

Microsoft Security Summit

Sécurisez vos fondations, libérez votre potentiel IA

Le 9 décembre 2025 | 9h00 – 17h00

Campus Cyber La Défense, 5-7 rue Bellini La Défense Ile de France 92800

Agenda Matin

09:30 - 10:00

Transformation through AI equals transformation of security – Paul Dominjon & Steve Dispensa

10:00 - 10:40

IA & cybersécurité : quels contrôles mettre en place pour la protection de vos données ? -
Guillaume Lagache & Saïda Laga

10:40 - 11:00

Pause & Village Partenaires

11:00 - 11:30

Table ronde : « Leadership en cybersécurité à l'ère de l'IA » Business France, La Poste

11:30 - 12:00

Les engagements de Microsoft sur la souveraineté des données - Cyril Voisin

12:00 - 12:30

NIS2/DORA : Des outils concrets pour renforcer votre cyber résilience - Etienne Lacour & Marina Djouadi

12:30 - 14:00

Déjeuner & Village Partenaires

Agenda après-midi

14:00 - 14:30

Anticipez, analysez, agissez : gardez une longueur d'avance sur les attaques – Khadidiatou Ba & Daniel Pasquier

14:30 - 15:15

Le SOC du futur à l'ère de l'IA agentique – Etienne Noiret & Rafik Mezil

15:15 - 15:45

Pause & Village Partenaires

15:45 - 16:15

Du chaos au contrôle - Maîtriser la réponse aux incidents – Anne-Sophie Le Jouan & Saad Nidifi

16:15 - 16:45

10 000 employés et 5 000 agents IA - Sécuriser l'identité à l'ère de l'IA – Franck Heilmann & Christophe Guerre

16:45

Final words

Transformation through AI equals transformation of security



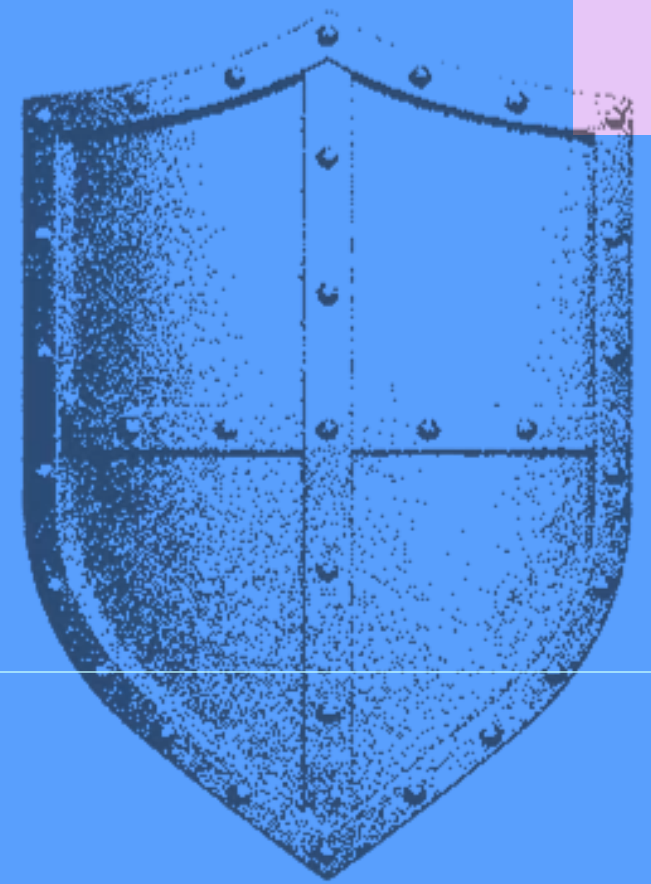
Paul Dominjon
Director Security Solutions



Steve Dispensa
CVP Security Solutions Area



Trust starts here



Securing beyond
boundaries

Steve Dispensa

CVP, Microsoft Security Solution Area



Ο ΠΕΡΙΚΛΗΣ ΑΓΟΡΕΥΕΙ

From
complexity
to trust



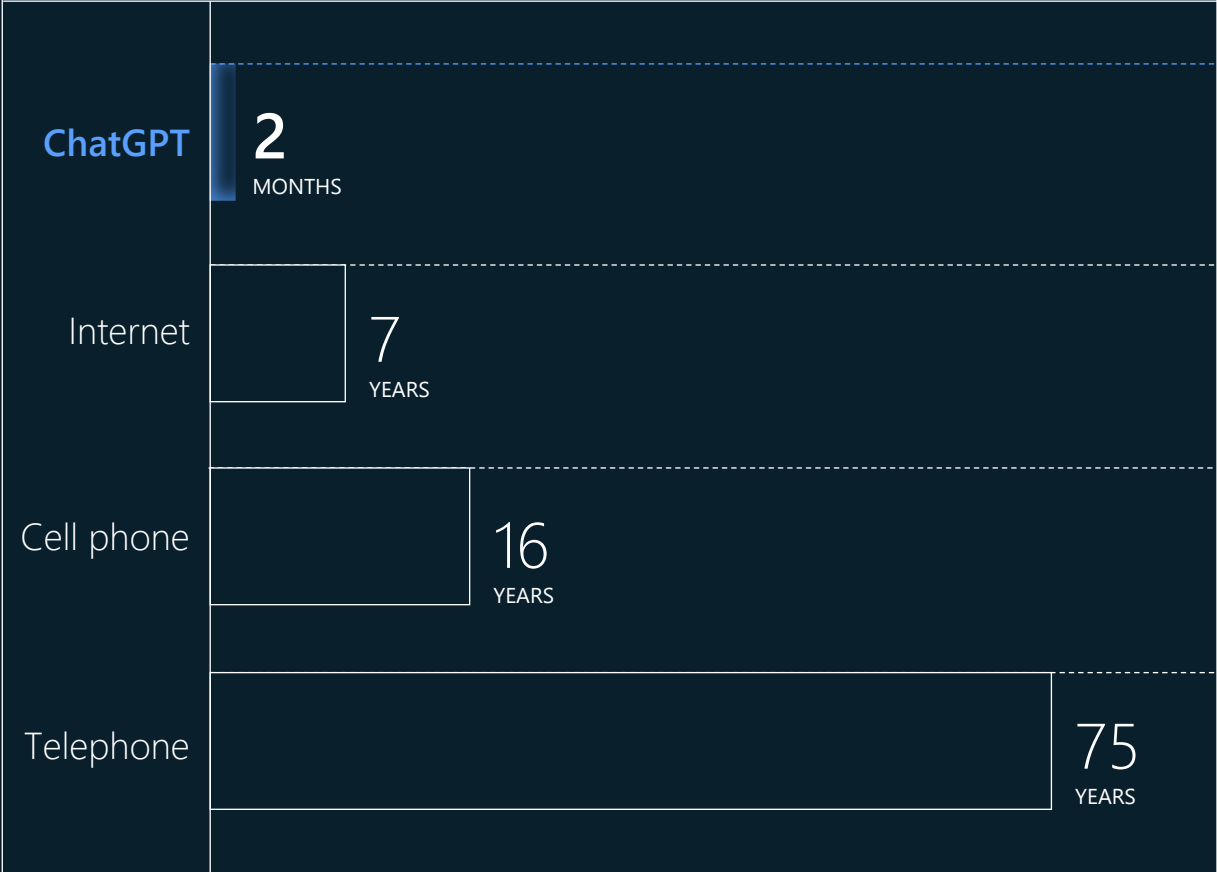
Secure AI

Building trust in a fast-moving world



AI is becoming foundational

Time to 100M users



1.8B+

People globally have used AI tools at work, in school in the last 6 months.

75%

Of organizations use GenAI in some form

AI is accelerating both sides:

30%

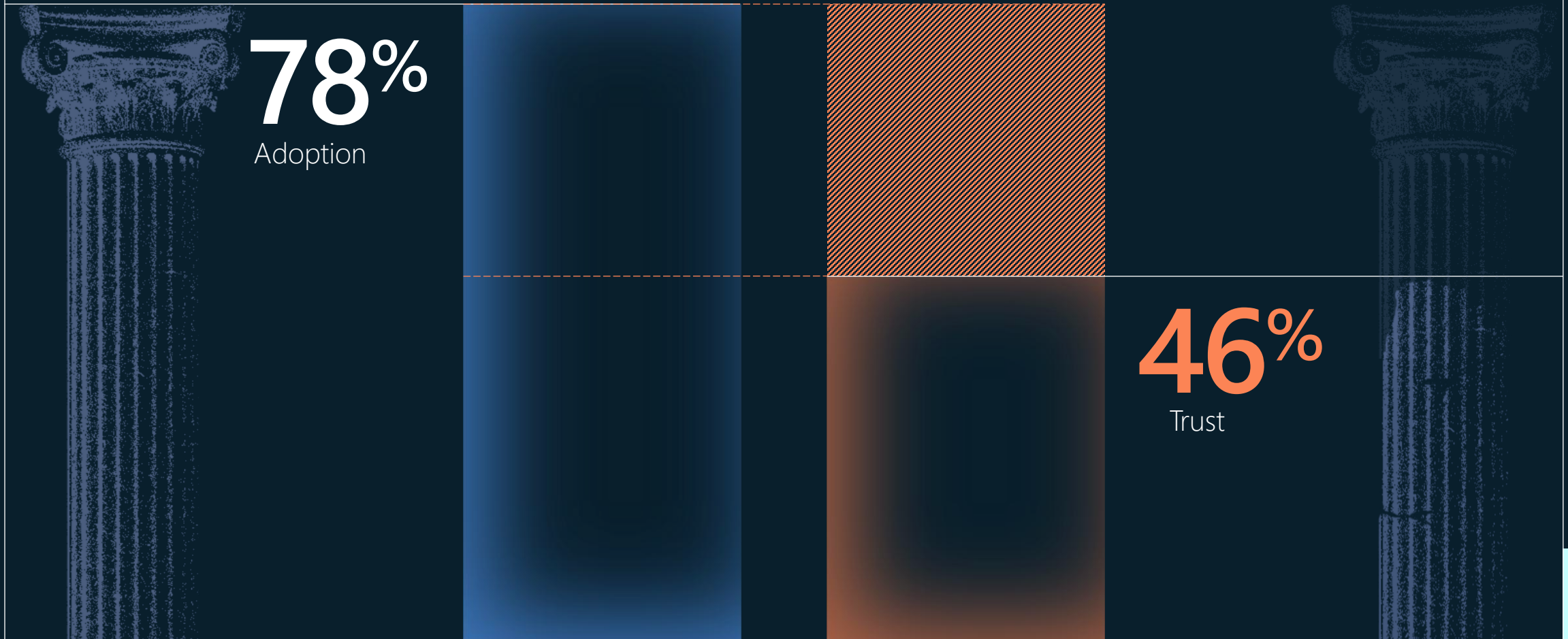
while

54%

Of defenders use AI tools

Of security pros report attackers using AI to increase threats

AI adoption is outpacing trust



Navigating
complexity
together



We face an unprecedented threat landscape

Speed

Average time from initial access to lateral movement (in 2025)

48
minutes

Fastest observed: 00:51

Scale

Security signals processed daily (2025)

78T
2024

100T
2025

Sophistication

Threat groups tracked by Microsoft (2025)

300+
2023

1.5K
2025

AI creates new attack surfaces

Traditional threat vectors				New AI attack surfaces			
	Application		Cloud		GenAI prompts and responses		Plug-ins and functions
	Network		Identity		AI Data and Orchestration		
	Data		Endpoints		Web data and source context		AI Models

Organizations are overwhelmed with complexity

A disconnected collection
of fragmented tools

41-60

Tools used by ~26% of organizations
surveyed by IDC

Widening
workforce gap Europe

400K

Cybersecurity professionals needed to
effectively secure organizations



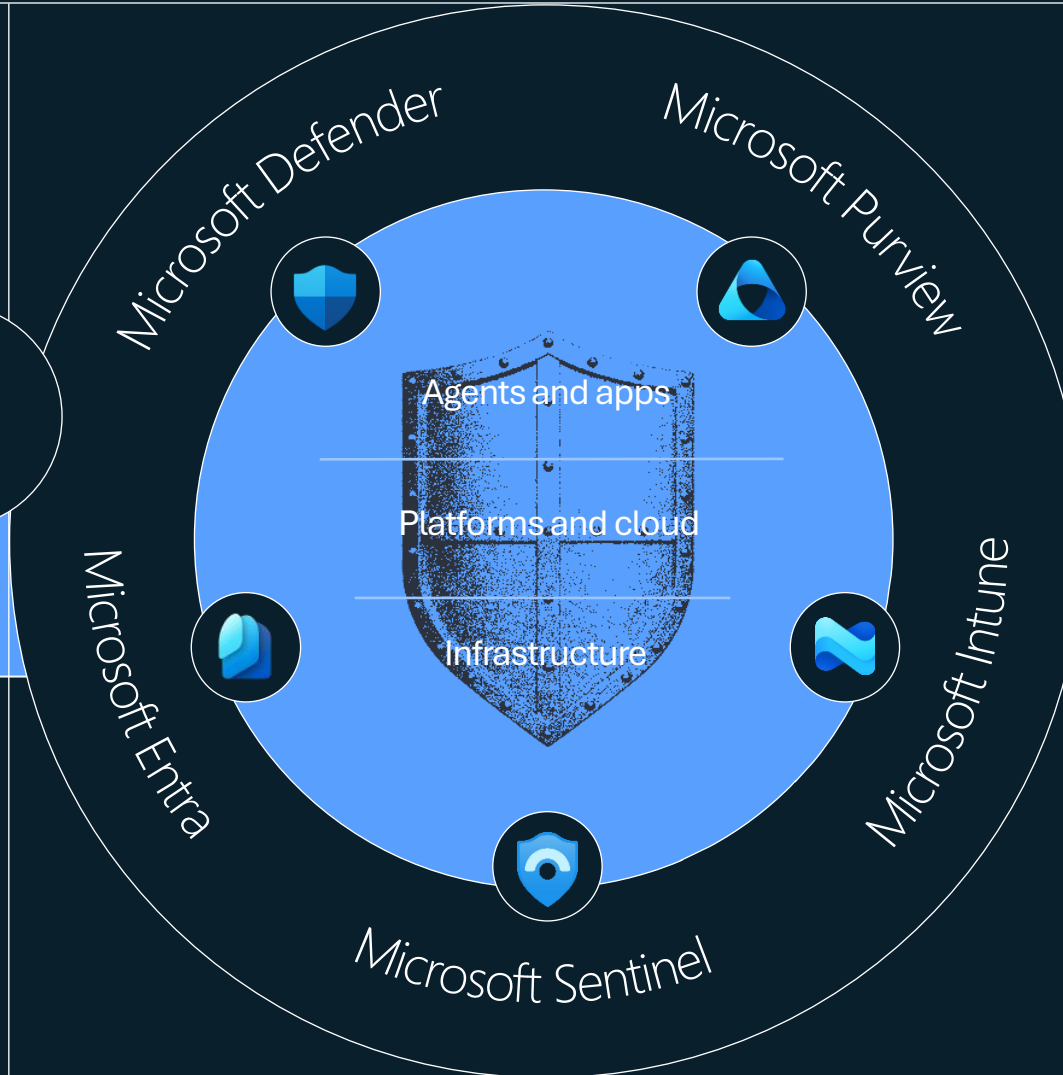
“ For Microsoft,
security is our **#1 job...**

Microsoft runs on **trust**,
& our success depends on
earning and maintaining it. ”

Satya Nadella ■ Chairman & CEO, Microsoft

Advancing our AI-first, end-to-end security platform

Threat intelligence
Powered by 100 trillion signals¹



Protecting
Microsoft and
our customers

Security services
Incident Response | Managed Services |
Dedicated Engineering

¹Based on Microsoft internal data. Accurate as of July 2025

Our solutions for today's security challenges

Modernize your security operations

Simplifying security operations and addressing tool fragmentation



Protect your data

Mitigating data security risks



Protect your cloud and AI

Detect and protect against cloud and AI risks



Weaving security into
and around every layer
of the AI stack



Agents and apps

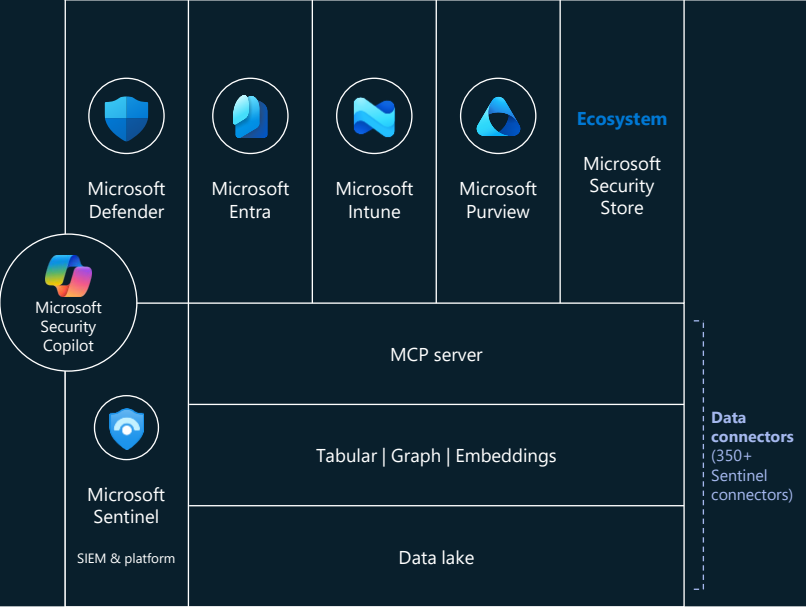
Platforms and cloud

Infrastructure

Security in the Age of Agentic AI

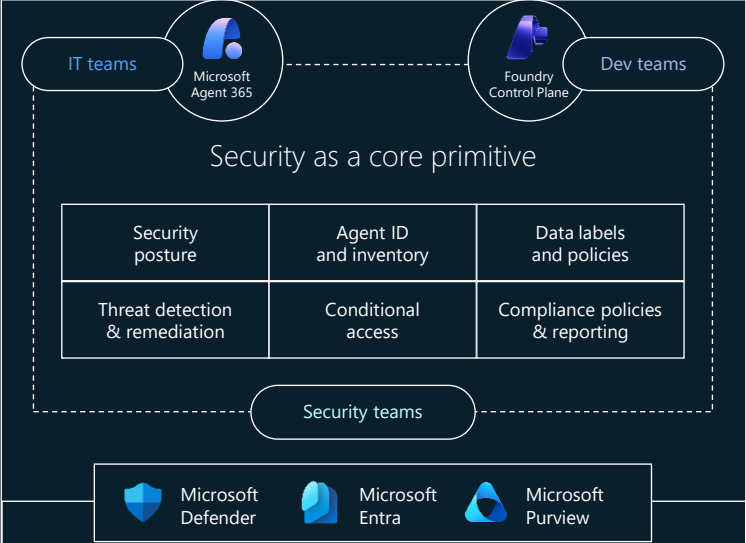
Secure with Agentic AI

AI-powered protection before harm occurs



Secure AI agents & apps

Delivering observability for every role



Secure Platforms and Cloud

AI powered end-to-end security



Protecting organizations at a global scale

\$80B

AI infrastructure
Investment in 2025

120+

countries

100T

security signals
processed daily

5B

emails screened daily for
malware and phishing

34k

security engineers
worldwide

38M

Identity risk detections
analyzed daily

15k

security partners in
our ecosystem

1M

organizations
protected

4.5M

new malware files
blocked daily

99%

lower risk of identity
compromise with
phishing-resistant MFA



Security makes
progress possible

From
complexity
to trust



“ We know
what we are,

but know not
what we
may be. ”

William Shakespeare ■ *Hamlet*



IA & cybersécurité

Quels contrôles mettre en place
pour la protection de vos données



Guillaume Lagache

Solution Engineer
Cybersecurity

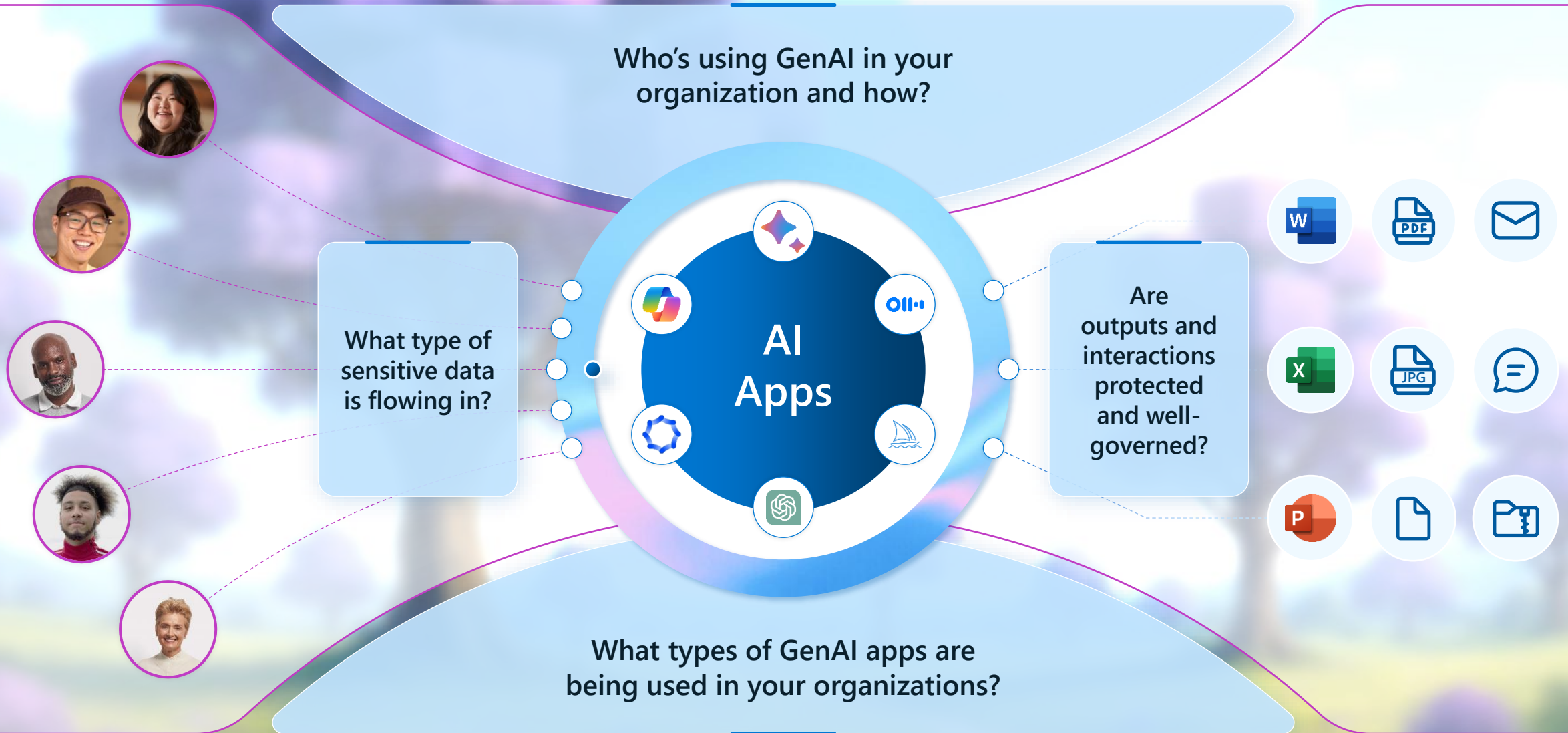


Saida Laga

Solution Engineer
Cybersecurity



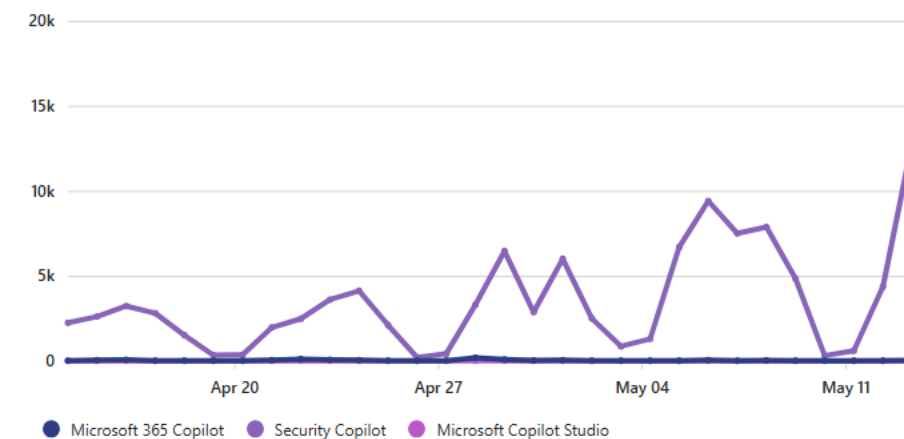
We are living in an AI first world



Activity

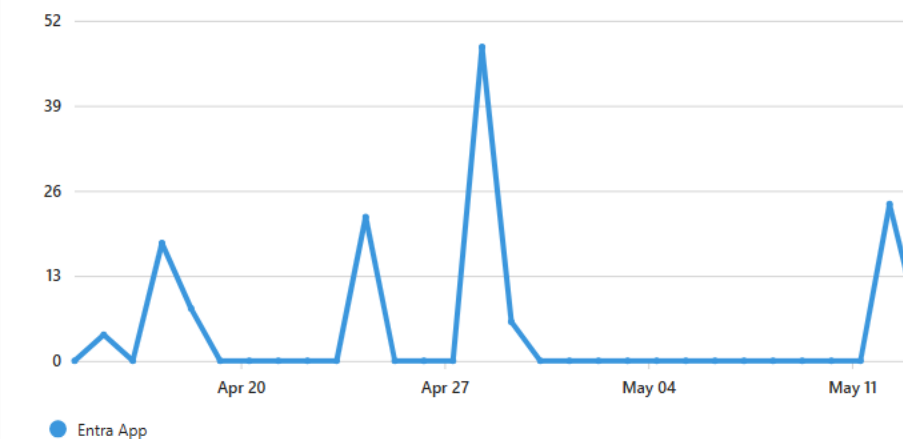
Total interactions over time (Microsoft Copilot and agents)

106,505 activities in the last 30 days

[View details](#)

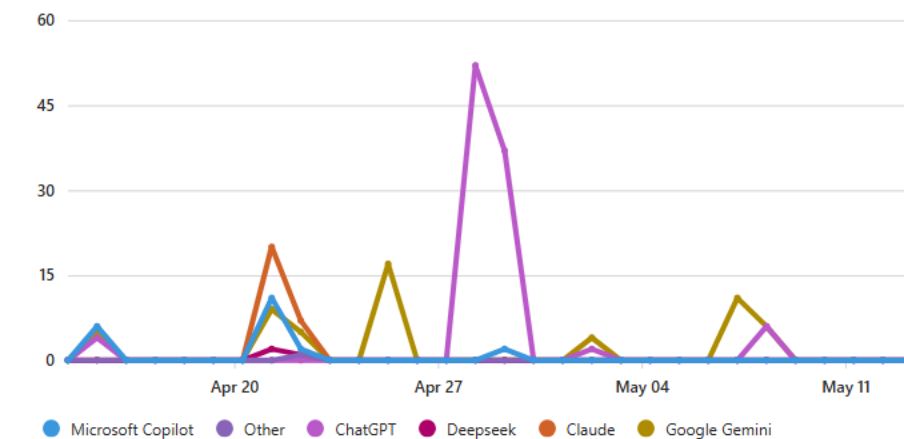
Total interactions over time (enterprise AI apps)

136 activities in the last 30 days

[View details](#)

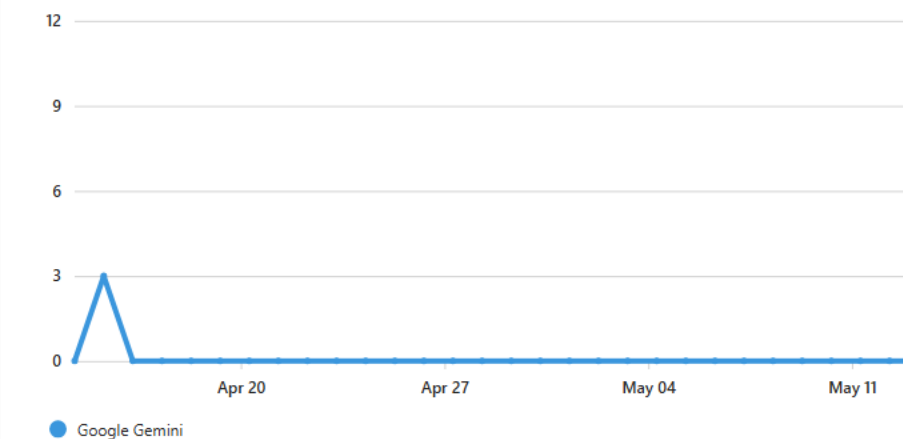
Total visits (other AI apps) ⓘ

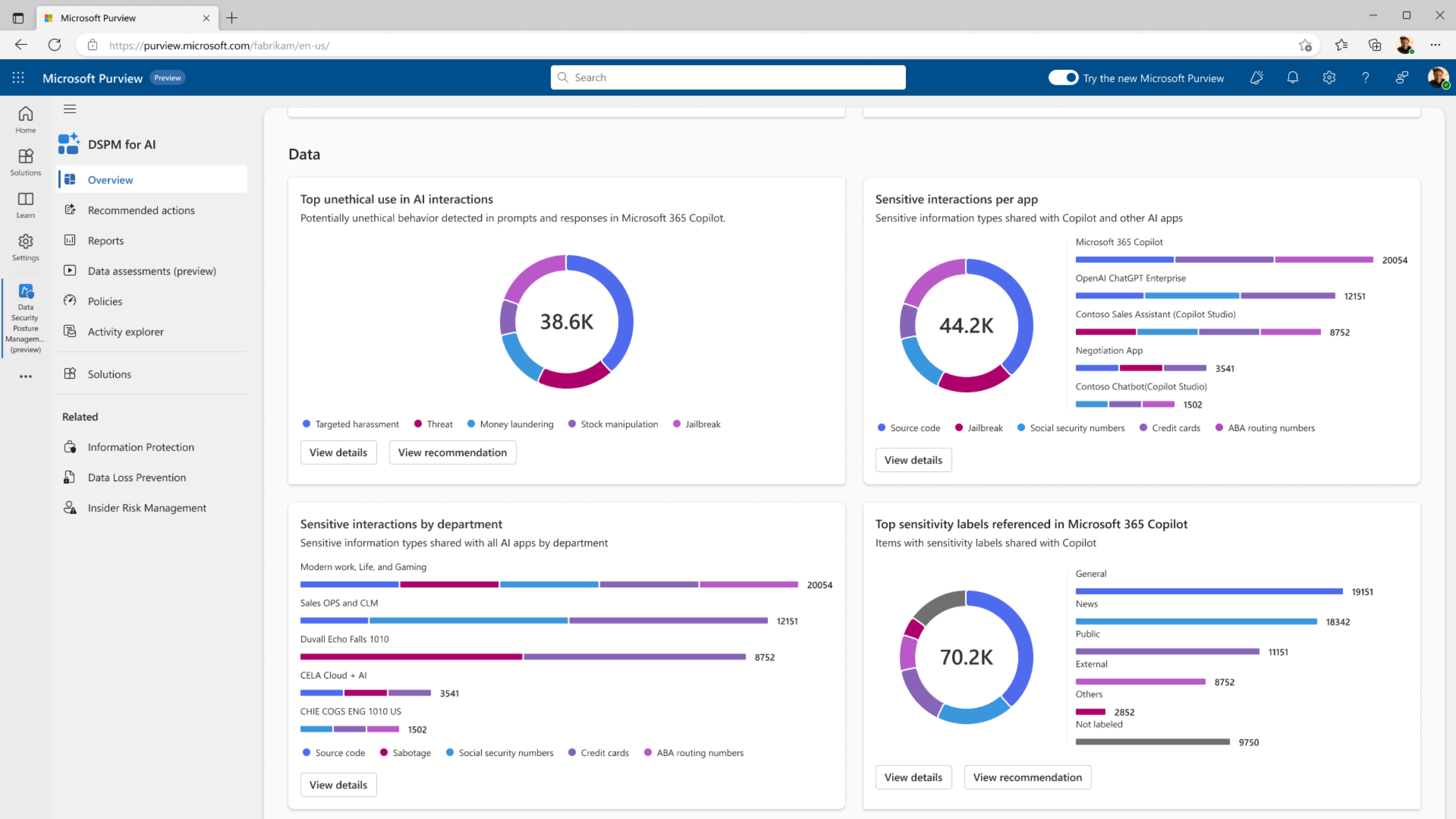
210 activities in the last 30 days

[View details](#)

Total interactions over time (other AI apps)

3 activities in the last 30 days

[View details](#)



- Home

Solutions

Agents

Learn

Settings

DSPM

Information protection

...

Tasks and actions

Setup tasks

Remediation actions

Reports
- DSPM (preview)

Posture

Objectives

AI observability (preview)

Discover

Apps and agents

Data risk assessments

Activity explorer

Asset explorer

Tasks and actions

Setup tasks

Remediation actions

Reports

Data security objectives

View and track data security objectives for your organization. Each objective highlights key risks to address, actions to take, and progress over time. This helps your organization stay aligned with your overall data security posture. [Learn more](#)

6

- Data discovery
- Data protection
- Data investigation

Data protection | Microsoft 365 Copilot

Prevent data exposure in Microsoft 365 Copilot interactions

30,916 Microsoft 365 Copilot and Microsoft Copilot interactions with sensitive data were detected from your organization in the last 30 days, an increase of 5%. This could indicate emerging patterns of data exposure.



30.9K interactions



25.2K ↗ +2%

User prompts

256 ↗ +3%

Files overshared

View remediation plan

View agent activity

Copilot prompts

View objective →

Take action to reduce risk

Taking action could reduce sensitive interactions from 30.9K to 22K, which is about a 29% decrease.

Data protection | Oversharing

Prevent oversharing of sensitive data

32,729 items are unlabeled and contain sensitive data from Microsoft 365 and Microsoft Fabric in the last 30 days, an increase of 4%. This could indicate emerging patterns of oversharing sensitive data.



21.1K files overshared



4.2K ↗ -2%

Files with sensitive data not labeled

356 ↗ -3%

Files shared externally

View remediation plan

View agent activity

Copilot prompts

View objective →

Take action to reduce risk

Taking action could reduce oversharing files from 32.7K to 16.3K, which is about a 50% decrease.

Data protection | Exfiltration

Data protection | Exfiltration

!

Prevent exfiltration to risky destinations

Prevent sensitive data from reaching risky destinations via email, devices, or cloud apps by enforcing controls that detect and block exfiltration attempts.

2.4K files at risk

↑ +5% in last 30 days

1.2K ↗ +2%

Files sent to personal domain

950 ↗ +3%

Files sent to external cloud

360 ↗ +3%

Files saved to USB

View remediation plan

View agent activity

Copilot prompts

Take action to reduce risk
Taking action could reduce exfiltrated files from 2.4K to 1.1K, which is about a 54% decrease.
View objective

Data discovery | AI apps

!

Discover unmonitored data sources referenced by AI apps

2,956 AI app interactions referenced unmonitored data sources in the last 30 days, an increase of 4%. Microsoft Purview supports these data sources but can't monitor them until they're connected. To discover and protect these data sources in DSPM, connect them to Microsoft Purview through partner-built connectors.

2.9K AI app interactions

↑ +4% in last 30 days

25 ↗ +2%

Domains belonging to these data sources

1.5K ↗ +3%

AI apps referencing these data sources

View remediation plan

View agent activity

Copilot prompts

Take action to reduce risk
Taking action could reduce AI interactions referring to unmonitored data sources to zero.
View objective

Data protection | Exfiltration

✓

Prevent exfiltration to unsanctioned AI apps

24,700 files were shared in unsanctioned AI apps in the last 30 days, a decrease of 5%. The risk is improving, but some sensitive data use in unsanctioned AI apps is still occurring.

24.7K files exfiltrated to AI apps

↓ -5% in last 30 days

1.2K ↘ -2%

Unique ChatGPT sessions

950 ↘ -3%

Unique Anthropic Claude sessions

360 ↘ -3%

Unique Microsoft Copilot sessions

View remediation plan

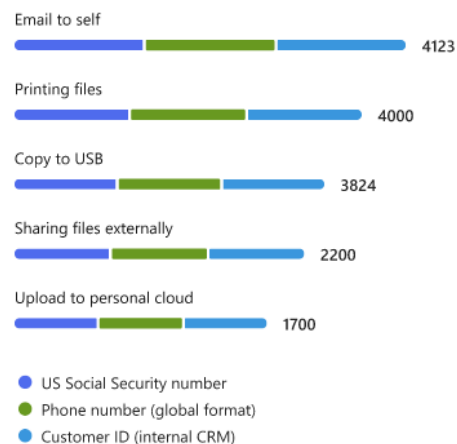
View agent activity

Copilot prompts

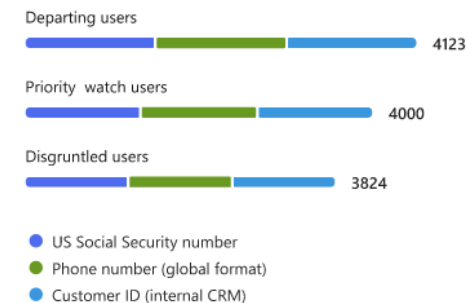
Monitor to identify new risks
No actions are required right now. New risks, such as data or users not covered by security controls can change your posture. Continuously monitoring your objectives helps protect your sensitive data.
View objective

[View exfiltration reports](#)

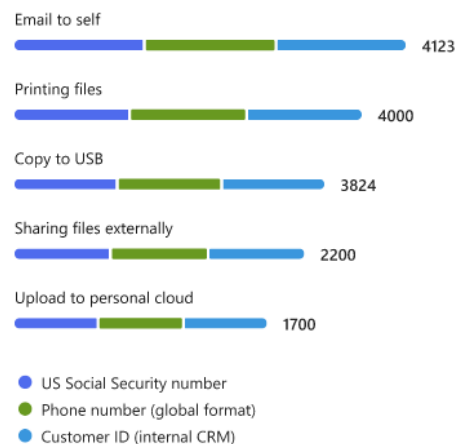
Review risk pattern



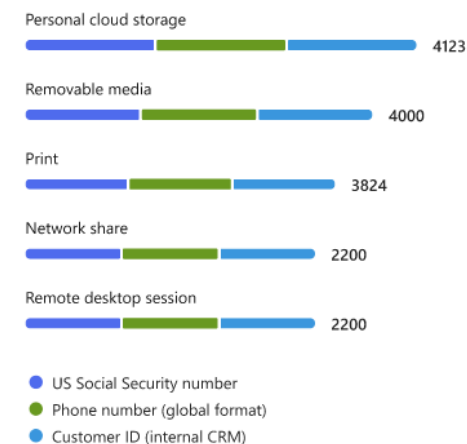
Review risk pattern



Review risk pattern



Review risk pattern



- Home

Solutions

Agents

Learn

Settings

DSPM

Information protection

...

DSPM (preview)

Posture

Objectives

AI observability (pre

Discover

Apps and agents

Data risk assessment

Activity explorer

Asset explorer

Tasks and actions

Setup tasks

Remediation actions

Reports

Risk pattern details: Files exfiltrated to personal accounts

Remediation plan to prevent exfiltration (4 actions)

Estimated impact: Reduce exfiltrated sensitive data by approximately 54%

View remediation plan

Number of items

Gmail

Outlook

Google Drive

Dropbox

Yahoo

iCloud

Hotmail

OneDrive

Box

AOL

External destinations

US Social Security number

Phone number (global format)

Customer ID (internal CRM)

Export

1,205 items

Filter

Filter by keyword

Activity type	User	Timestamp	Item	Internal data source	External destination	Sensitive info types
Email external to self	john.smith@example.com	August 5, 2023 11:00 AM	Presentation.pptx	OneDrive	Outlook	Public
Email external to self	alice.jones@sample.com	August 6, 2023 1:15 PM	Budget.xlsx	OneDrive	Yahoo	Confidential
Email external to self	bob.brown@company.com	August 7, 2023 9:45 AM	MeetingNotes.txt	SharePoint	Gmail	Company
Email external to self	carol.white@business.org	August 8, 2023 2:20 PM	ProjectPlan.docx	OneDrive	Outlook	Private
Email external to self	david.green@domain.com	August 9, 2023 3:00 PM	Invoice.pdf	SharePoint	Yahoo	Public
Email external to self	eve.black@website.net	August 10, 2023 4:30 PM	Feedback.doc	SharePoint	Outlook	Confidential
Email external to self	frank.stone@service.com	August 11, 2023 8:15 AM	Summary.pptx	OneDrive	Gmail	Company

Remediation plan: Prevent exfiltration to risky destinations

Increased risks detected in the last 30 days

An increasing number of files containing sensitive data were sent or saved to personal accounts, including by potentially risky users, such as departing users.

Remediation plan

Create targeted Data Loss Protection (DLP) and Insider Risk Management policies and deploy agents to accelerate protections for existing and emerging risks.

○ Policy not yet created

Prevent loss of sensitive data

Quickly create a DLP policy using the highlighted sensitive info types (SITs), targeting Exchange and devices, and including restricted domains. This limits unauthorized sharing, use, or transfer of sensitive information in devices, apps, and services, including AI apps and agents.

[View policy details](#)

Create custom policy in DLP [↗](#)

○ Policy not yet created

Detect and remediate potential insider risks

Quickly create an Insider Risk Management policy combining email indicators, the upload-to-web indicator, sensitive info types (SITs), and unallowed domains. This helps to detect, investigate, and address potential insider risks, such as data theft, data leaks, and other risky behaviors.

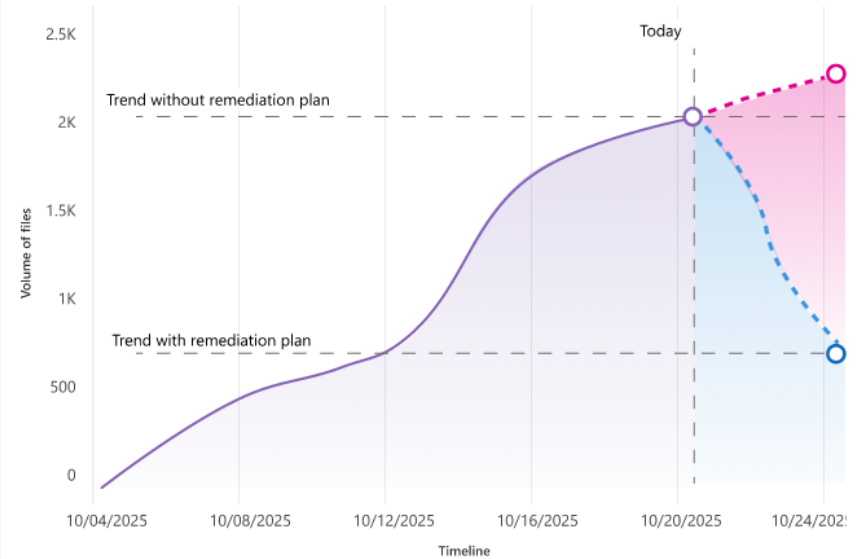
[View policy details](#)

Create custom policy in Insider Risk Management

Clear all

> Hide details

Estimated impact on risk pattern

[View remediation plan](#)

Apply

Cancel

360

↗ 2% in 30 days

- Home
- Solutions
- Agents
- Learn
- Settings
- DSPM
- Information protection
- ...
- Tasks and actions
- Setup tasks
- Remediation actions
- Reports
- DSPM (preview)
- Posture
- Objectives
- AI observability (preview)
- Discover
- Apps and agents
- Data risk assessments
- Activity explorer
- Asset explorer

Data security objectives

View and track data security objectives for your organization. Each objective highlights key risks to address, actions to take, and progress over time. This helps your organization stay aligned with your overall data security posture. [Learn more](#)

Data discovery

Data protection

Data investigation

Warning

30.9K interactions

+5% in last 30 days

25.2K

+2%

User prompts

256

+3%

Files overshared

View remediation plan

Copilot prompts

Data protection

Microsoft 365 Copilot

Prevent data exposure in Microsoft 365 Copilot interactions

30,916 Microsoft 365 Copilot and Microsoft Copilot interactions with sensitive data were detected from your organization in the last 30 days, an increase of 5%. This could indicate emerging patterns of data exposure.

Take action to reduce risk

Taking action could reduce sensitive interactions from 30.9K to 22K, which is about a 29% decrease.

Review objective

Warning

21.1K items overshared

+5% in last 30 days

4.2K

-2%

Total unlabeled items

356

-3%

Items shared externally

View remediation plan

Copilot prompts

Data protection

Oversharing

Prevent oversharing of sensitive data

32,729 items are unlabeled and contain sensitive data from Microsoft 365 and Microsoft Fabric in the last 30 days, an increase of 4%. This could indicate emerging patterns of oversharing sensitive data.

Take action to reduce risk

Taking action could reduce oversharing files from 32.7K to 16.3K, which is about a 50% decrease.

Review objective

Warning

Prevent exfiltration to risky destinations

Data protection

Exfiltration

- Home
- Solutions
- Agents
- Learn
- Settings
- DSPM
- Information protection
- ...
- DSPM (preview)
- Posture
- Objectives
- AI observability (pre
- Discover
- Apps and agents
- Data risk assessment
- Activity explorer
- Asset explorer
- Tasks and actions
- Setup tasks
- Remediation actions
- Reports

Remediation plan: Prevent data exposure in Microsoft 365 Copilot and Microsoft Copilot interactions

Control unethical behavior in AI

Detects future interactions so you can investigate and take action.

View policy details

You do not have permission to apply this action.

Review actions

Improvement actions pending

Boost your compliance health

Baseline AI regulation checks is completed and Microsoft has already configured and enforced few guardrails to safeguard your landscape. Reach your compliance objectives by implementing recommended improvement actions.

View progress

View all improvement actions

Protect your data from potential oversharing risks in Microsoft 365 (SharePoint and OneDrive)

Data assessments provide you with insights on potential oversharing risks in your organizations along with remediation actions to clean up your permissions on data.

View details

View Microsoft 365 default assessment results

Hide details

Estimated impact on risk pattern

Timeline	Trend with remediation plan	Trend without remediation plan
10/15	0	0
10/20	8K	8K
10/25	16K	16K
10/30	18K	18K
11/05 (Today)	30K	30K
11/10	10K	38K

Clear all

Apply

Cancel

View remediation plan

Copilot prompts

Data risk assessments (Microsoft)

Use data assessments to identify potential oversharing risks in your organization. They also provide fixes to limit access to sensitive data.

Microsoft 365

Microsoft Fabric

Item-level scanning and remediation available in custom assessments. You can now create custom assessments to scan individual files in SharePoint for potential oversharing and take remediation actions. [Learn more about item-level remediations.](#)

Create custom assessment

Assess and prevent oversharing of sensitive data in Microsoft 365

1 Identify

Review assessment results for users accessing sensitive items. You can review the weekly results from the [Microsoft 365 default assessment](#) or [create custom assessments](#) to review specific data sources and users.

2 Protect

Limit Microsoft Copilot access to sensitive data and apply label and retention policies to Fabric workspaces and data.

3 Monitor

Conduct SharePoint site and access reviews to evaluate permissions and user access.

Default assessment

Assesses oversharing of sensitive data for the top 100 SharePoint sites based on how many times the sites are accessed. Results are derived from data collected over the last 30 days.

Results

Total items

1.0M

Last updated

Oct 27, 2025

View details

Sensitive data detected

136

Next update

Nov 3, 2025

Link sharing data with anyone

136

Frequency

Weekly

View default assessment

Custom Microsoft 365 assessments

Custom assessments review specific data sources and users to identify potential oversharing of sensitive data. If the results are expired, you can duplicate the assessment to refresh the results.

+ Create custom assessment

Delete (#)

5 items

Custom assessment name

Data scan

Potentially overshared items

Started on

Completed on

Results expire in

Actions

Data risk assessment > Finance data assessment 10/13/2025

Finance data assessment 10/13/2025

OverviewPotentially overshared items New

136 potentially overshared items detected

136 items are potentially overshared in your scoped data sources. An item is identified as potentially overshared if it has a sharing link that's accessible to external or anonymous users. View detected items and remediate as needed.

View items

Assessment details

Sources included64

Potentially overshared items136

StatusCompleted

Completed onOctober 25, 2025

Total items

12.8M

Scanned for sensitive info types

Not scanned

Sensitivity labels applied to items

Labeled5762

Not labeled8456

No sensitive info types detected

Sensitive info types detected

Unscanned items

Items shared with

Anyone5762

People in your organization8456

Specific people8752

People outside your organization188K

SharePoint

OneDrive

Data assessment results

Review potential oversharing risks in your org and take action, such as limiting access to sensitive data and evaluating access to SharePoint sites.

Export

7 items

Home

Solutions

Agents

Learn

Settings

DSPM

Information protection

DSPM (preview)

Posture

Objectives

AI observability (preview)

Discover

Apps and agents

Data risk assessments

Activity explorer

Asset explorer

Tasks and actions

Setup tasks

Remediation actions

Reports

← Back to Data Risk Assessment

Contoso merger assessment

Contoso merger assessment

OverviewPotentially overshared itemsNew

✓ Resolve✉ Notify⌵ More actions

10 items

☐	> Name	Sharing link type	Sensitivity label	Owner	Last modified date	Last Action	Remediation status
☐	⌵ https://zava.sharepoint.com/sites/contoso						--
☐	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	🔄 Pending
☐	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	🔄 Pending
☐	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline	10/13/2025	--	🔄 Pending
☐	Contoso merger strategy.pptx	Anyone	General	Robine Kline	10/13/2025	--	🔄 Pending
☐	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	🔄 Pending
☐	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	🔄 Pending
☐	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	🔄 Pending
☐	System_Admin_Credentials_2.text (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	🔄 Pending
☐	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	🔄 Pending
☐	⌵ /sites/operationsdepartment (1)						--
☐	System_setup_instructions.docx	Anyone	Confidential	Robine Kline	10/13/2025	--	🔄 Pending

← Back to Data Risk Assessment

Contoso merger assessment

Contoso merger assessment

Overview

Potentially overshared items New

✓ Resolve		✉ Notify	More actions ▾		10 items			
☐	>	Name	Sharing link type	Sensitivity label	Owner	Last modified date	Last Action	Remediation status
☐	▼	https://zava.sharepoint.com/sites/contoso						--
☒		Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	 Pending
☒		Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	 Pending
☒		System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline	10/13/2025	--	 Pending
☐		Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	 Pending
☐		Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	 Pending
☐		Due diligence report.docx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	 Pending
☐		System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	 Pending
☐		Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	 Pending
☐	▼	/sites/operationsdepartment (1)						--
☐		System_setup_instructions.docx	Anyone	Confidential	Robine Kline	10/13/2025	--	 Pending

Home

Solutions

Agents

Learn

Settings

DSPM

Information protection

...

Tasks and actions

Setup tasks

Remediation actions

Reports

DSPM (preview)

Posture

Objectives

AI observability (preview)

Discover

Apps and agents

Data risk assessments

Activity explorer

Asset explorer

Tasks and actions

Setup tasks

Remediation actions

Reports

← Back to Data Risk Assessment

Contoso merger assessment

Contoso merger assessment

Overview

Potentially overshared items New

✓ Resolve

✉ Notify

More actions ▾

☐	> Name	Sharing link type	Sensitivity label	Owner
☐	⌵ https://zava.sharepoint.com/sites/contoso			
☒	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline
☒	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline
☒	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline
☐	Contoso merger strategy.pptx	Anyone	General	Robine Kline
☐	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline
☐	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline
☐	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline
☐	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline
☐	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline
☐	⌵ /sites/operationsdepartment (1)			
☐	System_setup_instructions.docx	Anyone	Confidential	Robine Kline

Resolve 3 items

Items to resolve

Contoso status.docx (1), Contoso passwords.txt (2), System_Admin_Credentials_Contoso

Resolving these items mean you've determine they're not overshared. They'll be flagged as "Remediated" in the status column

Resolve items

Home

Solutions

Agents

Learn

Settings

DSPM

Information protection

...

Tasks and actions

Setup tasks

Remediation actions

Reports

DSPM (preview)

Posture

Objectives

AI observability (preview)

Discover

Apps and agents

Data risk assessments

Activity explorer

Asset explorer

Tasks and actions

Setup tasks

Remediation actions

Reports

← Back to Data Risk Assessment

Contoso merger assessment

Contoso merger assessment

Overview

Potentially overshared items New

✓ Resolve

✉ Notify

More actions ▾

☐	> Name	Sharing link type	Sensitivity label	Owner
☐	✓ https://zava.sharepoint.com/sites/contoso			
☐	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline
☐	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline
☐	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline
☒	Contoso merger strategy.pptx	Anyone	General	Robine Kline
☐	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline
☐	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline
☐	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline
☐	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline
☐	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline
☐	✓ /sites/operationsdepartment (1)			
☐	System_setup_instructions.docx	Anyone	Confidential	Robine Kline

Send a notification

✕

An email will be sent to the site owners about the violations found in their sites. You can also copy the URL that will be sent in the email and pass it directly to the owner.

☐	Name	Owners	Status	Actions
☒	System_admin_cre...	Cassandra Dunn	⌛ Pending	📄 Copy URL

Send (1)

← Back to Data Risk Assessment

Contoso merger assessment

Contoso merger assessment

OverviewPotentially overshared itemsNew

✓ Resolve

✉ Notify

More actions ▾

☐ > Name

☐ ✓ https://zava.sharepoi

Remove sharing link

Apply sensitivity label

10 items

	Name	Sharing link type	Sensitivity label	Owner	Last modified date	Last Action	Remediation status
☐	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline	10/13/2025	Resolved	✓ Remediated
☐	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline	10/13/2025	Resolved	✓ Remediated
☐	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline	10/13/2025	Resolved	✓ Remediated
☐	Contoso merger strategy.pptx	Anyone	General	Robine Kline	10/13/2025	Notified	✓ Remediated
☒	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	⌛ Pending
☐	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	⌛ Pending
☐	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	⌛ Pending
☐	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	⌛ Pending
☐	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	⌛ Pending
☐	✓ /sites/operationsdepartment (1)						--
☐	System_setup_instructions.docx	Anyone	Confidential	Robine Kline	10/13/2025	--	⌛ Pending

Home

Solutions

Agents

Learn

Settings

DSPM

Information protection

...

DSPM (preview)

Posture

Objectives

AI observability (preview)

Discover

Apps and agents

Data risk assessments

Activity explorer

Asset explorer

Tasks and actions

Setup tasks

Remediation actions

Reports

Back to Data Risk Assessment

Contoso merger assessment

Contoso merger assessment

Overview

Potentially overshared items New

Resolve

Notify

More actions

	Name	Sharing link type	Sensitivity label	Owner
☐	> https://java.sharepoi...			
☐	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline
☐	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline
☐	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline
☐	Contoso merger strategy.pptx	Anyone	General	Robine Kline
☒	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline
☐	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline
☐	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline
☐	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline
☐	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline
☐	> /sites/operationsdepartment (1)			
☐	System_setup_instructions.docx	Anyone	Confidential	Robine Kline

Apply sensitivity label

Choose a sensitivity label

Choose a sensitivity label

Public

General

Confidential

Highly Confidential

Apply label

Home

Solutions

Agents

Learn

Settings

DSPM

Information protection

...

☰

DSPM (preview)

Posture

Objectives

AI observability (preview)

Discover

Apps and agents

Data risk assessments

Activity explorer

Asset explorer

Tasks and actions

Setup tasks

Remediation actions

Reports

← Back to Data Risk Assessment

Contoso merger assessment

Contoso merger assessment

Overview

Potentially overshared items New

✓ Resolve

✉ Notify

More actions ▾

☐

> Name

☐

https://zava.sharepoi...

☐ Contoso status.docx (1)

☐ Contoso passwords.txt (2)

☐ System_Admin_Credentials_Contoso

☐ Contoso merger strategy.pptx

☐ Contoso FY25 financials.xlsx (2)

☒ Contoso employee info.xlsx (2)

☐ Due diligence report.docx (2)

☐ System_Admin_Credentials_2.txt (2)

☐ Contoso FY24 financials.xlsx (2)

☐

/sites/operationsdepartment (1)

☐ System_setup_instructions.docx

g link type

Sensitivity label

Owner

Anyone

Unlabeled

Confidential

Confidential

General

General

Confidential

Confidential

Confidential

Anyone

Confidential

- Remove sharing link
- Apply sensitivity label

Remove sharing link

Items to remove sharing link

Name	Access link type
Contoso employee info.xlsx (2)	Anonymous

Remove

[← Back to Data Risk Assessment](#)

Contoso merger assessment

Contoso merger assessment

Overview

Potentially overshared items New

✓ Resolve

✉ Notify

More actions ▾

10 items

☐	> Name	Sharing link type	Sensitivity label	Owner	Last modified date	Last Action	Remediation status
☐	▼ https://zava.sharepoint.com/sites/contoso						--
☐	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline	10/13/2025	Resolved	✓ Remediated
☐	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline	10/13/2025	Resolved	✓ Remediated
☐	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline	10/13/2025	Resolved	✓ Remediated
☐	Contoso merger strategy.pptx	Anyone	General	Robine Kline	10/13/2025	Notified	✓ Remediated
☐	Contoso FY25 financials.xlsx (2)	Anyone	General	Robine Kline	10/13/2025	Labeled	✓ Remediated
☐	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	Link removed	✓ Remediated
☐	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	⌚ Pending
☐	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	⌚ Pending
☐	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	⌚ Pending
☐	▼ /sites/operationsdepartment (1)						--
☐	System_setup_instructions.docx	Anyone	Confidential	Robine Kline	10/13/2025	--	⌚ Pending

Home

Solutions

Learn

Settings

Data Lifecycle Managem...

Communi... Compliance

Compliance Manager

Information Protection

DSPM for AI

DSPM for AI

Overview

Recommendations

Reports

Apps and agents

Preview

Policies

Activity explorer

Data risk assessments

Apps and agents

Dashboard to understand the depth of Purview deployment in protecting AI applications.

Apps

Agents

Refresh

Export

9 items

Search

Group list

Edit columns

AI app	Protection status	Prompt Trend	User Trend	Response Trend	Data protection	Data compliance	Agents	
Microsoft Copilot Studio (1)								
☐	Microsoft Copilot Studio	Monitored				0 policies	1 Policies	2
Copilot experiences & agents (3)								
☐	Microsoft 365 Copilot	Monitored				2 Policies	1 Policies	1
☐	Copilot in Fabric	Monitored	No data available	No data available	No data available	0 policies	0 policies	-
☐	Security Copilot	Monitored				0 policies	1 Policies	1
Enterprise AI apps (2)								
☐	ChatGPT Enterprise	Monitored	No data available	No data available	No data available	0 policies	0 policies	-
☐	Entra App	Monitored				0 policies	0 policies	1
Other AI apps (3)								
☐	ChatGPT	Monitored			No data available	2 Policies	1 Policies	1
☐	Claude	Monitored			No data available	2 Policies	1 Policies	1
☐	Google Gemini	Monitored			No data available	2 Policies	1 Policies	2

Data Security Posture Management for AI

En quelques mots

- Disposez d'une visibilité sur **l'utilisation de l'IA générative** grâce à des rapports, des tendances et des recommandations.
- **Recommandations de politiques** basées sur les principaux risques liés aux données dans l'usage de l'IA générative au sein de votre organisation.
- Panneau de contrôle pour **toutes les politiques liées à l'IA**, couvrant la prévention des pertes de données (DLP) et la gestion des risques internes.
- **Évaluation des risques** liés aux données pour identifier les sites SharePoint trop permissifs.
- Rapports sur l'utilisation des **applications et agents GenAI**, incluant les usages risqués et les interactions sensibles ou non éthiques.

*L'arrivée de Copilot n'est pas seulement
une **révolution de la productivité** :*

*c'est **l'opportunité inattendue** qui
pousse votre organisation à
transformer sa gestion des données
trop longtemps mise de côté.*

*Élevant votre stratégie de gouvernance
bien au-delà d'une simple question de
sécurité liée à l'IA.*



Copilot aide les utilisateurs à générer du contenu, analyser des données et répondre à des questions en s'appuyant sur les fichiers, e-mails et discussions internes de l'organisation.

Une stratégie de sécurité proactive devient incontournable.

*Il émerge de **nouveaux risques** en matière de sécurité des données. Copilot respecte les autorisations existantes de l'utilisateur. Cela signifie que toute **lacune ou incohérence** dans la gouvernance des données de l'organisation (surpartage, données obsolètes ou de mauvaise qualité, accès incohérents) peut être amplifiée par Copilot, augmentant ainsi le **risque d'exposition de données sensibles**.*



Quels risques souhaitons-nous couvrir ?

Fuite et surexposition de données sensibles

Copilot accède à toutes les informations pour lesquelles un utilisateur dispose des autorisations. Si un utilisateur a accès à des données sensibles, Copilot aura le même accès, ce qui peut entraîner l'inclusion de données confidentielles dans ses réponses. Le « surpartage » d'informations constitue donc un risque majeur.

Shadow AI

Le « Shadow AI » désigne l'utilisation par les employés d'outils d'IA non approuvés en dehors de l'environnement Microsoft 365 géré. Cela pose des risques importants en matière de sécurité et de conformité.

Données de mauvaise qualité ou obsolètes

Si les données sont mal gérées, désorganisées ou contiennent des données superflues, Copilot peut refléter ces problèmes et les amplifier. Cela peut entraîner des réponses inexactes ou trompeuses et accroître les risques de fuite de données. Ce principe, « garbage in, garbage out », s'applique ici avec des implications de sécurité amplifiées.

Conformité réglementaire

Le traitement des données sensibles par l'IA doit respecter les réglementations en vigueur (par exemple, RGPD, HIPAA), et un manque de contrôle peut entraîner une non-conformité.

Sécurisation d'un déploiement de M365 Copilot

1 - Préparer

Préparez un pilote réussi

Sélectionnez les utilisateurs, préparer l'accompagnement, définissez les critères de succès

2 - Nettoyer

Rangez votre chambre

Evaluer les problèmes de partages excessifs et gérez le cycle de vie des données

3 – Protéger

Concentrez-vous sur les joyaux de la couronne

Comprenez vos données, puis identifiez et protégez les plus sensibles

4 - Consolider

Passez à la vitesse supérieure

Utilisez les fonctionnalités avancées pour une meilleur gouvernance et gérer les risques internes

5 - Industrialiser

Adaptez et faites évoluer votre gouvernance IT

Recherchez et explorez de nouveaux sujets, et affinez vos processus

Préparation du pilote

À propos des utilisateurs



100 à 250 utilisateurs constituent un bon point de départ pour suivre les retours d'expérience.



Profils variés qui reflètent la diversité des rôles et des usages au sein de votre organisation.



Incluez **différents niveaux hiérarchiques** et des degrés variés de **compétence technique**.



Définissez des Champions : ils deviennent des ambassadeurs des bonnes pratiques et des relais pour les retours utilisateurs et le support.



Utilisateurs volontaires et motivés : ils facilitent l'adoption et fournissent des retours constructifs.



Intégrez des utilisateurs qui manipulent déjà des données sensibles.



Change Management



Sensibilisation : Ils doivent être informés de l'utilisation responsable de l'IA et des politiques de sécurité



Prompt Academy : Former les utilisateurs à créer des prompts efficaces et puissants.



Communication continue : Animer le pilote avec une stratégie de communication solide : exemples de prompts, avertissements, communauté.



Compréhension des étiquettes : S'assurer qu'ils comprennent le fonctionnement des étiquettes de sensibilité et leur impact sur l'interaction avec Copilot.



Canal de feedback : Définir un canal efficace pour recueillir tous les retours et assurer le support.



"Garbage In, Garbage Out" et importance de l'hygiène des données : Rappeler que la qualité des réponses dépend directement de la qualité des données.

« Pen-testez » Copilot

How-to

Objectif : Évaluer si Copilot peut révéler des informations sensibles, stratégiques ou confidentielles qui ne devraient pas être accessibles à l'utilisateur, ou assister dans des actions malveillantes (même indirectement).

Hypothèse de base : L'utilisateur n'a pas d'accès direct ou légitime à ces informations/actions, mais tente de les obtenir via Copilot, qui dispose d'un périmètre de données plus large.

Méthode de test : Soumettre des prompts et analyser les réponses de Copilot :

- Révèle-t-il des noms de projets confidentiels ?
- Des noms de clients sensibles ?
- Des données financières non publiques ?
- Des informations sensibles sur les employés (salaires, ...) ?
- Des vulnérabilités internes ?
- Comment gère-t-il les demandes de contournement des processus ?

Guide pour l'analyse des réponses

Refus explicite : C'est la meilleure réponse de Copilot face à des prompts malveillants.

Réponses génériques ou hors sujet : Si Copilot répond de manière très générale ou sans inclure d'informations sensibles, c'est un bon signe.

Fuite d'informations : Toute mention de noms, chiffres, projets ou vulnérabilités qui ne devraient pas être publics ou accessibles à l'utilisateur constitue une faille de sécurité.

Assistance au contournement : Si Copilot suggère des alternatives pour obtenir l'information ou réalise des actions facilitant une intention malveillante.

Essayez ces prompts au début de votre projet pour identifier les priorités et les problèmes de sur partage.

Réessayez-les une fois que vous aurez mis en place les bonnes pratiques décrites ensuite.



NETTOYER

Rangez votre chambre



Tâches basiques sur **SharePoint et Teams**

Analyser le **top 100 de vos sites les plus utilisés** avec l'admin center SharePoint.

Renforcez vos stratégies SharePoint et Teams

- Niveau de confidentialité par défaut
- Désactiver « Tout le monde sauf les utilisateurs externes »
- Définissez le comportement de partage des sites

Demandez aux **propriétaires de site** de faire du ménage

- Revoir les membres des sites
- Passez les sites de public à privé
- Revoir les groupes sans propriétaires



Profitez de **SharePoint Advanced Management**

- **Découverte** des sites avec données en **sur partage**.
- **Assistance à la revue des accès** pour les propriétaires de sites.
- **Remise à plat** des accès sur les sites critiques.
- **Exclusion de sites critiques** pour empêcher Copilot de raisonner dessus.

Gérez le **cycle de vie de la donnée**



Une **gestion efficace du cycle de vie des données** est essentielle pour maintenir un environnement Microsoft 365 **propre, sécurisé et conforme**, en particulier avec l'introduction de Copilot.

Des **politiques claires de conservation** (ou de suppression) des prompts et des réponses de Copilot doivent être définies afin de garantir que les informations sensibles soient conservées pendant la durée requise à des fins d'audit et de conformité.



Les **politiques d'expiration** pour les groupes et sites inactifs sont également essentielles **pour éviter la prolifération de contenu et le surpartage**. Cela contribue à maintenir un environnement Microsoft 365 organisé et sécurisé.

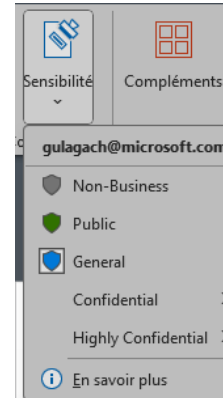
The image depicts a serene landscape under a bright, hazy sky. In the foreground, a field of small, vibrant purple flowers stretches across the bottom. Several trees are scattered across the scene. The most prominent tree on the left is large and has a thick, gnarled trunk. Its canopy is composed of numerous small, three-dimensional purple cubes, giving it a pixelated or blocky appearance. To its right, there are three smaller trees of similar design, also made of purple cubes. The background is a soft, out-of-focus expanse of light purple and white, suggesting a distant horizon or a misty atmosphere. The overall color palette is dominated by shades of purple and pink, creating a dreamlike and ethereal mood.

PROTEGER

Les joyaux de la couronne

Protéger les données sensibles dans les interactions

La première étape pour protéger les données sensibles est de les **identifier**. Microsoft Purview permet la **découverte et la classification automatiques** des données sensibles à travers divers services M365.



Filter on labels, info types, or categories

All locations > SharePoint

The number of site/folder items listed below and on the left is a calculation and may not match the total number of actual items you'll see if you open a specific site/folder.

Export

Name	Files
https://m365x53676902.sharepoint.com/sites/operations	110
https://m365x53676902.sharepoint.com/sites/newemployeeonboarding	4

Search

Search

Trainable Classifiers

Pii Retention Policy	8
Finance	1610
Agreements	1334
Statement of Work	1333
Procurement	579
Legal Agreements	550
Legal Affairs	114

L'utilisation de **Types d'Informations Sensibles** (SITs) prédéfinis ou personnalisés, ainsi que de classifieurs entraînés, permet de détecter des données sensibles **dans les prompts et les réponses** des utilisateurs Copilot.

Pour un état des lieux précis des données, les outils comme **eDiscovery** et **Content Explorer** sont inestimables. Ils permettent de croiser les informations avec les listes de sites SharePoint pour identifier les zones à risque et les volumes.

Copilot DLP et Chiffrement des données

Les **politiques DLP** peuvent être configurées pour **empêcher Copilot de résumer ou de référencer du contenu sensible**. Spécifiquement, Copilot peut être empêché de raisonner sur des fichiers labellisés (qu'ils soient chiffrés ou non)

le **Chiffrement à double clé** (DKE) offre le plus haut niveau de protection pour les données **extrêmement sensibles**. Les données protégées par DKE sont inaccessibles à Copilot.

résume ce doc [TEST Label.docx](#)

 Copilot 

Le document **TEST Label.docx** est protégé, ce qui empêche l'accès à son contenu pour en faire un résumé.

Tu peux soit :

- Me fournir une version non protégée du document,
- M'indiquer les grandes lignes ou copier-coller le texte ici pour que je puisse t'aider à le résumer.

Souhaitez-tu essayer l'une de ces options ?

The image features a surreal landscape. In the foreground, a field of small, vibrant purple flowers stretches across the bottom. Several trees of varying sizes are scattered across the scene. The trees are composed of a dark brown trunk and a dense canopy of small, three-dimensional purple cubes. The largest tree is on the left, with a thick trunk and a wide, spreading canopy. To its right, there are three smaller trees, each also made of purple cubes. The background is a bright, hazy white, suggesting a very bright sky or a misty atmosphere. The overall color palette is dominated by shades of purple and brown.

CONSOLIDER

Passer à la vitesse supérieure

Superviser les interactions utilisateurs

Communication Compliance est un outil puissant pour **superviser les interactions** des utilisateurs.

Il permet de détecter les **comportements à risque** et les interactions **non éthiques** avec l'IA, en se basant sur les types d'informations sensibles définis.

Cela inclut la détection d'activités qui tentent de **contourner** les instructions de Copilot ou de générer du contenu inapproprié.

The screenshot displays the Microsoft Communication Compliance interface. The top navigation bar includes tabs for 'Pending (57)', 'Resolved (5)', and 'Exports'. Below this, there are filter options and a table of interactions. The table has columns for 'Subject', 'Tags', 'Sender', and 'Recipients'. One interaction, 'Copilot in Word', is selected. To the right, a detailed view of this interaction is shown, including a 'Summary' tab, a 'Prompt entered' section, and a 'Response returned' section. The prompt asks for a summary of 'Project Dragon', and the response states that the information is confidential and not disclosed.

Subject	Tags	Sender	Recipients
Copilot in Teams	...	nestorwilke@contoso.com	Copilot
Copilot in Word	...	adelevance@contoso.com	Copilot
Copilot in PowerPoint	...	Copilot	cc@contoso.com
Copilot in Outlook	...	jhernandez@contoso.com	Copilot
Copilot in Loop	...	rsanchez@contoso.com	Copilot

Copilot in Word

Summary Plain text User history

Conditions detected: Secret Projects (Dragon) [View all](#)

Prompt entered Microsoft Word

Adele Vance Asked Copilot in Word on Oct 16, 2023 at 4:53 PM (UTC)

Give me a summary of project dragon and when it will be announced?

Response returned

Copilot in Word Replied on Oct 16, 2023 at 4:53 PM (UTC)

I apologize, but I am unable to summarize this topic as it pertains to a confidential project. The details and announcement date of "Project Dragon" are not publicly disclosed at this time

[Resolve](#) [Summarize](#) [Notify](#) [Tag as](#) ...

Appliquer **dynamiquement** des politiques de sécurité en fonction des actions à risque.

Un Utilisateur fait une **série** d'actions à **risque**

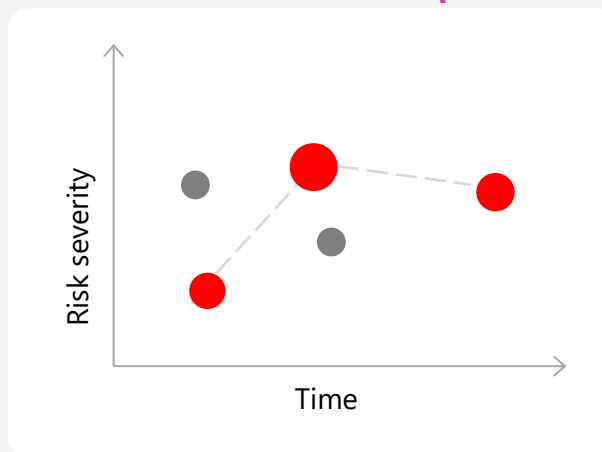


Les actions dévient de la normalité ou des habitudes

- Il a une série d'activité à risque dans les interactions Copilot
- Il télécharge une centaine de documents contenant des données sensibles



Identification de la **séquence** des événements comme un **modèle de risque**



Utilisation de l'IA pour l'analyse de risque



Ajout automatique de l'utilisateur dans des stratégies de sécurité plus fortes



Blocage des actions jusqu'à l'investigation

- Ne peut plus accéder aux contenus sensibles
- Ne peut plus partager ou télécharger
- Ne peut plus supprimer

Trouver l'équilibre entre productivité et réduction des risques

Recertifier les accès utilisateurs

Des audits réguliers des permissions et des accès sont essentiels pour prévenir l'escalade des privilèges et le sur-partage.

Les révisions d'accès (**Access Reviews**) garantissent que les utilisateurs ont toujours les permissions appropriées et que les accès sont révoqués lorsqu'ils ne sont plus nécessaires.

 **CONTOSO** demo

Please review users' access to the Operations group in Contoso

Megan Bowen, your organization requested that you approve or deny continued access for one or more users to the **Operations** group in the **Test 46** review. The review period will end on **May 8, 2020**.

[Start review >](#)

Learn how to [perform an access review](#) and more about [Azure Active Directory access reviews](#).

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Facilitated by

 Microsoft

[←](#) Access reviews

Contoso Sales Group Review

Please review members of 'Contoso Sales' [See details](#)

[✓ Approve](#) [✗ Deny](#) [? Don't know](#) [↺ Reset decisions](#) [☑ Accept recommendations](#) [Filter](#)

 Name ↑	Recommendation	Decision	Reviewed by
 John Falzon johnfalzon@contoso.com	Approve Last signed in (Jan 5, 2022) less than 30 days before review began		Details
 Sofia Gomes sofiagomes@contoso.com	Deny Last sign-in date unknown		Details
 Lei Liao leiliao@contoso.com	Deny Last sign-in date unknown		Details

INDUSTRIALISER

- Prise en charge des nouvelles alertes et rapports
- Recherche des interactions dans les outils eDiscovery
- Exécuter en routine les Data Risk Assesements
- Revue régulière des accès et des groupes

**Adaptez et faites évoluer votre
gouvernance IT**



ULTIME RECOMMANDATION

Faites vous accompagner par un partenaire

Leadership en cybersécurité à l'ère de l'IA

Témoignage de nos clients



Michel Dubois
Directeur Scientifique et Technique
Groupe La Poste



Olivier Lievens
CIO
Business France



Les engagements de Microsoft sur la souveraineté des données



Cyril Voisin

Customer Security Officer Manager, EMEA



Souveraineté numérique?

attention croissante à la sécurité des données,
à la conformité, ainsi qu'aux questions de commerce
mondial et de géopolitique



**Exigences
réglementaires**



**Traitements IA
souverains**



**Pas d'accès de
l'opérateur de
cloud**



**Résidence
des données**



**Continuité
d'activité**

Souveraineté numérique

La **souveraineté numérique** est la capacité de participer à l'économie numérique de manière sécurisée, indépendante et avec des contrôles autodéterminés.

Notre approche de la souveraineté numérique



Accessible à tous : la souveraineté numérique est une capacité fondamentale des services Microsoft



Via des contrôles bien gouvernés : assurés par l'intermédiaire de **mesures opérationnelles, contractuelles et techniques**



Dépendante de la charge de travail : les exigences en matière de contrôle souverain varient en fonction de la sensibilité et de la criticité

Au cours de la dernière décennie, Microsoft a beaucoup investi dans la sécurité, la confidentialité des données, et la conformité

! Jalon important

2016

- ! Lancement du cloud souverain allemand avec un tiers de confiance local
- ! Investissement de 3 milliards de dollars pour doubler la capacité cloud en Europe
- Contestation de l'ordonnance étatsunienne de non-divulgaration à propos des données clients, pour des raisons de transparence
- 30 régions Azure actives

2018

- ! Première grande entreprise technologique à appliquer les droits relatifs aux données du RGPD à ses clients dans le monde entier
- Respect de l'échéance RGPD

2020

- ! Lancement de « Défendre vos données » pour s'opposer légalement aux demandes gouvernementales d'accès aux données
- Engagement à indemniser en cas de divulgation de données personnelles en violation du RGPD
- Réaffirmation de l'opposition aux portes dérobées de chiffrement imposées par les gouvernements

2022

- ! Lancement de Microsoft Cloud for Sovereignty avec une résidence des données, une confidentialité et une conformité renforcées.
- ! Introduction du module complémentaire Résidence avancée des données
- Plus de 60 régions Azure actives
- Extension du programme Go Local à 15 pays
- Plus de 100 certifications de conformité, dont plus de 50 spécifiques à certaines régions

2024

- Extension de la Limite des données UE à la phase 2, ajoutant les données personnelles pseudonymisées et la télémétrie en région.
- Réduction des transferts de données hors UE en conservant les données et métadonnées des services cloud Microsoft en Europe

2017

- ! Engagement à assurer la conformité totale au RGPD pour tous les services cloud d'ici l'entrée en vigueur en 2018
- Victoire politique avec la limitation des ordonnances de non-publication par le Département de la Justice étatsunien
- Révision des contrats et contrôles de confidentialité pour soutenir la conformité des clients

2019

- ! Lancement des premiers centres de données cloud en Afrique et au Moyen-Orient, permettant le stockage local des données
- Extension des droits de confidentialité CCPA de Californie à tous les clients étatsuniens, adoptant une posture « au-delà de la conformité »
- 54 régions Azure actives

2021

- ! Annonce de la Limite des données UE pour Microsoft Cloud
- Engagement à stocker et traiter toutes les données clients UE dans des centres de données européens d'ici fin 2022

2023

- Lancement de la phase 1 de la Limite des données UE, stockage des données clients principales dans des centres de données européens
- Extension du programme Go Local à plus de 25 pays

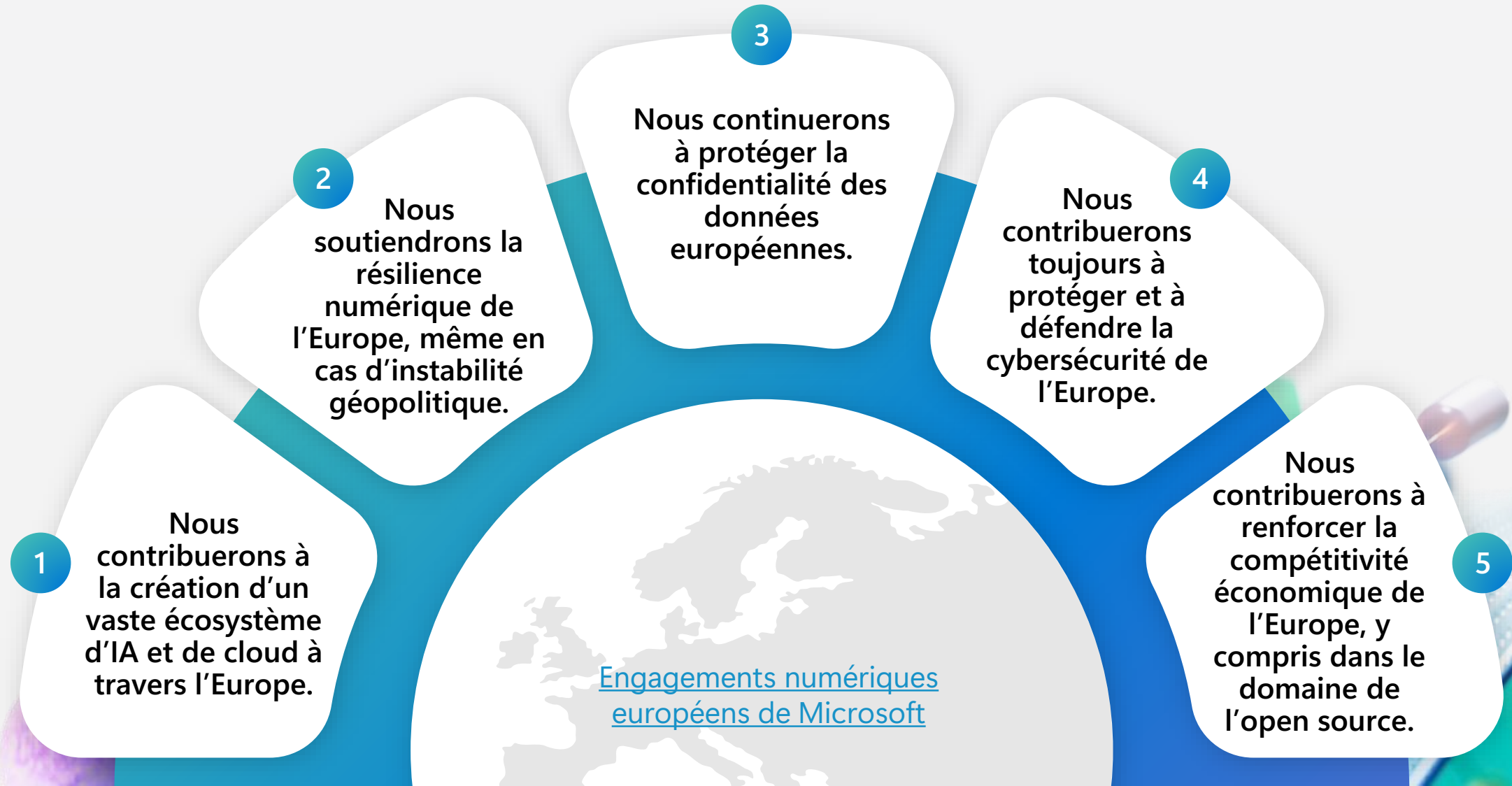
2025

- ! Finalisation de la Limite des données UE (phase 3) avec toutes les données clients UE dans des centres de données européens
- ! Annonce de l'expansion du Microsoft Sovereign Cloud aux environnements cloud publics et privés
- Lancement des fournisseurs nationaux de Cloud Bleu (France) et Delos (Allemagne).
- Annonce de 5 engagements européens sur les données
- Plus de 70 régions Azure actives
- Plus de 20 milliards de dollars investis dans l'infrastructure cloud européenne depuis 2023

→ 2026+

Engagements numériques européens de Microsoft

Brad Smith (Président de Microsoft) sur la résilience numérique
face à la volatilité géopolitique, Bruxelles, 30 avril 2025



Engagements numériques européens de Microsoft

1

Nous contribuerons
à la création d'un
vaste écosystème
d'IA et de cloud à
travers l'Europe.

Respect des lois européennes

Plateformes de cloud souverain

Investissements cloud en Europe

Investissements cloud de Microsoft en Europe



Engagements numériques européens de Microsoft

2

Nous soutiendrons la résilience numérique de l'Europe, même en cas d'instabilité géopolitique.

Un cloud européen pour l'Europe

Un engagement de résilience numérique

Partenariats de continuité d'activité

Engagements numériques européens de Microsoft

3

Nous
continuerons
à protéger la
confidentialité
des données
européennes.

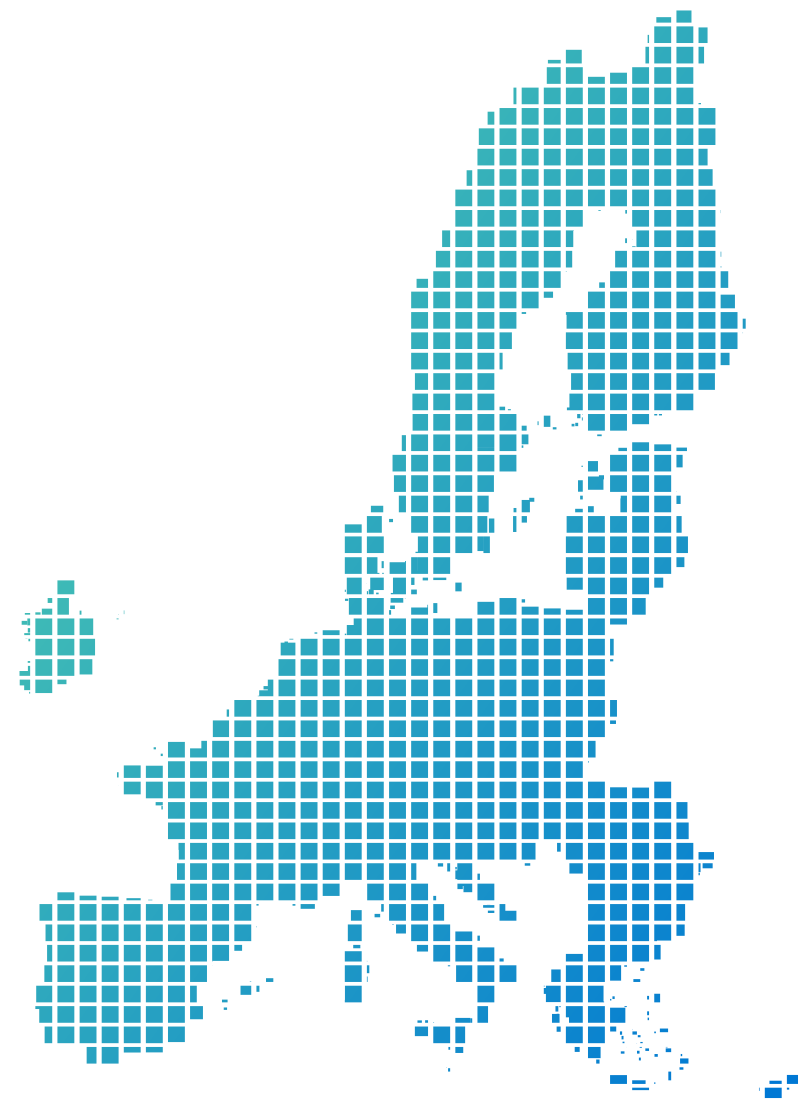
Engagement *Défendre vos données*

Frontière de données de l'UE
EU Data Boundary

Sécuriser et chiffrer les données clients



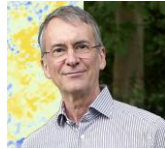
La frontière de
données de l'UE
(*EU Data Boundary*)
comprend la résidence
du traitement des
données par l'IA



Engagements numériques européens de Microsoft

4

Nous contribuerons toujours à protéger et à défendre la cybersécurité de l'Europe.



Nouveau RSSI Adjoint
pour l'Europe

Accélération de la conformité avec
notre projet *SFI Data Boundary*

Protections supplémentaires

Engagements numériques européens de Microsoft

5

Nous contribuerons à renforcer la compétitivité économique de l'Europe, y compris dans le domaine de l'open source.

Principes d'accès à l'IA

Accès ouvert à travers l'Europe

Fondation pour l'Europe

Microsoft Sovereign Cloud

spectre complet de capacités de souveraineté, à travers des solutions intégrées d'IA, de productivité, de sécurité et de plateforme cloud.

Contrôles souverains

Cloud public souverain

Les données demeurent en Europe, selon le droit européen

Opérations et accès contrôlés par le personnel européen

Choix des modèles d'IA et traitement IA qui restent en Europe

Cloud privé souverain

Opérations continues dans des environnements hybrides ou déconnectés

Cloud et productivité intégrés avec Microsoft 365 Local

Capacités d'IA et prise en charge GPU avancée avec Azure Local

Clouds partenaires nationaux

Environnements cloud spécialisés avec les services Microsoft 365 et Azure, pour les charges de travail d'infrastructure critiques afin de répondre aux critères de propriété et d'expertise locales.

- **Allemagne** : Cloud Delos conçu pour répondre aux exigences Cloud du BSI
- **France** : **Bleu** conçu pour répondre aux exigences de SecNumCloud

← Plateforme de gestion et de développement cohérente →

La souveraineté numérique avec Microsoft Sovereign Cloud

Participer à l'économie numérique de manière sécurisée, indépendante et avec des contrôles autodéterminés

Contrôles opérationnels

Advanced Data Residency
for Microsoft 365

Data Guardian

Regulated Environment
Management

Contrôles sur les données

Azure Key Vault Premium

Azure Key Vault Managed HSM

External Key Management

Sovereign Landing Zones

Customer Lockbox

Azure Confidential Computing



Cloud partenaire national - BLEU

- Une co-entreprise entre Orange et Capgemini
- Le gouvernement a agréé un opérateur local indépendant de Microsoft pour exploiter un « cloud de confiance » pour le secteur public français
- Cloud en France avec une appropriation locale et une infrastructure isolée **conçue pour répondre aux exigences de SecNumCloud**



Admissibilité principale



- SI sensible pour les OIV et les OSE
- Les SI sensibles sous la doctrine du « cloud au centre »

Autres certifications ciblées



Norme ISO 27001



HDS (Hébergement des Données de Santé) v2

Répondre aux exigences de souveraineté

Via un processus de gouvernance des risques et des bénéfices

1

Analyser les **risques de souveraineté** basés sur la probabilité et l'impact

2

Identifier les **risques et bénéfices**, les actifs critiques, les applications et les données et cartographier les dépendances

3

Comprendre les **options technologiques et architecturales**

4

Concevoir en équilibrant le **niveau de risque acceptable** et la réduction acceptable des bénéfices

5

Préparer et tester **les plans de continuité d'activité et la stratégie de sortie**

Microsoft Sovereign Cloud prend en charge les scénarios clés de souveraineté numérique



**Exigences
réglementaires**



**Traitements IA
souverains**



**Pas d'accès de
l'opérateur de
cloud**



**Résidence
des données**



**Continuité
d'activité**

NIS2/DORA

Des outils concrets pour
renforcer votre cyber résilience



Etienne Lacour

Solution Engineer Director
Cybersecurity



Marina Djouadi

Solution Engineer
Cybersecurity



		
Type juridique	Directive à transposer dans les législations nationales	Règlement directement applicable dans tous les États membres
Entrée en vigueur	Transposition dans les lois nationales attendue (normalement octobre 2024...)	Applicable depuis le 17 janvier 2025
Périmètre d'application	Entités essentielles (énergie, transport, santé, etc.) et importantes (160K entreprise pour la France, subdivisée en catégories criticité et taille)	Entités financières (banques, assureurs, prestataires TIC critiques pour la finance) (1379 entreprises en se basant sur ACPR + 19 TIC – dont Microsoft)
Objectifs clés	Améliorer la posture de cybersécurité , gouvernance, détection et réponse aux incidents dans divers secteurs	Assurer la résilience opérationnelle dans le secteur financier : continuité et intégrité des services TIC
Gouvernance & responsabilité	Exige implication de la direction dans la politique cybersécurité et responsabilité renforcée	Exigences similaires dédiées à la direction, avec responsabilité directe sur la résilience ICT
Gestion des risques	Approche proactive : identification, surveillance, atténuation + sécurité de la chaîne d'approvisionnement	Gestion intégrale du risque ICT , tests réguliers, attention particulière aux prestataires tiers
Tiers / Sous-traitance	Obligation de sécuriser la chaîne d'approvisionnement et d'intégrer les risques tiers	Supervision directe des prestataires ICT critiques par les autorités, clauses contractuelles , suivi continu
Détection & signalement d'incidents	Notification rapide d'incidents aux autorités compétentes + rapports de suivi	Signalement prescrit des incidents ICT majeurs (notification initiale, rapports intermédiaires, finaux)
Tests de résilience	Recommandation de réaliser des tests de vulnérabilité et de pénétration	Tests obligatoires (« threat-led penetration testing » annuels + tests de résilience opérationnelle périodiques)
Sanctions & contrôles	Multiplie les sanctions jusqu'à 2 % du CA mondial pour non-conformité – Contrôle par l'ANSSI en France	Mécanisme d'application rigoureux aligné sur les réglementations financières, sanctions significatives – contrôle par ACPR, AMF, ESAs

Les objectifs et chantiers de NIS2



NIS2 Objectives							
Manage Security Risk		Protecting Against Cyber Attack		Detecting Cyber Security Incidents		Minimizing The Impacts Of Cyber Security Incidents	
NIS Principals							
A1: Governance	A2: Risk Management	B1: Service Protection Policies And Processes	B2: Identity And Access Control	C1: Security Monitoring	C2: Proactive Security Event Discovery	D1: Response And Recovery Planning	D2: Lessons Learned
A3: Asset Management	A4: Supply Chain	B3: Data Security	B4: System Security				
		B5: Resilient Networks And Systems	B6: Staff Awareness And Training				

Modèle de responsabilités partagées dans le Cloud

	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Microsoft	Shared	Customer	Customer
	Network controls	Microsoft	Shared	Customer	Customer
	Operating system	Microsoft	Microsoft	Customer	Customer
Responsibility transfers to cloud provider	Physical hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

Microsoft	Customer	Shared
-----------	----------	--------

Le modèle de responsabilités partagés permet de déléguer certaines briques infrastructure à votre fournisseurs de Services.

Par exemple : Lorsque les clients utilisent un service SaaS comme M365, Microsoft traite **80 % de l'infrastructure**, le client doit donc de se concentrer sur la mise en œuvre et la maintenance des 20 % de contrôles restants

Cas particulier pour les Fournisseurs de Services Numériques (TIC)

Les **acteurs du numérique** ne seront pas soumis aux exigences relatives aux mesures de sécurité transposées à l'échelle nationale - Ils sont soumis à un acte d'exécution publié par la commission européenne le 17 octobre 2024 qui précise les mesures à appliquer

Les acteurs du numériques correspondent aux types d'entités suivants :

Annexe 1 :

- Les fournisseurs de services DNS
- Les registres des noms de domaine de premier niveau
- Les entités fournissant des services d'enregistrement de noms de domaine
- Les fournisseurs de services d'informatique en nuage
- Les fournisseurs de services de centres de données
- Les fournisseurs de réseaux de diffusion de contenu
- Les fournisseurs de services gérés
- Les fournisseurs de services de sécurité gérés

Annexe 2 :

- Les fournisseurs de places de marché en ligne
- Les fournisseurs de moteurs de recherche en ligne
- Les fournisseurs de plateformes de services de réseaux sociaux

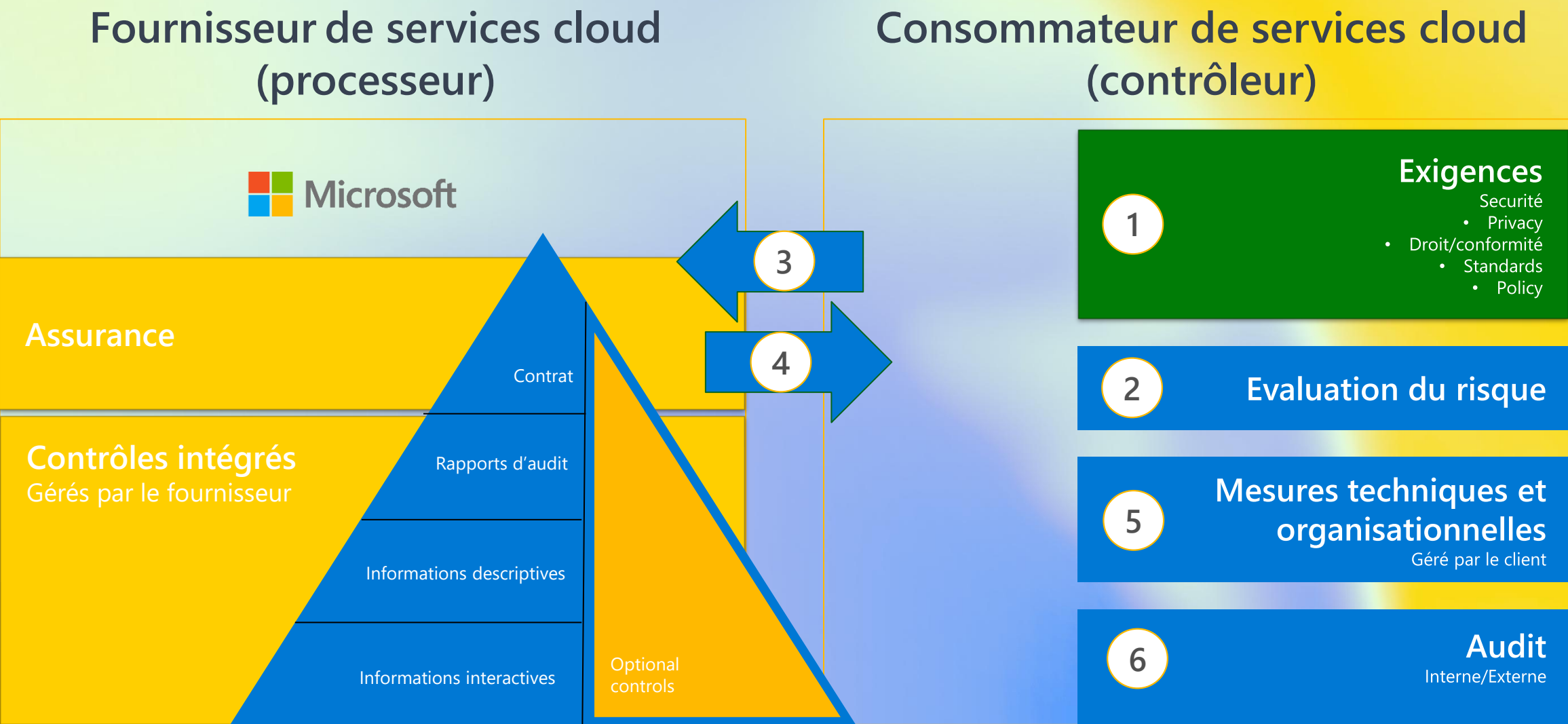
"Security is our top priority and we are committed to working with others across the industry to protect our customers."

Satya Nadella
Chief Executive Officer, Microsoft Corporation

Garantir la sécurité pour permettre votre transformation numérique grâce à une plateforme complète, une intelligence unique et des partenariats étendus.



Processus de certification



Microsoft Compliance – Trust Center

Offres de conformité réglementaire et sectorielle
(RGPD, ISO 27001, HDS...)



Certification/Assurances



Conformité Microsoft
Documentation et ressources Microsoft dont vous avez besoin pour commencer à utiliser la conformité pour votre entreprise ou organisation.

Conformité réglementaire & secteur
Conseils Microsoft sur la conformité avec les secteurs d'activité et les normes et réglementations internationales & nationales.

- Règlement général sur la protection des données (RGPD)**
Conseils pour vous aider à respecter les droits et à remplir les obligations du RGPD lors de l'utilisation des produits et services Microsoft.
- Offres pour la conformité Microsoft**
Microsoft propose un ensemble complet d'offres de conformité pour aider vos organisation à se conformer aux exigences nationales, régionales et sectorielles régissant la collecte et l'utilisation des données.
- Microsoft Cloud**
Découvrez comment Microsoft 365 et l'IA en charge les besoins de votre organisation.

Certification de service
Utilisez des ressources et une documentation de conformité organisées par des experts pour prendre en charge vos évaluations des risques de Microsoft services en ligne.

- Prise en main**
 - Formation de base sur la façon dont Microsoft protège les données
 - Guide d'évaluation des risques pour Microsoft Cloud
- Intelligence artificielle (IA)**
 - Vue d'ensemble de l'IA
 - Rapport de transparence IA 2024
 - Copilot pour les données, la confidentialité et la sécurité Microsoft 365
 - Comment Microsoft 365 fournit une IA digne de confiance
 - Démarrage rapide de Copilot pour l'évaluation des risques Microsoft 365
- Infrastructure**
 - Architecture
 - Sécurité des centres de données
 - Résilience et continuité
 - Sécurité réseau
- Opérations**
 - Enregistrement d'audit et surveillance
 - Chiffrement et gestion des clés
 - Gestion des identités et des accès
 - Gestion des incidents
 - Confidentialité et gestion des données
 - Opération de développement de sécurité
 - La gestion des menaces et des vulnérabilités
- Planification et personnel**
 - Gouvernance, risque et conformité
 - Responsabilité humaine
 - Gestion de fournisseurs
- Rapports et évaluations**
 - Rapports SOC
 - Rapports ISO
 - BCDR
 - Tests de pénétration

Offres pour la conformité Microsoft

Découvrez comment les produits et services Microsoft aident vos organisation à respecter les normes de conformité réglementaire.

Offres de conformité Azure, Dynamics 365 et Microsoft 365

Informations pour Azure, Dynamics 365, Microsoft 365 et Power Platform, ainsi que d'autres services pour faciliter l'application des réglementations.

Global	Global	Gouvernement
- Point de référence CIS - Attestation CSA-STAR - Certification CSA-STAR - Auto-évaluation CSA-STAR - CyberDIX - ISO 20000-1 :2011 - ISO 22301 - ISO 27001	- ISO 27017 - ISO 27018 - ISO 27701 - ISO 9001 - SOC 1 - SOC 2 - SOC 3 - WCAG	- CIS - CNSSI - DPARS - Dod 15 - Dod 18 - Dod 19 - EAR (U)
Secteur d'activité	Secteur d'activité	Secteur
23 NYCRR Part 500 - AFM + DNB (Pays-Bas) - APRA (Australie) - AMF et ACPR (France) - CDSA - DPP (Royaume-Uni) - EBA (UE) - FACT (Royaume-Uni) - ICA + PRA (Royaume-Uni)	- FERPA - FFEC (Etats-Unis) - FINMA (Suisse) - FISC (Japon) - PSA (Danemark) - GLBA (Etats-Unis) - GSMA - GxP - MLPS (Chine)	- HITRUST - DNF (P) - Conna - MARS - MAS + - MPA - NBB + - NEN-7 - NERC

<https://aka.ms/dpa> (contrat, SLA)

<https://aka.ms/compliance> certification

[Solutions de cybersécurité et de conformité NIS2 | Sécurité Microsoft](#)

[Conformité DORA | Centre de gestion de la confidentialité Microsoft](#)

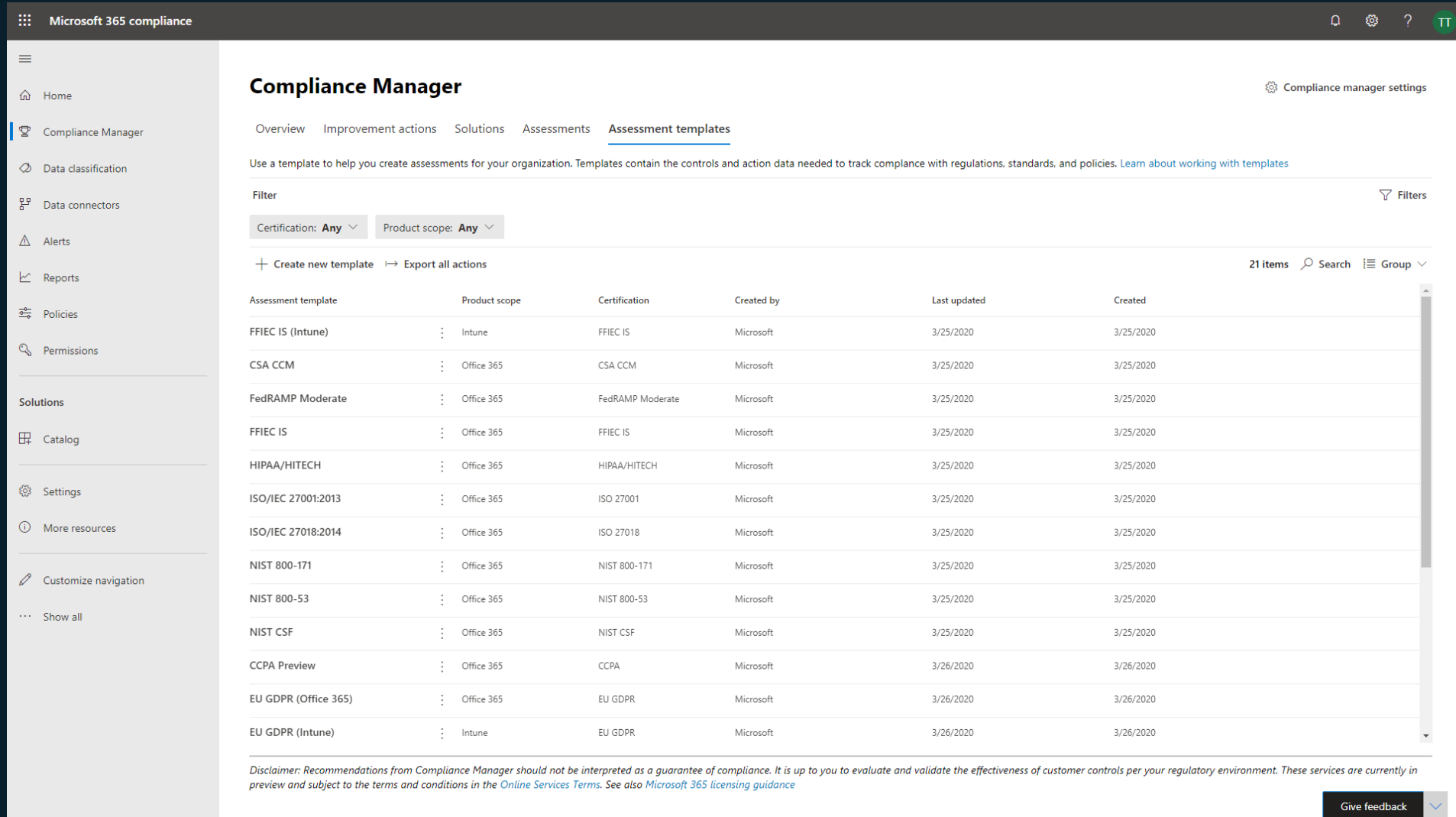


NIS2 Objectives							
Manage Security Risk		Protecting Against Cyber Attack		Detecting Cyber Security Incidents		Minimizing The Impacts Of Cyber Security Incidents	
NIS Principals							
A1: Governance	A2: Risk Management	B1: Service Protection Policies And Processes	B2: Identity And Access Control	C1: Security Monitoring	C2: Proactive Security Event Discovery	D1: Response And Recovery Planning	D2: Lessons Learned
A3: Asset Management	A4: Supply Chain	B3: Data Security	B4: System Security				
		B5: Resilient Networks And Systems	B6: Staff Awareness And Training				

Comment les clients peuvent-ils **mesurer** leur **conformité** aux exigences dans leur périmètre de responsabilité ?

Comment Microsoft peut les aider ?

Evaluer sa conformité avec Compliance Manager



The screenshot displays the Microsoft 365 Compliance Manager interface. The left sidebar contains navigation options: Home, Compliance Manager (selected), Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Solutions, Catalog, Settings, More resources, and Customize navigation. The main content area is titled 'Compliance Manager' and shows the 'Assessment templates' tab. Below the tab, there is a filter section with 'Certification: Any' and 'Product scope: Any'. A table lists 21 assessment templates, including FFIEC IS (Intune), CSA CCM, FedRAMP Moderate, FFIEC IS, HIPAA/HITECH, ISO/IEC 27001:2013, ISO/IEC 27018:2014, NIST 800-171, NIST 800-53, NIST CSF, CCPA Preview, EU GDPR (Office 365), and EU GDPR (Intune). Each row shows the template name, product scope, certification, created by, last updated, and created date. A disclaimer at the bottom states: 'Disclaimer: Recommendations from Compliance Manager should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are currently in preview and subject to the terms and conditions in the Online Services Terms. See also Microsoft 365 licensing guidance.' A 'Give feedback' button is located in the bottom right corner.

Microsoft 365 compliance

Compliance Manager

Overview Improvement actions Solutions Assessments **Assessment templates**

Use a template to help you create assessments for your organization. Templates contain the controls and action data needed to track compliance with regulations, standards, and policies. [Learn about working with templates](#)

Filter Filters

Certification: **Any** Product scope: **Any**

+ Create new template → Export all actions 21 items Search Group

Assessment template	Product scope	Certification	Created by	Last updated	Created
FFIEC IS (Intune)	Intune	FFIEC IS	Microsoft	3/25/2020	3/25/2020
CSA CCM	Office 365	CSA CCM	Microsoft	3/25/2020	3/25/2020
FedRAMP Moderate	Office 365	FedRAMP Moderate	Microsoft	3/25/2020	3/25/2020
FFIEC IS	Office 365	FFIEC IS	Microsoft	3/25/2020	3/25/2020
HIPAA/HITECH	Office 365	HIPAA/HITECH	Microsoft	3/25/2020	3/25/2020
ISO/IEC 27001:2013	Office 365	ISO 27001	Microsoft	3/25/2020	3/25/2020
ISO/IEC 27018:2014	Office 365	ISO 27018	Microsoft	3/25/2020	3/25/2020
NIST 800-171	Office 365	NIST 800-171	Microsoft	3/25/2020	3/25/2020
NIST 800-53	Office 365	NIST 800-53	Microsoft	3/25/2020	3/25/2020
NIST CSF	Office 365	NIST CSF	Microsoft	3/25/2020	3/25/2020
CCPA Preview	Office 365	CCPA	Microsoft	3/26/2020	3/26/2020
EU GDPR (Office 365)	Office 365	EU GDPR	Microsoft	3/26/2020	3/26/2020
EU GDPR (Intune)	Intune	EU GDPR	Microsoft	3/26/2020	3/26/2020

Disclaimer: Recommendations from Compliance Manager should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are currently in preview and subject to the terms and conditions in the [Online Services Terms](#). See also [Microsoft 365 licensing guidance](#)

Give feedback

Score de conformité | Hiérarchisation des actions de **remédiation** | **Evaluation** semi-automatique

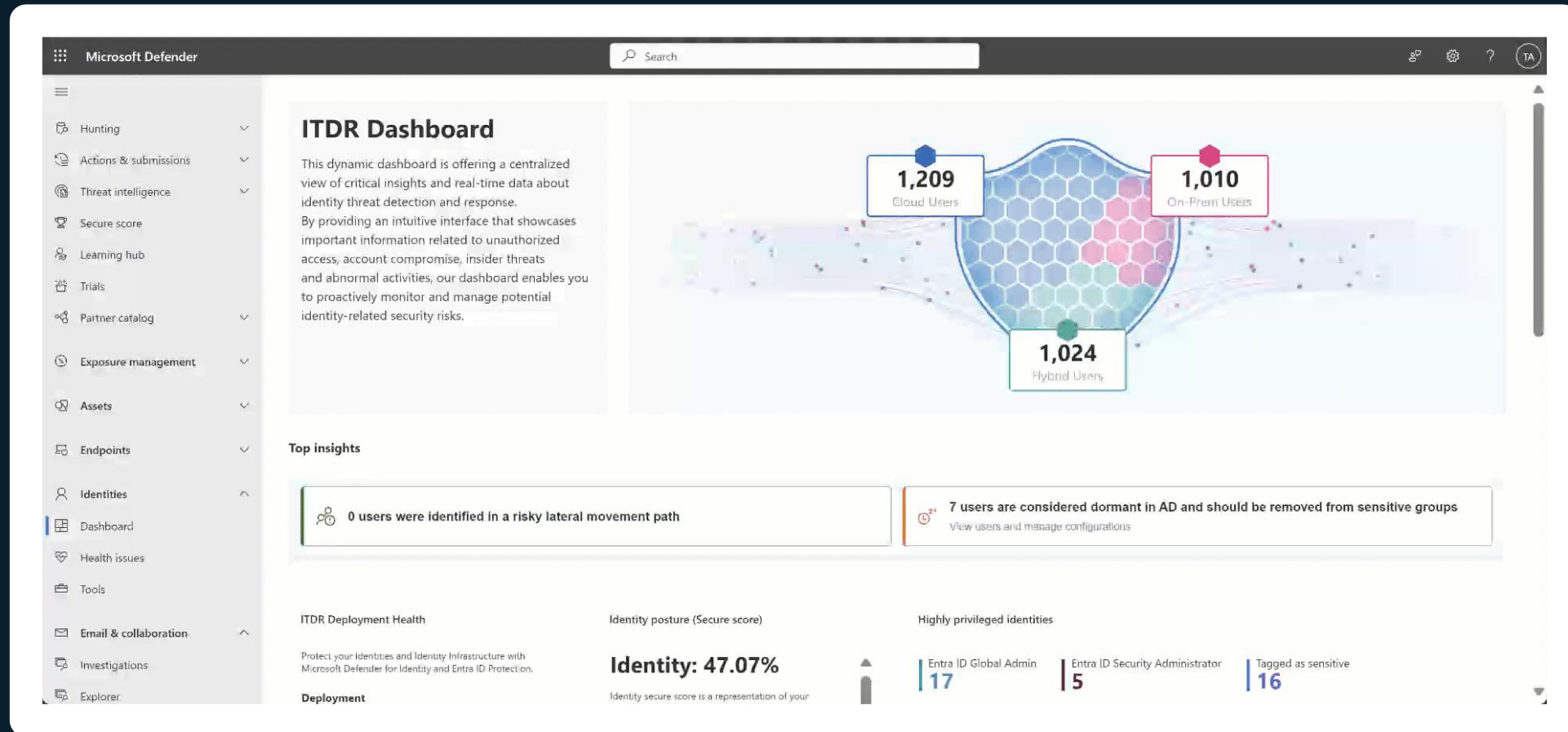


NIS2 Objectives							
Manage Security Risk		Protecting Against Cyber Attack		Detecting Cyber Security Incidents		Minimizing The Impacts Of Cyber Security Incidents	
NIS Principals							
A1: Governance	A2: Risk Management	B1: Service Protection Policies And Processes	B2: Identity And Access Control	C1: Security Monitoring	C2: Proactive Security Event Discovery	D1: Response And Recovery Planning	D2: Lessons Learned
A3: Asset Management	A4: Supply Chain	B3: Data Security	B4: System Security				
		B5: Resilient Networks And Systems	B6: Staff Awareness And Training				

L'**identité** est identifiée comme un des principaux vecteurs d'attaque, et l'un des piliers de la directive.

Comment Microsoft, peut-il aider à la protéger ?

Détection et réponse aux menaces liées aux identités



Sécurisation transparente des identités avec une **solution intégrée**

Automatiser la gouvernance des identités

Entitlement Management

- Crée des **Access Packages** pour gérer les accès aux applications, groupes, etc.
- Automatise les demandes d'accès.

Access Reviews

- Revues périodiques

Privileged Identity Management

- Gestion des rôles à temps et approbation

Lifecycle Workflows

- Automatisation de workflows pour les identités (onboarding, rôle).

Politiques de conformité et sécurité

- MFA, conditions d'accès, et intégration avec Zero Trust.



10 000 employés et 5 000 agents IA - Sécuriser l'identité à l'ère de l'IA



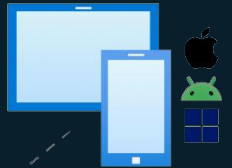
Franck Heilmann
Senior Product Manager



Christophe Guerre
Cloud Solution Architect

SaaS apps

Cloud infrastructure



tra

On-premises apps

Active Directory



L'un des objectifs des cyberattaquants est le **vol d'informations**.

Peux-tu m'en dire plus ?
 Comment Microsoft peut m'aider à répondre à cette exigence de NIS2 ?

NIS2 Objectives							
Manage Security Risk		Protecting Against Cyber Attack		Detecting Cyber Security Incidents		Minimizing The Impacts Of Cyber Security Incidents	
NIS Principals							
A1: Governance	A2: Risk Management	B1: Service Protection Policies And Processes	B2: Identity And Access Control	C1: Security Monitoring	C2: Proactive Security Event Discovery	D1: Response And Recovery Planning	D2: Lessons Learned
A3: Asset Management	A4: Supply Chain	B3: Data Security	B4: System Security				
		B5: Resilient Networks And Systems	B6: Staff Awareness And Training				

Sécurité des données : l'approche de Microsoft



Découvrez, classifiez et étiquetez automatiquement vos données et empêchez l'accès non autorisé dans vos services et les applications.



Comprenez les données et le contexte de vos données pour identifier les risques les plus élevés.

IA & cybersécurité

Quels contrôles mettre en place pour la protection de vos données



Activez la protection pour empêcher les utilisateurs d'accéder à des données sensibles via des stratégies approuvées de gestion des accès conditionnels.



Guillaume Lagache
Solution Engineer
Cybersecurity



Saida Laga
Solution Engineer
Cybersecurity



Analysez le contexte de vos données à l'échelle grâce à l'enquête de sécurité des données directement à partir d'un cas de gestion des risques internes.



Information
Protection

Data Security
Investigations

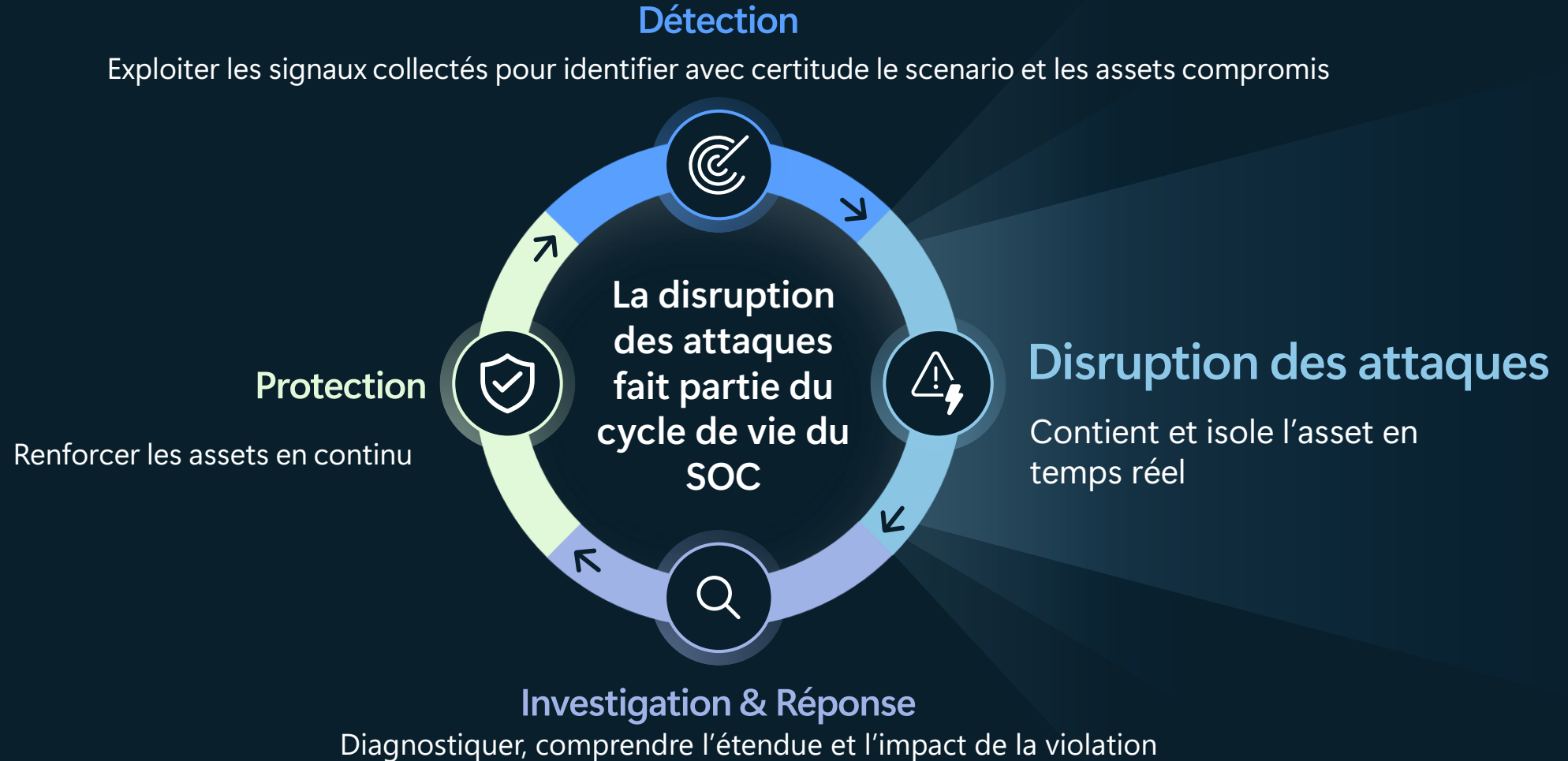
Environnements hybrides, Cloud, SaaS, appareils, navigateurs, applications et agents IA.



Quelles solutions permettent de répondre à l'exigence de **notification des incidents** aux régulateurs ?

NIS2 Objectives							
Manage Security Risk		Protecting Against Cyber Attack		Detecting Cyber Security Incidents		Minimizing The Impacts Of Cyber Security Incidents	
NIS Principals							
A1: Governance	A2: Risk Management	B1: Service Protection Policies And Processes	B2: Identity And Access Control	C1: Security Monitoring	C2: Proactive Security Event Discovery	D1: Response And Recovery Planning	D2: Lessons Learned
A3: Asset Management	A4: Supply Chain	B3: Data Security	B4: System Security				
		B5: Resilient Networks And Systems	B6: Staff Awareness And Training				

Détecter et répondre aux incidents



Détecter et répondre aux incidents

XDR + SIEM

Microsoft Security

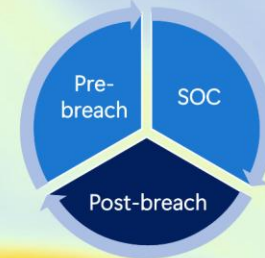
Du chaos au contrôle - Maîtriser la réponse aux incidents



Anne-Sophie Le Jouan
Cybersecurity and Cloud
Solutions Architect Director



Saad NIDIFI
Cybersecurity Cloud Solution
Architect



Couche
opérationnelle

Défense
autonome

Couche
d'intelligence



Microsoft
Security
Copilot

Principes NIS2 associés aux principales solutions Microsoft (*)

Principes NIS2		Produits Microsoft	
A1:	Governance	Defender CSPM, Entra	
A2:	Risk Management	Defender XDR and Purview Compliance Manager and Insider Risk Management	
A3:	Asset Management	Defender CSPM, Defender for Endpoint	
A4:	Supply Chain	Defender XDR, Entra and DevOps	
B1:	Service Protection Policies And Processes	Defender for API	
B2:	Identity And Access Control	Entra	
B3:	Data Security	Microsoft 365 Purview (Information Protection, Data Loss Prevention, Insider Risk Management)	
B4:	System Security	Defender for Endpoint, Defender for IoT and Intune	
B5:	Resilient Networks And Systems	Azure Network Security	
B6:	Staff Awareness And Training	O365 Phishing Simulation, Learning Paths, Policy Tips in Purview	
C1:	Security Monitoring	Defender XDR, Microsoft Sentinel	
C2:	Proactive Security Event Discovery	Defender XDR, Microsoft Sentinel	
D1:	Response And Recovery Planning	Defender XDR, Azure Backup and Recovery, M365 Backup and Archiving	
D2:	Lessons Learned	Security Copilot	

(*) non exhaustif et indicatif

Ressources

<https://aka.ms/dpa> (contrat, SLA)

<https://aka.ms/compliance> certification

[Solutions de cybersécurité et de conformité NIS2 | Sécurité Microsoft](#)
[Conformité DORA | Centre de gestion de la confidentialité Microsoft](#)

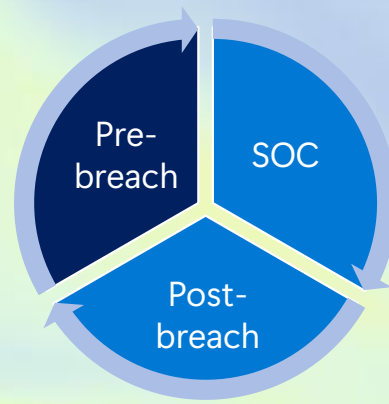
Anticipez, analysez, agissez : gardez une longueur d'avance sur les attaques



Khadidiatou BA
Solution Engineer



Daniel Pasquier
Solution Engineer



État des lieux

Charge moyenne d'une équipe sécurité:

393,419 ressources

(Apps, données, infra, postes de travail, contrôles, réseau, utilisateurs...)

Nombre moyen d'expositions par organisation:

830,639 Expositions

(CVE, contrôles mal configurés, identités privilégiées, secrets...)

Le temps moyen pour réduire l'exposition:

58 jours

(Prioriser selon le risque, valider la faisabilité, mobiliser les équipes)

Délai moyen avant exploitation des failles

5 jours



TOUT VA BIEN



CHANGE HEALTHCARE : RETOUR SUR L'ATTAQUE RANSOMWAREE DE 2024

ACCÈS INITIAL

- « *Leaked credentials* », Portail distant Citrix

DÉPLACEMENT LATÉRAL

- Comptes de service compromis, privilèges excessifs et contrôles d'authentification faibles
- Extraction de données 6TB+

DÉPLOIEMENT DE RANSOMWARE

- Systèmes centraux chiffrés, arrêt opérationnel

IMPACT SUR L'ENTREPRISE

- L'attaque a perturbé les opérations à l'échelle nationale (US)

COÛT DE LA VIOLATION

- Le coût total devrait dépasser 1 milliard de dollars

Passer de la réaction à la prévention



Niveaux de maturité pré-incident

1 Réactif

- Agir après coup
- Corriger lorsqu'une faille fait la une.
- *C'est comme mettre sa ceinture de sécurité après l'accident de voiture.*



2 Proactif

- Sécurité durable : un programme continu pour réduire les expositions
- Analyse et correction régulières tout au long de l'année.
- *C'est maintenir sa voiture en bon état grâce à l'entretien régulier.*

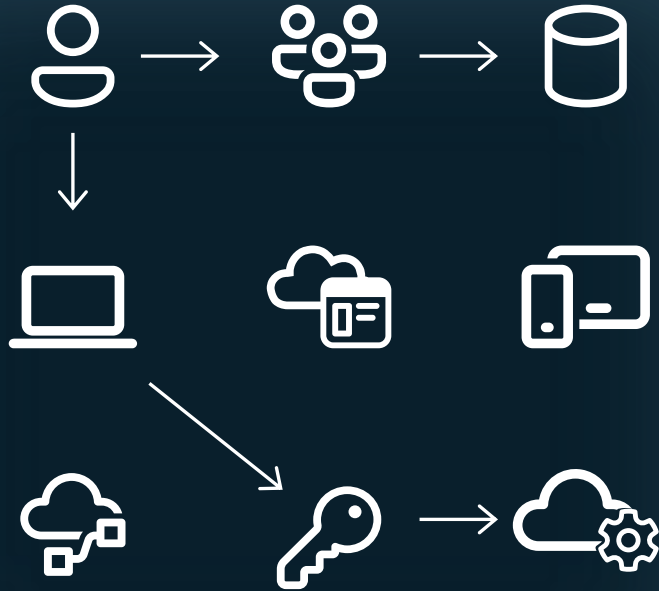


3 Préemptif

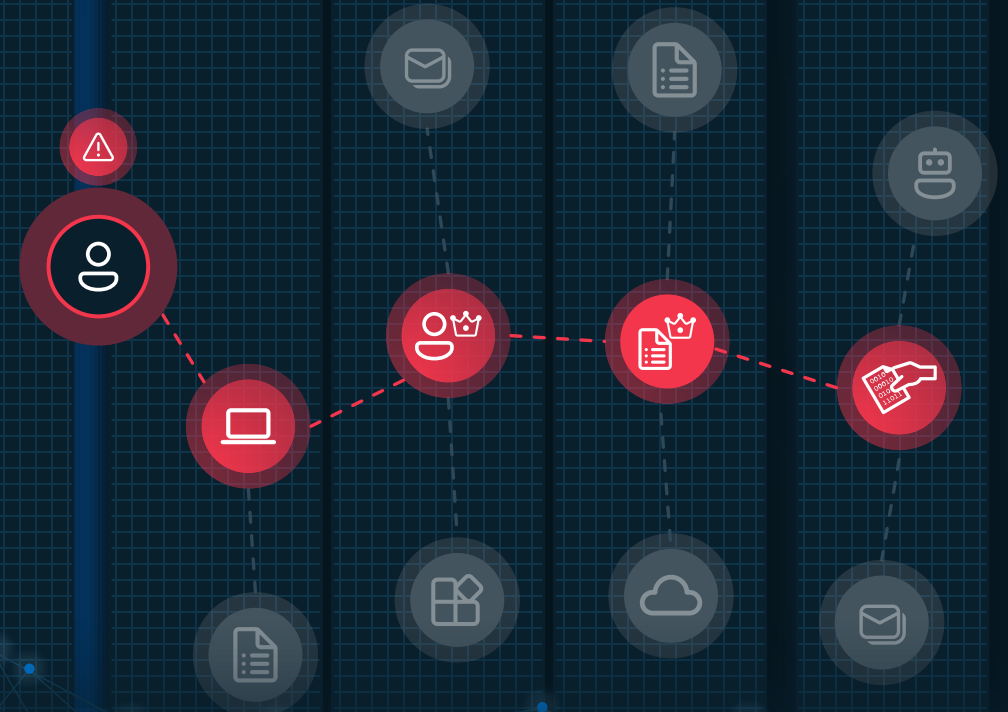
- Durcissement automatique
- Des agents qui réduisent en continu l'exposition aux menaces, de manière autonome et prudente
- *C'est une voiture autonome qui évite le danger avant même que vous ne l'ayez vu.*

Anticiper les menaces, c'est d'abord connaître sa surface d'attaque

Pré-incident



Post-incident



Carte des expositions

Découvrez Microsoft Security Exposure Management

Centraliser toutes les données et processus de sécurité

Actifs informatiques

Menaces

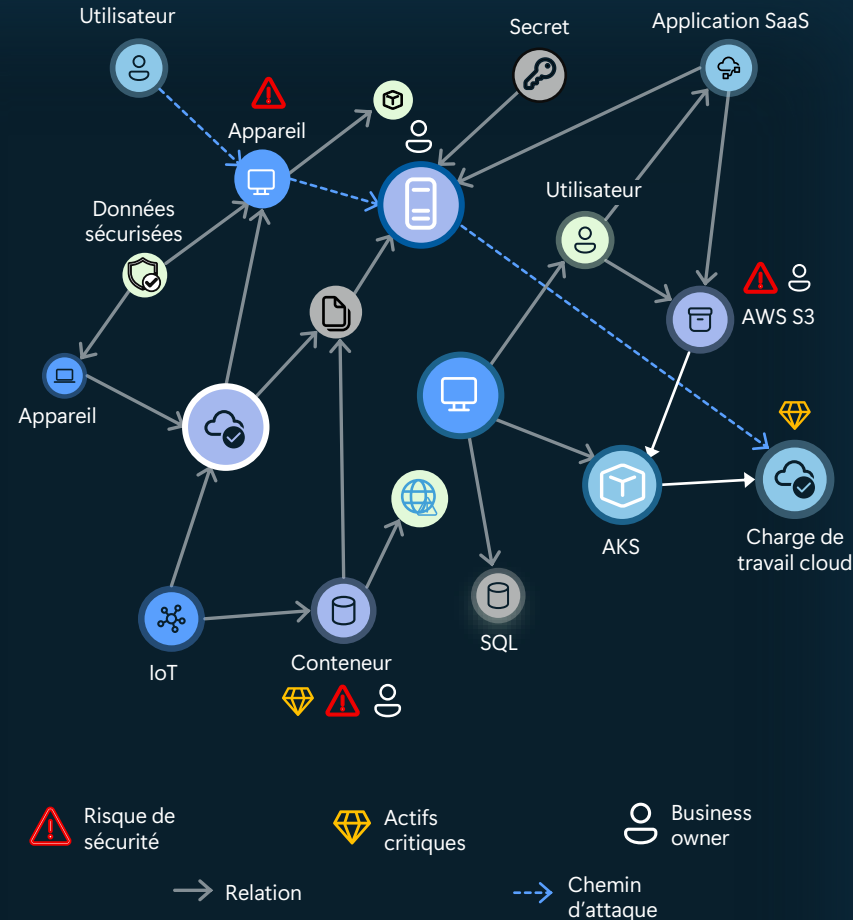
Droits d'accès et privilèges

Vulnérabilités et risques

Données, Apps, GenAI...

Entrée

Construisez un graphe relationnel de toutes les entités numériques



Minimisez votre exposition

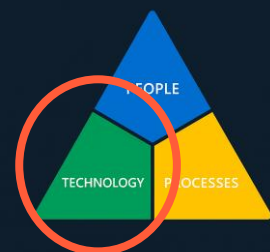
Découverte de la surface d'attaque en continue

Identification des actifs critiques

Analyse des chemins d'attaque et recommandations

Remediation et gouvernance

Sortie



Connecteurs pour inventaire unifiée des ressources

Intégration native avec les produits de sécurité Microsoft, connecteurs pour s'intégrer à la sécurité non-Microsoft

Sécurité des points de terminaison	Sécurité des e-mails	Sécurité de l'identité	Gestion des vulnérabilités	SaaS sécurité	Sécurité des applications	Sécurité cloud	Surface d'attaque externe	CMDB
Microsoft Defender for Endpoint	Microsoft Defender for Office 365	Microsoft Entra ID	Microsoft Defender Vulnerability Management	Microsoft Defender for Cloud Apps	Microsoft Defender for Cloud	Microsoft Defender for Cloud	Microsoft Defender EASM	Microsoft Intune
Microsoft Defender for IoT	Proofpoint	Microsoft Defender for Identity	Qualys*	Obsidian	Synk	Wiz*	Censys	ServiceNow
CrowdStrike*	Avanan	Okta	Tenable*	Adaptive Shield	Checkmarx	Prisma Cloud*		
SentinelOne*		Duo	Rapid7*					
↓								

*Disponible dès aujourd'hui

Asset metadata | Operational usage | Configuration data | Policy state | Security findings | Health state

Data Connectors

Explore the supported data connectors below. These connectors enable you to aggregate all your data and connect external data sources seamlessly to manage your security posture more effectively. Use the Search box to find specific connectors or apply filters to refine your search.

Connected

14

Connectors

18

Search

Default Microsoft connectors

All your connected Microsoft Security products are automatically integrated into exposure management at no extra cost. If you have the product, it's connected by default. If not, you can get it, and it will connect automatically.



Microsoft Defender For Endpoint

Connected

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.



Microsoft Defender For Identity

Connected

Microsoft Defender for Identity is a cloud-based security solution that helps secure your identity monitoring across your organization.



Microsoft Defender For Cloud Apps

Connected

Microsoft Defender for Cloud Apps is a cloud access security broker (CASB) that operates on multiple clouds. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.



Microsoft Defender For Cloud

Connected

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) that is made up of security measures and practices that are designed to protect cloud-based applications from various cyber threats and vulnerabilities.



Microsoft Defender For Office

Connected

Microsoft Defender for Office 365 is a seamless integration into Microsoft 365 subscriptions that protects against threats in email, links (URLS), file attachments, and collaboration tools.



Microsoft Defender for Vulnerability Management

Connected

Defender Vulnerability Management delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices.

Show more

External connectors



External connectors consolidate and enrich security data across your environment, providing valuable insights for effective exposure management.



ServiceNow CMDB

Connected

Connect your ServiceNow CMDB service to Exposure Management to provide a single source of truth for tracking and managing IT assets. Collect and consolidate them to provide additional context to your security posture.

[View Status](#)

Qualys

Connected

Connect your Qualys service to Exposure Management to seamlessly access and manage all your devices and vulnerabilities in one place.

View Status

**Rapid7**

Connected

Connect your Rapid7 service to Exposure Management to seamlessly access and manage all your devices and vulnerabilities in one place.

View Status



Tenable

Connection Error

Connect your Tenable service to Exposure Management to seamlessly access and manage all your devices and vulnerabilities in one place.

View Status



Wiz

Connected

Connect your Wiz account with Microsoft exposure platform to see your devices and vulnerabilities in one place.

View Status



Palo Alto Prisma Cloud

Connected

Connect your PaloAlto account with Microsoft exposure platform to see your devices and vulnerabilities in one place.

View Status



CrowdStrike Falcon early preview feature

Connection Error

Connect your CrowdStrike account with Microsoft exposure platform to see your devices and vulnerabilities in one place.

SentinelOne early preview feature

Connected

Connect your SentinelOne account with Microsoft exposure platform to see your devices and vulnerabilities in one place.



TrendMicro early preview feature

☐ Not connected

Connect your TrendMicro account with Microsoft exposure platform to see your devices and vulnerabilities in one place.

Environment Filter : Off Scope filter : Off

AI models

AI model registries

AI model endpoints

AI services

AI platforms

AI agents

AI search services

Defender coverage



Refresh Export

11 items Search Customize columns

Selected filter set: **None**   Save

Asset type: Any 

Asset label: Any

Environment: Any

CVE ID: Any

Criticality level: Any Defender coverage: Any 

Risk factors: Any

Cloud tags: Any

 Add filter

Name	Asset type	Asset label	Environment	Criticality level	Defender coverage	Recommendations	Alerts	Attack Paths	Risk factors
Agent24	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
chat summarize	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
Agent385	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
Agent624	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
agent-template-assistant	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
FinancialAssistant	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
Agent315	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
Agent898	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
Agent251	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
ContosoHR	AI agent	Microsoft Foundry ...	Azure	■■■■ None	Covered	0	No alerts	0	No recommendations
agent-quick-start-88132	AI agent	AWS Bedrock agent	AWS	■■■■ None	Covered	1	No alerts	0	No risk factors

 Create rules for devices

Assign criticality levels to your assets

Onboard them now

^① Transient devices have been automatically filtered out from some tabs to minimize noise. This filtering is determined by an internal algorithm, which mainly depends on the frequency of appearances of these discovered devices. To disable this automatic filtering, navigate to the filter menu.

Partially identified devices

265

15

6

10

12

45

Onboard Offboard Export

Search

30 Days

Customize columns Filter

Filters: Transient device: No Partially Identified Devices: No Exclusion state: Not Excluded

☐	Name ↓	IP	Criticality level	Device type	Risk level ⓘ	Exposure level ⓘ	OS platform	OS version	Sensor health state	Onboarding status	Discovery sources	Tags	Device role	Managed by
☐	woodgrove-tunnel	10.88.0.1		Server	■■■ No known ri...	▲ Medium	Linux	9.4	● Active	✓ Onboarded	 			Success
☐	woodgrove-srv1-linux.4cvpdnh...	10.0.0.5		Workstation	■■■ No known ri...	▲ Low	Linux	18.4	● Active	✓ Onboarded	 			Success
☐	woodgrove-srv1	10.0.0.4	■■■■ Very high	Server	■■■ No known ri...	▲ High	Windows Server 20...	1809	● Active	✓ Onboarded	 	Internet facing		Success
☐	woodgrove-sql	10.0.0.7	■■■ Medium	Server	■■■ Medium	▲ Medium	Windows Server 20...	21H2	● Active	✓ Onboarded	 	Internet facing		Success
☐	woodgrove-gsa01	172.16.66.12		Server	■■■ No known ri...	▲ High	Windows Server 20...	21H2	● Active	✓ Onboarded	 			Success
☐	woodgrove-dc03.woodgrove.net	172.16.66.68	■■■ Medium	Server	■■■ Medium	▲ Medium	Windows Server 20...	21H2	● Active	✓ Onboarded	 	Full Remediation	DNS, Domain Cont...	Unknown
☐	win11VM	10.0.0.11		Workstation	■■■ No known ri...	No data available	Windows	11	● Active	⚠ Can be onboarded	 			Unknown
☐	wgavdsh-0			Workstation	■■■ No known ri...	No data available	Windows 11	23H2	● Active	⚠ Can be onboarded				Unknown
☐	wg-aaddsappsrv.aadds.woodg...	172.16.2.6	■■■■ Very high	Server	■■■ No known ri...	▲ High	Windows Server 20...	1607	○ Inactive	✓ Onboarded	 	Test		Success
☐	tmvmeastus2fd29329	10.0.0.4		Unknown	■■■ No known ri...	No data available	Linux	Other	● Active	✗ Insufficient info	 			Unknown
☐	tmvmeastus2fc407a4	10.0.0.6		Unknown	■■■ No known ri...	No data available	Linux	Other	● Active	✗ Insufficient info	 			Unknown

Microsoft Defender XDR

General

Account

Session details

Email notifications

Advanced features

Permissions and roles

Streaming API

Rules

Asset rule management

Alert tuning

Critical asset management

Service accounts classification

Automated response

Identities

Devices

Agents

Overview

Feedback

 **How protected are your critical assets?**
Gain insights and recommendations in the critical asset protection initiative.

 **There are 152 attack paths leading to critical assets**
View them and take action here

Critical asset management

Manage the criticality level of your organization's assets, either according to predefined classifications or by creating your own custom ones.

Note: While we employ behavior-based logic to automatically identify assets of interest, there may be instances where not all relevant assets are identified. To ensure comprehensive coverage, we encourage you to utilize our custom queries feature to proactively search for critical assets.

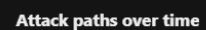
- + Create a new classification

153 items Suggest new classification Customize columns

Classification	Status	Assets	Pending approval	Criticality level	Created on	Updated on	Last run time	Created by
Predefined classifications (131)								
Tenable High Criticality	On	0	0	High				Microsoft
Wiz Very High Criticality	On	0	-	Critical				Microsoft
Wiz High Criticality	On	0	-	High				Microsoft
Wiz Medium Criticality	On	0	-	Medium				Microsoft
Wiz Low Criticality	Off	0	-	Low				Microsoft
Rapid7 Very High Criticality	On		0	Critical				Microsoft
Rapid7 High Criticality	On	0	0	High				Microsoft
Rapid7 Medium Criticality	On	0	0	Medium				Microsoft
Rapid7 Low Criticality	On	0	0	Low				Microsoft
ServiceNow High Criticality	On		0	High				Microsoft
ServiceNow Medium Criticality	On	0	0	Medium				Microsoft

Attack path management

Gain deep visibility into attack paths, focus on critical choke points, and reduce risks to safeguard your most valuable assets with attack path management. This tool offers a new perspective on your exposure, aiding in validating the potential risk of security findings.



Top 5 choke points

Name	Risk Level	Attack paths	Critical targets
b83bcd68-69cd-419e-b018-de3c75b6741b	Critical	15	15
hello-contoso	Critical	10	10
hello-contoso	Critical	7	7
hello-contoso	Critical	7	7
hello-contoso	Critical	7	7

[Show more](#)

Top 5 attack path scenarios

Name	Risk Level	Attack paths
Internet exposed container with high severity vulnerabilities allows lateral movement to azure ...	■■■■ Critical	17
Azure DevOps repository with public access allows lateral movement to azure storage account ...	■■■■ Critical	16
Internet exposed container with high severity vulnerabilities allows lateral movement to azure ...	■■■■ Critical	10
Internet exposed container with high severity vulnerabilities	■■■■ Critical	7
Internet exposed Azure VM with high severity vulnerabilities allows lateral movement to azure ...	■■■■ Critical	2

[Show more](#)

 New Attack paths just got sharper. You'll now see only the most urgent, externally sourced threats. Stay focused, stay secure. [Learn more](#)

Overview **Attack paths** Choke points

Explore the potential attack paths that attackers could use to breach your environment, and

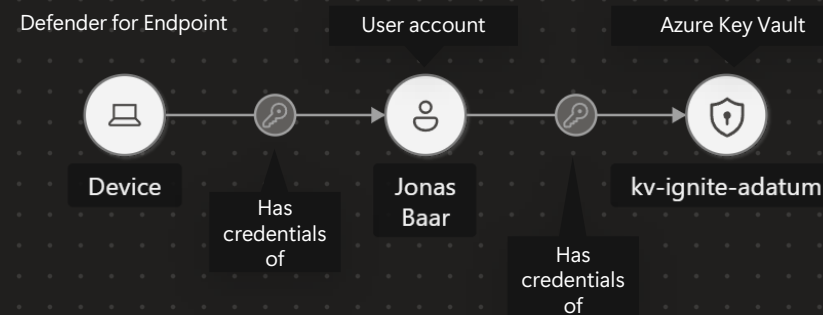
Filters: Entry point type: Any X Target type: Any X Target criticality: Any X

Attack path name	Entry point	Entry point type	Target
> Azure DevOps repository with public access all...		ADO repository	
> Azure DevOps repository with public access all...		ADO repository	
Device with high severity vulnerabilities allows I... Device with high severity vulnerabilities allo... Device with high severity vulnerabilities allo... Device with high severity vulnerabilities allo... Device with high severity vulnerabilities allo... Device with high severity vulnerabilities allo... Device with high severity vulnerabilities allo... Device with high severity vulnerabilities allo... Device with high severity vulnerabilities allo... Device with high severity vulnerabilities allo...	Not available Not available Not available Not available Not available Not available Not available Not available Not available Not available	Device Device Device Device Device Device Device Device Device Device	kv-i kv-v Myt fw-c kv-a Des fw-c woc wg

Device with high severity vulnerabilities allows lateral movement to Critical Azure Key Vault

Medium Azure

Graph Recommendations



Risk factors

Vulnerabilities	Weak authentication	Lateral movement
-----------------	---------------------	------------------

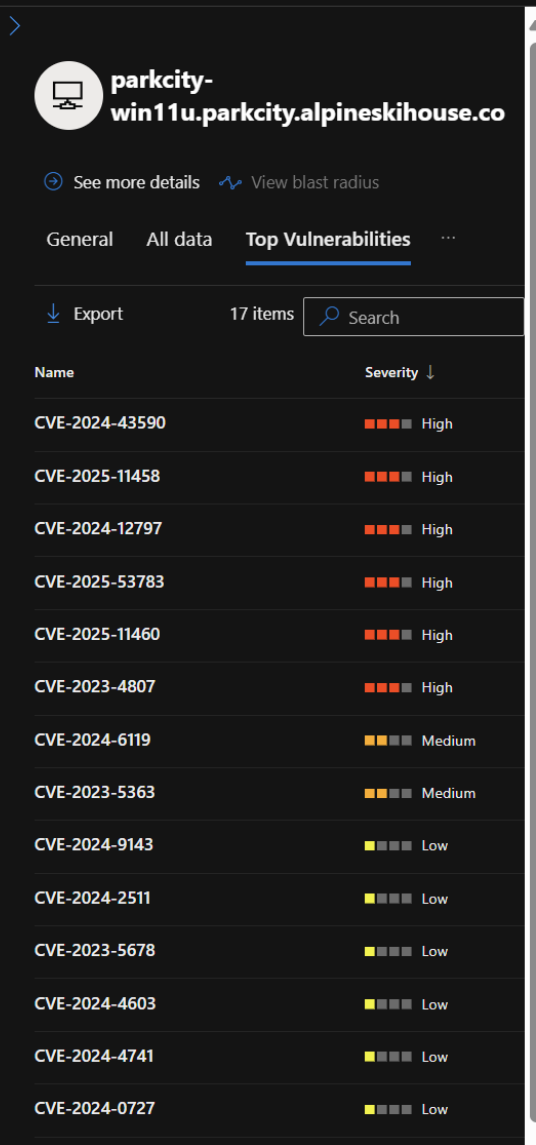
Description

A device has high severity vulnerabilities Device has multiple security issues that allow an adversary to compromise the device with high privileges and dump a cloud user's credentials The user has permissions to read data from the key vault

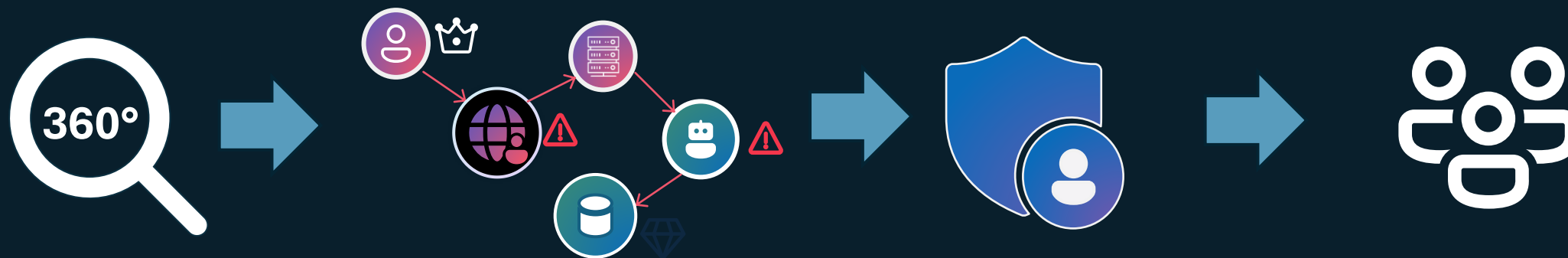
Attack Story

1. Attacker can exploit the vulnerabilities and gain control on the device
2. Attacker can dump the Primary Refresh Token of a logged on Entra user using credential dump tools
3. Attacker can use the identity to steal keys & secrets from the key vault
4. Attacker can steal keys & secrets from the Azure Key Vault

☰ Scope filter : Off ⓘ



Leçons à tirer de l'attaque Change Healthcare avec Microsoft Security Exposure Management



DECOUVERTE

Vue 360° sur les actifs, tel que les Accès distant, Comptes/IDs, machines, K8s, API, Storages, Databases, APIs, AI Agents, AI Gen Apps, Oauth Apps...

PRIORISATION

Cartographier les méthodes d'authentification et les vulnérabilités... mise en évidence automatique des chemins d'attaques permettant l'accès aux données les plus sensibles ou actifs critiques

VALIDATION

Signalez Citrix avec un MFA manquant comme remédiation prioritaire; Simuler un accès avec des identifiants volés, confirmer la facilité de compromission

MOBILISATION

Mettre en œuvre rapidement le MFA, restreindre l'accès, former et surveiller; assigner une gouvernance, une stratégie

Passer d'un travail sans fin à une sécurité durable

Flux continu de **failles de sécurité**



Traiter les priorités, puis anticiper
avec des initiatives stratégiques

Initiatives

Scope filter : Off

Key initiatives

SaaS Security

53%

No change (last 14 days)

Endpoint Security

78%

↓ -6% (last 14 days)

Cloud Security [Preview]

49%

No change (last 14 days)

Ransomware Protection V2

49%

↑ 3% (last 14 days)

Identity Security

70%

No change (last 14 days)

Domain initiatives

Threat initiatives

14-day trend	Initiative name	Mark as favorite	Current score	Workloads	14 day change drift	Last updated	Last calculated
	Business Email Compromise - Financial fraud Business email compromise (BEC) financial fraud is a social engineering attack that aims to steal money or sensitive information. The attacker tricks the target into believing they are interacting with a trusted entity to conduct either personal or professional business. After deceiving the target, the attacker persuades them to share valuable information or process a payment.	☆	82%	Defender for Office, Microsoft Information Protection, Defender for Cloud Apps, Entra ID,...	No change	Oct 10, 2025 12:21:46 AM	Oct 10, 2025 11:46:17 AM
	CIS M365 Foundations Benchmark The CIS Microsoft 365 Foundations Benchmark (v3.0.0) is a set of security assessments developed by the Center for Internet Security (CIS). It provides prescriptive guidance for establishing a secure baseline configuration for Microsoft 365. The benchmark includes configuration baselines and best practices for securely configuring a system. The benchmark is internationally recognized as a security standard for defending IT systems and data against cyber attacks. This initiative contains...	☆	60%	Defender for Cloud Apps	No change	Oct 10, 2025 12:21:46 AM	Oct 10, 2025 11:46:43 AM
	Cloud Security [Preview] This initiative aims to reflect the status around cloud security coverage, ROI, health, configuration and performance. It consists of measurements across multiple domains and disciplines to provide security managers with a high-level view into how posture is enforced in cloud ops.	☆	49%	Defender for Cloud	No change	Oct 9, 2025 5:20:30 AM	Oct 10, 2025 11:46:33 AM
	Critical Asset Protection Critical asset protection refers to the strategies, processes, and technologies implemented to	☆	59%	Defender for Cloud, Defender for Endpoint	↑ 10%	Oct 10, 2025 10:13:06 AM	Oct 10, 2025 11:46:14 AM

Pour résumer – Microsoft Security Exposure Management vous aide à anticiper, analyser et agir



Voir au-delà des
Silos :
Approche **Plateforme**



Adopter la
perspective d'un
attaquant



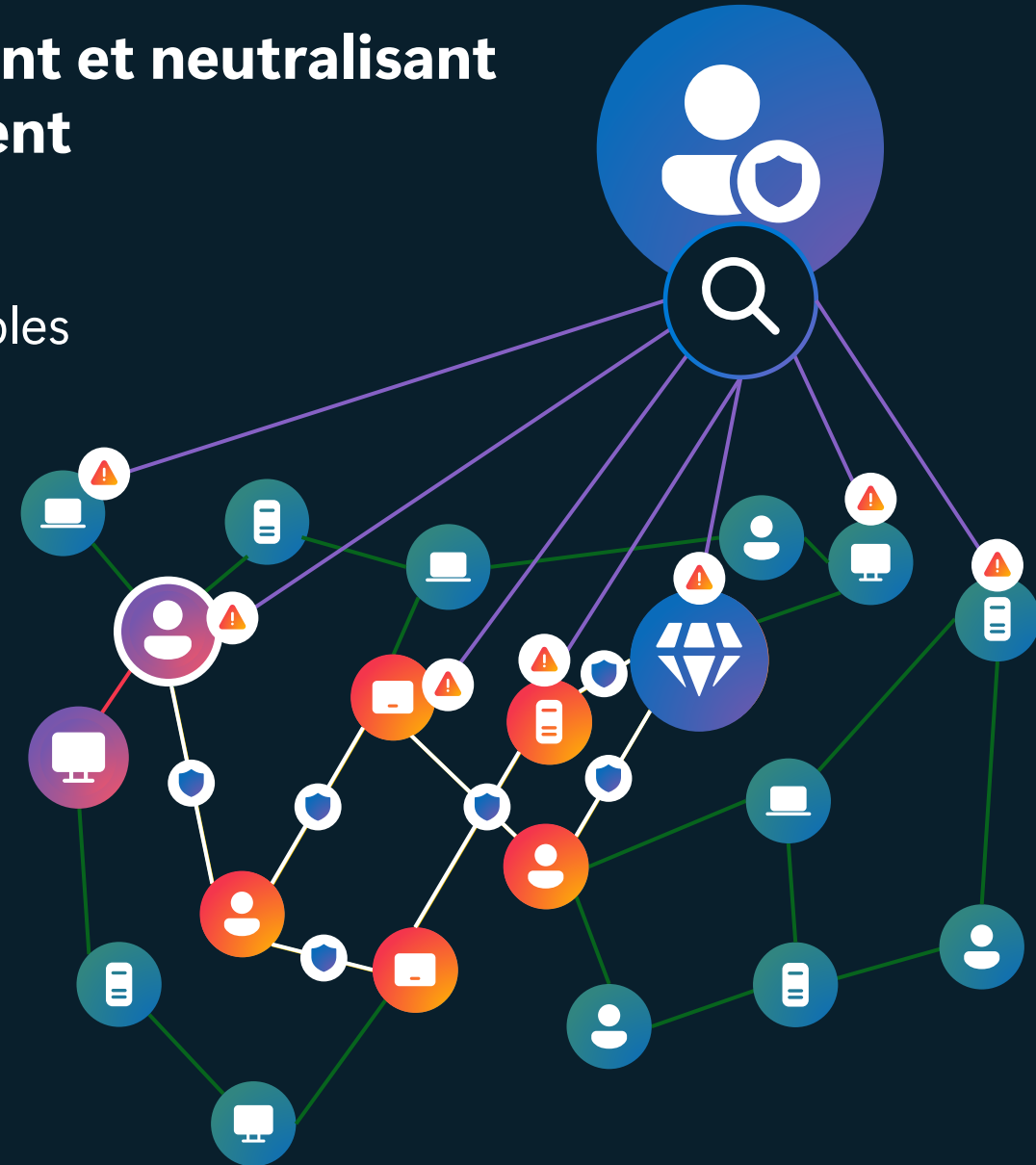
Mesurer et
prioriser
l'exposition

Vision : Sécurité Préemptive avec l'IA...

Objectif : Devancer les attaquants en détectant et neutralisant les menaces avant qu'elles n'existent réellement

Caractéristiques clés :

- **Analyse prédictive**, l'IA identifie des patterns faibles
- **Détection comportementale**, repérage d'anomalies par l'IA
- **Cyber-Deception**, leurres pour réponse anticipée
- **Agents IA 24/7**, cartographie dynamique et continue des chemins d'attaque et correction automatique (Autonomous Hardening AI agents)
- **Orchestration automatisée**, IA applique des mesures correctives sans intervention humaine



Gartner Says That in the Age of GenAI, Preemptive Capabilities, Not Detection and Response, Are the Future of Cybersecurity

STAMFORD, Conn., September 18, 2025

Comment démarrer



Accéder à Microsoft Security Exposure Management dans le portail Defender



Visualiser, analyser et agir en fonction des informations d'exposition



Classifier les assets 'Critiques'



Se former avec Microsoft Learn ou Tech Community

Le SOC du futur à l'ère de l'IA agentique



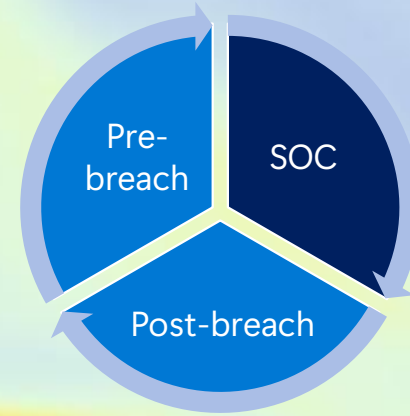
Etienne Noiret

CISSP
Cyber Security Solution
Engineer

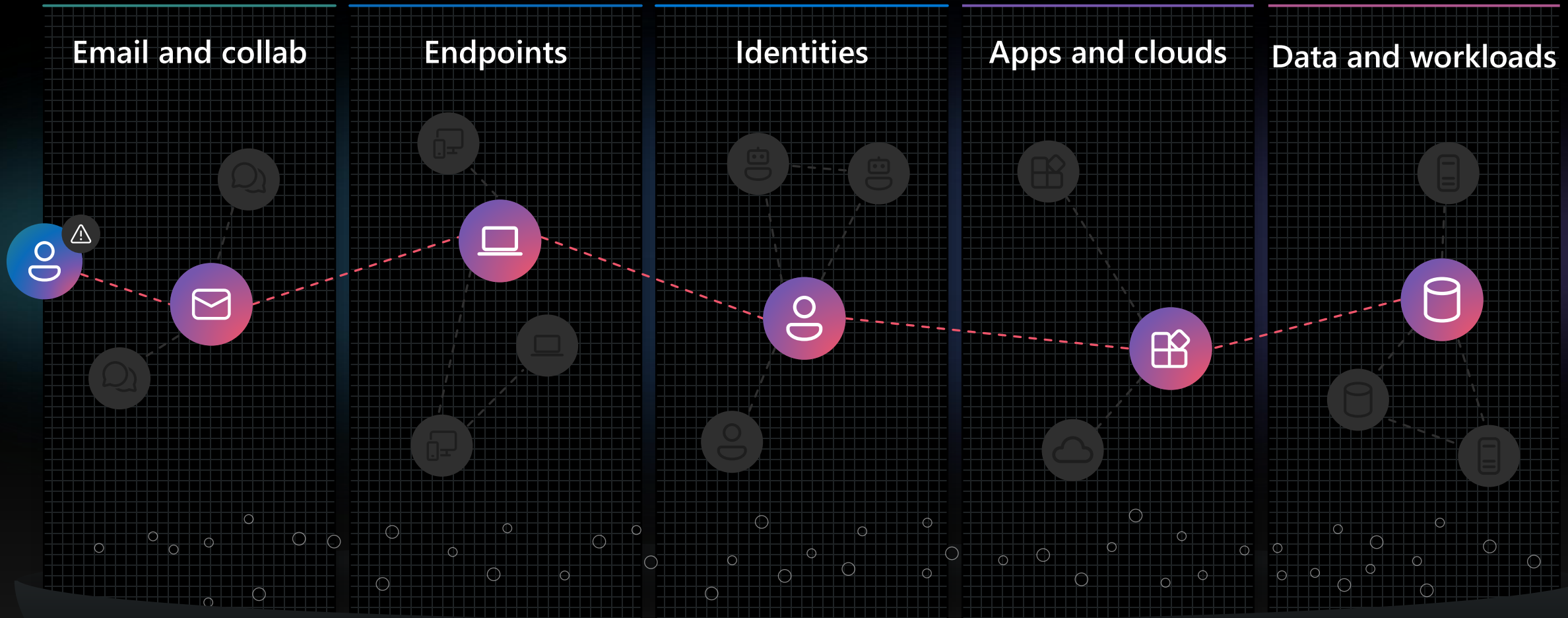


Rafik Mezil

CISSP
Cyber Security Solution
Engineer



Les attaquants pensent en Graphe



Un graphe multi-couches

Des projections adaptées aux cas d'usage



Graphe d'incident

Chemins réels observés

Graphe de renseignement sur les menaces

Chemins TTP connus de l'attaquant

Graphe d'attaque

Chemins théoriques possibles

Graphe de sécurité

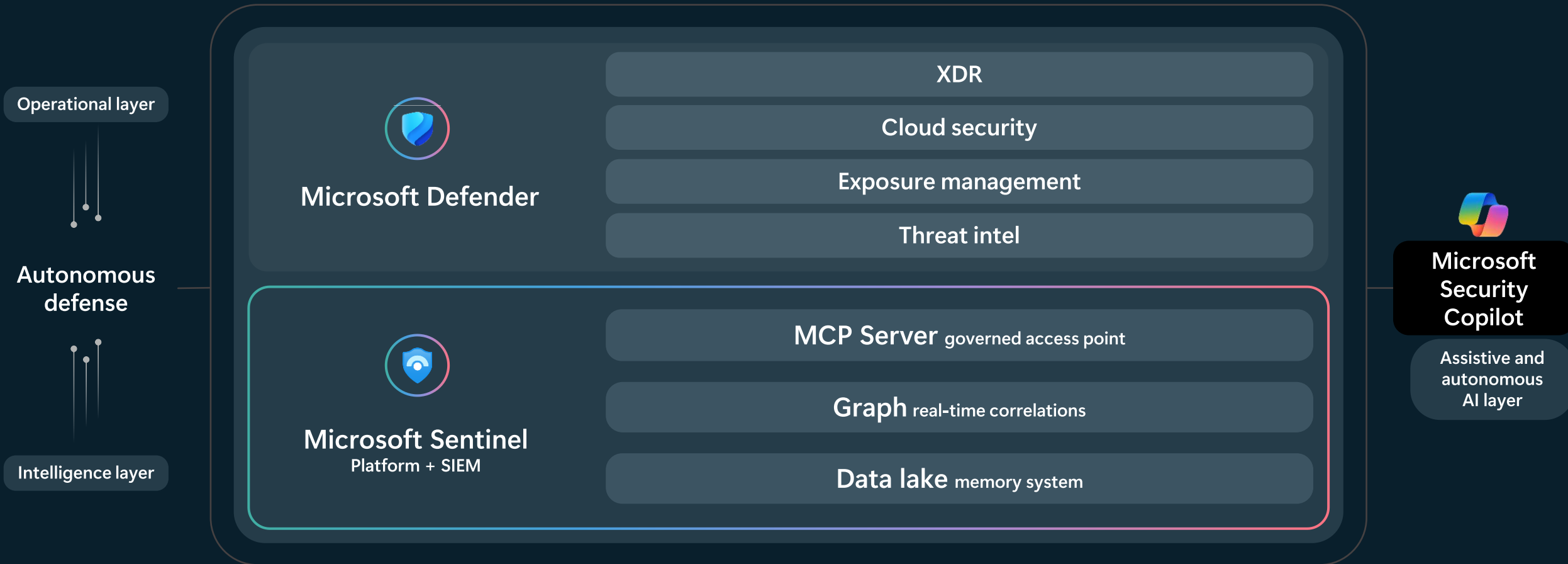
Configuration et topologie des actifs

Utiliser le graphe pour se défendre



- **Nous attaquons** le Graphe pour voir les chemins potentiels
- **Nous chassons** les activités des acteurs de la menace dans le Graphe
- **Nous investiguons** sur les attaques dans le Graphe
- **Nous renforçons** le Graphe en améliorant notre architecture et ingénierie de sécurité
- **Nous contenons** les attaques en prenant des mesures pour stopper la progression de l'acteur de la menace
- **Nous protégeons** en anticipant où l'attaque pourrait se propager dans le Graphe, puis en renforçant les défenses, en ajoutant du terrain et en supprimant les points faibles

Le Graphe comme fondation de la plateforme sécurité



Attack Disruption évolue vers Predictive Shielding

Le SOC est constamment en mode « **Réaction** », ce qui rend difficile de suivre la vitesse des attaquants et leur capacité à pivoter facilement vers la prochaine vulnérabilité.



Le « **Predictive Shielding** » offre une défense proactive en identifiant les chemins d'attaque et en appliquant des actions de durcissement ciblées « **just-in-time hardening** » sur les actifs critiques.



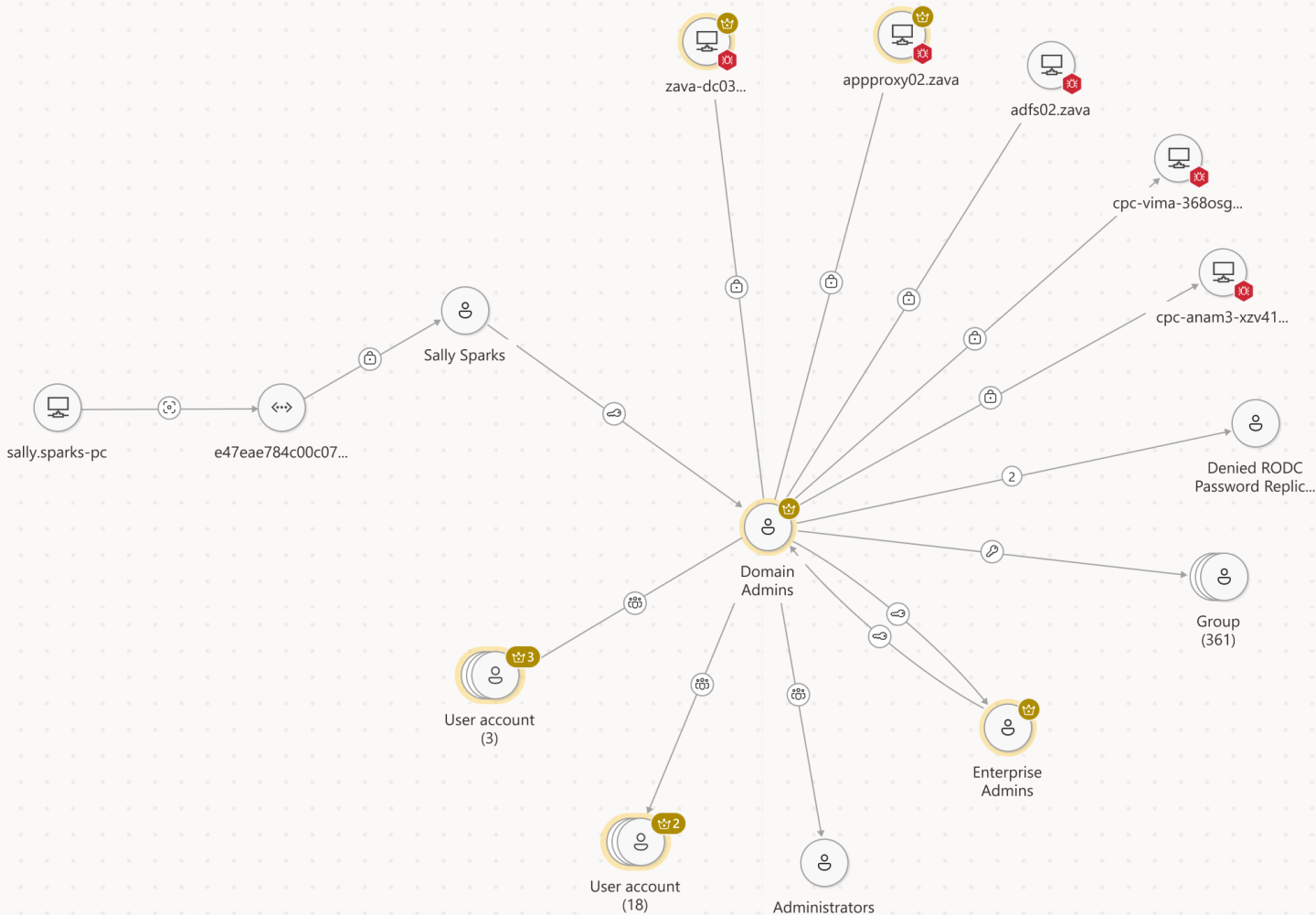
Advanced hunting

New hunt

New graph tab

Predefined scenarios

Selected scenario: Paths between two entities



ID 1134731: Multi-stage incident involving Privilege escalation related to multiple users



 Your data may contain security risks or sensitive information. Leverage AI to identify and analyze the impacted data by creating a data security investigation. [Learn about Data Security Investigations](#)

Investigate this incident

Attack story Alerts (6) Assets (6) Evidence and response (40) Similar incident Summary

Detection & categories

Incident graph ☒ Group similar entities  Layout 

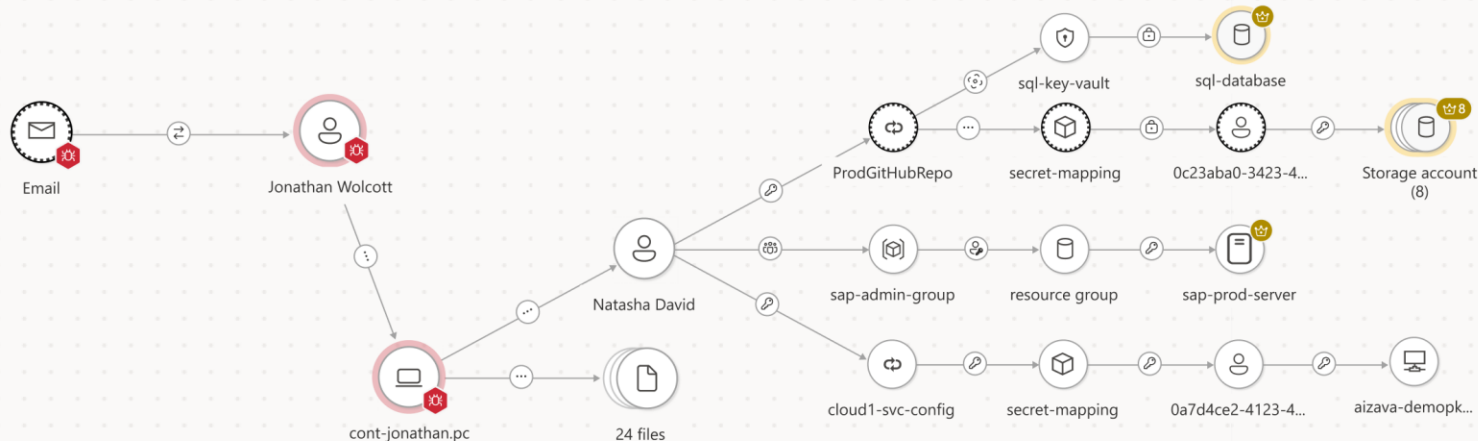
[View full blast radius list \(102 paths\)](#)

Alerts

Jul 02, 2023 4:36 AM | Active

Purview IRM ('2a04e39a') Project Obsidian

Natasha David

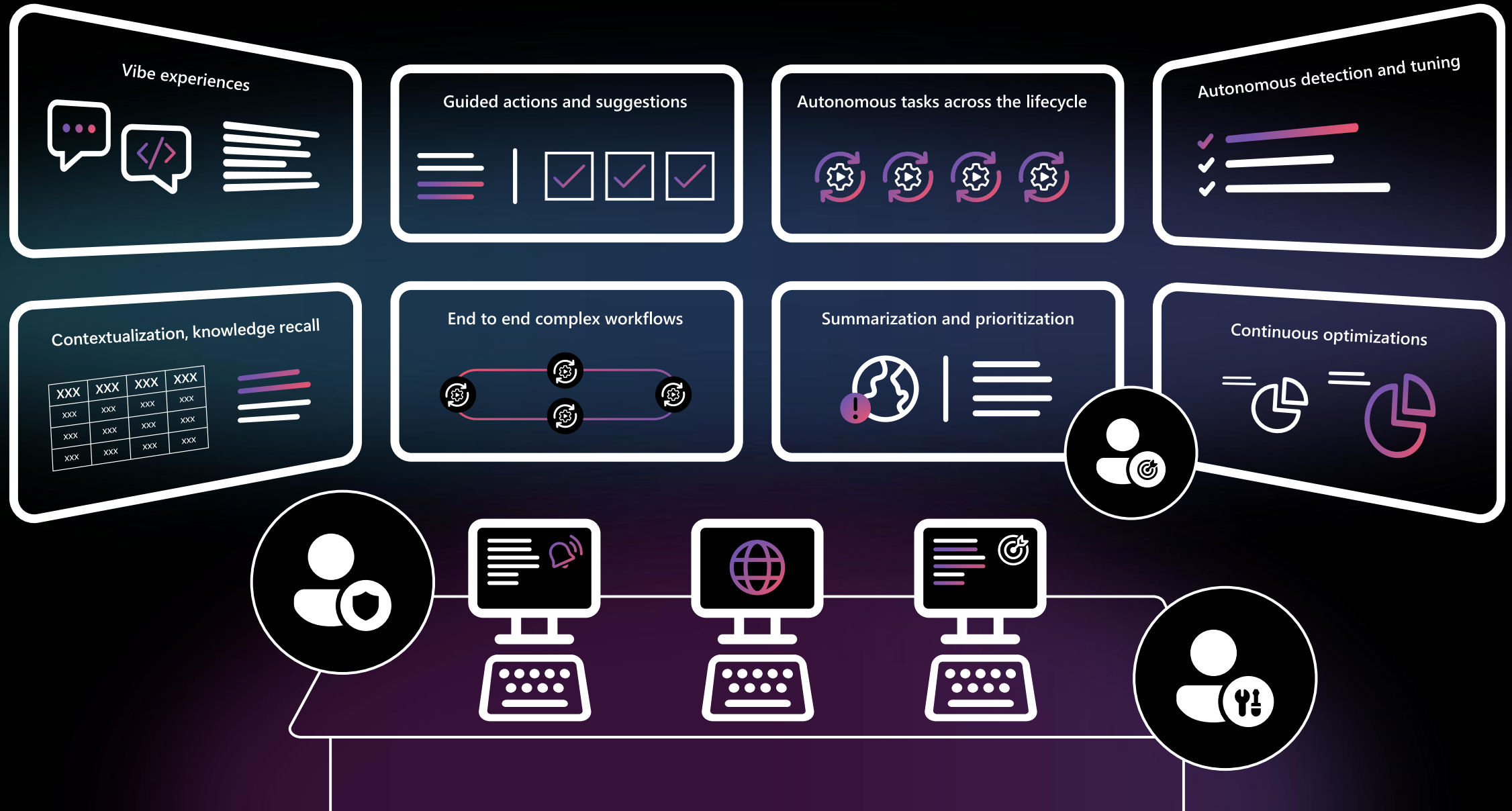


— Connection - - - Association



Et maintenant : **GenAI** et **Agents**

Dans cette nouvelle ère pour le SOC, l'IA sera partout



Chemin vers un SOC augmenté



Level of
autonomy

Zero

Assistive

Partial

High

Full



I'll do it

Assistive

Do it with me

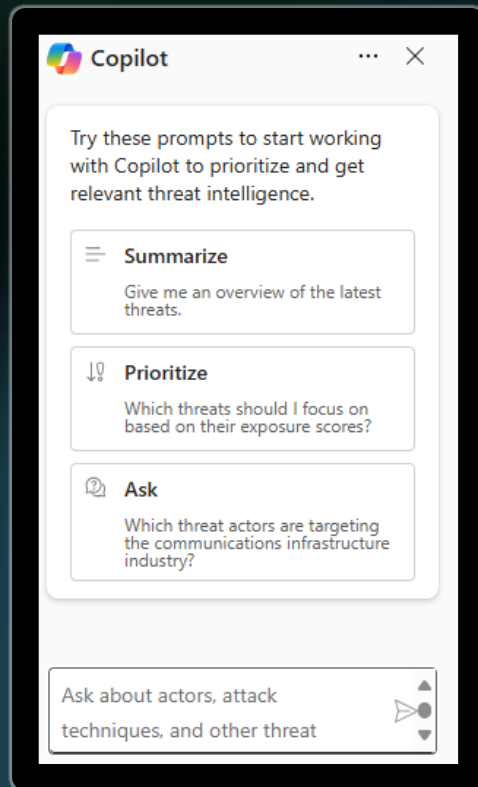
Autonomous

Do it for me

Security Copilot intégré à Microsoft Defender

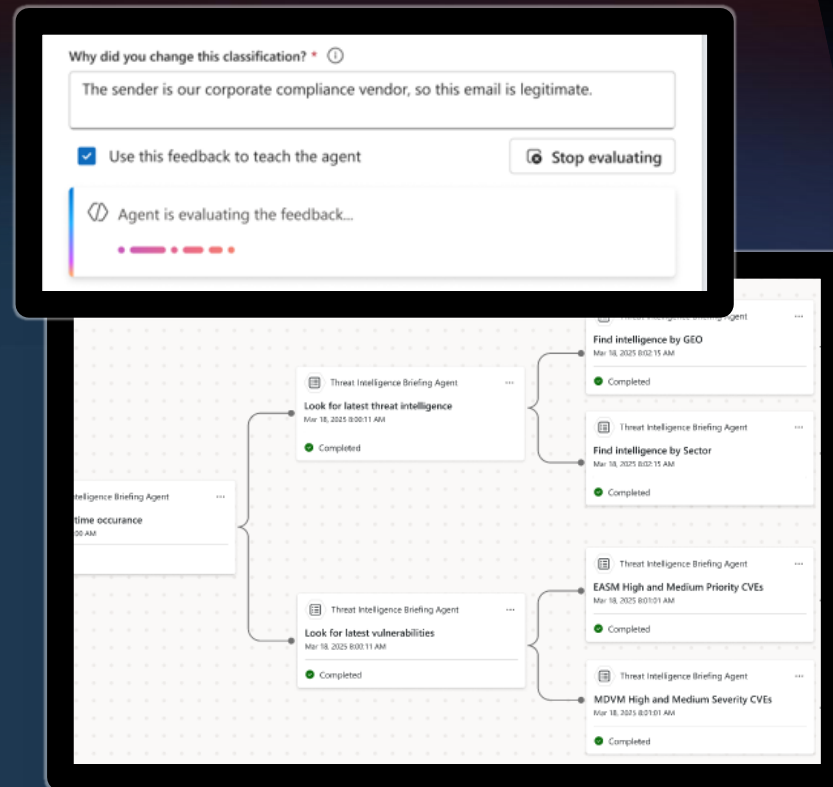
Assistive

Capacités embarquées



Autonomous

Agents prêts à l'emploi



Agents développés à façon

Security Copilot

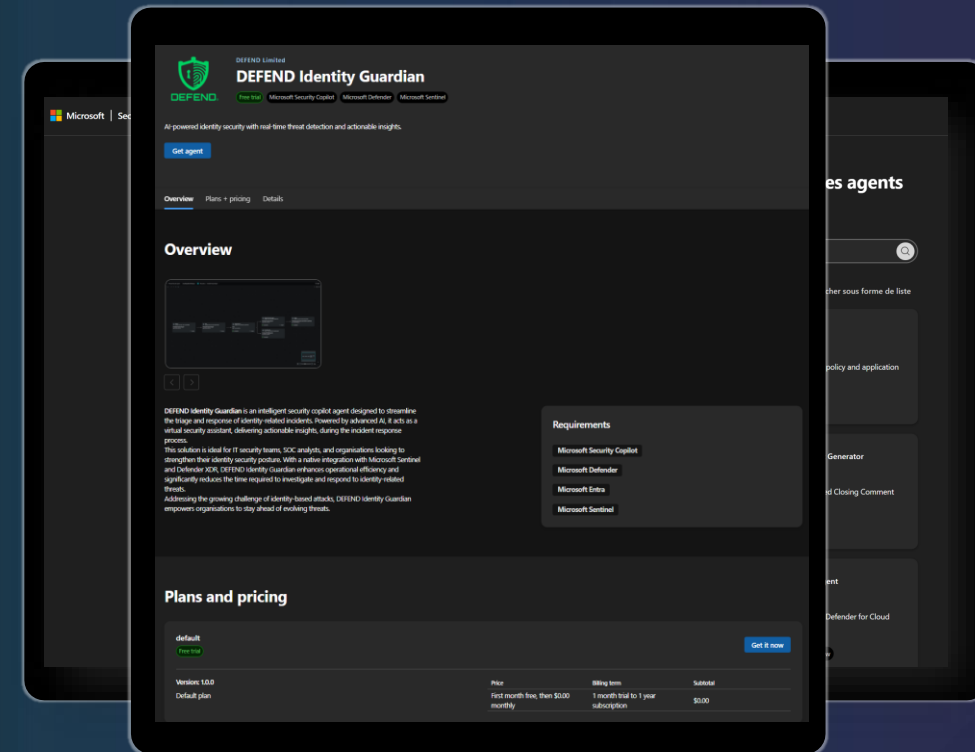
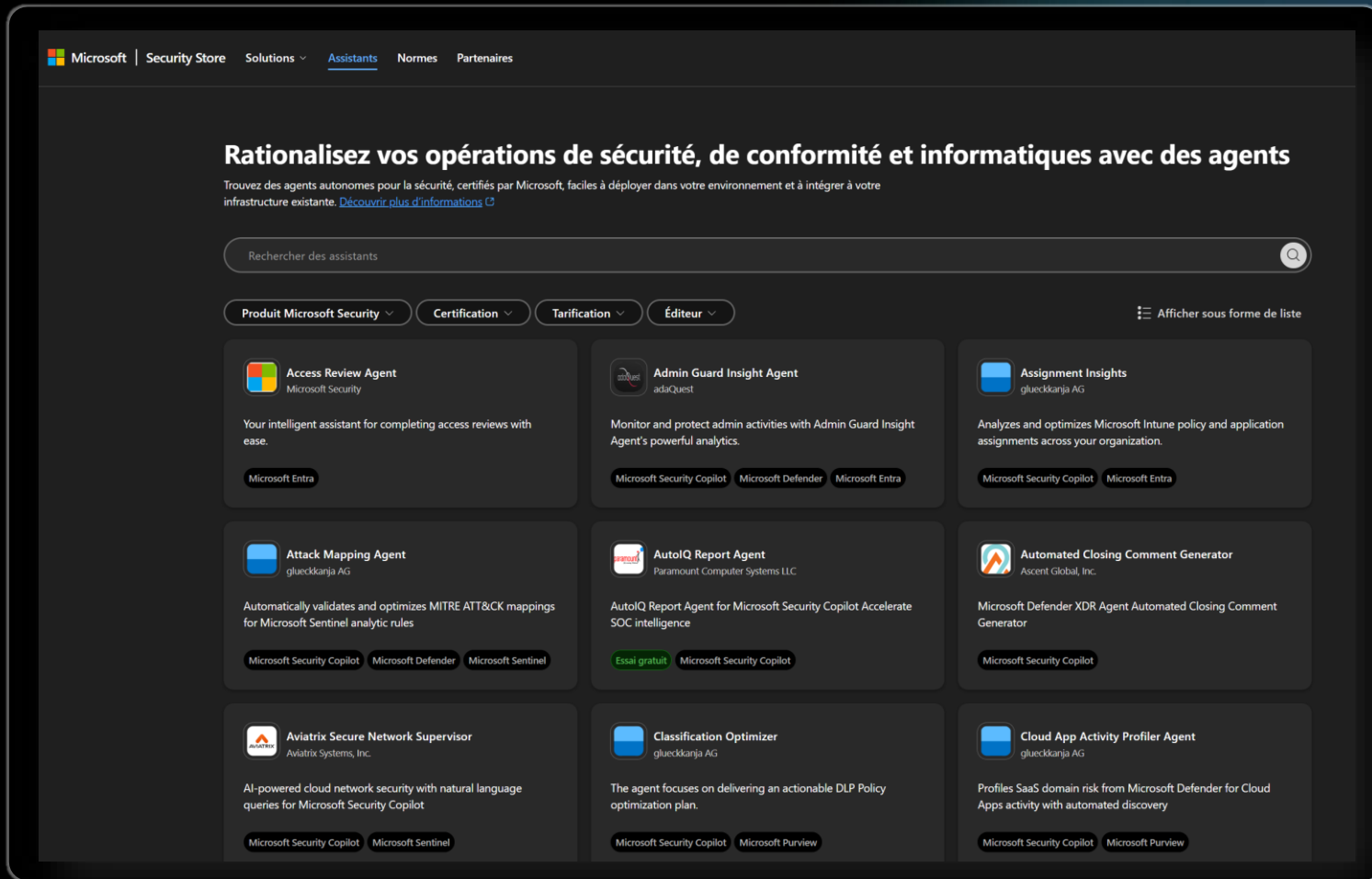
Describe what you want your agent to do

Create an agent that notifies me for anomalous activity linked to priority assets



Microsoft Security Store

Place de marché pour découvrir et déployer des solutions de sécurité et agents



Découverte des agents

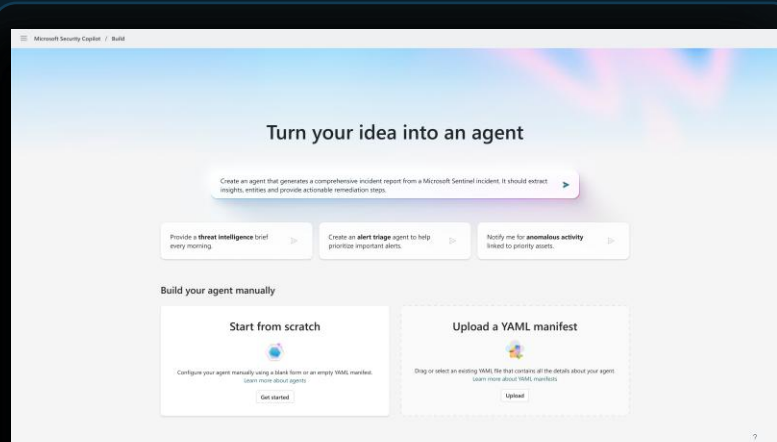
→ Set up en quelques clicks

Développez vos propres agents Security Copilot!

Des agents adaptés à vos besoins – sans développer de code

Via Security Copilot

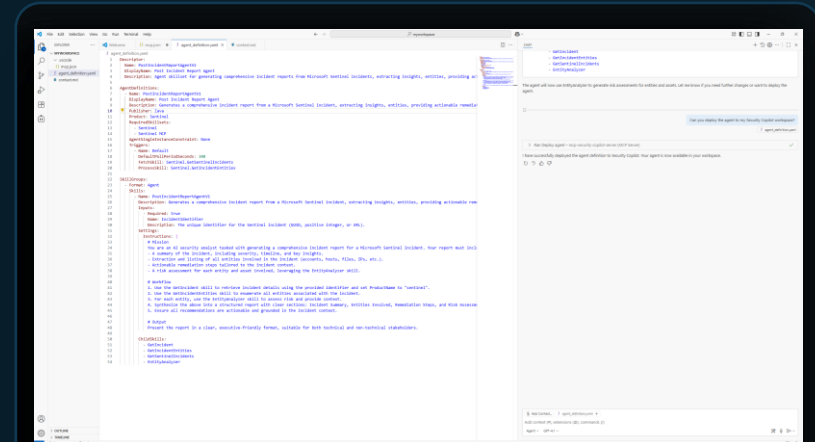
Au travers de wizards et de prompts depuis la console Security Copilot



Create an agent that generates a comprehensive incident report from a Microsoft Sentinel incident. It should extract insights, entities and provide actionable remediation steps.

Via votre environnement de développement préféré (VS Code, GitHub Copilot)

Langage naturel et vibe-coding pour construire des agents interagissant avec les serveurs MCP



Create an agent that generates a comprehensive incident report from a Microsoft Sentinel incident. It should extract insights, entities, and provide actionable remediation steps.

Domaines et compétences à couvrir à terme

Anticiper et prévenir

Adaptive and contextual threat intelligence



Autonomous hardening



Red teaming



Détecter et bloquer

Agent-powered attack disruption



Predictive shielding



False negative detection



Detection engineering tuning



Trier et investiguer

Autonomous alert triage



Auto investigation



Threat hunting



Malware analysis



Décider et répondre

Decision confidence scoring



Cross-vendor orchestration



Récupérer et optimiser

Translate lessons learned into detections, hunts, and playbooks



Monitor for control drift



Regression checks and reporting



Standard Operation Procedure (SOP) pour les réponses guidées

Importez vos procédures internes pour que Copilot adapte ses réponses à vos standards et protocoles, rendant la réponse plus fiable et efficace.

The screenshot displays the Microsoft Defender Security Copilot interface. The browser address bar shows the URL `https://defender.microsoft.com/securitysettings/securitycopilotindefender`. The page title is "Security Copilot in Defender". The left sidebar contains navigation icons, and the main content area is titled "Custom guidebooks".

Under "Custom guidebooks", there is a section for "Add new guidebook" with buttons for "Activate" and "Deactivate". Below this, a table lists guidebooks, with one currently in the "Pending review" state. A modal dialog titled "Add guidebook with Copilot" is open, providing instructions for adding a guidebook.

Add guidebook with Copilot

- 1. Upload file**
Use a PDF, text, or Word file (up to 3 MB) with content Copilot can use to prepare a guidebook.
- 2. Review guidebook**
In the 'Pending review' tab, activate or delete the AI-generated guidebook.

At the bottom of the modal, there are two buttons: "Upload file" and "Cancel".

Incident - Microsoft Defender

https://defender.microsoft.com/incident/2089/overview?tid=0527ecb7-06fb-4769-b324-fd4a3bb865eb

Zava

Microsoft Defender

Search

Incidents > Multi-stage incident involving Initial access & Defense evasion involving one user reported by multiple sources

Multi-stage incident involving Initial access & Defense evasion involi...

CopilotManage incident

HighActiveUnassigned

Attack storyAlerts (26)Assets (9)Investigations (0)Evidence and Response (12)SummarySimilar incidents (0)

Alerts

Play attack storyUnpin allShow all

Sep 16, 2024 3:41 AMIn progressActivity from a Tor IP addressu1596

Sep 16, 2024 3:41 AMNewSuspicious behavior: Impossible travel activityu1596u1596

Sep 16, 2024 4:12 AMNewActivity from a Tor IP addressu1596

Sep 16, 2024 4:12 AMResolvedAnonymous IP addressu1596

Sep 16, 2024 4:12 AMResolvedAnonymous IP addressu1596

Sep 16, 2024 4:13 AMNewAnomalous Tokenu1596

Sep 16, 2024 4:13 AMResolvedAnonymous IP addressu1596

Incident graphLayoutGroup similar nodes

u1596@ash.zava

u1596

3 Cloud Applications

cybersoc

4 IPs

2 IPs

192.42.116.186

CommunicationAssociation

Tasks

Status: OpenSort

Add task

Completed tasks 0/13

NewCustom guidebook

Force a password reset

Force a password reset if the user is not passwordless and you suspect their password may have been compromised.

Mark as completed

AI-generated content may be incorrect. Check for accuracy.

NewCustom guidebook

Temporary Access Password

Contact Local Technology Services (LTS) to issue a Temporary Access Password (TAP) and revoke user tokens.

Mark as completed

AI-generated content may be incorrect. Check for accuracy.

NewCustom guidebook

Send an email to the local LTS office to work with the user to go passwordless.

Mark as complete

AI-generated content may be incorrect. Check for accuracy.

Prevent

Uncategorized

Agent Dynamic Threat Detection Agent

Avant : investigations manuelles, outils dispersés, angles morts.

Maintenant : un agent analyse automatiquement incidents et télémétrie, détecte les failles et génère alertes avec contexte et actions.

The screenshot displays the Microsoft Defender portal interface. The top navigation bar includes the 'Zava' logo and a search bar. The main header shows the incident title: 'ID 140020: Malicious AWS federated sign-in using a compromised Entra ID account (attack disruption)'. Below the header, there are tabs for 'Attack story', 'Alerts (5)', 'Activities (8)', 'Assets (3)', 'Evidence (2)', 'Similar incident', and 'Summary'. The 'Alerts' tab is selected, showing a list of alerts. One alert is highlighted with a red box: 'Aug 20, 2025 6:17:04 PM | New Suspicious Connected Apps Reconnaissance Activity | Jonathan Wolcott | 218.107.132.66'. To the right of the alerts list is an 'Incident graph' showing a network of entities and their relationships. The graph includes nodes for 'Zava Bonus', 'JonathanW@zava.com', 'Jonathan Wolcott Disabled', '218.107.132.66', 'db_backup_job Disabled', and 'AWSAdminRole Session revoked'. The graph is interactive, with a 'Group similar entities' toggle and a 'Layout' dropdown menu.

Incidents - Microsoft Defender

Microsoft Defender

https://defender.microsoft.com/Incidents/id140020

Zava

Microsoft Defender

Search

Incidents > Malicious AWS federated sign-in using a compromised Entra ID account (attack disruption)

ID 140020: Malicious AWS federated sign-in using a compromised Entra ID account (attack disruption)

High

Active

Unassigned

Unclassified

Last update time: Aug 20, 2025 6:26:12 PM

Attack disruption

Critical Asset

Compromised Credentials

Agent

Manage incidentTaskCopilot

Attention

Attack disruption initiated multiple response actions. For more details, go to the Activities tab or visit the Action center.

Attack story

Alerts (5)

Activities (8)

Assets (3)

Evidence (2)

Similar incident

Summary

Detection & categories

Incident graph

Active alerts

5\5

Categories

3

First activity

Aug 20, 2025 12:10:02 PM

Last activity

Aug 20, 2025 6:26:12 PM

Alerts

Aug 20, 2025 12:10:02 PM | Active

Email messages removed after delivery

JonathanW@zava.comJonathanW@zava.comZava Bonus

Aug 20, 2025 6:15:07 PM | Active

Possible compromised user account sign-in

Jonathan Wolcott 218.107.132.66

Aug 20, 2025 6:17:04 PM | New

Suspicious Connected Apps Reconnaissance Activity

Jonathan Wolcott 218.107.132.66

Aug 20, 2025 6:22:32 PM | Active

Malicious AWS federated sign-in with compromised Entra ID account

JonathanW@zava.comAWSAdminRole218.107.132.66

Aug 20, 2025 6:26:12 PM | Active

Malicious AWS IAM user backdoor account

db_backup_job

Group similar entities

Layout

New query tab

JonathanW@zava.com

Jonathan Wolcott Disabled

218.107.132.66

AWSAdminRole Session revoked

db_backup_job Disabled

Suspicious Connected App...

Dynamic Threat Detection agent

Aug 20, 2025 6:17:04 PM

AI-generated content may be incorrect. Check it for accuracy.

Unusual enumeration or metadata access activity targeting federated or OAuth-connected applications has been detected. Such activity may indicate an attacker attempting to discover integrated services or identity trust relationships—such as AWS, Salesforce, or Google—that rely on the organization's identity provider.

Recommended actions:

Suspicious Connected Apps Reconnaissance Activity

MediumNewUnknown

Open alert pageManage incident

This is an AI-generated alert by the Dynamic Threat Detection Agent (preview). Learn more

Alert State

ClassificationAssigned to

Not setUnassigned

Set classification

Alert Details

Alert ID

dl49fecfd6-67c3-be69-3e00-08de1c9d

Detection source

Security Copilot

Categories

Reconnaissance

Generated on

Service source

Defender XDR

MITRE ATT&CK

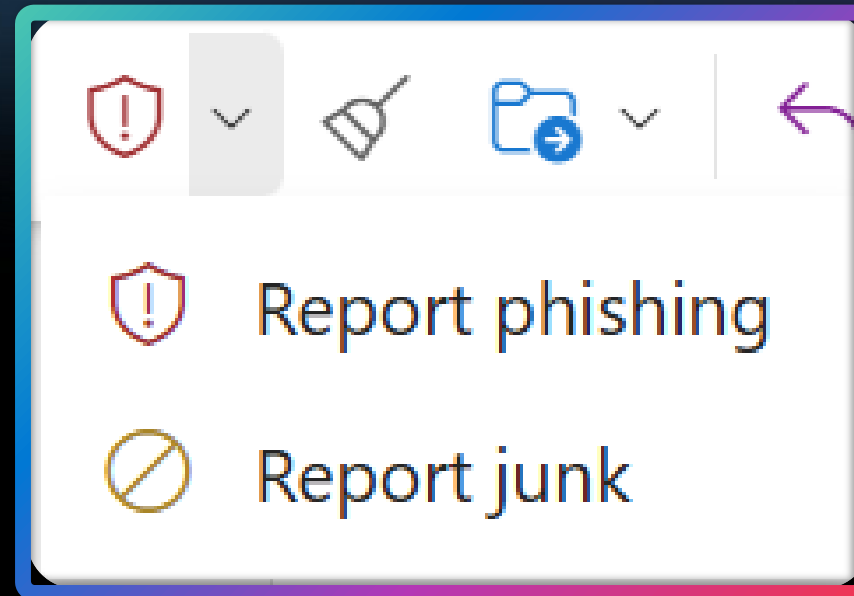
Cloud Service Discovery (T1526)

First activity

Agent Phishing Triage

Avant : des centaines d'alertes à trier, beaucoup de faux positifs.

Maintenant : l'agent gère automatiquement les emails signalés, filtre le bruit et livre un verdict rapide.





Agents > Phishing Triage Agent



Phishing Triage Agent

Preview

Active

Pause

Edit agent

Overview Performance Activity

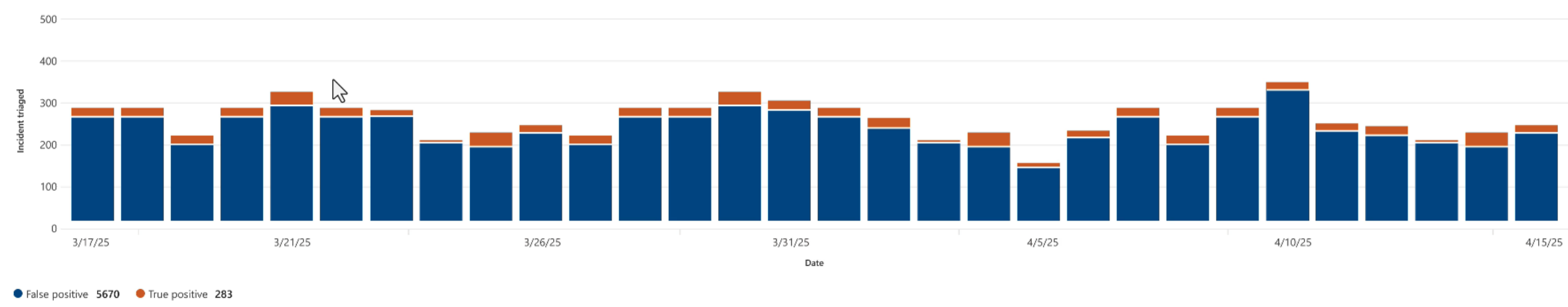
Last 30 days

Incidents resolved 95%

Mean time to triage 10min

Incident triage results

See details



Agent Threat Hunting

Avant : syntaxe complexe, investigations lentes.

Maintenant : investigation en langage naturel, guidée par l'agent avec réponses et actions rapides.

Microsoft Defender

Search

Advanced hunting

New hunt

New hunt

Schema

Search

Favorites

Defender XDR and Sentinel

Apps & identities

Email & collaboration

Devices

Defender Vulnerability Management

Exposure management

LogManagement

Custom Logs

Active Directory Health Check

AzureResources

Microsoft Sentinel

Anomalies

ASimAuditEventLogs

ASimAuthenticationsEventL...

Run query

Last 30 Days

Save

Create detection rule

Query

1

Get started

Results

Query history

Query name	Run date ↓	KQL	Tenant	Tenant ID
Email events	Jul 2, 2025 19:28	<pre>CloudAppEvents 1. where ActionType == "MailItemsAccessed" //Defines the action type we want to filter on 2. extend Folders = RawEventData.Folders[0] //Set variable and then use the index to trim the [] to data can be accessed</pre>	Inceptos	43634736
Unnamed	Jul 2, 2025 16:32	<pre>CloudAppEvents 1. where ActionType == "MailItemsAccessed" //Defines the action type we want to filter on 2. extend Folders = RawEventData.Folders[0] //Set variable and then use the index to trim the [] to data can be accessed</pre>	Magna Malesuada	34634763
Unnamed	Jul 2, 2025 16:28	<pre>CloudAppEvents 1. where ActionType == "MailItemsAccessed" //Defines the action type</pre>	Ullamcorper	35235235

Security Copilot

Hey Kat! Ready to hunt?
Start your threat-hunting journey with Copilot. Ask questions about your data or use the suggested prompts below to uncover patterns and potential threats.

Am I affected by Container Escape Vulnerability in runc? |

Threat Hunting Agent

AI-generated content may be incorrect. Check it for accuracy.

SHTML file extensions are an uncommon file type often used to deliver malware or used in phishing....

Collect all Server IDs

Show me office files with saved passwords, in english

Threat analytics - Microsoft Defen

Advanced hunting- Microsoft Def

Incident- Microsoft Defender

https://defender.microsoft.com/advancedhunting

zava Microsoft Defender

Search

Selected workspace: Zava Copilot Help resources

Advanced hunting

New hunt New hunt

Schema Run query Last 7 Days Save Create detection rule

Search

Favorites

Defender XDR and Sentinel

Apps & identities

Email & collaboration

Devices

Defender Vulnerability Management

Exposure management

LogManagement

Custom Logs

Active Directory Health Check

AzureResources

Microsoft Sentinel

Anomalies

ASimAuditEventLogs

ASimAuthenticationsEventL...

ASimDhcpEventLogs

ASimDnsActivityLogs

ASimFileEventLogs

ASimNetworkSessionLogs

ASimProcessEventLogs

ASimRegistryEventLogs

Query

on UserPrincipalName project TimeGenerated, Id, Description, Score

Get started Results Query history

Summary by Copilot

AI-generated content may be incorrect. Check it for accuracy.

Observations

High-score anomalies (0.7) concentrated on August 1st; sporadic anomalies scored low.

Logon originated from Burien, United States, using IP 107.189.30.22

Anomalies includes uncommon actions, apps, and resources accessed.

Results visualization

Group by: Activity type

Events

Jul 12 Jul 22 Aug 1 Aug 11 Aug 21 Aug 31

Export

14 Results

Search

00:20:195

Filters: Add filter

Timestamp	ID	Description	Score
July 12, 2025 11:31AM	oa74db6425ebc42766...	Suspicious high volume (20) of failed login attempts (event 4625) with logon type (3-...	0.03
July 27, 2025 10:43 AM	oa23db6425erdfewb...	Suspicious high volume (6) of successful login events (event 4624) observed to device...	0.1
Aug 03, 2025 6:01 AM	a8792-25ebc4276w1b...	Action uncommonly performed by user during sign-in from Burien, US using IP 1.1.1.1.	0.7

Security Copilot

there were anomalous sign-ins by the user cloud_sync_user. Most anomalies occurred on August 1st - the day of the incident - with a spike of 6 anomalies. These had high anomalousness scores of 0.7, compared to sporadic low-score anomalies on other days. The event involved a logon from Burien, United States, using IP address 107.189.30.22

Detected behaviors included:

Action uncommonly performed by the user

App uncommonly used by the user

Resource uncommonly accessed

Uncommon high volume of actions

Country uncommonly connected from

Insights:

The IP address 107.189.30.22 used in the anomalous sign-in is associated with a public DNS service and has been observed in multiple suspicious authentication attempts globally.

See the logic behind the query

Recommended actions

Disable user 'cloud_sync_user'

Prevent further use of credentials in your organization.

Apply in Take Actions wizard

Show me all binaries executed inside these containers

Check if these containers pulled images from untrusted registries

What other actions were performed by the same user?

Ask a question about your data.

Threat Hunting Agent

AI-generated content may be incorrect

Transformation des équipes SOC à l'ère des agents IA

Avant

Spécialistes de niche

Threat hunters, intel analysts, intégrateurs d'outils

Experts SOC (L2)

Résolution d'incidents complexes hors de portée des analystes juniors

Analystes SOC (L1)

Triage manuel, investigations répétitives

Après

Strategic advisors

Anticipation des menaces, alignement de la stratégie du SOC aux risques et attentes métier

Scale optimizers

Optimisation des capacités autonomes et intelligentes, allocation des ressources

Scale operators

Gestion des équipes IA, validation des résultats, gestion de la masse

Compétence de base : analyste cyber



Announcing

Security agents in your daily workflow

Security Copilot now included for all Microsoft 365 E5 customers



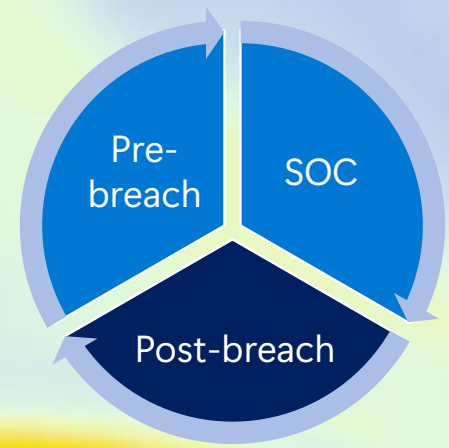
Du chaos au contrôle - Maîtriser la réponse aux incidents



Anne-Sophie Le Jouan
Cybersecurity and Cloud
Solutions Architect Director



Saad NIDIFI
Cybersecurity Cloud Solution
Architect



Définition du chaos, la Crise Cyber

Impacts



Financier



Réputation

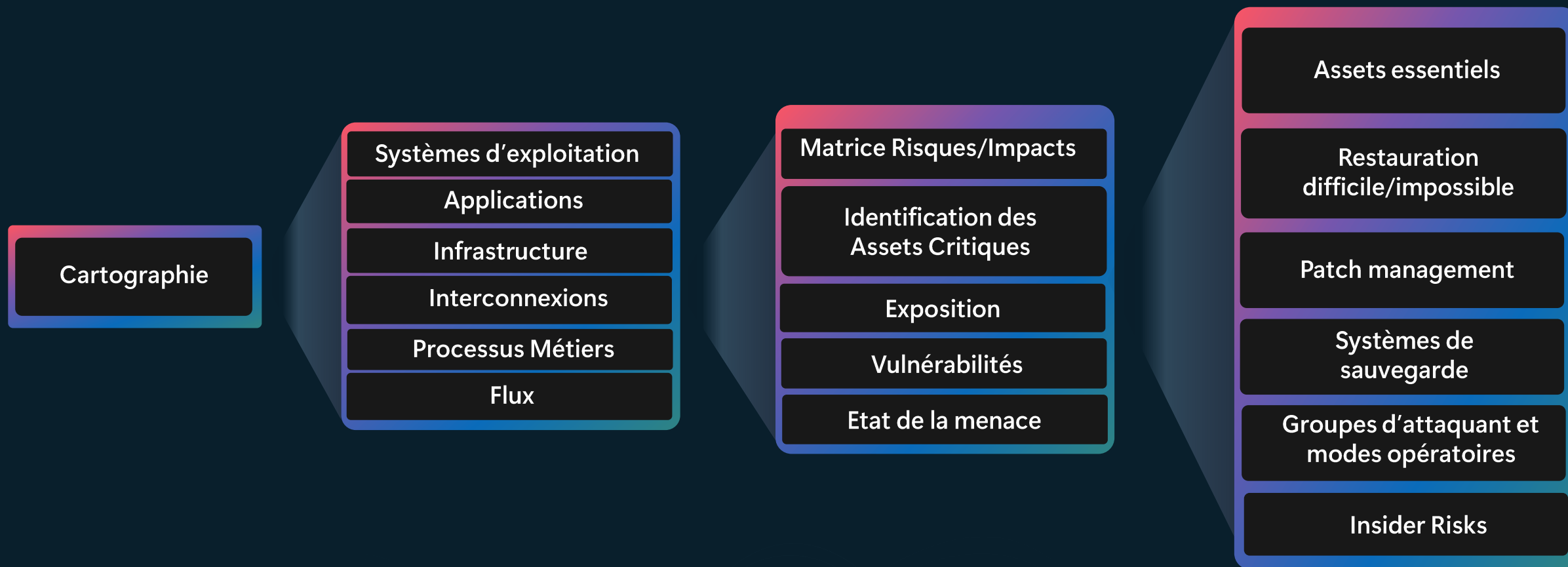


Opérationnel



Stratégique

Les bonnes pratiques à employer



La gestion de crise, les 3 piliers



Process & Communication

Plan de Reprise d'Activité (PRA)
Plan de Continuité d'Activité (PCA)



Outillage de Sécurité

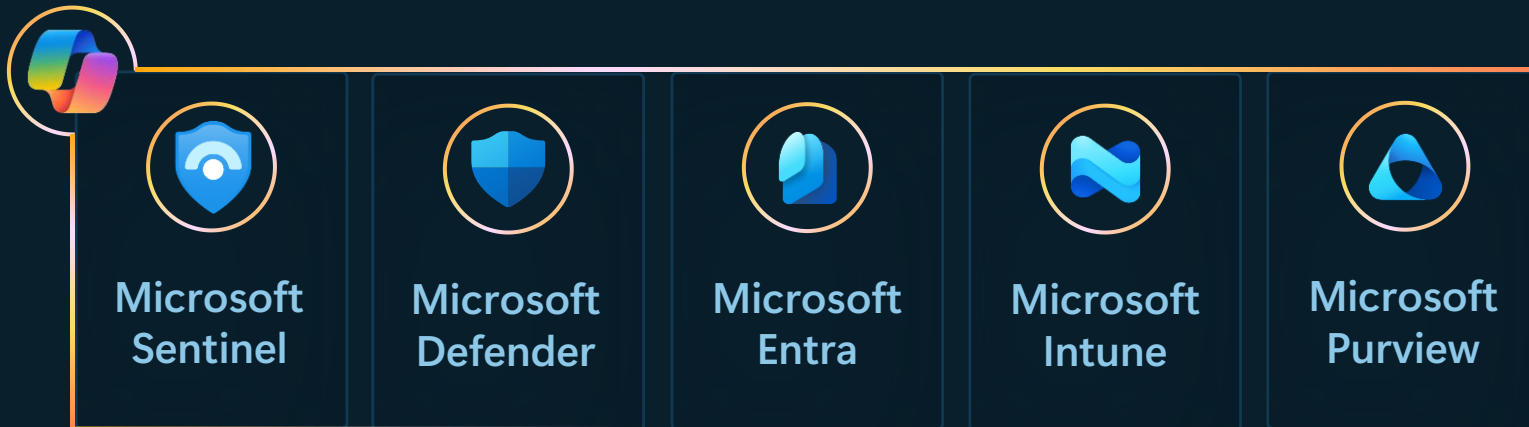
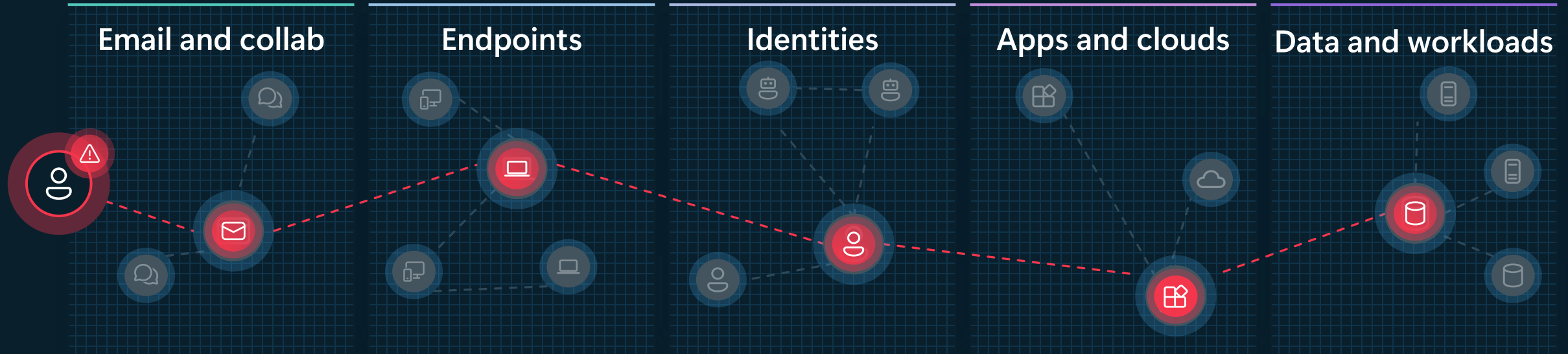
Protection des assets et données
Monitoring en temps réel



Cellule de Crise

Différents stakeholders:
CIR | IT | Executif | Métier | MSSP | Editeurs

Les attaquants pensent en Graph



...et la suite sécurité Microsoft également

L'outillage – Détecter et endiguer le chaos



Un attaquant peut utiliser plusieurs chemins d'attaque

Tout cela est rendu possible grâce à l'exploitation des signaux provenant des solutions de la plateforme Microsoft Defender.



Hybrid
identities



Endpoints
and IoT



Email and
collaboration



SaaS
apps



Data



Cloud
workloads



Non-Microsoft

L'outillage – Détecter et endiguer le chaos



L'Attack disruption peut s'adapter dynamiquement à ces derniers

Tout cela est rendu possible grâce à l'exploitation des signaux provenant des solutions de la plateforme Microsoft Defender.



Hybrid
identities



Endpoints
and IoT



Email and
collaboration



SaaS
apps



Data

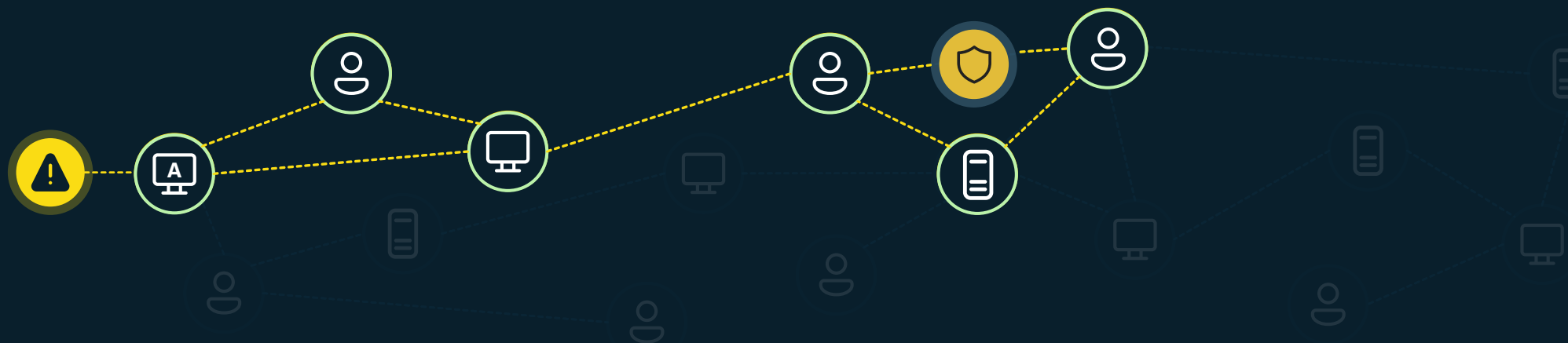


Cloud
workloads



Non-Microsoft

L'outillage – Détecter et endiguer le chaos



Le **Predictive Shielding** vient ensuite durcir les équipements susceptibles d'être touchés.

Tout cela est rendu possible grâce à l'exploitation des signaux provenant des solutions de la plateforme Microsoft Defender.



Hybrid
identities



Endpoints
and IoT



Email and
collaboration



SaaS
apps



Data



Cloud
workloads



Non-Microsoft

Comprendre le contexte et les actions

The screenshot displays the Microsoft Sentinel 'Incidents' page. A sidebar on the left contains navigation links: Home, Exposure management, Investigation & response (highlighted), Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, Cloud infrastructure, Operational technology, Security Copilot, Agents, Security Store, Cases, SOC optimization, Reports, Learning hub, Trials, More resources, and System.

The main content area is titled 'Incidents' and includes an 'Email notification' toggle. Below the title, a section 'Most recent incidents and alerts' contains three summary cards, which are circled in red and purple:

- Incidents addressed by agent:** Out of the total incidents it can handle, 102/104 in the last 30 days.
- Attack disruptions:** Automated actions stopped attacks, 8 in the last 30 days.
- Queue reduction:** Shorter and more comprehensive view, 46% in the last 30 days.

Below these cards, there are links for 'Export', 'Copy list link', and 'Refresh'. A filter bar shows 'Filter set: Save' and various filters: Status: Any, Alert severity: Any, Incident severity: Any, Service/detection sources: Any, and Tags: Critical asset. The main table lists incidents with columns for Incident name, Incident ID, Priority score, Tags, Severity, Investigation state, Categories, Impacted assets, Active alerts, and Severity. A red box highlights a specific incident row, and a purple box highlights the 'Tags' column for that row, showing tags like 'Critical asset', 'Defender Experts', 'OAuth App Abuse', 'Ransomware', 'Critical asset', 'PCI', 'Lateral Movement', 'Credential Phish', 'Escalated', 'sdf', 'BEC Fraud', 'Attack Disruption', and 'Credential Phish'.

Incident name	Incident ID	Priority score	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Severity
Compromised user account identified through att...	36932	100	Critical asset, Defender Experts +1	High	2 investigation states	Privilege escalation, Crede...	Gehad Amangeldiyewa	0/3	Def
Compromised user account used to create a malic...	36281	100	Critical asset, OAuth App Abuse +1	High	2 investigation states	Initial access, Execution, Pe...	Elvia Atkins, 6 Apps, mdc-d4ai-a	18/18	Mic
Human-operated ransomware attack was launche...	36193	100	Ransomware, Critical asset +8	High	2 investigation states	Execution, Defense evasion...	7 Devices, 7 Accounts, 3 Cloud Re	45/45	Enc
Exfiltration incident on one endpoint	36000	100	Critical asset, PCI	High		Exfiltration	win11-ash-u3968, Sam Mukeshimana	39/39	Mic
Hands-on keyboard attack was launched from a c...	36074	100	Critical asset, Lateral Movement +1	High	3 investigation states	Credential access, Discover...	2 Devices, 4 Accounts	0/21	Enc
Hands-on keyboard attack was launched from a c...	34881	100	Critical asset, Credential Phish +4	High	4 investigation states	Initial access, Execution, Cr...	RAYT-PC.zava-corp.com, 5 Accounts	0/26	Enc
Exfiltration incident on one endpoint	33707	100	Critical asset, Escalated, sdf	Medium		Exfiltration	alpiniski-u4090, Sambath Anarbaiuly	5/5	Mic
Exfiltration incident on one endpoint	33577	100	Critical asset	Medium		Exfiltration	desktop-raau95q, Sambath Anarbaiuly	20/21	Mic
User account compromise identified from a know...	31809	100	Critical asset, BEC Fraud, Attack Disruption	High	2 investigation states	Initial access, Persistence, ...	Lee Gu	8/13	Mic
Multi-stage incident involving Initial access & Lat...	31754	100	Critical asset, Credential Phish	High	2 investigation states	Initial access, Lateral move...	2 Accounts, Kerstin Krueger	0/4	Off
Multi-stage incident involving Initial access & Priv...	31421	100	Critical asset	High		Initial access, Execution, Pe...	Daisy Phillips, Daisy Phillips, 2 Apr	6/6	Mic
Hands-on keyboard attack was launched from a c...	15672	100	Critical asset, Credential Phish +4	High	4 investigation states	Initial access, Execution, Pe...	RAYT-PC.zava-corp.com, 3 Accounts	0/39	Enc
Human-operated ransomware attack was launche...	15606	100	Ransomware, Critical asset +6	High	2 investigation states	Execution, Defense evasion...	5 Devices, 2 Accounts, jump-srv-a	0/47	Enc
Multi-stage incident involving Command and con...	33355	97	Critical asset	High		Command and control, Exfi...	2 Devices, 2 Accounts	20/20	Enc
Multi-stage incident involving Privilege escalation	36537	96	Critical asset	High		Privilege escalation, Creden...	7danek Romann	2/2	Def

Tirer le plein potentiel des outils avec Security Copilot



Et mesurer la progression*



22% Plus rapide



7% Plus précis



97% Veulent réitérer son utilisation

Source : Essai contrôlé randomisé (RCT) de Microsoft Security Copilot avec des analystes de sécurité expérimentés, réalisé par le Bureau du Chief Economist de Microsoft, janvier 2024.

Interagir avec les éléments importants

Incidents > Human-operated ransomware attack was launched from a compromised asset (attack disruption)

Human-operated ransomware attack was launched from a compromised asset (attack disruption)

High

Active

Mimik Emails - AlpineSkiHouse

Ransomware

Critical asset

Credential Phish

Lateral Movement

Attack Disruption

Predictive Shielding

HumOR

+3

Attention: Attack disruption initiated multiple response actions. For more details, go to the [Activities](#) tab or visit the [Action center](#).

Incident linked to case: 1115 - Incident Investigation - 3998. [Learn more about cases](#)

Attack story

Alerts (45)

Activities

Assets (17)

Investigations (0)

Evidence and Response (82)

Recommended actions (24)

Summary

Similar incidents (2)

Alerts

Play attack story

Unpin all

Show all

Dec 2, 2025 10:09 AM

New

Suspicious invocation of a high-risk 'Defense Evasion' operation by a service principal detected (Preview)

2... 27bf9e71-106d-...

2 Clo...

Dec 2, 2025 10:18 AM

New

Compromised account conducting hands-on-keyboard attack

rayt-pc.zava-corp.com

rayt

Dec 2, 2025 10:18 AM

New

Mimikatz credential theft tool

rayt-pc.zava-corp.com

rayt

Dec 2, 2025 10:18 AM

New

Compromised account conducting hands-on-keyboard attack

rayt-pc.zava-corp.com

rayt

Dec 2, 2025 11:47 AM

New

Risk of tampering using Safe Mode reboot as part of a Ransomware attack (attack disruption)

2 Devices

2 Users

Dec 2, 2025 11:50 AM

New

Risk of tampering using Safe Mode reboot as part of a Ransomware attack (attack disruption)

2 Devices

2 Users

Dec 2, 2025 12:01 PM

New

Hands-on-keyboard attack involving multiple devices

laurenceg-pc.zava-corp...

2 Us...

Dec 2, 2025 12:04 PM

New

Potential human-operated malicious activity

jump-srv.zava-c...

Johnie McC...

Dec 2, 2025 12:05 PM

New

Report incident inaccuracy

Incident graph

Layout

Group similar nodes

The incident graph illustrates the relationships between various entities during the attack. Nodes represent assets (like rayt-pc, laurenceg-pc, jump-srv), users (like johniemcc, rayt), and processes (like powershell.exe, mimikatz.exe). Edges represent communication (solid lines) and association (dashed lines). The graph shows a complex web of interactions, with rayt-pc acting as a central hub for many activities.

Priority assessment 100

Incident details

Impacted assets

Evidence

Active alerts in this incident (45/45)

High (36) Medium (8) 2 more

View all alerts

Incident summary

Last updated: Dec 7, 2025 8:18 PM

A high severity incident, "Human-operated ransomware attack was launched from a compromised asset (attack disruption)", occurred between 2025-12-02 09:09:50 UTC and 2025-12-02 14:16:51 UTC. The incident triggered an automatic Attack Disruption action and was tagged as Credential Phish, Lateral Movement, and Ransomware. Affected users and devices include 'johniemcc', 'rayt', 'aaronb', 'laurenceg-pc', 'rayt-pc', 'lydiab-pc', 'jump-srv', and 'jump-srv-vm'.

Automated Response Actions: Automated actions included disabling and containing the user 'johniemcc' at 2025-12-02 11:30:21 UTC, containing IP 10.2.0.8, and preventing Safe Boot in the domain 'zava-corp.com'. These actions were later reversed as the threat was mitigated.

The attack began at 2025-12-02 09:09:50 UTC with a suspicious defense evasion operation from IP 91.165.169.168 (FR - France) targeting 'jump-srv-vm' and 'virtualmachines'. By 2025-12-02 09:18:30 UTC, a hands-on-keyboard attack was underway, with the compromised account 'johniemcc' and the use of credential theft tools such as mimikatz.exe and powershell.exe (PID: 11040) on rayt-pc (high exposure and risk). Multiple credential access attempts were observed, including the execution of mimikatz.exe, modification of LSASS memory, and attempts to access Primary Refresh Tokens, primarily on rayt-pc.

Between 2025-12-02 10:47:53 UTC and 2025-12-02 11:28:40 UTC, ransomware activity escalated. Files with extensions like .lockbit appeared on laurenceg-pc, lydiab-pc (high exposure and risk), and jump-srv (medium exposure, high risk). Attackers tampered with system recovery settings using vssadmin.exe (PID: 14064) and bcdedit.exe (PID: 12944), and leveraged WMI and PsExec for lateral movement. Multiple suspicious logons and remote sessions were recorded, including successful logons by 'johniemcc' and 'rayt' on various devices.

The attack was characterized by repeated use of credential theft, lateral movement, and ransomware deployment across several high-risk endpoints, with automated disruption actions helping to contain the spread.

See less

See prompts

Accélérer la compréhension et la prise de décision



Triage

New Copilot

Contact user [sba491@zava-private.com](#) on Teams, and ask them to confirm their activity Hi.

We noticed that on July 17, 2025 at 08:23 UTC, an email with the subject "Results on the email you

[See more](#)

[Contact user in Teams](#) [View user](#)

AI-generated content may be incorrect. Check it for accuracy.

Completed Phishing Triage Agent

Classify phishing email attempt as 'False positive' and resolve alert ID [faaf453cde-816d-db9f-42ad-08ddc50b2fb5](#)

The investigation concludes that the email is Non-Malicious because multiple tools confirmed its legitimacy. The email was identified as a genuine notification from a security service, with

[See more](#)

[Change classification](#) [View agent activity](#)

AI-generated content may be incorrect. Check it for accuracy.

Contain

New Copilot

Isolate device [jump-srv.zava-corp.com](#)

Other organizations tend to take this action for similar incidents.

[Isolate device](#) [View device](#)

AI-generated content may be incorrect. Check it for accuracy.

New Copilot

Isolate device [rayt-pc.zava-corp.com](#)

Other organizations tend to take this action for similar incidents.

[Isolate device](#) [View device](#)

AI-generated content may be incorrect. Check it for accuracy.

New Copilot

Isolate device [laurenceg-pc.zava-corp.com](#)

Other organizations tend to take this action for similar incidents.

[Isolate device](#) [View device](#)

AI-generated content may be incorrect. Check it for accuracy.

Remediate

Phishing Incident response playbook

View phishing investigation and response recommended steps for this incident

[Open phishing playbook](#)

Ransomware Incident response playbook

View ransomware investigation and response recommended steps for this incident

[Open ransomware playbook](#)

Resolve and export incident

Resolve the incident and export the incident to a PDF to ensure comprehensive documentation.

[Resolve and Export incident as PDF](#)

Tasks

Summary

Copilot

Incident summary

Last updated: Dec 7, 2025 8:18 PM

A high severity incident, "Human-operated ransomware attack was launched from a compromised asset (attack disruption)", occurred between 2025-12-02 09:09:50 UTC and 2025-12-02 14:16:51 UTC. The incident triggered an automatic Attack Disruption action and was tagged as Credential Phish, Lateral Movement, and Ransomware. Affected users and devices include 'johniemcc', 'rayt', 'aaronb', 'laurenceg-pc', 'rayt-pc', 'lydiab-pc', 'jump-srv', and 'jump-srv-vm'.

Automated Response Actions: Automated actions included disabling and containing the user 'johniemcc' at 2025-12-02 11:30:21 UTC, containing IP 10.2.0.8, and preventing Safe Boot in the domain 'zava-corp.com'. These actions were later reversed as the threat was mitigated.

The attack began at 2025-12-02 09:09:50 UTC with a suspicious defense evasion operation from IP 91.165.169.168 (FR - France) targeting 'jump-srv-vm' and 'virtualmachines'. By 2025-12-02 09:18:30 UTC, a hands-on-keyboard attack was underway, with the compromised account 'johniemcc' and the use of credential theft tools such as `mimikatz.exe` and `powershell.exe` (PID: 11040) on `rayt-pc` (high exposure and risk). Multiple credential access attempts were observed, including the execution of `mimikatz.exe`, modification of LSASS memory, and attempts to access Primary Refresh Tokens, primarily on `rayt-pc`.

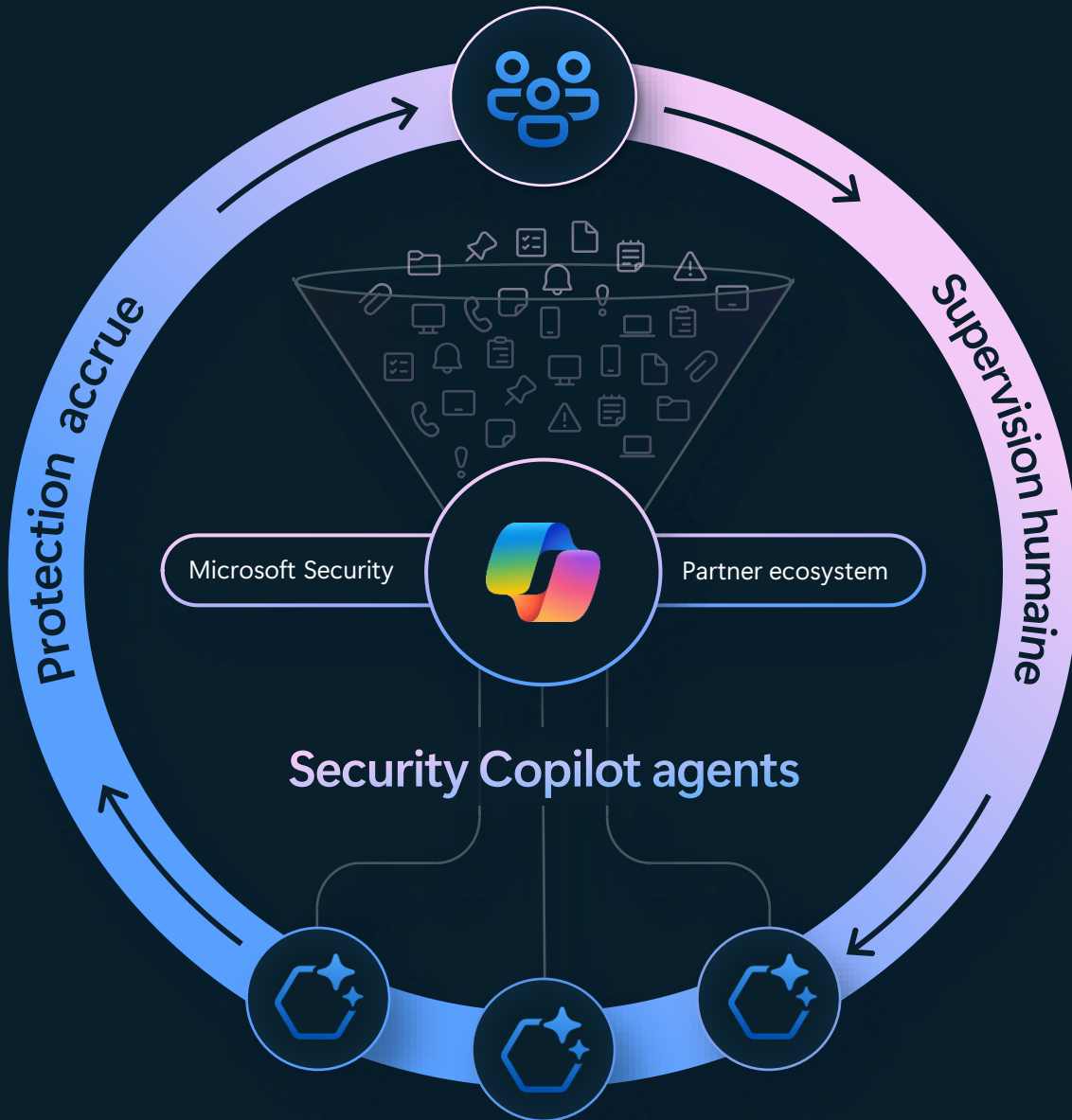
Between 2025-12-02 10:47:53 UTC and 2025-12-02 11:28:40 UTC, ransomware activity escalated. Files with extensions like `.lockbit` appeared on `laurenceg-pc`, `lydiab-pc` (high exposure and risk), and `jump-srv` (medium exposure, high risk). Attackers tampered with system recovery settings using `vsadmin.exe` (PID: 14064) and `bcdedit.exe` (PID: 12944), and leveraged WMI and PsExec for lateral movement. Multiple suspicious logons and remote sessions were recorded, including successful logons by 'johniemcc' and 'rayt' on various devices.

The attack was characterized by repeated use of credential theft, lateral movement, and ransomware deployment across several high-risk endpoints, with automated disruption actions helping to contain the spread.

[See less](#)

[See prompts](#)

Défense intelligente avec Security Copilot Agents



Microsoft & Partner ecosystem*



Phishing Triage



SOC Analyzer



Data Leak Agent



Attack Mapping Agent



Threat Intelligence Briefing Agent



Domain Spoofing



L1 SOC Triage Agent



Ransomware Kill Chain



Threat Intelligence Briefing



Forensic Agent

*Liste non exhaustive et extraite du Security Store, toujours en cours d'évolution

Microsoft, Intelligence-Driven Investigations

820K

Entreprises protégées dans
190 pays

100T

Signaux de sécurité
traités par jour

1,500+

Groupes
d'attaquants

30M

IOCs
traités par jour

34,000

Dedicated Security Professionals

\$20B

Investment in security
over 5 years

AI powered
predictions

L'Offre CIR - Aider client et partenaire à rétablir le calme

Services Proactifs

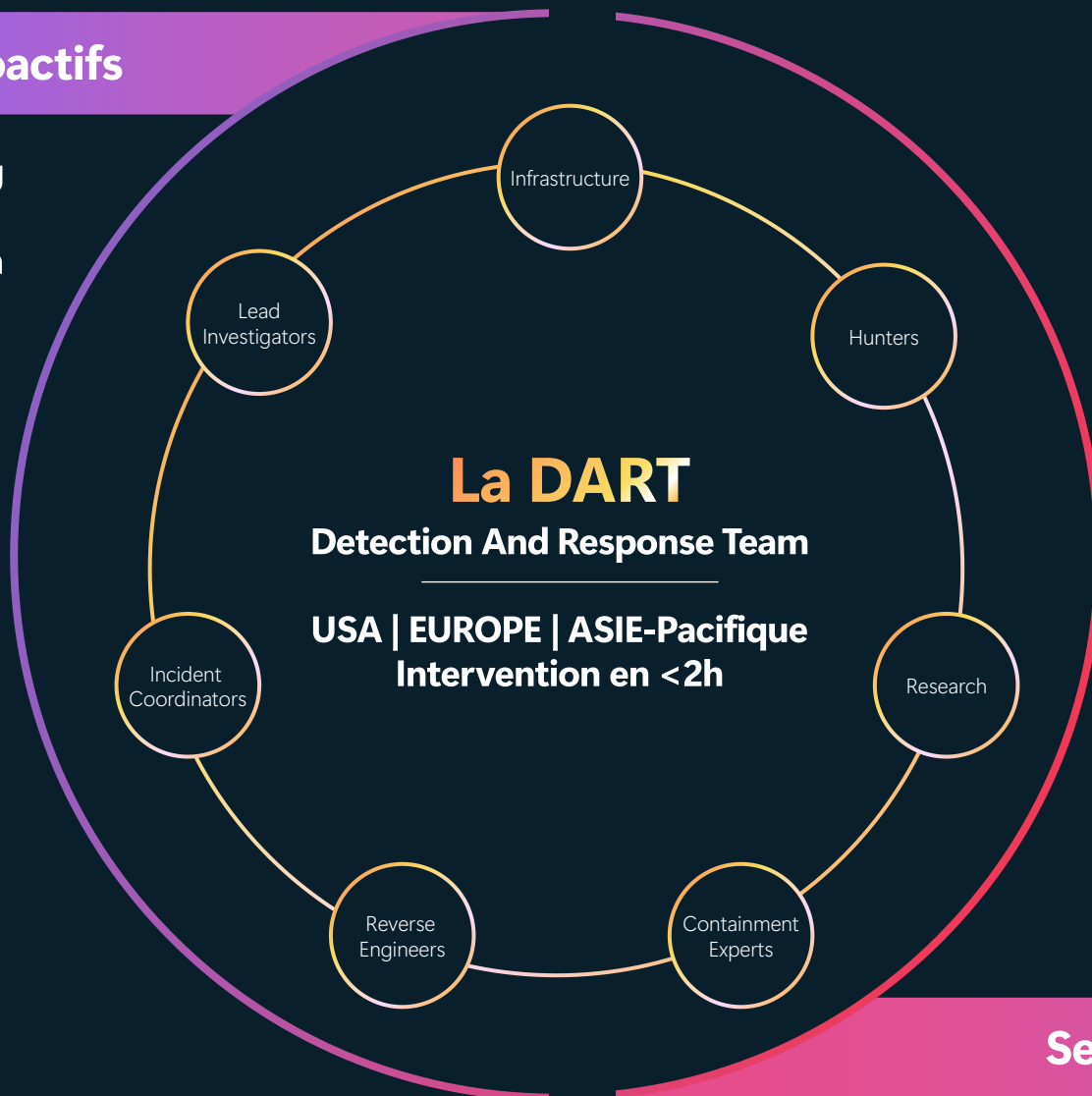
Threat intel Briefing

Evaluation de compromission

Evaluation d'architecture:
Zero Trust | Resilience

Validation du plan
de réponse à Incident

Tabletops



Deep Expertise

Travail en collaboration
avec les cyberassureurs

Intervention coordonnée
avec les partenaires

Services Reactifs

L'objectif CIR - la maîtrise de la menace et de sa posture



Threat Hunting et Investigation

Analyse de Root-Cause
—
Compromissions latentes
—
Reverse Engineering
—
Vulnérabilités



Reprise d'activité

Isolation et éradication
—
Reconstruction des systèmes
—
Validation d'intégrité



Maturité sur la posture de sécurité

Modèle de Tiering
—
Architecture Zero Trust
—
identités AD et Entra ID
—
Policies et Controle Plane



Amélioration Continue

Vulnerability Baseline Design
—
System Hardening

Rapports détaillés

L'Offre CIR - Aider client et partenaire à rétablir le calme

Scenario	Contrat Unified	Service CIR
Réponse à Incidents 24x7	✓	✓
Compte-rendu d'investigation incluant les découvertes et recommandations	✓	✓
Threat Hunting proactif		✓
Investigations environnement Cloud (Azure and M365)	✓	✓
Investigations On-premise et Linux		✓
Reverse Engineering des fichiers suspects		✓
Isolation & Durcissement Tier 0		✓
AD/Entra ID Recovery post compromission	Partiel	✓

10 000 employés et 5 000 agents IA - Sécuriser l'identité à l'ère de l'IA



Franck Heilmann
Senior Product Manager



Christophe Guerre
Cloud Solution Architect

Paysage du marché des agents IA

110 M en 2025

1.3 Milliard

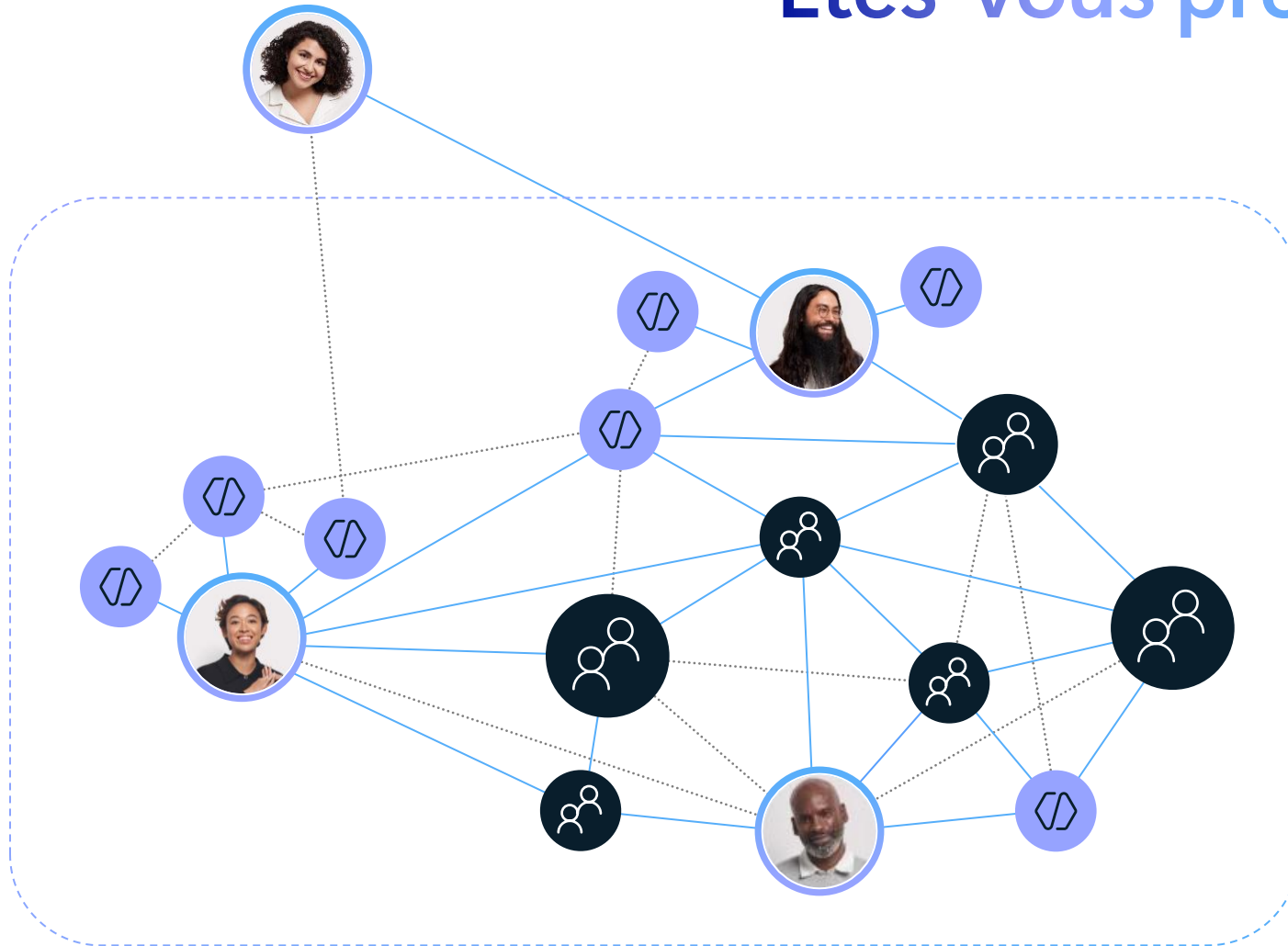
d'agents IA d'ici 2028

2025

2028

Source : IDC Info Snapshot, 1,3 milliard d'agents IA d'ici 2028, doc #US53361825, mai 2025

Les agents sont déjà là ! Êtes-vous prêt?



Comment puis-je obtenir de la **visibilité** sur la prolifération des agents dans mon environnement?

Quels **droits d'accès** et privilèges chaque agent devrait-il avoir ?

Puis-je **retracer et auditer** les actions effectuées par chaque agent ?

Comment **prévenir les attaques** et protéger les agents de mon organisation ?

Types d'agents

Agent d'assistance

Tâches uniques, spécifiques, définies et répétitives

« *Résume cet e-mail.* »

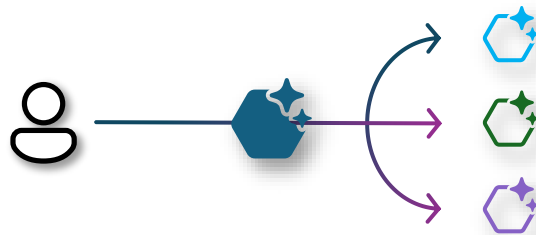
« Résume-moi cette conversation »



Agit à la demande de l'utilisateur et en son nom

Agent autonome

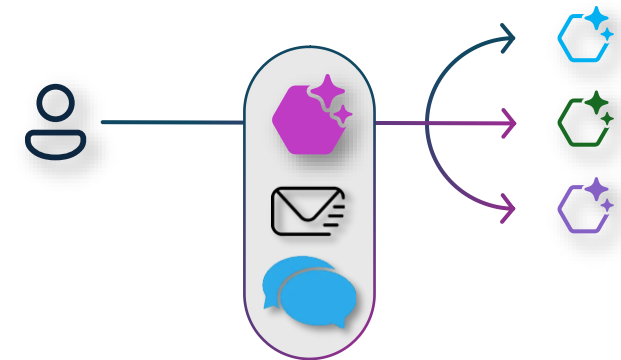
Complexe, orienté vers des objectifs.
Élabore des plans pour atteindre les résultats



Coordonne les actions en son nom propre et selon un planning défini

Collègue numérique

Axé sur l'apprentissage
Imite la prise de décision humaine

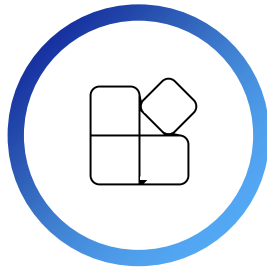


Fourni ses propres accès et ressources ;
atteint les objectifs en son nom propre et son propre calendrier

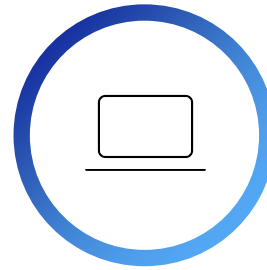
Les agents sont un nouveau type d'identité



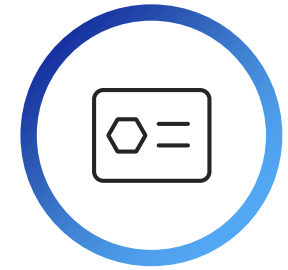
Utilisateur



Appli



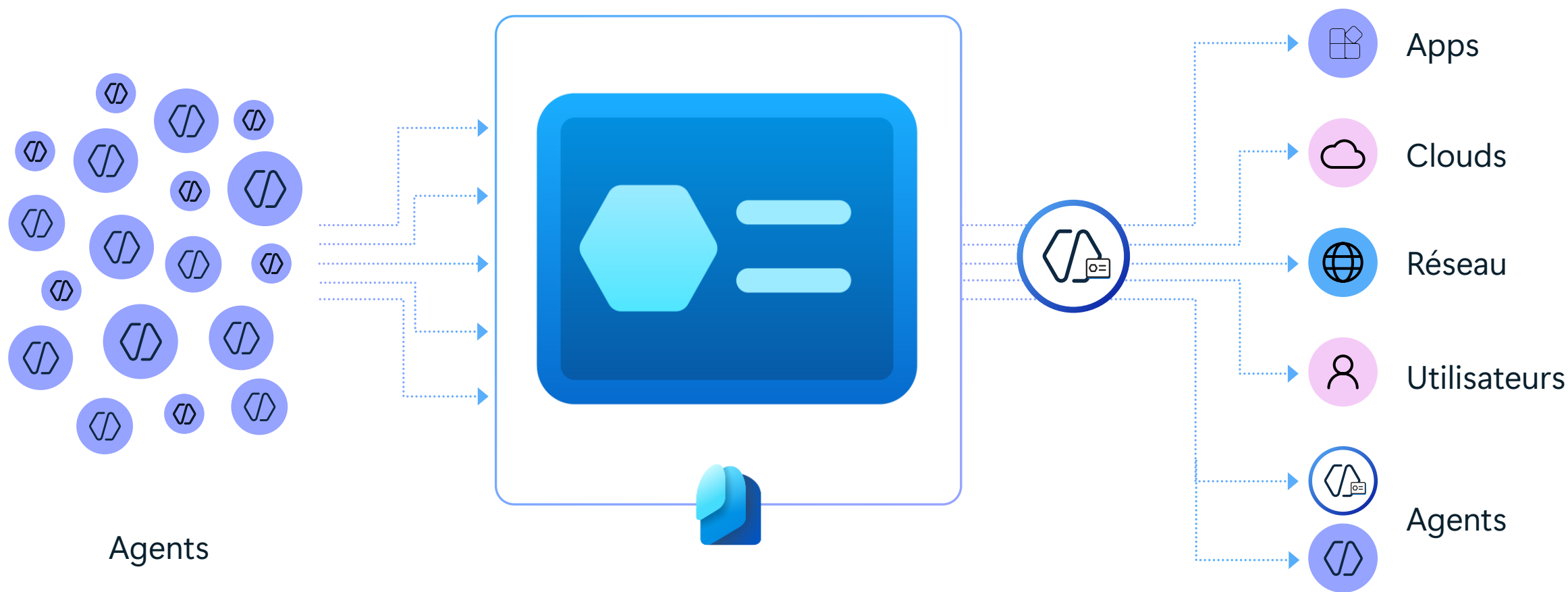
Appareil



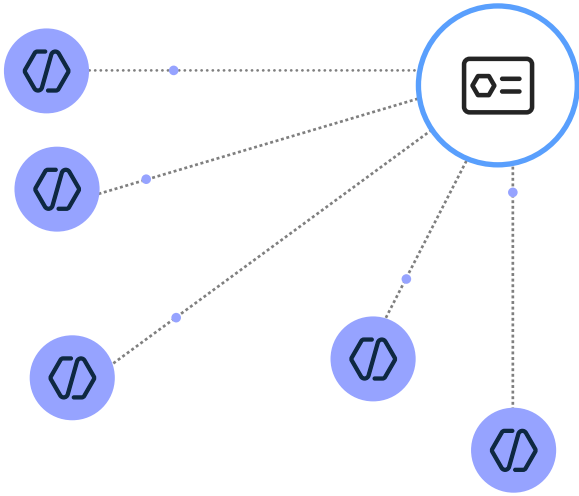
Agent

Microsoft Entra Agent ID

Sécuriser l'accès pour les agents IA – **tout comme vous le feriez pour des employés** – grâce à **une gestion, une protection et une gouvernance d'accès de niveau entreprise des identités des agents.**



Microsoft Entra Agent ID



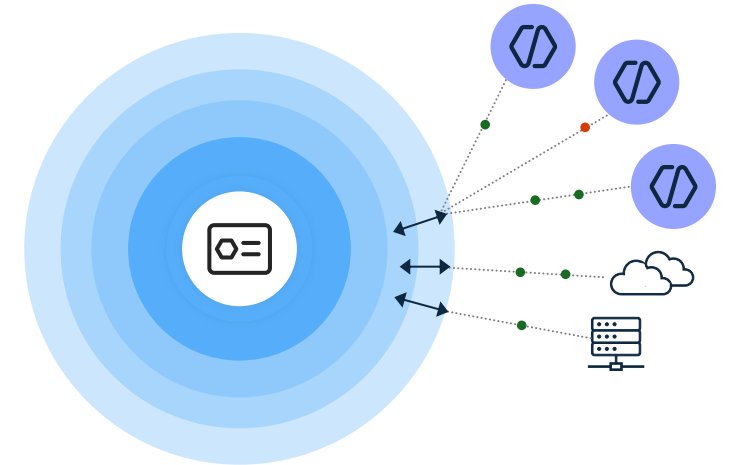
Enregistrer

et gérer les agents d'IA



Gouverner

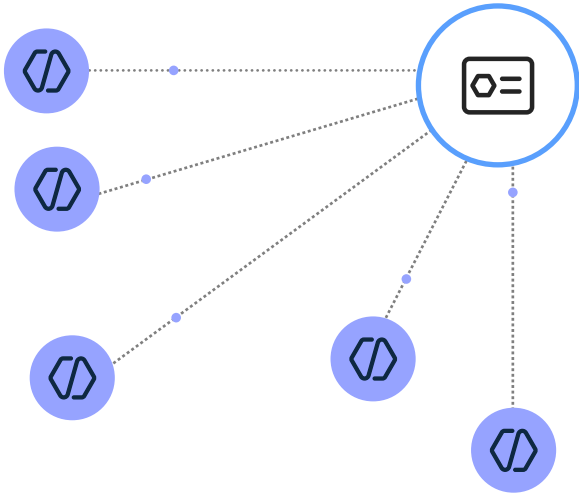
Identités des agents et cycle de vie



Protéger

Accès des agents aux ressources

Microsoft Entra Agent ID



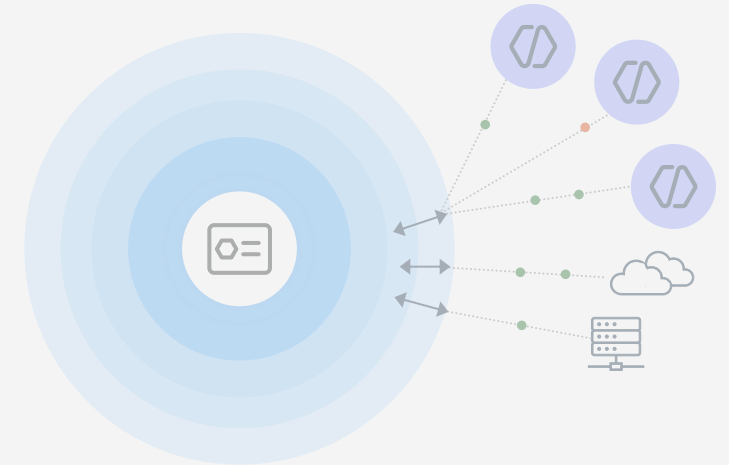
Enregistrer

et gérer les agents d'IA



Gouverner

Identités des agents et cycle de vie

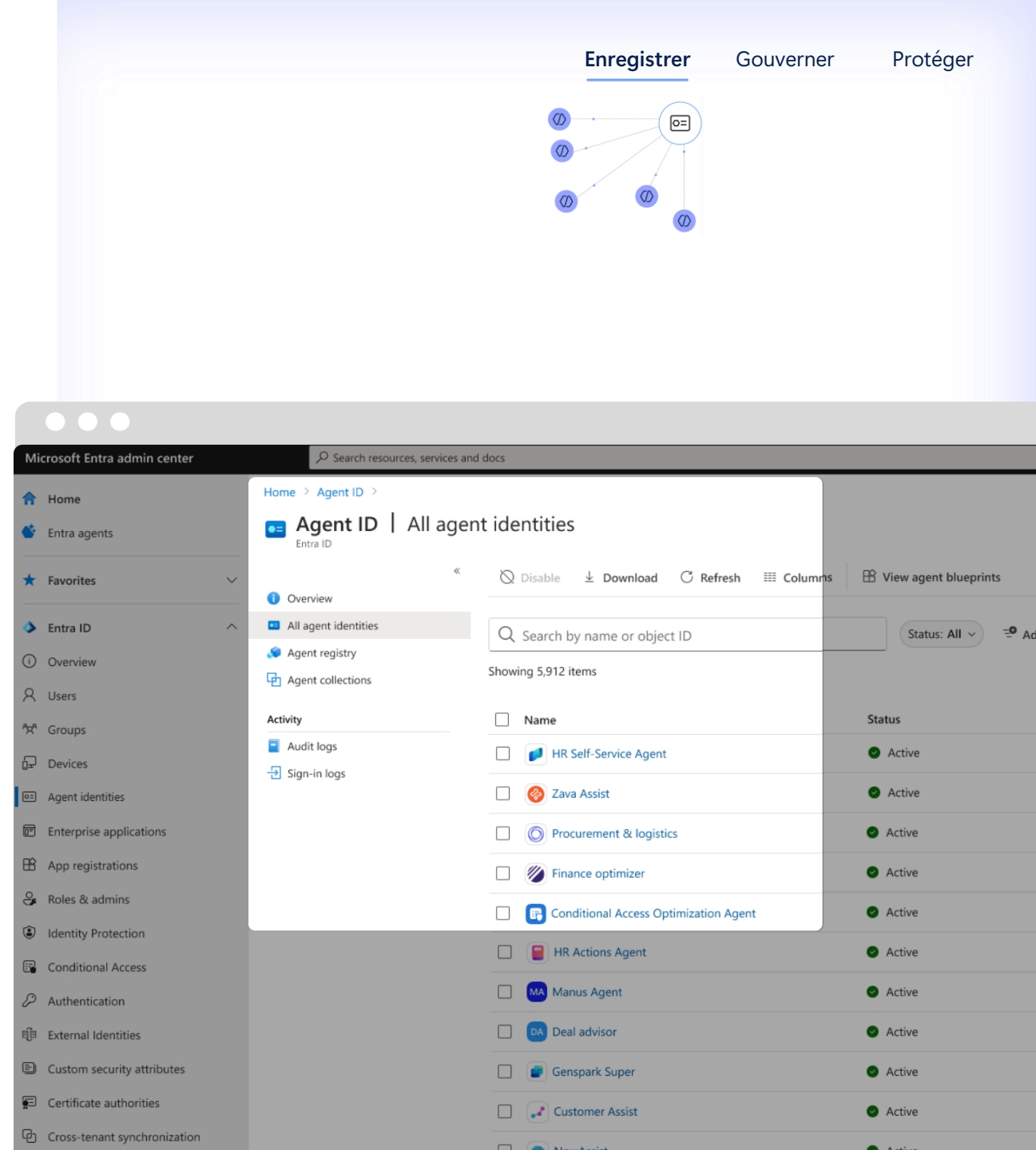


Protéger

Accès des agents aux ressources

Entra Agent ID

- Fournir une Identité adaptée à **tous les type d'agents**
- Garantir que les identités des agents IA sont **traçables, authentifiés, autorisés et sécurisés**
- Facilite l'intégration et la sécurisation d'agents grâce **aux APIs et SDKs**, quelque soit la plateforme .



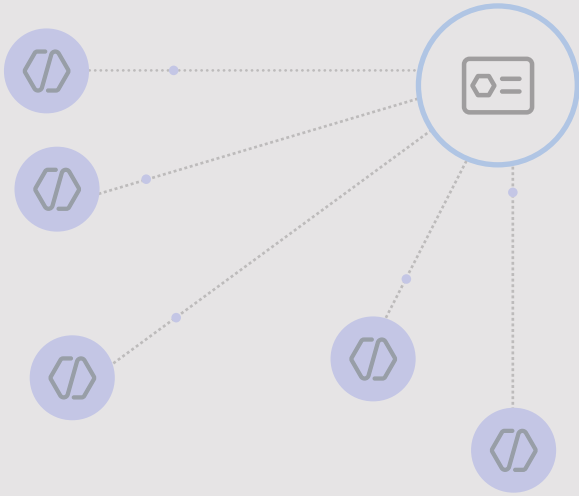
Entra Agent Registry

- Cataloguer les agents dans un **registre global**
- Sécuriser la **découverte et la communication** entre Agents
- Grouper et sécuriser la découverte de vos agents en utilisant les **collections d'agents**.

The screenshot shows the Microsoft Entra admin center interface. The top navigation bar includes 'Enregistrer', 'Gouverner', and 'Protéger'. The left sidebar shows the navigation menu with 'Agent ID' selected. The main content area displays the 'Agent ID | Agent registry' page. The page includes a search bar, a refresh button, and a table of agents.

Name	Registry ID	Platform
Image Recognition Agent	jpg5qtp-hr5o-iq9s-me2r-le4t2n4p6...	PixelNova AI
Inventory Management Agent	58b744c1-e3b9-4205-8016-dbc9194...	Adatum
Procurement & logistics	microsoftCopilotStudio_055beb02-87...	Copilot Studio
Content Generation Agent	10314218-d641-48aa-aa2c-e9e2ea6a...	BrightMind Systems
HR Actions	microsoftAzureFoundry_088beb02-8...	Microsoft Foundry
Deal advisor	microsoftCopilotStudio_055beb02-87...	Copilot Studio
Conditional Access Optimization Agent	becef3a5-8a8b-4b6b-87b5-bace1fb5...	Security Copilot
Manus	0a52a0fb-5b3b-4ebc-b231-5cc98f7b...	Manus AI
HR self-service	microsoftCopilotStudio_055beb02-87...	Copilot Studio
Finance optimizer	microsoftCopilotStudio_055beb02-87...	Copilot Studio

Microsoft Entra Agent ID



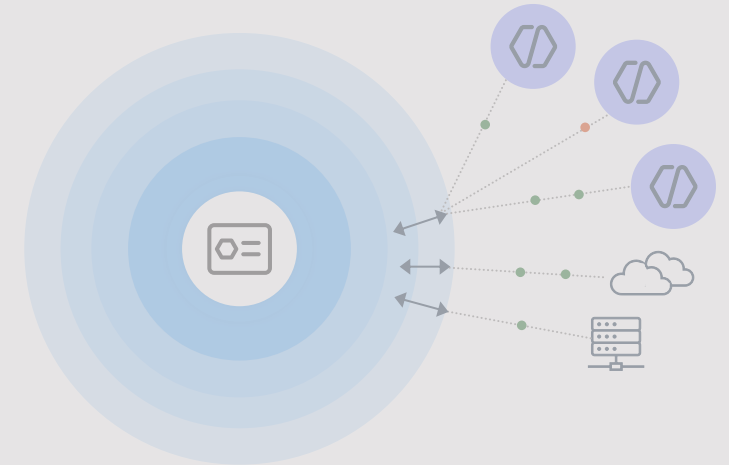
Enregistrer

et gérer les agents d'IA



Gouverner

Identités des agents et cycle de vie



Protéger

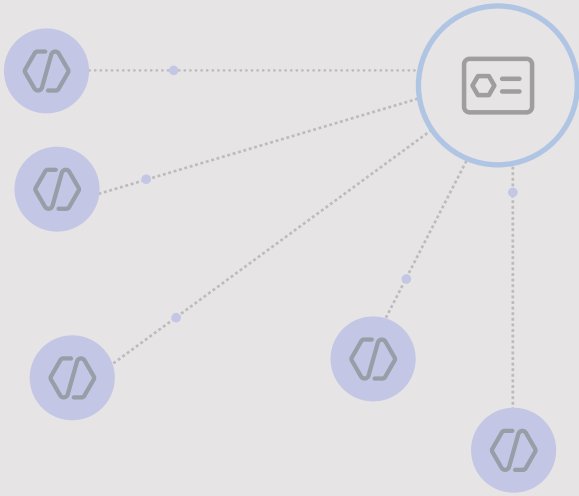
Accès des agents aux ressources

Gouverner l'identité des agents et leur cycle de vie

- Attribuer des **sponsors** à chaque Identité d'agent pour les maintenir sous surveillance humaine.
- Gérer le **cycle de vie de l'agent**, de la création à la désactivation, à grande échelle.
- Imposer le « **moindre privilège** » avec les Packages d'accès pour agents.



Microsoft Entra Agent ID



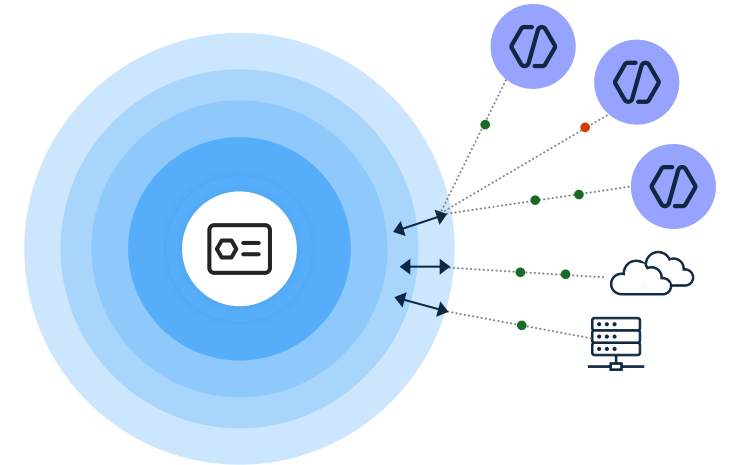
Enregistrer

et gérer les agents d'IA



Gouverner

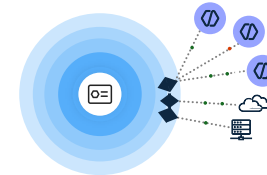
Identités des agents et cycle de vie



Protéger

Accès des agents aux ressources

Protéger l'accès des agents aux ressources



Signaux de risque

Accès aux ressources non familières

Pic de connexion

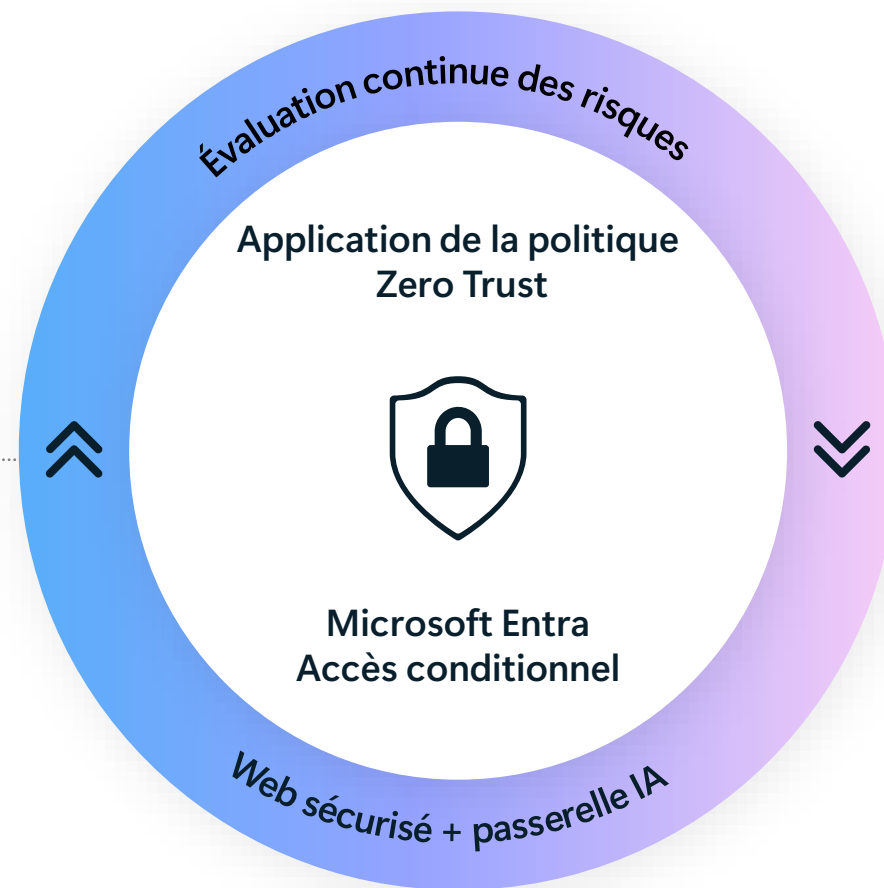
Tentative d'accès ratée

Connexion par un utilisateur à risque

Attributs de sécurité personnalisés



Agents IA



Bloquer



IaaS · PaaS · Datacenter



Agents IA



Internet · Microsoft 365 · SaaS



On-premises

Microsoft Entra Agent ID... Accès sécurisé pour les agents IA



Enregistrer et intégrer les agents avec aisance



Gouverner l'identité des agents et leurs cycles de vie



Protéger l'accès des agents aux ressources



Copilot Studio



Microsoft Foundry



Copilot Security



Microsoft 365 Copilot



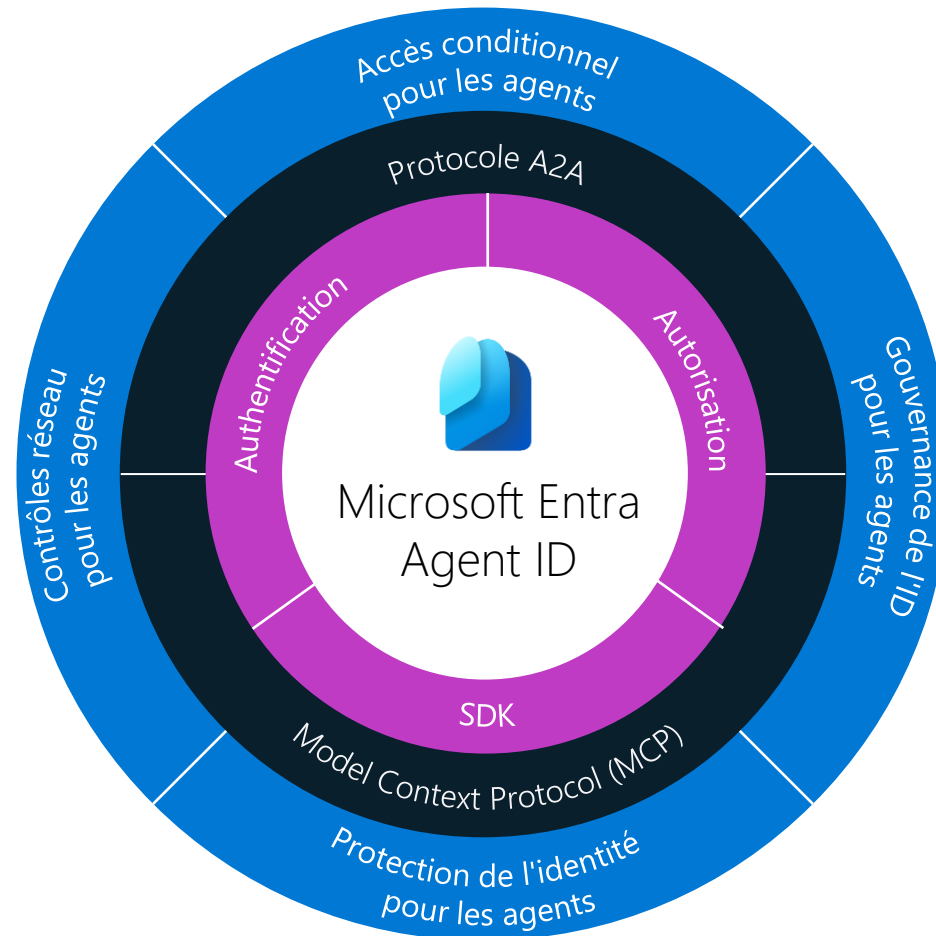
Teams



LinkedIn

SDK + APIs

aka.ms/entra/sdk/agentid



workday

servicenow

Ignite 2025
Public Preview

Commencez avec Microsoft Entra Agent ID

Visiter notre site
web



Liser notre
documentation



Essayer
maintenant



Thank you

Microsoft Security Summit Survey

