RESOLVE

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

RESOLVE

# / 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

RESOLVE

# / 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

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

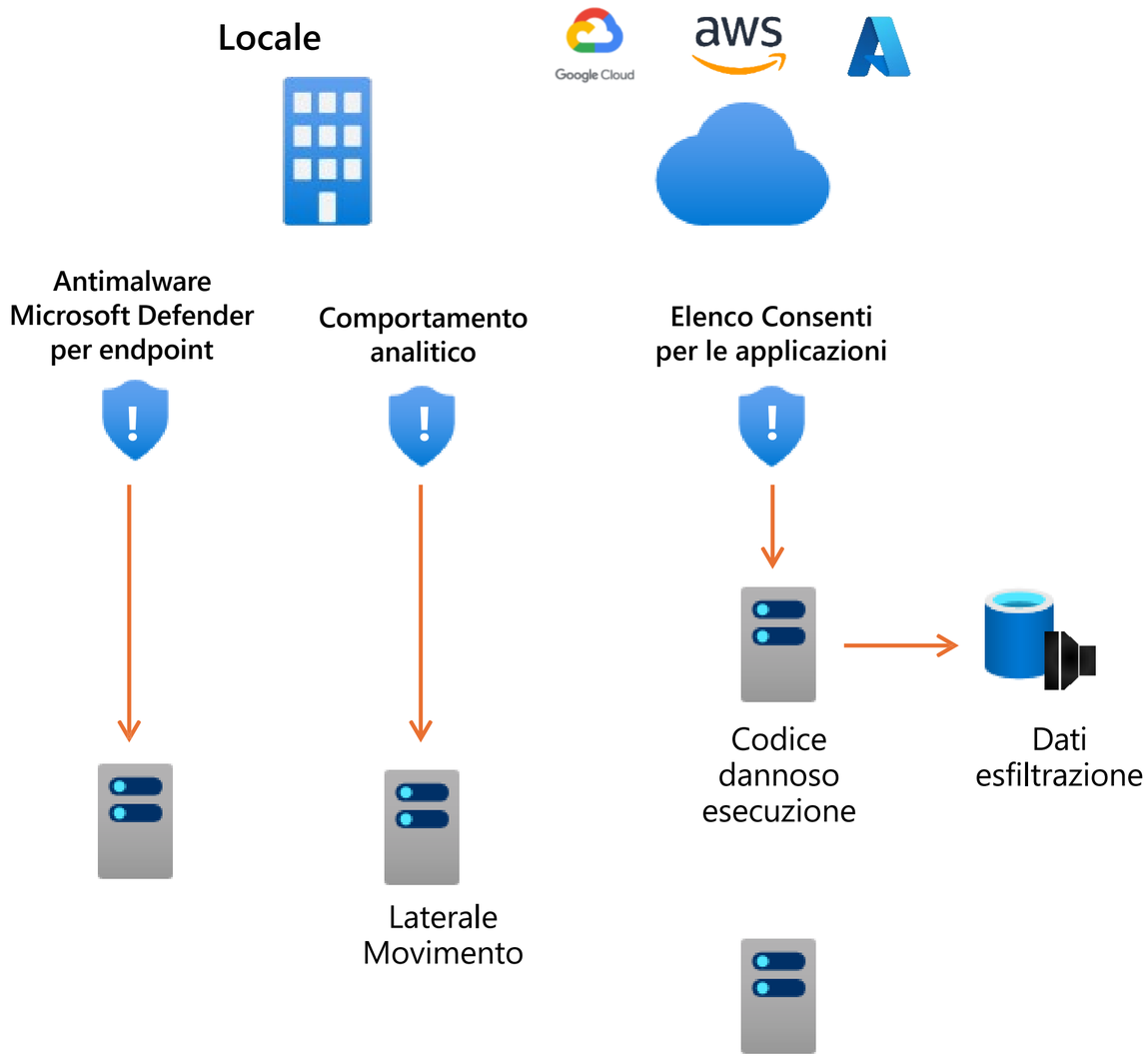
01. MICROSOFT DEFENDER FOR SERVER

# 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 detenction e risposta
- Valutazione delle vulnerabilità

### Ottimizzato per gli ambienti cloud

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



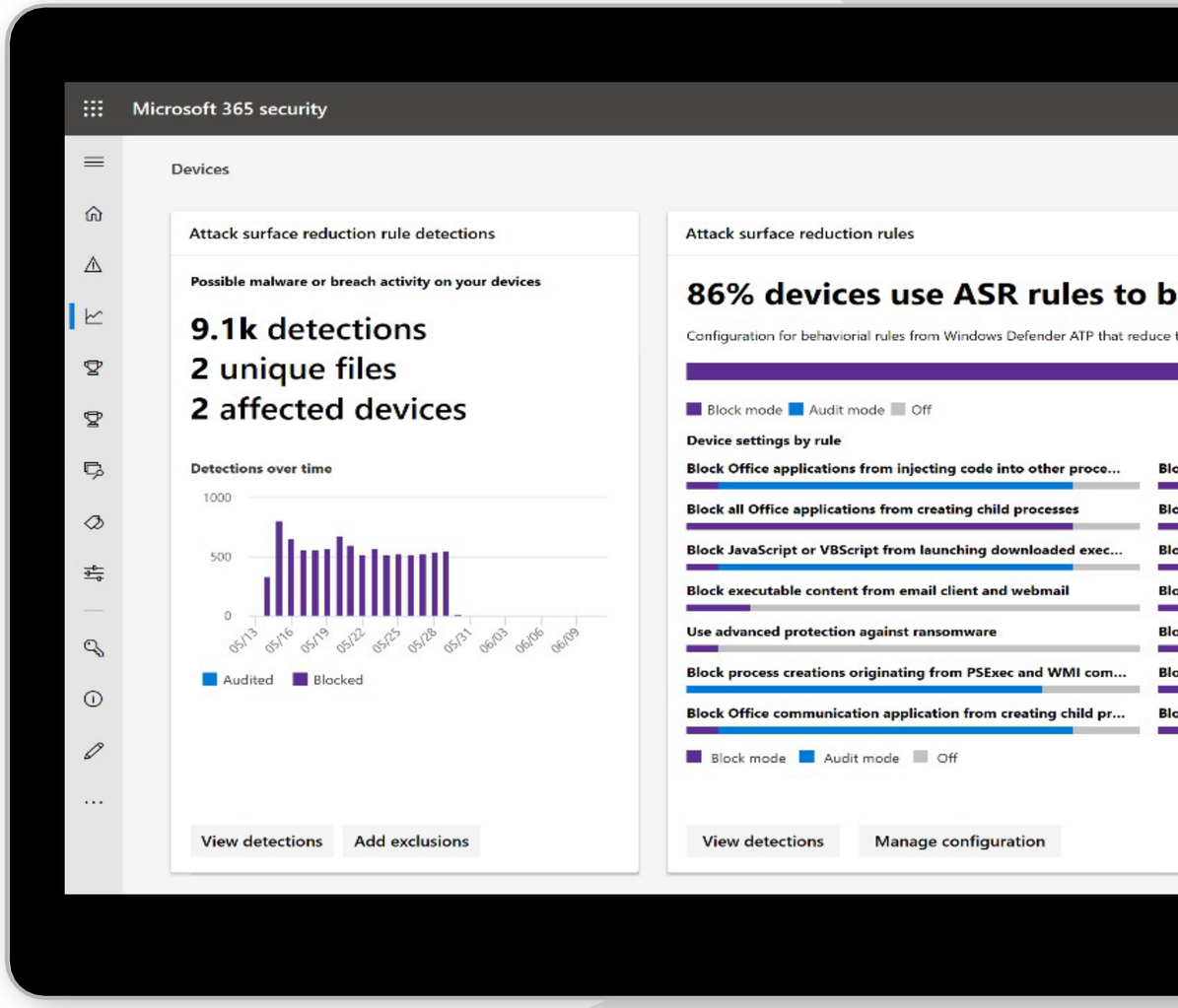


# Riduzione della superficie di attacco

## Basato su Microsoft Defender per endpoint

### Eliminare il rischio di attacco riducendo la superficie

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




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

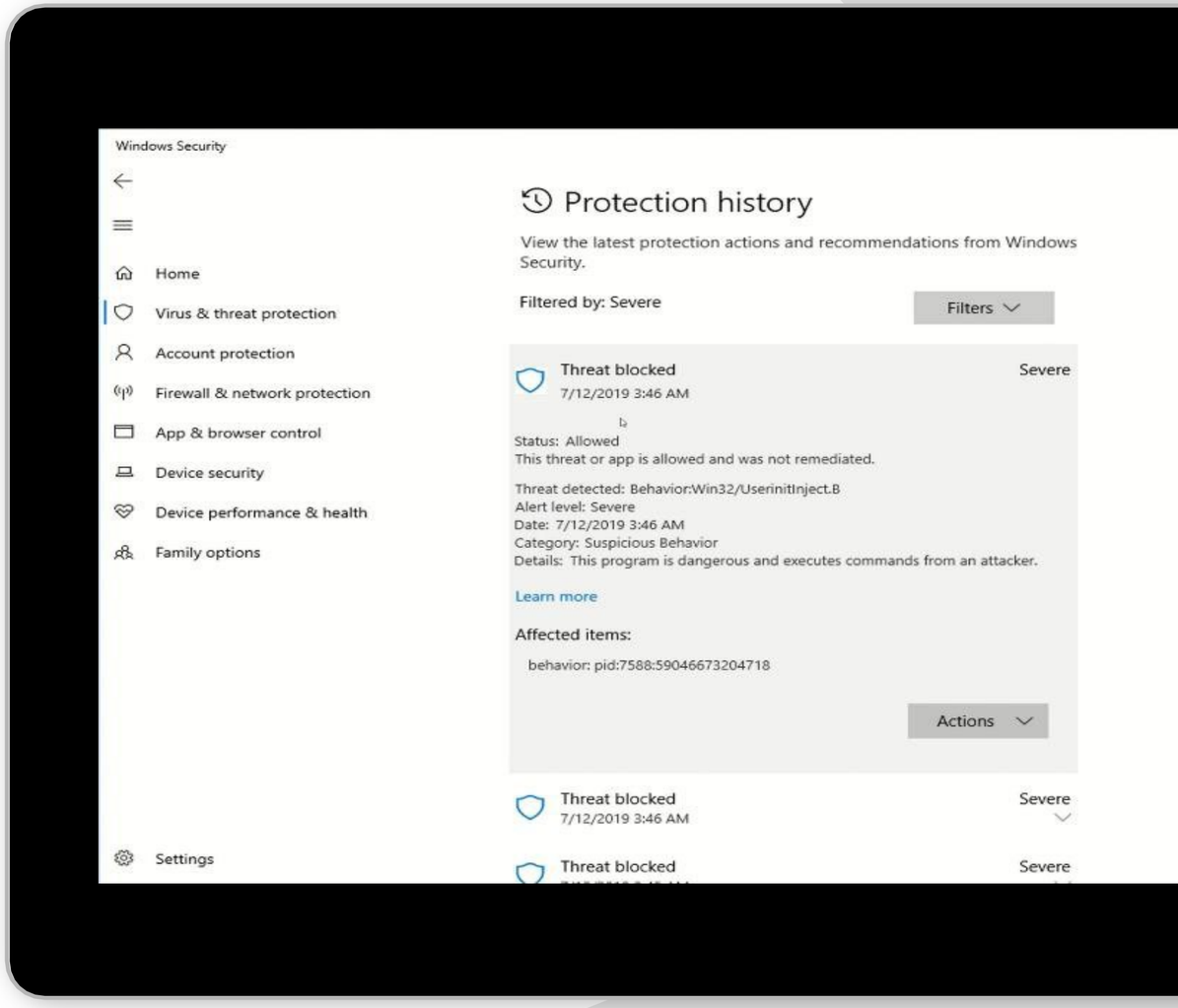
RESOLVE

# 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




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

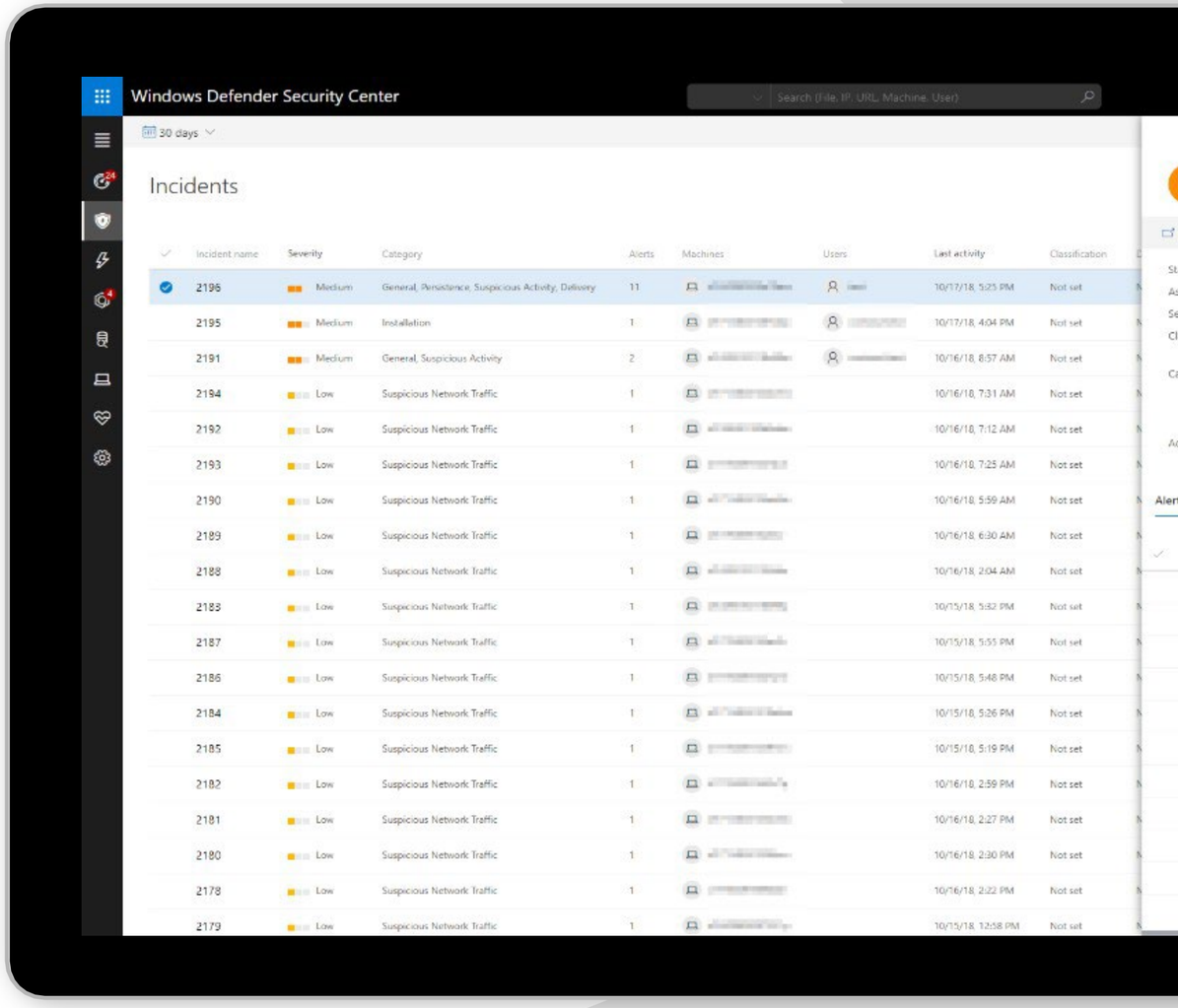
RESOLVE

# 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

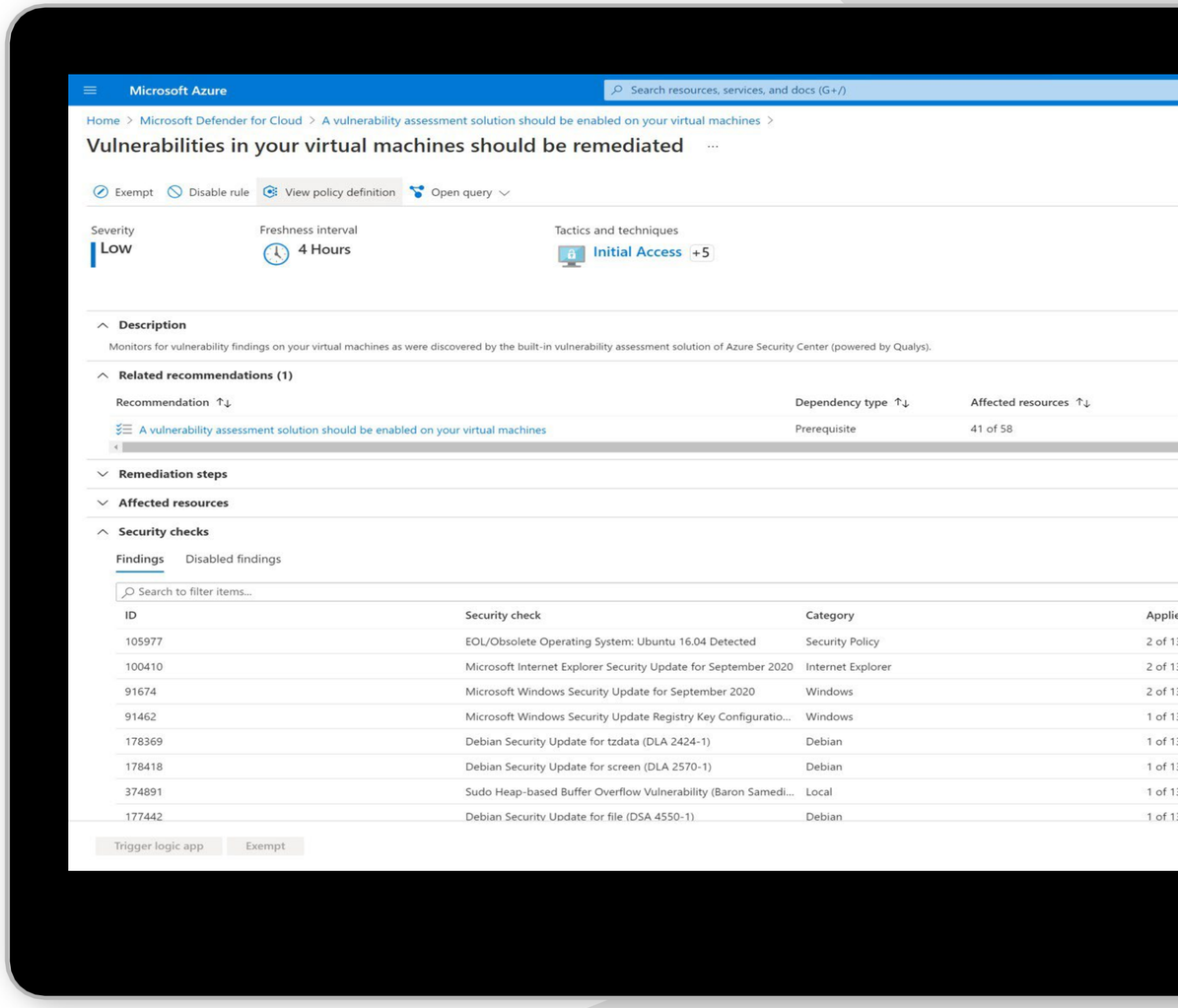
Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

# 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




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

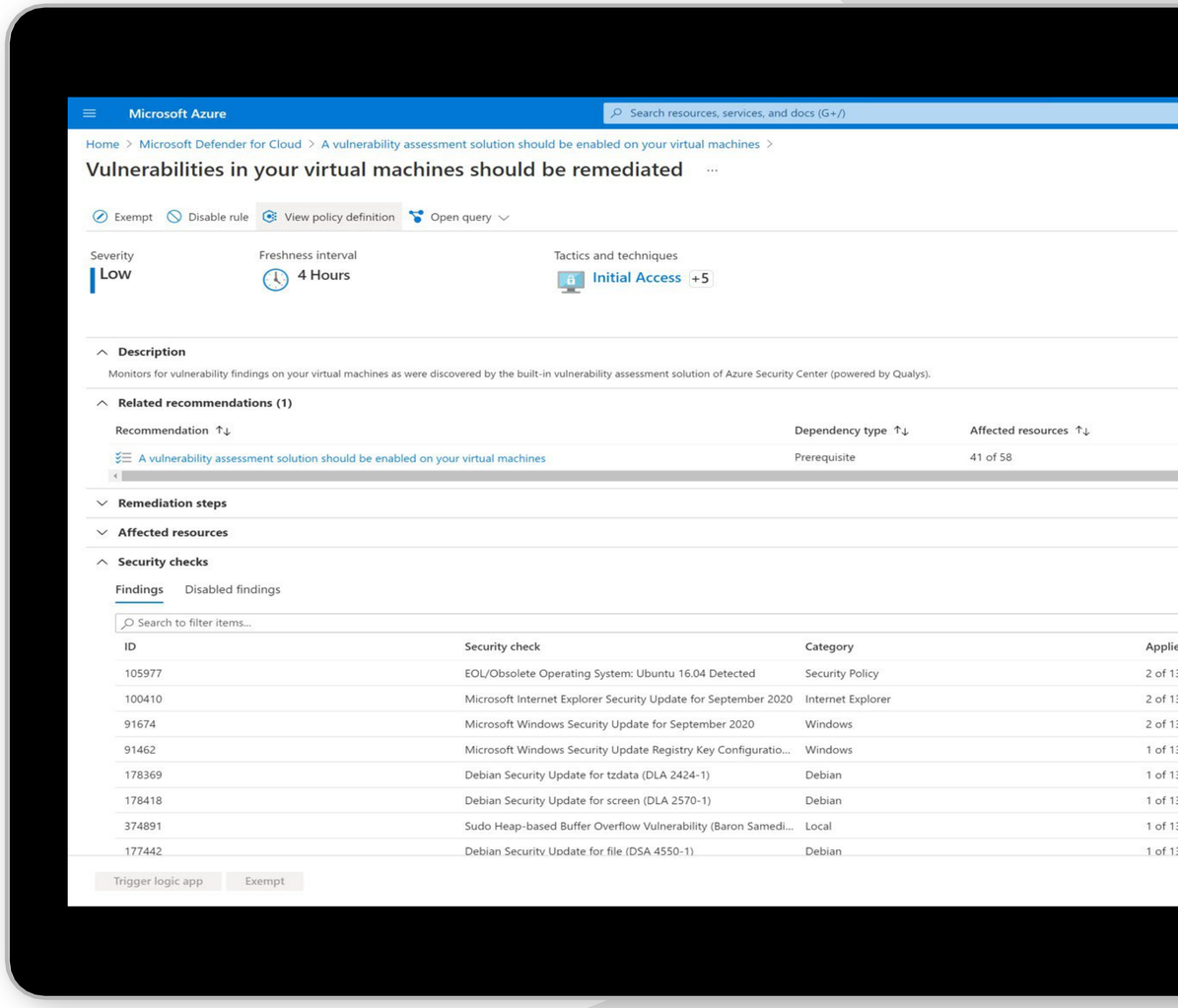
Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

# 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




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

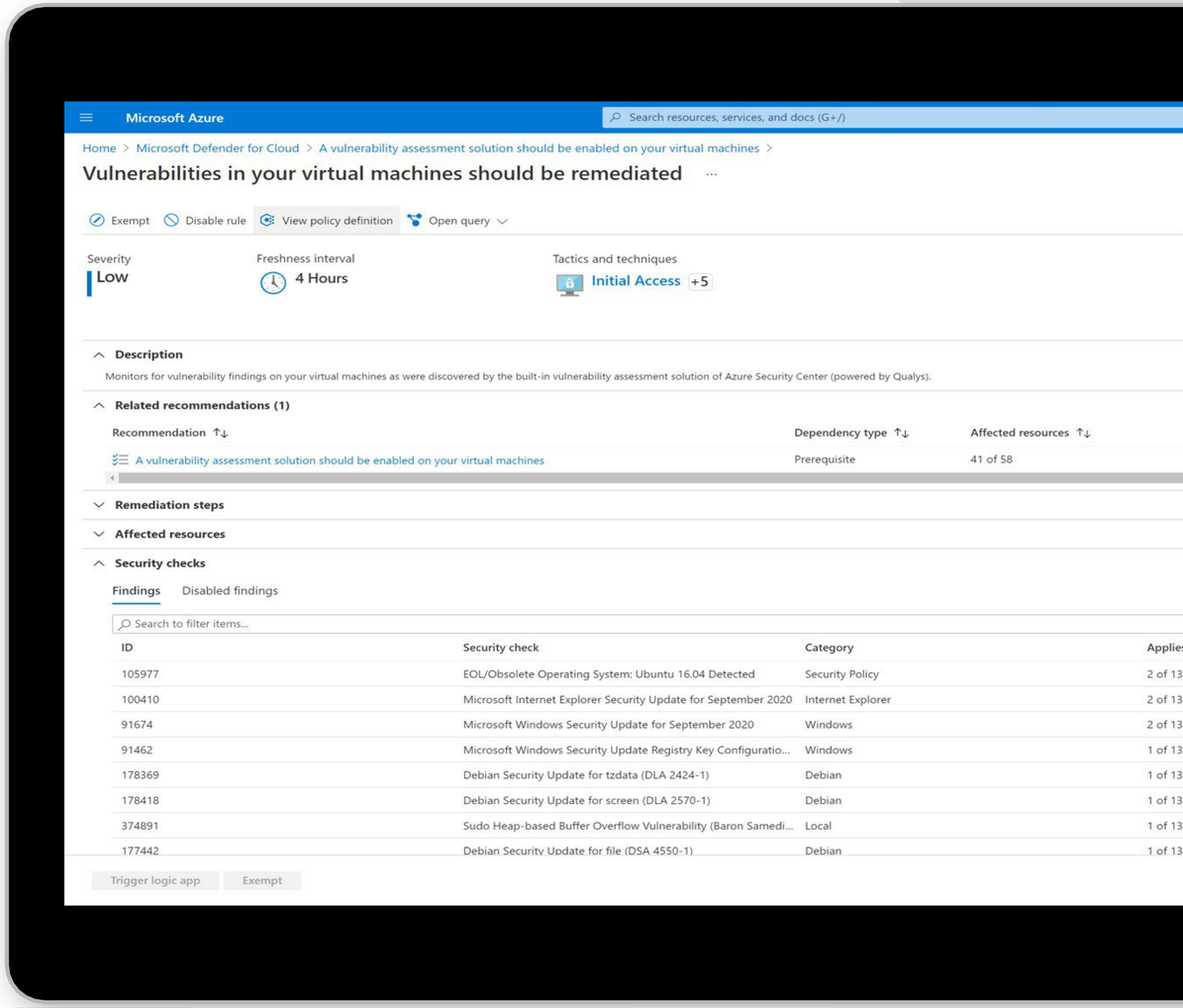
Microsoft Solutions Partner
Modern Work

RESOLVE

# 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




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

RESOLVE

# 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 multiclou 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

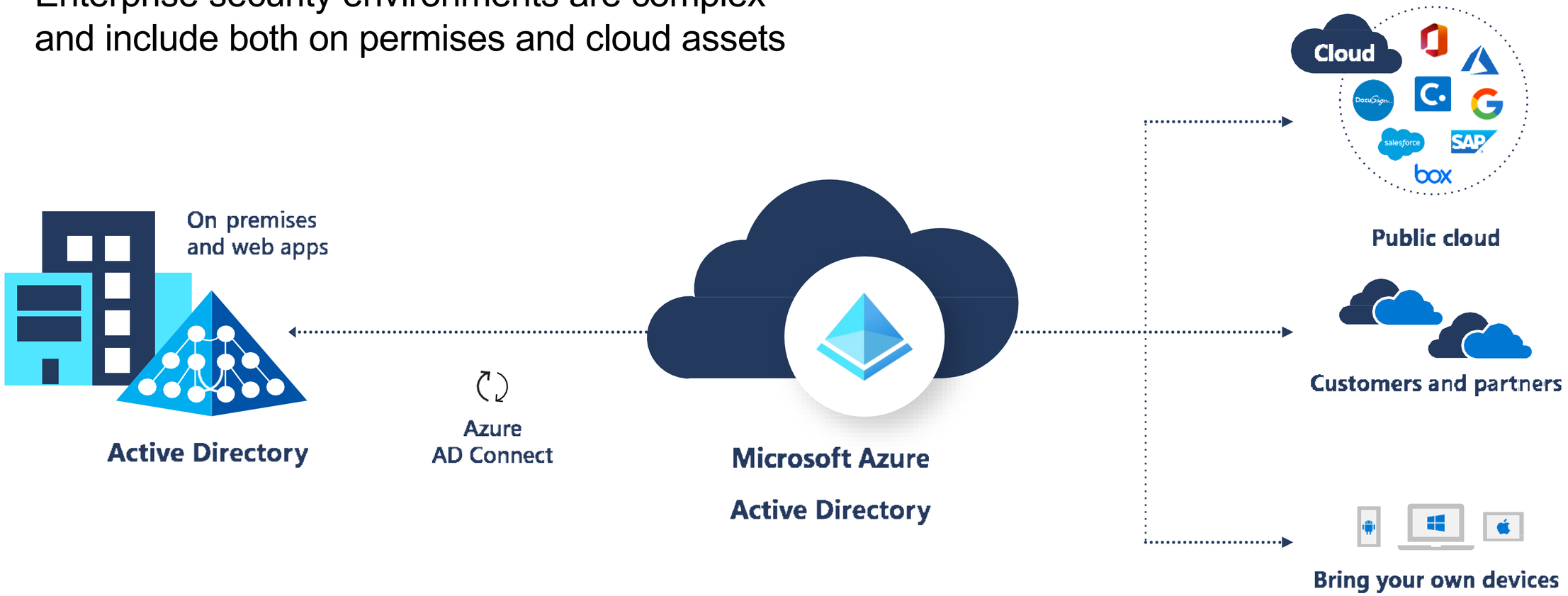
**Azure Arc** abilita la gestione del cloud e le protezioni di sicurezza

Un unico piano di controllo per qualsiasi risorsa, ovunque

# INTEGRAZIONE CON MICROSOFT DEFENDER XDR

# La complessità del panorama della sicurezza delle identità aziendali

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




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

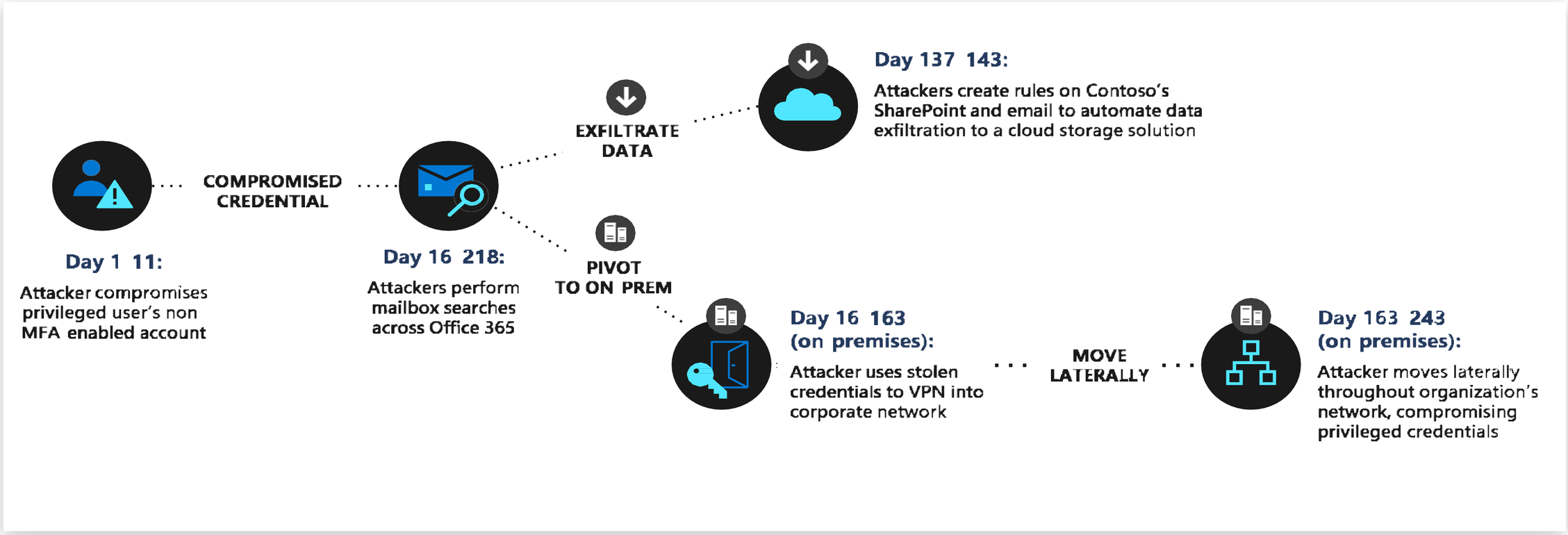
Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

# La complessità del panorama della sicurezza delle identità aziendali

One example of how happens and compromise an entire organisation




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

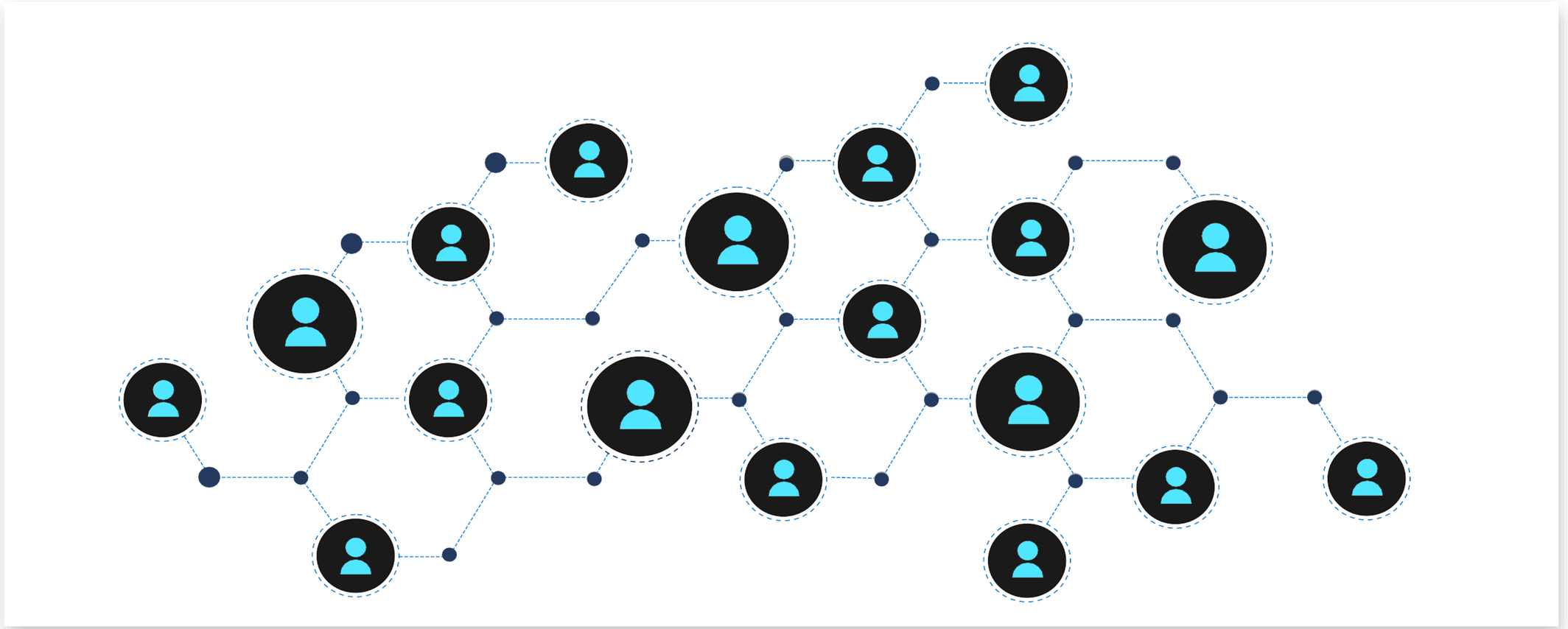
Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

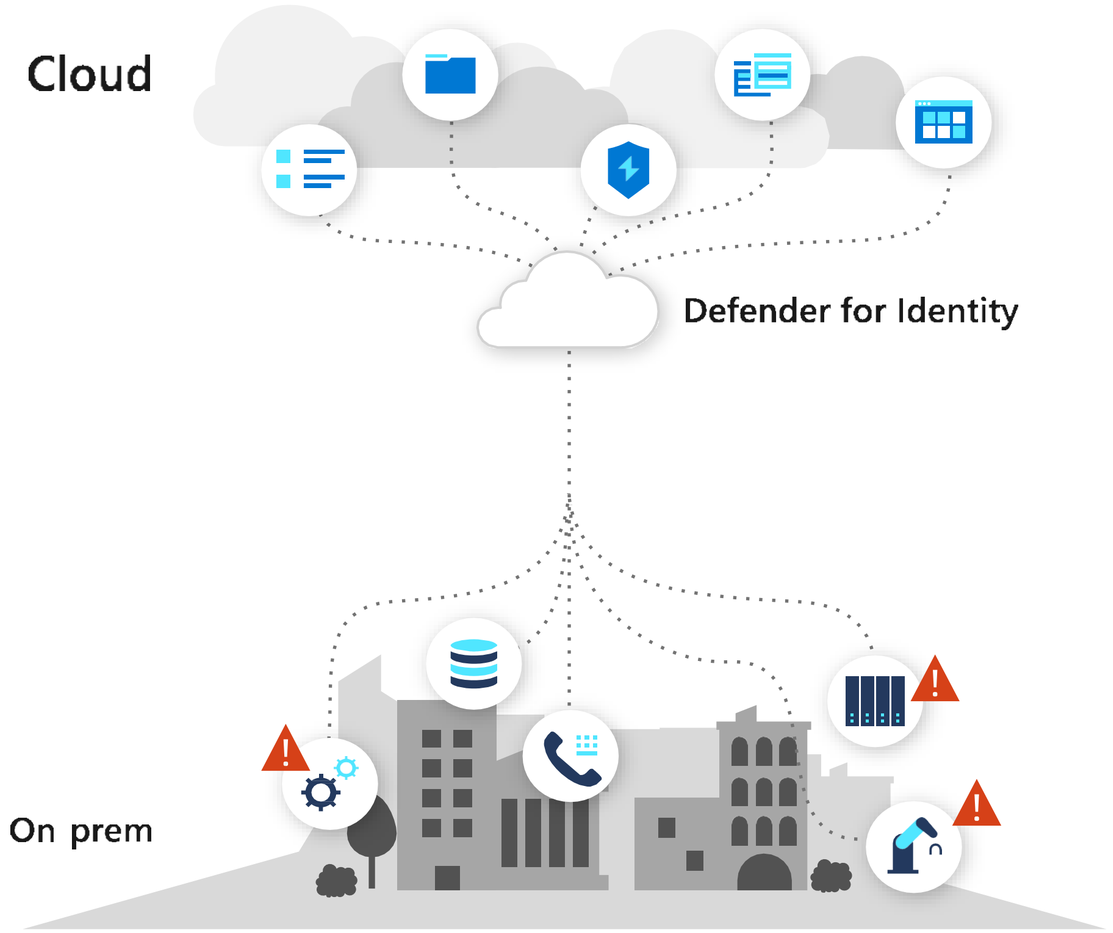
RESOLVE

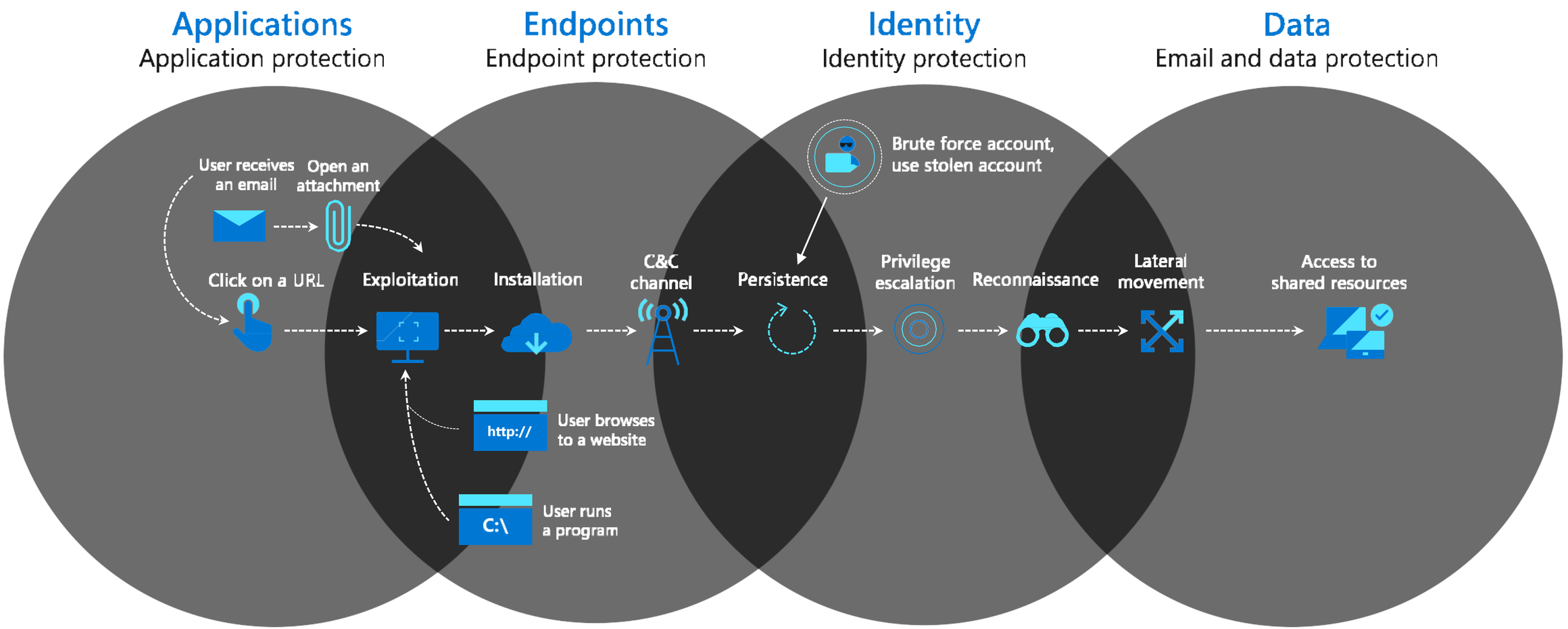
# Un nuovo perimetro di sicurezza: l'identità dell'utente

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






Microsoft

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

RESOLVE

# 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 Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

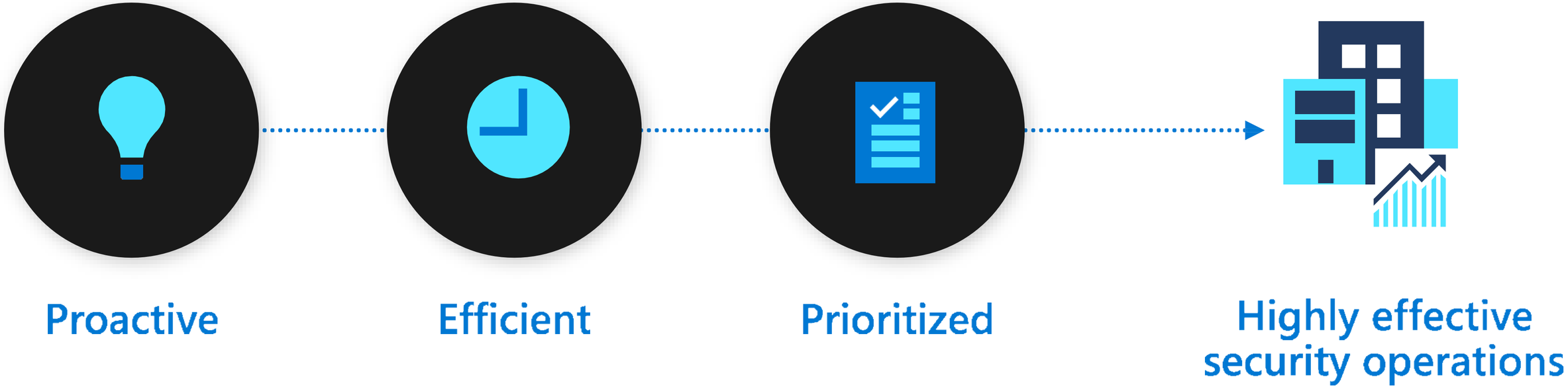
Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

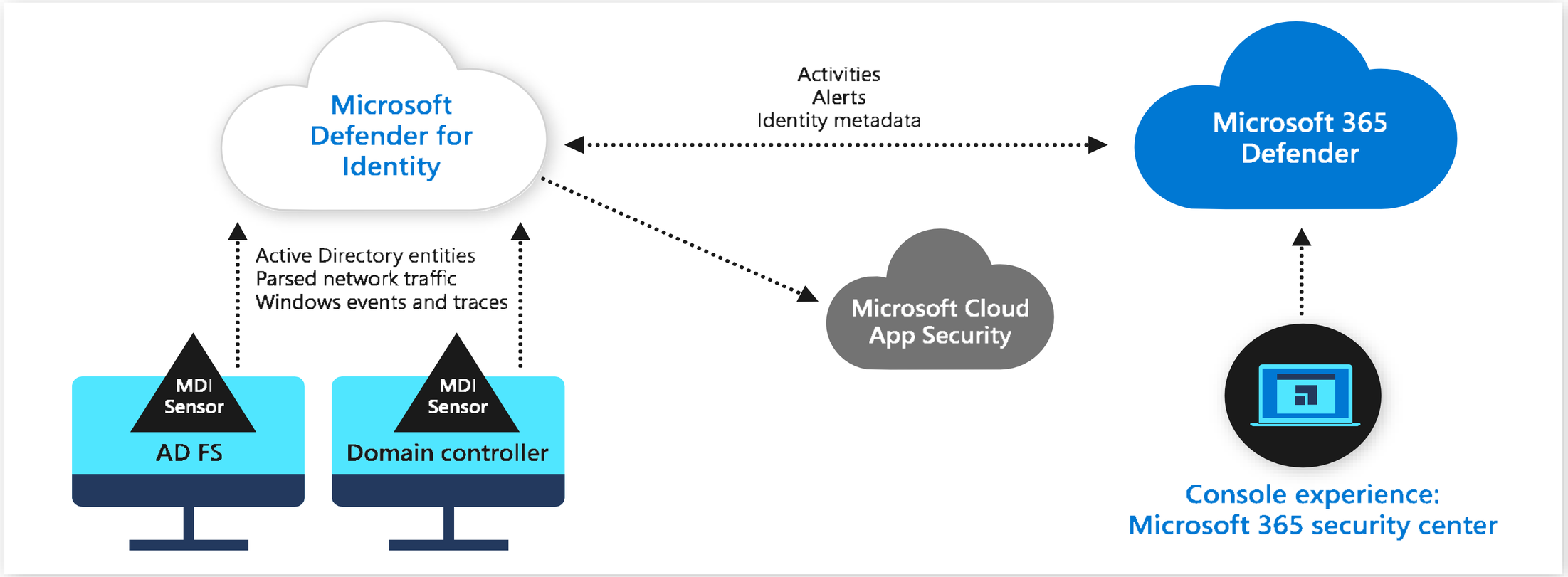
# Microsoft Defender for Identity: la chiave per potenziare la difesa

Supporting and enabling enterprise security operations



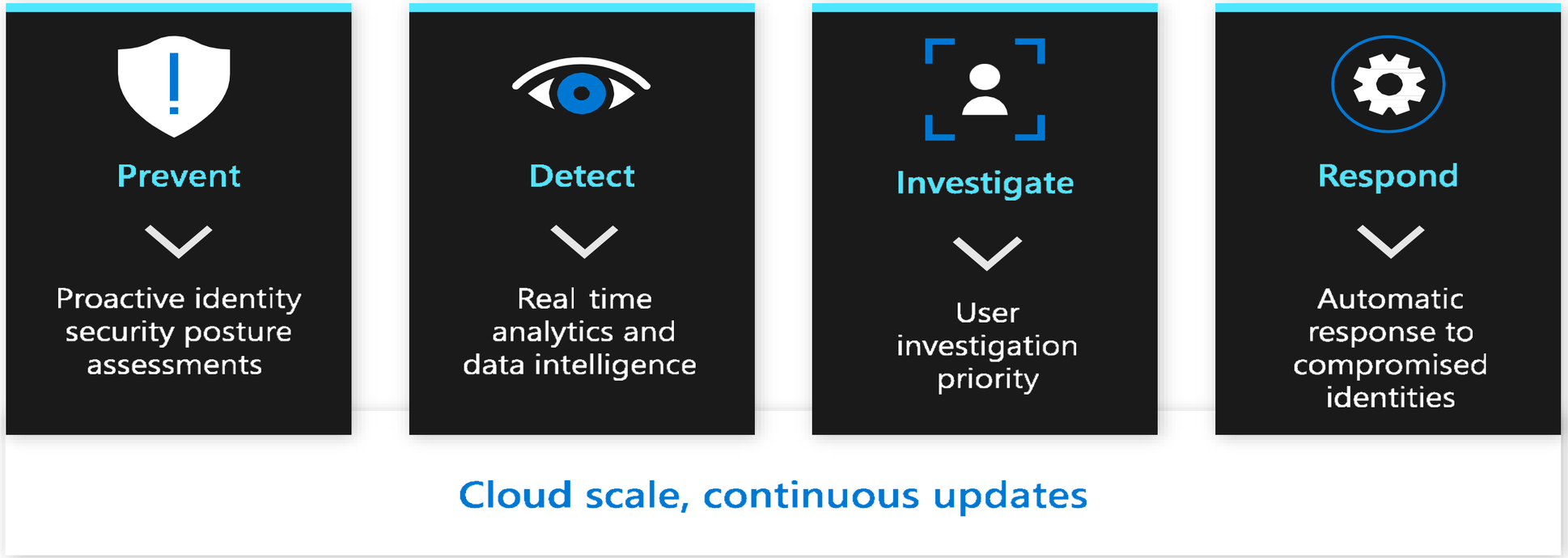
# Architettura di Microsoft Defender per identità Microsoft Defender for Identity architecture

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



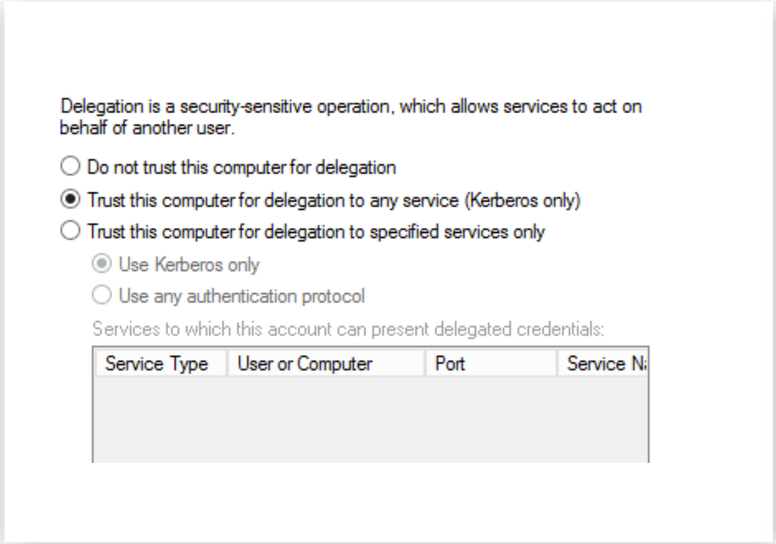
MICROSOFT DEFENDER FOR IDENTITY

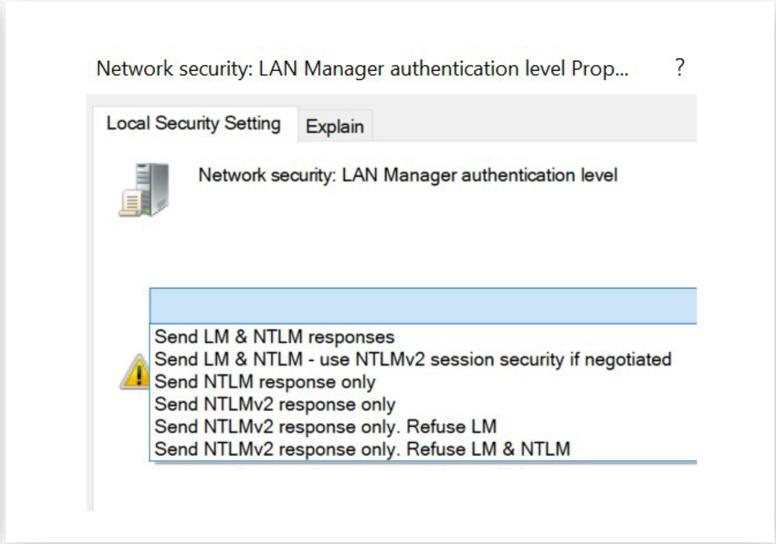
# Prevent

# Attack surface reduction

Prevent

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


## Clear text authentication

Exposed passwords

## Unconstrained delegation rights

Rogue impersonation

## Legacy authentication in use

Easier to attack

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

RESOLVE

# 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

Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

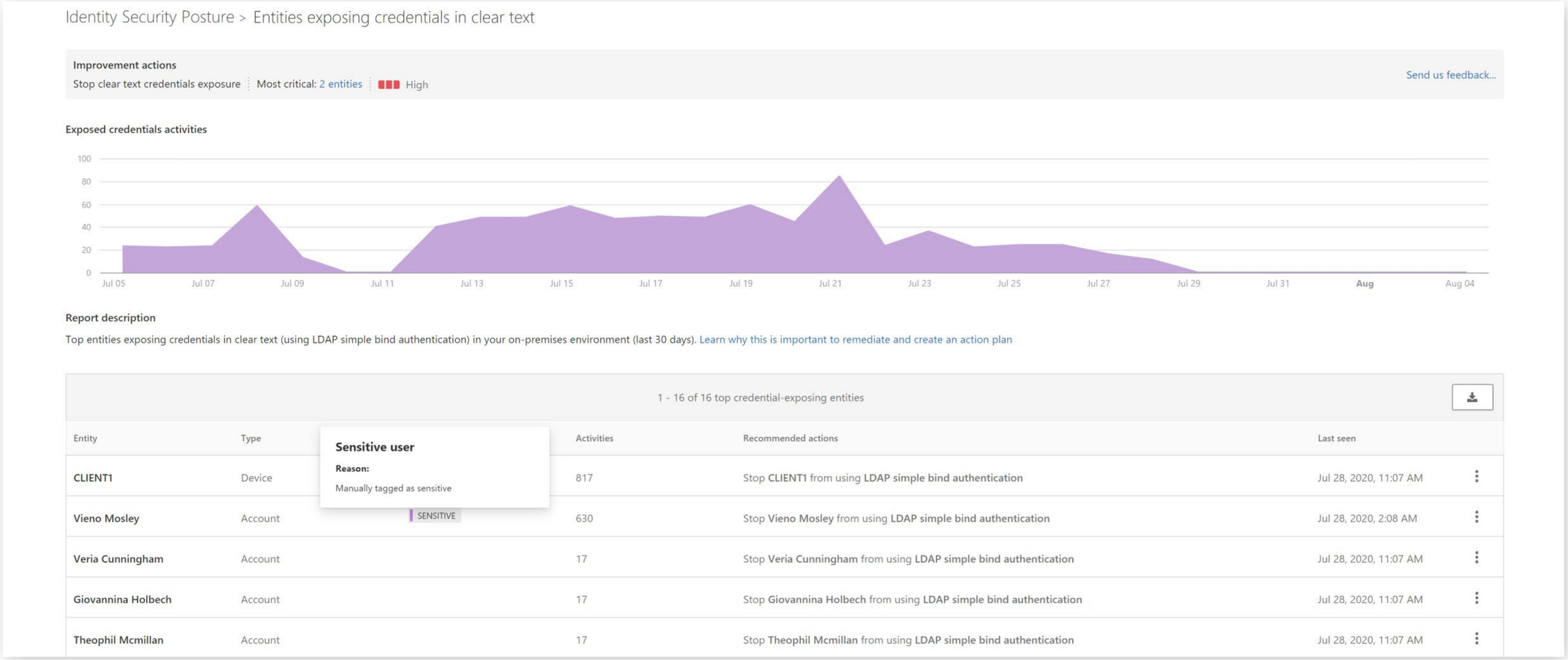
Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

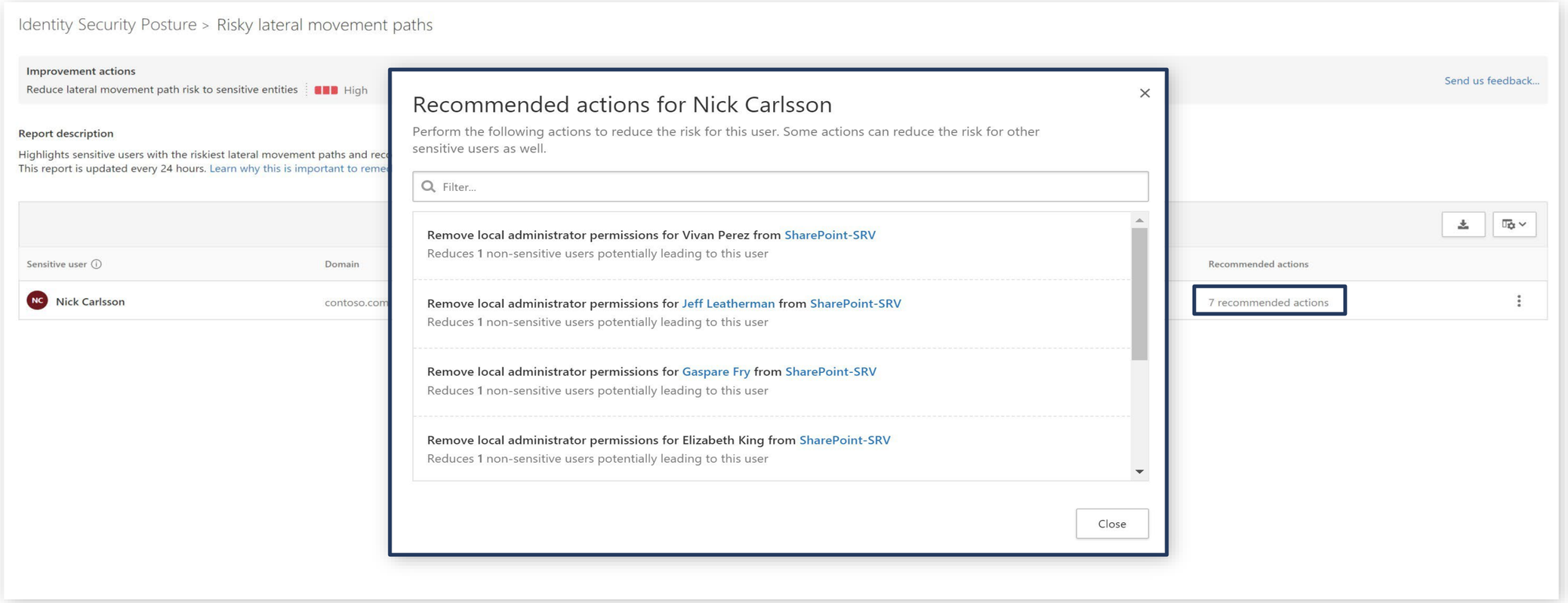
RESOLVE

# View top entities that are exposing credentials in clear text



# Percorsi di movimento laterale rischiosi

## View top sensitive accounts that carry lateral movement risk




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

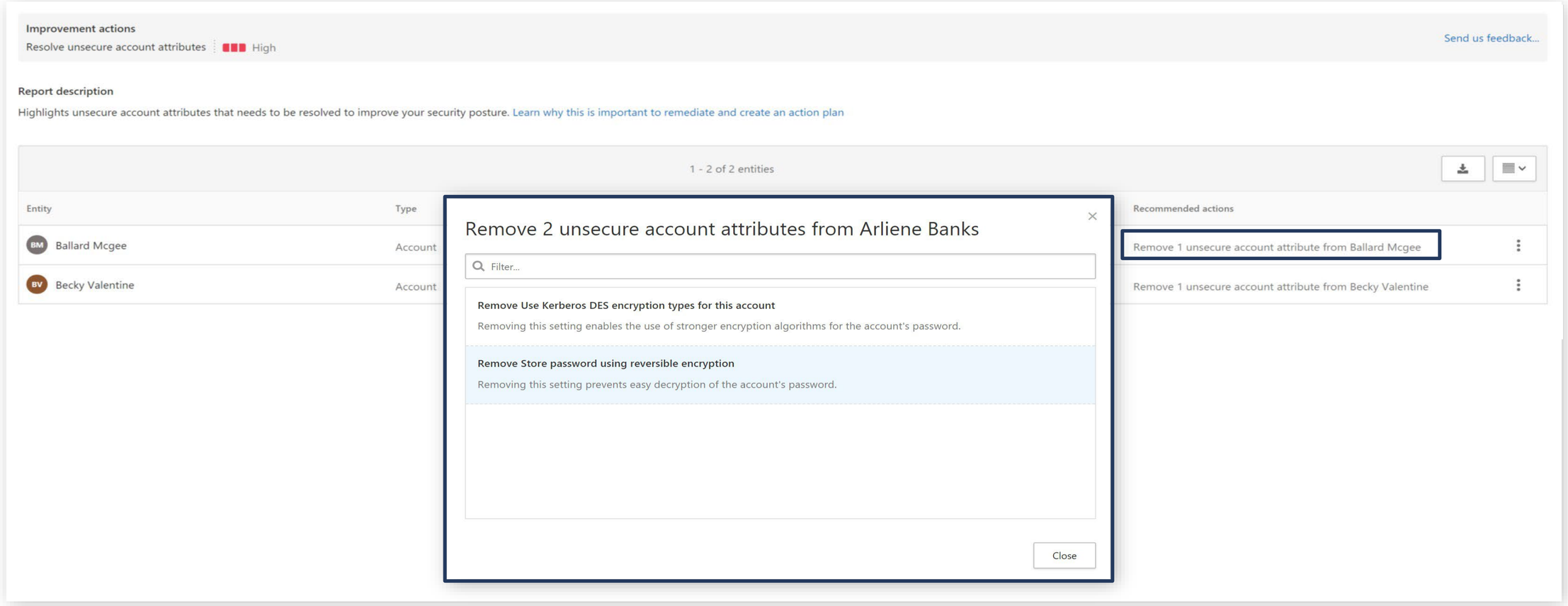
Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

# Esposizione degli account inattivi/scaduti

## Discover inactive and expired accounts in sensitive groups




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

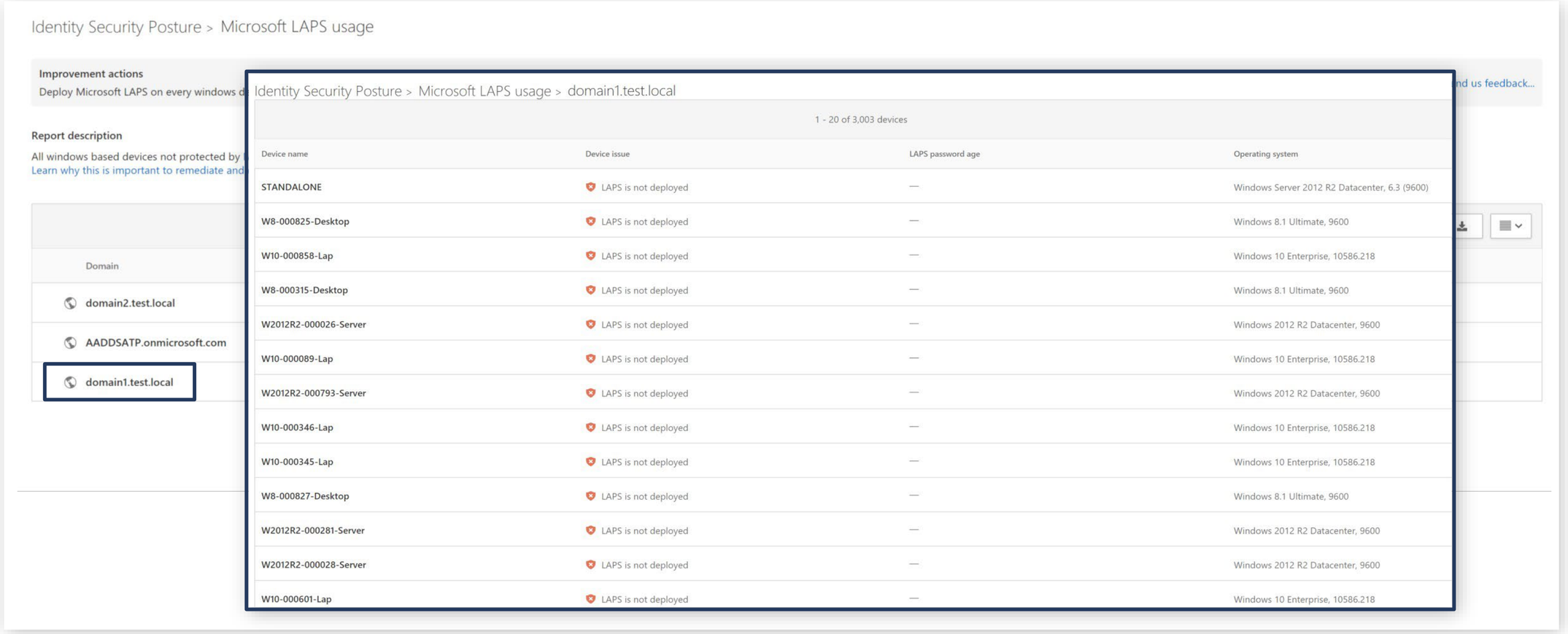
Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

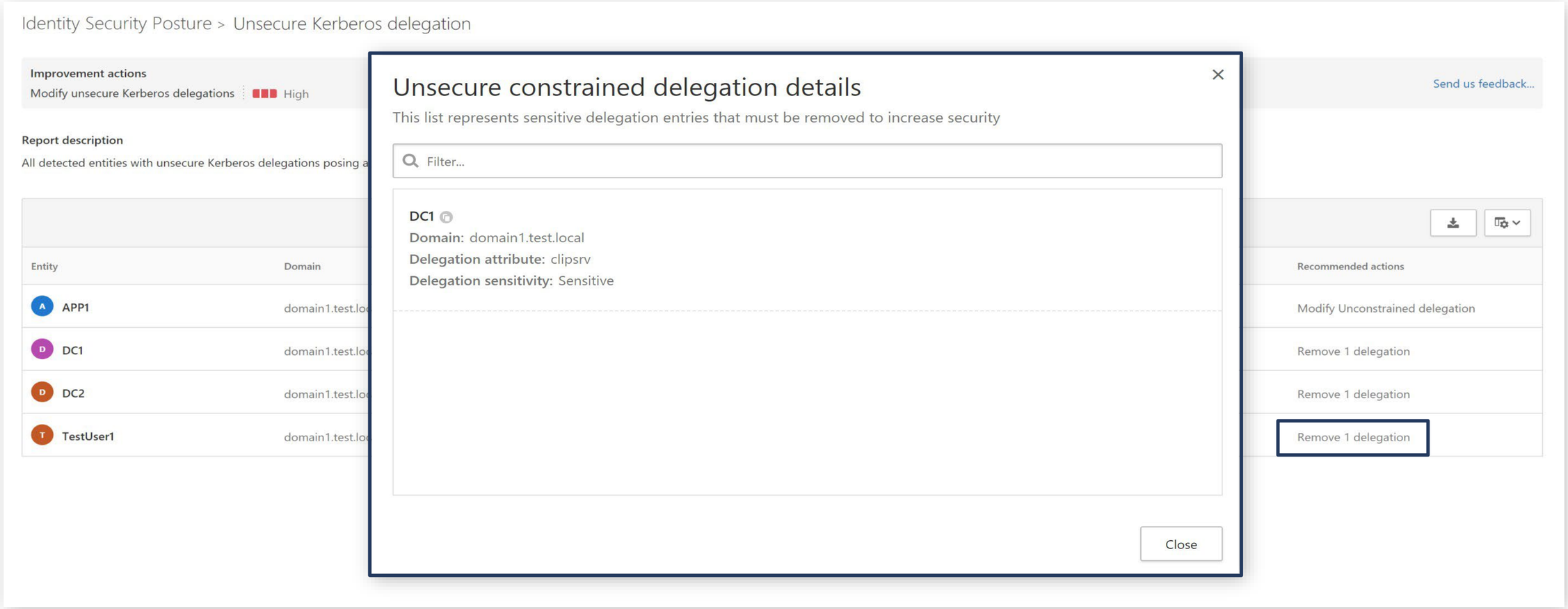
# Utilizzo di Microsoft LAPS

## Highlight which devices don’t use Local Administrator Password Solution



# Delega Kerberos non sicura

For apps that request end user access credentials to access resources




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

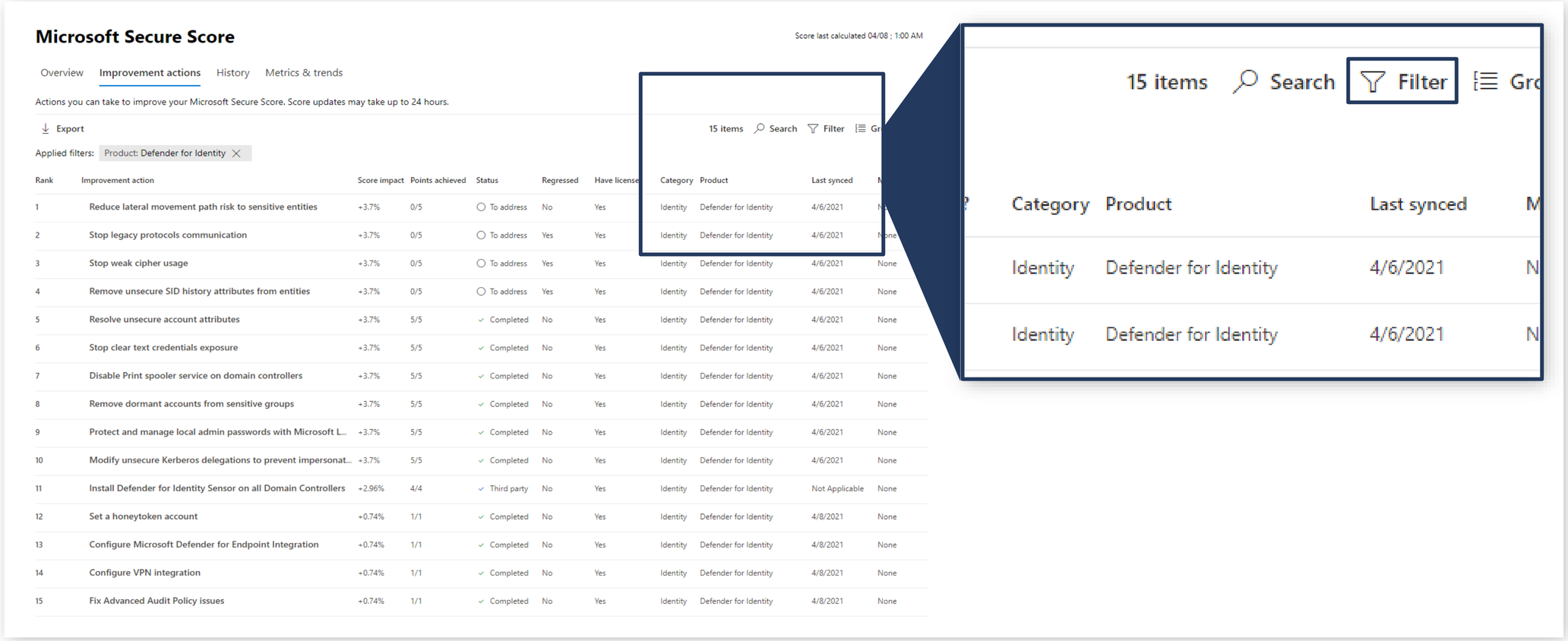
Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

# Tenere traccia dei progressi in Secure Score

## Assessments can be found under improvement actions



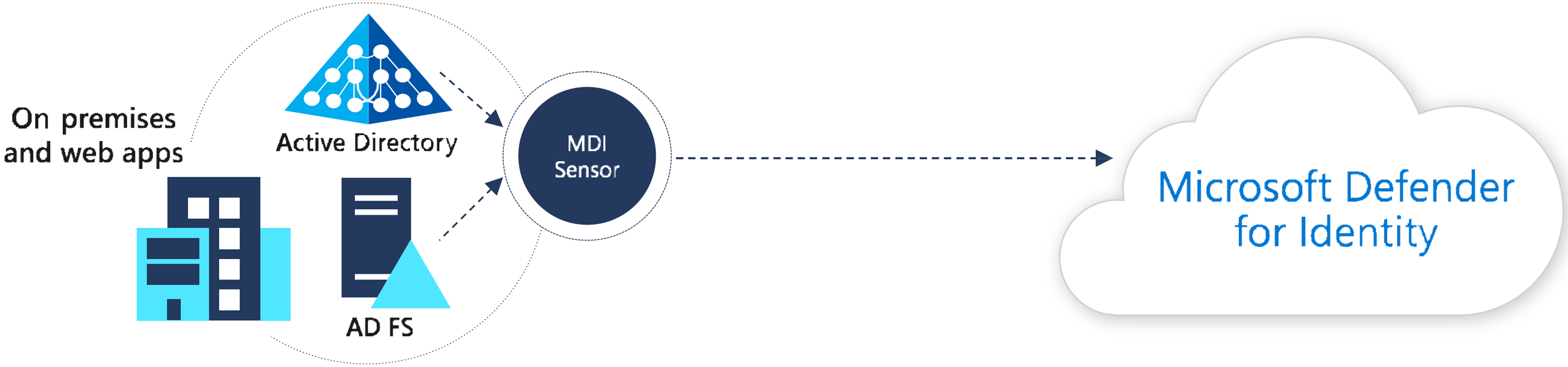
MICROSOFT DEFENDER FOR IDENTITY

# 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

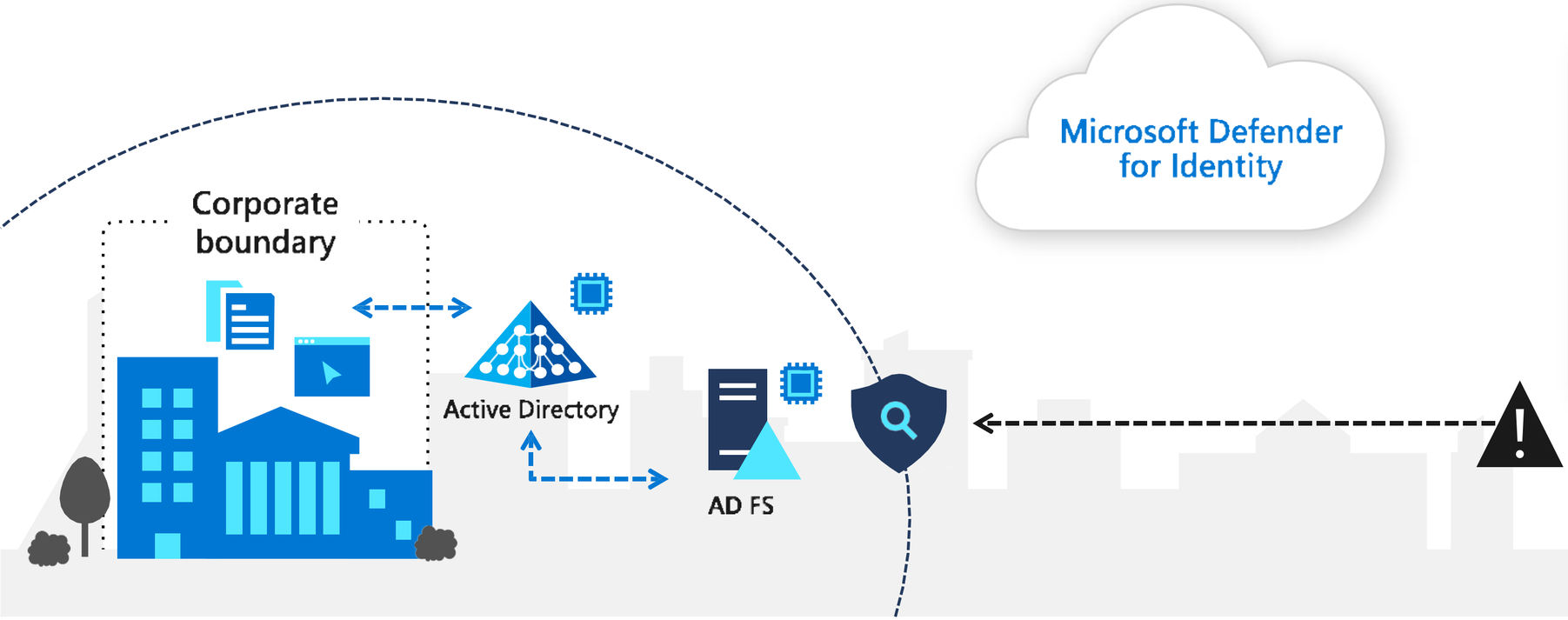
Data enrichment and correlation in the cloud, for real time detections

# Estensione del supporto ad ADFS

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

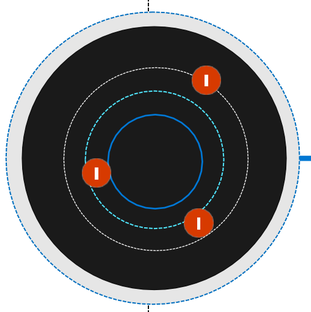
The Defender for Identity sensor now supports AD FS servers, extending advanced identity protection

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




Explore the impact of introducing an AD FS sensor as part of Defender for Identity's capabilities against on premise credential compromise like Nobelium

# 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)

Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

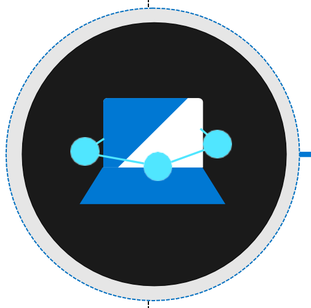
Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

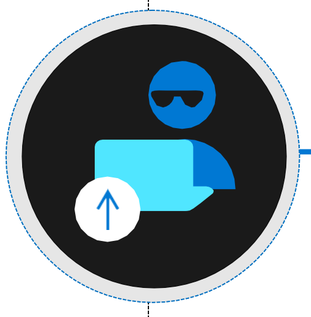
RESOLVE

# Funzionalità di rilevamento



## Lateral movement

- NTLM Relay and NTLM tampering
- Pass the Ticket
- Pass the Hash
- Overpass the Hash
- Suspicious groups membership changes
- Suspicious SID history injection
- Suspected Pass the Certificate
- Suspicious rogue certificate



## Persistence

- Golden Ticket attack
- DCShadow, DCSync
- Data exfiltration
- Code execution/service creation on DC & AD FS
- SMB packet manipulation
- Skeleton key
- Golden Ticket leveraging RBCD
- Suspicious print spooler registration
- DNS Remote code execution attempt (CV 2020 1305)
- ★ AD FS Dump activity

Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

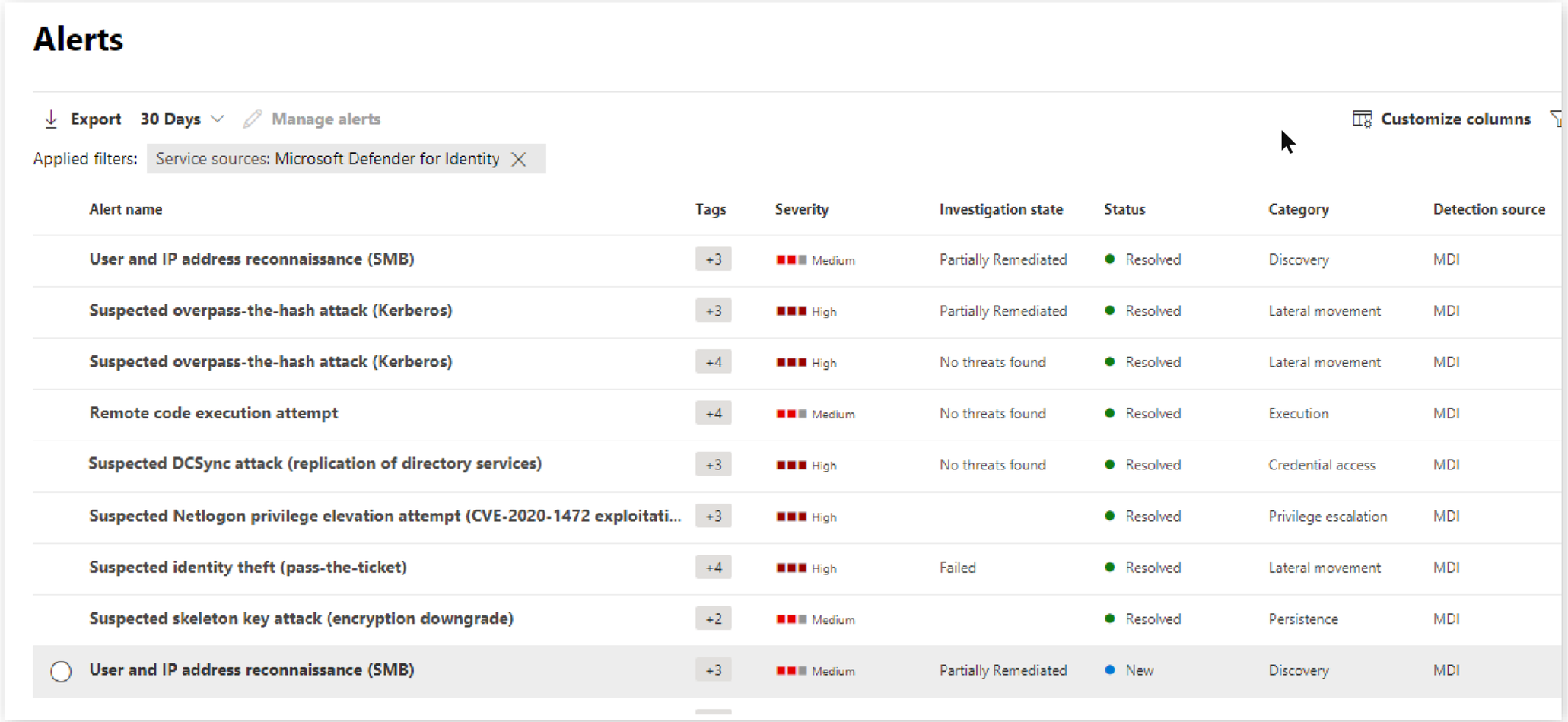
Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

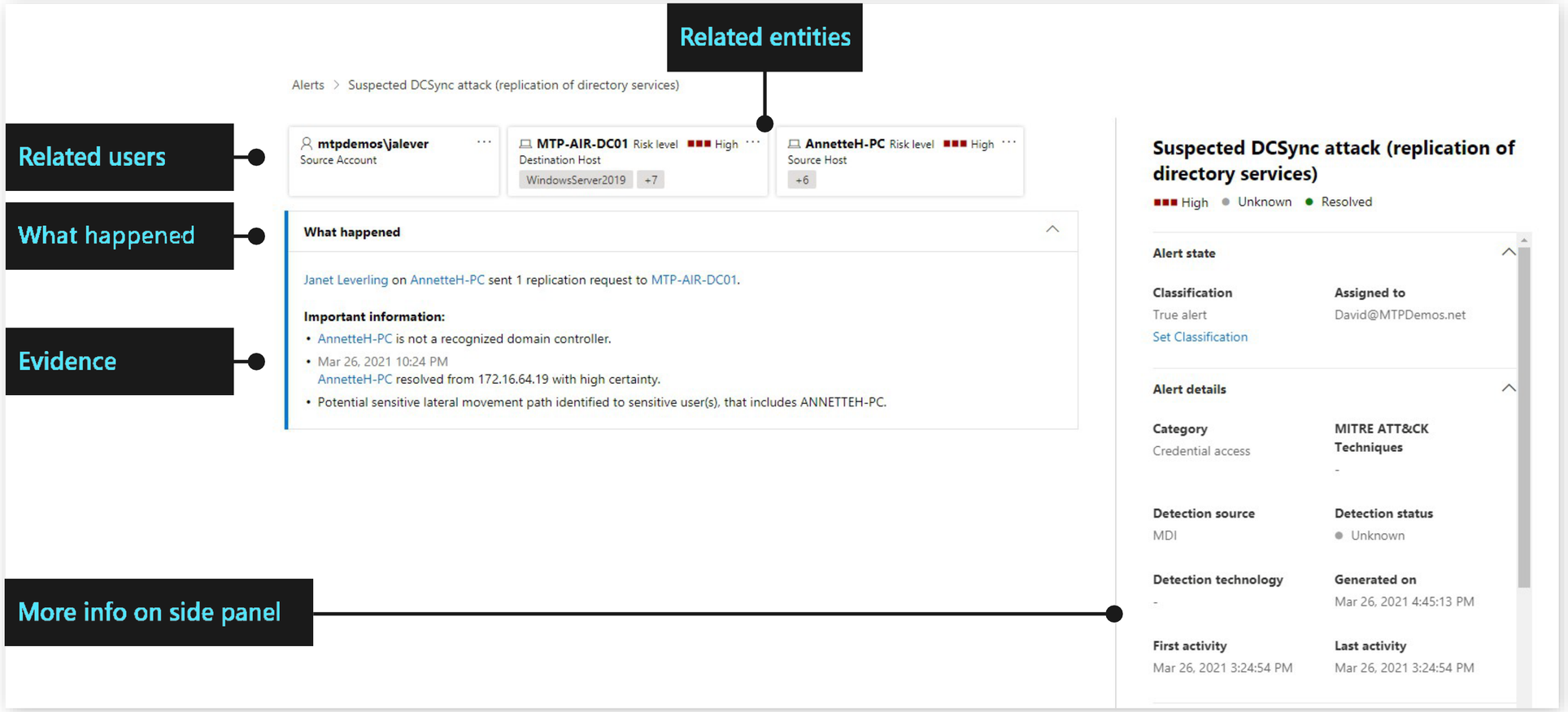
RESOLVE

# Panoramica degli avvisi di rilevamento




| 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



# Ampiezza di rilevamento: attività sospette e analisi del comportamento


High confidence suspicious activities representing attacks


User behavior anomalies, represent low fidelity signals

Maggiore visibilità

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

RESOLVE

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

Defender for Identity

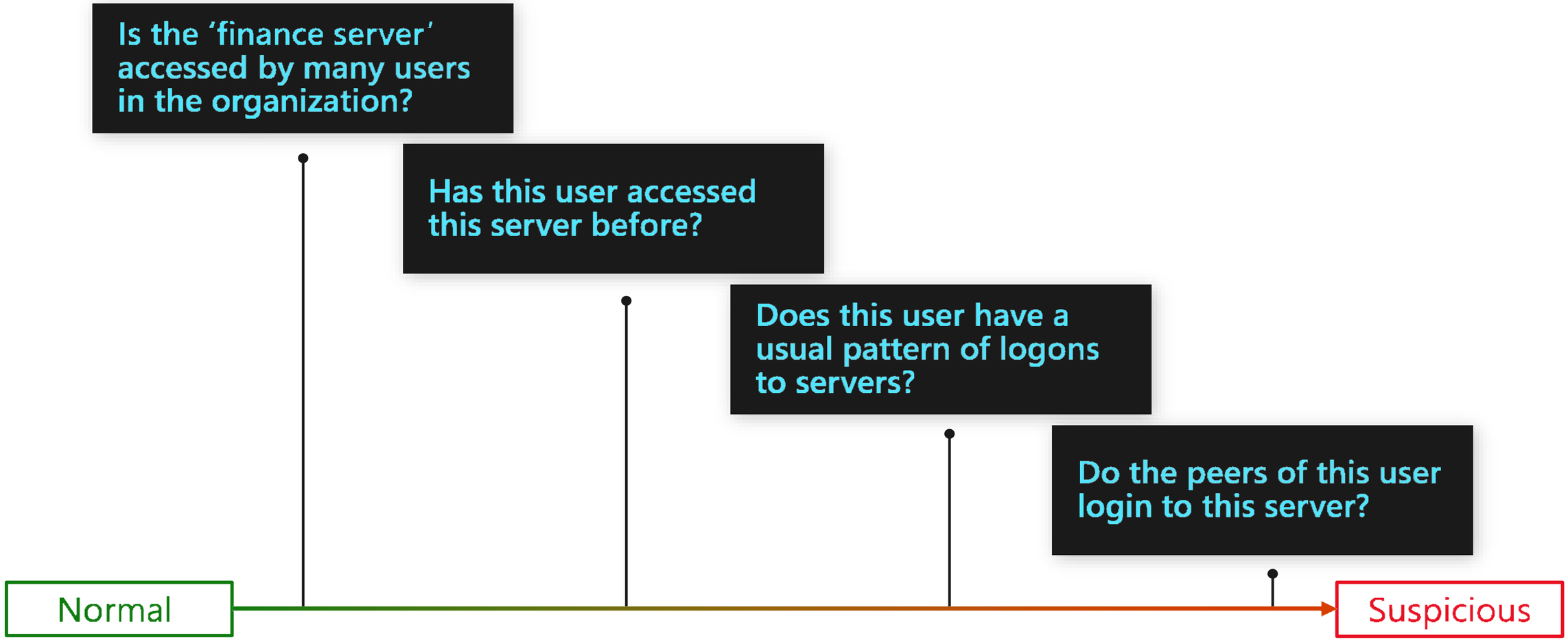
- Interactive login to device
- Access to on premises resources
- Remote connections to servers
- Failed logins behavior
- Code execution on domain controller

Microsoft Cloud App Security

- Access to cloud apps
- Usage of SharePoint Online sites
- User agent, location & ISP analytics
- Mailbox behavior

# Processo di analisi delle attività sospette

Example: User accesses the ‘finance’ server



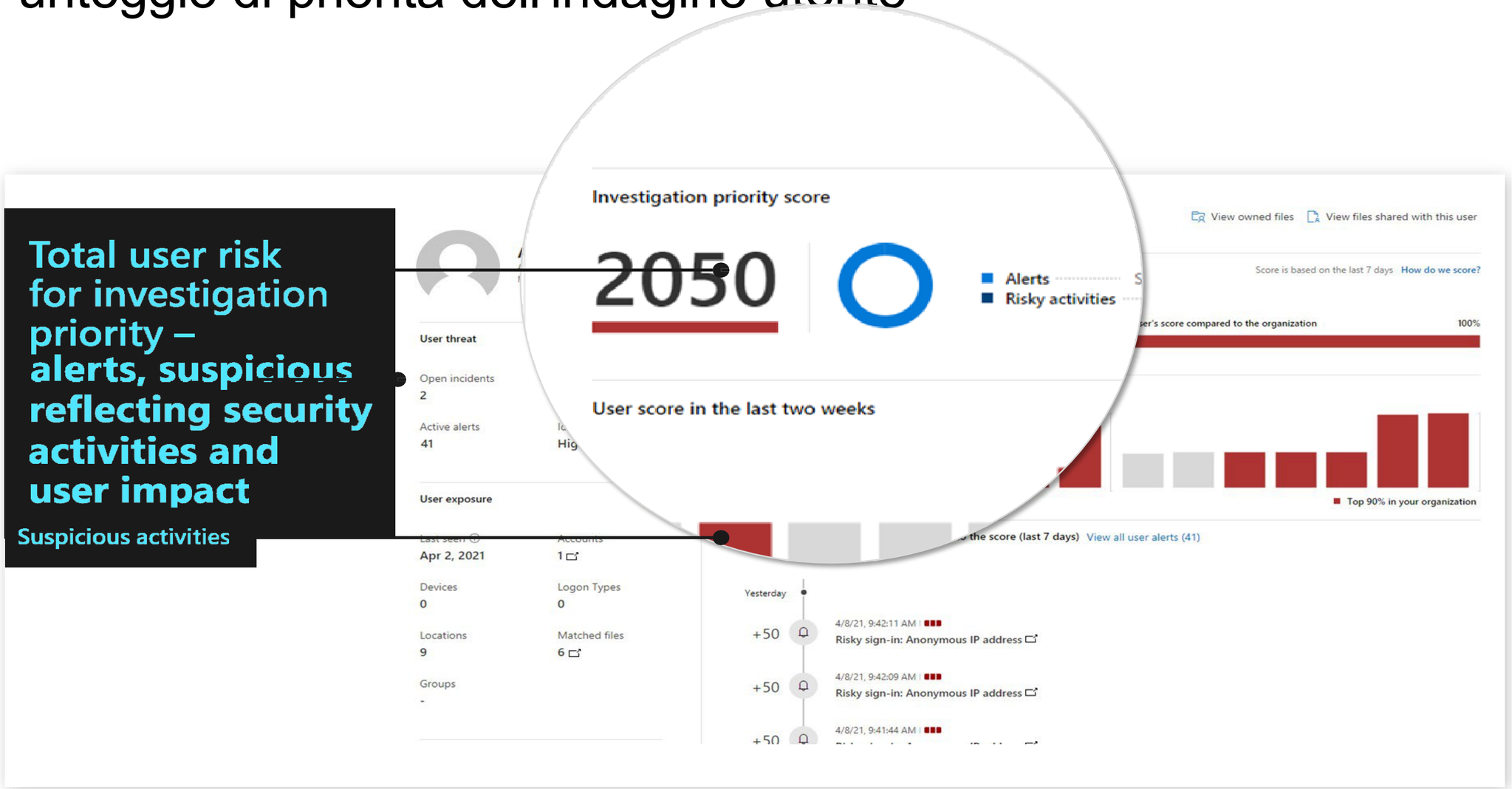
MICROSOFT DEFENDER FOR IDENTITY

# Investigate

# User investigation priority scoring

Investigate

# Punteggio di priorità dell'indagine utente




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

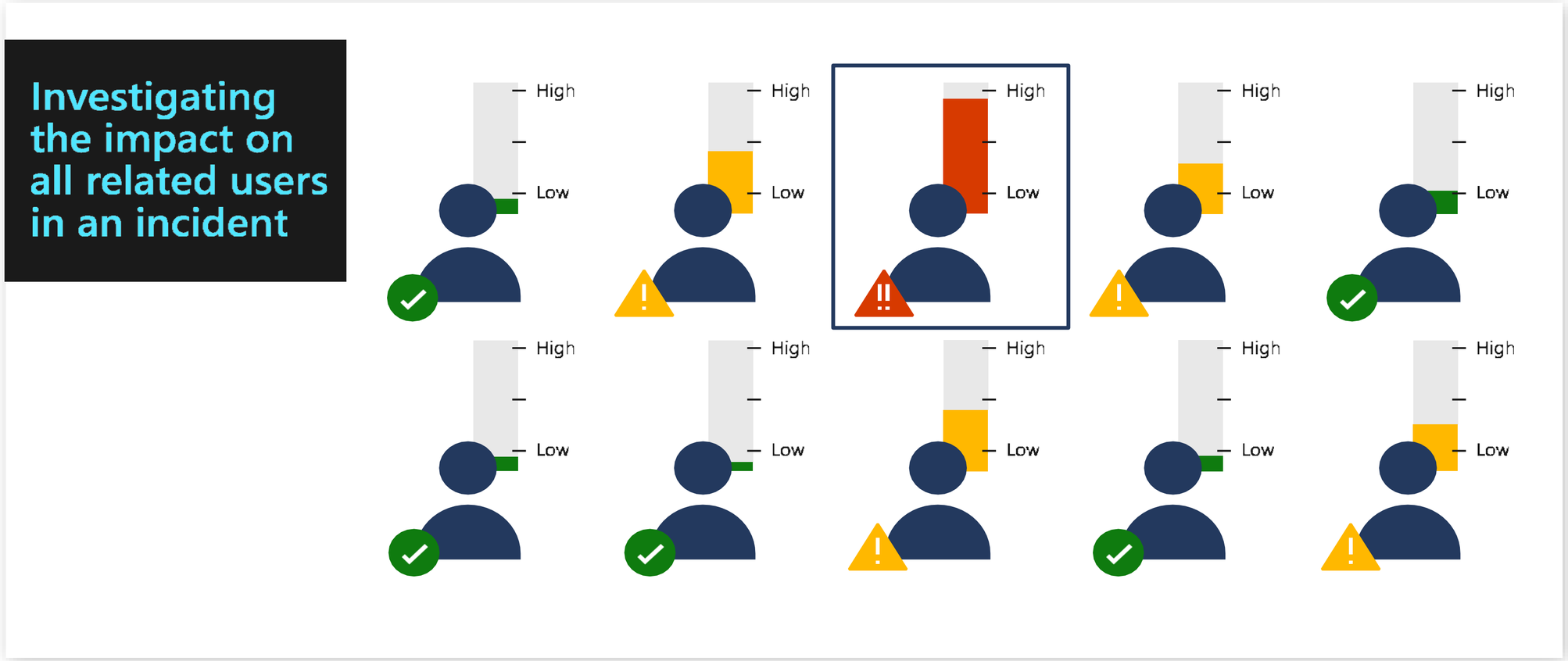
Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

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

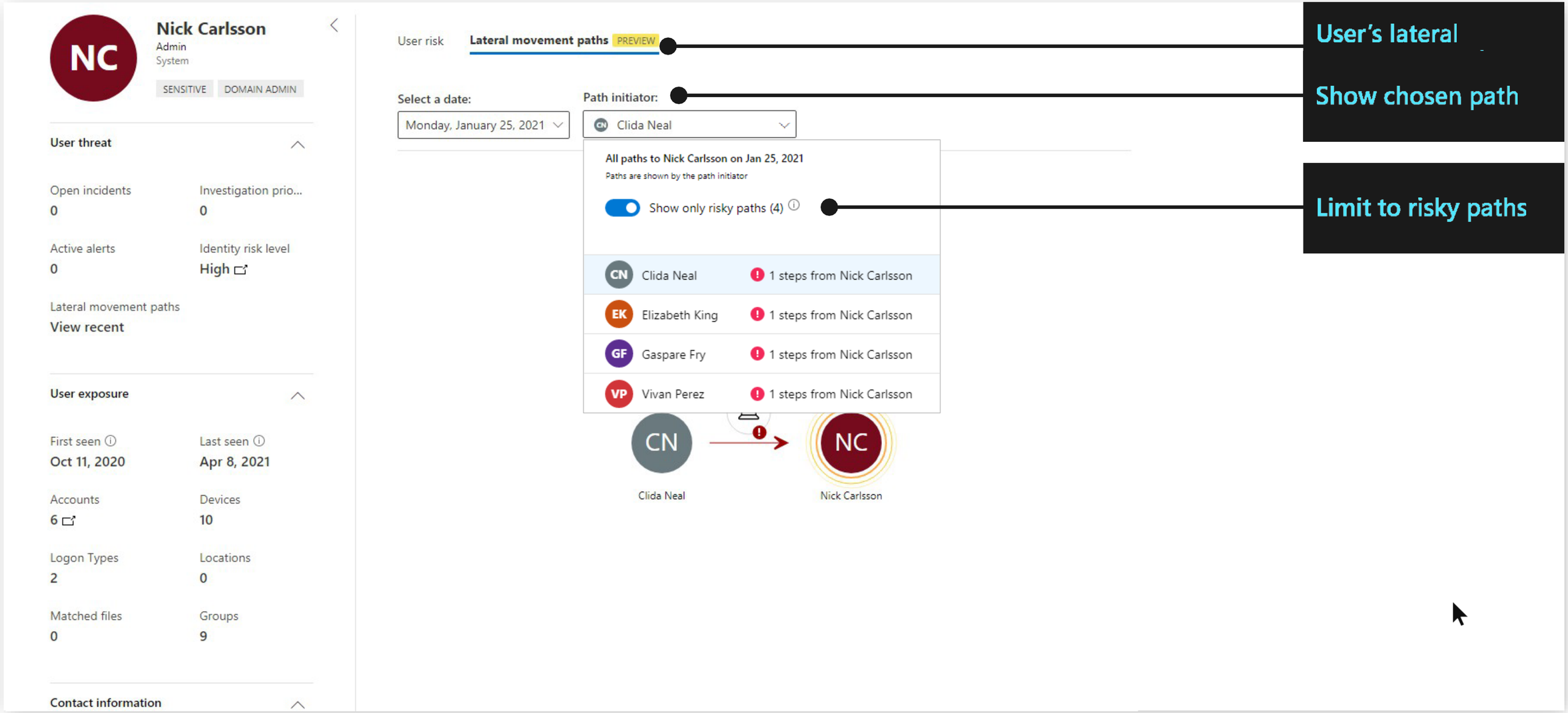


# Classificazione delle indagini sugli utenti

**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




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

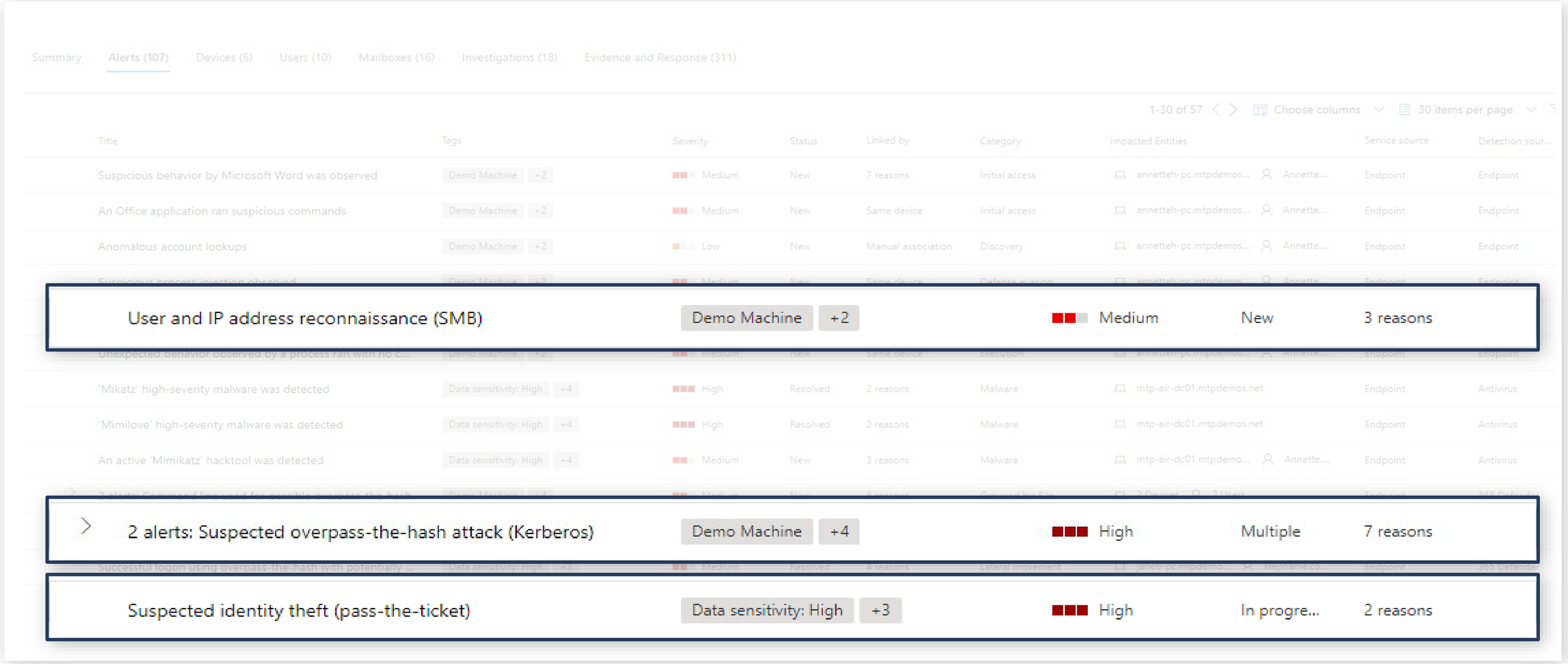
Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

# Eventi imprevisti di Microsoft 365 Defender




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

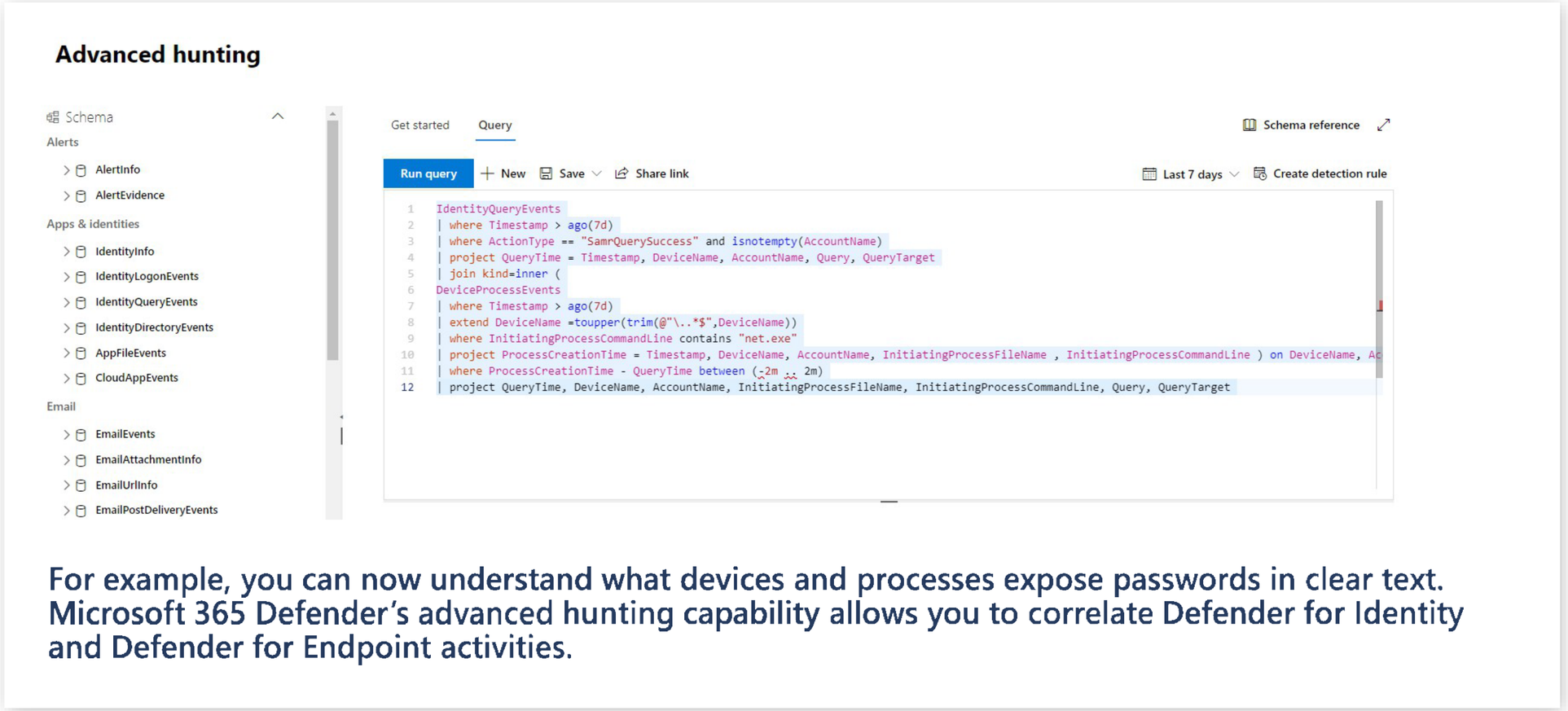
Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

# Caccia avanzata in Microsoft 365 Defender




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.

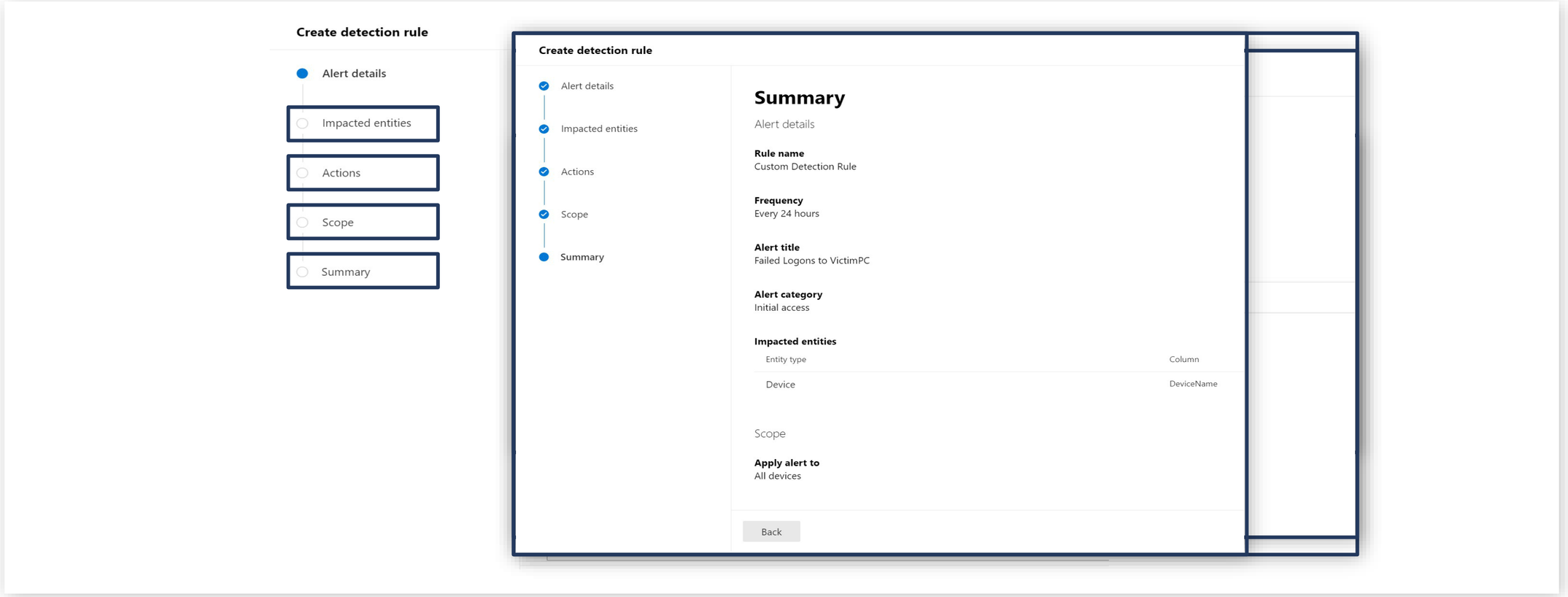
# Caccia avanzata in Microsoft 365 Defender

**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




Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

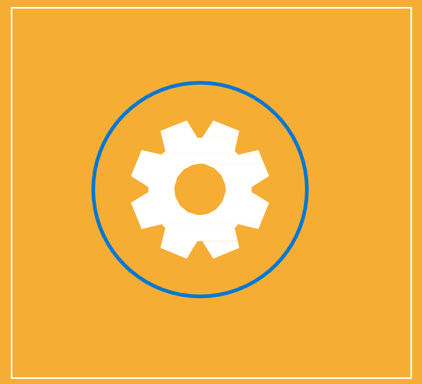
Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

RESOLVE

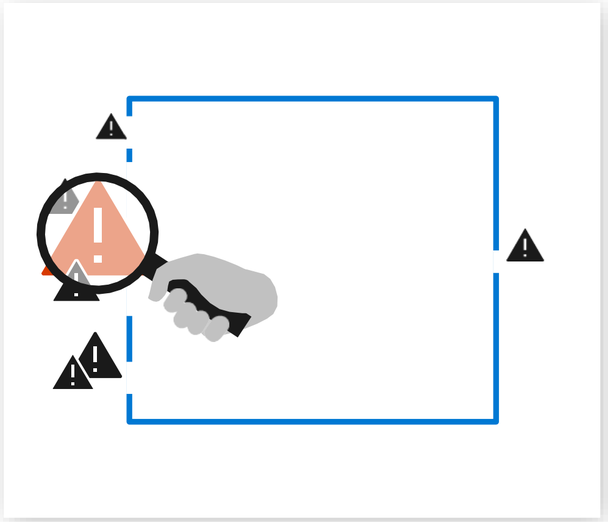
MICROSOFT DEFENDER FOR IDENTITY

# Respond
# Automated security workflows

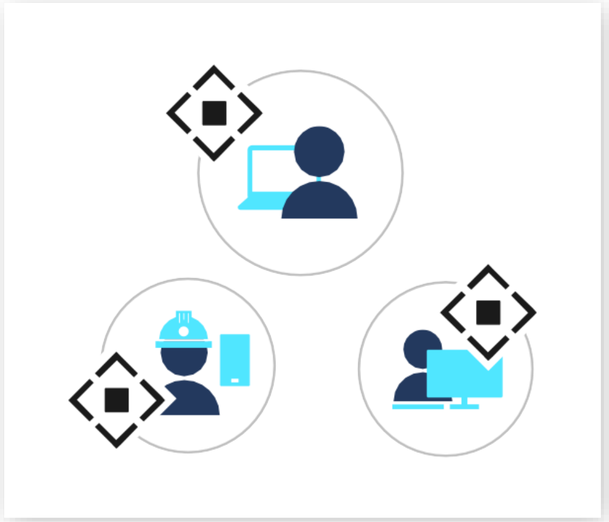


Respond

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



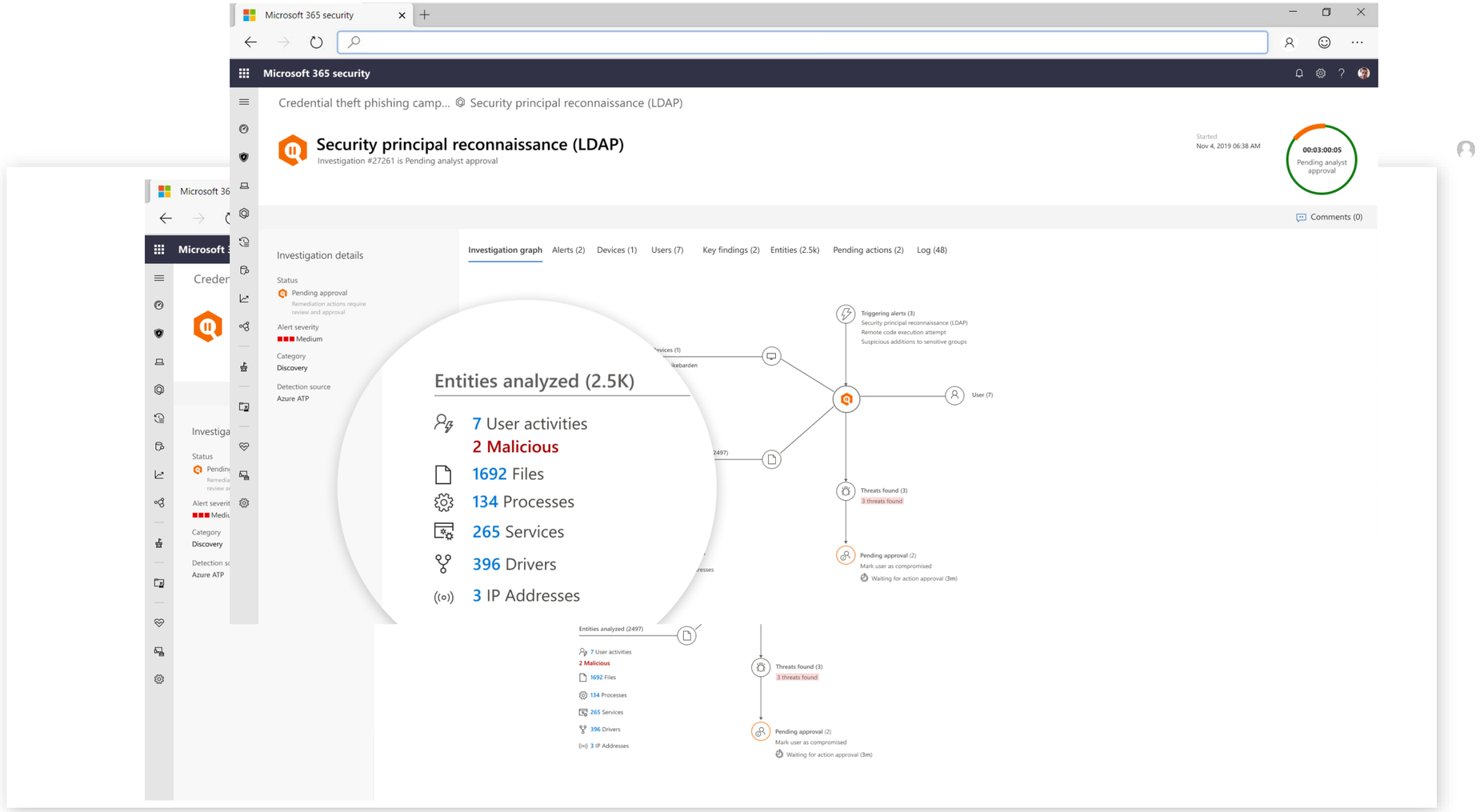
It’s easy to miss risky configurations…



Threats can originate anywhere…

Activity volume makes prioritization difficult…

# Risposta automatizzata agli eventi imprevisti di Microsoft 365 Defender




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

RESOLVE

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

RESOLVE

# / 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

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

RESOLVE

# / 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**

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

RESOLVE

## 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


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

RESOLVE

RESOLVE

by ErgonGroup