

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

A woman with long dark hair and glasses is shown in profile, looking at a laptop screen. She is wearing a light-colored button-down shirt. The background is a blurred cityscape at night with colorful bokeh lights in shades of blue, orange, and white. The text is overlaid on the right side of the image.

EMPOWERING DEFENDER E PURVIEW MASTERCLASS

mar 11.03 | 14:30-16:00

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.**



RESOL/E

/ AGENDA

1

MICROSOFT DEFENDER

- *Panoramica criteri per la protezione della posta elettronica*
- *Gestione regole di rilevamento delle minacce*
- *Protezione web e criteri di esclusione*

2

MICROSOFT PURVIEW

- *eDiscovery: cercare ed esportare contenuti*
- *Gestione del ciclo vita dei dati*

3

Q&A LIVE

Ognuna di queste licenze consente di accedere alle funzionalità di Microsoft Defender XDR tramite il portale di Microsoft Defender senza costi aggiuntivi:

- Microsoft 365 E5 o A5
- Microsoft 365 E3 con il componente aggiuntivo Microsoft 365 E5 Security
- Microsoft 365 E3 con il componente aggiuntivo Enterprise Mobility + Security E5
- Microsoft 365 A3 con il componente aggiuntivo sicurezza Microsoft 365 A5
- Windows 10 Enterprise E5 o A5
- Windows 11 Enterprise E5 o A5
- Enterprise Mobility + Security (EMS) E5 o A5
- Office 365 E5 o A5
- Microsoft Defender per endpoint
- Microsoft Defender per la protezione IoT - Enterprise IoT (include la protezione per i dispositivi IoT aziendali con la licenza Microsoft 365 E5 (ME5) o E5 Security)
- Microsoft Defender per identità
- Microsoft Defender for Cloud Apps o Cloud App Discovery
- Microsoft Defender per Office 365 (piano 2)
- Microsoft 365 Business Premium
- Microsoft Defender for Business

/ LICENZE DISPONIBILI PER I VARI SERVIZI

Per utilizzare i vari prodotti di Microsoft Defender, sono necessarie diverse licenze.



Microsoft Defender for Endpoint

Microsoft Defender for Endpoint Plan 1: Disponibile come licenza standalone o come parte di altri piani Microsoft 365

.

Microsoft Defender for Endpoint Plan 2: Include funzionalità avanzate di rilevamento e risposta

/ LICENZE DISPONIBILI PER I VARI SERVIZI

Per utilizzare i vari prodotti di Microsoft Defender, sono necessarie diverse licenze.



Microsoft Defender for Office 365

Microsoft Defender for Office 365 Plan 1: Protezione di base per email e collaborazione

Microsoft Defender for Office 365 Plan 2: Include funzionalità avanzate di protezione e gestione delle minacce

/ LICENZE DISPONIBILI PER I VARI SERVIZI

Per utilizzare i vari prodotti di Microsoft Defender, sono necessarie diverse licenze.



Microsoft Defender for Cloud Apps

Protezione per le applicazioni cloud, disponibile come licenza standalone o come parte di altri piani Microsoft 365



Microsoft Defender for Cloud

Protezione per le applicazioni cloud, disponibile come licenza standalone o come parte di altri piani Microsoft 365

/ LICENZE DISPONIBILI PER I VARI SERVIZI

Per utilizzare i vari prodotti di Microsoft Defender, sono necessarie diverse licenze.



Microsoft Defender for Cloud Apps

Protezione per le applicazioni cloud, disponibile come licenza standalone o come parte di altri piani Microsoft 365



Microsoft Defender for Identity

Richiede una licenza standalone o può essere incluso in piani come Microsoft 365 E5

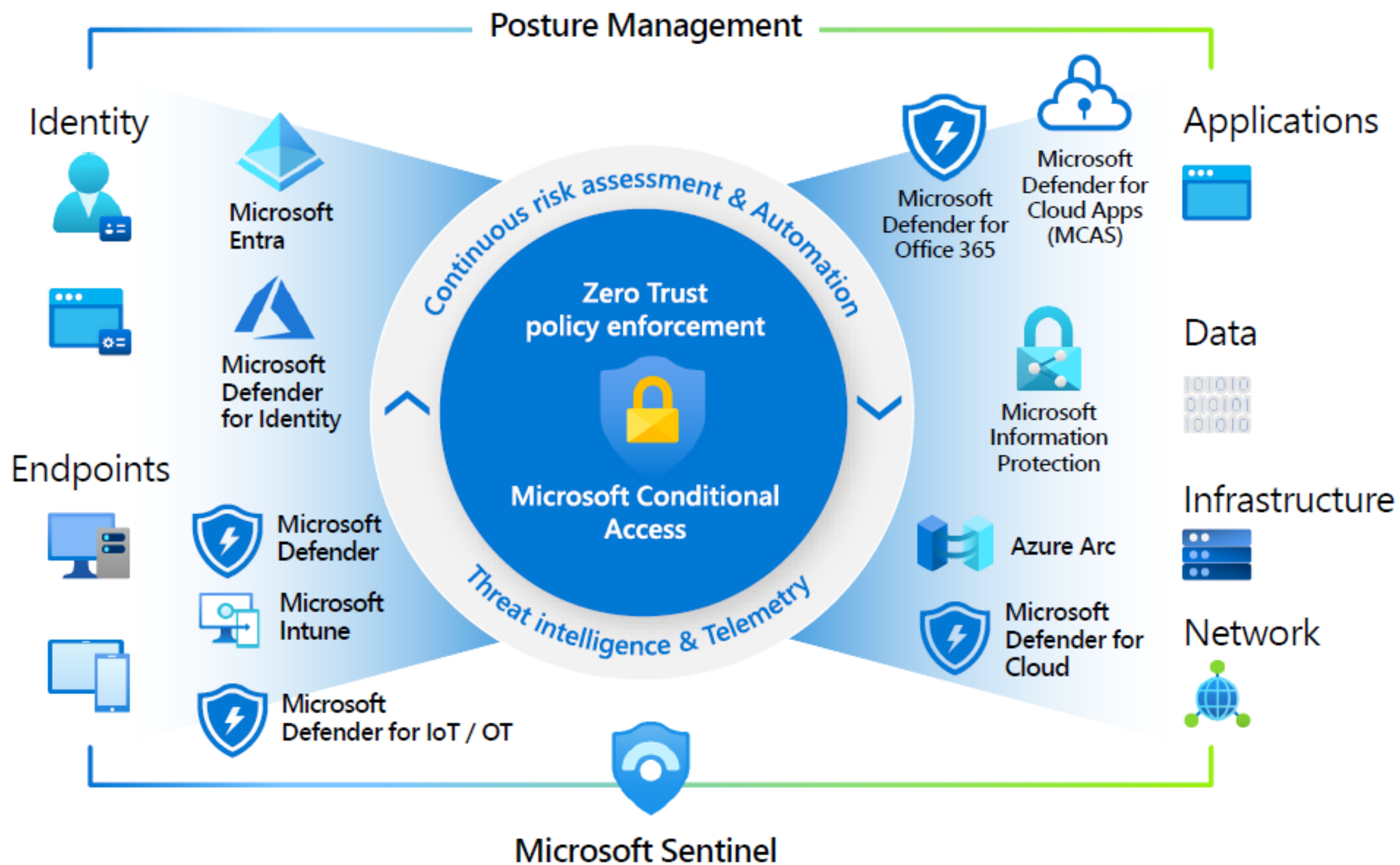
/ LA TECNOLOGIA MICROSOFT A SUPPORTO DELLA NIS2

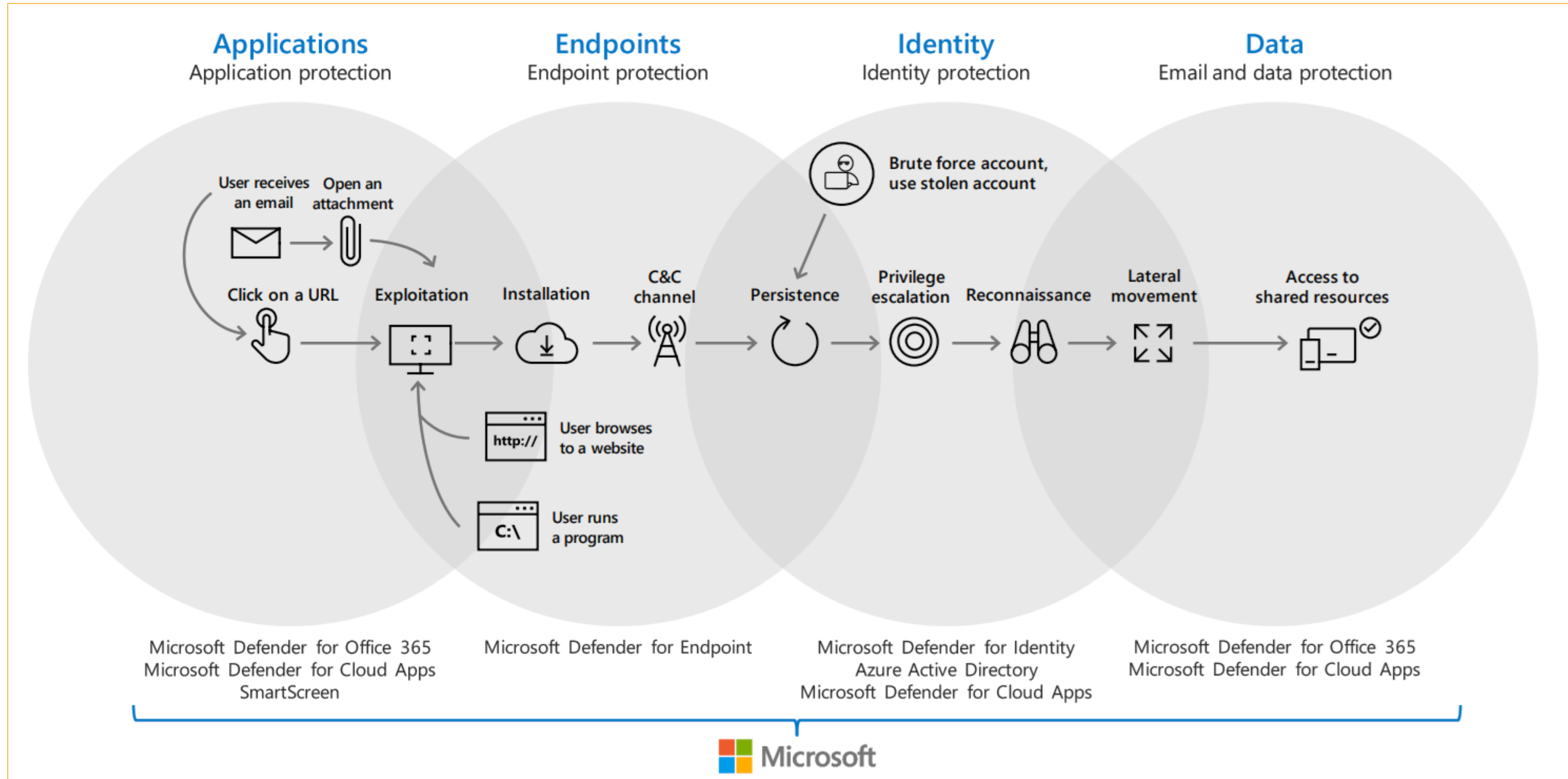
La nostra soluzione tecnologica:

Resolve è MS Partner Tier 1 di Microsoft ed adotta le sue avanzate soluzioni tecnologiche in quanto:

- affidabili
- facilmente accessibili
- complete

In questo modo possiamo garantire il massimo della sicurezza ed essere sempre aggiornati.





DEFENDER XDR



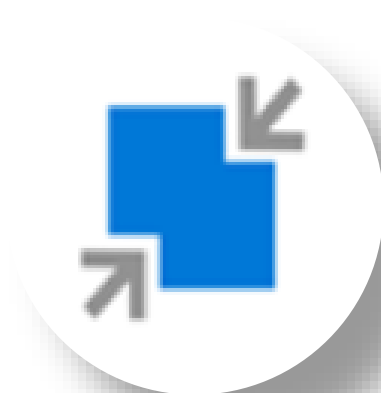


/ MICROSOFT DEFENDER PER ENDPOINT

Microsoft Defender per Endpoint è disponibile in due piani, Defender per Endpoint Piano 1 e Piano 2. Per il Piano 2 è ora disponibile un nuovo componente aggiuntivo di Gestione delle vulnerabilità di Microsoft Defender.



**Gestione
delle
vulnerabilità
di Microsoft
Defender**



**Riduzione
superficie
d'attacco**



**Protezione
di nuova
generazione**



**Rilevamento
e reazione
dagli
endpoint**



**Indagine e
correzione
automatizzate**



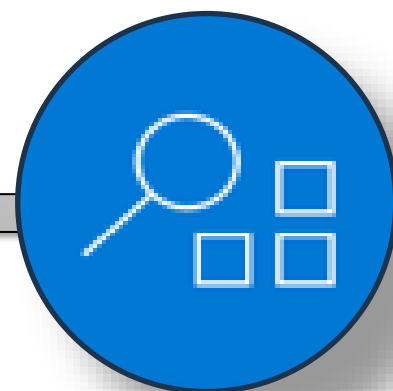
**Microsoft
Threat
Experts**

Amministrazione e configurazione centralizzate, API

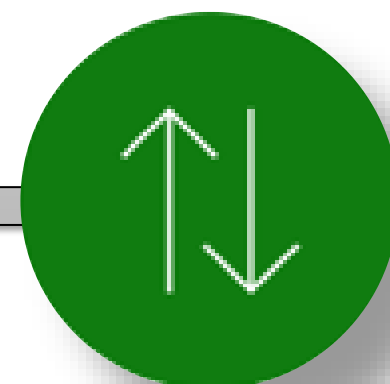


Gestione delle vulnerabilità di Microsoft Defender

Ridurre il rischio cibernetico con l'individuazione delle vulnerabilità,
la definizione delle priorità in base al rischio e la correzione.



Individuazione e monitoraggi
continui



Definizione delle priorità
Intelligente basata sui rischi



Correzione e traccia

/ GESTIONE DELLE VULNERABILITÀ DI MICROSOFT DEFENDER

La riduzione del rischio informatico richiede una gestione completa delle vulnerabilità basata sui rischi per identificare, valutare, correggere e tenere traccia di tutte le vulnerabilità più importanti tra gli asset più critici, il tutto in un'unica soluzione.

La gestione delle vulnerabilità di Defender offre visibilità delle risorse, valutazioni intelligenti e strumenti di correzione integrati per Windows, macOS, Linux, Android, iOS e dispositivi di rete. L'uso di Intelligence per le minacce Microsoft, le stime della probabilità di violazione, i contesti aziendali e le valutazioni dei dispositivi Gestione delle vulnerabilità di Defender assegna priorità in modo rapido e continuo alle principali vulnerabilità degli asset più critici e fornisce raccomandazioni sulla sicurezza per attenuare i rischi.

/ RIDUZIONE SUPERFICIE D'ATTACCO

La superficie di attacco dell'organizzazione include tutte le posizioni in cui un utente malintenzionato potrebbe compromettere i dispositivi o le reti dell'organizzazione.

Ridurre la superficie di attacco significa proteggere i dispositivi e la rete dell'organizzazione, lasciando agli utenti malintenzionati un minor numero di modi per eseguire gli attacchi.

La configurazione delle regole di riduzione della superficie di attacco in Microsoft Defender per endpoint può essere utile.

Le regole di riduzione della superficie di attacco sono destinate a determinati comportamenti software, ad esempio:

- Avvio di file eseguibili e script che tentano di scaricare o eseguire file
- Esecuzione di script offuscati o in altro modo sospetti
- Esecuzione di comportamenti che le app in genere non avviano durante il normale lavoro quotidiano

/ PROTEZIONE DI NUOVA GENERAZIONE

Microsoft Defender per endpoint include la protezione di nuova generazione per intercettare e bloccare tutti i tipi di minacce emergenti. La maggior parte del malware moderno è polimorfico, il che significa che muta costantemente per eludere il rilevamento. Non appena viene identificata una variante, ne prende il posto un'altra. Questa rapida evoluzione sottolinea la necessità di soluzioni di sicurezza agili e innovative.

Le protezioni di nuova generazione, ad esempio Microsoft Defender Antivirus, bloccano il malware usando modelli di Machine Learning locali e basati sul cloud, analisi del comportamento ed euristica. Microsoft Defender Antivirus usa tecnologie predittive, machine learning, scienza applicata e intelligenza artificiale per rilevare e bloccare il malware al primo segno di comportamento anomalo.

/ RILEVAMENTO E REAZIONE DAGLI ENDPOINT

Le funzionalità di rilevamento e risposta degli endpoint in Defender per endpoint offrono rilevamenti avanzati degli attacchi quasi in tempo reale e interattivi. I responsabili della sicurezza possono assegnare priorità agli avvisi in modo efficace, ottenere una visibilità completa su una violazione e adottare azioni di risposta per correggere le minacce.

Quando viene rilevata una minaccia, il sistema genera un avviso e un analista avvia le indagini. Gli avvisi che presentano tecniche di attacco simili o che possono essere attribuiti alla stessa persona vengono aggregati in un'entità chiamata *incidente*. L'aggregazione di avvisi consente di analizzare e rispondere in modo completo alle minacce.

/ INDAGINE E CORREZIONE AUTOMATIZZATE

La tecnologia nell'indagine automatizzata usa vari algoritmi di ispezione e si basa sui processi usati dagli analisti della sicurezza. Le funzionalità AIR sono progettate per esaminare gli avvisi e intervenire immediatamente per risolvere le violazioni. Le funzionalità AIR riducono significativamente il volume degli avvisi, consentendo alle operazioni di sicurezza di concentrarsi sulle minacce più sofisticate e altre iniziative ad alto valore.

Tutte le azioni correttive, siano esse in sospeso o già completate, vengono monitorate nel Centro azioni. Nel Centro azioni vengono approvate (o rifiutate) le azioni in sospeso e le azioni completate possono essere annullate, se necessario.

/ MICROSOFT THREAT EXPERTS

Le notifiche degli attacchi endpoint (precedentemente definite Microsoft Threat Experts - Notifica di attacco mirato) consentono di individuare in modo proattivo le minacce più importanti per la rete, tra cui intrusioni di hacker, attacchi keylogger o attacchi avanzati come lo spionaggio informatico. Queste notifiche vengono visualizzate come nuovo avviso.

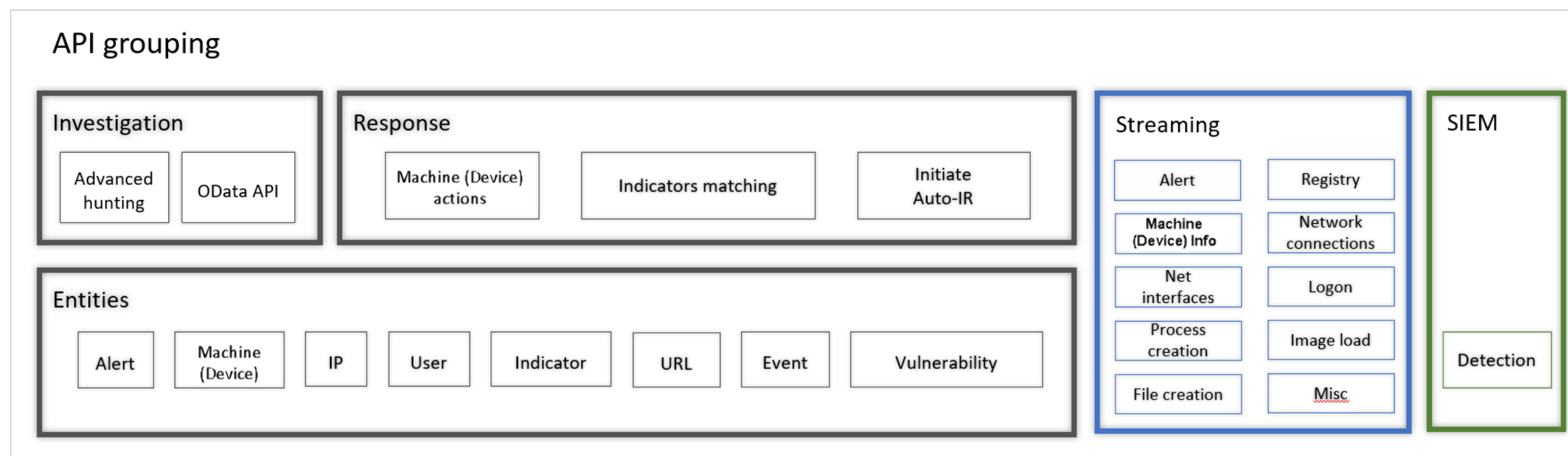
Il servizio di ricerca gestita include:

- Monitoraggio e analisi delle minacce, riducendo i tempi di attesa e i rischi per l'azienda
- Intelligenza artificiale addestrata da Hunter per scoprire e assegnare priorità agli attacchi noti e sconosciuti
- Identificare i rischi più importanti, aiutando i CSC a ottimizzare il tempo e l'energia
- Ambito di compromissione e la quantità di contesto che può essere recapitata rapidamente per abilitare una risposta SOC veloce

/ AMMINISTRAZIONE E CONFIGURAZIONE CENTRALIZZATE, API

Il portale di Microsoft Defender offre al team di sicurezza un'esperienza end-to-end affidabile per la configurazione, la distribuzione e il monitoraggio. Inoltre, Microsoft Defender per endpoint supporta Criteri di gruppo e altri strumenti non Microsoft usati per la gestione dei dispositivi.

Defender per endpoint offre un controllo granulare delle operazioni che gli utenti con accesso al portale possono visualizzare e eseguire grazie alla flessibilità del controllo degli accessi in base al ruolo.





Office 365

/ MICROSOFT DEFENDER FOR OFFICE

Microsoft Defender per Office 365 è un servizio di filtro della posta elettronica basato sul cloud che consente di proteggere l'organizzazione da minacce avanzate agli strumenti di posta elettronica e collaborazione, ad esempio phishing, compromissione della posta elettronica aziendale e attacchi malware. Defender per Office 365 fornisce anche funzionalità di analisi, ricerca e correzione per aiutare i team di sicurezza a identificare, assegnare priorità, analizzare e rispondere in modo efficiente alle minacce.

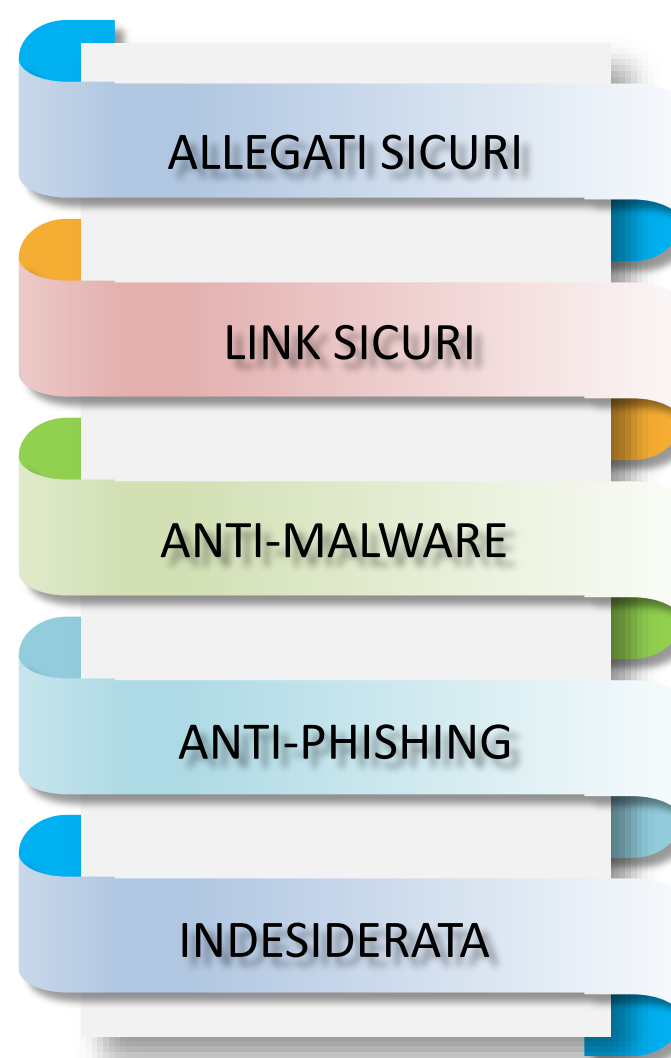


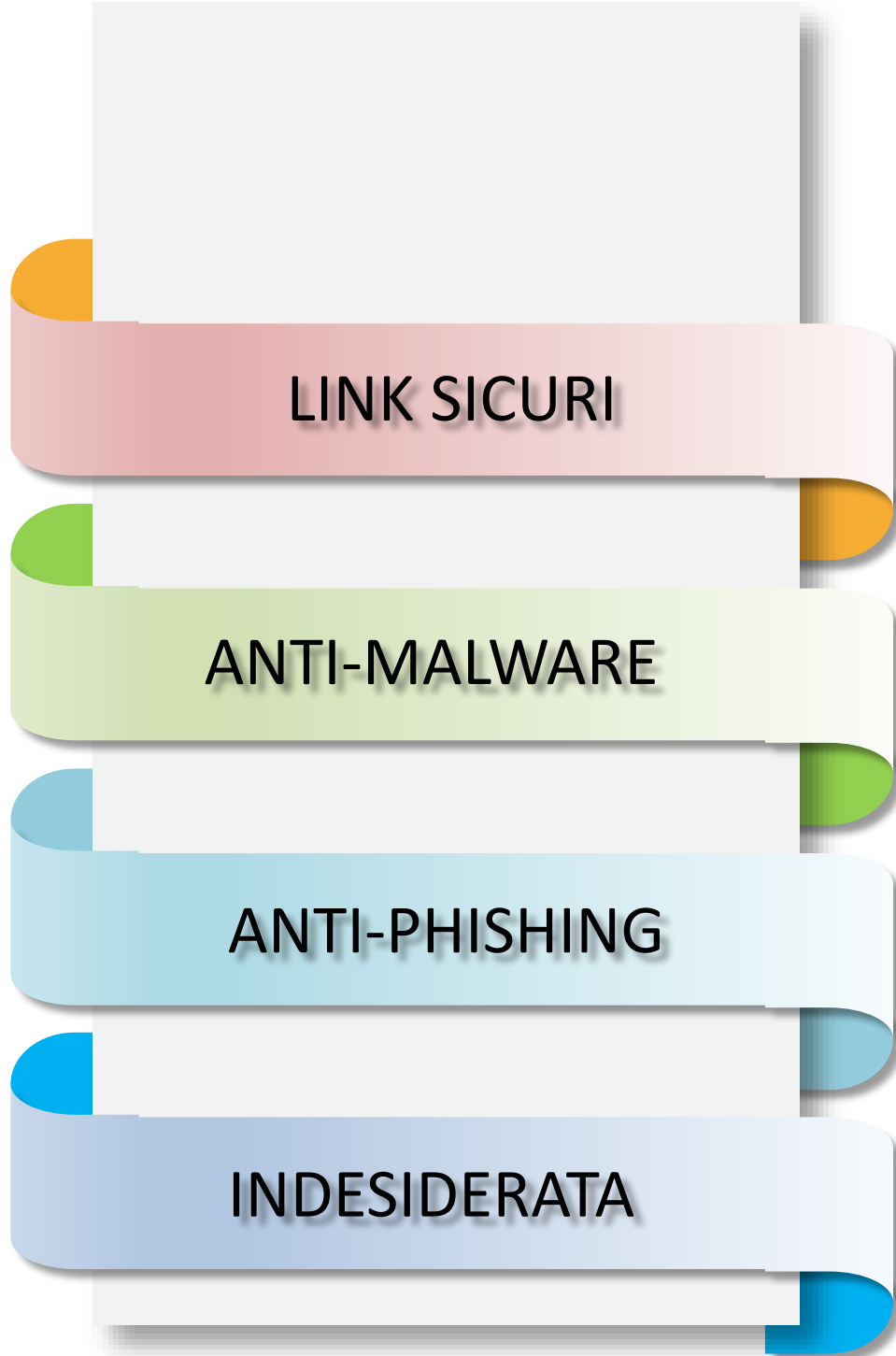


Office 365

/ MICROSOFT DEFENDER FOR OFFICE

Microsoft Defender per Office 365 è un servizio di filtro della posta elettronica basato sul cloud che consente di proteggere l'organizzazione da minacce avanzate agli strumenti di posta elettronica e collaborazione, ad esempio phishing, compromissione della posta elettronica aziendale e attacchi malware. Defender per Office 365 fornisce anche funzionalità di analisi, ricerca e correzione per aiutare i team di sicurezza a identificare, assegnare priorità, analizzare e rispondere in modo efficiente alle minacce.





LINK SICURI

ANTI-MALWARE

ANTI-PHISHING

INDESIDERATA

ALLEGATI SICURI

Allegati sicuri in Microsoft Defender per Office 365 offrono un ulteriore livello di protezione per gli allegati di posta elettronica.

Dopo che gli allegati vengono analizzati dalla protezione antimalware in Exchange Online Protection (EOP), vengono aperti in un ambiente virtuale per verificare la presenza di minacce prima di essere recapitati ai destinatari

ALLEGATI SICURI

ANTI-MALWARE

ANTI-PHISHING

INDESIDERATA

LINK SICURI

Link sicuri in Microsoft Defender per Office 365 offrono protezione contro i link dannosi utilizzati in attacchi di phishing e altre minacce.

Questa funzionalità esegue la scansione e la riscrittura degli URL nei messaggi di posta elettronica in entrata e verifica i link al momento del clic in email, Microsoft Teams e app di Office supportate

LINK SICURI

ALLEGATI SICURI

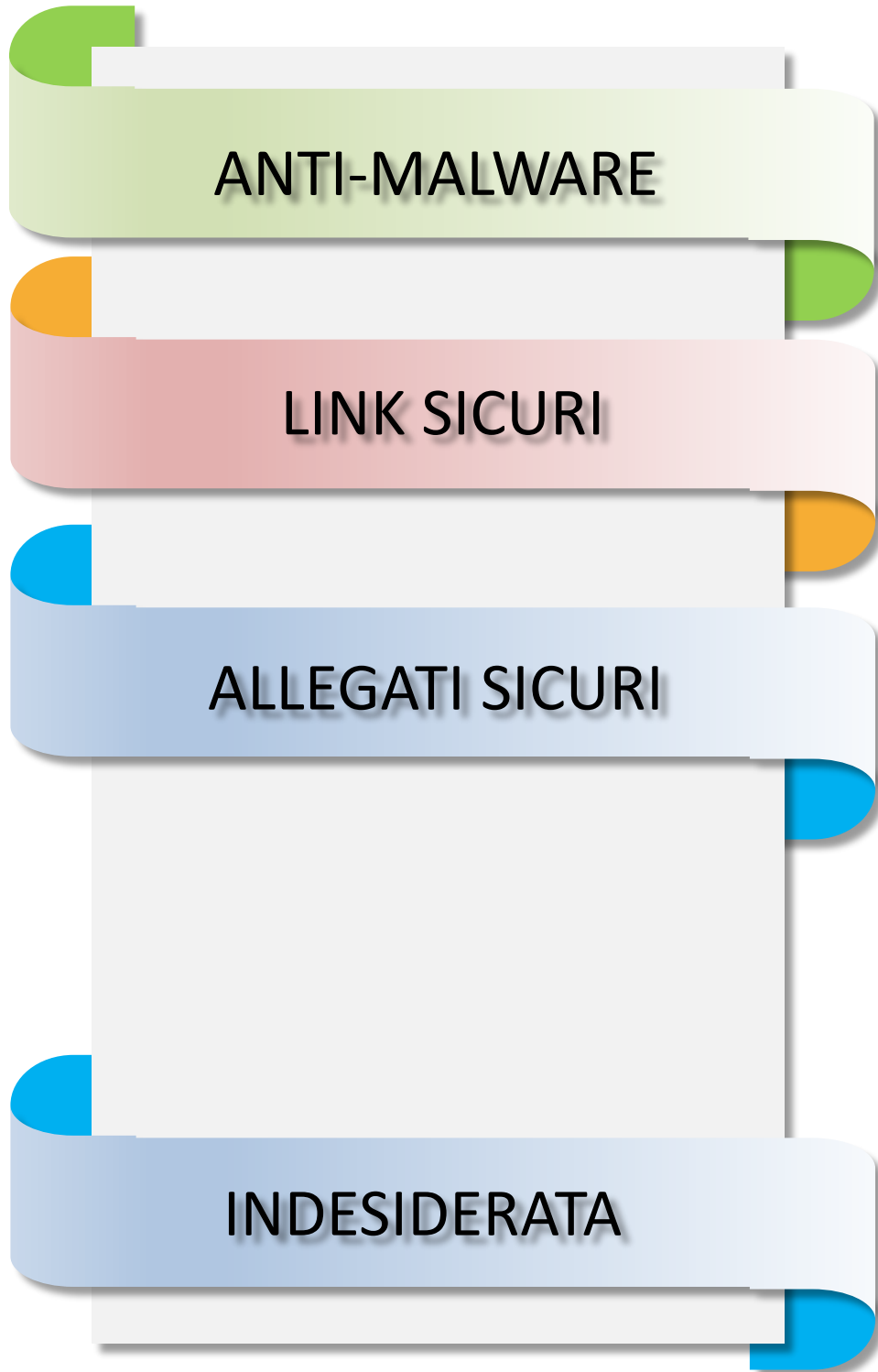
ANTI-PHISHING

INDESIDERATA

ANTIMALWARE

La protezione antimalware in Microsoft Defender per Office 365 offre una difesa multilivello contro malware noti e sconosciuti. Utilizza la scansione euristica per rilevare minacce anche nelle fasi iniziali di un attacco.

Le politiche antimalware predefinite si applicano automaticamente a tutti i destinatari, ma è possibile creare politiche personalizzate per utenti, gruppi o domini specifici. I messaggi contenenti malware vengono messi in quarantena e solo gli amministratori possono visualizzarli e rilasciarli



ANTI-MALWARE

LINK SICURI

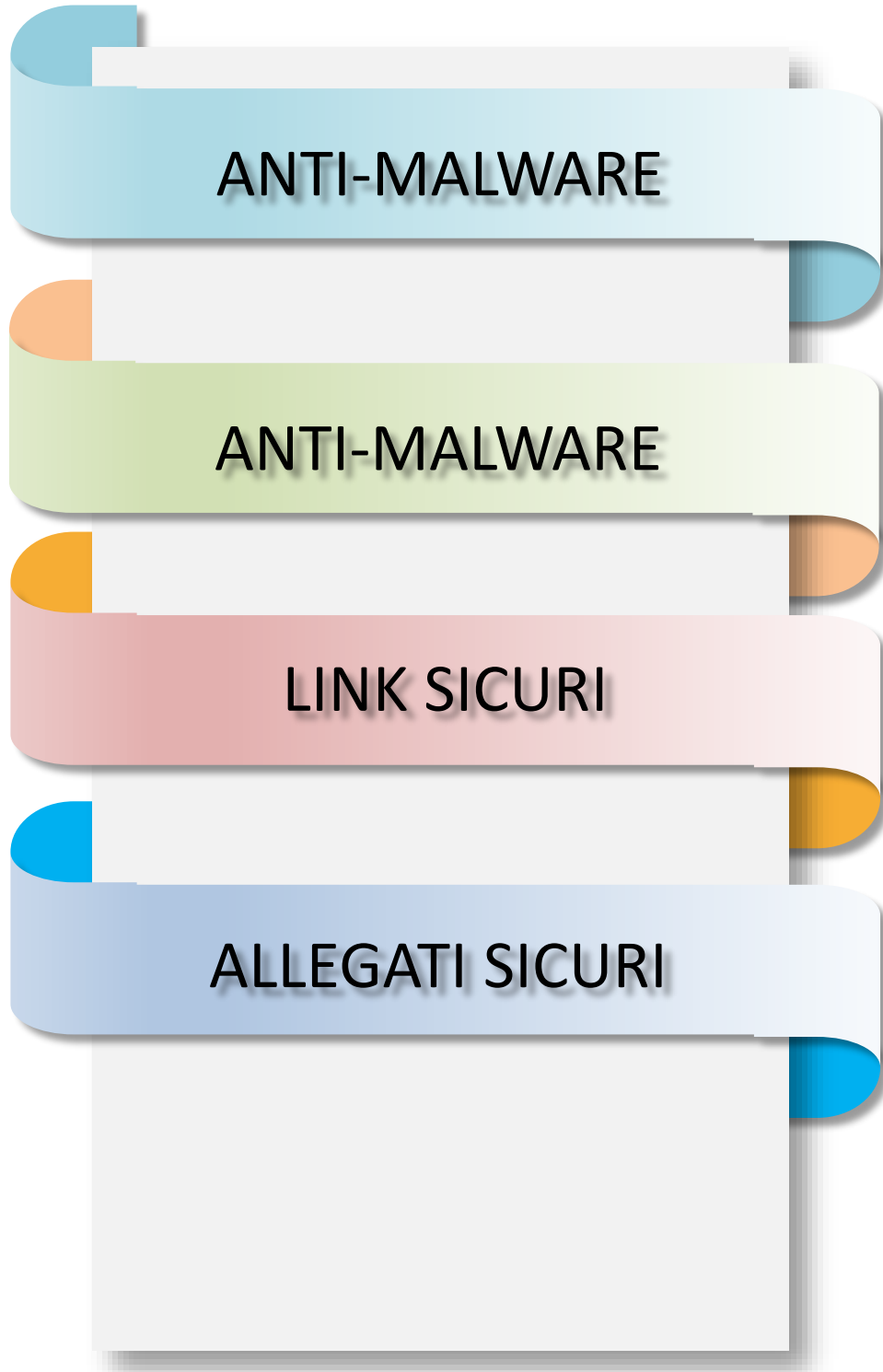
ALLEGATI SICURI

INDESIDERATA

ANTI PHISHING

Le politiche anti-phishing in Microsoft Defender per Office 365 offrono protezione avanzata contro attacchi di phishing e spoofing. Queste politiche includono:

- **Protezione contro l'impersonificazione:** Difende contro l'impersonificazione di utenti, domini e mittenti.
- **Soglie di rilevamento avanzate:** Utilizza algoritmi di intelligenza artificiale e apprendimento automatico per rilevare attacchi sofisticati.
- **Suggerimenti di sicurezza al primo contatto:** Avvisa gli utenti quando ricevono email da mittenti sconosciuti.
- **Visualizzazione delle campagne:** Analizza i messaggi coinvolti in attacchi di phishing coordinati.



ANTI-MALWARE

ANTI-MALWARE

LINK SICURI

ALLEGATI SICURI

POSTA INDESIDERATA

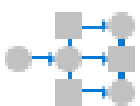
La protezione dalla posta indesiderata in Microsoft Defender per Office 365 utilizza tecnologie avanzate di filtro per identificare e separare i messaggi indesiderati da quelli legittimi.

Ecco i punti principali:

- **Filtri di contenuto:** Utilizzano tecnologie proprietarie per rilevare e bloccare la posta indesiderata e i tentativi di phishing.
- **Criteri predefiniti e personalizzati:** I criteri predefiniti si applicano automaticamente a tutti i destinatari, ma è possibile creare criteri personalizzati per utenti, gruppi o domini specifici.
- **Quarantena:** I messaggi identificati come posta indesiderata o phishing vengono messi in quarantena, e solo gli amministratori possono gestirli.

Microsoft Defender for Office 365 protection stack

Edge protection



Network throttling



IP reputation/throttling



Domain reputation



Directory-based edge filtering



Backscatter detection

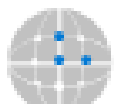


Enhanced filtering for on-prem routing

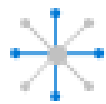
Sender intelligence



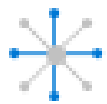
Account compromise detection



DMARC DKIM, SPF, ARC



Intra-org spoof intelligence



Cross-domain spoof intelligence



Bulk filtering



Mailbox intelligence



Mailbox intelligence impersonation



User impersonation

micro@microsoft.com

Domain impersonation

Content filtering



Transport custom rules



AV engines



Type blocking



Attachment reputation blocking



Heuristic clustering



ML models



Tenant allow/block lists



URL reputation blocking



Content heuristics



Safe attachments



Linked content detonation



URL detonation

Post-delivery protection



Safe links



Phish zero-hour auto-purge



Malware zero-hour auto-purge



Spam zero-hour auto-purge



Campaigns



End-user reporting



Office clients



OneDrive/SharePoint



URL detonation



/ MICROSOFT DEFENDER FOR APP CLOUD

Le app SaaS (Software as a Service) sono onnipresenti negli ambienti di lavoro ibridi e la protezione delle app SaaS e dei dati importanti che archiviano è una grande sfida per le organizzazioni. L'aumento dell'utilizzo delle app, combinato con i dipendenti che accedono alle risorse aziendali al di fuori del perimetro aziendale, ha introdotto anche nuovi vettori di attacco. Per combattere questi attacchi in modo efficace, i team di sicurezza hanno bisogno di un approccio che protegga i dati all'interno delle app cloud oltre l'ambito tradizionale dei cloud access security broker (CASB).



Scopri le applicazioni SaaS



autorizzato app\$



Protezione da app a app

Individuare e correggere integrazioni di terze parti



Gestione della postura di sicurezza SaaS (SSPM)

Configurazioni errate | Procedure consigliate

Correggere configurazioni rischiose



Protezione continua dalle minacce

Rilevare, analizzare e rispondere
agli attacchi con Microsoft 365 Defender



Protezione delle informazioni:

Esposizione dei dati sensibili

Violazione dei file di governance

... e altro ancora

Home

Gestione dell'esposizione

Indagine e risposta

Threat intelligence

Risorse

Microsoft Sentinel

Identità

Endpoint

Email & collaborazione

App cloud

Cloud Discovery

Catalogo di app cloud

App oath

Governance delle app

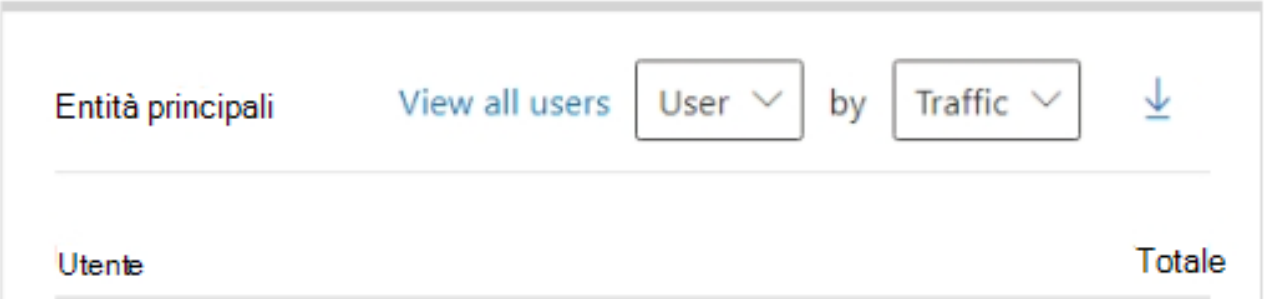
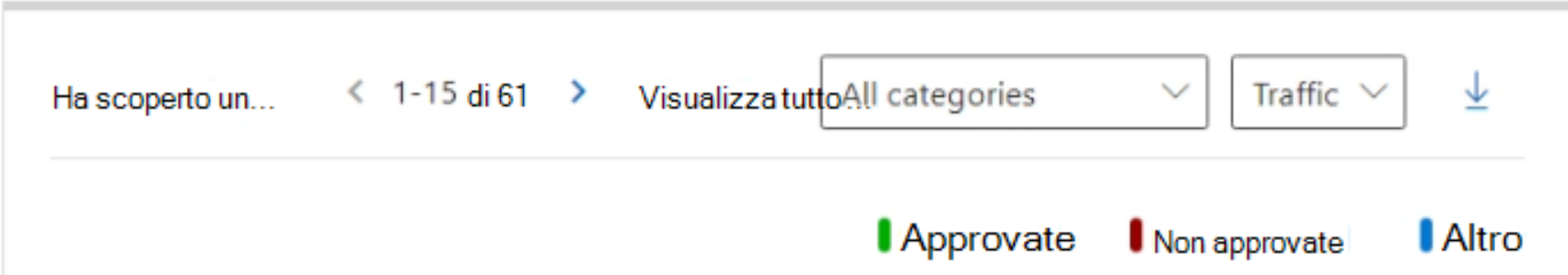
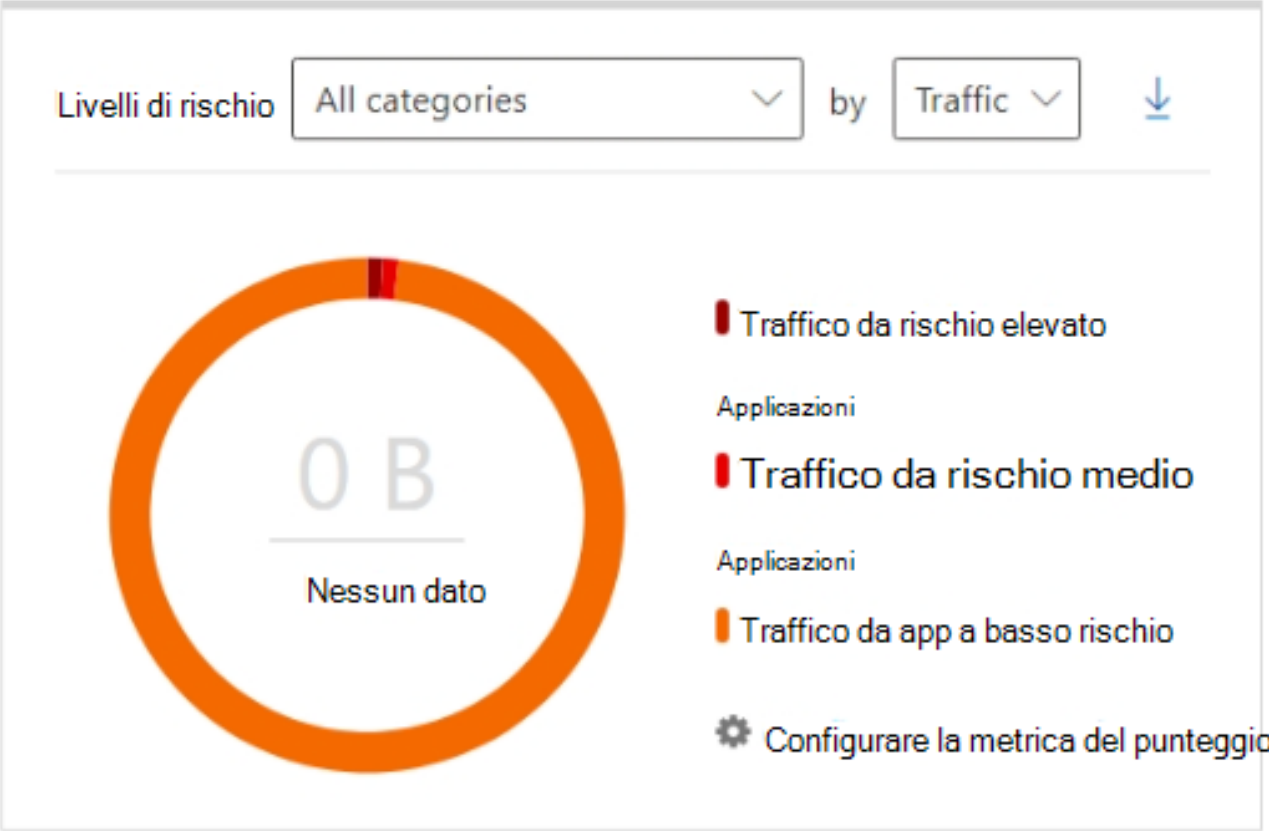
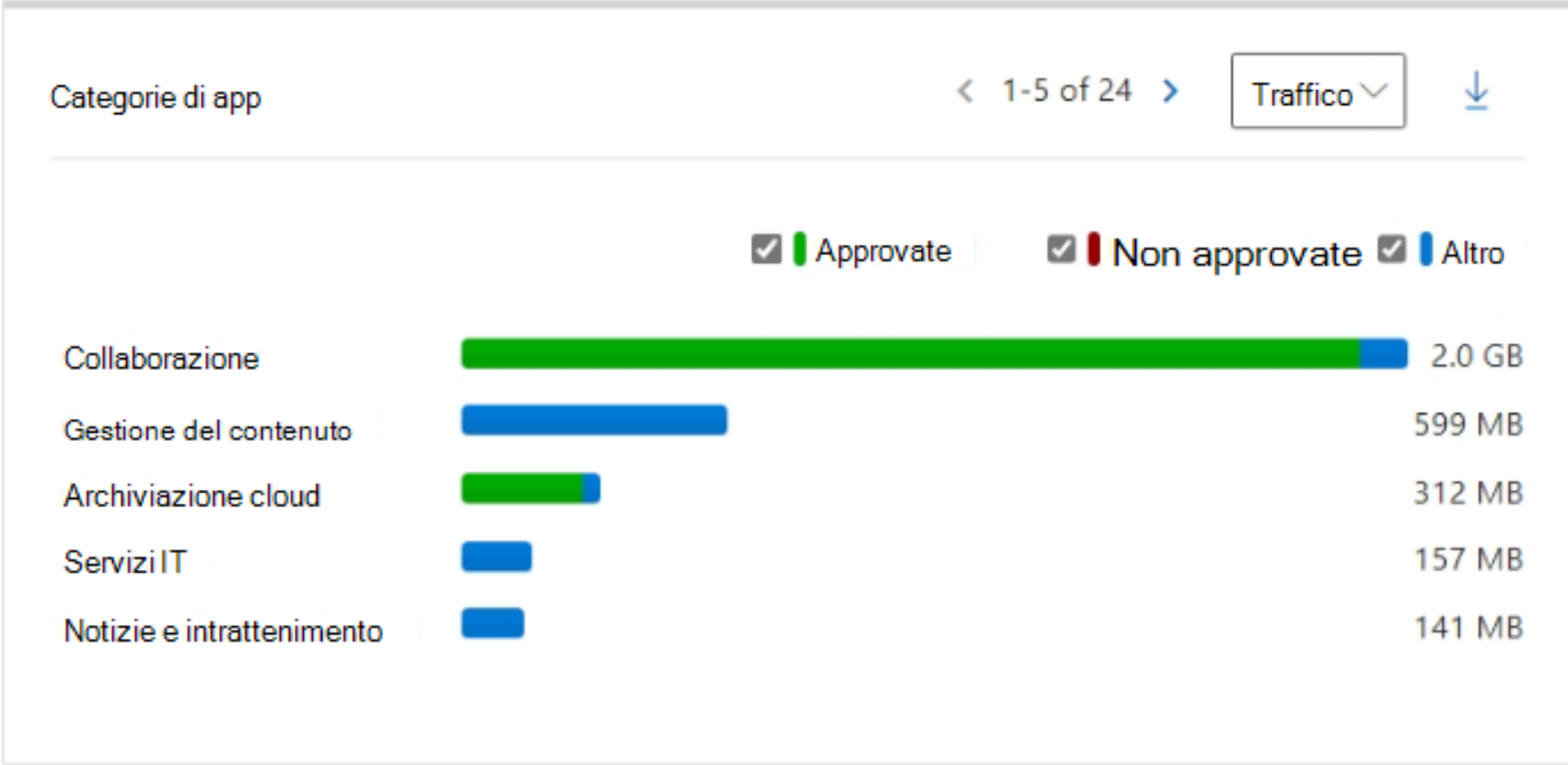
File

Cloud Discovery

Aggiornato il 31 luglio 2024, 10:19

Dashboard App individuate Risorse individuate Indirizzi IP Utenti Dispositivi

App	Indirizzi IP	Utenti	Dispositivi	Traffico
61	14	14	14	3.5 GB ↑ 1.2 GB ↓ 2.3 GB



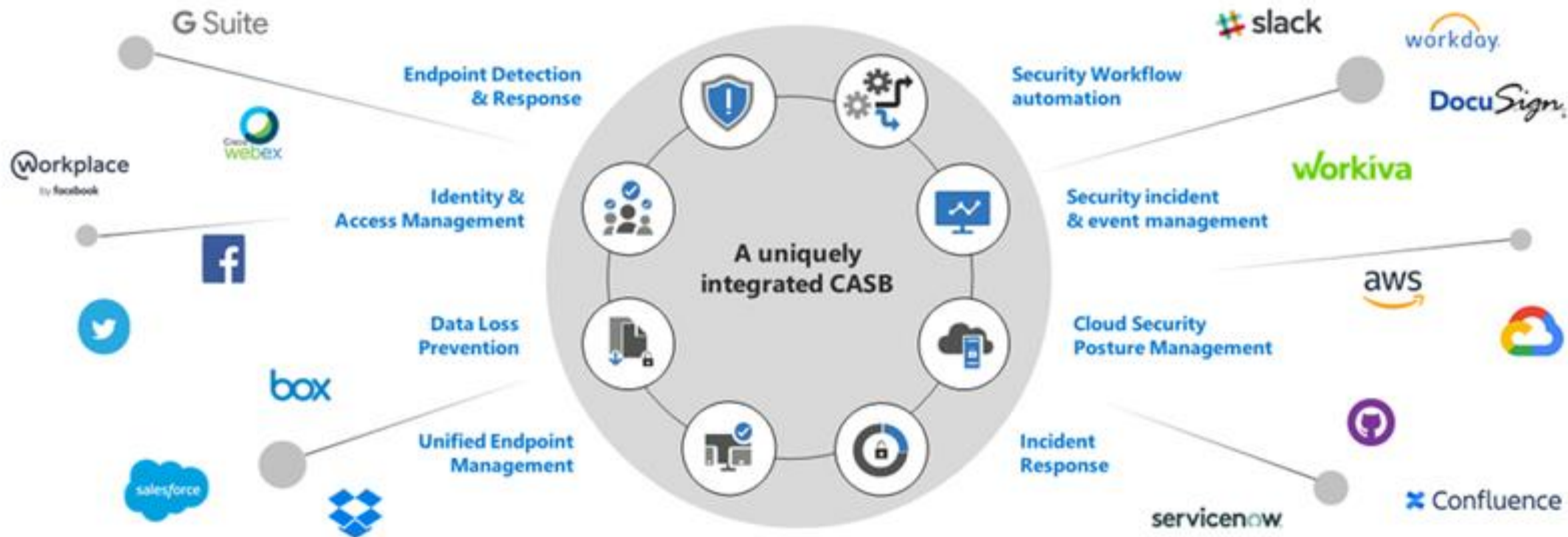
Microsoft Cloud App Security

The go-to CASB for Office 365 and Azure that loves 3rd party

Simple deployment

Natively integrated across the broader Microsoft product stack to deliver unique capabilities

Rooted in supporting any app





/ **MICROSOFT DEFENDER FOR CLOUD**

Microsoft Defender per il cloud è una piattaforma di protezione delle applicazioni nativa del cloud costituita da misure e procedure di sicurezza progettate per proteggere le applicazioni basate sul cloud da varie minacce informatiche e vulnerabilità. Microsoft Defender per il cloud combina le funzionalità di:

- Soluzione devSecOps (Development Security Operations) che unifica la gestione della sicurezza a livello di codice in ambienti multcloud e con più pipeline
- Una soluzione di gestione del comportamento di sicurezza cloud (CSPM) che illustra le azioni che è possibile eseguire per evitare violazioni.
- Una piattaforma CWPP (Cloud Workload Protection Platform) con protezioni specifiche per server, contenitori, archiviazione, database e altri carichi di lavoro.

Microsoft Defender for Cloud

Unify your DevOps
Security Management



Strengthen and manage your
cloud security posture



Protect your cloud
workloads



aws



NOVITA'

FEBBRAIO 2025

Dashboard di sicurezza dei dati e
dell'intelligenza artificiale

Calcolatore dei costi MDC (anteprima)

31 framework normativi degli standard
multicloud nuovi e migliorati

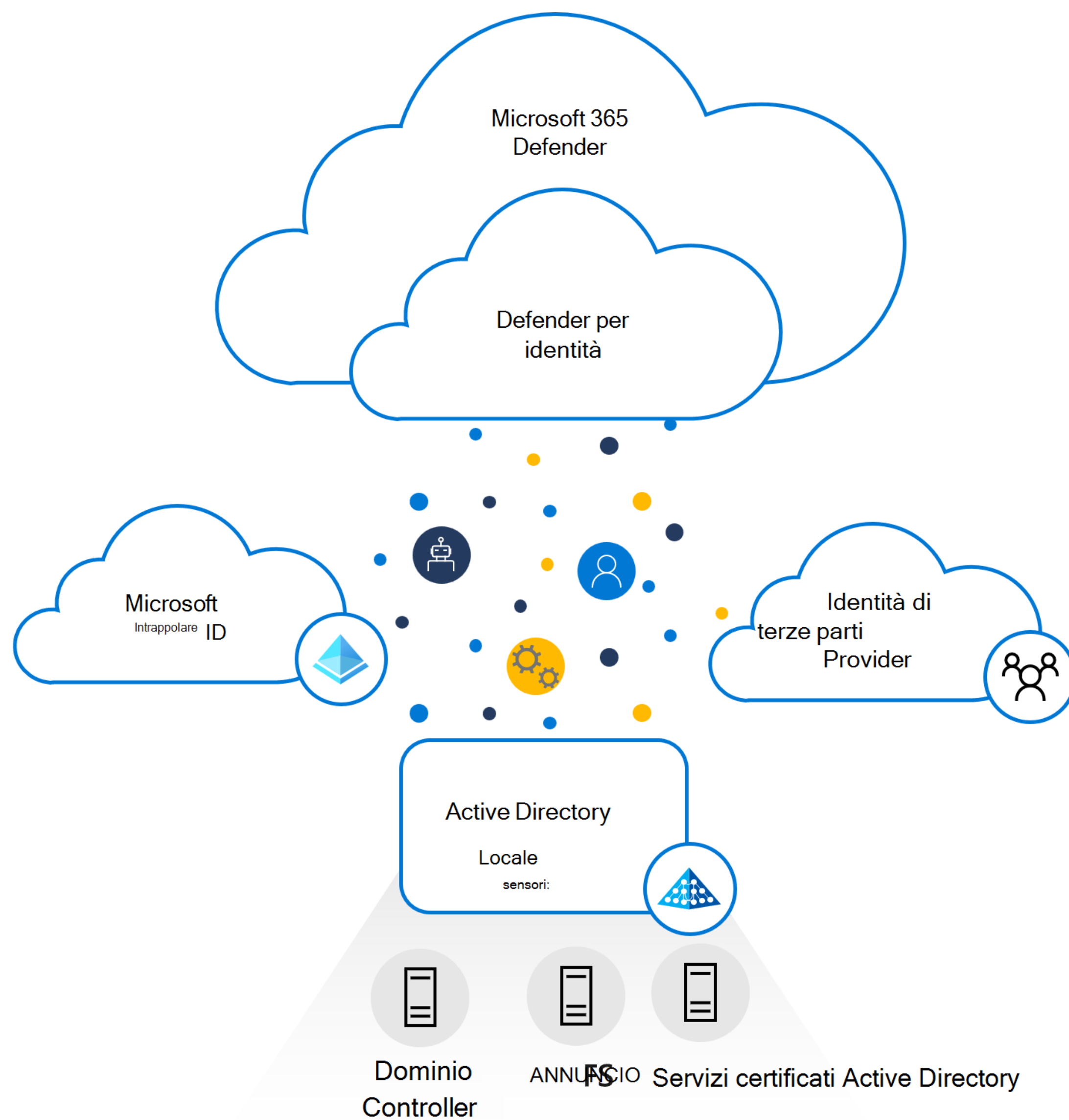
RESOL/E
by ErgonGroup



/ MICROSOFT DEFENDER FOR IDENTITY

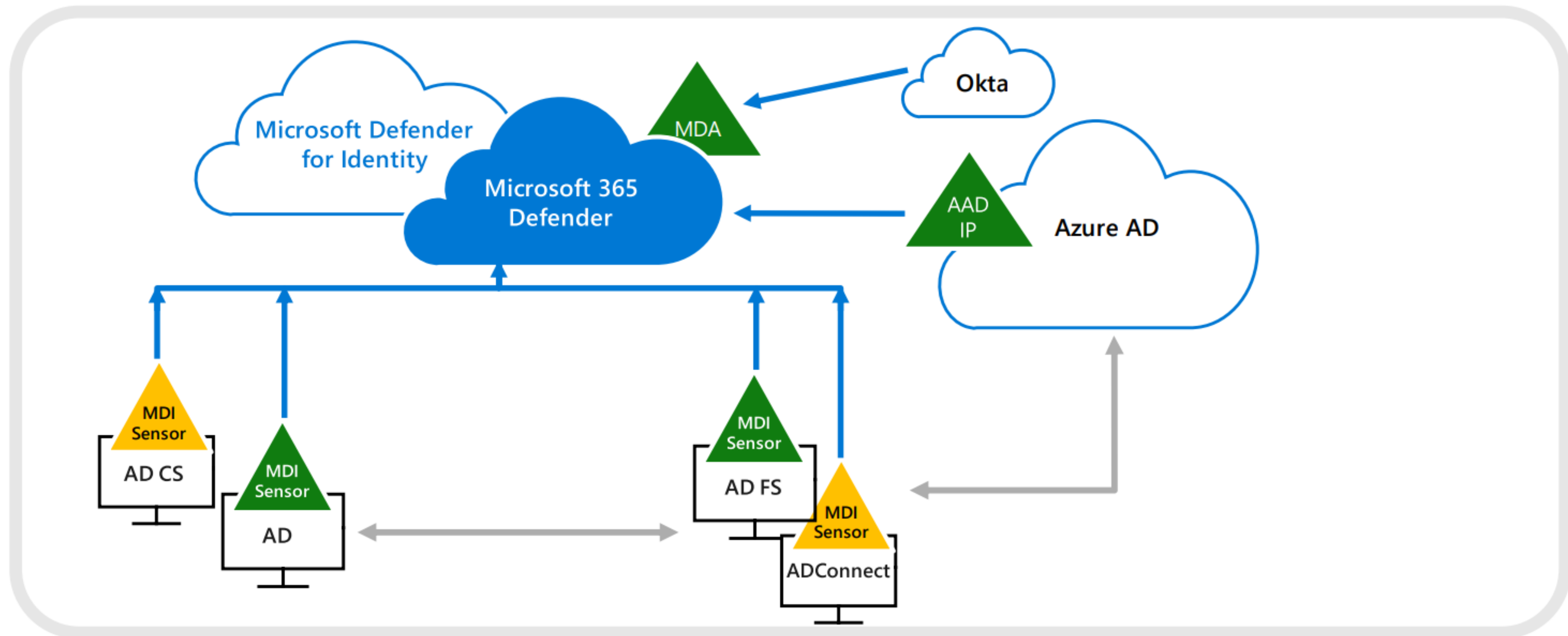
Microsoft Defender per identità è una soluzione di sicurezza basata sul cloud che consente di proteggere il monitoraggio delle identità nell'intera organizzazione.

- **Prevenire le violazioni**, usando valutazioni proattive del comportamento di sicurezza delle identità
- **Rilevare le minacce**, usando l'analisi in tempo reale e l'intelligence dati
- **Analizzare le attività sospette**, usando informazioni sugli eventi imprevisti chiare e interattive
- **Rispondere agli attacchi**, usando la risposta automatica alle identità compromesse



Identifica e correggi gli attacchi all'intera infrastruttura di identità

Il futuro dell'MDI è quello di replicare le capacità di rilevamento e risposta, applicate su AD/ADFS, per l'intera infrastruttura di identità, nonché la correlazione di segnali e incidenti per colmare le pericolose lacune.



Respond

Automatic response
to compromised
identities

Prevent

Proactive identity
security posture
assessments

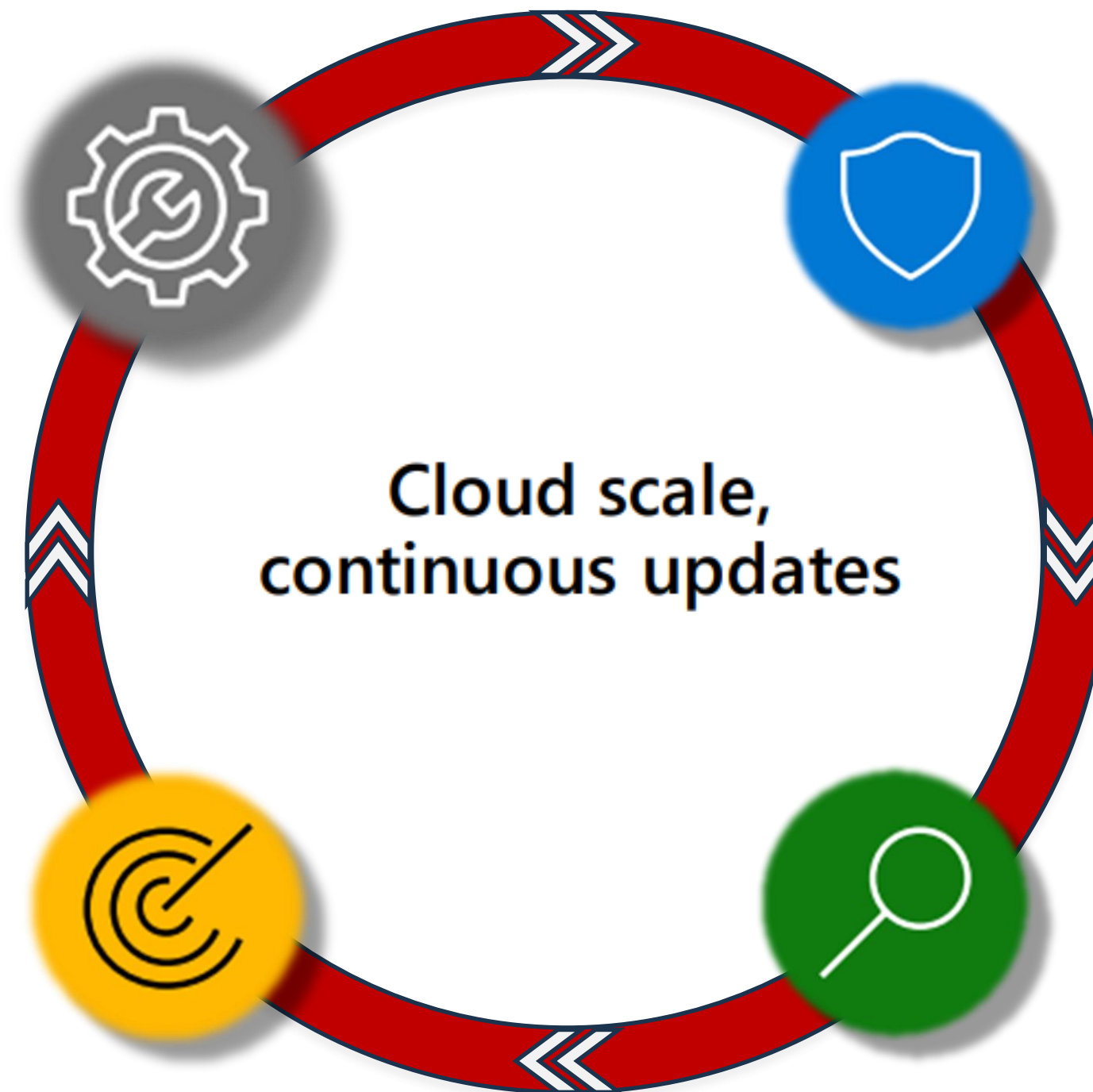
Cloud scale,
continuous updates

Detect

Real-time analytics
and data intelligence

Investigate

User investigation
priority





/ MICROSOFT DEFENDER FOR ENTRA ID

Microsoft Entra ID Protection è una soluzione di identità basata su cloud che aiuta le organizzazioni a prevenire, rilevare e porre rimedio alla compromissione dell'identità in tempo reale.

Analizzando gli utenti e i modelli di accesso in base a punteggi di rischio integrati da varie fonti, ID Protection protegge dagli attacchi basati sull'identità come password spray, brute force, phishing, dispositivi infetti e credenziali trapelate.





È progettato per rilevare e investigare minacce avanzate, identità compromesse e azioni dannose da parte di insider dirette alla tua organizzazione. Fornisce monitoraggio e profilazione in tempo reale del comportamento e delle attività degli utenti e genera avvisi per attività sospette.



Fornisce un set più completo di capacità di protezione e gestione dell'identità. Include funzionalità come accesso condizionale basato sul rischio, protezione dell'identità, gestione delle identità privilegiate e altro ancora.

COME FUNZIONA MICROSOFT ENTRA ID PROTECTION



Proteggere l'accesso con fattori di autenticazione ad alta sicurezza e resistenti al phishing.

Applicare policy di accesso adattivo basate sul rischio per prevenire la compromissione dell'identità.



Proteggere l'accesso con fattori di autenticazione ad alta sicurezza e resistenti al phishing.

Ottieni informazioni approfondite sulla tua postura di sicurezza dell'identità.

Applicare policy di accesso adattivo basate sul rischio per prevenire la compromissione dell'identità.



Proteggere l'accesso con fattori di autenticazione ad alta sicurezza e resistenti al phishing.

CONSIDERARE QUESTE SOGLIE QUANDO SI STABILISCE UNA POLITICA DI RISCHIO PER L'UTENTE

Una soglia bassa massimizza la protezione dell'identità se la tua organizzazione richiede una postura di sicurezza più elevata.

Una soglia media bilancia sicurezza e usabilità.

Una soglia elevata riduce il numero di volte in cui una politica viene attivata e riduce al minimo l'impatto sull'utente

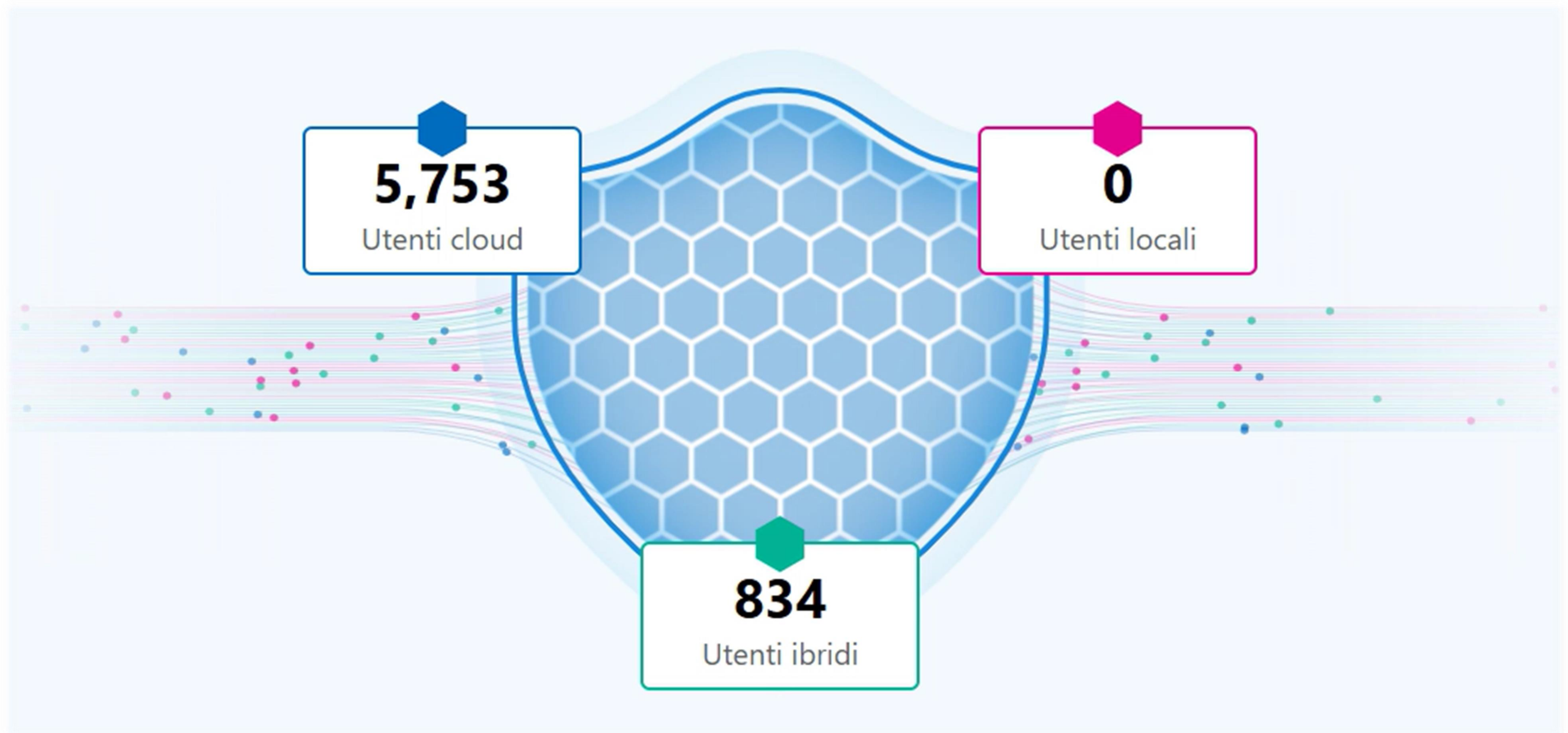
LOW

MEDIUM

HIGH



CONTROLLO IN TEMPO REALE DELLE IDENTITÀ



Dashboard ITDR

Questa dashboard dinamica offre una vista centralizzata di informazioni critiche e dati in tempo reale sul rilevamento e la risposta alle minacce all'identità. Fornendo un'interfaccia intuitiva che mostra informazioni importanti relative ad accessi non autorizzati, compromissione dell'account, minacce interne e attività anomale, la nostra dashboard ti consente di monitorare e gestire in modo proattivo i potenziali rischi per la sicurezza correlati all'identità.



/ MICROSOFT DEFENDER SENTINEL

Microsoft Sentinel è un sistema SIEM nativo del cloud e scalabile che offre una soluzione intelligente e completa per l'orchestrazione SIEM e la sicurezza, l'automazione e la risposta (SOAR). Microsoft Sentinel offre il rilevamento delle minacce informatiche, l'indagine, la risposta e la ricerca proattiva, con una visione panoramica dell'intera azienda.

Microsoft Sentinel incorpora anche servizi di Azure collaudati, come Log Analytics e App per la logica, e arricchisce l'indagine e il rilevamento con l'intelligenza artificiale. Usa il flusso di intelligence sulle minacce di Microsoft ma consente anche di usare la propria intelligence sulle minacce.

È possibile usare Microsoft Sentinel per alleviare il carico associato ad attacchi sempre più sofisticati, volume crescente degli avvisi e lunghi tempi di risoluzione

Soluzioni SIEM che consentono di inserire dati, monitorare, inviare avvisi, effettuare ricerche, indagini, rispondere e connettersi a prodotti, piattaforme e servizi diversi.

Microsoft Azure

Search resources, services, and docs (G+)

ALPINE SKI HOUSE

Home > Microsoft Sentinel > Microsoft Sentinel

» Microsoft Sentinel | Content hub ...

Selected workspace: 'cybersoc'

Search

Refresh

SIEM Migration

Guides & Feedback

General

Overview (Preview)

Logs

News & guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Watchlist

Automation

Settings

350

Solutions

273

Standalone contents

195

Installed

32

Updates

Search...

Status : AllContent type : AllSupport : AllProvider : AllCategory : AllContent sources : All

Solutions (350)

See more

Amazon Web Services

Microsoft Sentinel, Microsoft Corporation

Security - Cloud Security

Analytics rule (57)Data connector (2)+2

InstalledUpdates

Azure Activity

Microsoft Sentinel, Microsoft Corporation

IT Operations

Analytics rule (13)Data connector+2

Installed

Cisco Umbrella

Microsoft Sentinel, Microsoft Corporation

Security - Automation (SOAR), Security - Cloud Security

Analytics rule (10)Data connector+4

InstalledUpdates

Standalone (273)

See more

Workbook (53)

See more

Workbook

Analytics Health & Audit

Microsoft

IT Operations, Platform

Installed

Workbook

Workspace Usage Report

Community

IT Operations

Installed

Workbook

ACSC Essential 8

Microsoft

Compliance, IT Operations

Installed

Cisco Umbrella

Cisco Provider

Microsoft Support

2.0.4 Version

Description

Note: There may be *known issues* pertaining to this Solution, please refer to them before installing.

The [Cisco Umbrella](#) solution for Microsoft Sentinel enables you to ingest [Cisco Umbrella events](#) stored in Amazon S3 into Microsoft Sentinel using the Amazon S3 REST API.

Underlying Microsoft Technologies used:

This solution takes a dependency on the following technologies, and some of these dependencies either may be in [Preview](#) state or might result in additional ingestion or operational costs:

a. [Azure Monitor HTTP Data Collector API](#)

b. [Azure Functions](#)

Data Connectors: 1, **Parsers:** 1, **Workbooks:** 1, **Analytic Rules:** 10, **Hunting Queries:** 10, **Custom Azure Logic Apps Connectors:** 4, **Playbooks:** 4

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Manage

Actions

View details

RESOL/E

by ErgonGroup

Riproduzione riservata @Resolve

Raccogliere i dati per tutti gli utenti, i dispositivi, le applicazioni e l'infrastruttura, sia in locale che in più cloud.

Microsoft Sentinel | Data connectors

Selected workspace: 'cybersecuritysoc'

Search

News & guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Refresh

Guides & Feedback

Azure Active Directory (Azure AD) is now Microsoft Entra ID. [Learn more](#)

190 Onboarded Connectors

38 Connected

0 Updates

More content at Content hub

Search by name or provider

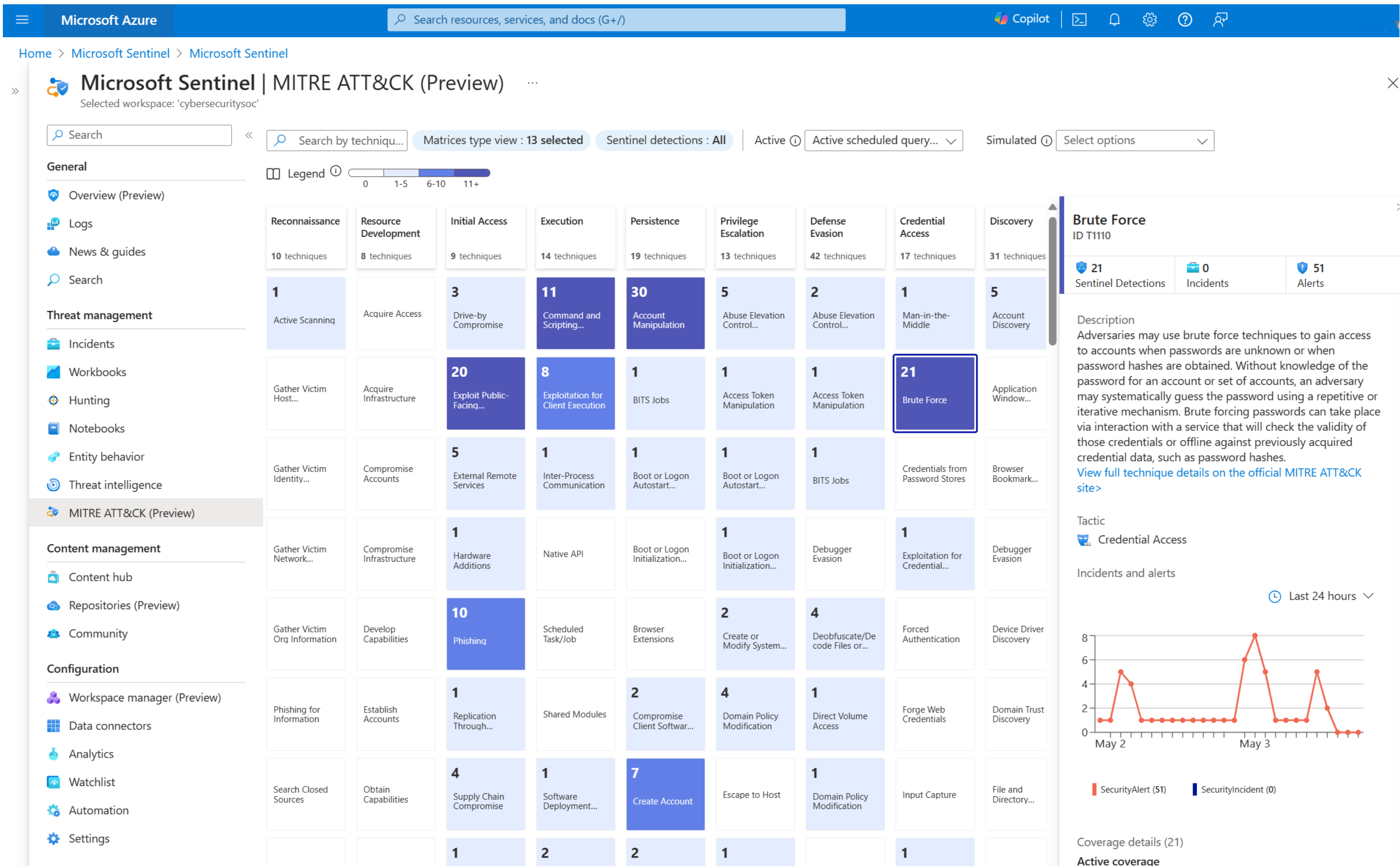
Providers : Microsoft

Data Types : All

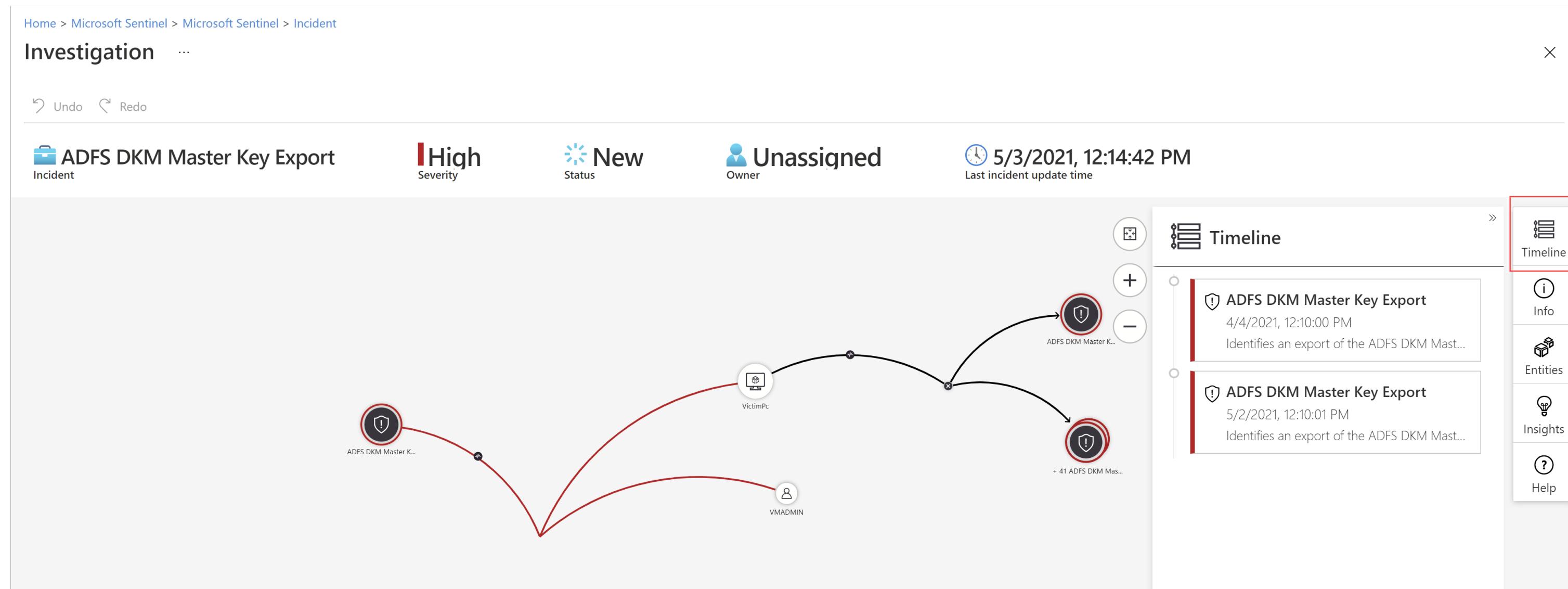
Status : All

Status	Connect...	Content Source	Updates
	Azure Act... Microsoft	Solution Azure Activity	
	Azure Bat... Microsoft	Solution Azure Batch Account	
	Azure Co... Microsoft	Solution Azure Cognitive Search	
	Azure Dat... Microsoft	Solution Azure Data Lake Storage Gen1	
	Azure DD... Microsoft	Solution Azure DDoS Protection	

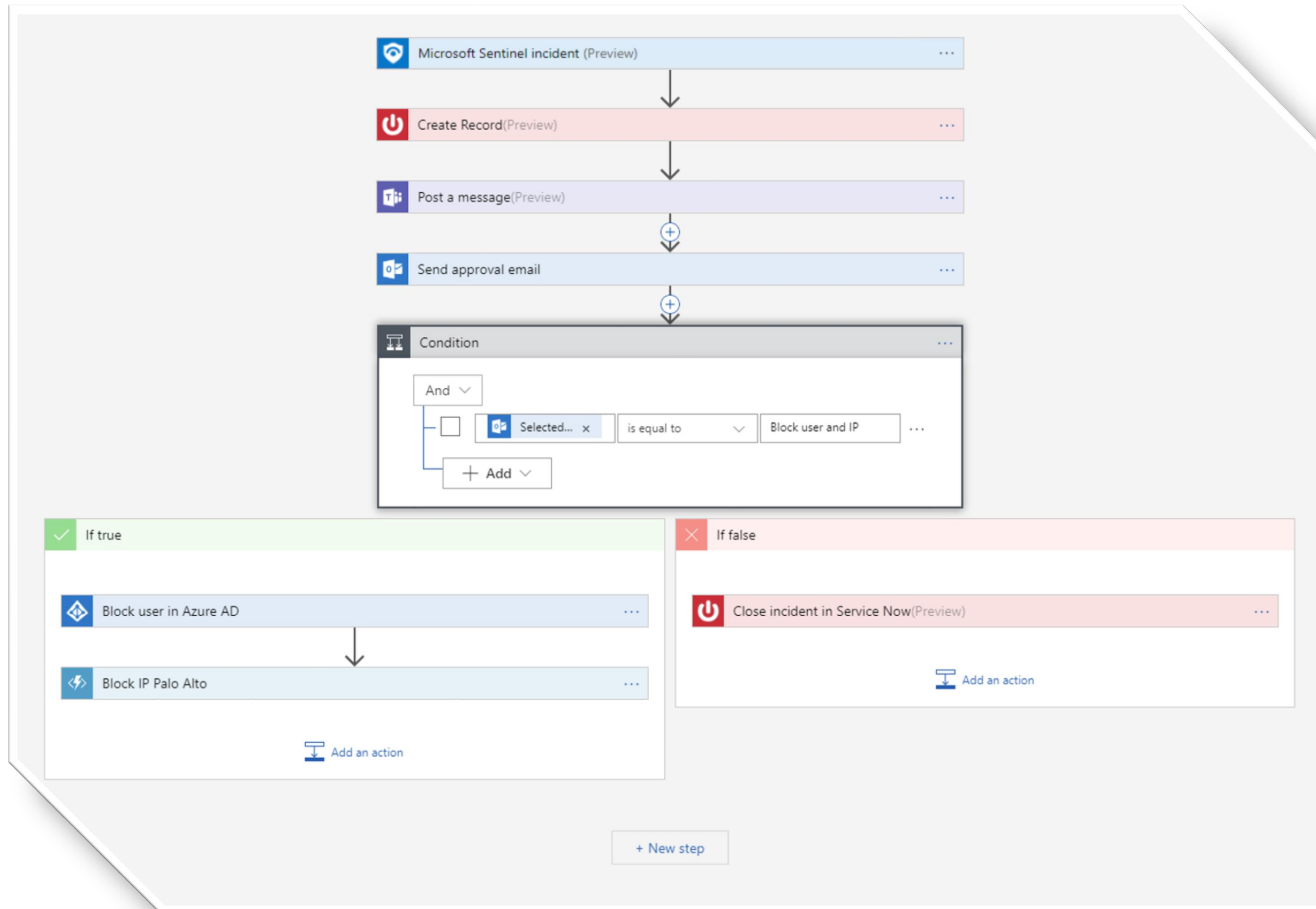
Rilevamento di minacce precedentemente non individuate e riduzione al minimo dei falsi positivi grazie alle funzionalità di analisi e alla straordinaria intelligence sulle minacce di Microsoft.



Analisi delle minacce tramite intelligenza artificiale e rilevamento delle attività sospette su larga scala, sfruttando i vantaggi di anni di esperienza di Microsoft a livello di cybersecurity.



Automatizzare e semplificare l'orchestrazione con flussi automatici





/ MICROSOFT COPILOT FOR DEFENDER

Microsoft Security Copilot unisce la potenza dell'intelligenza artificiale e delle competenze umane per aiutare i team di sicurezza a rispondere agli attacchi in modo più rapido ed efficace. Security

Copilot è incorporato nel portale di Microsoft Defender per fornire ai team di sicurezza funzionalità avanzate per analizzare e rispondere agli eventi imprevisti, cercare le minacce e proteggere l'organizzazione con informazioni sulle minacce pertinenti.

Copilot in Defender è disponibile per gli utenti che hanno effettuato il provisioning dell'accesso a Security Copilot.

FUNZIONALITÀ PRINCIPALI



1 Indagare e rispondere a incidenti come un esperto

FUNZIONALITÀ PRINCIPALI



2 Riepilogare rapidamente
gli incidenti

FUNZIONALITÀ PRINCIPALI



3 Intervenire sugli incidenti
tramite risposte guidate

FUNZIONALITÀ PRINCIPALI



4 Eseguire facilmente
l'analisi degli script

FUNZIONALITÀ PRINCIPALI



5 Generare riepiloghi dei dispositivi

FUNZIONALITÀ PRINCIPALI



6 Analizzare i file in modo tempestivo

FUNZIONALITÀ PRINCIPALI



7 Analizzare immediatamente
le identità

FUNZIONALITÀ PRINCIPALI



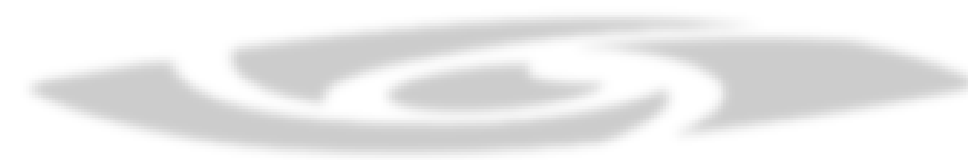
8 Scrivere report degli incidenti
in modo efficiente

FUNZIONALITÀ PRINCIPALI



9 Generare query KQL dall'input
in linguaggio naturale

MICROSOFT PURVIEW





MICROSOFT PURVIEW

Microsoft Purview è una piattaforma completa progettata per aiutare le organizzazioni a gestire, proteggere e governare i dati ovunque si trovino..





MICROSOFT PURVIEW

Microsoft Purview è una piattaforma completa progettata per aiutare le organizzazioni a gestire, proteggere e governare i dati ovunque si trovino..

1 Visibilità dei dati

Ottenere una visione
completa dei dati
all'interno
dell'organizzazione,
mappando e classificando
i dati sensibili



MICROSOFT PURVIEW

Microsoft Purview è una piattaforma completa progettata per aiutare le organizzazioni a gestire, proteggere e governare i dati ovunque si trovino..

2 Protezione dei dati

Proteggere le informazioni sensibili, come la prevenzione della perdita di dati (Data Loss Prevention) e la gestione dei rischi interni (Insider Risk Management)



MICROSOFT PURVIEW

Microsoft Purview è una piattaforma completa progettata per aiutare le organizzazioni a gestire, proteggere e governare i dati ovunque si trovino..

3 Governance dei dati

Gestire i servizi di dati su
ambienti on-premises,
multicloud e SaaS,
garantendo la conformità
alle normative e la
sicurezza dei dati



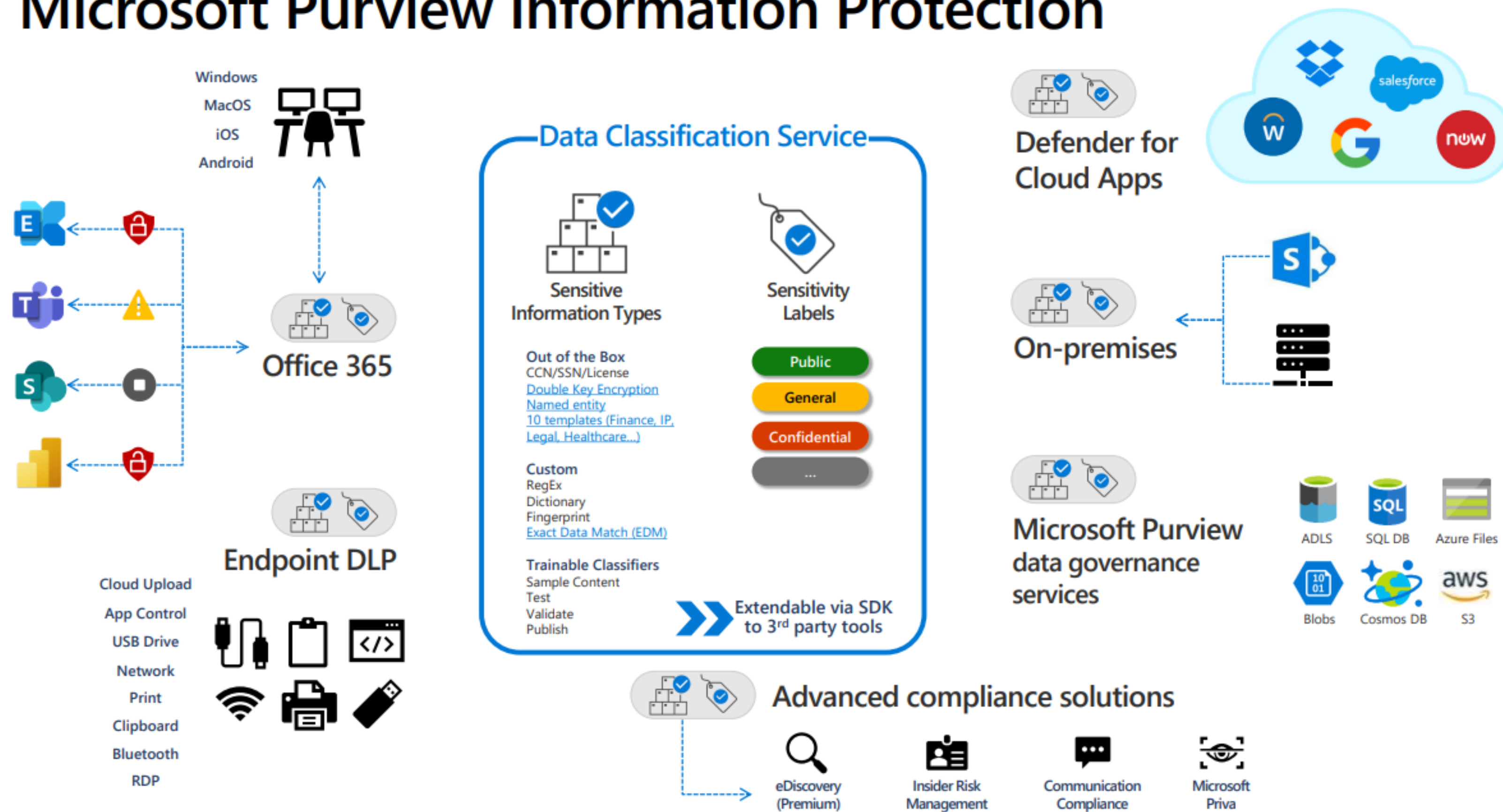
MICROSOFT PURVIEW

Microsoft Purview è una piattaforma completa progettata per aiutare le organizzazioni a gestire, proteggere e governare i dati ovunque si trovino..

4 Gestione dei rischi e conformità

Supporta la gestione dei rischi critici e dei requisiti normativi, creando un ambiente sicuro per l'uso dei dati

Microsoft Purview Information Protection



/ CLASSIFICARE I DATI E APPLICARE ETICHETTE DI RISERVATEZZA UNIFICATE AI DATI SENSIBILI



Excel

Confidential...

Confidential\All Employees • Saving...

MOD Administrator

File name

Confidential Customer List.xlsx

Location

02-Confidential
Contoso » Shared Documents » Seed data

Version History

Sensitivity

admin@M365x02473751.onmicrosoft.com

Personal

Public

General

Confidential

Highly Confidential

Help

Conditional Formatting

Format as Table

Cell Styles

Cells

Editing

Analyze Data

Sensitivity

	C	D	E	F
1	Muhammed MacIntyre	3	-213.25	38.94
2	Barry French	293	457.81	208.16
3	Barry French	293	46.71	8.69
4	Clay Rozendal	483	1198.97	195.99
5	Carlos Soltero	515	30.94	21.78
6	Carlos Soltero	515	4.43	6.64
7	Carl Jackson	613	-54.04	7.3
8	Carl Jackson	613	127.70	42.76
9	Monica Federle	643	-695.26	138.14
10	Dorothy Badders	678	-226.36	4.98
11	Neola Schneider	807	-166.85	4.28
12	Neola Schneider	807	-14.33	3.95
13	Carlos Daly	868	134.72	21.78
14	Carlos Daly	868	114.46	47.98
15	Claudia Miner	933	-4.72	5.28
16	Neola Schneider	995	782.01	30.80

Outlook & OWA

Contoso Electronics

Outlook

Search

New message

U.S. Sales

Private group • 7 members

Send email

This month

U.S. Sales

Sensitivity

Discard

Personal

Public

General

Confidential

Highly Confidential

Anyone (unrestricted)

All Employees

Mobile

Contoso Confidential. Sensitive business data that

M&A Plan –

January 2019, CONTOSO

M&A ID: #CO0151500

An M&A proposal regarding the potential

“Shanghai.” Prepared by the Contoso Merg

department at Contoso, Colorado during Q

Colorado - 319 W. 4th Street, P.O. Box 123

555-1234

Sensitivity

Public

General

Confidential

Highly Confidential

Learn More...

Unified & Built-in: Native labeling across all apps and modalities

AutoSave Project Obsidian Spec.docx Highly Confidential \All Employees

Search (Alt+Q)

MOD Administrator

File Home Insert Draw Design Layout References Mailings Review View Help

Undo Paste Cut Copy Format Painter Clipboard

Font: Segoe UI, 11, Bold, Italic, Underline, Text Color, Background Color

Paragraph: Bullets, Numbering, Indentation, Alignment, Line and Paragraph Spacing

Styles: Normal, No Spacing, Heading 1, Heading 2, Title, Subtitle, Subtle Emphasis

Find, Replace, Select, Dictate, Voice, Sensitivity, Editor, Reuse Files

admin@M365x02473751.onmicrosoft.com

- Personal
- Public
- General >
- Confidential >
- ✓ Highly Confidential >

Project Obsidian

Updated Engine Chip Design

Automated Car Team
Feb 4, 2022

Contacts	Email	Timeline
Lidia Holloway	lidia@contosoelectronics.com	Q4 FY 22

Built-in: End user manual labeling in Office apps across Windows, Mac, iOS, and Android

With our new investments in automated cars we need to redesign the AI500 chip to pull more

Page 1 of 3 156 words Highly Confidential \All Employees Text Predictions: On Accessibility: Investigate

Type here to search

Windows taskbar: Raining now 8:53 AM 2/28/2022

New sensitivity label

- ☒ Name & description
- ☒ **Scope**
- ☐ Files & emails
- ☐ Teams meetings & chats
- ☐ Groups & sites
- ☐ Schematized data assets (preview)
- ☐ Finish

Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

- ☒ **Files & emails**
Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.
- ☒ **Meetings**
Configure access and permission settings for Teams meetings and content restrictions for Teams chats.
- ☒ **Groups & sites**
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.
- ☒ **Schematized data assets (preview)**
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Unified: Labeling across Microsoft 365 & schematized data assets

Microsoft Purview

EA

Edit sensitivity label

✓ Name & description

✓ Scope

● Files & emails

■ Encryption

□ Content marking

□ Auto-labeling for files and emails

□ Teams meetings & chats

□ Groups & sites

□ Schematized data assets (preview)

□ Finish

Encryption

Control who can access files and email messages that have this label applied. [Learn more about encryption settings](#)

☐ Remove encryption if the file or email is encrypted

☒ Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

[Assign permissions](#)

9 items

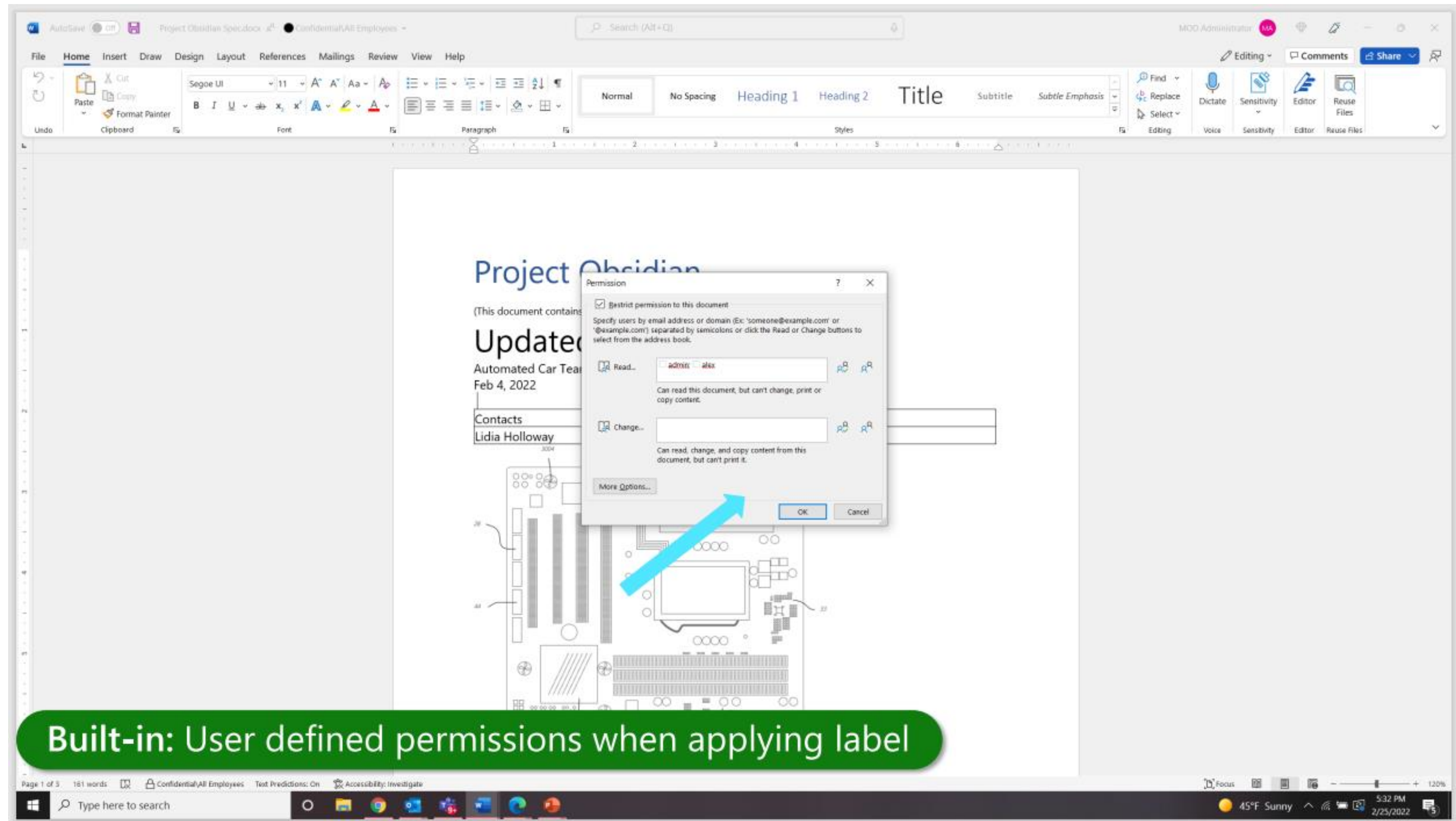
Users and groups	Permissions		
Abraham@ediscodf.onmicrosoft.com	Co-Author		
Carol@ediscodf.onmicrosoft.com	Co-Author		
DeerPark@ediscodf.onmicrosoft.com	Co-Author		
FBIACComplianceTeam@ediscodf.onmicrosoft.com	Co-Author		
Russel@ediscodf.onmicrosoft.com	Co-Author		
allemployees@ediscodf.onmicrosoft.com	Co-Author		
ediscodf.onmicrosoft.com	Co-Author		
test@ediscodf.onmicrosoft.com	Co-Author		
tu1@ediscodf.onmicrosoft.com	Co-Author		

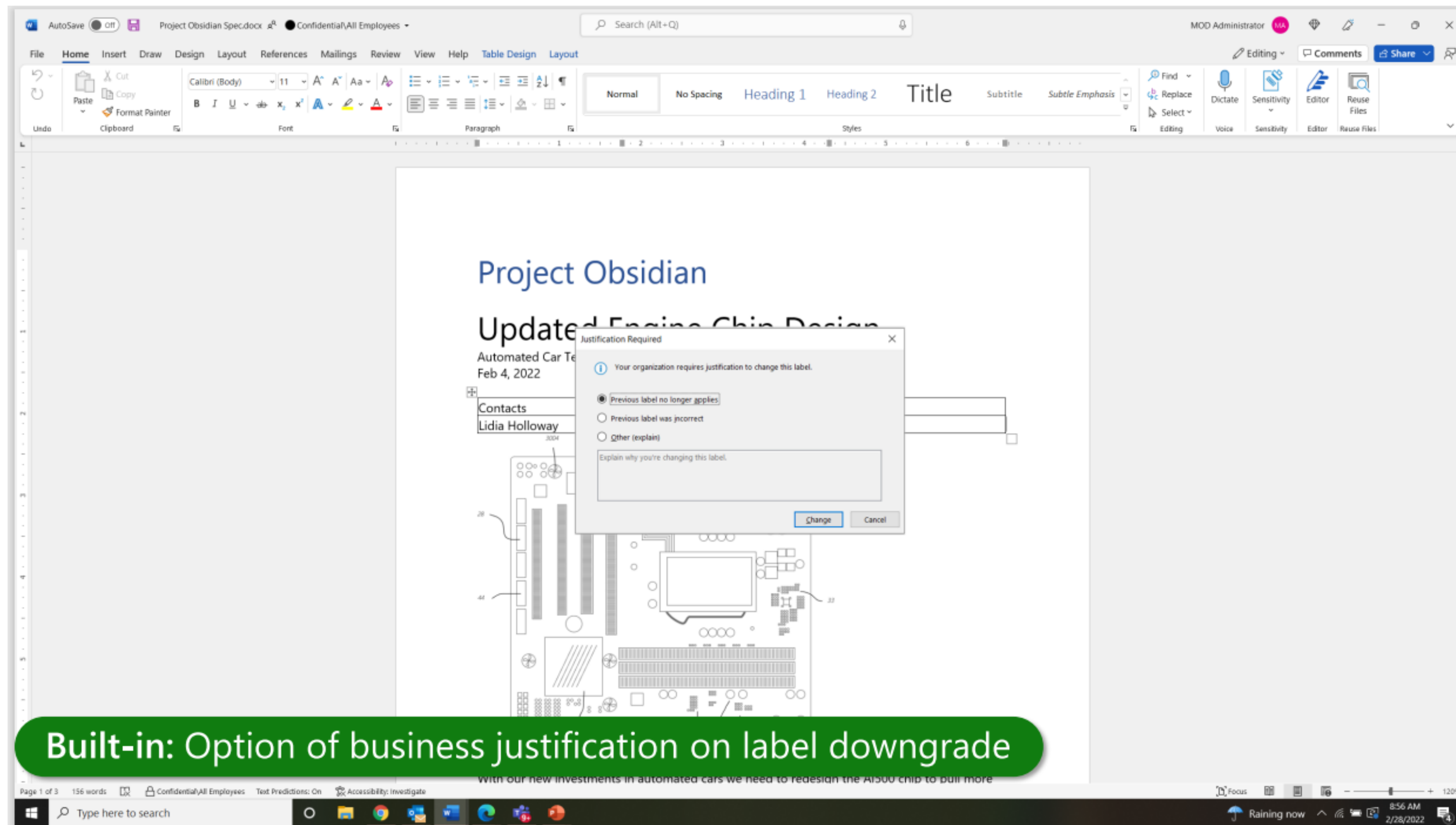
Unified: Double key encryption & User defined permissions protection

Back

Next

Cancel





Microsoft Purview

Auto-labeling > New policy

Info to label

Name

Locations

Policy rules

Label

Policy mode

Finish

Choose info you want this label applied to

Choose an industry regulation to see the policy templates you can use to classify that info or create a custom policy to start from scratch.

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Search for specific templates

All countries or regions

Categories

Financial

Medical and health

Privacy

Custom

Enhanced

Templates

U.S. Gramm-Leach-Bliley Act (GLBA) Enhanced

Australia Health Records Act (HRIIP Act) Enhanced

U.S. Health Insurance Act (HIPAA) Enhanced

Australia Privacy Act Enhanced

General Data Protection Regulation (GDPR) Enhanced

Japan Personally Identifiable Information (PII) Data Enhanced

Japan Protection of Personal Information Enhanced

U.S. Patriot Act Enhanced

U.S. Personally Identifiable Information (PII) Data Enhanced

U.S. State Breach Notification Laws Enhanced

U.S. Health Insurance Act (HIPAA) Enhanced

Helps detect the presence of information subject to United States Health Insurance Portability and Accountability Act (HIPAA). This enhanced template extends the original by also detecting people's full names, medical terms and conditions, and U.S. physical addresses.

Protect this information:

- PII Identifiers
- ICD-9/10 code descriptions
- All Full Names
- All Medical Terms And Conditions
- U.S. Physical Addresses

Trainable classifiers

Search

Select all

Source code

Microsoft Corporation

Offensive language

Microsoft Corporation

Harassment

Microsoft Corporation

Profanity

Microsoft Corporation

Threat

Microsoft Corporation

Project Obsidian

Contoso

Add

Cancel

Intelligent: OOB & Custom classifiers to label data

RESOLVE
by ErgonGroup

Riproduzione riservata @Resolve

Microsoft Purview

Home

Compliance Manager

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Trials

Solutions

Catalog

App governance

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Data lifecycle management

Information protection

Information Barriers

Privacy Risk Management

Information protection > General Data Protection Regulation (GDPR) Enhanced

General Data Protection Regulation (GDPR) Enhanced

Turn on policyRestart simulationEdit policyDelete policy

Simulation overviewItems to review

Recommendation

Turn on policy or review sample of matching files

We've done detecting all files that match your policy, but we're still putting together sample files to review. You can review the ones we've gathered so far or, if you're satisfied with the results, turn on the policy now. It will take around 1 day to apply the label to matching files in your org.

Turn on policyReview matching files

Files ready to review

47 matched files to review

Number of files displayed is a sample of the total matching files from each site included in the policy (up to 100 files per site).

Sensitive info types

Total matching files per policy rule

47 matching files from 63 sites

Breakdown of how many files match your policy's rules. When the policy is turned on, it will take around 1 day to apply the label to these files.

Rule	Location	Matched items
General Data Pro...	OneDrive	24
General Data Pro...	SharePoint	23

Details

Policy name

General Data Protection Regulation (GDPR) Enhanced

Status

Simulation complete

Simulation start date/time

Yesterday at 5:21 PM

Label and policy settings

LabelConfidential/All Employees

Exchange overwrite labelfalse

Info to label

Austria Physical Addresses

Belgium Physical Addresses

Bulgaria Physical Addresses

Croatia Physical Addresses

Cyprus Physical Addresses

Czech Republic Physical Addresses

Denmark Physical Addresses

Estonia Physical Addresses

Finland Physical Addresses

France Physical Addresses

Germany Physical Addresses

Greece Physical Addresses

Hungary Physical Addresses

Ireland Physical Addresses

Italy Physical Addresses

Latvia Physical Addresses

Lithuania Physical Addresses

Luxembourg Physical Addresses

Malta Physical Addresses

Netherlands Physical Addresses

Poland Physical Addresses

Portuguese Physical Addresses

Romania Physical Addresses

Intelligent: Simulation mode to test policy effectiveness

RESOLVE

by ErgonGroup

Riproduzione riservata @Resolve

EMPOWERING DEFENDER E PURVIEW

/ 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

/ Super Early Bird fino al 31/05

**CLOUD
CONFERENCE
ITALIA**

=



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

/ IT & Microsoft Training



Resolve è partner di Upskill, Società specializzata nella **formazione e nei servizi formativi**, che accompagna aziende, persone e istituzioni nello sviluppo di percorsi di alta formazione manageriale.

Scopri i corsi per IT Manager, Sistemisti, Data Analyst, Sviluppatori e Utenti finali.

CORSI MICROSOFT

CORSI DIGITAL & IT

CORSI TRAINING UTENTE



RESOL/E

EMPOWERING INTUNE E ENTRA ID

/ 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