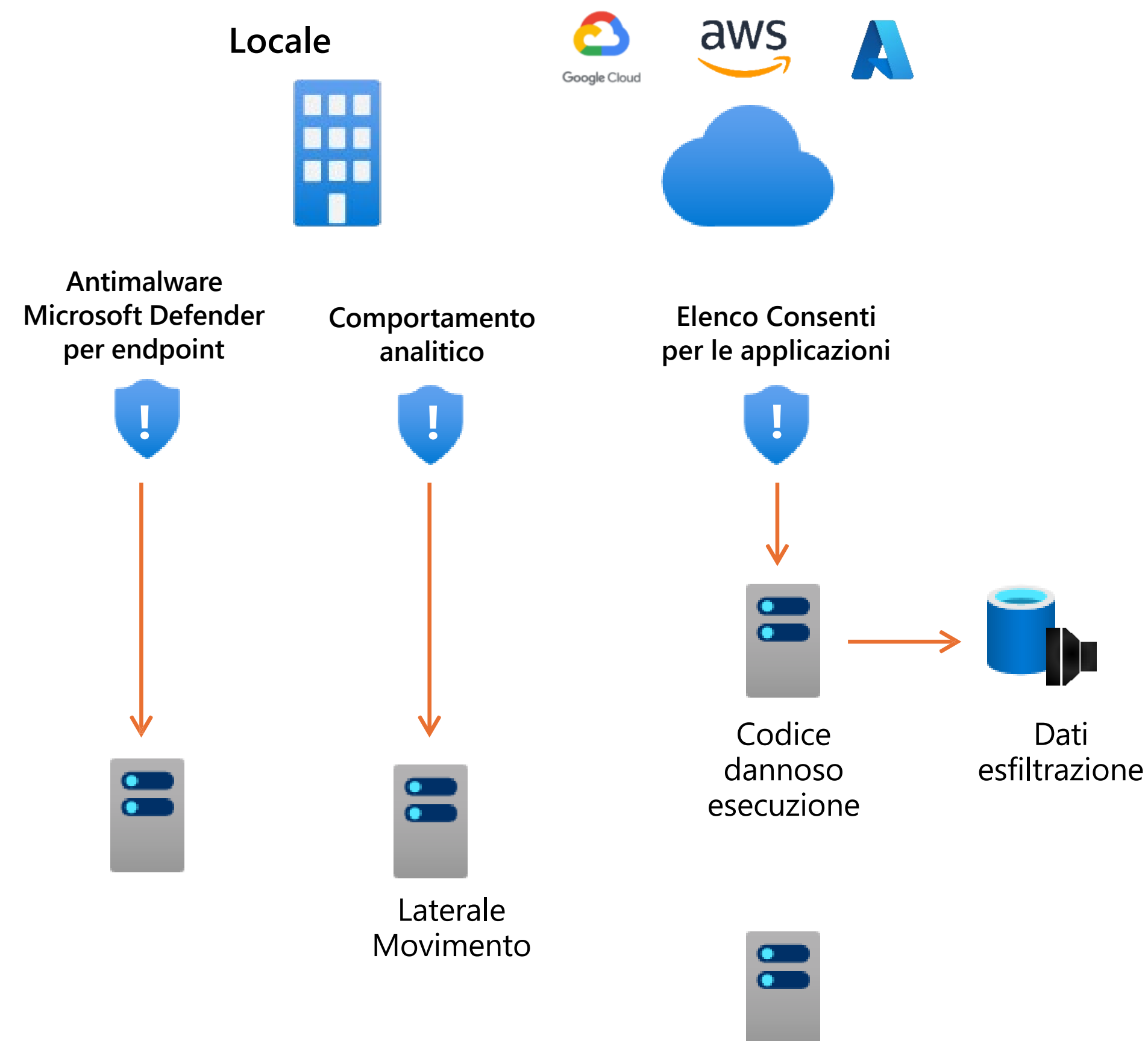
01. MICROSOFT DEFENDER FOR SERVER

PROTEZIONE MULTI-CLOUD E ON-PREMISES

/ Proteggi i tuoi server dalle minacce

Microsoft Defender per server

- Visualizzazione della sicurezza centrale delle macchine virtuali
- Esperienza di onboarding semplice con provisioning automatico senza attriti
- Rilevamento di macchine non monitorate



/Proteggi le macchine in ambienti ibridi e multi-cloud

Microsoft Defender per server



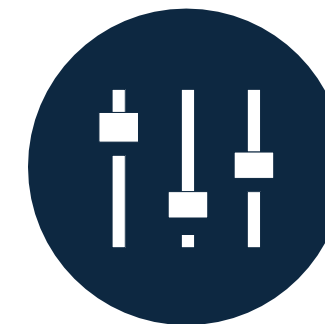
Supporto multicloud

- Supporta tutti i server windows e Linux
- Copertura per gestione servizi incluso Amazon EC2 e Google Compute Engine



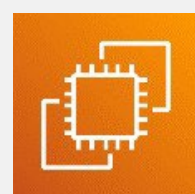
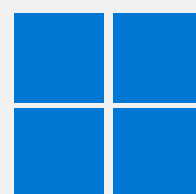
Soluzione EDR leader del settore

- Integrato con Defender for Endpoint
- Protezione antivirus di nuova generazione
- Endpoint detection e risposta
- Valutazione delle vulnerabilità



Ottimizzato per gli ambienti cloud

- Controllo adattivo delle applicazione
- Accesso JIT alle VM
- Monitoraggio integrità file
- Hardening di rete adattivi

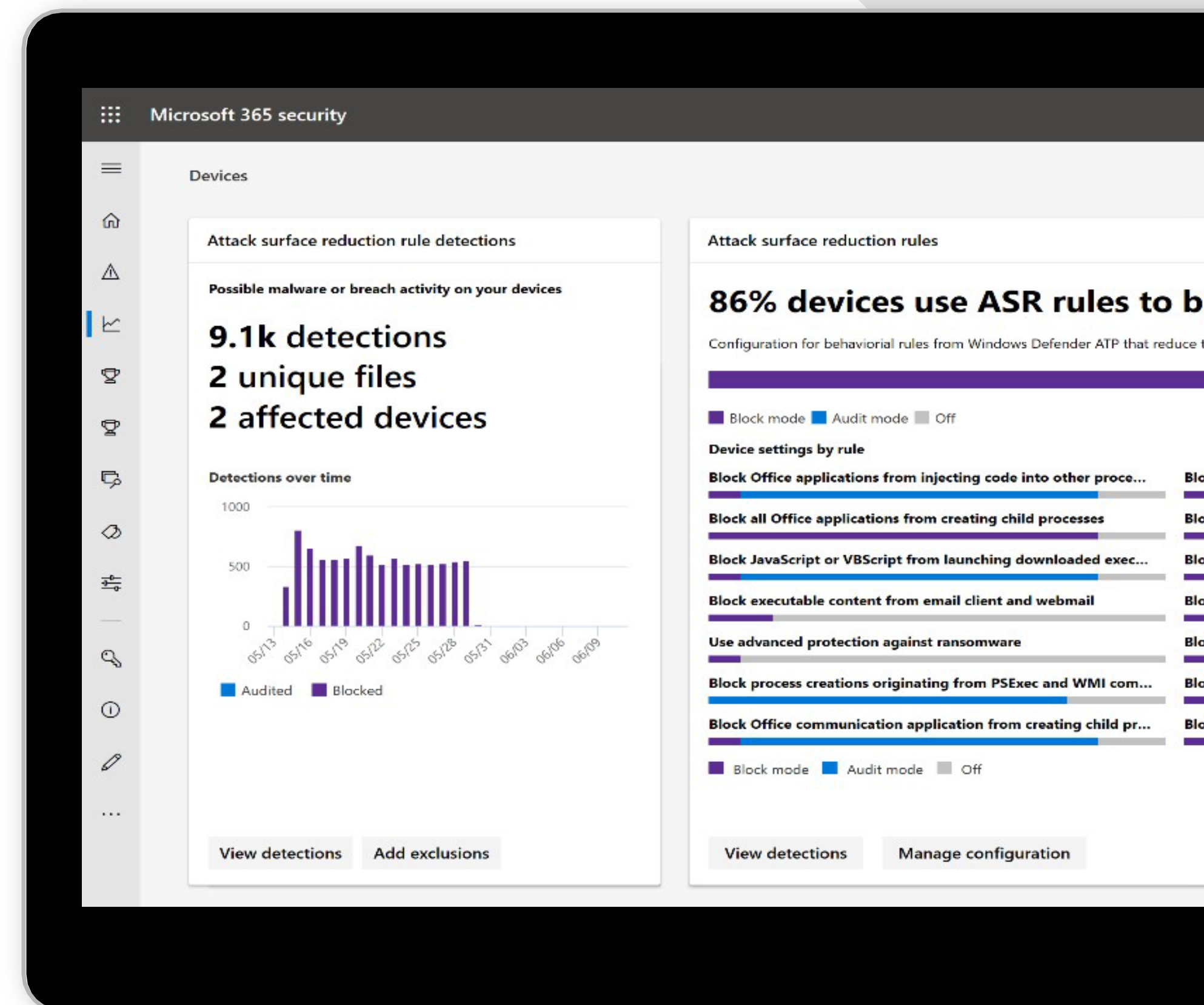


/ Riduzione della superficie di attacco

Basato su Microsoft Defender per endpoint

Eliminare il rischio di attacco
riducendo la superficie

- Hardening del sistema senza interruzioni
- Personalizzazione che si adatta all'organizzazione
- Visualizzazione degli impatti e semplice attivazione di comandi

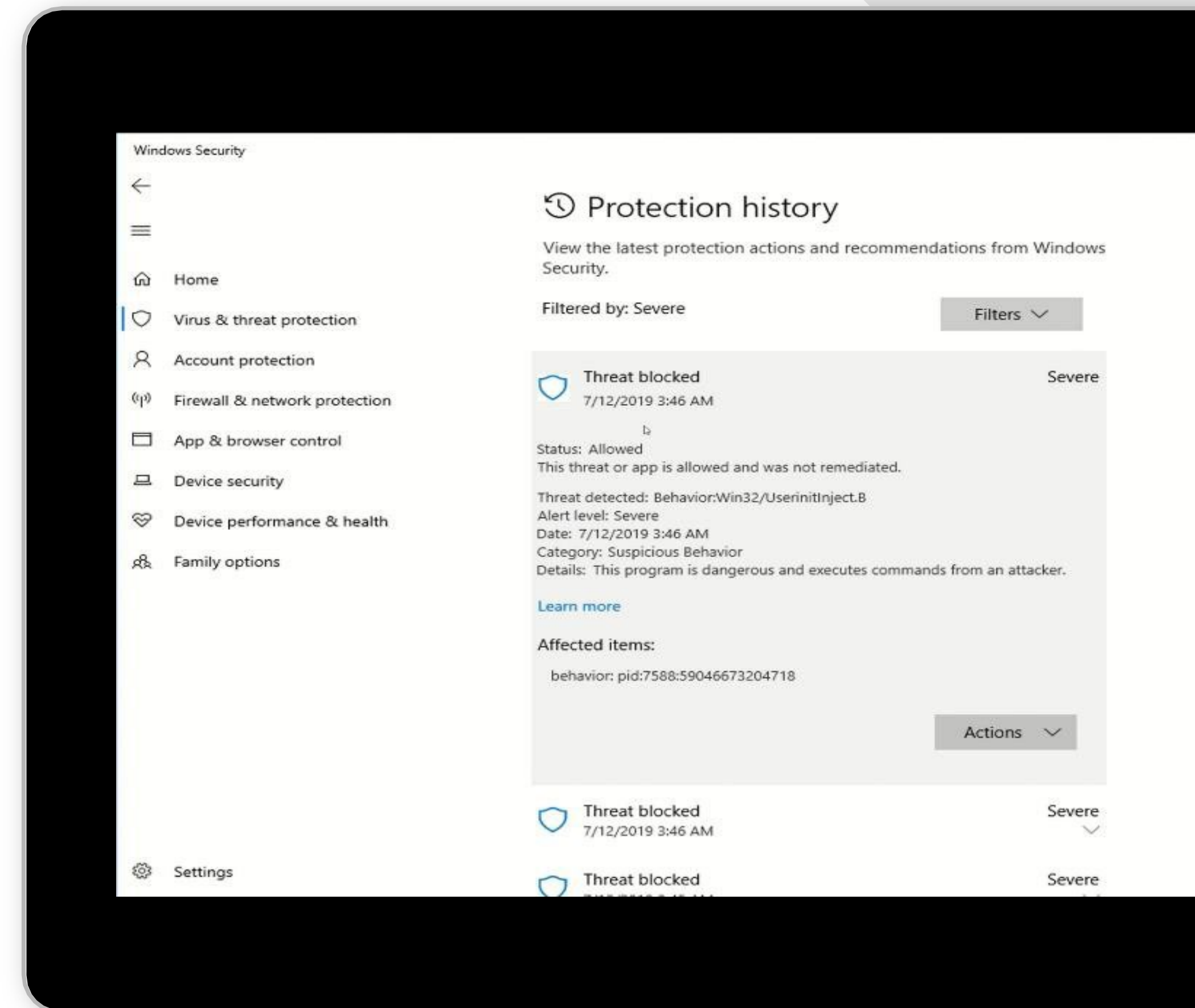


/ Protezione antivirus di nuova generazione

Basato su Microsoft Defender per endpoint

Blocca e affronta thread sofisticati e malware

- Protezione in tempo reale basata sul comportamento
- Blocco dei file con codice malevole
- Blocca le attività dannose da applicazioni affidabili e non affidabili



/ Protezione antivirus di nuova generazione

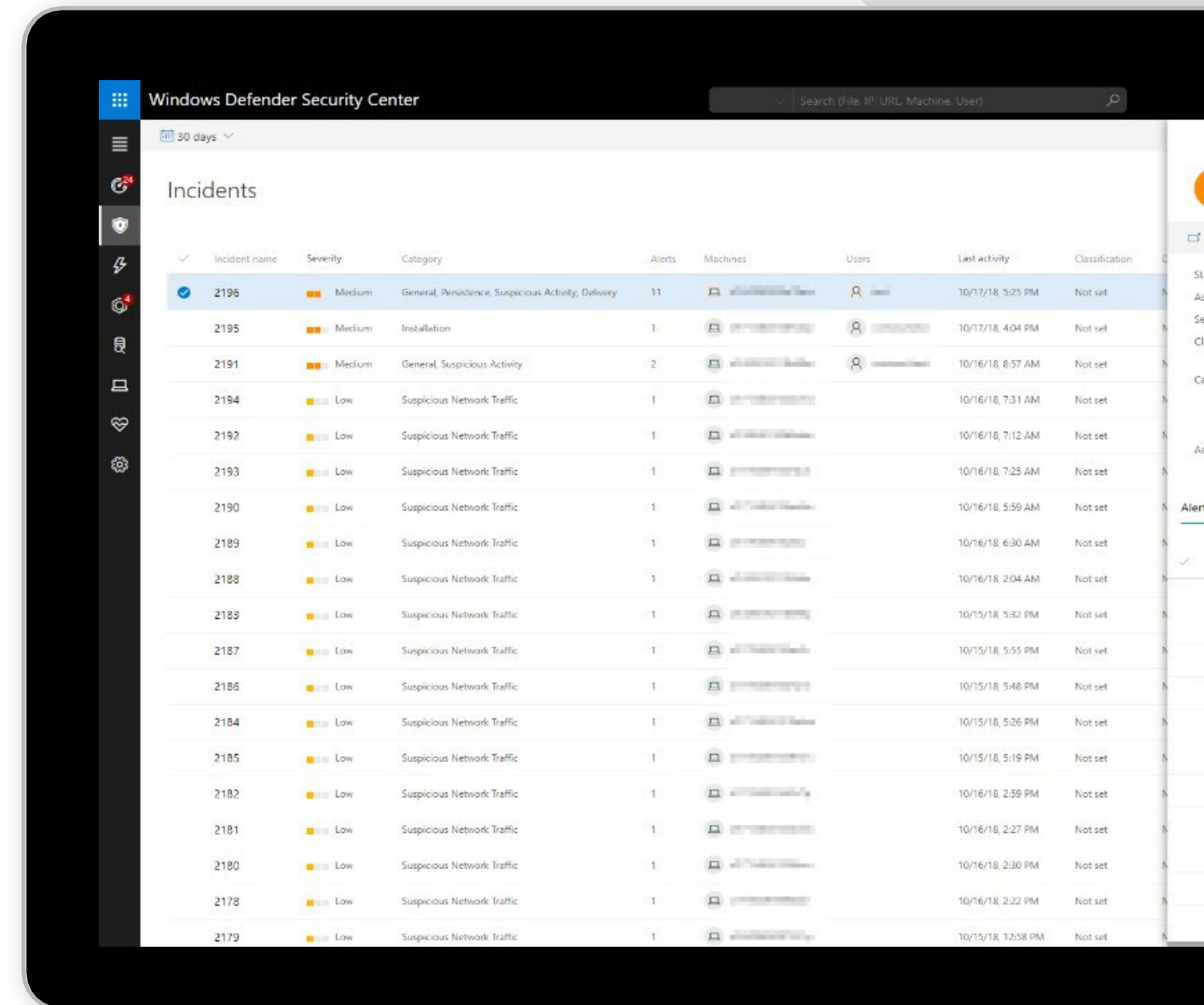
Basato su Microsoft Defender per endpoint

Rileva e indaga sugli attacchi persistenti avanzati

- Avviso comportamentale correlato
- Indagine e ricerca su sei dati di mese
- Ricco set di strumenti per rispondere alle azioni



Demonstrated industry leading optics and detection capabilities in MITRE ATT&CK® based evaluation.



Microsoft
Solutions Partner
Business Applications

Microsoft
Solutions Partner
Data & AI
Azure

Microsoft
Solutions Partner
Infrastructure
Azure

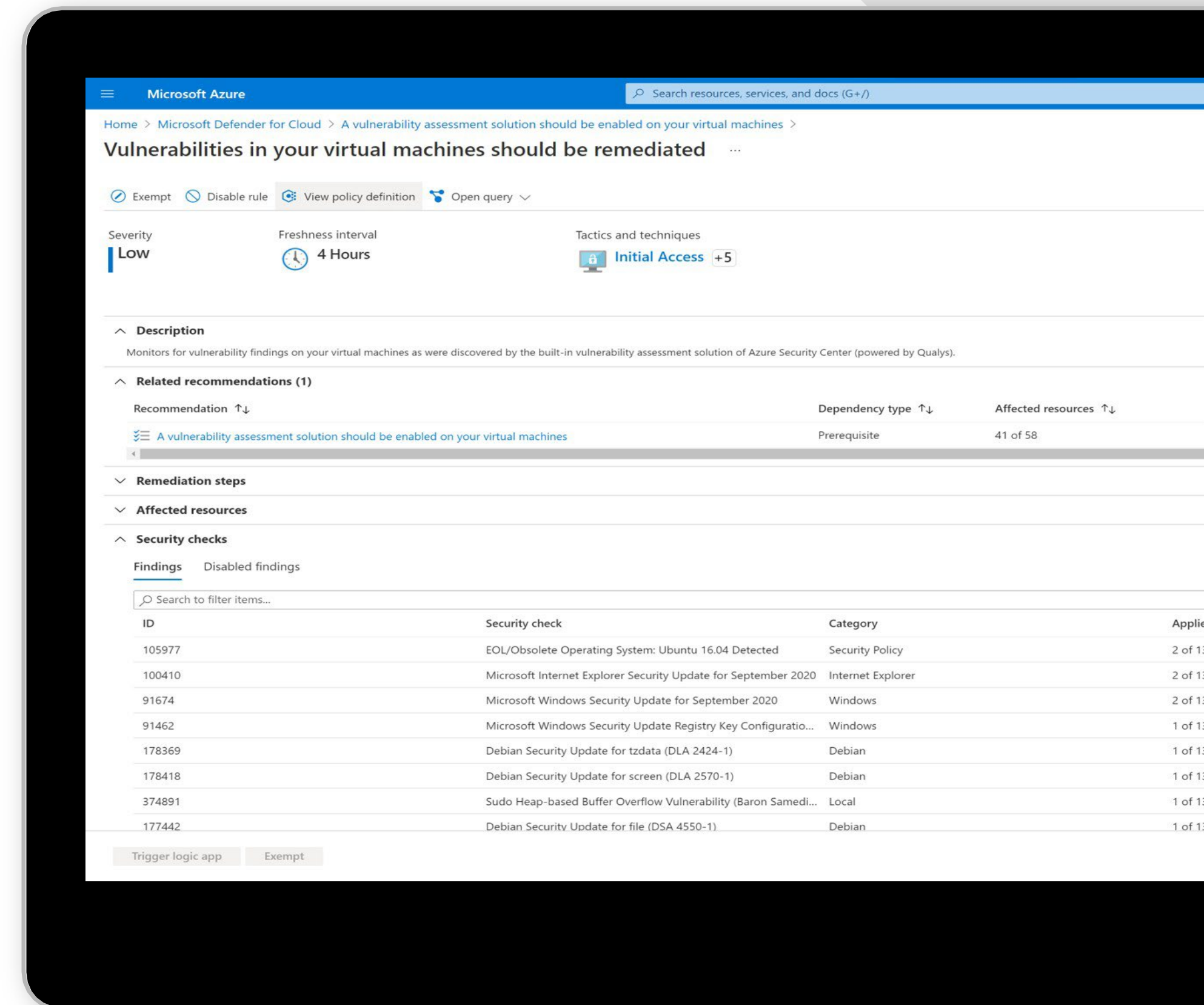
Microsoft
Solutions Partner
Digital & App Innovation
Azure

Microsoft
Solutions Partner
Modern Work

RESOL/E

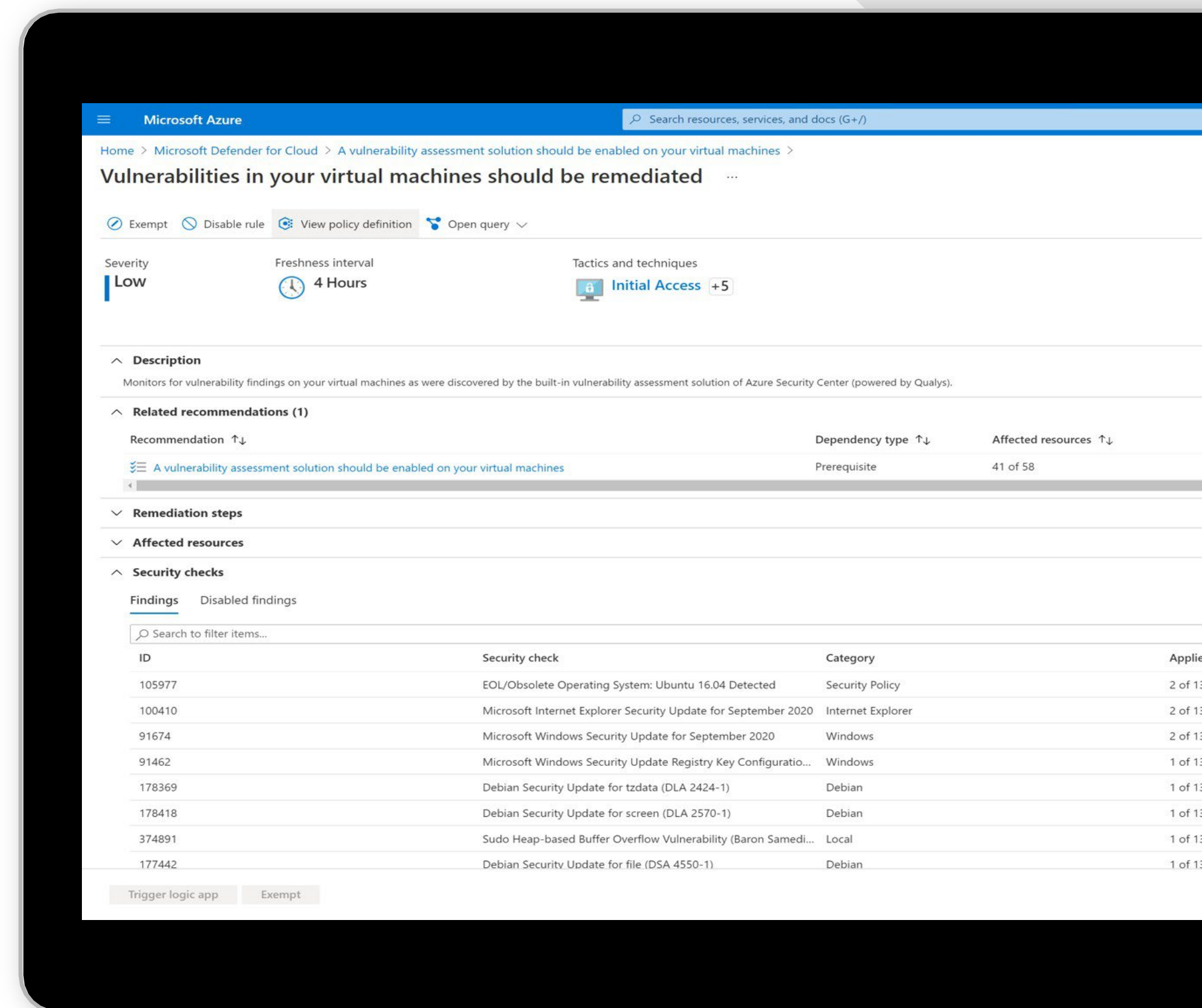
/ Valuta le tue macchine virtuali e i tuoi contenitori per individuare le vulnerabilità

- Distribuzione automatizzata dello scanner di vulnerabilità
- Scansione continua sulle applicazioni installate e ricerca delle vulnerabilità per sistemi Linux e Windows
- Visibilità delle vulnerabilità trovate nel Security Center Portal e API
- Scegliere tra le funzionalità di gestione dei thread e delle vulnerabilità di Qualys e Microsoft



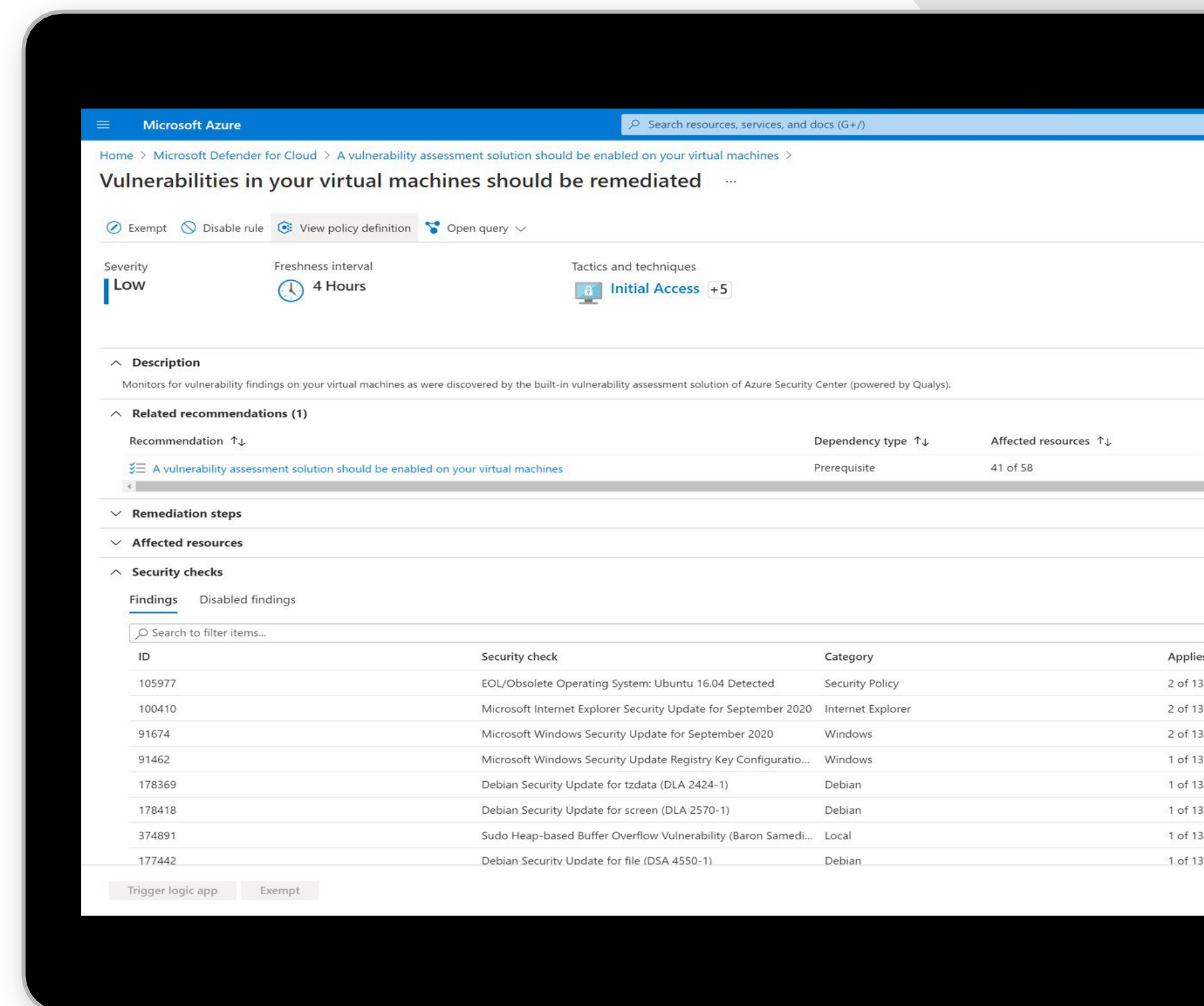
/ Accesso JIT alle VM

→ Bloccare il traffico in ingresso verso le macchine virtuali, riducendo l'esposizione agli attacchi e fornendo al contempo un facile accesso per connettersi alle macchine virtuali quando necessario

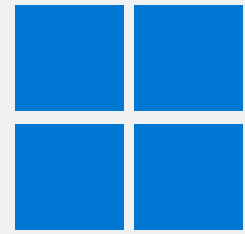


/ Monitoraggio dell'integrità dei file

- Esamina il file del sistema operativo, i registri di Windows, il software applicativo, il file di sistema Linux e altro ancora, alla ricerca di modifiche che potrebbero indicare un attacco
- Selezionare i file che si desidera monitorare utilizzando i suggerimenti o la tua logica



/ Sistemi operativi supportati



Windows Server 2012 R2

Windows Server 2016

Windows Server, versione 1803 o
successiva Windows Server 2016

Windows Server 2022



Red Hat Enterprise Linux 7.2+

Red Hat Enterprise Linux 8.x

CentOS 7.2+, 8

Ubuntu 16.04, 18.04, 20.04

SUSE Linux Enterprise Server 12, 15

Oracle Linux 7.2 o

versioni successive Oracle

Linux 8.x

Amazon Linux 2

/ Abilitazione

- Abilitare Defender per i server P1 o P2 nel portale di Azure (un clic)
- Installare l'agente Azure Arc in server cloud locali e non Azure
- MDE verrà fornito automaticamente, tramite il MDE, Windows C MDE, Estensioni Linux
- I server on-premise sono ora integrati in Defender for Cloud e Defender for Endpoint



1. Il server esegue l'onboarding in Azure Arc (il server è quindi individuabile da Defender per i server)
2. Defender per server effettua quindi automaticamente il provisioning di MDE in questo server come estensione
3. Le funzionalità di Defender per endpoint sono ora disponibili nel server

Confronto delle funzionalità

Caratteristica	Defender per server P1 (\$5)*	Defender per server P2 (\$ 15)*
Integrazione di Defender per endpoint	✓	✓
Licenze	✓	✓
Provisioning di Defender per endpoint	✓	✓
Visualizzazione unificata	✓	✓
Rilevamento delle minacce a livello di sistema operativo (basato su agente)	✓	✓
Rilevamento delle minacce a livello di rete (senza agente)		✓
Componente aggiuntivo per la gestione delle vulnerabilità di Microsoft Defender		✓
Politica di sicurezza e conformità normativa		✓
Inserimento dati gratuito (500 MB) nelle aree di lavoro		✓
Accesso just-in-time alle macchine virtuali		✓
Monitoraggio dell'integrità dei file		✓
Protezione avanzata dell'host Docker		✓
Aggiornamenti e patch di sistema		✓
Scansione senza agente		✓

/ Usare Azure Arc per connettere i carichi di lavoro ovunque a Microsoft Defender for Cloud

- Azure Arc sblocca scenari ibridi e multicloud in modo da poter gestire tutte le risorse in modo coerente
- Applica la conformità e semplifica la reportistica di audit
- Organizzazione e inventario delle risorse con una visualizzazione unificata nel portale di Azure Tags
- Proprietari di server con una visualizzazione e una correzione per soddisfare il controllo degli accessi in base al ruolo di compliance in Azure

Azure Arc abilita la gestione del cloud e le protezioni di sicurezza

Un unico piano di controllo per qualsiasi risorsa, ovunque

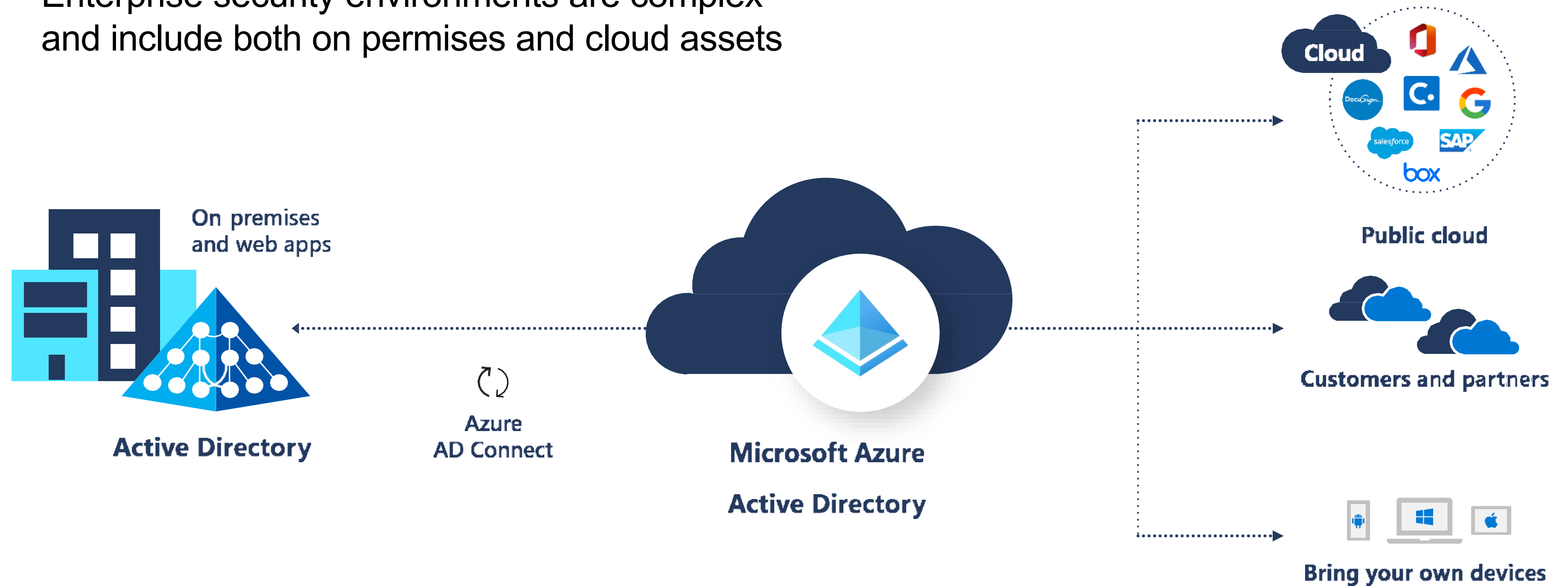


02. MICROSOFT DEFENDER FOR IDENTITY

INTEGRAZIONE CON MICROSOFT DEFENDER XDR

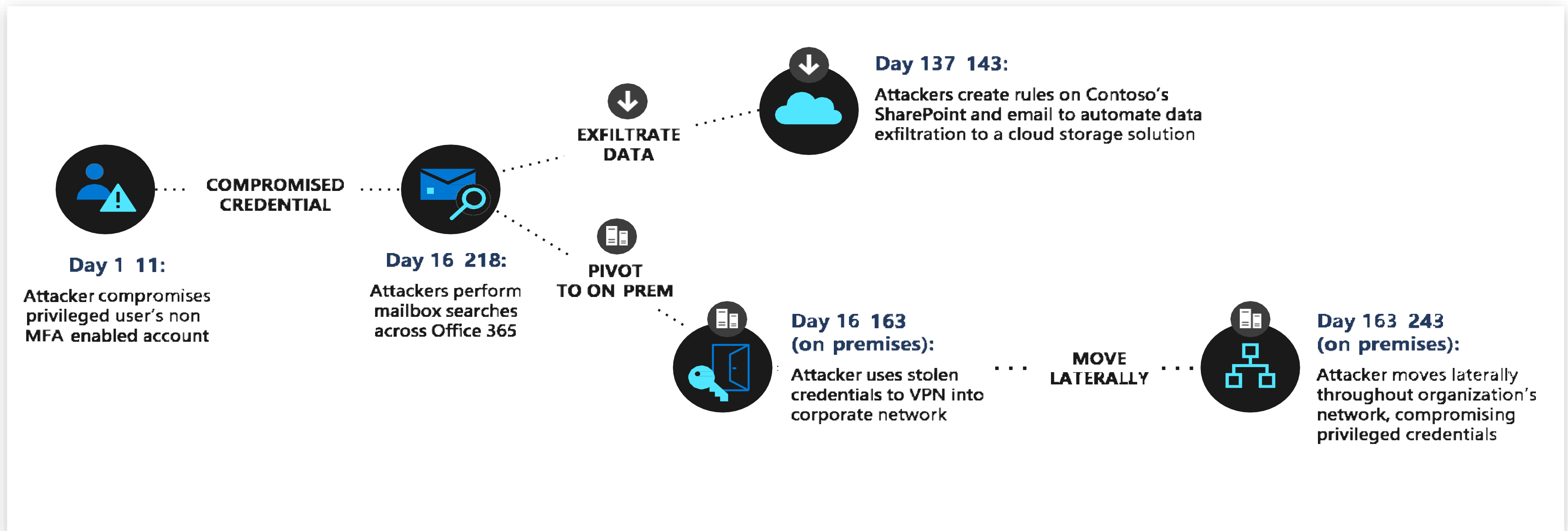
/ La complessità del panorama della sicurezza delle identità aziendali

Enterprise security environments are complex – and include both on premises and cloud assets



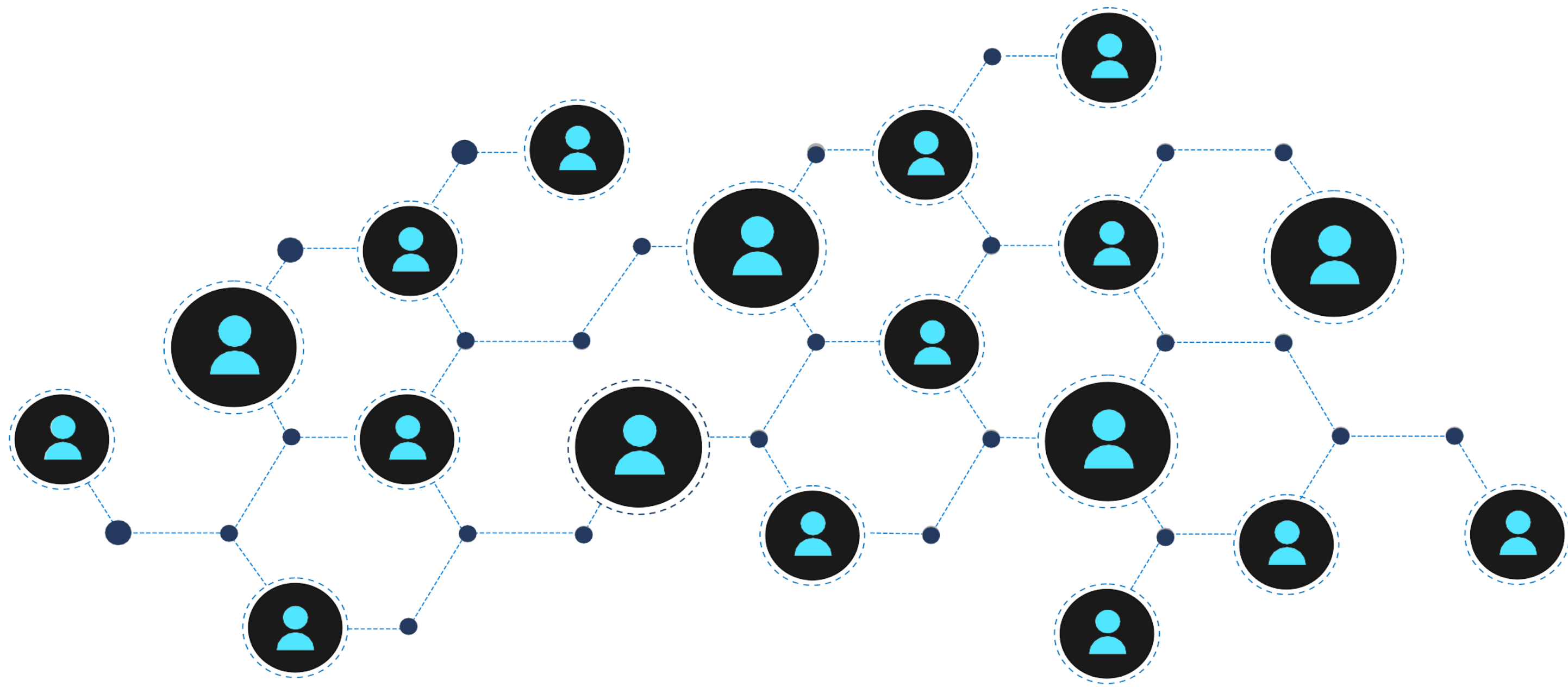
/ La complessità del panorama della sicurezza delle identità aziendali

One example of how happens and compromise an entire organisation

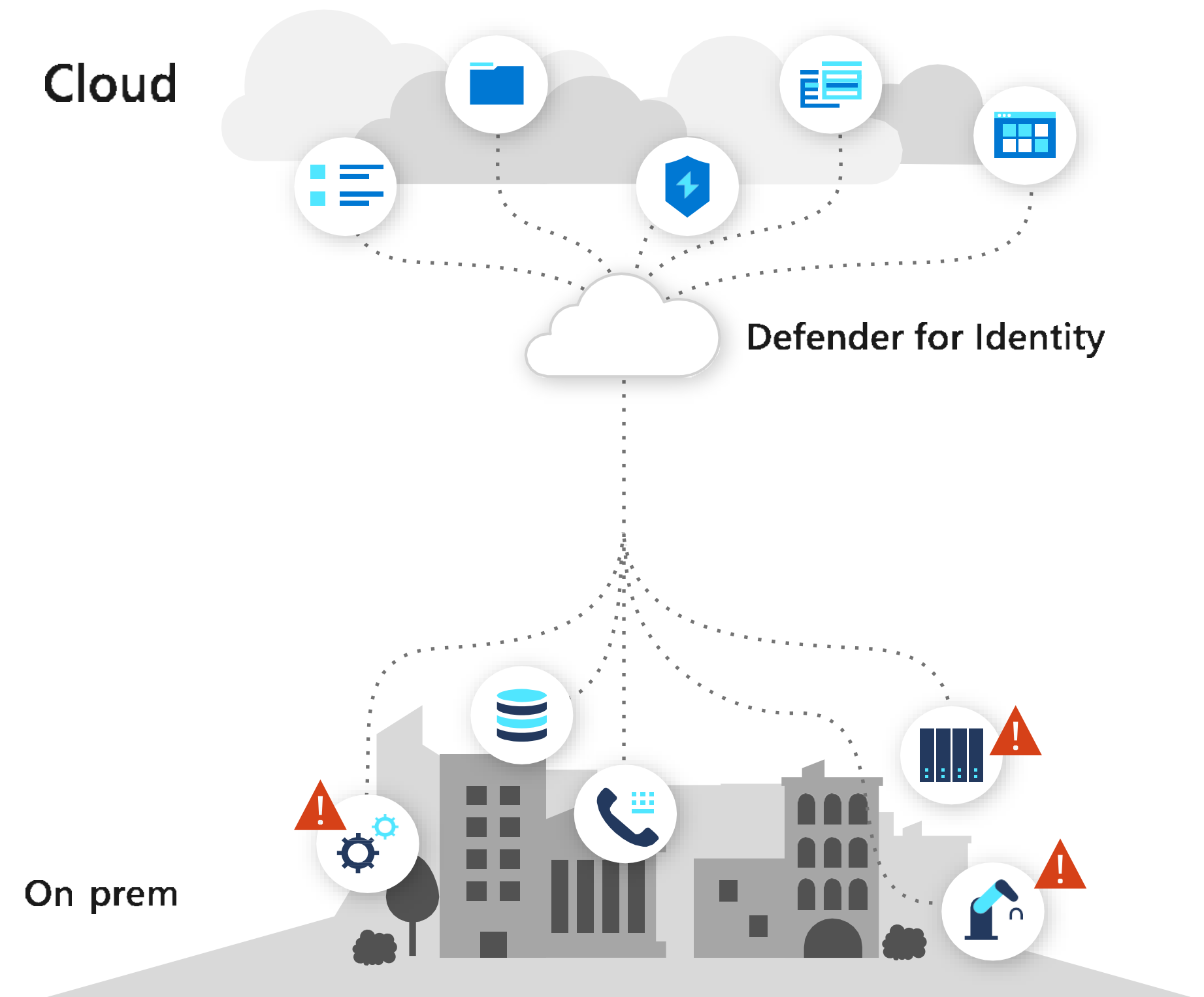


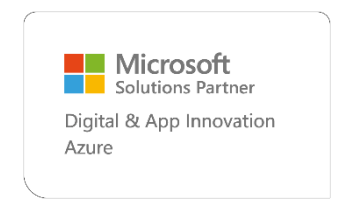
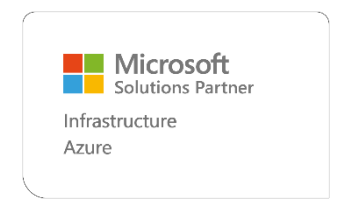
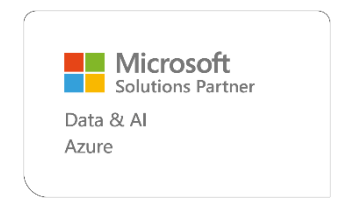
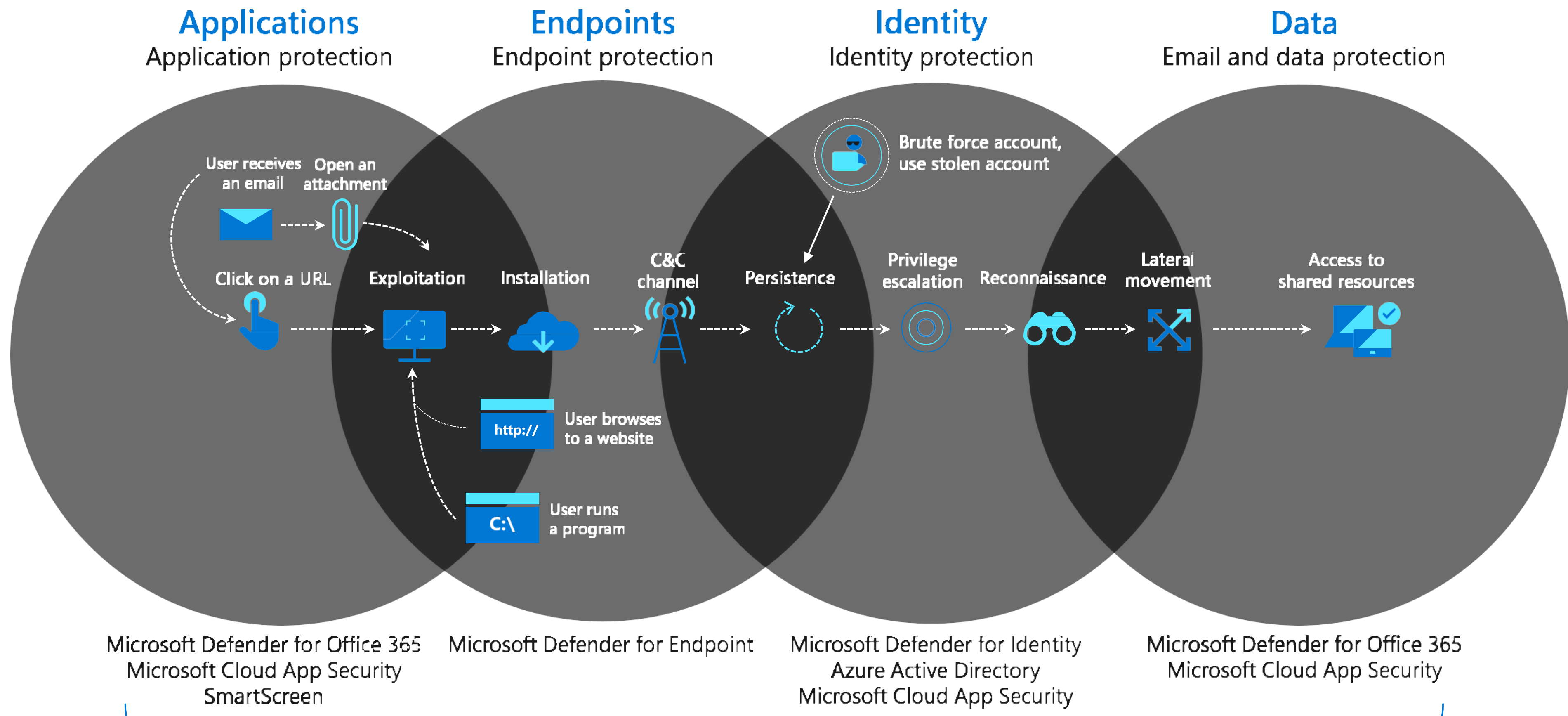
/ Un nuovo perimetro di sicurezza: l'identità dell'utente

Users are the new perimeter and a single compromised user can lead to a business shutdown



Microsoft Defender for Identity
monitora le risorse locali e si
integra con le soluzioni di
sicurezza cloud





RESOL/E

/ Microsoft Defender for Identity: una parte essenziale della protezione dell'intera azienda



Microsoft Defender for Identity

Prevent, detect, investigate, and respond to compromised users and lateral movements in **on premises environments.**



Microsoft Cloud App Security & Azure AD Identity Protection

Complete identity protection for **on premises and cloud environments.**

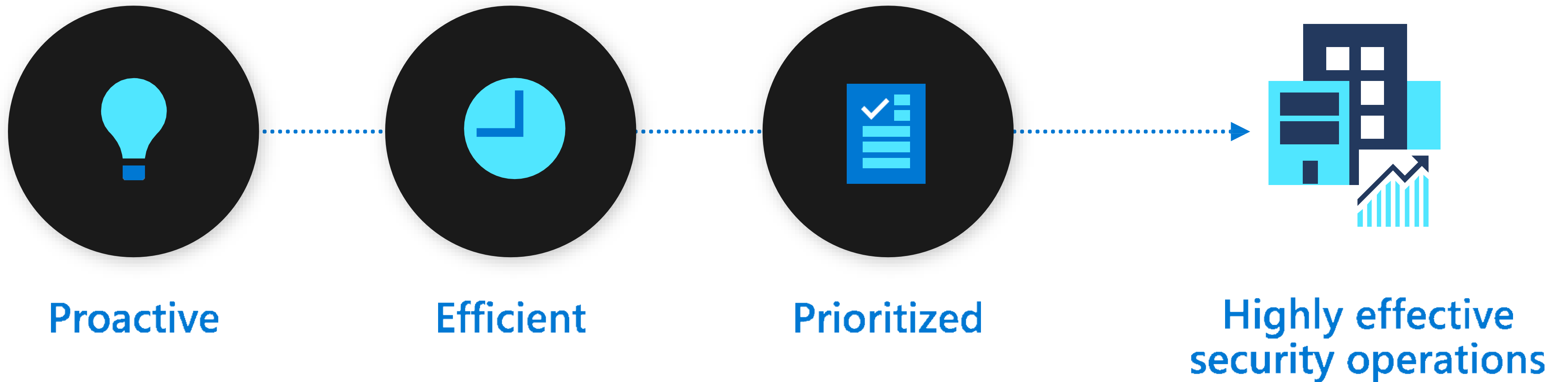


Microsoft 365 Defender

Security incidents, automated Investigation and response, and advanced hunting **across devices, identities, apps.**

/ Microsoft Defender for Identity: la chiave per potenziare la difesa

Supporting and enabling enterprise security operations



Microsoft
Solutions Partner
Business Applications

Microsoft
Solutions Partner
Data & AI
Azure

Microsoft
Solutions Partner
Infrastructure
Azure

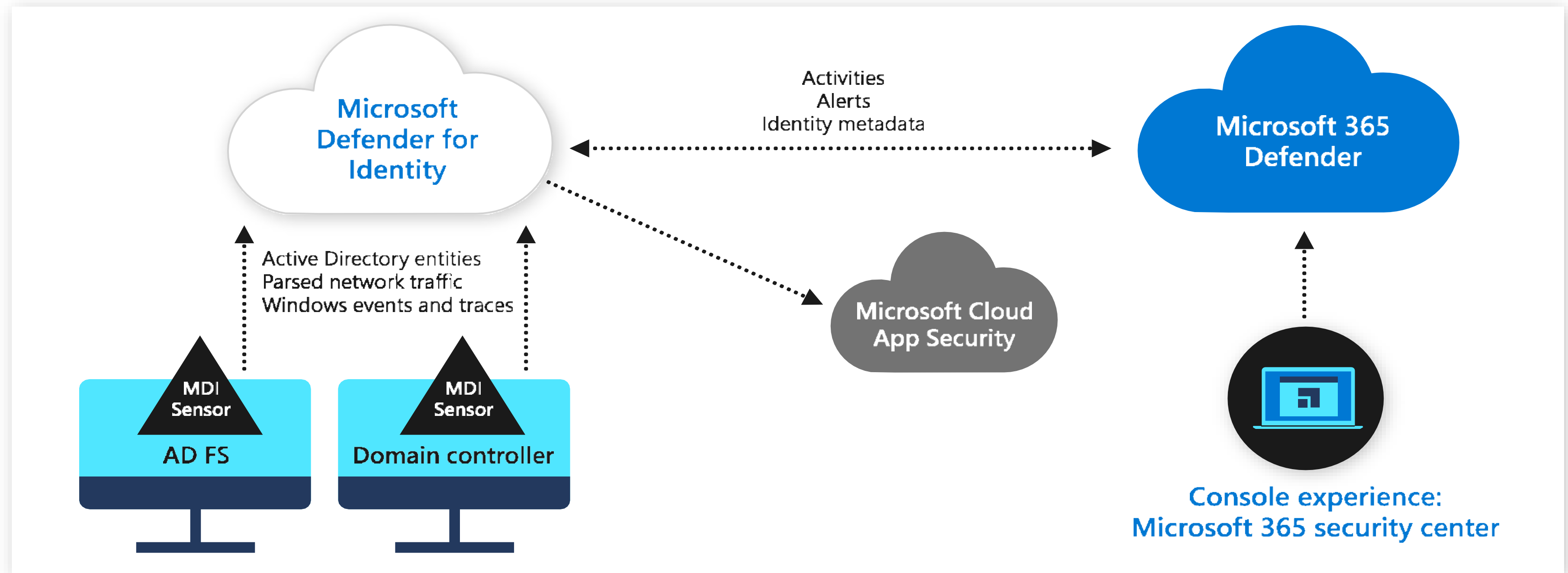
Microsoft
Solutions Partner
Digital & App Innovation
Azure

Microsoft
Solutions Partner
Modern Work

RESOL/E

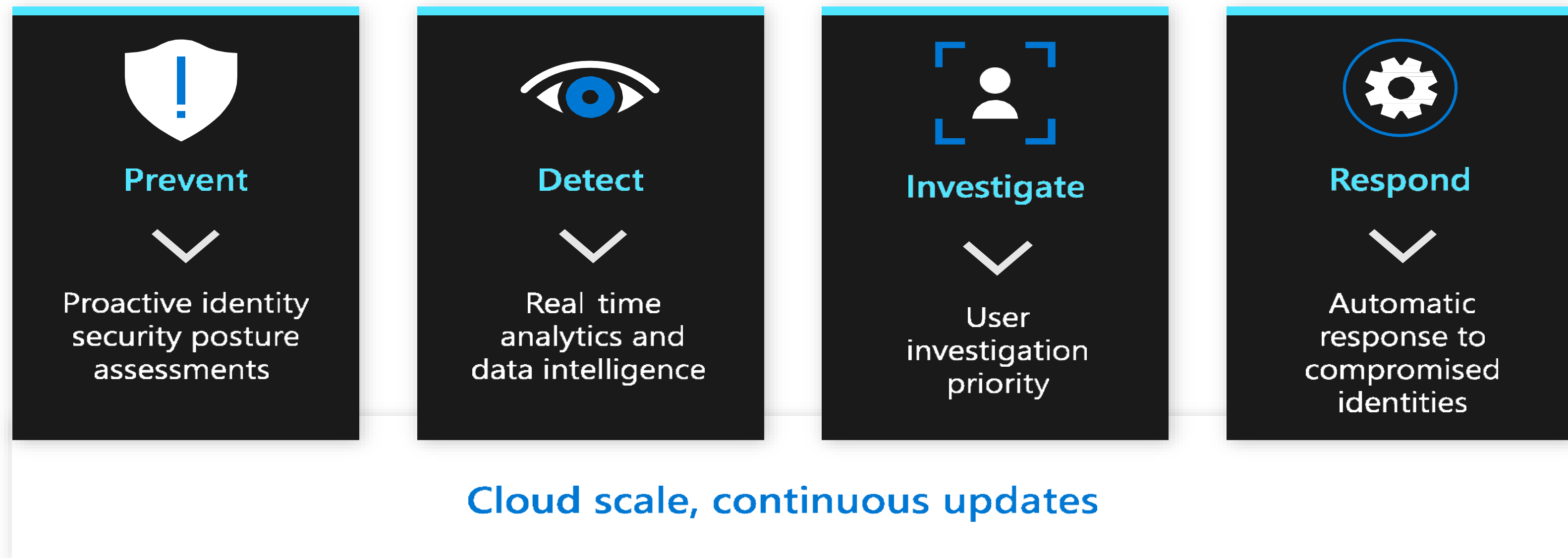
/ Architettura di Microsoft Defender per identità Microsoft Defender for Identity architecture

Defender for identity learns about your network, enables detection of anomalies, and warns you of suspicious activities



/ Architettura di Microsoft Defender per identità Microsoft Defender for Identity architecture

Defender for identity learns about your network, enables detection of anomalies, and warns you of suspicious activities



Prevent

Attack surface reduction



Prevent

Proactive identity security posture assessments help SecOps find and correct on permises identity vulnerabilities – because risky configurations mean lower security

```
+ Tcp: Flags=...AP..., SrcPort=3138, DstPort=LDAP(389),
- Ldap: Bind Request, MessageID: 3, Version: 3
  - Parser: Bind Request, MessageID: 3
    + ParserHeader:
    + MessageID: 3
    + OperationHeader: Bind Request, 0(0)
    - BindRequest: Version:3, Name:Wingtiptoys\Randy, i
      + Version: 3
      + Name: Wingtiptoys\Randy
      - authentication: Authentication type = simple
        + AuthenticationTypeHeader: Authentication typ
          SimpleAuthentication: Password1
```

Clear text authentication

Exposed passwords

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

☐ Do not trust this computer for delegation

☒ Trust this computer for delegation to any service (Kerberos only)

☐ Trust this computer for delegation to specified services only

☒ Use Kerberos only

☐ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name
--------------	------------------	------	--------------

Unconstrained delegation rights

Rogue impersonation

Network security: LAN Manager authentication level Properties ?

Local Security Setting Explain

Network security: LAN Manager authentication level

Send LM & NTLM responses

Send LM & NTLM - use NTLMv2 session security if negotiated

Send NTLM response only

Send NTLMv2 response only

Send NTLMv2 response only. Refuse LM

Send NTLMv2 response only. Refuse LM & NTLM

Legacy authentication in use

Easier to attack

/ Report di valutazione del comportamento di sicurezza delle identità

Gain visibility to potential identity risks to reduce the attack surface

- Entities exposing credentials in clear text
- Legacy protocols usage
- Weak cipher usage
- Unsecure Kerberos delegation
- Domain controllers with Print Spooler service available
- Dormant entities in sensitive groups
- Unmonitored domain controllers
- Microsoft LAPS usage
- Risky lateral movement paths
- Unsecure SID history attributes
- Unsecure account attributes

View top entities that are exposing credentials in clear text

Identity Security Posture > Entities exposing credentials in clear text

Improvement actions

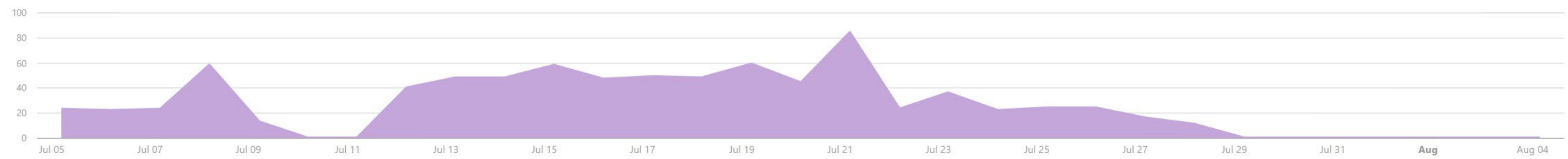
Stop clear text credentials exposure

Most critical: 2 entities

High

Send us feedback...

Exposed credentials activities



Report description

Top entities exposing credentials in clear text (using LDAP simple bind authentication) in your on-premises environment (last 30 days). [Learn why this is important to remediate and create an action plan](#)

1 - 16 of 16 top credential-exposing entities

Entity	Type	Activities	Recommended actions	Last seen
CLIENT1	Device	817	Stop CLIENT1 from using LDAP simple bind authentication	Jul 28, 2020, 11:07 AM
Vieno Mosley	Account	630	Stop Vieno Mosley from using LDAP simple bind authentication	Jul 28, 2020, 2:08 AM
Veria Cunningham	Account	17	Stop Veria Cunningham from using LDAP simple bind authentication	Jul 28, 2020, 11:07 AM
Giovannina Holbech	Account	17	Stop Giovannina Holbech from using LDAP simple bind authentication	Jul 28, 2020, 11:07 AM
Theophil Mcmillan	Account	17	Stop Theophil Mcmillan from using LDAP simple bind authentication	Jul 28, 2020, 11:07 AM

/ Percorsi di movimento laterale rischiosi

View top sensitive accounts that carry lateral movement risk

Identity Security Posture > Risky lateral movement paths

Improvement actions
Reduce lateral movement path risk to sensitive entities ■ ■ ■ High

Report description
Highlights sensitive users with the riskiest lateral movement paths and recommended actions to reduce risk. This report is updated every 24 hours. [Learn why this is important to remediate](#)

Sensitive user ⓘ	Domain
 Nick Carlsson	contoso.com

Recommended actions for Nick Carlsson

Perform the following actions to reduce the risk for this user. Some actions can reduce the risk for other sensitive users as well.

Filter...

- Remove local administrator permissions for Vivan Perez from [SharePoint-SRV](#)
Reduces 1 non-sensitive users potentially leading to this user
- Remove local administrator permissions for Jeff Leatherman from [SharePoint-SRV](#)
Reduces 1 non-sensitive users potentially leading to this user
- Remove local administrator permissions for Gaspare Fry from [SharePoint-SRV](#)
Reduces 1 non-sensitive users potentially leading to this user
- Remove local administrator permissions for Elizabeth King from [SharePoint-SRV](#)
Reduces 1 non-sensitive users potentially leading to this user

Close

[Send us feedback...](#)

Recommended actions
7 recommended actions

/ Esposizione degli account inattivi/scaduti

Discover inactive and expired accounts in sensitive groups

Improvement actions

Resolve unsecure account attributes High

[Send us feedback...](#)

Report description

Highlights unsecure account attributes that needs to be resolved to improve your security posture. [Learn why this is important to remediate and create an action plan](#)

1 - 2 of 2 entities

Entity

Type

BM

Ballard McGee

Account

BV

Becky Valentine

Account

Remove 2 unsecure account attributes from Arlene Banks

Filter...

Remove Use Kerberos DES encryption types for this account

Removing this setting enables the use of stronger encryption algorithms for the account's password.

Remove Store password using reversible encryption

Removing this setting prevents easy decryption of the account's password.

Close

Recommended actions

Remove 1 unsecure account attribute from Ballard McGee

Remove 1 unsecure account attribute from Becky Valentine

/ Utilizzo di Microsoft LAPS

Highlight which devices don't use Local Administrator Password Solution

Identity Security Posture > Microsoft LAPS usage

Improvement actions
Deploy Microsoft LAPS on every windows device

Report description
All windows based devices not protected by LAPS
[Learn why this is important to remediate and how to fix it](#)

Domain

- domain2.test.local
- AADDSATP.onmicrosoft.com
- domain1.test.local**

Identity Security Posture > Microsoft LAPS usage > domain1.test.local

1 - 20 of 3,003 devices

Device name	Device issue	LAPS password age	Operating system
STANDALONE	✖ LAPS is not deployed	—	Windows Server 2012 R2 Datacenter, 6.3 (9600)
W8-000825-Desktop	✖ LAPS is not deployed	—	Windows 8.1 Ultimate, 9600
W10-000858-Lap	✖ LAPS is not deployed	—	Windows 10 Enterprise, 10586.218
W8-000315-Desktop	✖ LAPS is not deployed	—	Windows 8.1 Ultimate, 9600
W2012R2-000026-Server	✖ LAPS is not deployed	—	Windows 2012 R2 Datacenter, 9600
W10-000089-Lap	✖ LAPS is not deployed	—	Windows 10 Enterprise, 10586.218
W2012R2-000793-Server	✖ LAPS is not deployed	—	Windows 2012 R2 Datacenter, 9600
W10-000346-Lap	✖ LAPS is not deployed	—	Windows 10 Enterprise, 10586.218
W10-000345-Lap	✖ LAPS is not deployed	—	Windows 10 Enterprise, 10586.218
W8-000827-Desktop	✖ LAPS is not deployed	—	Windows 8.1 Ultimate, 9600
W2012R2-000281-Server	✖ LAPS is not deployed	—	Windows 2012 R2 Datacenter, 9600
W2012R2-000028-Server	✖ LAPS is not deployed	—	Windows 2012 R2 Datacenter, 9600
W10-000601-Lap	✖ LAPS is not deployed	—	Windows 10 Enterprise, 10586.218

/ Delega Kerberos non sicura

For apps that request end user access credentials to access resources

Identity Security Posture > Unsecure Kerberos delegation

Improvement actions
Modify unsecure Kerberos delegations High

Report description
All detected entities with unsecure Kerberos delegations posing a risk

Entity	Domain
A APP1	domain1.test.local
D DC1	domain1.test.local
D DC2	domain1.test.local
T TestUser1	domain1.test.local

Unsecure constrained delegation details

This list represents sensitive delegation entries that must be removed to increase security

Filter...

DC1

Domain: domain1.test.local

Delegation attribute: clipsrv

Delegation sensitivity: Sensitive

Close

[Send us feedback...](#)

Download Settings

Recommended actions

- Modify Unconstrained delegation
- Remove 1 delegation
- Remove 1 delegation
- Remove 1 delegation**

/ Tenere traccia dei progressi in Secure Score

Assessments can be found under improvement actions

Microsoft Secure Score Score last calculated 04/08 ; 1:00 AM

Overview Improvement actions History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

↓ Export

Applied filters: Product: Defender for Identity ✕

Rank	Improvement action	Score impact	Points achieved	Status	Regressed	Have license	Category	Product	Last synced	M
1	Reduce lateral movement path risk to sensitive entities	+3.7%	0/5	○ To address	No	Yes	Identity	Defender for Identity	4/6/2021	N
2	Stop legacy protocols communication	+3.7%	0/5	○ To address	Yes	Yes	Identity	Defender for Identity	4/6/2021	None
3	Stop weak cipher usage	+3.7%	0/5	○ To address	Yes	Yes	Identity	Defender for Identity	4/6/2021	None
4	Remove unsecure SID history attributes from entities	+3.7%	0/5	○ To address	Yes	Yes	Identity	Defender for Identity	4/6/2021	None
5	Resolve unsecure account attributes	+3.7%	5/5	✓ Completed	No	Yes	Identity	Defender for Identity	4/6/2021	None
6	Stop clear text credentials exposure	+3.7%	5/5	✓ Completed	No	Yes	Identity	Defender for Identity	4/6/2021	None
7	Disable Print spooler service on domain controllers	+3.7%	5/5	✓ Completed	No	Yes	Identity	Defender for Identity	4/6/2021	None
8	Remove dormant accounts from sensitive groups	+3.7%	5/5	✓ Completed	No	Yes	Identity	Defender for Identity	4/6/2021	None
9	Protect and manage local admin passwords with Microsoft L...	+3.7%	5/5	✓ Completed	No	Yes	Identity	Defender for Identity	4/6/2021	None
10	Modify unsecure Kerberos delegations to prevent impersonat...	+3.7%	5/5	✓ Completed	No	Yes	Identity	Defender for Identity	4/6/2021	None
11	Install Defender for Identity Sensor on all Domain Controllers	+2.96%	4/4	✓ Third party	No	Yes	Identity	Defender for Identity	Not Applicable	None
12	Set a honeytoken account	+0.74%	1/1	✓ Completed	No	Yes	Identity	Defender for Identity	4/8/2021	None
13	Configure Microsoft Defender for Endpoint Integration	+0.74%	1/1	✓ Completed	No	Yes	Identity	Defender for Identity	4/8/2021	None
14	Configure VPN integration	+0.74%	1/1	✓ Completed	No	Yes	Identity	Defender for Identity	4/8/2021	None
15	Fix Advanced Audit Policy issues	+0.74%	1/1	✓ Completed	No	Yes	Identity	Defender for Identity	4/8/2021	None

15 items Search Filter

Category Product Last synced

Identity Defender for Identity 4/6/2021

Identity Defender for Identity 4/6/2021

Identity Defender for Identity 4/6/2021

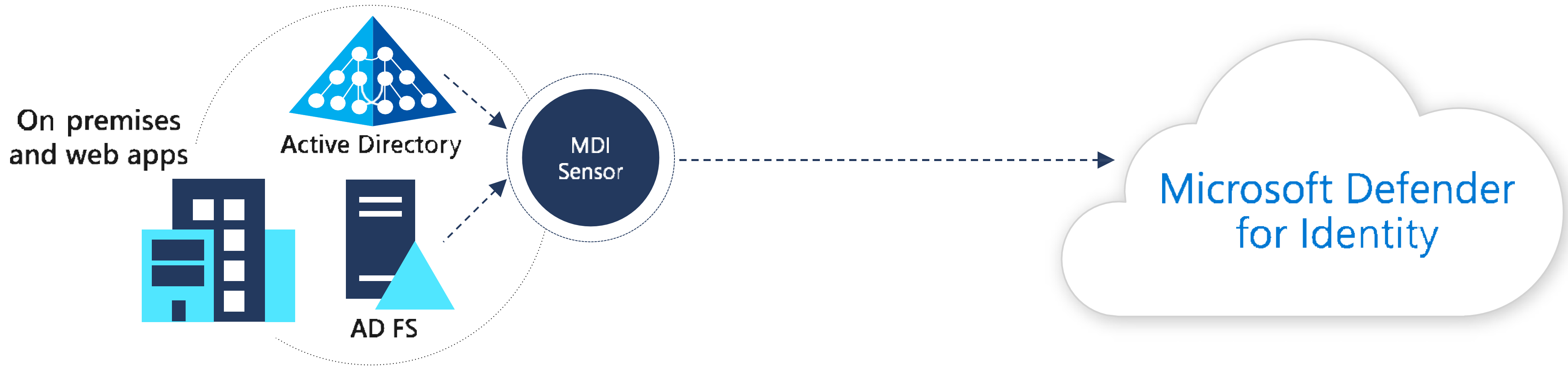
Detect

Real – time analytics and data intelligence



Detect

/ Origini dati e tecnologie di Microsoft Defender per identità



Network traffic analytics

Inspect network traffic:
NTLM, Kerberos, LDAP,
RPC, DNS, SMB

Security events and Active Directory data

Inspect events, event
tracing and profile active
directory entities

User behavior analytics

Profile users and entities
behavior, identify
behavior anomalies

Cloud based real time detections

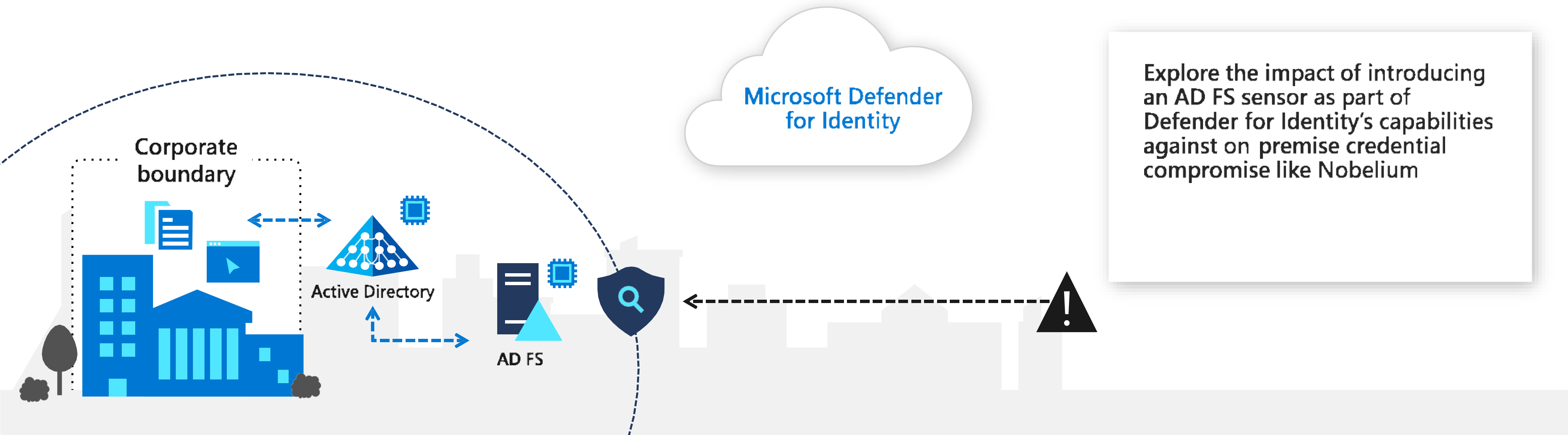
Data enrichment and
correlation in the cloud,
for real time detections

/ Estensione del supporto ad ADFS

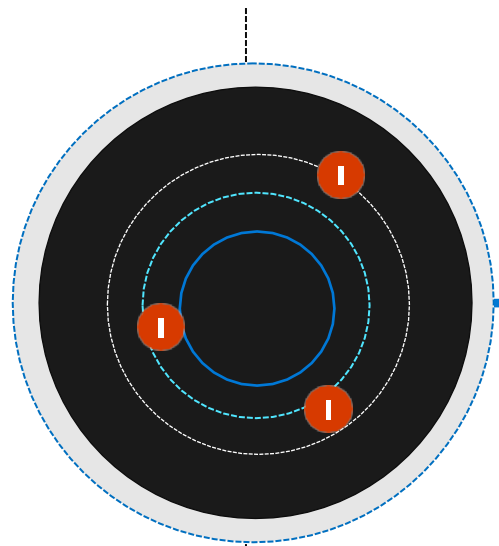
AD FS still plays a huge part in many organizations' identity capabilities

The Defender for Identity sensor now supports AD FS servers, extending advanced identity protection

Microsoft is committed to offering cloud powered solutions to help secure all on premises identities



/ Funzionalità di rilevamento



Reconnaissance

Security principal enumeration (LDAP)
Users group membership enumeration
Users and IP address enumeration

Hosts and server name enumeration (DNS)
Resource access suspicious activities
Reconnaissance by targeted entity attributes

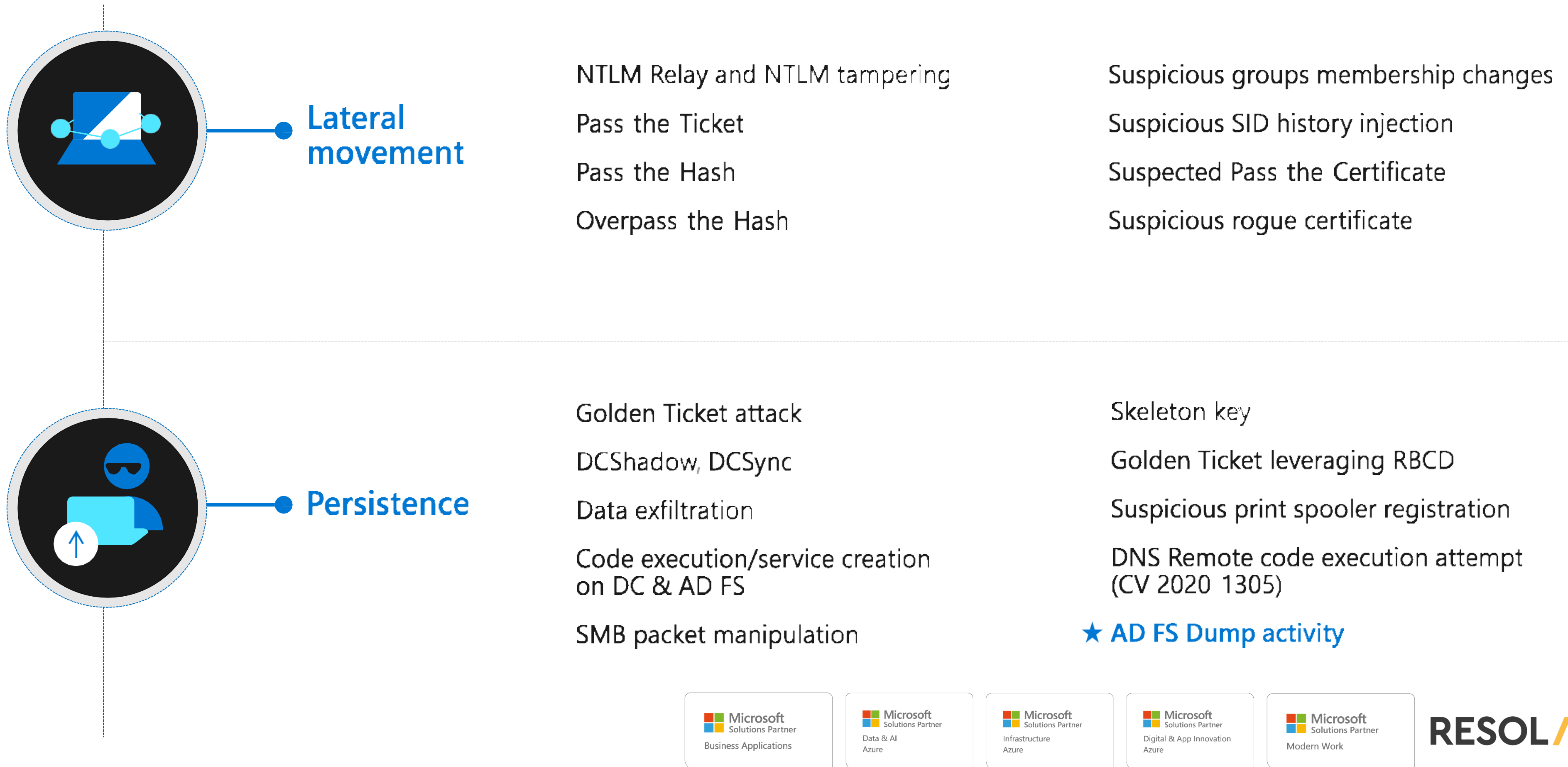


Credential access

Brute force attempts (now also detected via AD FS)
Suspicious VPN connection
Honeytoken account suspicious activities

Logon/failed logon suspicious activities
Suspected Kerberos SPN exposure
Suspicious DC password change using NetLogon (CVE 2020 1472)

/ Funzionalità di rilevamento



/ Panoramica degli avvisi di rilevamento

Alerts

Export

30 Days

Manage alerts

Customize columns

Applied filters: Service sources: Microsoft Defender for Identity

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source
User and IP address reconnaissance (SMB)	+3	Medium	Partially Remediated	Resolved	Discovery	MDI
Suspected overpass-the-hash attack (Kerberos)	+3	High	Partially Remediated	Resolved	Lateral movement	MDI
Suspected overpass-the-hash attack (Kerberos)	+4	High	No threats found	Resolved	Lateral movement	MDI
Remote code execution attempt	+4	Medium	No threats found	Resolved	Execution	MDI
Suspected DCSync attack (replication of directory services)	+3	High	No threats found	Resolved	Credential access	MDI
Suspected Netlogon privilege elevation attempt (CVE-2020-1472 exploitati...	+3	High		Resolved	Privilege escalation	MDI
Suspected identity theft (pass-the-ticket)	+4	High	Failed	Resolved	Lateral movement	MDI
Suspected skeleton key attack (encryption downgrade)	+2	Medium		Resolved	Persistence	MDI
☐ User and IP address reconnaissance (SMB)	+3	Medium	Partially Remediated	New	Discovery	MDI

/ Dettagli dell'avviso di rilevamento: Sospetto attacco DCSync

Related users

What happened

Evidence

More info on side panel

Alerts > Suspected DCSync attack (replication of directory services)

Related entities

mtpdemos\jalever
Source Account

MTP-AIR-DC01
Destination Host
WindowsServer2019 +7

AnnetteH-PC
Source Host
+6

What happened

Janet Leverling on AnnetteH-PC sent 1 replication request to MTP-AIR-DC01.

Important information:

- AnnetteH-PC is not a recognized domain controller.
- Mar 26, 2021 10:24 PM
- AnnetteH-PC resolved from 172.16.64.19 with high certainty.
- Potential sensitive lateral movement path identified to sensitive user(s), that includes ANNETTEH-PC.

Suspected DCSync attack (replication of directory services)

High Unknown Resolved

Alert state

Classification

True alert

Set Classification

Assigned to

David@MTPDemos.net

Alert details

Category

Credential access

MITRE ATT&CK Techniques

-

Detection source

MDI

Detection status

Unknown

Detection technology

-

Generated on

Mar 26, 2021 4:45:13 PM

First activity

Mar 26, 2021 3:24:54 PM

Last activity

Mar 26, 2021 3:24:54 PM

Microsoft
Solutions Partner
Business Applications

Microsoft
Solutions Partner
Data & AI
Azure

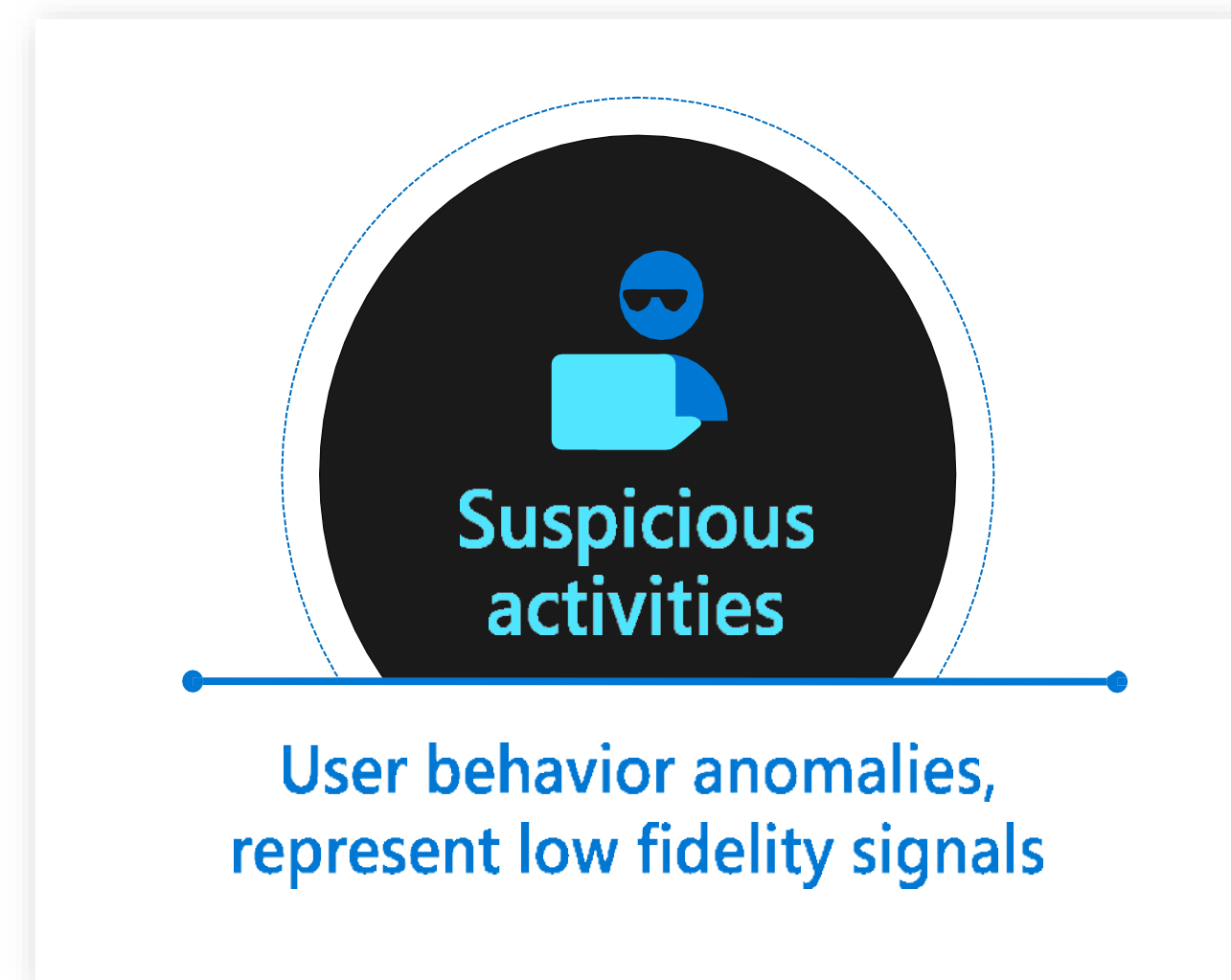
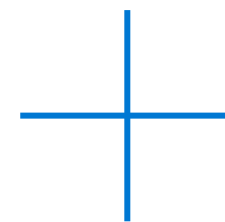
Microsoft
Solutions Partner
Infrastructure
Azure

Microsoft
Solutions Partner
Digital & App Innovation
Azure

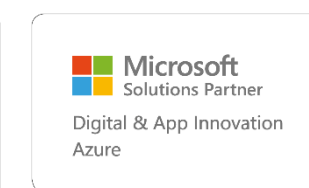
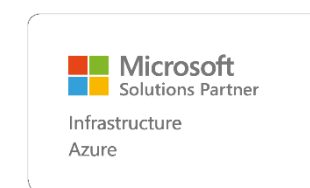
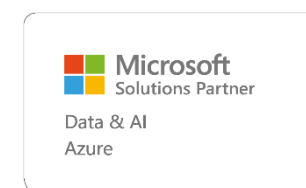
Microsoft
Solutions Partner
Modern Work

RESOL/E

/ Ampiezza di rilevamento: attività sospette e analisi del comportamento

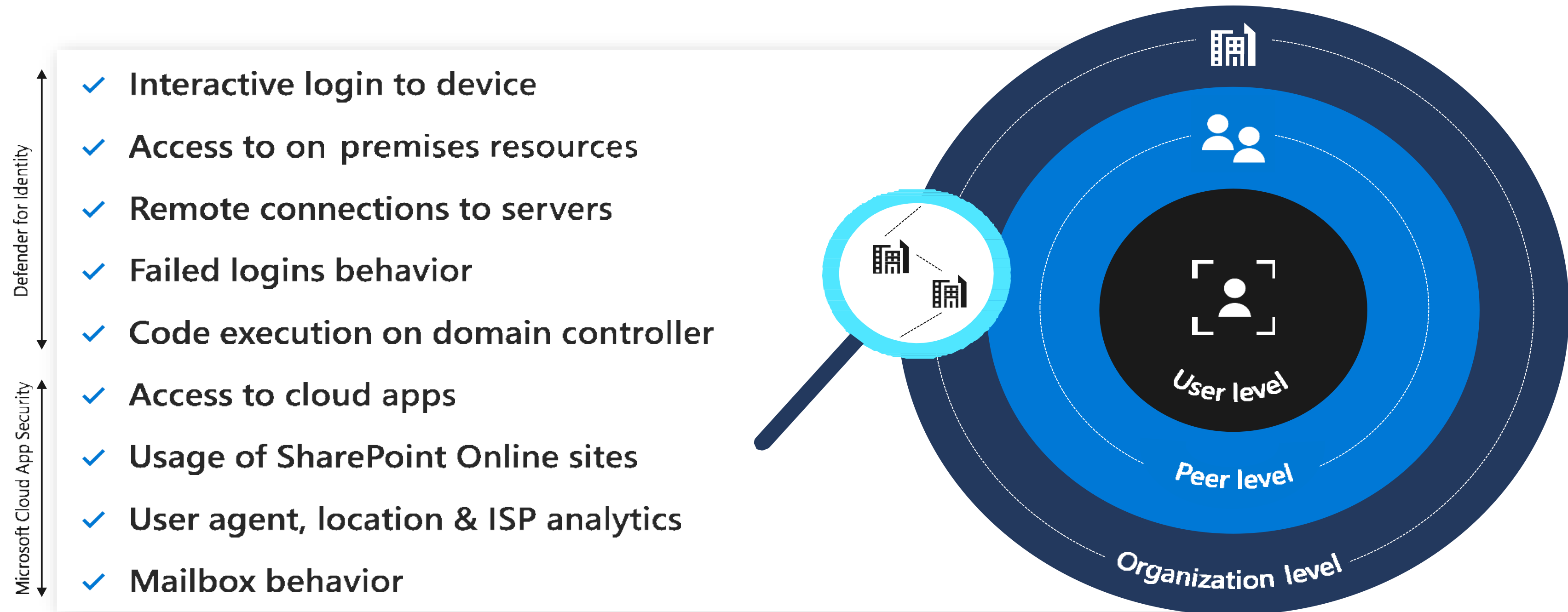


Maggiore visibilità



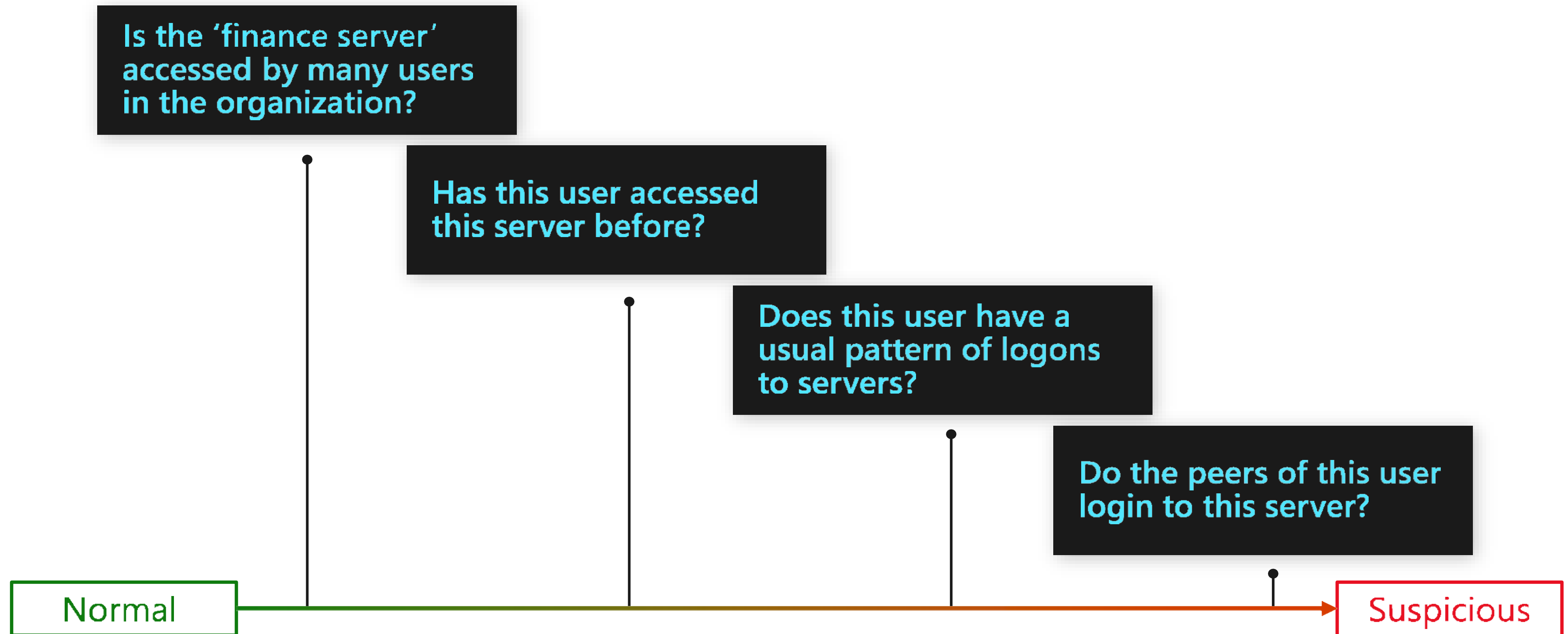
RESOL/E

Analisi del comportamento delle attività per utente, peer e organizzazione in Microsoft Defender for Identity e Cloud App Security



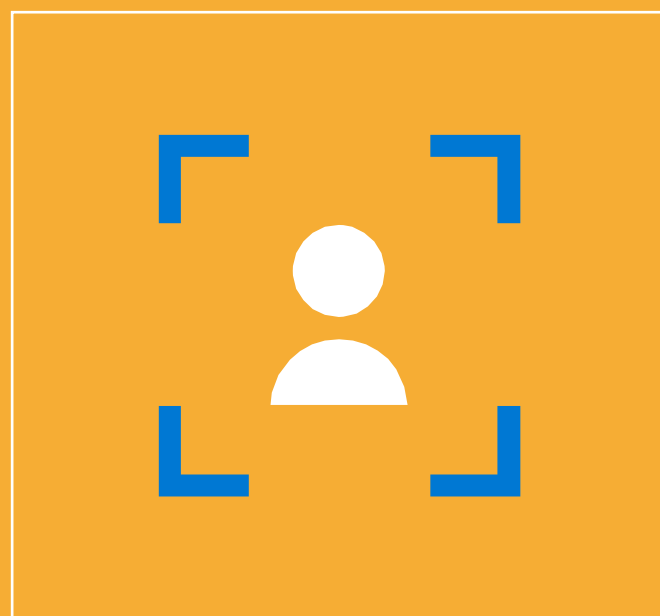
/ Processo di analisi delle attività sospette

Example: User accesses the 'finance' server



Investigate

User investigation priority scoring

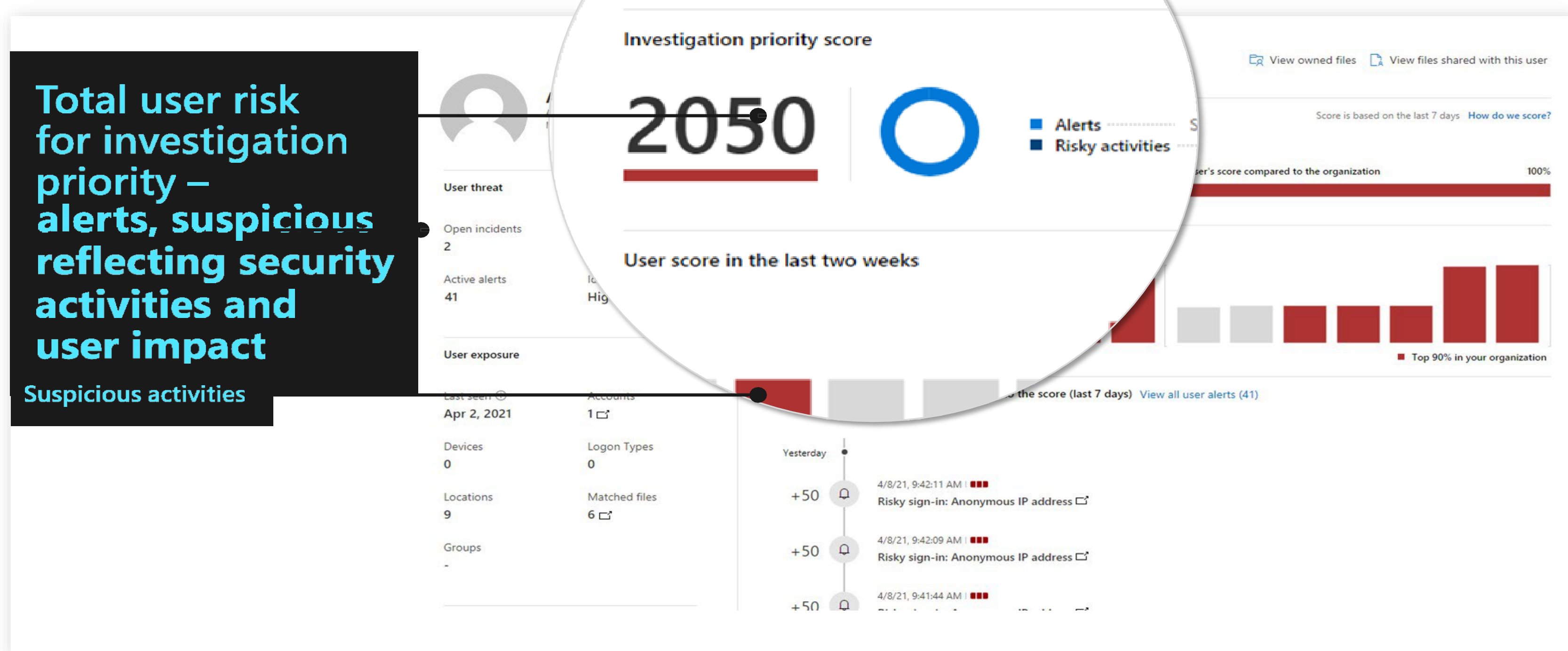


Investigate

/ Punteggio di priorità dell'indagine utente

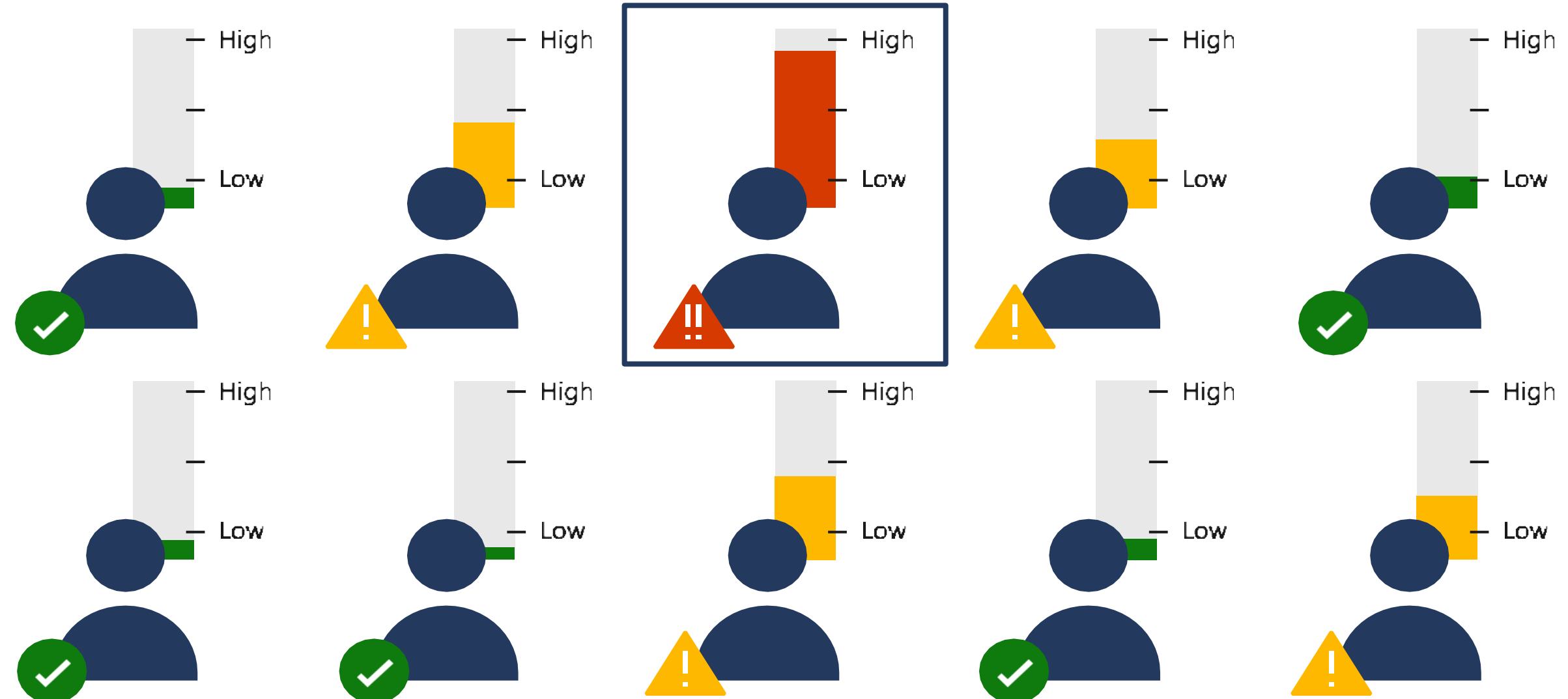
Total user risk for investigation priority – alerts, suspicious activities and user impact

Suspicious activities



Definizione delle priorità delle indagini sulle minacce e sugli attacchi basati sull'identità

Investigating
the impact on
all related users
in an incident



/ Classificazione delle indagini sugli utenti

Highlight top users to investigate through investigation priority

User	Title	Investigation priority ↓
 aarifs	Administrative	 2050
 andrew.fuller	Vice President of Sales	 750
 Janet.Leverling	Sr. Azure Stack Operator	 50
 annhill	Purchasing Assistant	0
 Stephanie.Conroy	Senior IT Services Engineer	0
 anstahl	Port Technician - WC60	0
 alexw	Marketing Assistant	0
 jogoldb	Senior UI Design Engineer	0
 alexwilber	Marketing Assistant	0

/ Indagine sull'identità



Nick Carlsson
Admin
System

SENSITIVE DOMAIN ADMIN

User threat

Open incidents
0

Investigation prio...
0

Active alerts
0

Identity risk level
High

Lateral movement paths
View recent

User exposure

First seen
Oct 11, 2020

Last seen
Apr 8, 2021

Accounts
6

Devices
10

Logon Types
2

Locations
0

Matched files
0

Groups
9

Contact information

User risk

Lateral movement paths PREVIEW

Select a date:
Monday, January 25, 2021

Path initiator:
CN Clida Neal

All paths to Nick Carlsson on Jan 25, 2021
Paths are shown by the path initiator

Show only risky paths (4)

CN Clida Neal 1 steps from Nick Carlsson

EK Elizabeth King 1 steps from Nick Carlsson

GF Gaspare Fry 1 steps from Nick Carlsson

VP Vivan Perez 1 steps from Nick Carlsson

CN Clida Neal

NC Nick Carlsson

User's lateral

Show chosen path

Limit to risky paths

/ Eventi imprevisti di Microsoft 365 Defender

Summary Alerts (107) Devices (6) Users (10) Mailboxes (16) Investigations (18) Evidence and Response (311)									
1-30 of 57 < > Choose columns 30 items per page									
Title	Tags	Severity	Status	Linked by	Category	Impacted Entities	Service source	Detection sour...	
Suspicious behavior by Microsoft Word was observed	Demo Machine +2	Medium	New	7 reasons	Initial access	annetteh-pc.mtpdemos...	Endpoint	Endpoint	
An Office application ran suspicious commands	Demo Machine +2	Medium	New	Same device	Initial access	annetteh-pc.mtpdemos...	Endpoint	Endpoint	
Anomalous account lookups	Demo Machine +2	Low	New	Manual association	Discovery	annetteh-pc.mtpdemos...	Endpoint	Endpoint	
Suspicious process injection observed	Demo Machine +2	Medium	New	Same device	Defense evasion	annetteh-pc.mtpdemos...	Endpoint	Endpoint	
User and IP address reconnaissance (SMB)									
Demo Machine +2		Medium	New	3 reasons					
Unexpected behavior observed by a process ran with no C...	Demo Machine +2	Medium	New	Same device	Execution	annetteh-pc.mtpdemos...	Endpoint	Endpoint	
'Mikatz' high-severity malware was detected	Data sensitivity: High +4	High	Resolved	2 reasons	Malware	mtp-air-dc01.mtpdemos.net	Endpoint	Antivirus	
'Mimilove' high-severity malware was detected	Data sensitivity: High +4	High	Resolved	2 reasons	Malware	mtp-air-dc01.mtpdemos.net	Endpoint	Antivirus	
An active 'Mimikatz' hacktool was detected	Data sensitivity: High +4	Medium	New	3 reasons	Malware	mtp-air-dc01.mtpdemo...	Endpoint	Antivirus	
2 alerts: Suspected overpass-the-hash attack (Kerberos)									
Demo Machine +4		High	Multiple	7 reasons					
Successful logon using overpass-the-hash with potentially ...	Data sensitivity: High +3	Medium	Resolved	4 reasons	Lateral movement	janet-pc.mtpdemo...	Endpoint	365 Defender	
Suspected identity theft (pass-the-ticket)									
Data sensitivity: High +3		High	In progre...	2 reasons					

/ Caccia avanzata in Microsoft 365 Defender

Advanced hunting

Schema

Alerts

- AlertInfo
- AlertEvidence

Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- AppFileEvents
- CloudAppEvents

Email

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents

Get started

Query

Schema reference

Run query

+ New

Save

Share link

Last 7 days

Create detection rule

```
1 IdentityQueryEvents
2 | where Timestamp > ago(7d)
3 | where ActionType == "SamrQuerySuccess" and isnotempty(AccountName)
4 | project QueryTime = Timestamp, DeviceName, AccountName, Query, QueryTarget
5 | join kind=inner (
6 DeviceProcessEvents
7 | where Timestamp > ago(7d)
8 | extend DeviceName =toupper(trim(@"\.*$",DeviceName))
9 | where InitiatingProcessCommandLine contains "net.exe"
10 | project ProcessCreationTime = Timestamp, DeviceName, AccountName, InitiatingProcessFileName , InitiatingProcessCommandLine ) on DeviceName, AccountName
11 | where ProcessCreationTime - QueryTime between (-2m .. 2m)
12 | project QueryTime, DeviceName, AccountName, InitiatingProcessFileName, InitiatingProcessCommandLine, Query, QueryTarget
```

For example, you can now understand what devices and processes expose passwords in clear text. Microsoft 365 Defender's advanced hunting capability allows you to correlate Defender for Identity and Defender for Endpoint activities.

/ Caccia avanzata in Microsoft 365 Defender

Enumerazione delle risorse del controller di dominio di alto valore seguite da tentativi di accesso per convalidare le credenziali rubate in prossimità del tempo

```
MaxTime == 1d;  
let MinNumberLogon = 5;  
dispositivi che tentano l'enumerazione di  
IdentityQueryEvents controller di dominio di valore  
elevato  
| dove Timestamp > ago(30d)  
| dove Applicazione == "Active Directory"  
| dove QueryTarget in ("Controller di dominio di sola lettura") //asset di controller di dominio di sola  
lettura di alto valore  
| Timestamp del progetto, Protocollo, Query, DeviceName, AccountUpn  
| join kind = innerunique (  
dispositivi che tentano di accedere {MaxTime} dopo  
l'enumerazione IdentityLogonEvents  
| dove Timestamp > ago(30d)  
| dove ActionType == "LogonSuccess"  
| progetto LogonTime = Timestamp, DeviceName, DestinationDeviceName) su DeviceName  
| dove LogonTime tra (Timestamp .. (Timestamp + MaxTime))  
| summarize n=dcount(NomeDispositivoDestinazione), TargetedDC = makeset(NomeDispositivoDestinazione) per  
Timestamp, Protocollo, NomeDispositivo  
| dove n >= MinNumberLogon
```

/ Regole di rilevamento personalizzate

Build your own alerts to monitor what what's important to you

Create detection rule

● Alert details

○ Impacted entities

○ Actions

○ Scope

○ Summary

Create detection rule

✓ Alert details

✓ Impacted entities

✓ Actions

✓ Scope

● Summary

Summary

Alert details

Rule name
Custom Detection Rule

Frequency
Every 24 hours

Alert title
Failed Logons to VictimPC

Alert category
Initial access

Impacted entities

Entity type	Column
Device	DeviceName

Scope

Apply alert to
All devices

Back

 Microsoft
Solutions Partner
Business Applications

 Microsoft
Solutions Partner
Data & AI
Azure

 Microsoft
Solutions Partner
Infrastructure
Azure

 Microsoft
Solutions Partner
Digital & App Innovation
Azure

 Microsoft
Solutions Partner
Modern Work

RESOL/E

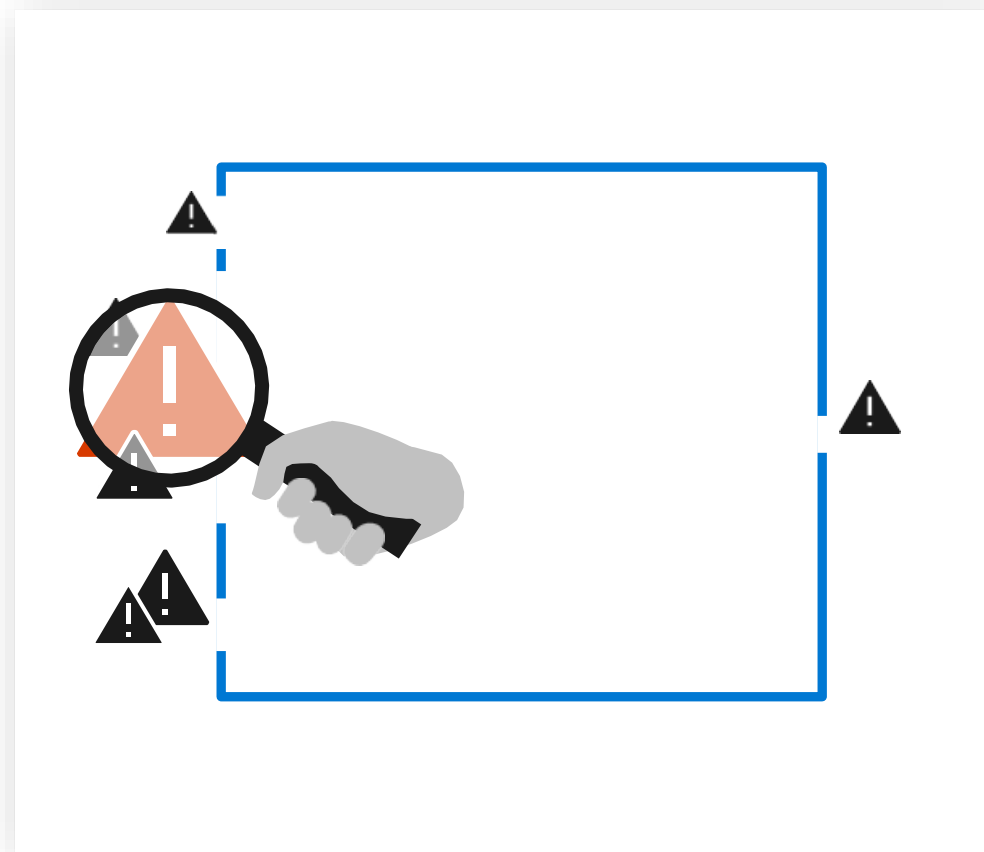
Respond

Automated security workflows

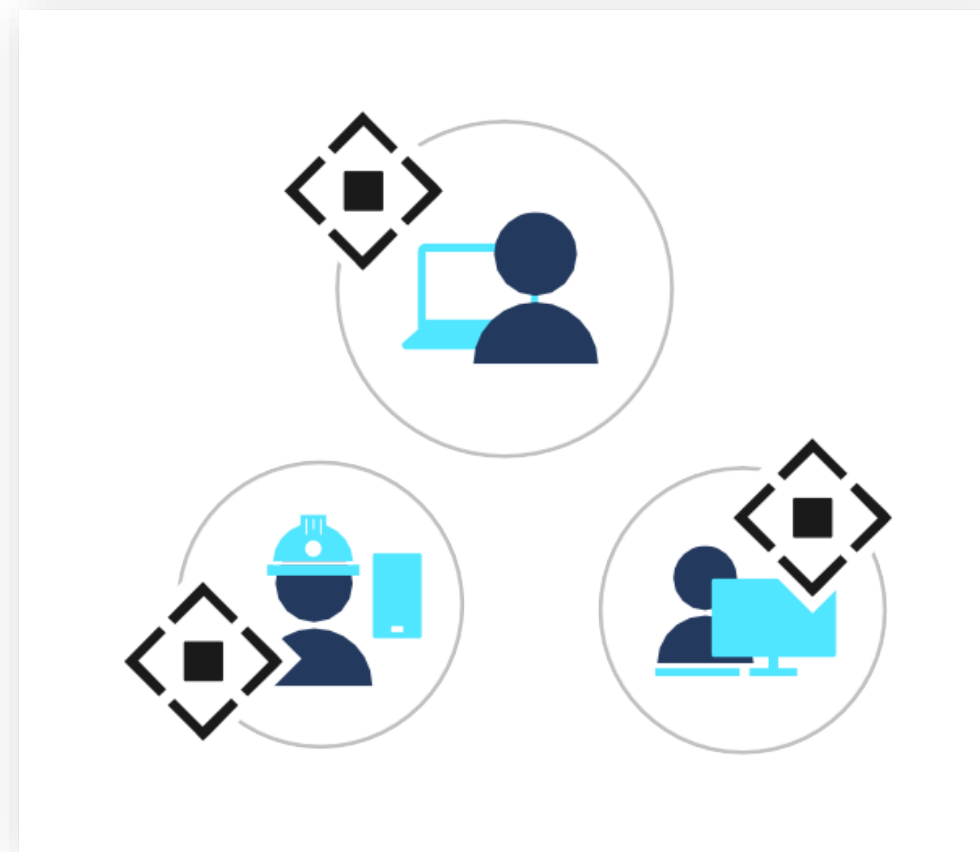


Respond

/ Un'ampia gamma di rischi per la sicurezza dell'identità



It's easy to miss risky configurations...

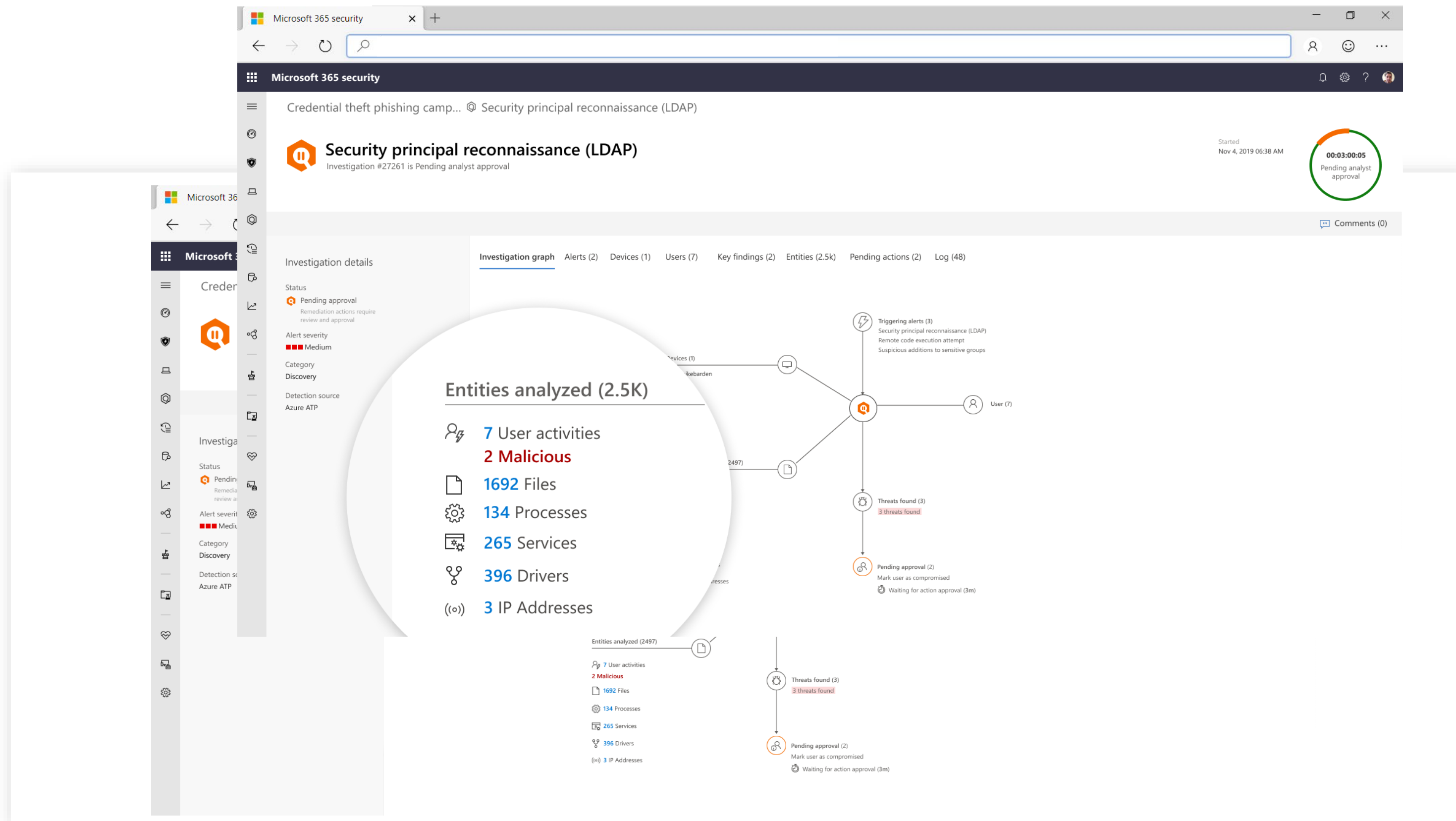


Threats can originate anywhere...



Activity volume makes prioritization difficult...

/ Risposta automatizzata agli eventi imprevisti di Microsoft 365 Defender



CYBERSECURITY AVANZATA

/ DOMANDE

Chiedete in chat le vostre curiosità

 **Microsoft**
Solutions Partner
Business Applications

 **Microsoft**
Solutions Partner
Data & AI
Azure

 **Microsoft**
Solutions Partner
Infrastructure
Azure

 **Microsoft**
Solutions Partner
Digital & App Innovation
Azure

 **Microsoft**
Solutions Partner
Modern Work

RESOL/E

/ CLOUD CONFERENCE ITALIA 2025



📅 **23 Ottobre**
📍 **BHR di Treviso**



RESOL/E

/ IT & MICROSOFT TRAINING

CORSO NIS2



Impara rafforzare la governance IT con misure tecniche ed organizzative che soddisfano la NIS2

Quando:

16 settembre dalle 9.00 alle 13.00

Dove:

Online, Piattaforma Teams

Docente:

Vincenzo Pagano

/ CLOUD VIABILITY ASSESSMENT



Stai valutando la migrazione della tua infrastruttura in Cloud?

Puoi candidarti per il Cloud Viability Assessment di Microsoft, avrai

- / un report che dettaglia i **costi operativi** previsti per l'azienda
- / un'analisi **costi/benefici**
- / una sintesi degli **step di migrazione**

Scrivici a info@resolve-consulenza.it

CYBERSECURITY AVANZATA

/ CONTATTI

Resolve è la società di 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



RESOL/E

RESOL/E

by ErgonGroup