Seguridad y Privacidad del dato en tiempos de IA Generativa

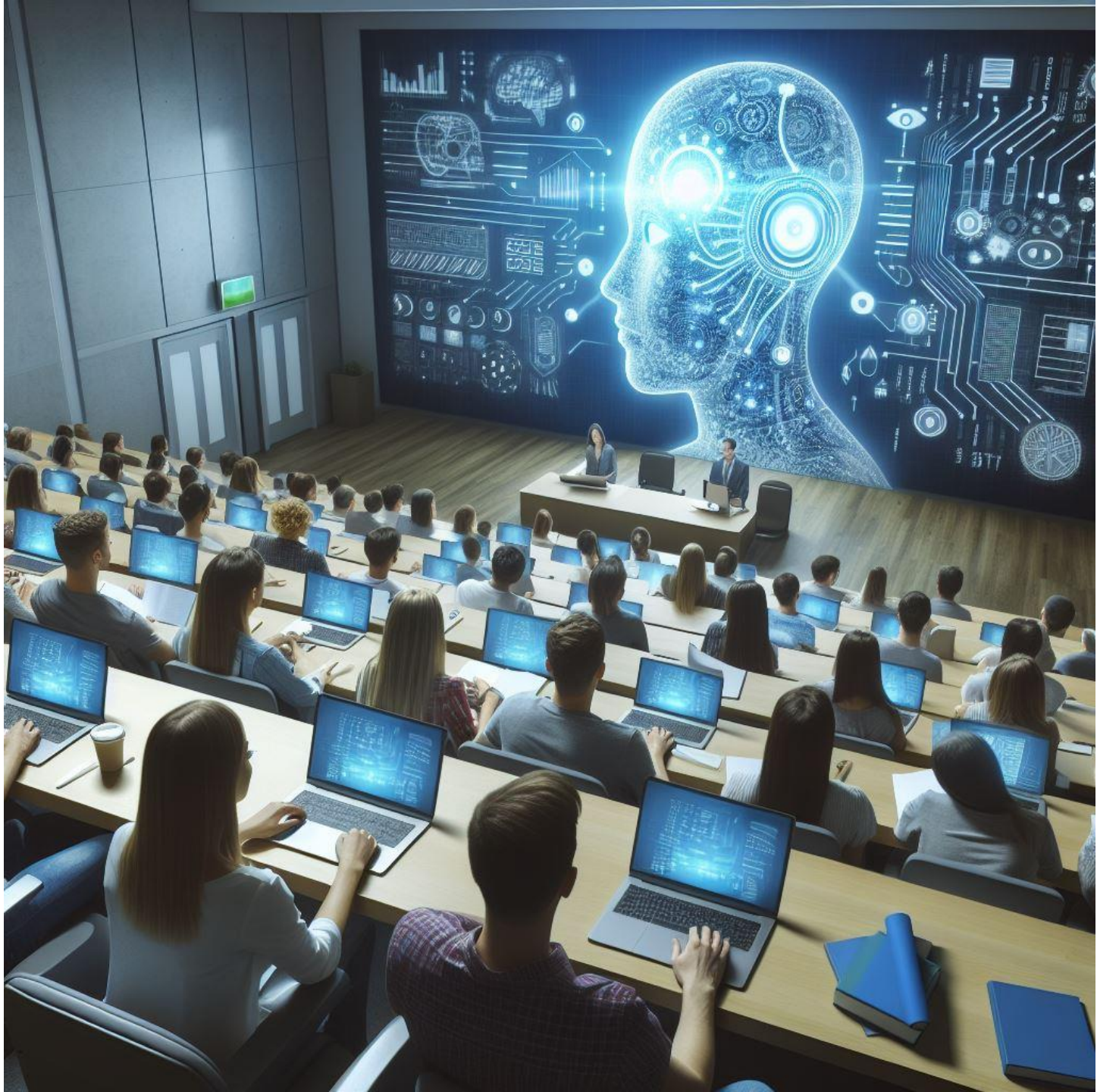
Pedro Moreno
Head of MW & Security | Microsoft Education

Mamen Ugarte
Head of Azure | Microsoft Education

Vicente Alcaraz
Head of Software & Cloud | Bechtle

Microsoft

BECHTLE



Contenidos

Ciberataques en instituciones educativas

Panorama actual

4305

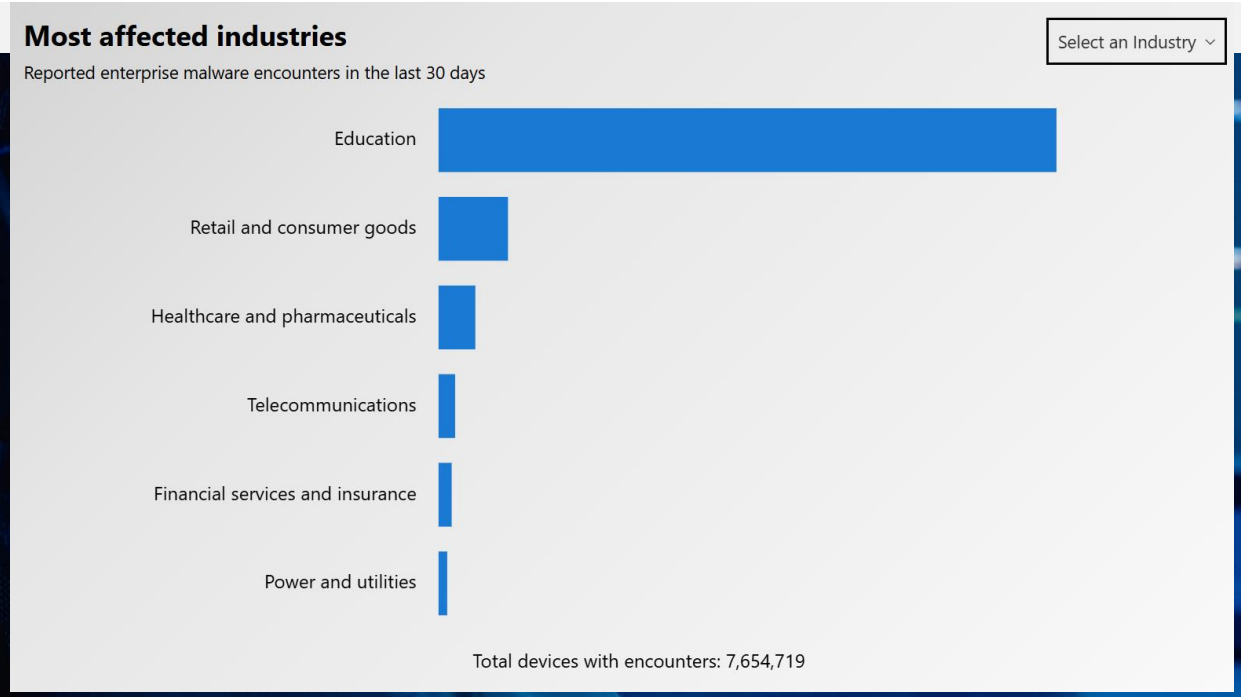
Instituciones educativas afectadas por ataques de ransomware

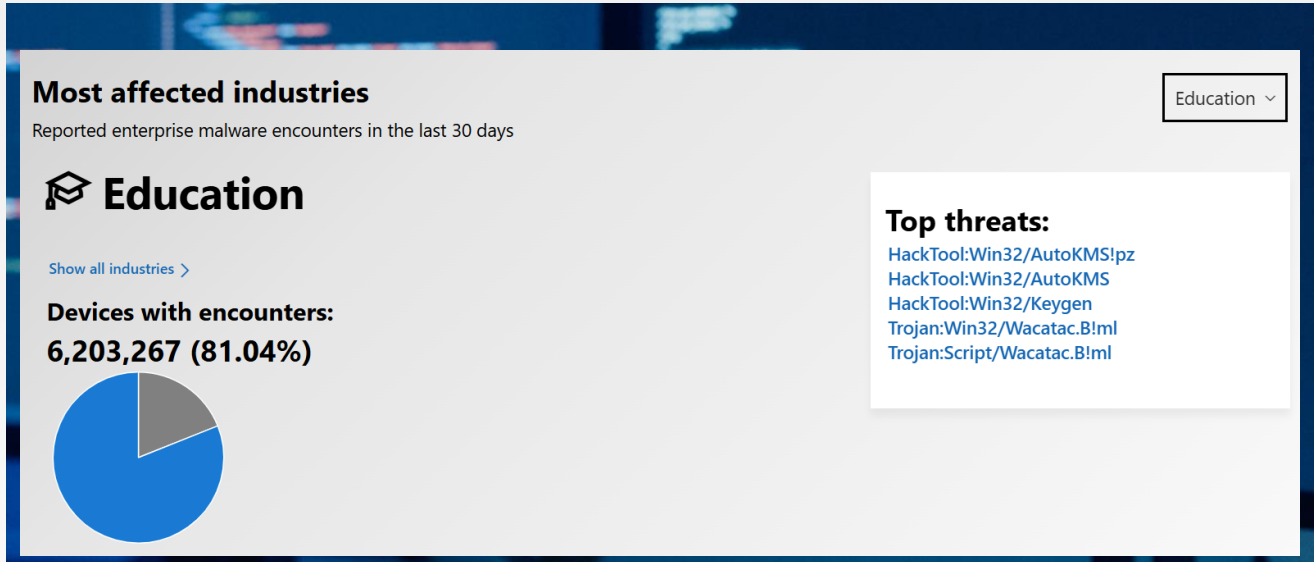
61%

Ataques generados por robo o extracción por fuerza bruta de credenciales

$20B

Costes por recuperación y por quedarse fuera de servicio



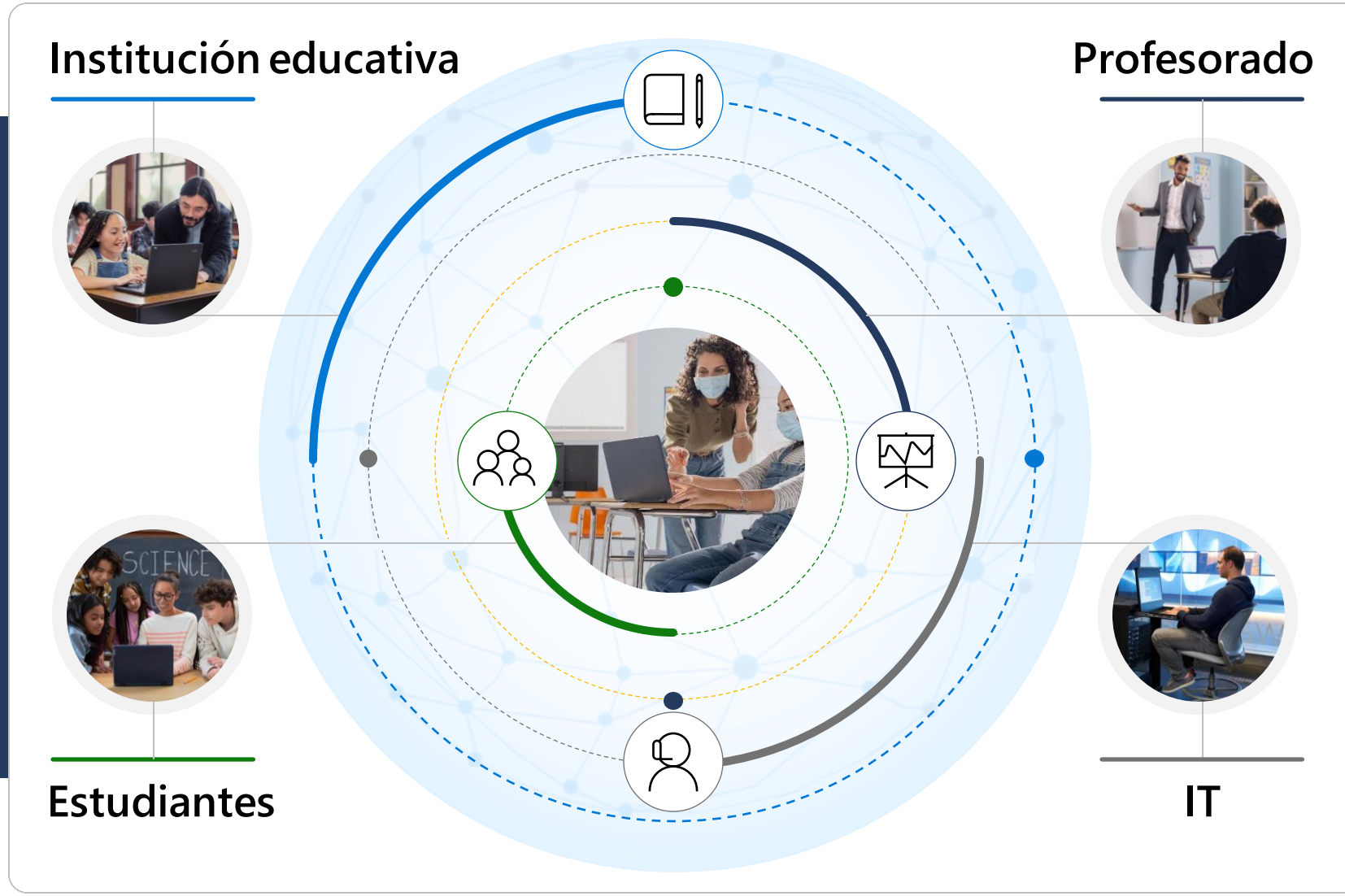


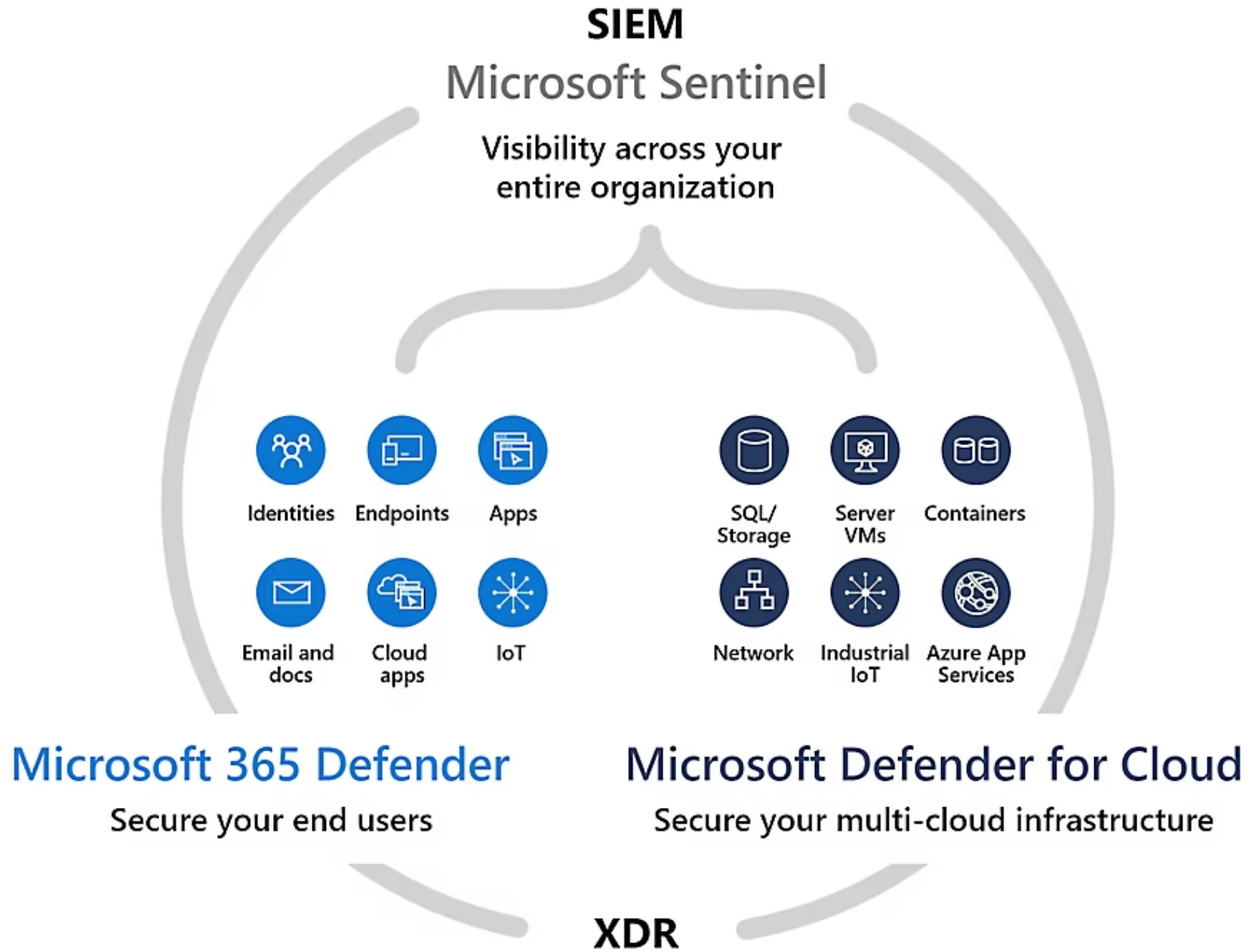
Protege tu institución educativa de los riesgos de un ciberataque

Microsoft 365 Security

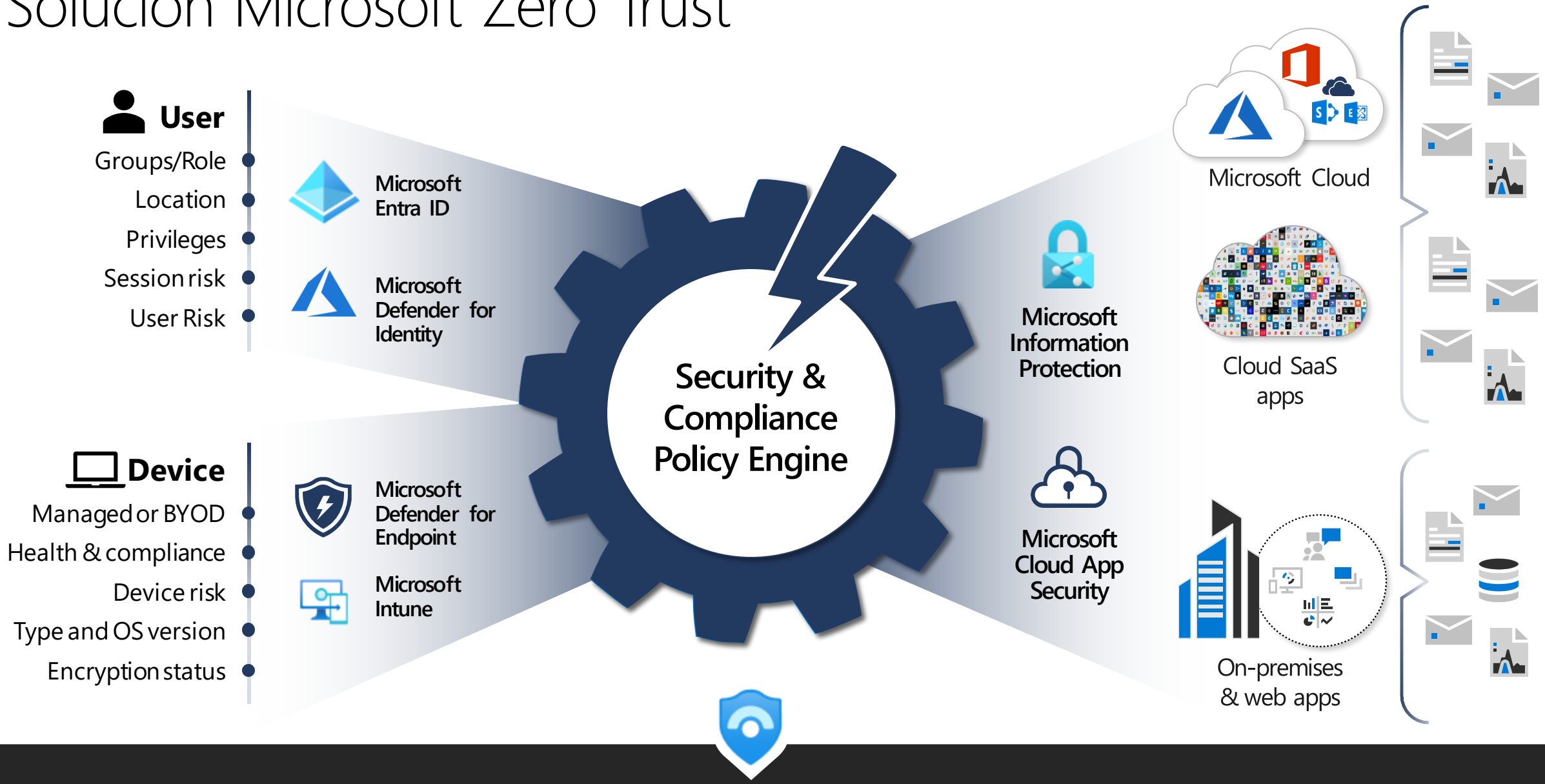
Experiencias educativas seguras mediantes

- Solución única
- Eficiente en costes




SIEM
Microsoft Sentinel
Visibility across your entire organization
Identities
Endpoints
Apps
Email and docs
Cloud apps
IoT
SQL/ Storage
Server VMs
Containers
Network
Industrial IoT
Azure App Services
Microsoft 365 Defender
Secure your end users
Microsoft Defender for Cloud
Secure your multi-cloud infrastructure
XDR

Solución Microsoft Zero Trust



Protección a lo largo de una cadena de ataques

Microsoft for Cloud App and Purview

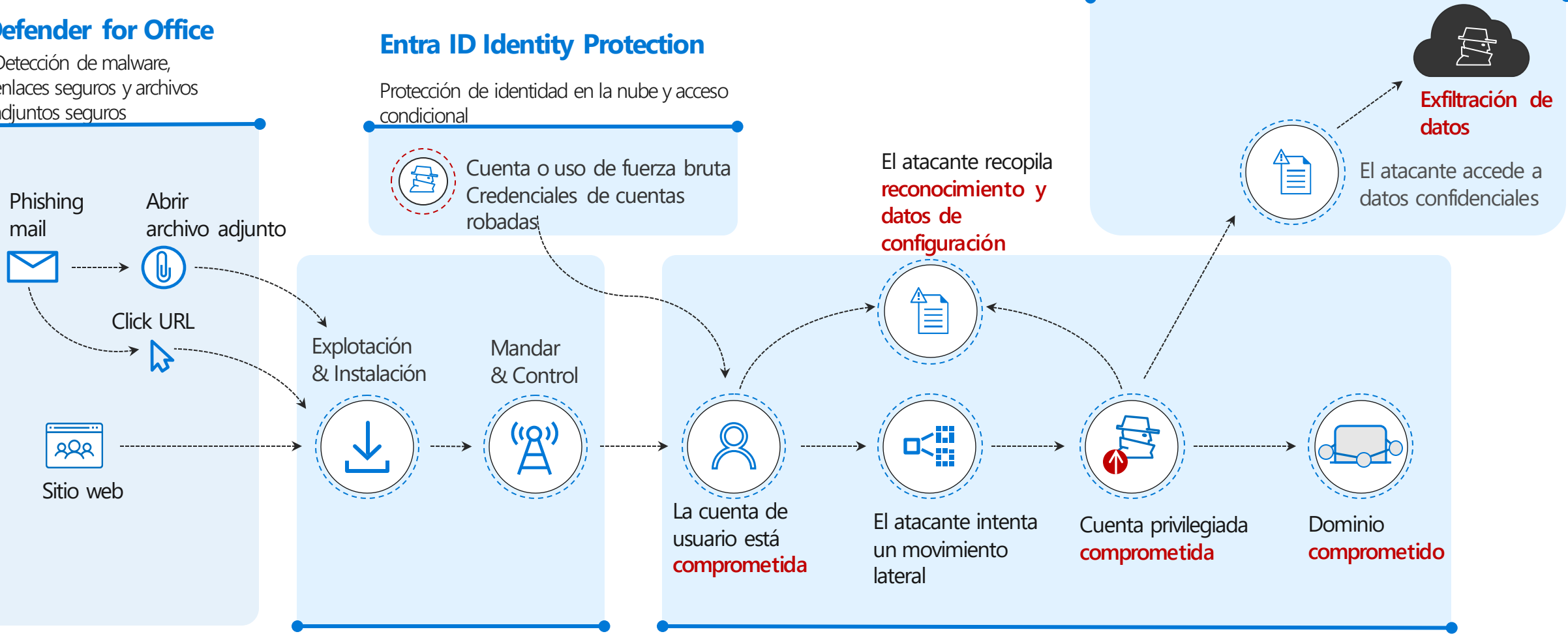
Extiende la protección y el acceso condicional a otras aplicaciones en la nube

Defender for Office

Detección de malware, enlaces seguros y archivos adjuntos seguros

Entra ID Identity Protection

Protección de identidad en la nube y acceso condicional



Defender for Endpoints

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

Defender for Identity

On-premises identity protection

Protect it all
with Microsoft Security

News Analyst reports Microsoft Defender for Endpoint · 5 min read

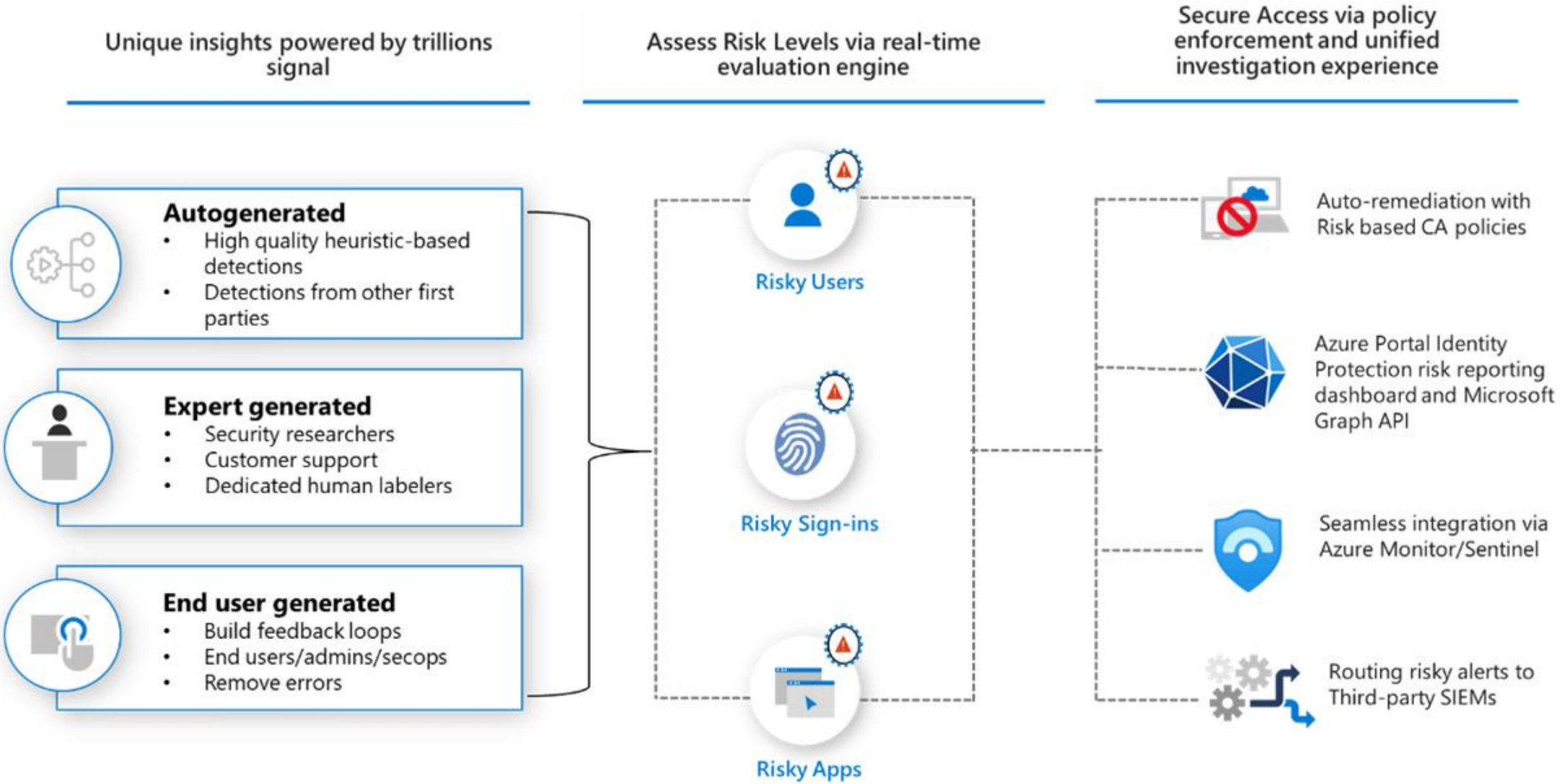
Microsoft is named a Leader in the 2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

By Rob Lefferts, Corporate Vice President, Microsoft Threat Protection

Protección de la Identidad

Microsoft

Protección de la identidad



Protección de la Información

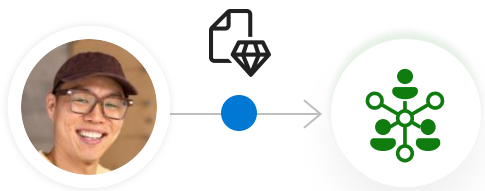
Microsoft

La IA aflora la falta de gobernanza de nuestros datos

Visibilidad insuficiente del uso de aplicaciones de IA puede dar lugar a problemas de seguridad y cumplimiento.

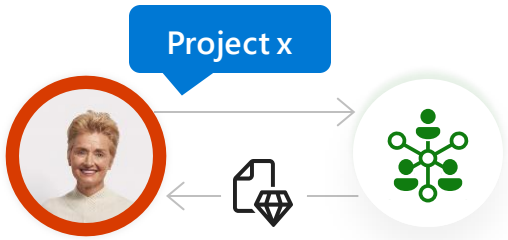
1

Fuga de datos:
Los usuarios pueden filtrar sin intención datos confidenciales a las aplicaciones de IA



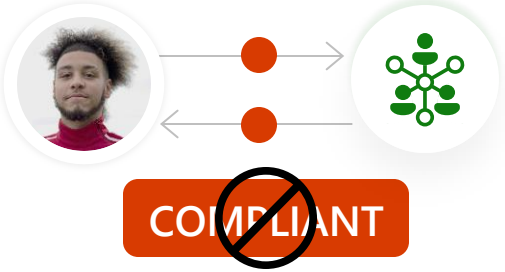
2

Intercambio excesivo de datos:
Los usuarios pueden acceder a datos confidenciales a través de aplicaciones de IA que no están autorizados a ver/editar

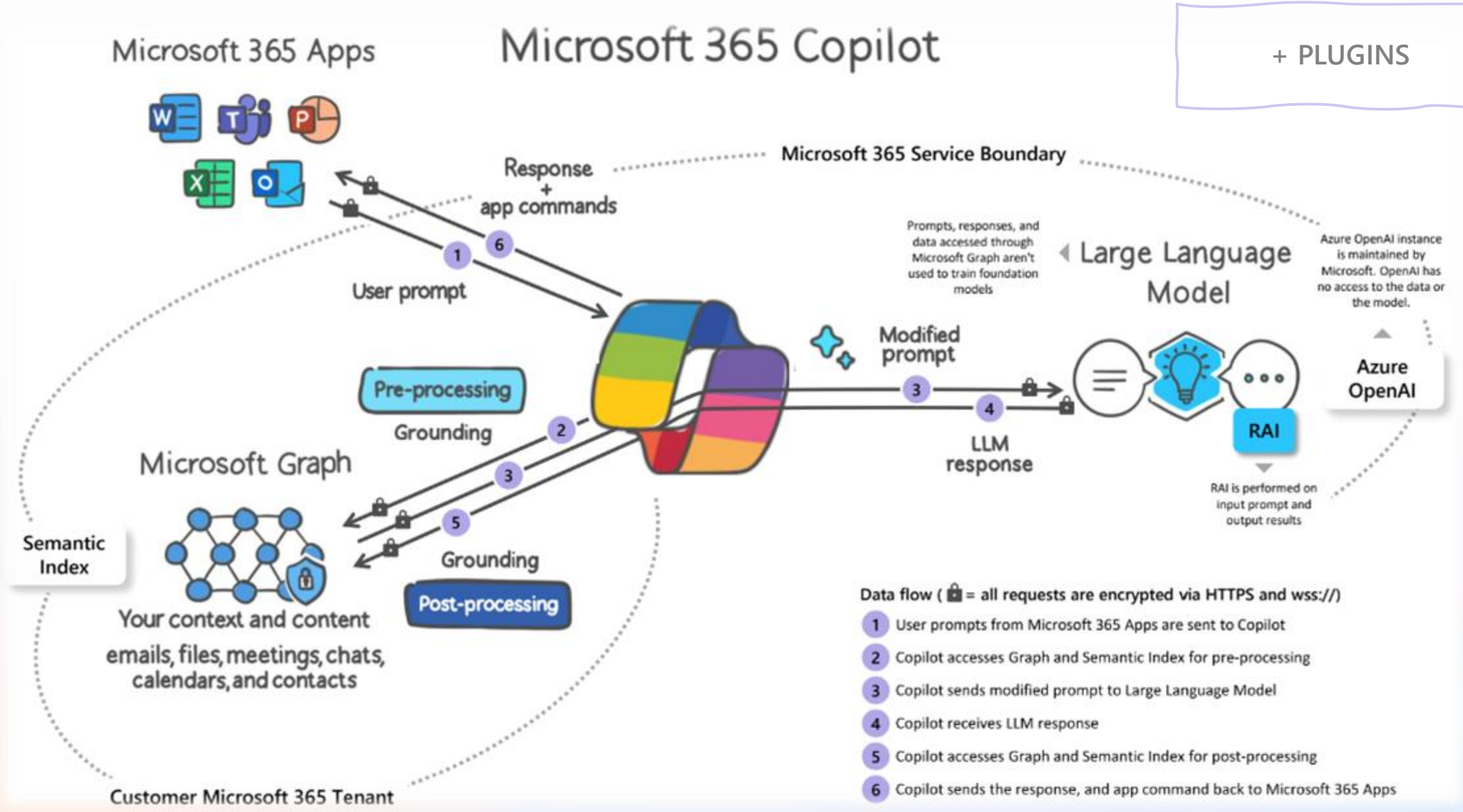


3

Uso de incumplimiento:
Los usuarios utilizan aplicaciones de IA para generar contenido poco ético u otro contenido de alto riesgo



Arquitectura básica - Microsoft 365 Copilot



Responsabilidades compartidas de seguridad para el uso de IA para Microsoft Copilot

Acceso al entorno de producción

Configure controles de acceso que restrinjan estrictamente el acceso permanente a los datos del cliente o al entorno de producción

Proteger los datos

Cifre los datos en reposo y en tránsito en función de los estándares industriales (BitLocker, TLS, etc.)

Acceso a aplicaciones de IA

Configure la política de control de acceso, aprovechando las soluciones de gestión de identidades y accesos

Proteja y controle los datos introducidos y creados por las aplicaciones de IA

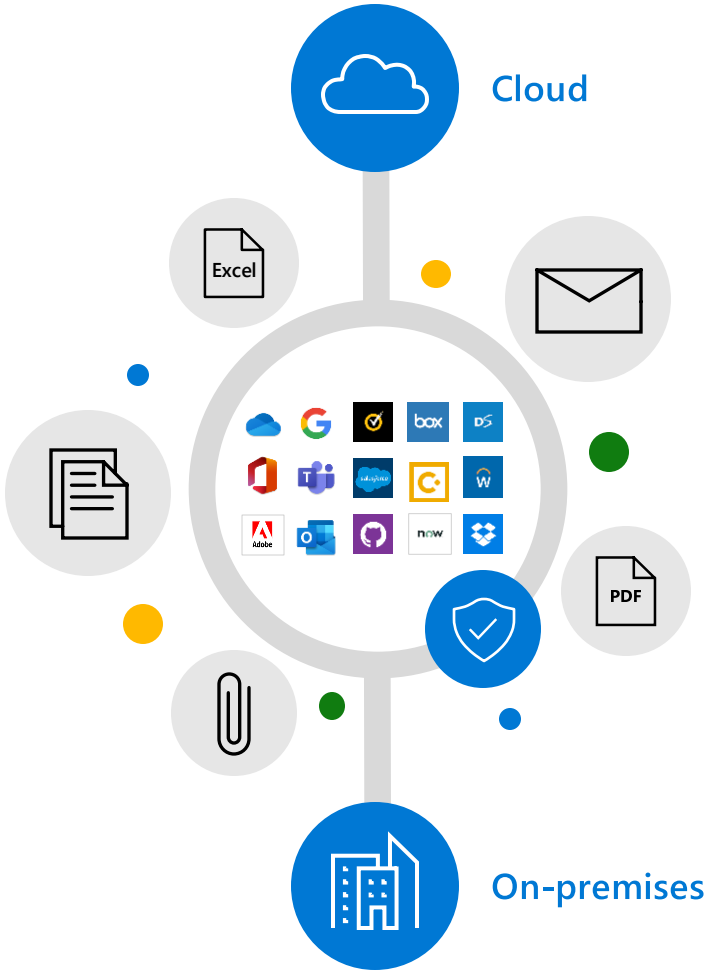
Aplique controles de seguridad y cumplimiento de datos en los datos en las interacciones de IA.

Responsabilidad del usuario sobre el uso de la IA

Implemente y opere la capacitación en seguridad de IA en toda la organización

Microsoft Purview Information Protection

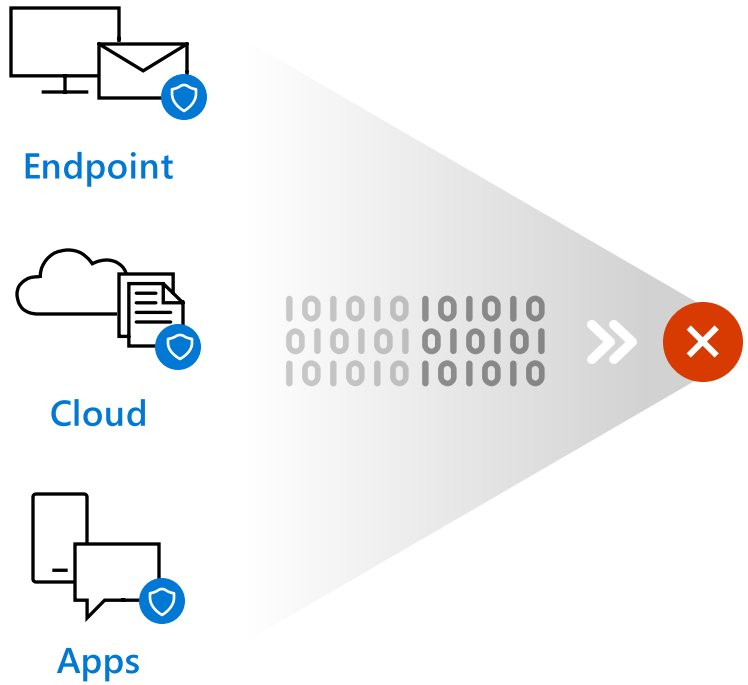
Una solución inteligente, integrada y extensible para conocer y proteger los datos confidenciales



- Descubra y clasifique datos a escala mediante la automatización y el aprendizaje automático
- Etiquetado y protección integrados
- La plataforma amplía la experiencia de protección
- Cifrado integrado en Microsoft 365: en reposo, en tránsito y en uso

Microsoft Purview Data Loss Prevention

Evite el intercambio accidental o no autorizado de datos confidenciales



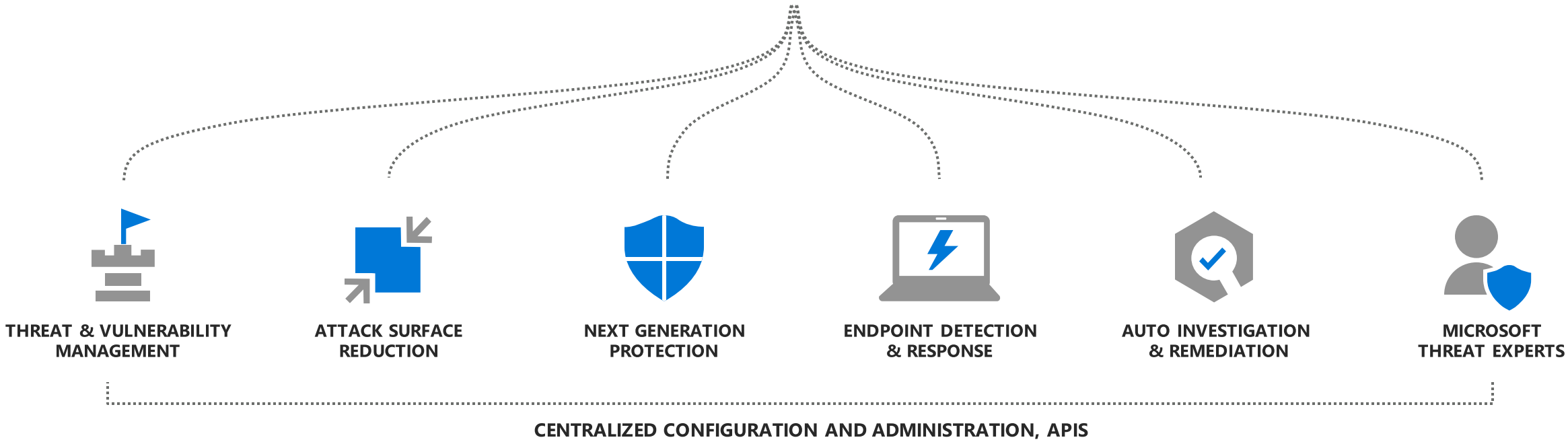
- Aplique automáticamente el cumplimiento de las regulaciones y las políticas internas en la nube y en las On-Premises
- Amplíe la directiva DLP a los endpoints, a los recursos compartidos de archivos locales, a las aplicaciones de usuario, a los exploradores y a los servicios
- Aplique una administración de políticas flexible para equilibrar la productividad de los usuarios

Protección de los Dispositivos

Microsoft

Microsoft Defender for Endpoint

Built-in. Cloud-powered.

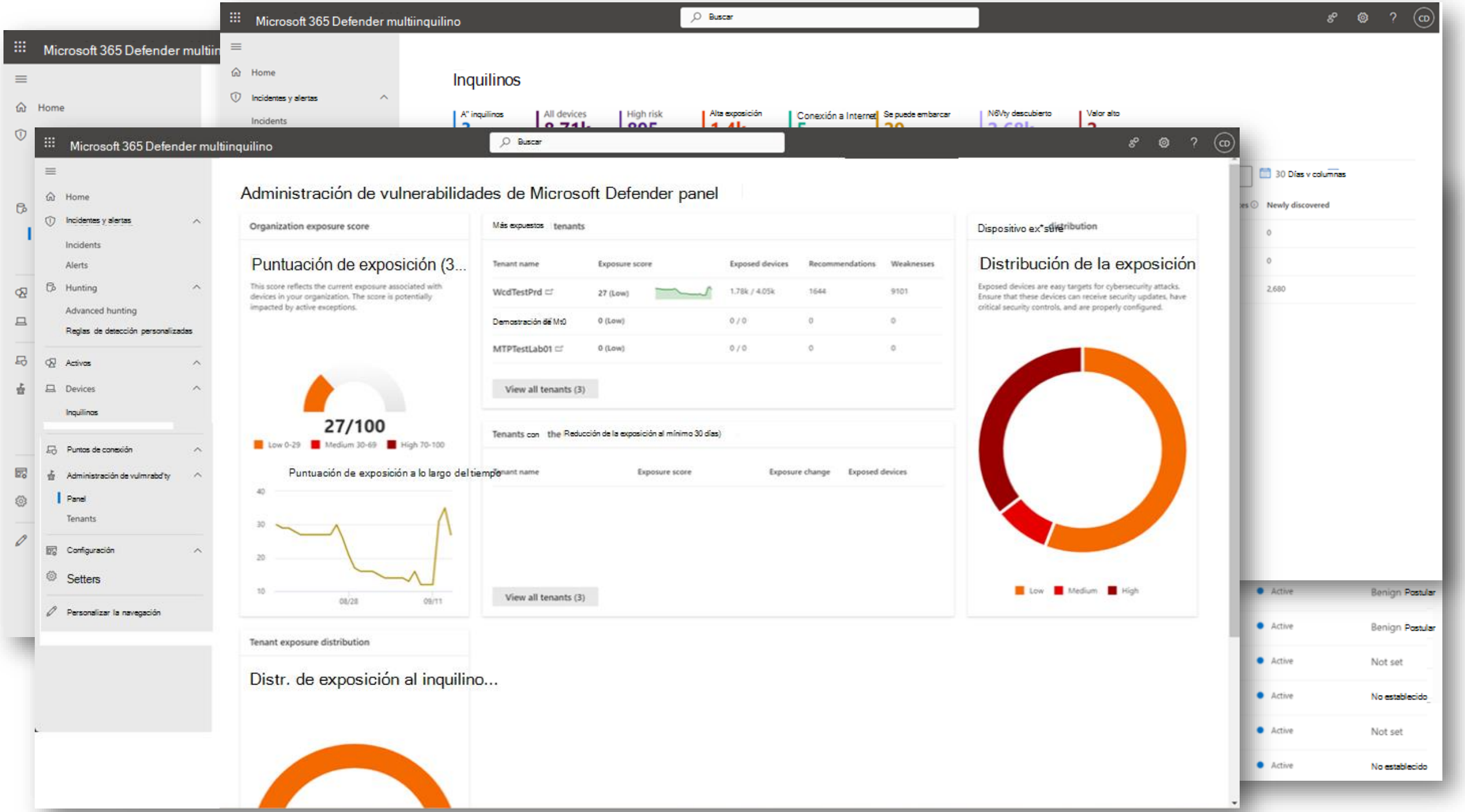


Microsoft Defender for Endpoint

Built-in. Cloud-powered.

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL blocking	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
API's, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts **		✓

** Includes Targeted Attack Notifications (TAN) and Experts on Demand (EOD). Customers must apply for TAN and EOD is available for purchase as an add-on.


Microsoft 365 Defender multiinquilino
Buscar
Home
Incidentes y alertas
Incidents
Inquilinos
Microsoft 365 Defender multiinquilino
Buscar
Home
Incidentes y alertas
Incidents
Alerts
Hunting
Advanced hunting
Reglas de detección personalizadas
Activos
Devices
Inquilinos
Puntos de conexión
Administración de vulnerabilidad
Panel
Tenants
Configuración
Setters
Personalizar la navegación
Administración de vulnerabilidades de Microsoft Defender panel
Organization exposure score
Puntuación de exposición (3...
This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.
27/100
Low 0-29
Medium 30-69
High 70-100
Puntuación de exposición a lo largo del tiempo
40
30
20
10
08/28
09/11
Más expuestos
tenants
Tenant name
Exposure score
Exposed devices
Recommendations
Weaknesses
WcdTestPrd
27 (Low)
1.78k / 4.05k
1644
9101
Demostración de MtO
0 (Low)
0 / 0
0
0
MTPTestLab01
0 (Low)
0 / 0
0
0
View all tenants (3)
Tenants con
the
Reducción de la exposición al mínimo 30 días)
Tenant name
Exposure score
Exposure change
Exposed devices
View all tenants (3)
Dispositivo exposure distribution
Distribución de la exposición
Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.
Low
Medium
High
Tenant exposure distribution
Distr. de exposición al inquilino...
30 Días y columnas
Newly discovered
0
0
2,680
Active
Benign Postular
Active
Benign Postular
Active
Not set
Active
No establecido
Active
Not set
Active
No establecido

Protección de Cargas onprem & Multinube

Microsoft

Microsoft Defender For Cloud

Evalúe, proteja y defienda sus cargas de trabajo híbridas y multinube

Fortalezca y administre su postura de seguridad

Secure configuration of resources

Management of compliance requirements

Detecte amenazas y proteja sus cargas de trabajo

Full-stack threat protection

Vulnerability assessment & management

Responda y automatice

Assess and resolve security alerts and incidents

Automate response

Automate with the tools of your choice

Microsoft Azure

Amazon Web Services

Google Cloud Platform

On-prem

Cobertura completa con detecciones dedicadas

Compute

- Any server
- Azure VMSS
- App Services
- Azure K8s
- Unmanaged K8s

Service Layer

- Azure DNS
- Key Vault
- Network Layer V1
- Resource Manager

Databases and Storage

- Blob storage
- File storage
- Maria DB
- Azure Cosmos DB
- Azure SQL
- MySQL
- Postgres SQL
- Unmanaged SQL

AWS workloads

- Amazon EKS
- Amazon EC2
- Unmanaged Kubernetes
- Unmanaged SQL

GCP workloads

- GKE clusters
- Google Compute
- Unmanaged Kubernetes
- Unmanaged SQL

On-premise workloads

- Kubernetes
- SQL Servers
- Servers

On-premise

Arc-enabled Security

Seguridad y gobernanza consistentes para su computación híbrida y multinube.

Microsoft Defender

Azure Monitor

Microsoft Sentinel

Azure Policy

Azure Update Manager

Azure Security across your infrastructure

Muévase más rápido con la detección y respuesta simplificadas a las amenazas

Infrastructure

Devices

Users

Applications

Microsoft Defender for cloud

Microsoft 365 Defender

Visión completa

Modernice sus operaciones de seguridad con Microsoft Sentinel

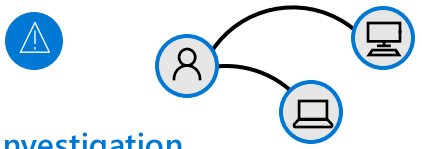
Cloud-native

Powered by AI

300+ partner integrations

Built-in automation

Detection
Correlate alerts into actionable incidents using machine learning



Investigation
Visualize the full scope of an attack

Response
Act immediately with built-in automation

Threat hunting
Hunt across all data with powerful search and query tools

Across multicloud, multiplatform

Powered by community + backed by Microsoft security experts

SIEM+XDR

SIEM+XDR
Learn more

Soluciones que ayudan a prevenir, detectar y responder a las amenazas a las que se enfrentan las universidades.

SIEM

Security Information and Event Management

Combina la gestión de la información de seguridad (SIM) y la gestión de eventos de seguridad (SEM) en un solo sistema de gestión de la seguridad

Microsoft Sentinel

XDR

Extended Detection and Response

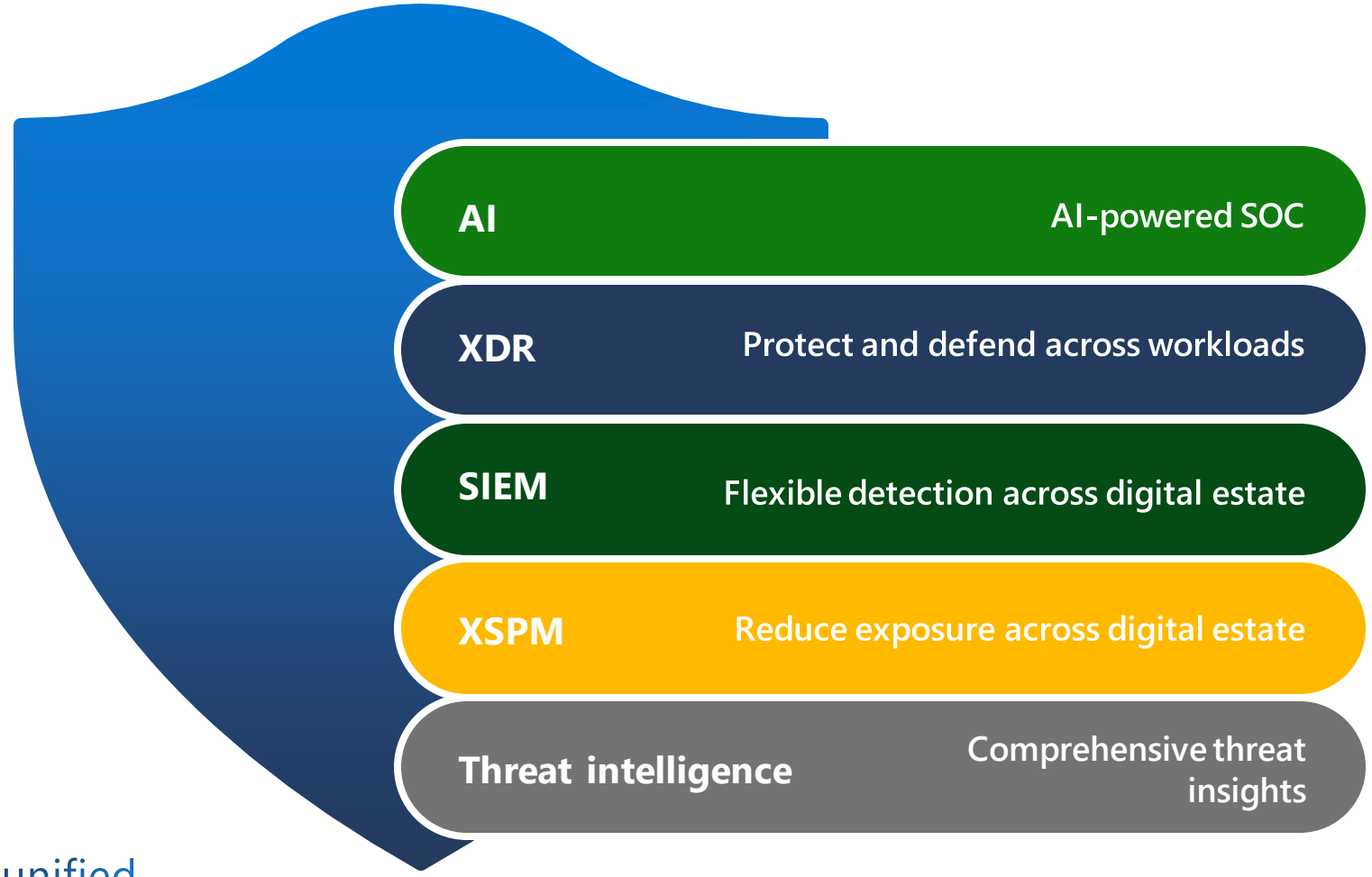
Ofrece un enfoque unificado y eficiente para prevenir, detectar y responder a amenazas sofisticadas como malware y ransomware

Microsoft 365 Defender

Microsoft 365 Defender for Cloud

Es hora de una plataforma unificada de operaciones de seguridad

Experiencia optimizada del analista | Asistencia específica | Protección y corrección automatizadas



- Generative AI
- Automation
- AI-enhanced features

- Detection and response across endpoints, clouds, applications, identity and other native workloads
- Investigation
- Response
- Threat hunting
- Incident management

- Monitoring everything
- Investigation
- Reporting
- UEBA
- SOAR
- Dashboarding
- Threat hunting
- Storage

- Broad asset coverage
- Attack path analysis
- Prioritized actions

- Threat actor profiles
- Infrastructure analysis
- Latest threat research
- Global insights

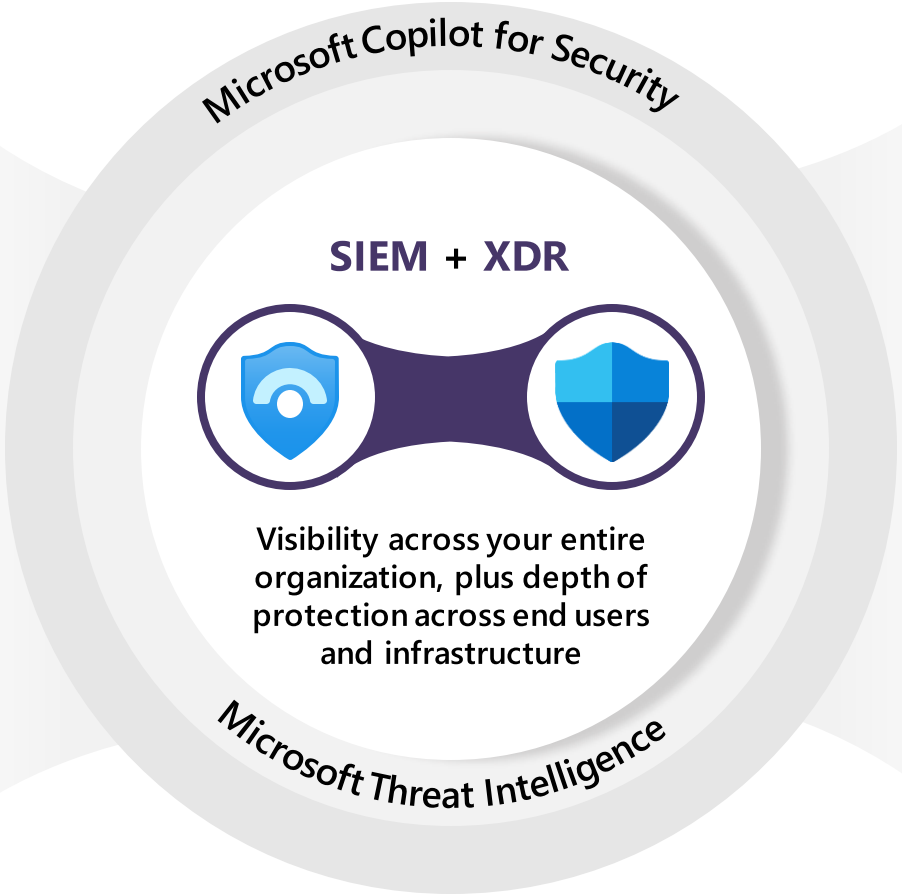
unified

Una única plataforma para todos sus datos de seguridad

Experiencia unificada de detección, investigación y respuesta.

300+ fuentes de datos que incluyen:

- Infrastructure
- Microsoft Azure
- Data
- Google Cloud Platform
- Android
- ServiceNow
- iOS
- Palo Alto
- CrowdStrike
- Email and collaboration
- Linux
- Applications
- Hybrid identities
- Amazon Web Services
- Cloud apps
- Windows
- SAP
- macOS
- Salesforce
- Endpoints and IoT
- Users
- Oracle
- Cisco
- Jira



- Prevenir
- Detectar
- Investigar
- Responder

Microsoft Defender

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

- Home
- Investigation & response
  - Incidents & Alerts
  - Hunting
  - Actions & submissions
  - Partner catalog
- Microsoft Sentinel
  - Search
  - Threat management
  - Content management
  - Configuration
- Threat intelligence
- Assets
- Endpoints
- Email & collaboration
- Cloud apps
- Optimize
- Reports
- Learning hub
- Trials
- More resources
- System

Key metrics indicate a positive trend in your organization's efficiency

The average time it takes to respond to and close incidents has decreased.

Mean time to acknowledge
10 minutes
↓ 65%

Mean time to close
3 minutes
↓ 25%

Time saved by automation
300 hours
↑ 82%

Guided Tour | Customize page

Unified incidents and alerts

145 active incidents

Service sources: Defender XDR, Sentinel, Defender for Cloud, Endpoint, Office, and Applications

In progress	Resolved
24	57

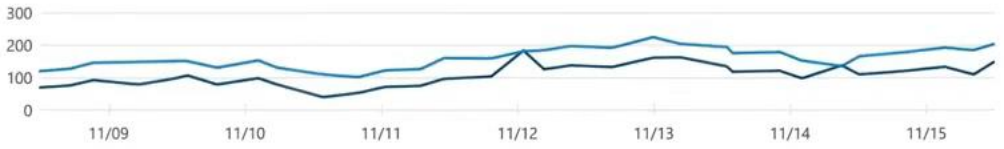
Active incidents by severity

High | Medium | Low | Informational

Closed incidents by classification

True positive | False positive | Benign positive | Undetermined

Closed incidents and alerts over time



View all incidents

Sentinel automation

33 automation rules

Closed incidents	Time saved	Actions performed
6	23 hours	259

Actions performed by type

Severity | Owner | Status | Comments

Configure automation rules | View workbook

Entities from Sentinel

Discovered entities related to incidents

12.3K Hosts

11.8K IPs

1.6k Azure resources

View all entities

Featured Threat intelligence articles

Storm-0062 attempts to exploit CVE 2023-22515 in Atlassian Confluence

Storm-0062

1 day ago | 5 indicators

Diamond Sleet compromises TeamCity servers

Diamond Sleet | T1584-Comrimise infrastru... | +2

6 day ago | 15 indicators

WS FTP Server critical vulnerabilities

T1190 - Exploit Public-Facin...

7 days ago | no indicators

Threat overview: Exfiltration

TA0010 - Exfiltration

9 days ago | no indicators

See more in Intel explorer

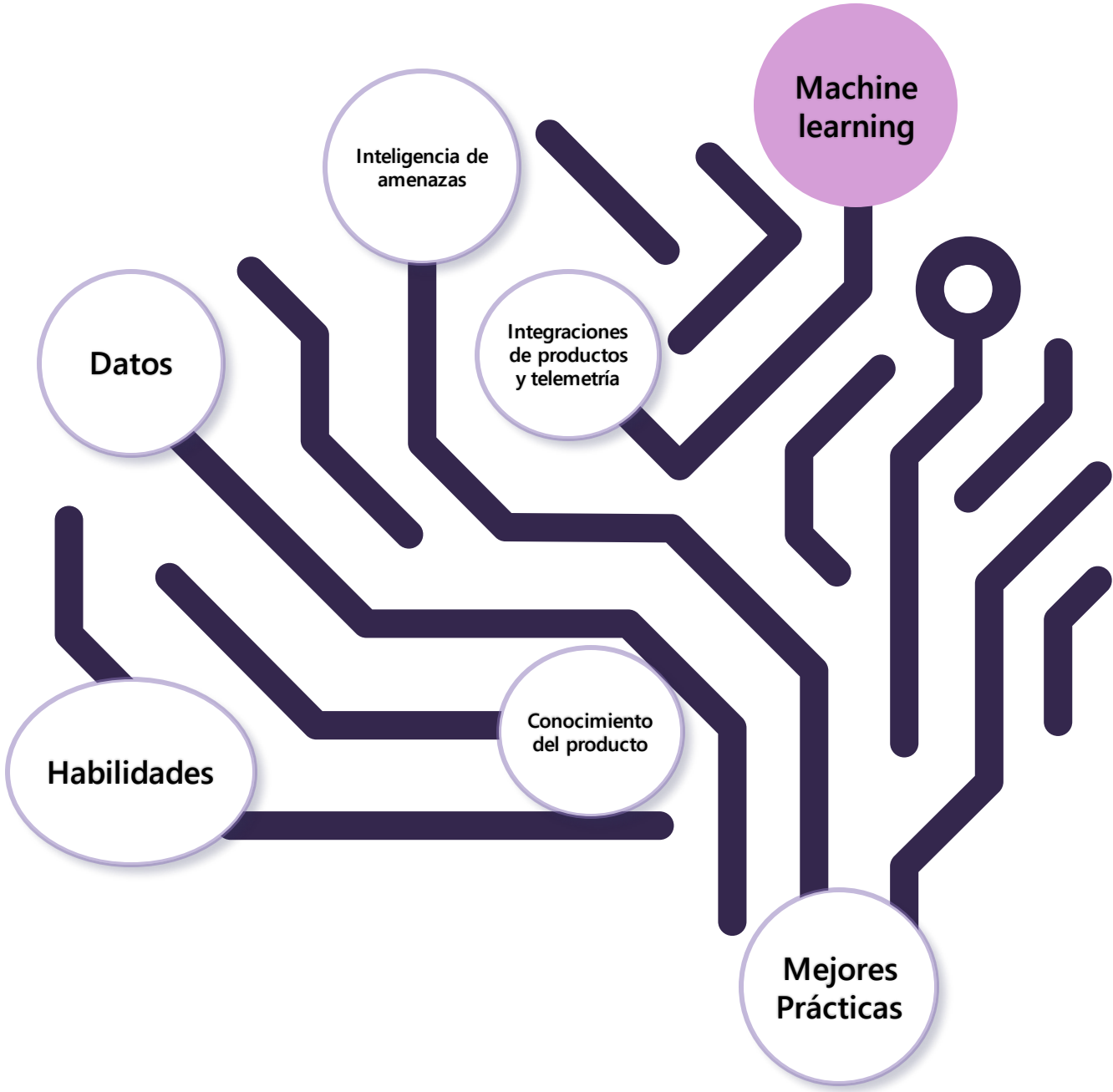
Sentinel data connectors

SOC optimization

Secure score

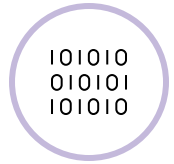
Microsoft Copilot for Security

El primer producto de seguridad de IA generativa que permite a los equipos de seguridad y TI defenderse a la velocidad y escala de las máquinas

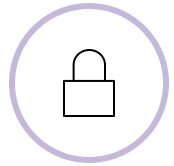


Construido con seguridad, privacidad y cumplimiento.

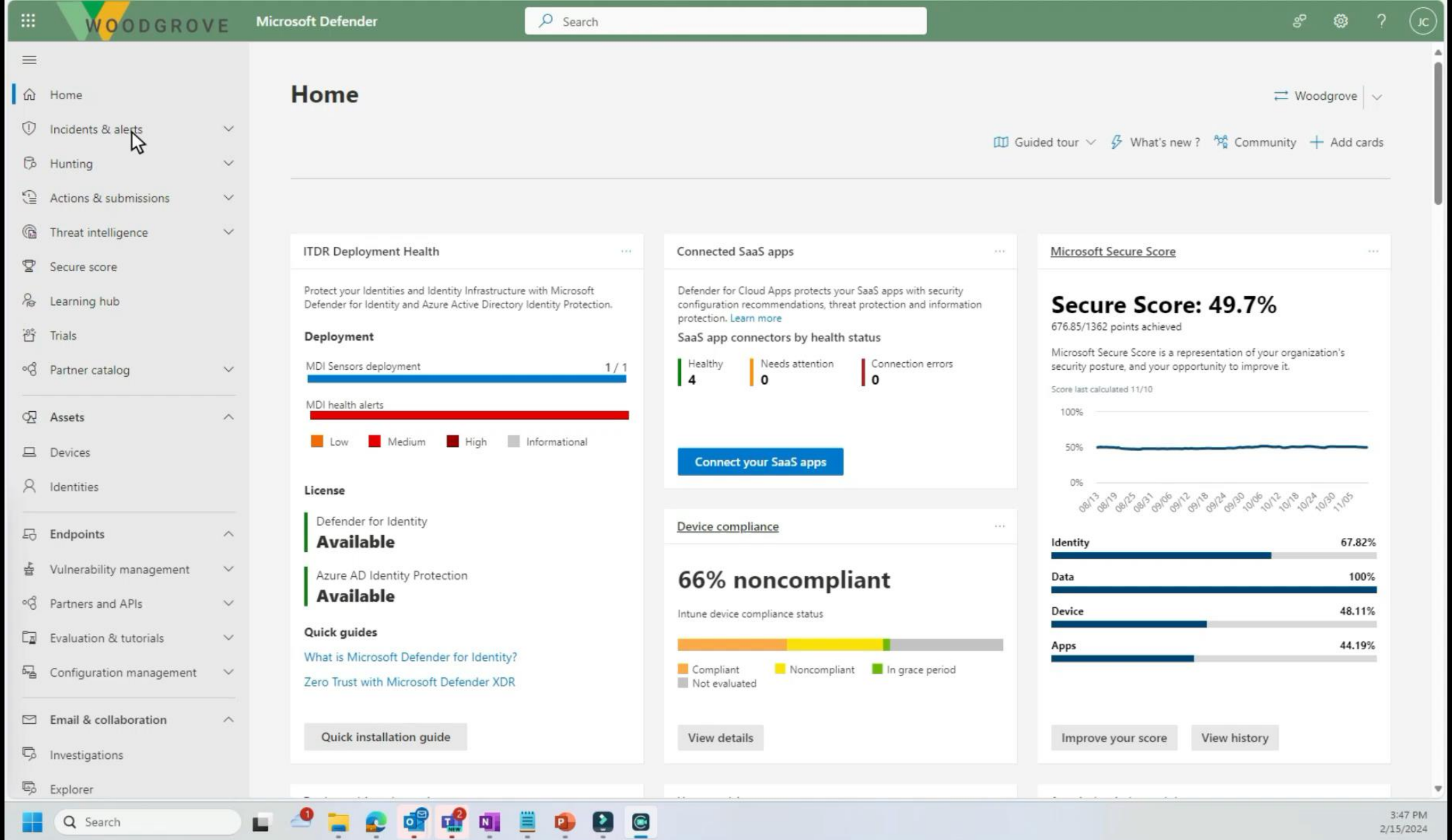
Tus datos son **tus** datos



Los datos **no** se utilizan para entrenar los modelos de IA básicos



Sus datos están protegidos por los controles de seguridad y cumplimiento empresarial **más completos**


WOODGROVE
Microsoft Defender
Search
JC
Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management
Email & collaboration
Investigations
Explorer
Home
Woodgrove
Guided tour
What's new ?
Community
Add cards
ITDR Deployment Health
Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Azure Active Directory Identity Protection.
Deployment
MDI Sensors deployment
1 / 1
MDI health alerts
Low
Medium
High
Informational
License
Defender for Identity
Available
Azure AD Identity Protection
Available
Quick guides
What is Microsoft Defender for Identity?
Zero Trust with Microsoft Defender XDR
Quick installation guide
Connected SaaS apps
Defender for Cloud Apps protects your SaaS apps with security configuration recommendations, threat protection and information protection. Learn more
SaaS app connectors by health status
Healthy
4
Needs attention
0
Connection errors
0
Connect your SaaS apps
Device compliance
66% noncompliant
Intune device compliance status
Compliant
Noncompliant
In grace period
Not evaluated
View details
Microsoft Secure Score
Secure Score: 49.7%
676.85/1362 points achieved
Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.
Score last calculated 11/10
100%
50%
0%
08/13
08/19
08/25
08/31
09/06
09/12
09/18
09/24
09/30
10/06
10/12
10/18
10/24
10/30
11/05
Identity
67.82%
Data
100%
Device
48.11%
Apps
44.19%
Improve your score
View history
Search
3:47 PM
2/15/2024

The script exhibits several actions that suggest malicious intent. It initiates a request to a website, attempts to locate and execute a specific file (`browsercore.exe`), and sends a request to a Microsoft login URL. The script then saves the response to a file in the temporary directory. Furthermore, it downloads two files (`psexec.exe` and `mimikatz_trunk.zip`) from the internet and stores them in the temporary directory with different names. These actions may be an attempt to avoid detection by security software. The downloaded files are well-known tools used for system exploitation and credential dumping, indicating that the script is likely part of a larger attack.

1. The script sends a request to the website vectorsandarrows.com.

```
curl vectorsandarrows.com

```

2. The script defines a function called `Get-UserPRTToken` that tries to locate and execute the `browsercore.exe` file from two possible locations. This function sends a request to `h**ps://0pm4injiht-qx4596ekfm.app.highlights.guide/common/oauth2/authorize` and retrieves the response.

```
function Get-UserPRTToken
{
    ...
    $p.StartInfo.FileName = $browserCore
    ...
    "uri":"h**ps://0pm4injiht-qx4596ekfm.app.highlights.guide/common/oauth2/authorize",
    ...
}

```

3. The script invokes the `Get-UserPRTToken` function and saves the output to a file named `prtt.bin` in the temporary directory.

```
Get-UserPRTToken > $Env:temp\prtt.bin

```

Ask anything about security, or type / for suggestions or * for promptbooks

AI-generated content can have mistakes. Make sure it's accurate before using it.

Contratación

Contratación Licencias
AM CRUE

Microsoft 365 Defender

Defender for Endpoint
Defender for Identity, Entra ID Protection
Defender for Office
Defender for Cloud Apps

Contratación Cloud
AM OCRE

Microsoft 365 Defender for Cloud

Microsoft Sentinel

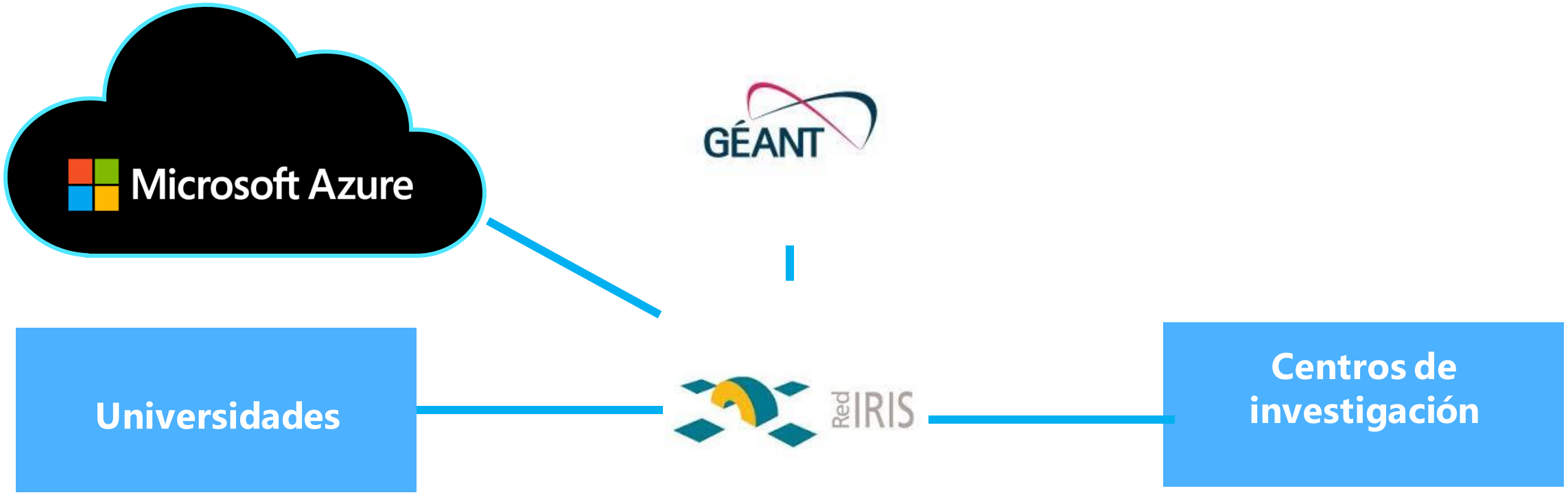
Microsoft Copilot for Security

Contratación Licencias - AM CRUE

Contratación Cloud - AM OCRE

Vicente Alcaraz
Head of Software & Cloud | Bechtle

La red como habilitadora de servicios



Acceso a Servicios en la nube:

- Servicios cognitivos
- Open AI/ML, analítica, BigData
- Almacenamiento y backup
- Kubernetes
- Ciberseguridad
- Escritorios virtuales

Acuerdo marco OCRE de GÉANT

Procedimiento de Contratación Pública
Framework:

- Descuento sobre el pay-as-you-go
- Exención del tráfico salida

Habilitando proyectos:

- Azure AI
- Modernización entorno datos
- Trabajo remoto seguro AVD
- Escalabilidad del LMS
- Ciberseguridad
- Modernización de aplicaciones
- Continuidad de negocio y recuperación ante desastres

Q&A

Universidades@Microsoft.com

Microsoft

BECHTLE

Gracias

Microsoft

BECHTLE