Ciberseguridad en acción

De la detección a la prevención inteligente

Agenda

Resumen del panorama de amenazas

Centros de operaciones de seguridad (SOC) en la actualidad

Transformación de SecOps con una plataforma unificada

Ejemplos de escenarios de amenazas

Análisis técnico de seguridad proactiva con Microsoft Security

Conclusiones y próximos pasos

Threat landscape

BRIEFING

POWERED BY:
Microsoft Threat Intelligence

78T Señales sintetizadas por día (2024)

300+ Actores únicos del Estado-nación y de la delincuencia financiera

Las tres principales tendencias en el panorama de amenazas

Las **amenazas** están creciendo y vendiendo sus herramientas a otros

El ransomware está evolucionando para dirigirse a dispositivos no gestionados y vectores similares de baja visibilidad

La velocidad, la escala y la sofisticación de los ataques no tienen precedentes

Inteligencia Artificial

Las empresas que utilizan la IA y la automatización para detectar y responder a las brechas de datos ahorran una media de 3 millones de dólares en comparación con las que no lo hacen.

En ambos bandos

En 2023, más delincuentes usarán los algoritmos de IA para identificar sistemas con una seguridad débil.

Para 2030 el mercado de productos de ciberseguridad con IA tendrá un valor cercano a los 139.000 millones de dólares, lo que supone un aumento de casi diez veces el valor del mercado de 2021.

Fuente IBM

NUEVAS AMENAZAS

Los 'piratas' de la 'Dark Web', al acecho del control de ChatGPT

tan sobre riesgos de 'ChatGPT'

Primera modificación: 03/03/2023 - 03:47

PORTADA / FORBES CENTROAMÉRICA

Así es cómo el ChatGPT facilita la vida de los delincuentes

Forbes Staff | marzo 27, 2023 @ 12:03:25 pm

Home > Tecnología

He probado a 'hackear' ChatGPT para que se salte las políticas de OpenAI y este es el resultado

TECNOLOGÍA Carolina González Valenzuela | 23 abr. 2023 1:00h.

Noticias · 20/04/2023

Por 7 se multiplica el número de hac
que hablan en la dark web sobre cór
manipular ChatGPT

Redacción Tekios · lectura 1 min · 770 vis

TECNOLOGÍA

Fake news, manipulación y hackeos: cómo ChatGPT es un "profundo riesgo para

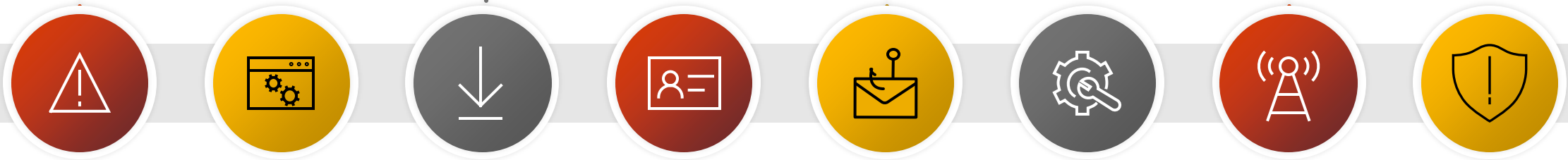
¿Pánico por chatGPT?

Pánico con ChatGPT

MATT BURGESS SEGURIDAD 14 DE ABRIL DE 2023

ChatGPT: el hackeo apenas comienza

Los adversarios utilizan la IA



Generación de malware

Detección automatizada de vulnerabilidades

Personalización de exploits

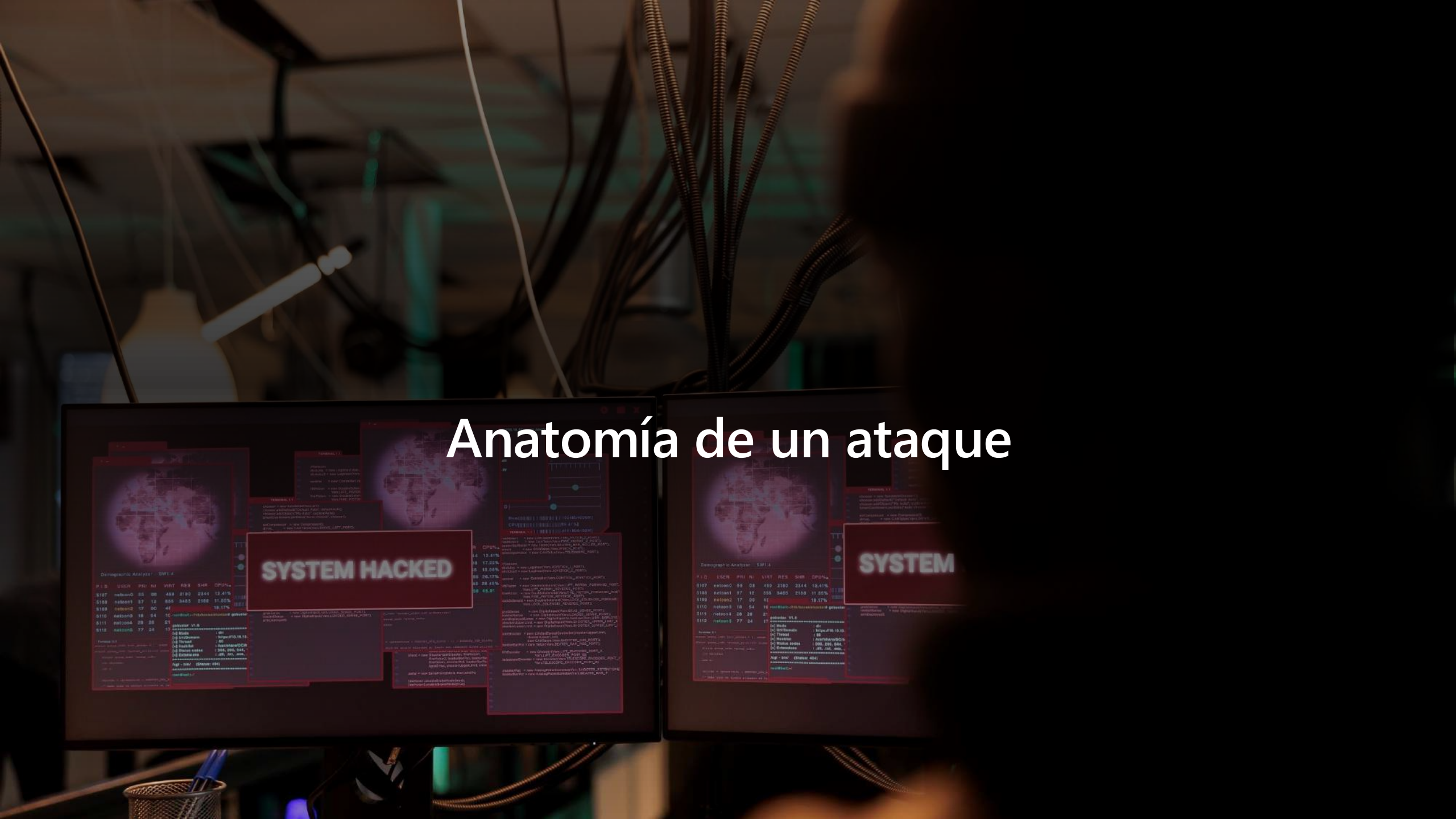
Password cracking

Phishing e ingeniería social

Enmascarar código malicioso

Comunicación y control de mando

Deepfakes: data, correo electrónico, voz



Anatomía de un ataque

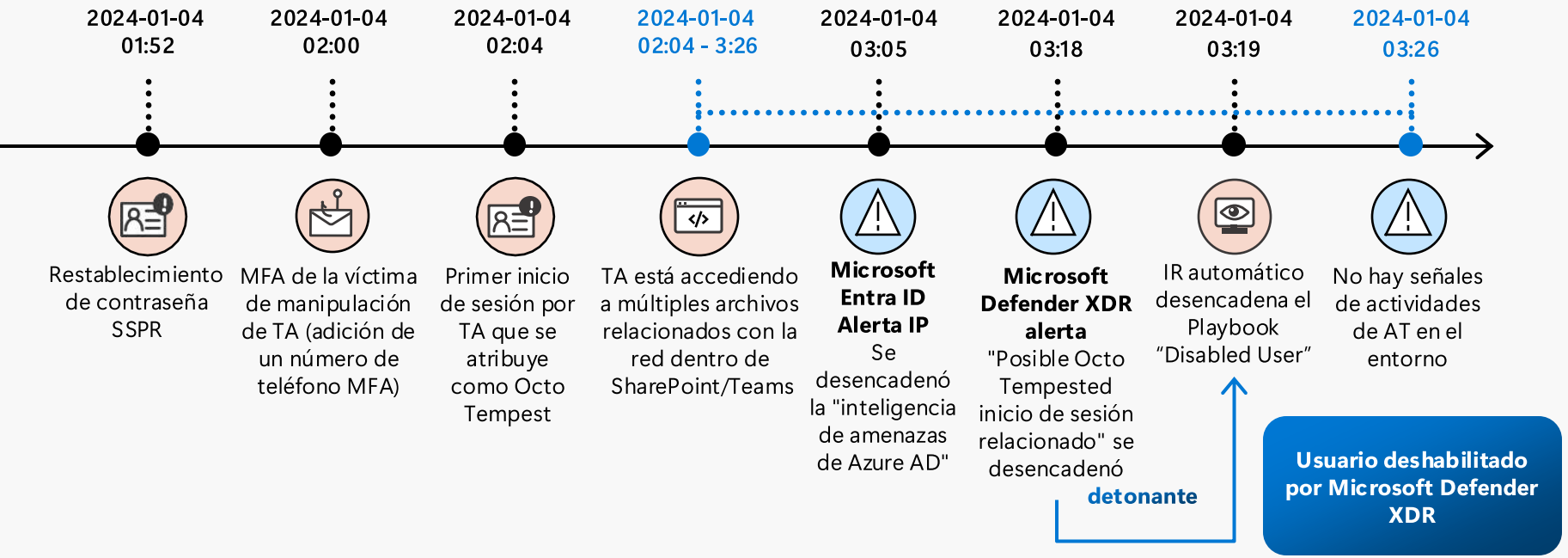
Intel profile: Octo Tempest

Motivación: Financiera

Alias: Scattered spider,0katpus

Objetivos: Intercambios de SIM, robo de criptomonedas o exfiltración de datos antes de operaciones de extorsión o ransomware

Estudio de caso de una cadena de ataque real de Octo Tempest: Interrumpida



Acceso inicial
- Ingeniería Social
- Enmascaramiento y suplantación de identidad

Descubrimiento
- Enumeración de la documentación interna
- Reconocimiento ambiental continuo

Acceso a credenciales, movimiento lateral
- Identificación de activos de nivel 0
- Acceso a entornos empresariales a través de VPN
- Recopilación de credenciales adicionales

Evasión de la defensa, ejecución
- Aprovechar la EDR y las herramientas de gestión
- Elusión del acceso condicional

Persistencia
- Instalación de una puerta trasera de confianza
- Manipulación de cuentas existentes
- Establecer el acceso a los recursos

Acciones sobre objetivos
- Preparación y exfiltración de datos robados
- Implementación del ransomware BlackCat

Panorama actual de amenazas

91%

Ciberataques que comienzan con el correo electrónico

30,720

Dominios generados por delincuentes cada tres días

$1.8B

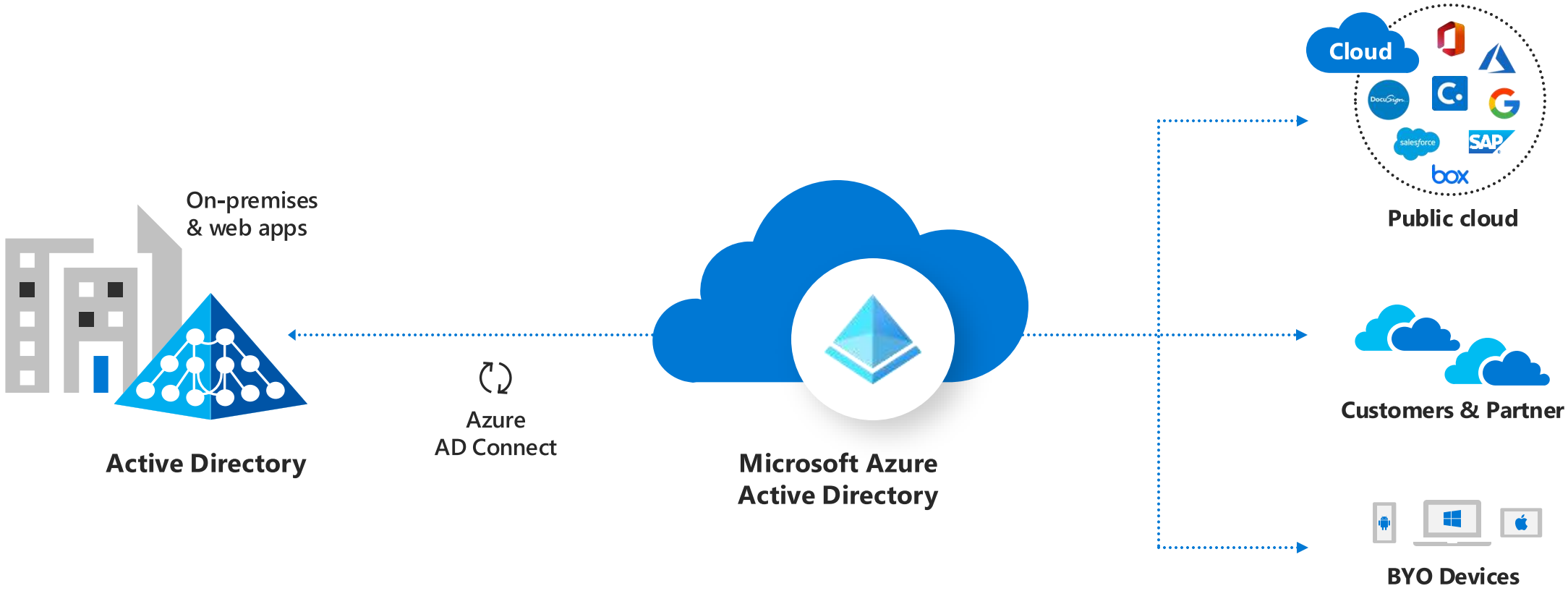
Pérdida atribuida al compromiso del correo electrónico empresarial solo en 2020

168K

Sitios de phishing eliminados

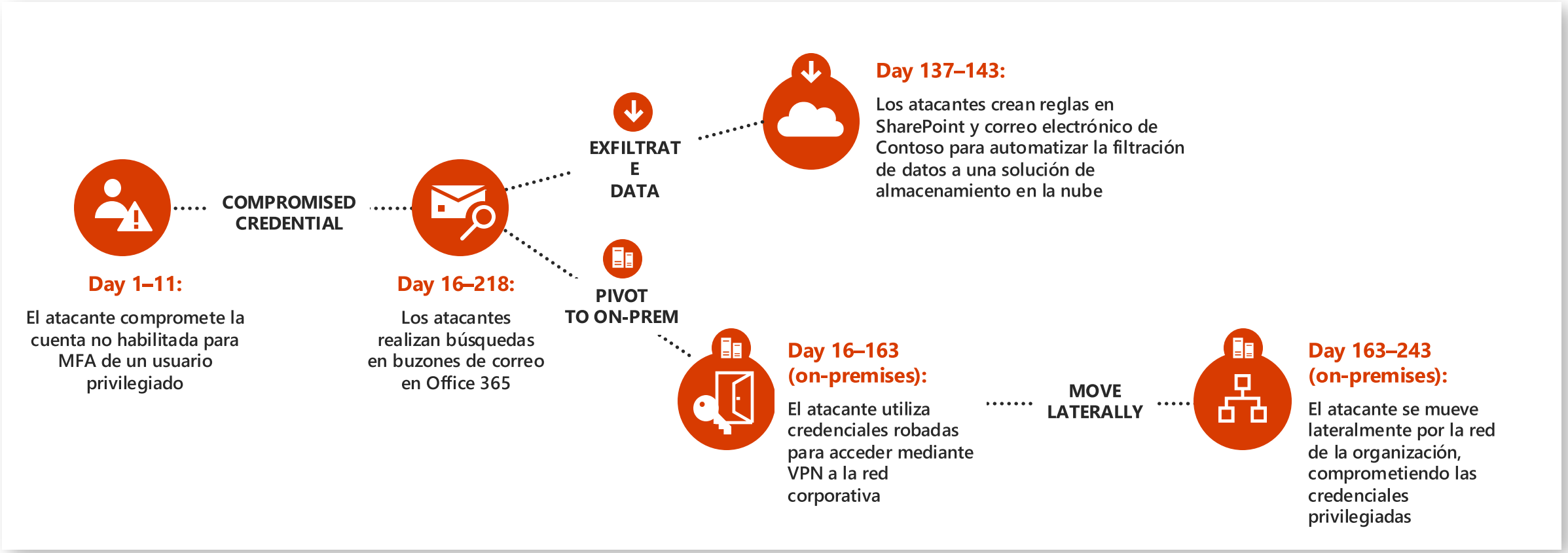
La complejidad del panorama de seguridad de la identidad empresarial

Los entornos de seguridad empresarial son complejos e incluyen activos tanto locales como en la nube.



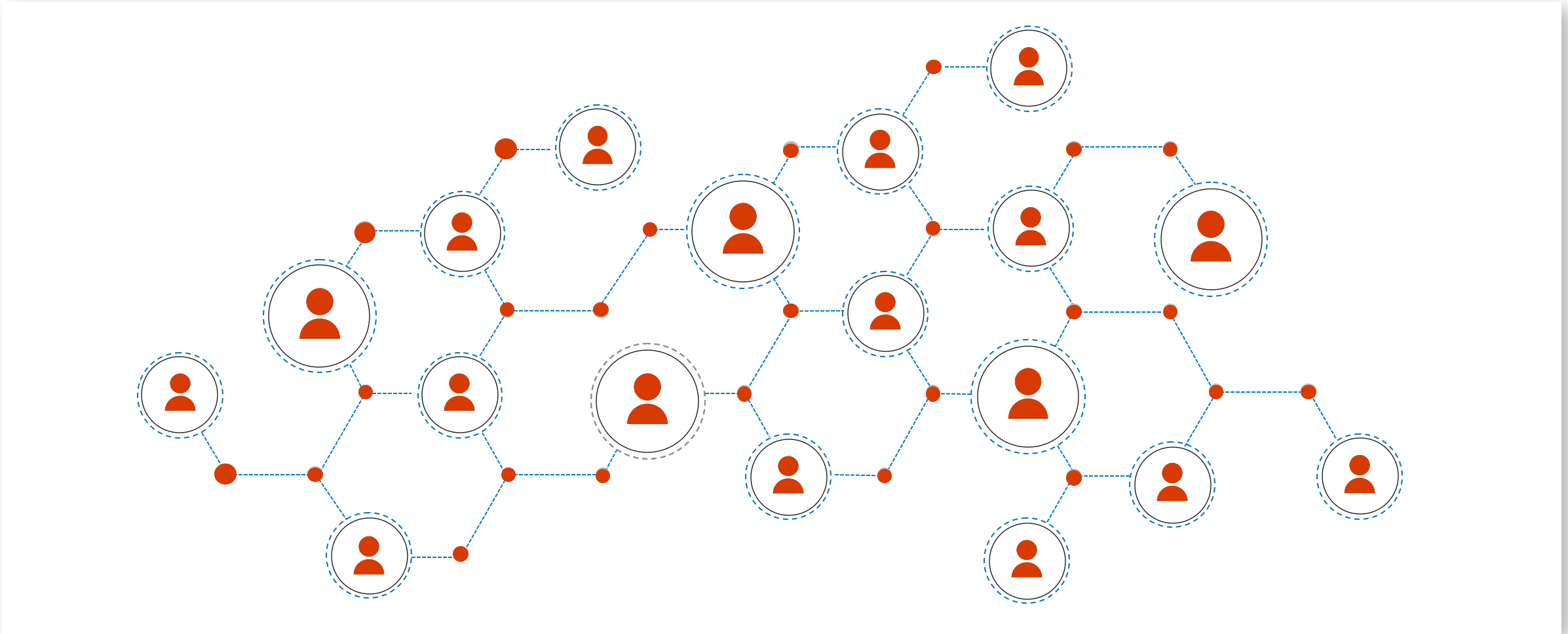
Anatomía de un ataque al entorno local y en la nube

Un ejemplo de cómo ocurre un ataque y compromete a toda una organización.



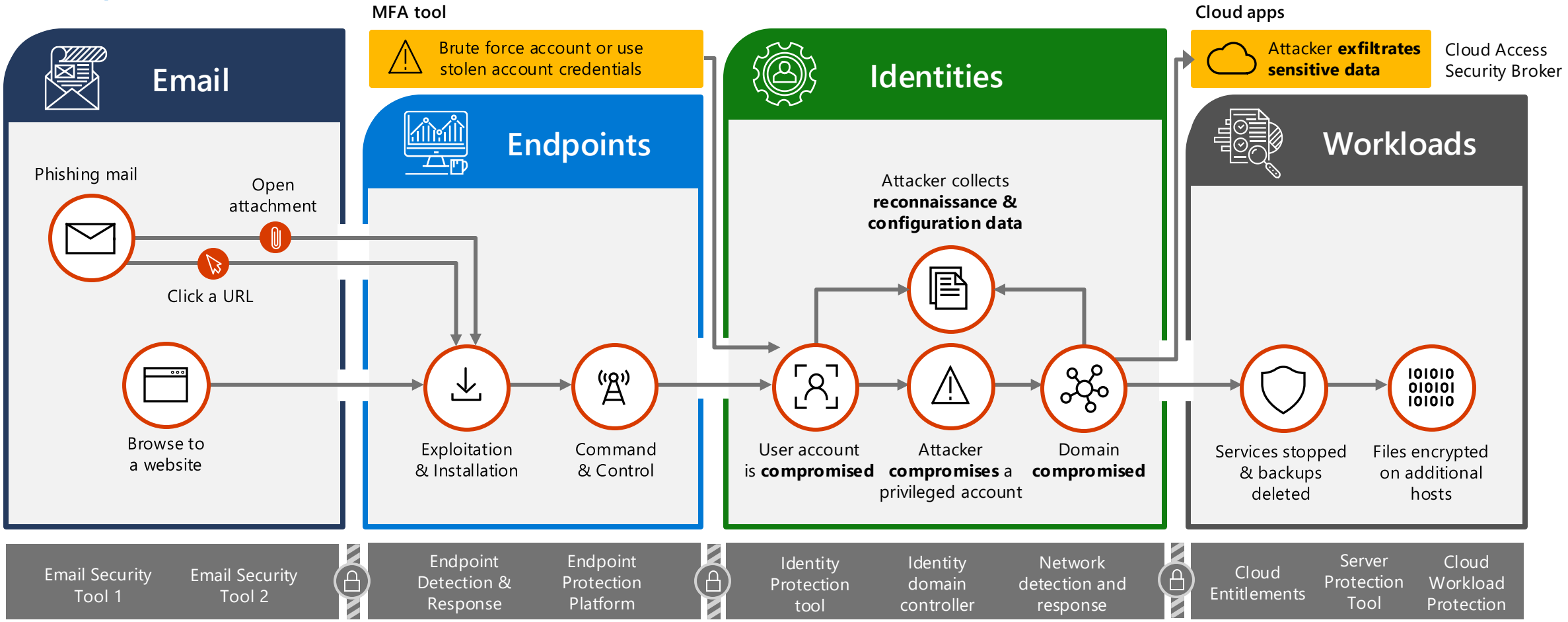
Un nuevo perímetro de seguridad - Identidad de usuario

Los usuarios son el nuevo perímetro y un solo usuario comprometido puede provocar el cierre de una empresa.

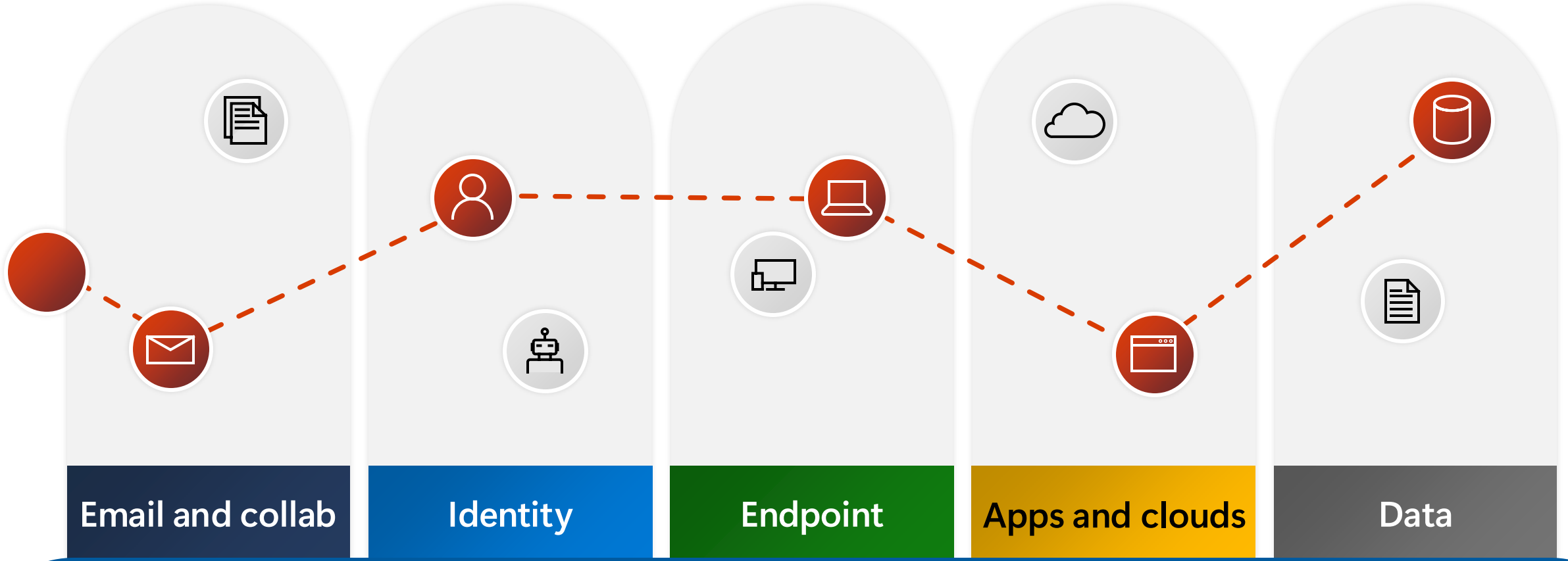


La seguridad aislada conduce a brechas en la cobertura

Múltiples herramientas que proporcionan una protección desigual a lo largo de la cadena de eliminación de ataques



Atacantes piensan en grafos



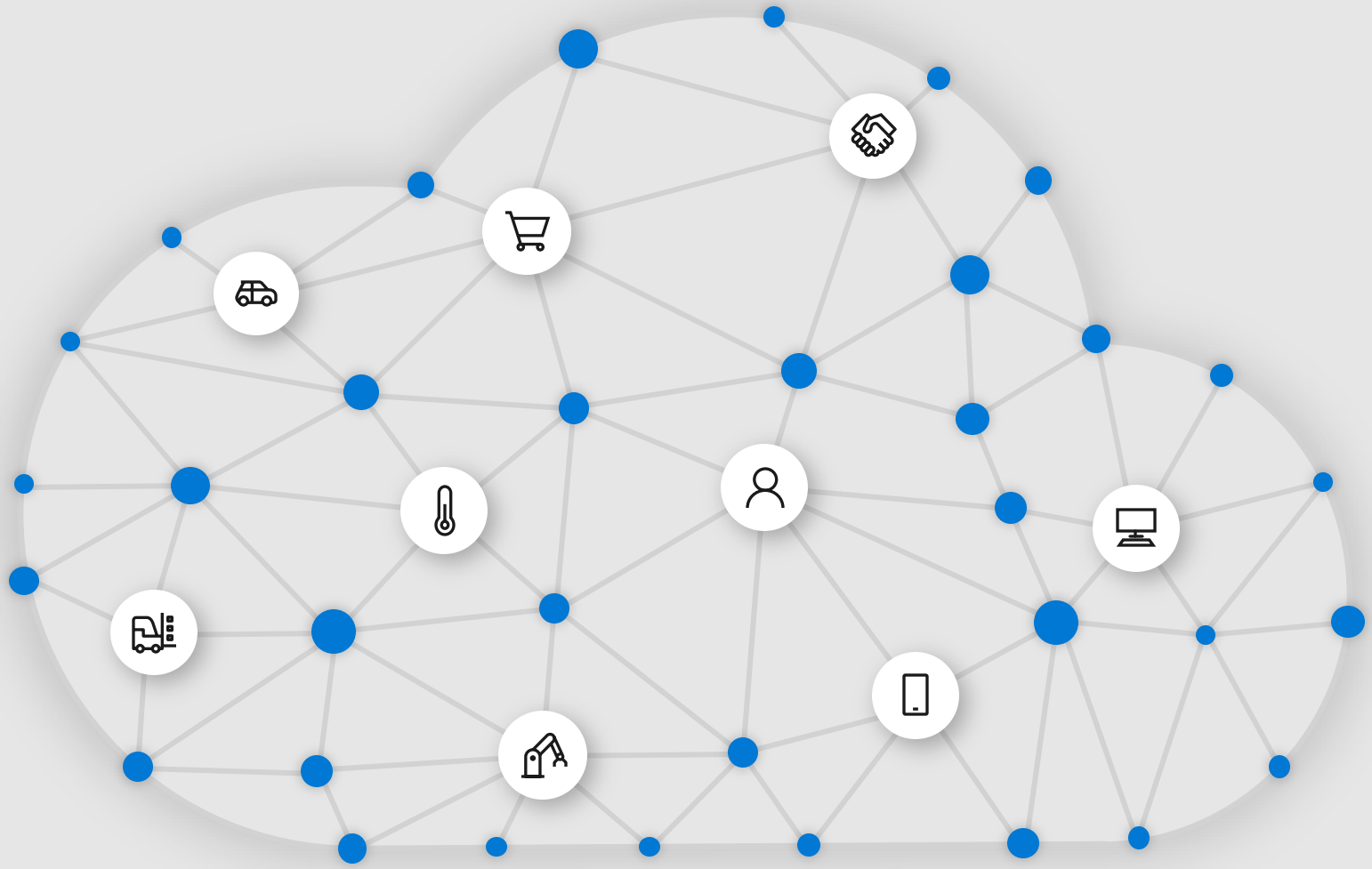
El tiempo medio para que un atacante acceda a los datos privados del phishing es de solo

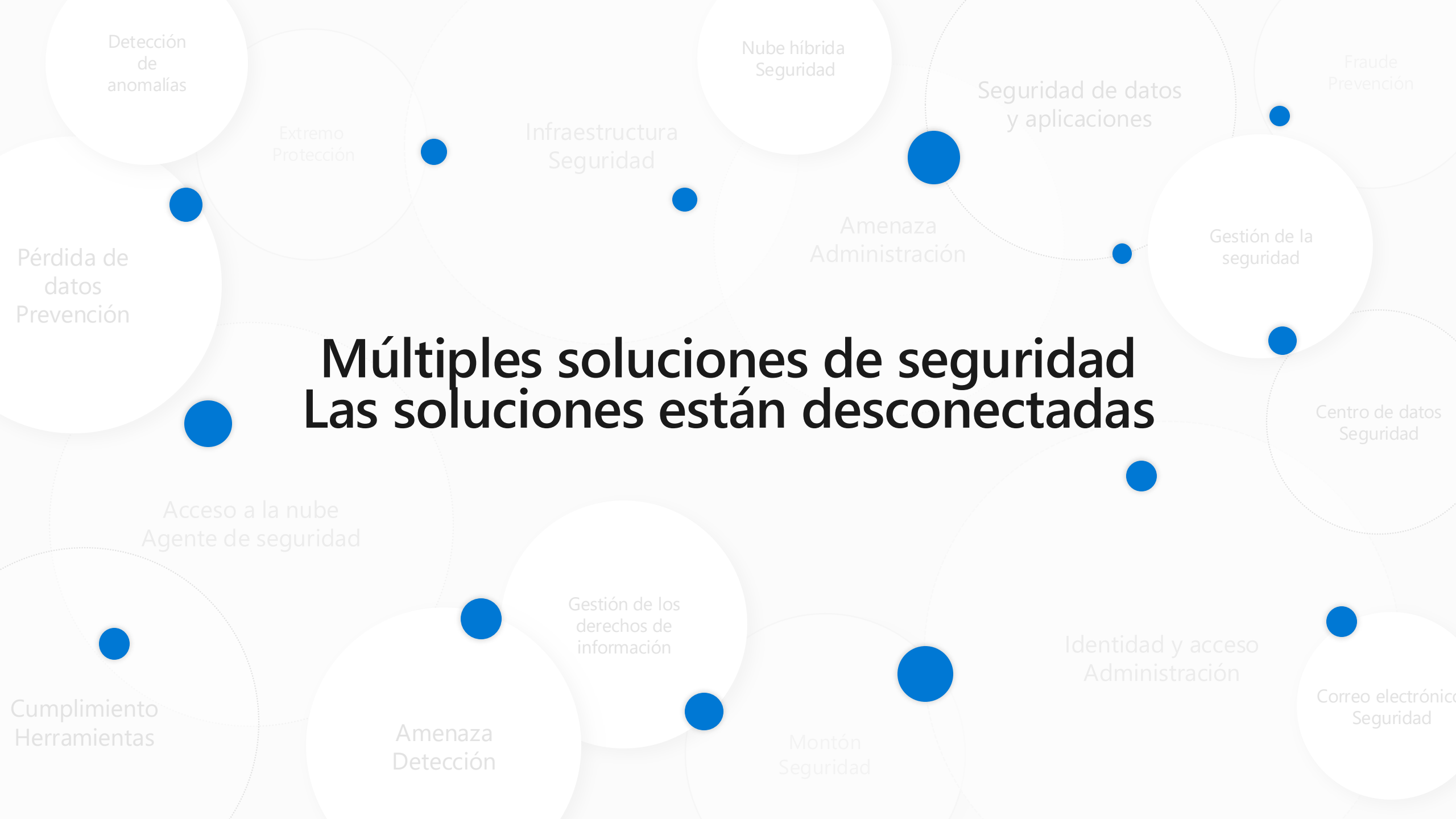
72 minutos[2]

2. 2022 Microsoft Digital Defense Report, p. 21

Los profesionales de SecOps trabajan dentro de portales


Vehículos
Ciudades inteligentes
Sensores
Sistemas energéticos
Mercados
Equipo
Socios
Clientes
Ciudadanos
Transporte
Local
Fabricantes
Dispositivos móviles

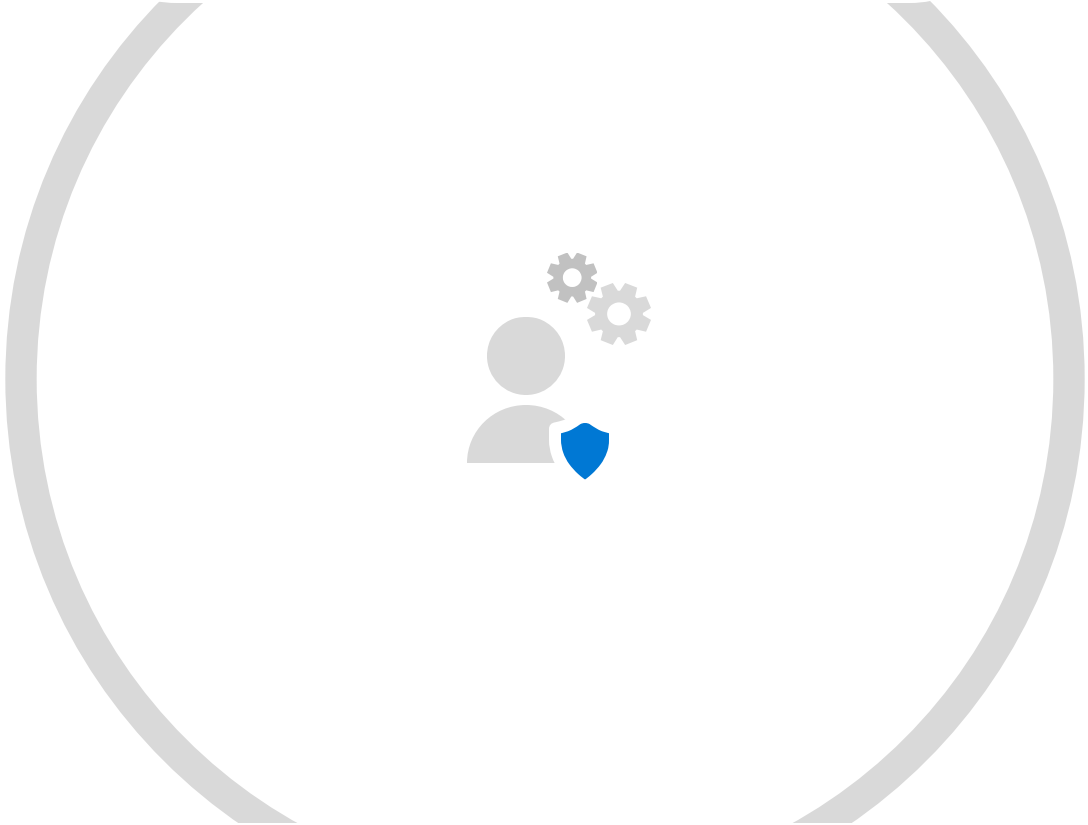




Múltiples soluciones de seguridad
Las soluciones están desconectadas

SIEM

Visibility across your entire organization



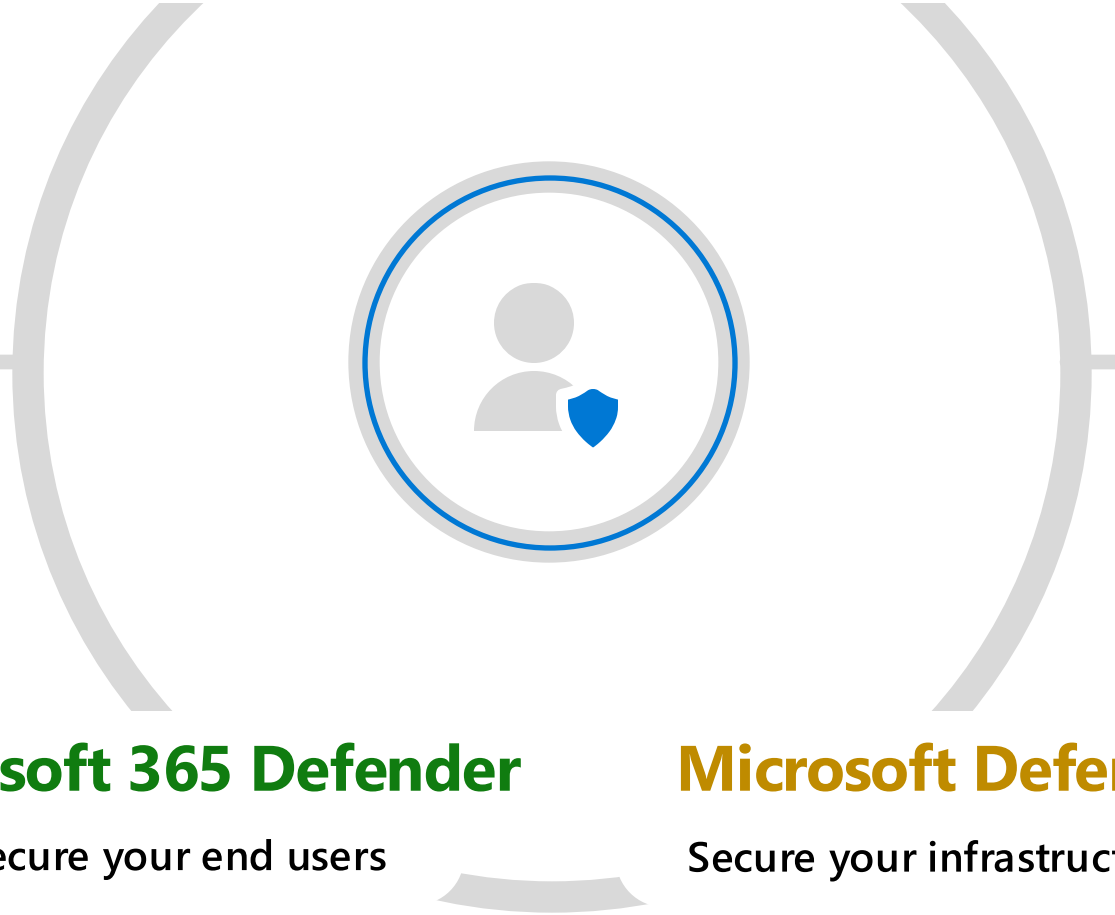
XDR

Protection across your end user and infrastructure environments

SIEM

Microsoft Sentinel

Visibility across your entire organization



Existing security portfolio

IA

Microsoft 365 Defender

Secure your end users

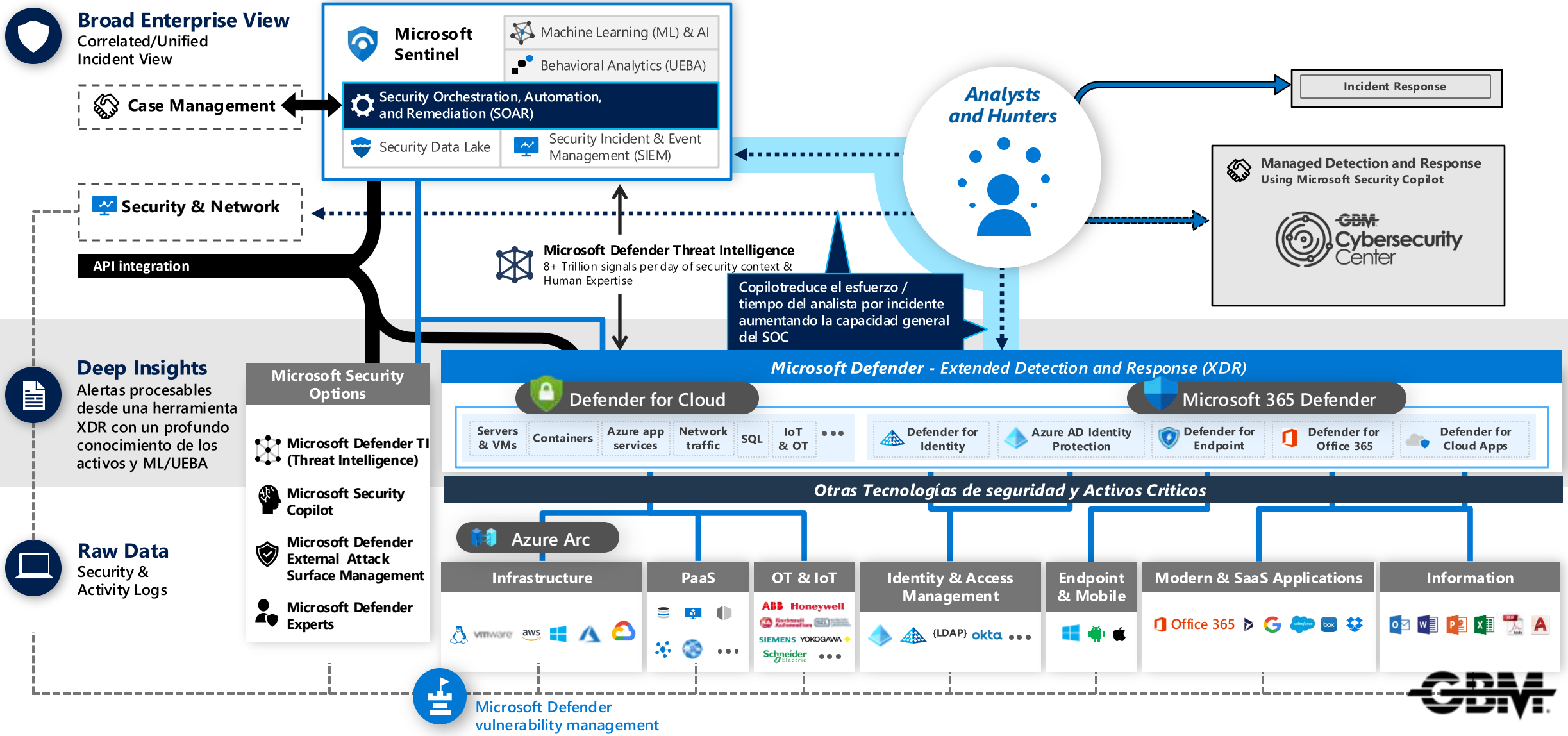
Microsoft Defender

Secure your infrastructure

XDR

Managed Detection & Response for Microsoft

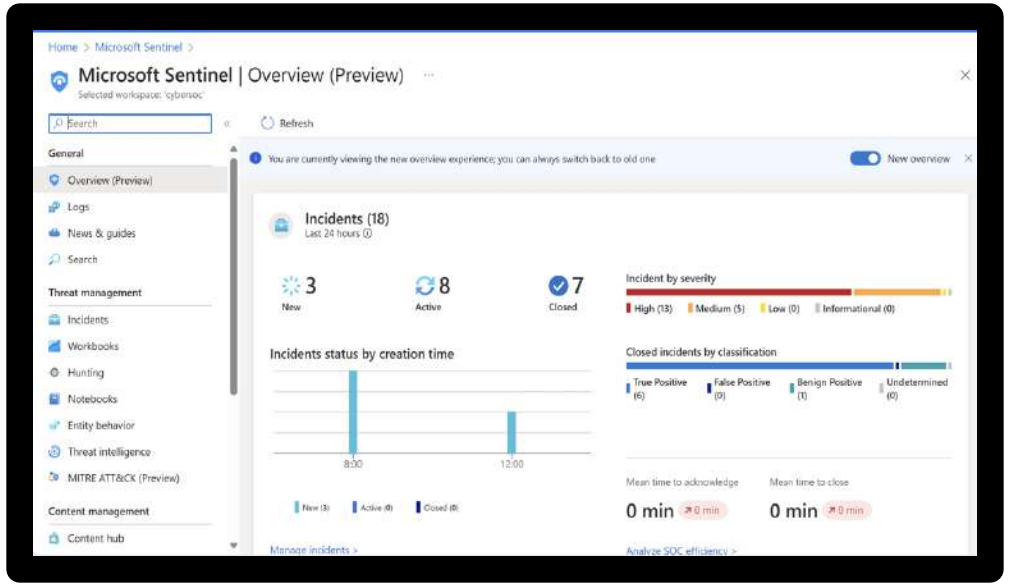
GBM Cybersecurity Center



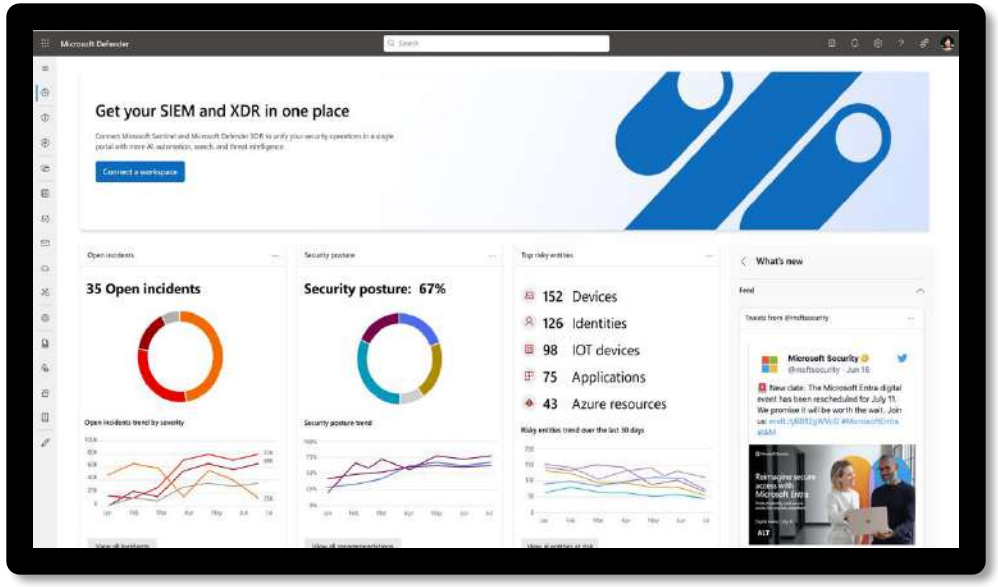
XDR + SIEM se está convirtiendo en una plataforma unificada de operaciones de seguridad

Hacer más con menos

Acelere su defensa contra amenazas con Microsoft Sentinel y Defender XDR juntos



Información general de Microsoft Sentinel en Azure Portal



Descripción general de la plataforma unificada

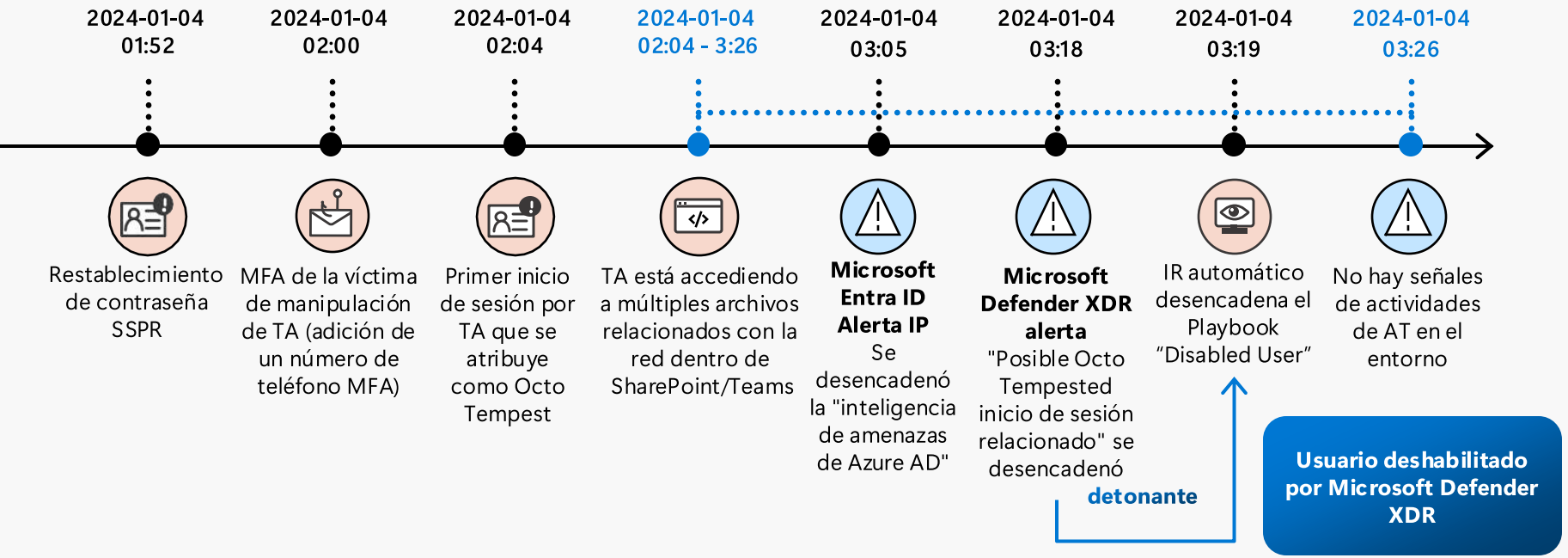
Intel profile: Octo Tempest

Motivación: Financiera

Alias: Scattered spider,0katpus

Objetivos: Intercambios de SIM, robo de criptomonedas o exfiltración de datos antes de operaciones de extorsión o ransomware

Estudio de caso de una cadena de ataque real de Octo Tempest: Interrumpida



Acceso inicial
- Ingeniería Social
- Enmascaramiento y suplantación de identidad

Descubrimiento
- Enumeración de la documentación interna
- Reconocimiento ambiental continuo

Acceso a credenciales, movimiento lateral
- Identificación de activos de nivel 0
- Acceso a entornos empresariales a través de VPN
- Recopilación de credenciales adicionales

Evasión de la defensa, ejecución
- Aprovechar la EDR y las herramientas de gestión
- Elusión del acceso condicional

Persistencia
- Instalación de una puerta trasera de confianza
- Manipulación de cuentas existentes
- Establecer el acceso a los recursos

Acciones sobre objetivos
- Preparación y exfiltración de datos robados
- Implementación del ransomware BlackCat

Los equipos de seguridad necesitan una fuerza multiplicadora

Los ataques ocurren en minutos y horas no días o meses

Los atacantes se están aprovechando de las herramientas aisladas

No hay suficiente ancho de banda para abordar la exposición al riesgo de manera eficaz

¿Cómo la IA y GBM hacen su parte?

Las probabilidades están en contra de los analistas de seguridad hoy en día

4,000

Ataques de contraseñas por segundo

72 mins

Tiempo medio para que un atacante acceda a tus datos privados si eres víctima de un correo electrónico de phishing

3.5M

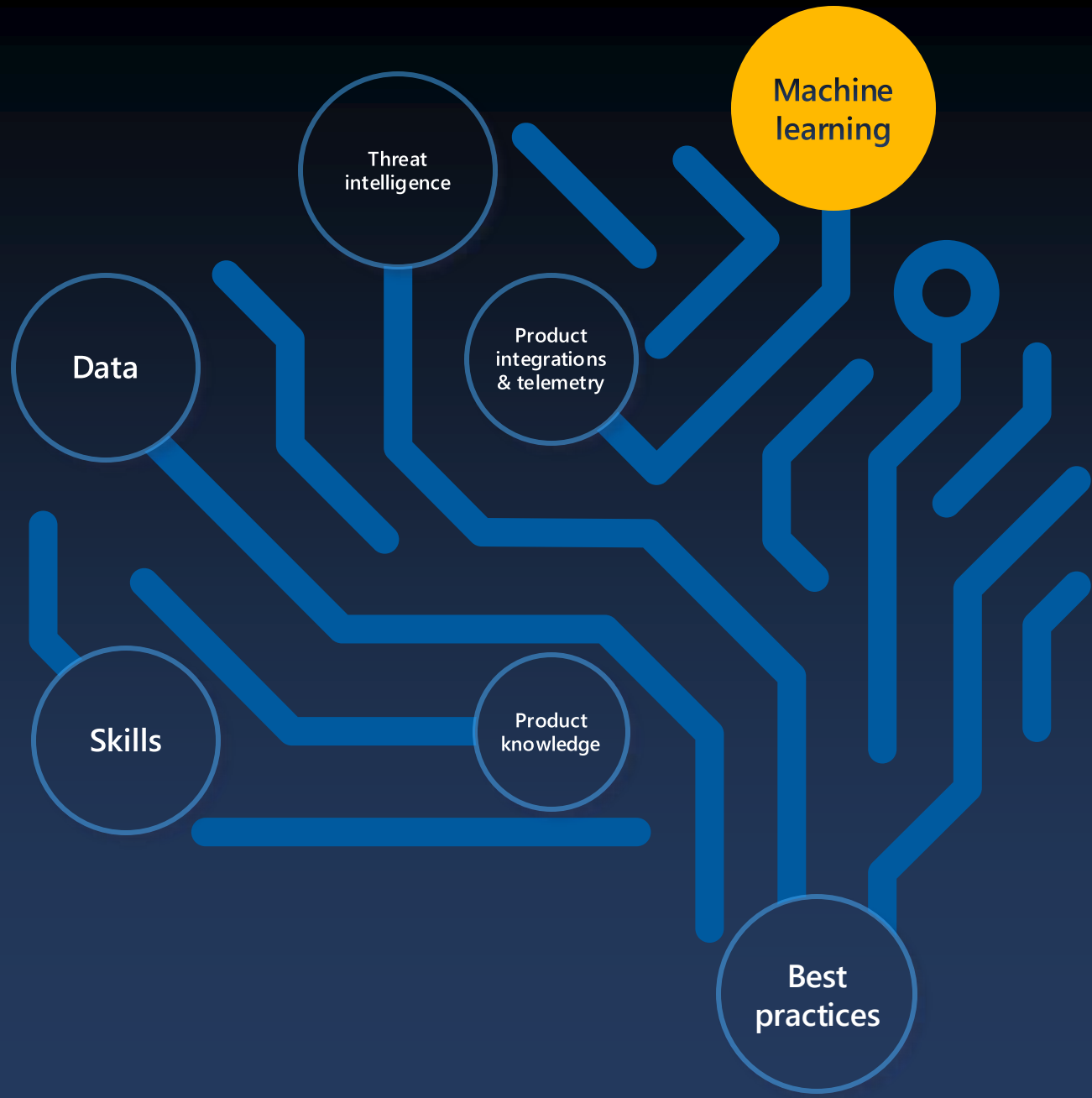
Escasez mundial de profesionales calificados en ciberseguridad

Necesitamos cambiar las reglas del juego

Microsoft Security Copilot

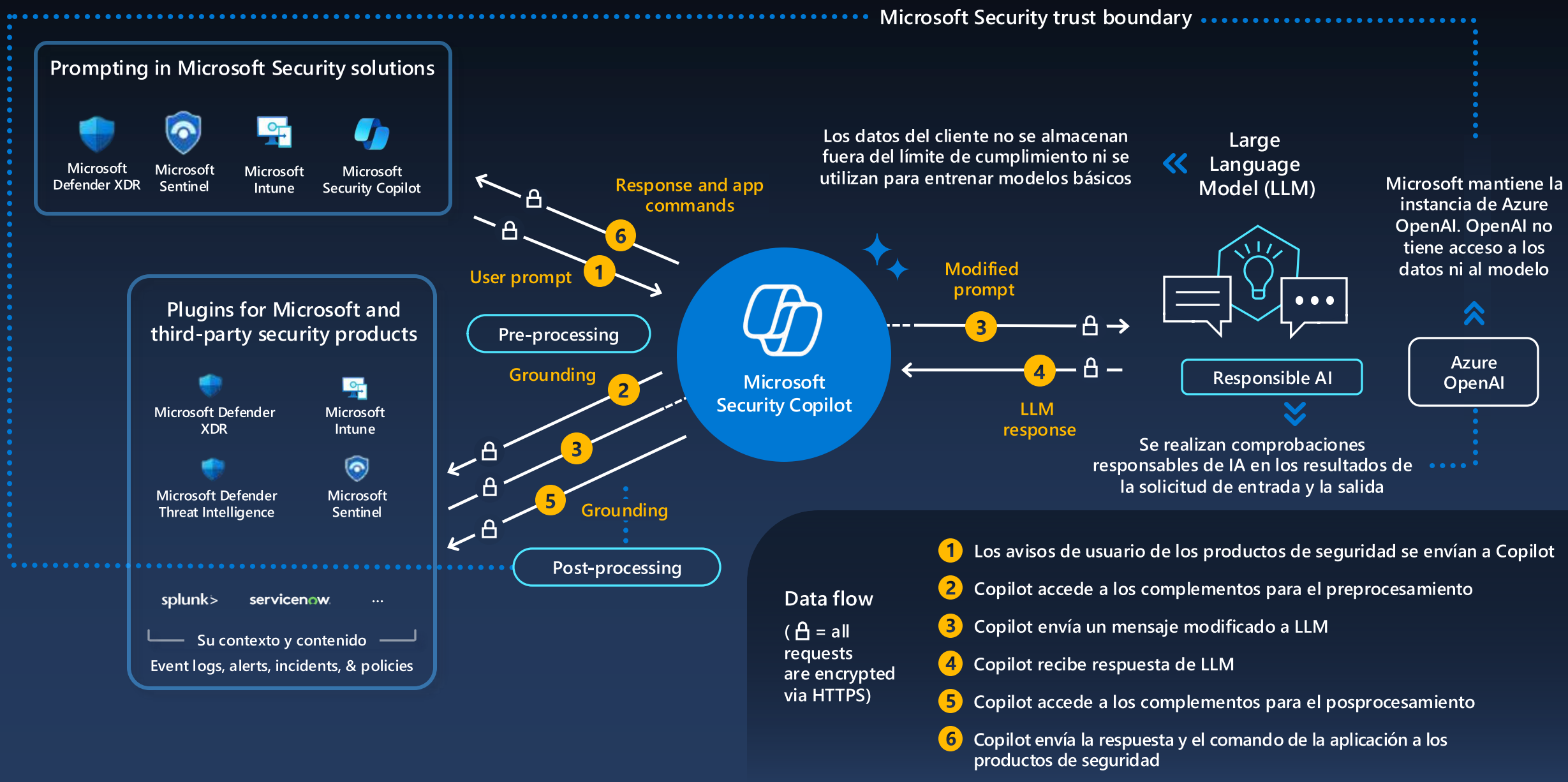
Microsoft Security Copilot

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



Microsoft's End-to-End Security

Flujo de datos para Microsoft Copilot for Security



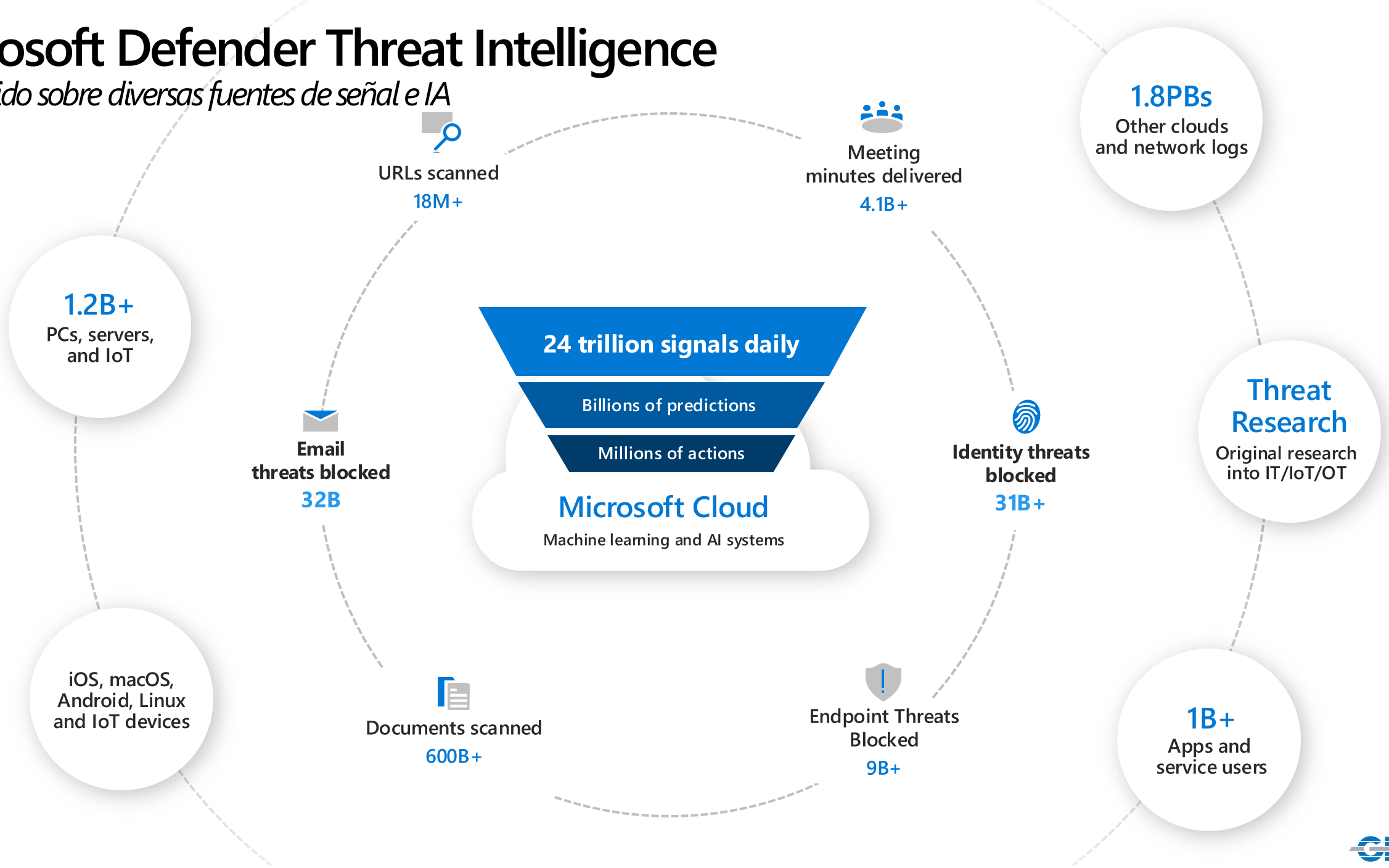
Data flow

(= all requests are encrypted via HTTPS)

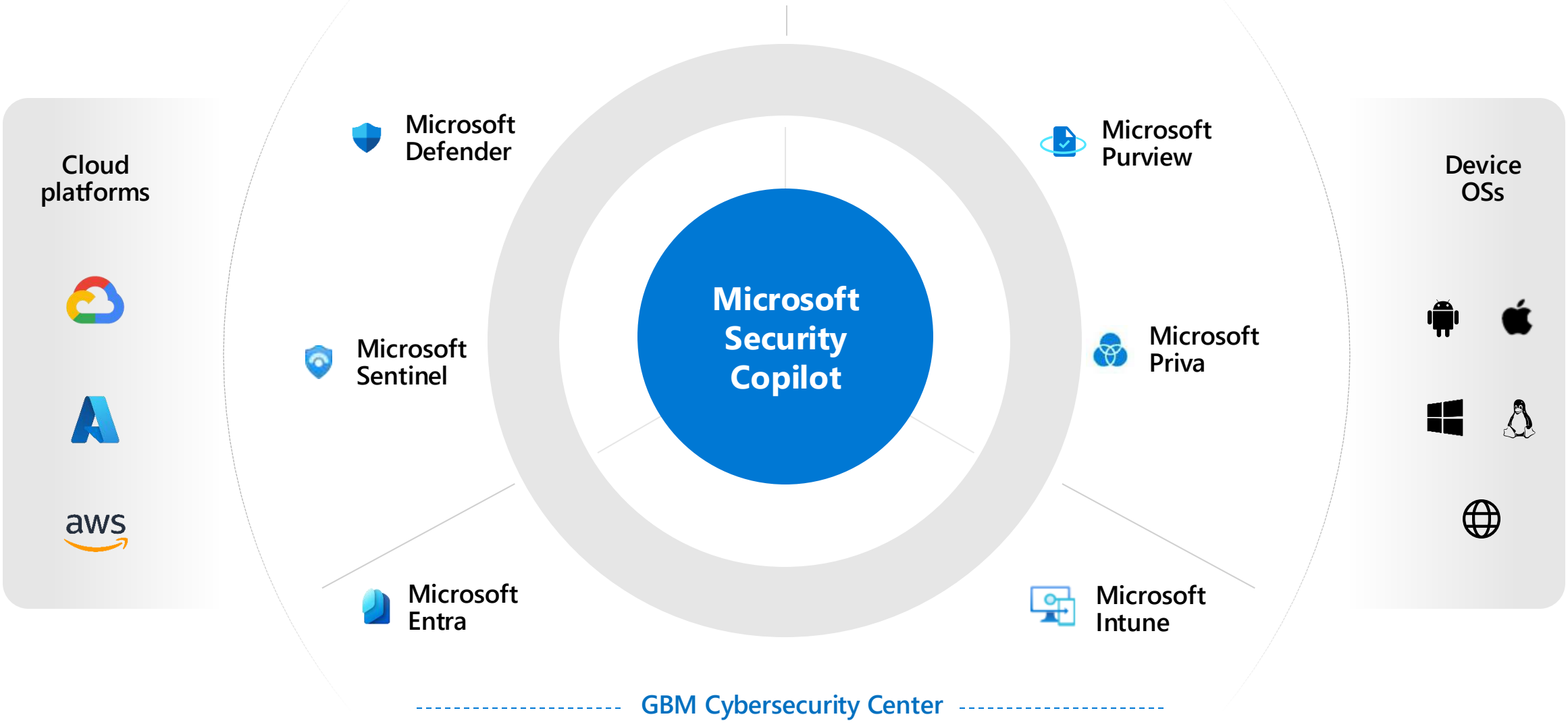
1. Los avisos de usuario de los productos de seguridad se envían a Copilot
2. Copilot accede a los complementos para el preprocesamiento
3. Copilot envía un mensaje modificado a LLM
4. Copilot recibe respuesta de LLM
5. Copilot accede a los complementos para el posprocesamiento
6. Copilot envía la respuesta y el comando de la aplicación a los productos de seguridad

Microsoft Defender Threat Intelligence

Construido sobre diversas fuentes de señal e IA



Portafolio de Seguridad de Microsoft



¿Cómo puedo mejorar mi postura de seguridad?

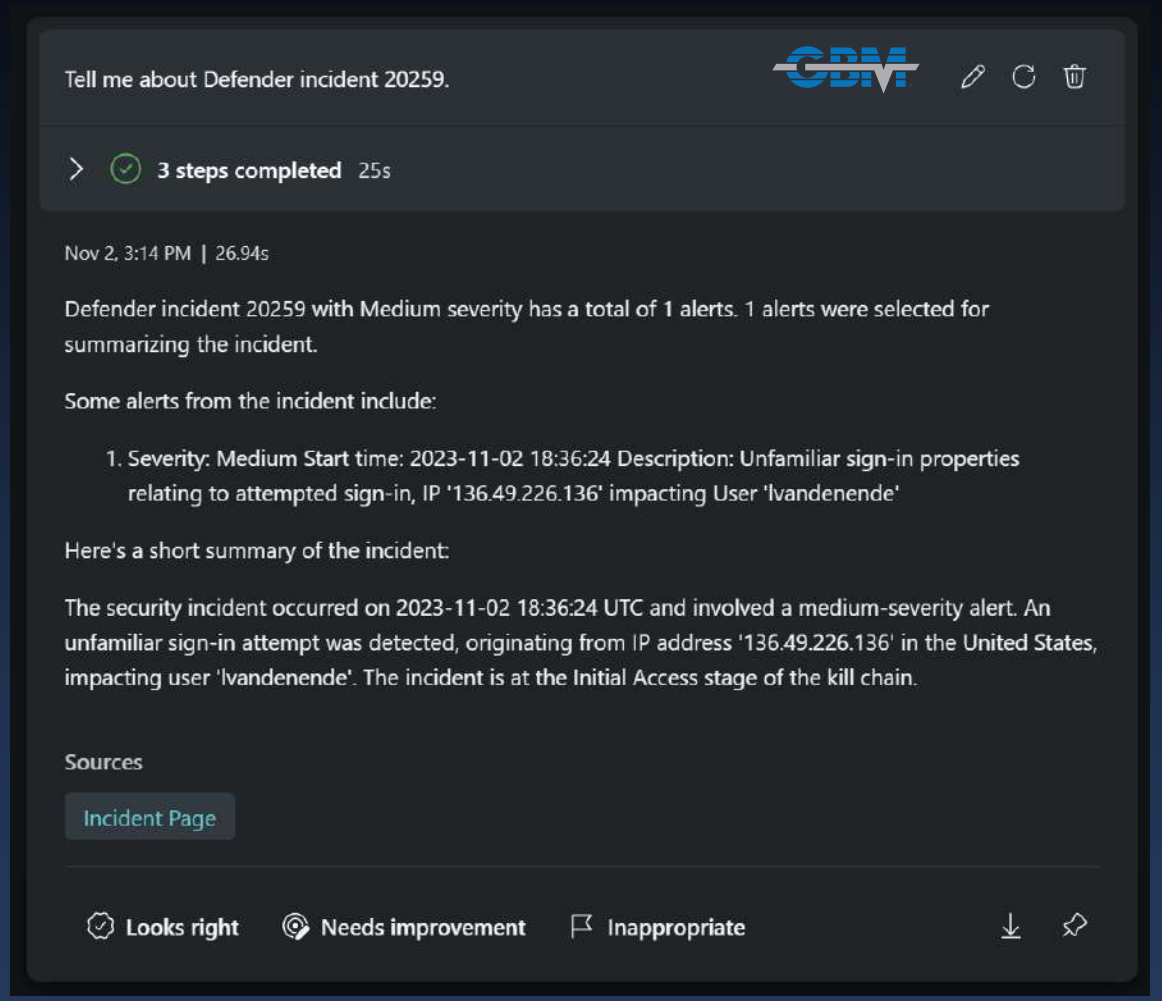
¿Alguna de mis máquinas se ve afectada?

Resuma este incidente en viñetas.

¿Cuáles son las alertas que más se activan?

¿Qué es log4shell?

Cuéntame sobre el incidente de Defender 20259.



Security Copilot in Unified SOC Platform

Contexto inteligente para alertas e incidents

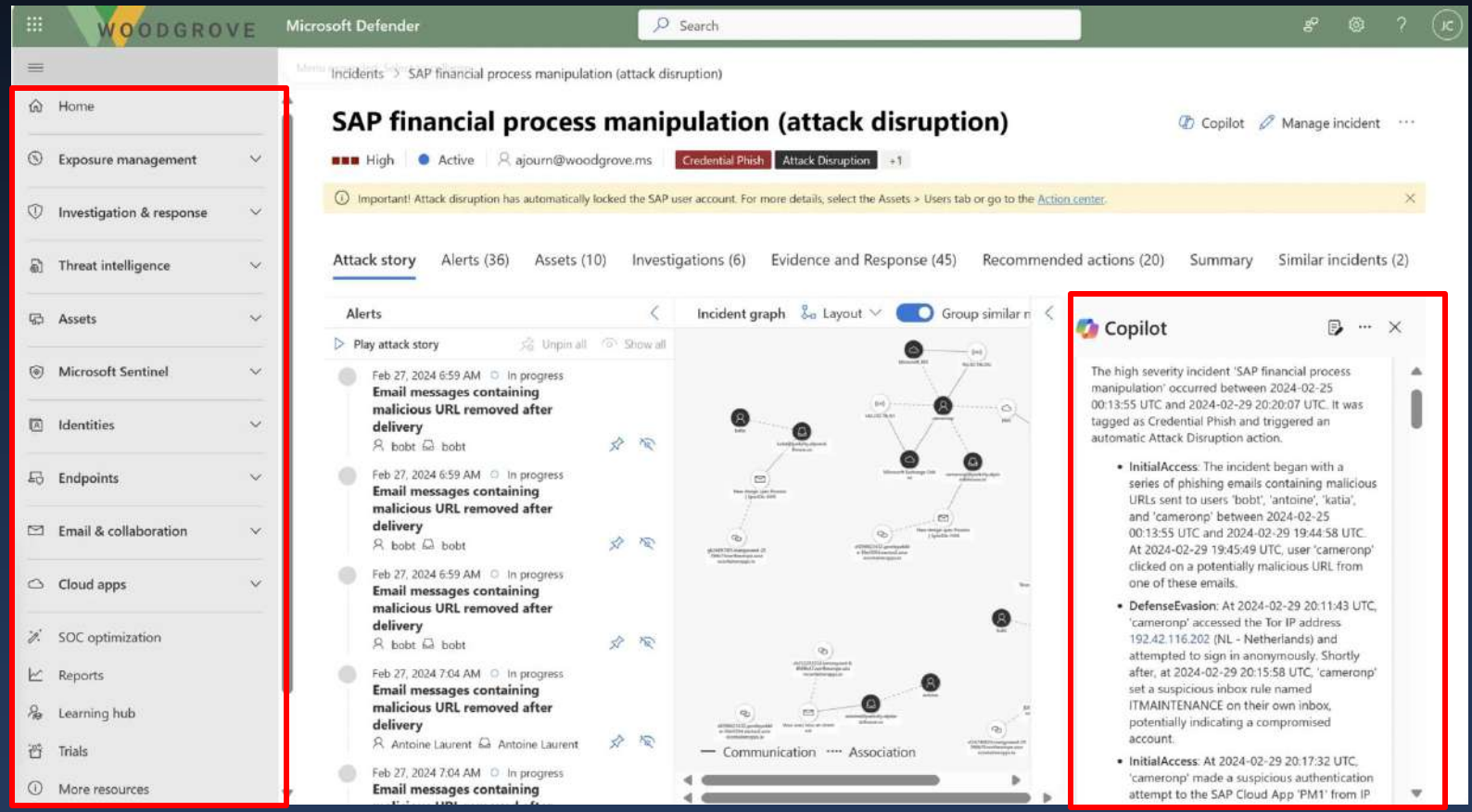
Evaluación rápida para las amenazas emergentes y la exposición de su organización. Respuestas con información enriquecida e impulsada por IA.

Investigación y respuesta rápidas

Security Copilot proporciona soporte integral a los analistas. Desde resúmenes de incidentes y respuestas, hasta la evaluación del impacto de los incidentes, pasando por recomendaciones prácticas para una investigación y corrección más rápidas.

Desbloquea habilidades avanzadas de SOC

Desbloquea nuevas habilidades que permiten a los analistas de todos los niveles completar tareas complejas, traduciendo lenguaje natural a KQL o analizando scripts maliciosos.



Security Copilot in Microsoft Intune

Respuesta más rápida

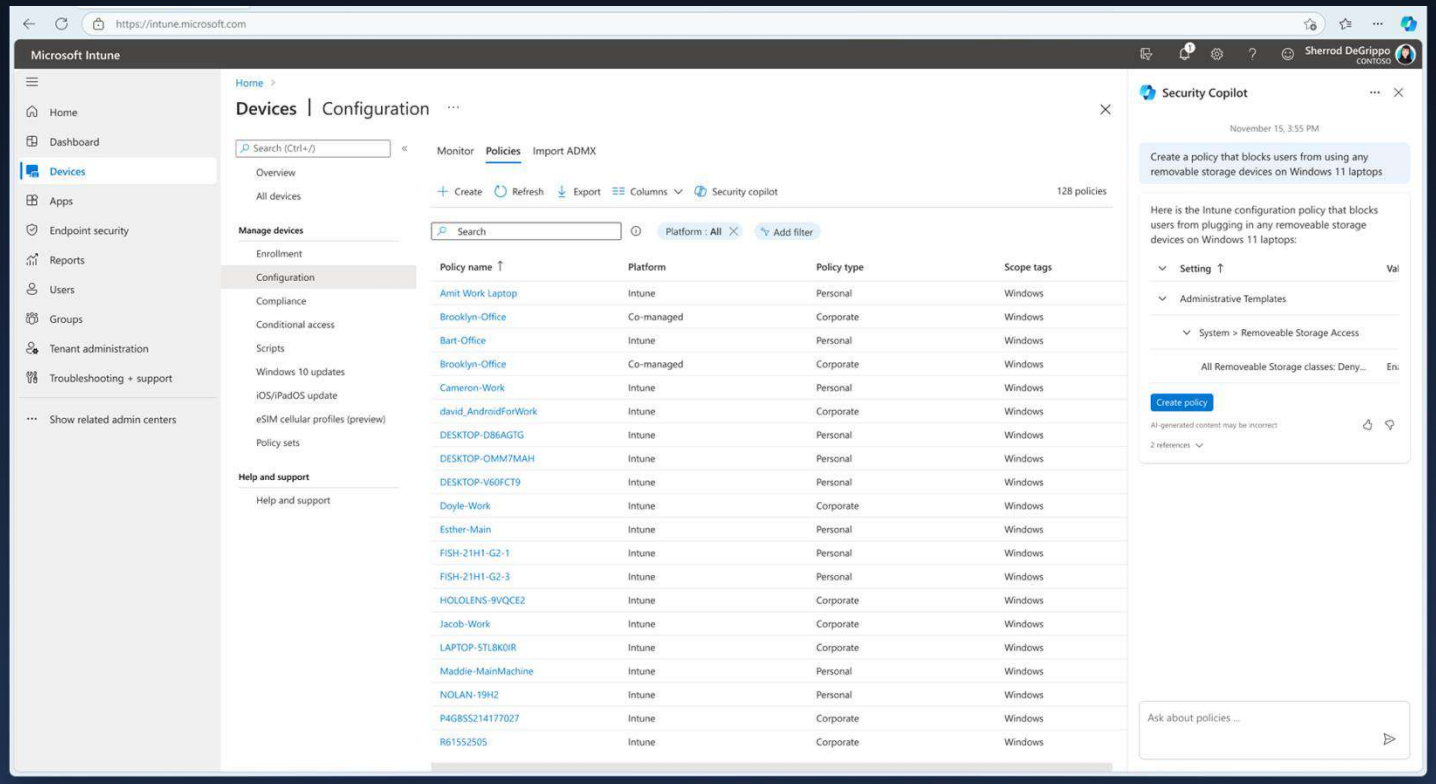
Responde rápidamente a amenazas, incidentes y vulnerabilidades con el contexto completo del dispositivo y la información y las acciones asistidas por IA.

Resultados más informados

Aplica de forma proactiva políticas específicas y solucione los problemas de los endpoints con análisis hipotéticos, orientación práctica y una comprensión profunda del estado del dispositivo, el usuario y la aplicación.

Gestión simplificada de la postura

Traduce rápidamente la intención empresarial en configuraciones y políticas recomendadas y compatibles mediante lenguaje natural.



Security Copilot in Microsoft Entra

Investigación rápida de riesgos de identidad

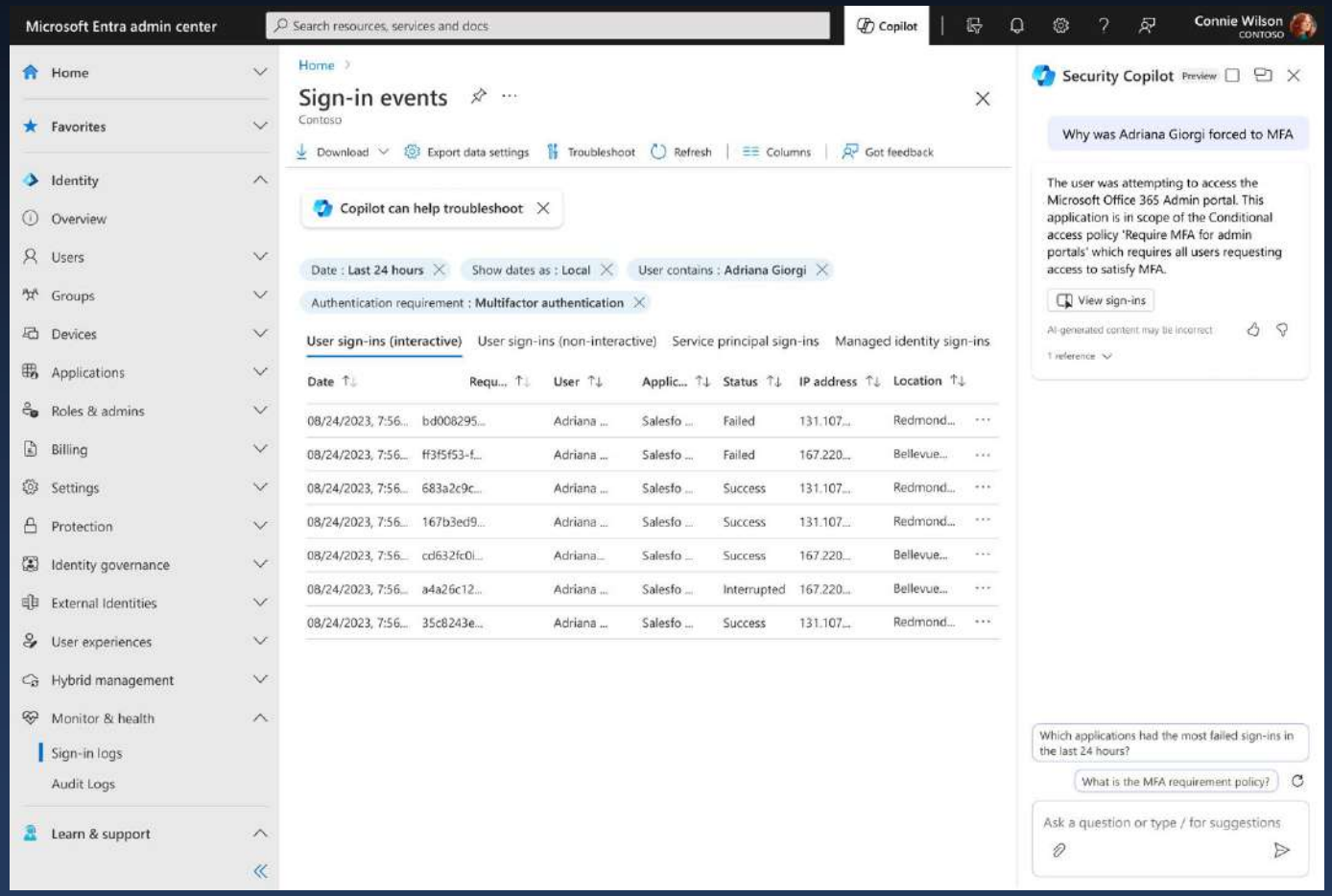
Explora los inicios de sesión y los usuarios de riesgo, comprendiendo el "por qué" y obteniendo información contextualizada sobre qué hacer para proteger las cuentas, todo en lenguaje natural.

Solución de problemas más rápido

Con el contexto al alcance de la mano, se encuentran brechas en las políticas de acceso, generando flujos de trabajo de identidad y llegando a la raíz del problema más rápido.

Nuevos niveles de eficiencia

Las recomendaciones guiadas permiten a los administradores de todos los niveles completar tareas complejas, como investigaciones de incidentes. El análisis del registro de inicio de sesión elimina la necesidad de realizar una inspección manual.



Security Copilot in Microsoft Purview

Visibilidad escalada

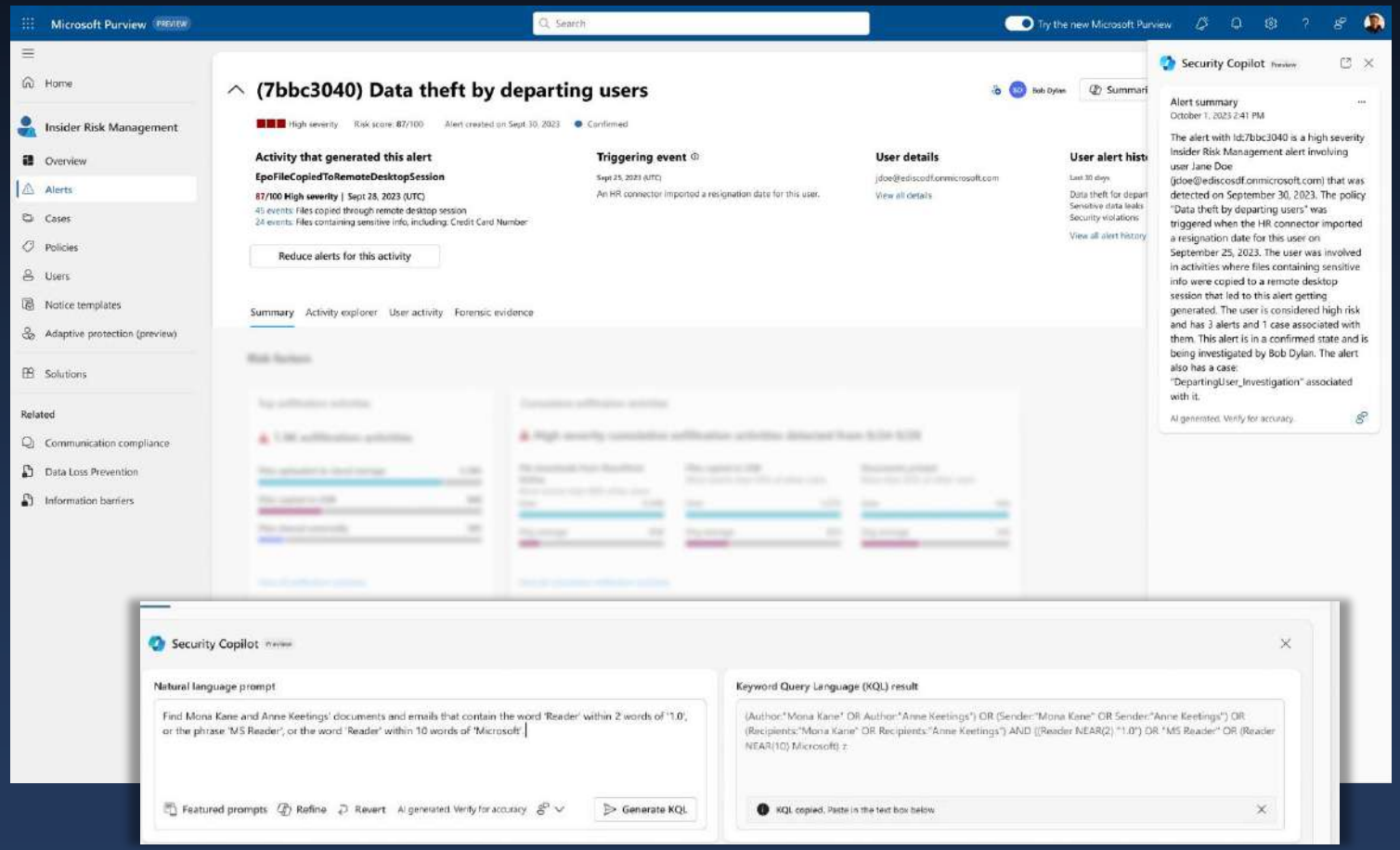
Visibilidad completa e integrada de todas las soluciones y una visión de los requisitos normativos de cumplimiento relevantes.

Resumen para la velocidad

Resumen rápido de las alertas que contienen una amplia gama de señales y contenido extenso para revisarlas desde el punto de vista de las políticas de seguridad y cumplimiento de datos.

Desbloquea habilidades expertas

Orientación paso a paso, realizando búsquedas en lenguaje natural y realiza investigaciones avanzadas sin lenguaje de consulta de palabras clave.



Security Copilot in Microsoft Defender for Cloud

Comprensión rápida de la postura

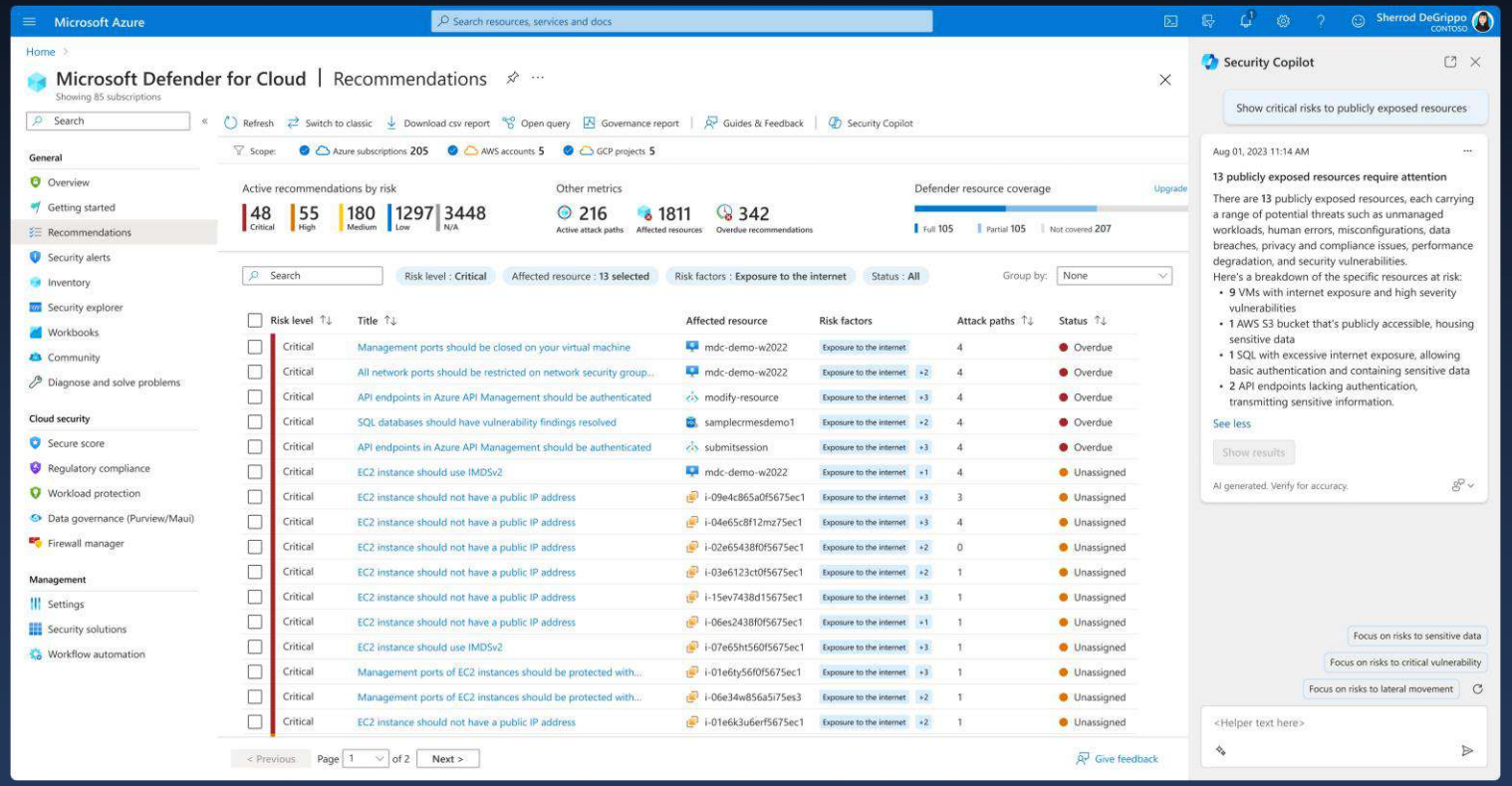
Identifica los riesgos más rápido aprovechando la información contextual de los datos confidenciales, las vulnerabilidades críticas, el movimiento lateral y mucho más.

Corrección guiada

Profundiza los riesgos críticos y recibe recomendaciones guiadas para priorizar las acciones de corrección más rápido, todo en lenguaje natural.

Trabaja de forma más inteligente

Información contextual sobre el riesgo, desgloses resumidos y orientación paso a paso a lo largo de una investigación. Identifique rápidamente a los usuarios clave y delegar la corrección.



Microsoft Defender Threat Intelligence (MDTI)

Inteligencia de amenazas terminada

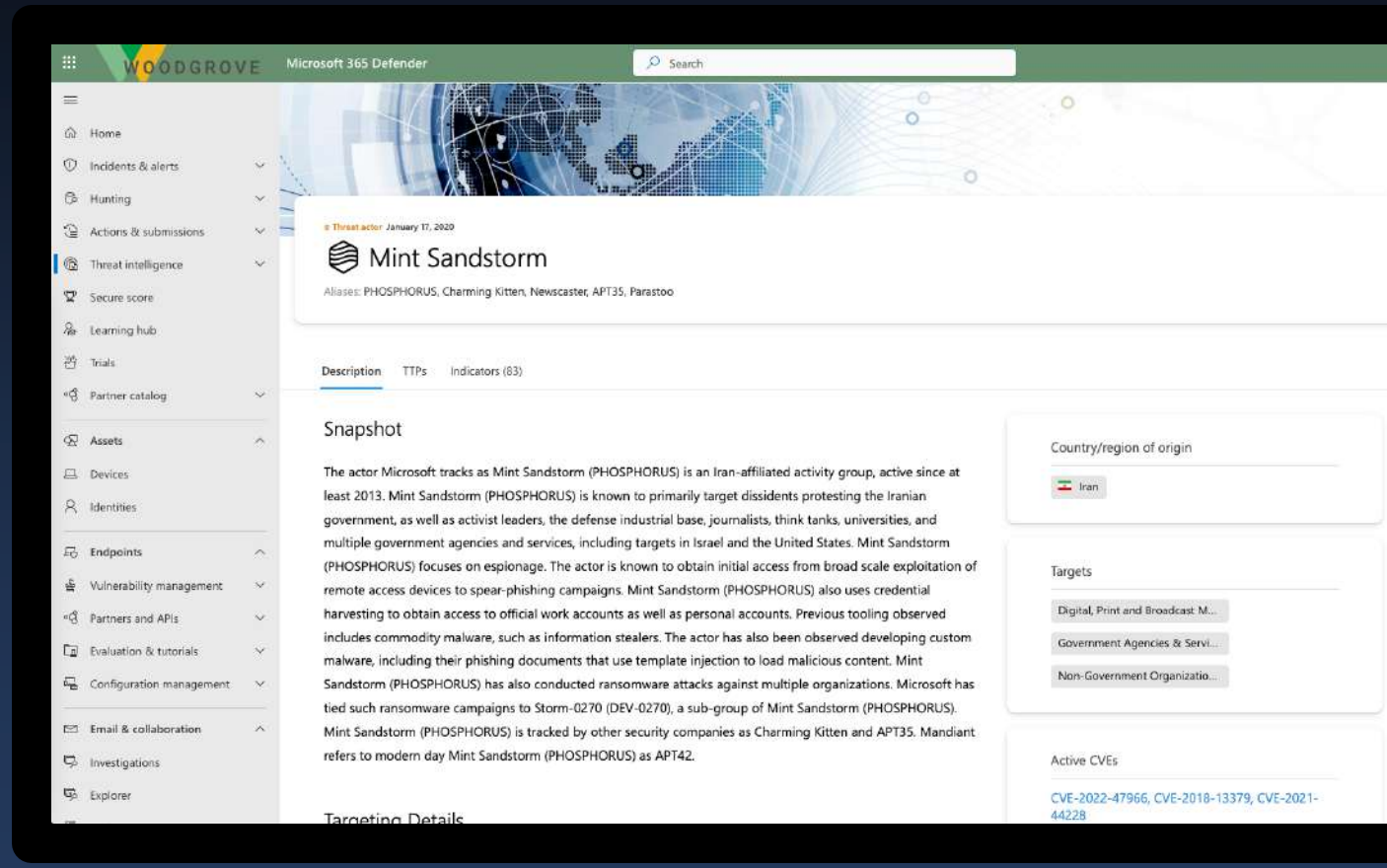
Consulte una biblioteca de artículos de inteligencia terminados, perfiles de inteligencia e informes de actividad, incluidos indicadores procesables y TTP creados y mantenidos por 10.000 expertos en seguridad para comprender y contextualizar rápidamente las amenazas.

Inteligencia de amenazas sin procesar

Pivote sobre conjuntos de datos únicos creados a partir de la detección automatizada y el análisis continuo en toda la infraestructura mundial para ayudarle a comprender la gravedad de una amenaza, bloquear los ataques de forma proactiva e inocular a la organización de futuras amenazas.

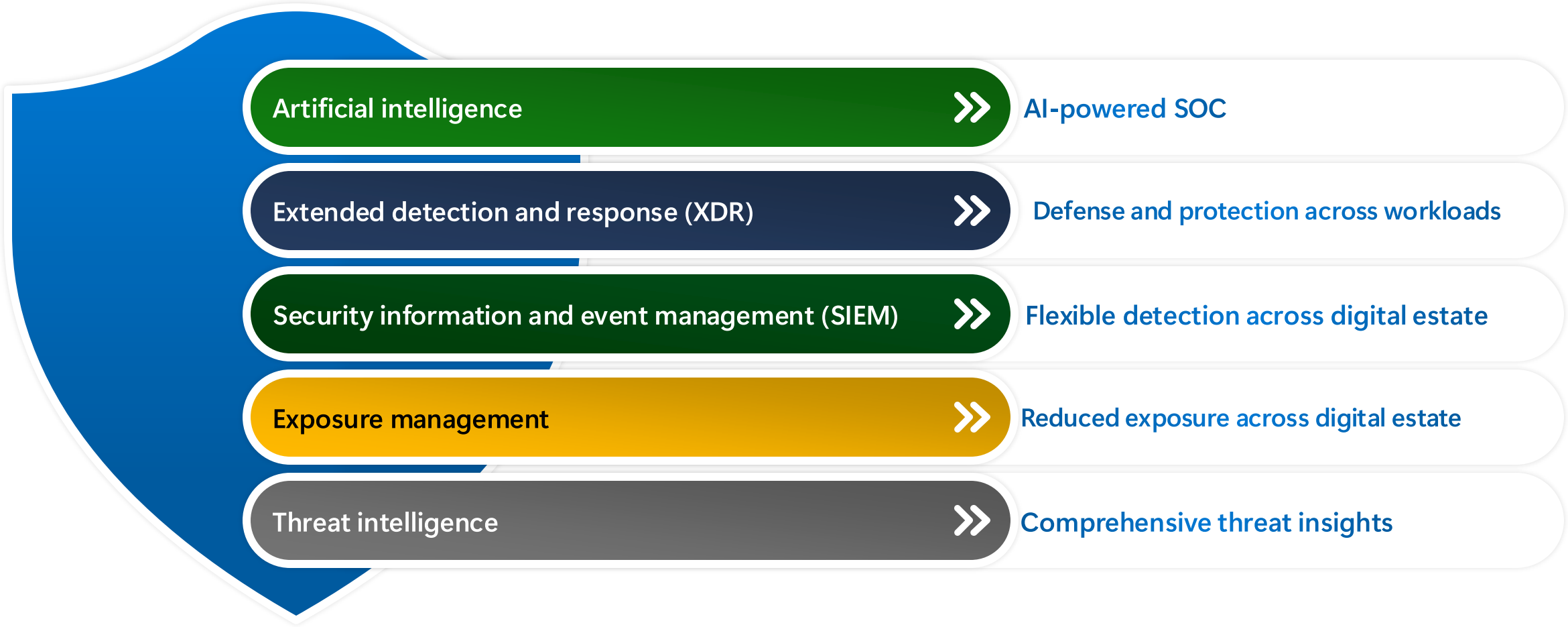
MDTI API

Mejore las herramientas y los flujos de trabajo existentes de SIEM y XDR enriqueciéndolos con inteligencia de amenazas hiperrelevante y un profundo conocimiento del panorama global de amenazas.



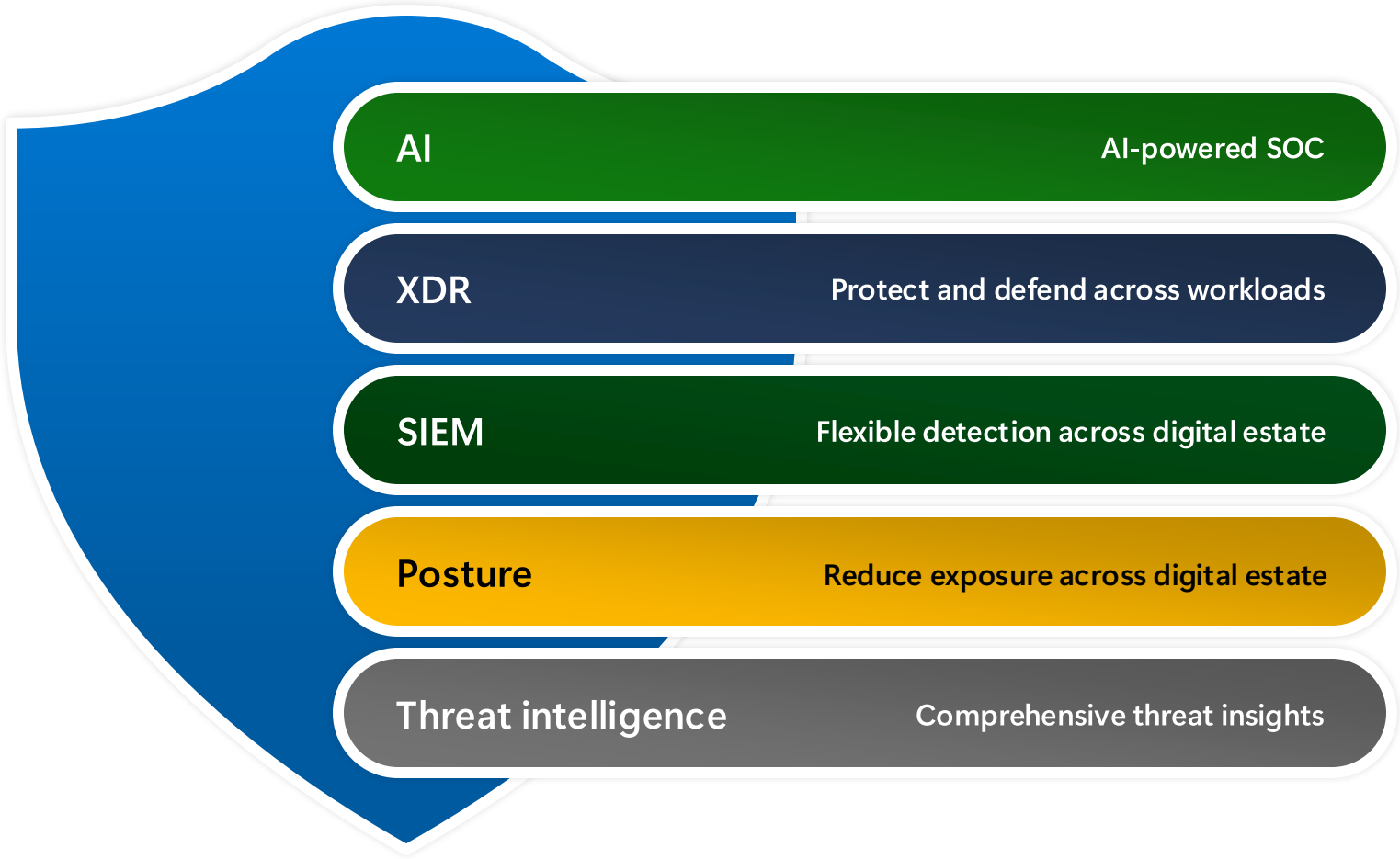
Under NDA only

Transforme SecOps con una Plataforma unificada



Construido desde cero para operaciones de seguridad

Experiencia de analista optimizada | 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 remediation
- Vulnerability management
- Attack surface insights
- Remediate risk

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

Microsoft Security Exposure Management

Reduzca su exposición al riesgo

Reducción de la superficie expuesta a ataques con una gestión unificada de la exposición

Exposure management
Overview
Attack surface
Map
Attack paths
Exposure insights
Initiatives
Metrics
Recommendations
Events
Secure score
Data connectors
Assets
Endpoints
Identities
Email & collaboration
Cloud apps
Reports
Health
Permissions
Settings
More resources

Exposure management overview

Add a suggestion | Guided tour

How protected is your organization?

Our security exposure management tool offers key insights, metrics and customized initiatives for a centralized overview of your risk landscape.

Your assets, at a glance

- Onboarded devices: 33
- Discovered devices: 589
- Internet facing devices: 0
- Cloud resources: 18.4k
- Identities: 7.7k

Vulnerability status

- Devices with Critical vulnerabilities: 118
- Devices with High vulnerabilities: 79
- Devices with Zero day vulnerabilities: 0

Key initiatives

See all

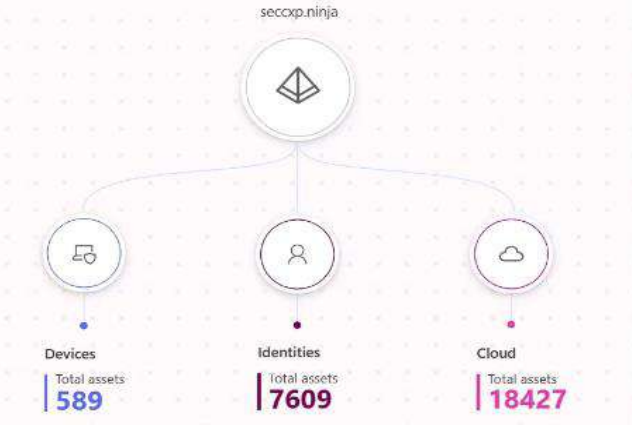
Ransomware Protection	Endpoint Security	Business Email Compromise - Financia...	Cloud Security [Preview]
60%	50%	74%	84%
↑ 3% (last 14 days)	No change (last 14 days)	↑ 10% (last 14 days)	↓ -1% (last 14 days)

Top metrics

Name	Current V
% of missing best practices for devices against "On-premise...	100%
% of endpoints where the host Firewall is disabled or misco...	100%
% Azure relational database without geo-redundant backup...	100%
% containers images with high severity vulnerabilities	100%
% of missing best practices in Sharepoint Admin Center to ...	100%
% storage accounts without network access restriction usin...	99.17%

Attack surface map

Search



Critical asset summary

Critical assets: 2824

Critical asset management

View in device inventory

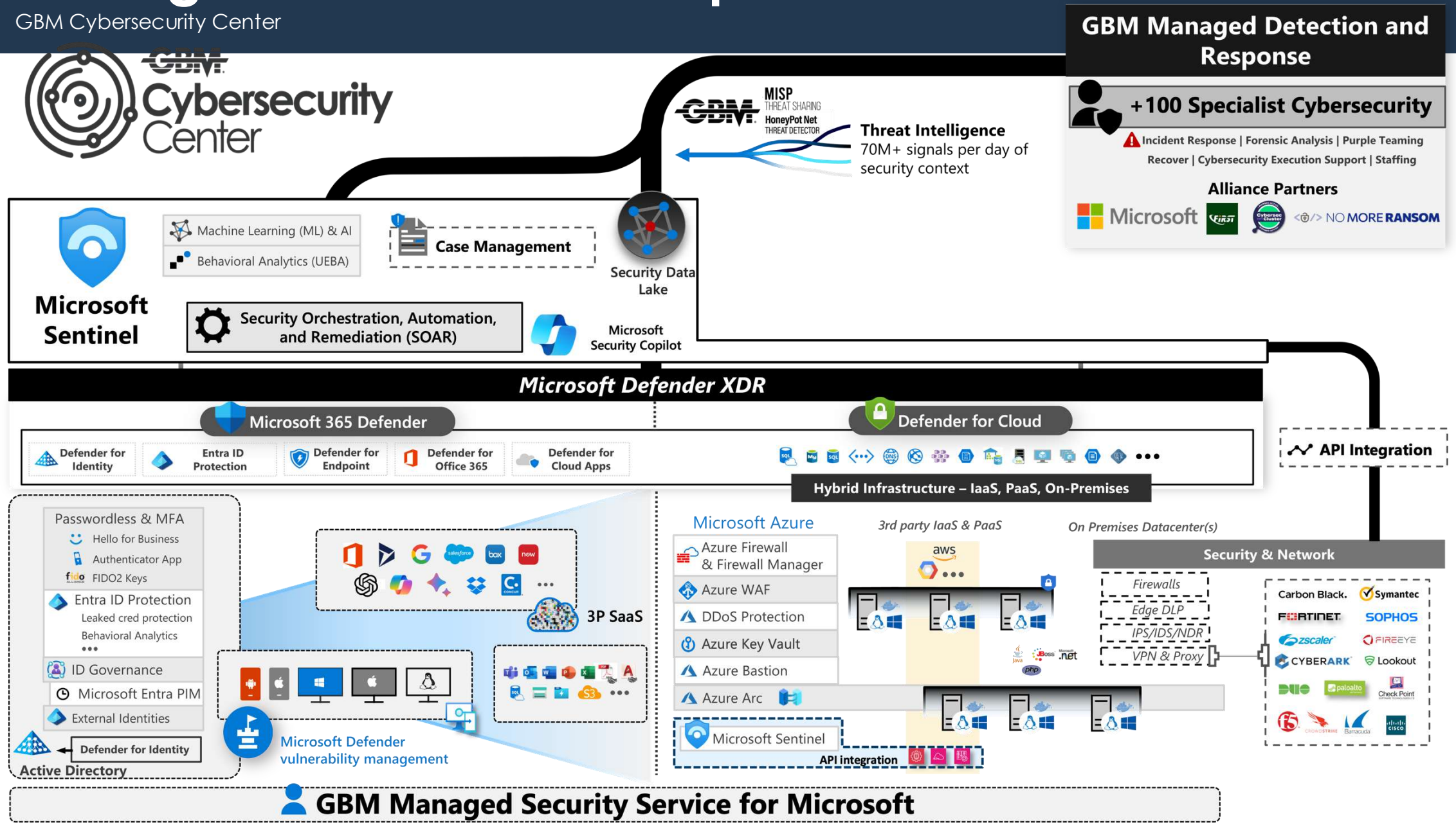
- Critical devices: 20
- Highly-exposed critical devices: 7
- Critical devices with high risk: 1
- Internet-facing critical devices: 3

View in advanced hunting

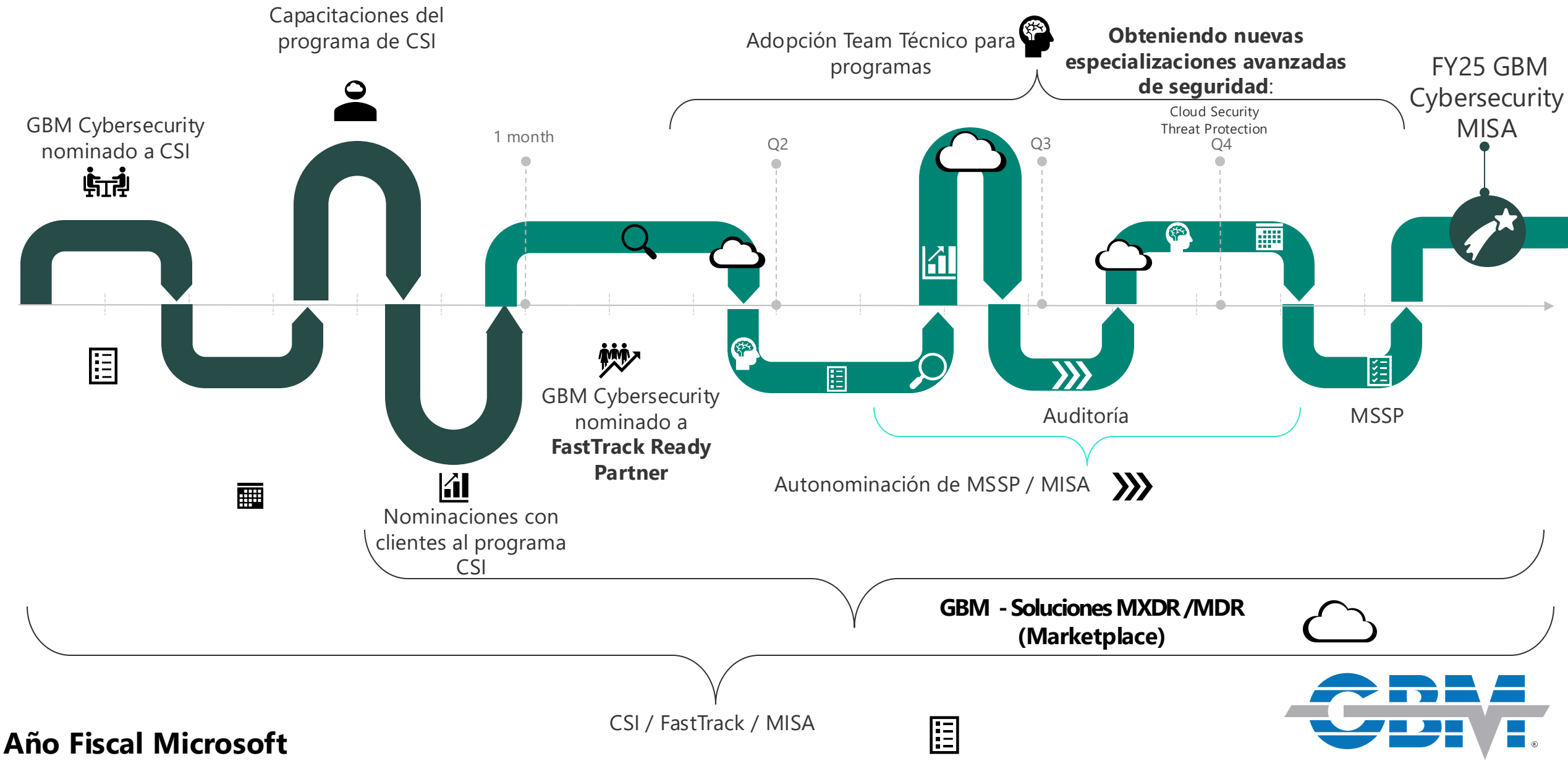
- Critical identities: 1669
- Critical cloud resources: 1135

Managed Detection & Response for Microsoft

GBM Cybersecurity Center



GBM Cybersecurity FY25 | Overview



Año Fiscal Microsoft

GBM Cybersercurity Investment

GBM en las Américas ahora forma parte de la iniciativa de **Inversión en Ciberseguridad (CSI) de Microsoft.** El programa de CSI es una inversión solo por invitación realizada por Microsoft a socios que cumplan ciertas especializaciones avanzadas de seguridad. Esta inversion está diseñada para acelerar **la adopción de plataformas de seguridad Microsoft 365 y Azure Security** a través de actividades de consultoría con los clientes.

Esta inversion tiene un alcance de dentro del año fiscal de Microsoft (FY25) el cual, nos permite posicionar a GBM como un asesor de seguridad de confianza.

- Threat Protection Engagement (Microsoft Defender XDR)
- Data Security Engagement (Microsoft Purview)
- Modern Sec Ops (Microsoft Sentinel / Microsoft Copilot for Security)

Requisitos: (**+500 licencias de Microsoft Entra ID Premium P1 y +250 usuarios activos en Exchange Online, SharePoint Online or Teams**).

Threat Protection Engagement

Pre-engagement Call
– 1 hour

- Introductions
- Engagement walk-through
- Expectations
- What's next

Engagement Questionnaire

Fill in and return the questionnaire

- Other pre-engagement preparations

Readiness (Optional)
– 1 hour

- Threat Protection Overview presentation

Kick-Off Meeting – 2 hours

- Engagement walk-through
- Engagement tools
- Expectations
- What's next

Define Scope – 2 hours

- Finalize "Selectable Modules"
- Define and document deployment scope

Change Management (Optional)

- Customer to go through their change management process and obtain approval for configuration changes as per defined scope

General Setup – 0.5 hour

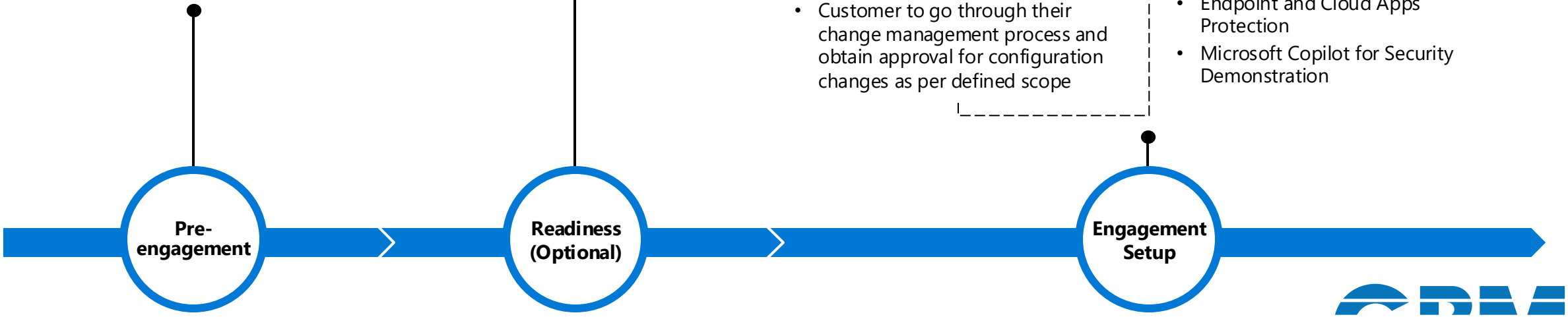
- Setup trial licenses
- Configure tenant

Mandatory Modules – 1 hour

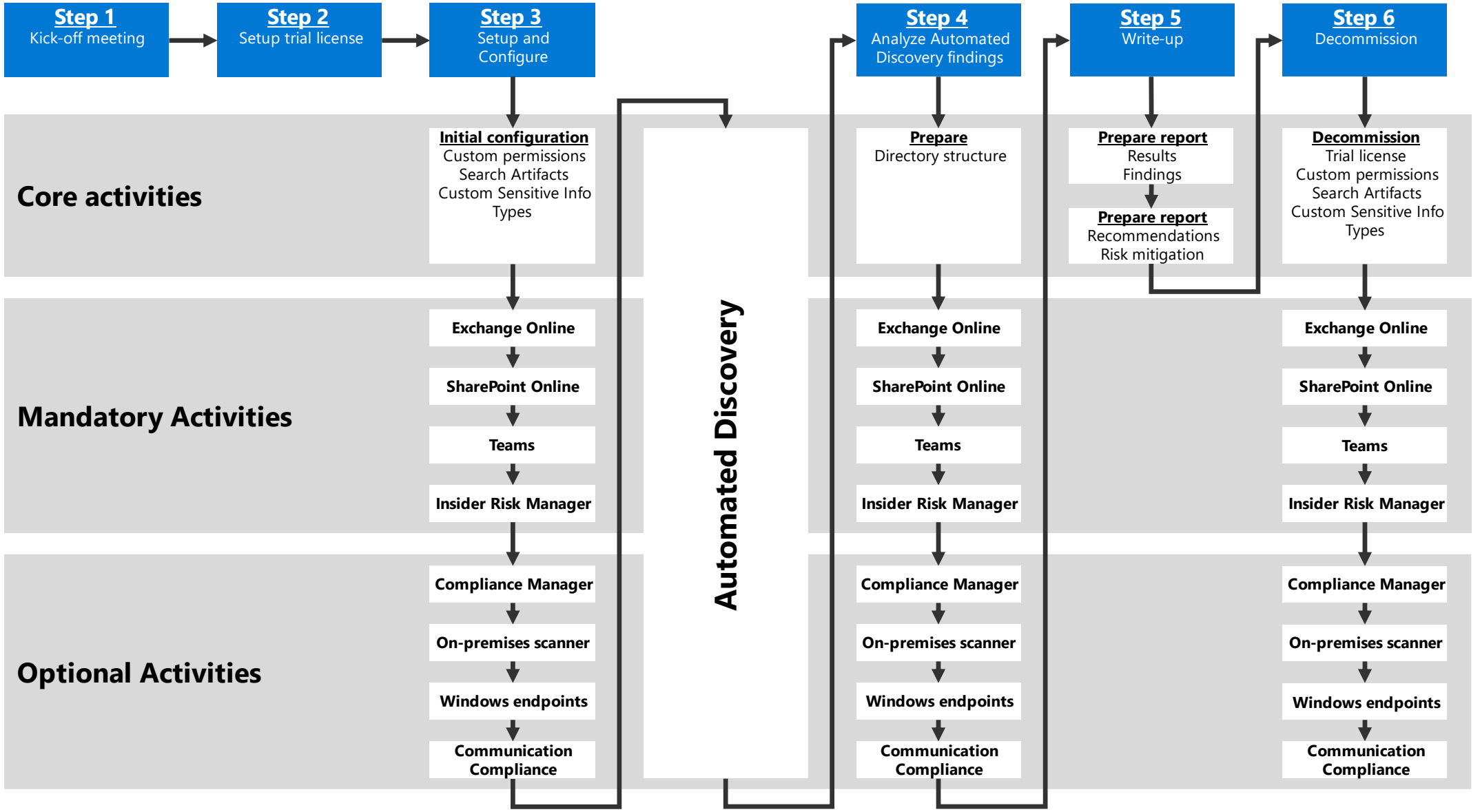
- Microsoft Defender Portal
- Cloud Identity Protection

Selectable Modules – 4-6 hours*

- Unified SecOps Platform
- Email Protection
- Endpoint and Cloud Apps Protection
- Microsoft Copilot for Security Demonstration



Data Security Engagement



FAQ’S


¡Gracias!
ευχαριστώ
Salamat Po
متشكرم
شكراً
Grazie
благодаря
ありがとうございます
Kiitos
Teşekkürler
谢谢
ขอบคุณครับ
Obrigado
شكريه
Terima Kasih
Dziękuję
Hvala
Köszönöm
Tak
Dank u Wel
дякую
Tack
Mulţumesc
спасибо
Danke
Cám ơn
Gracias
多謝晒
Ďakujem
תודה
நன்றி
Děkuji
감사합니다