

• UXPA 2026

TRUST, AUTONOMY, AND THE WORK THAT'S MOVING BEHIND THE SCREEN

Designing *Trust* in AI Systems

PRESENTED BY

Mary Gansallo

”

Think about a system that you *trust* today.

I'm *Mary Gansallo.*

Senior Product Designer, Microsoft

*Designing AI-powered experiences within Microsoft Entra,
a suite of identity and security products.*



My Journey *snippets*

Full-stack engineer

Built software in the consulting world.

Design bootcamp

Back home, I made the craft switch official.

Product Designer

Designing trust into AI-powered security.

Computer Science

Studied C.S., Minor in global terrorism at UMD.

HCI, in Barcelona

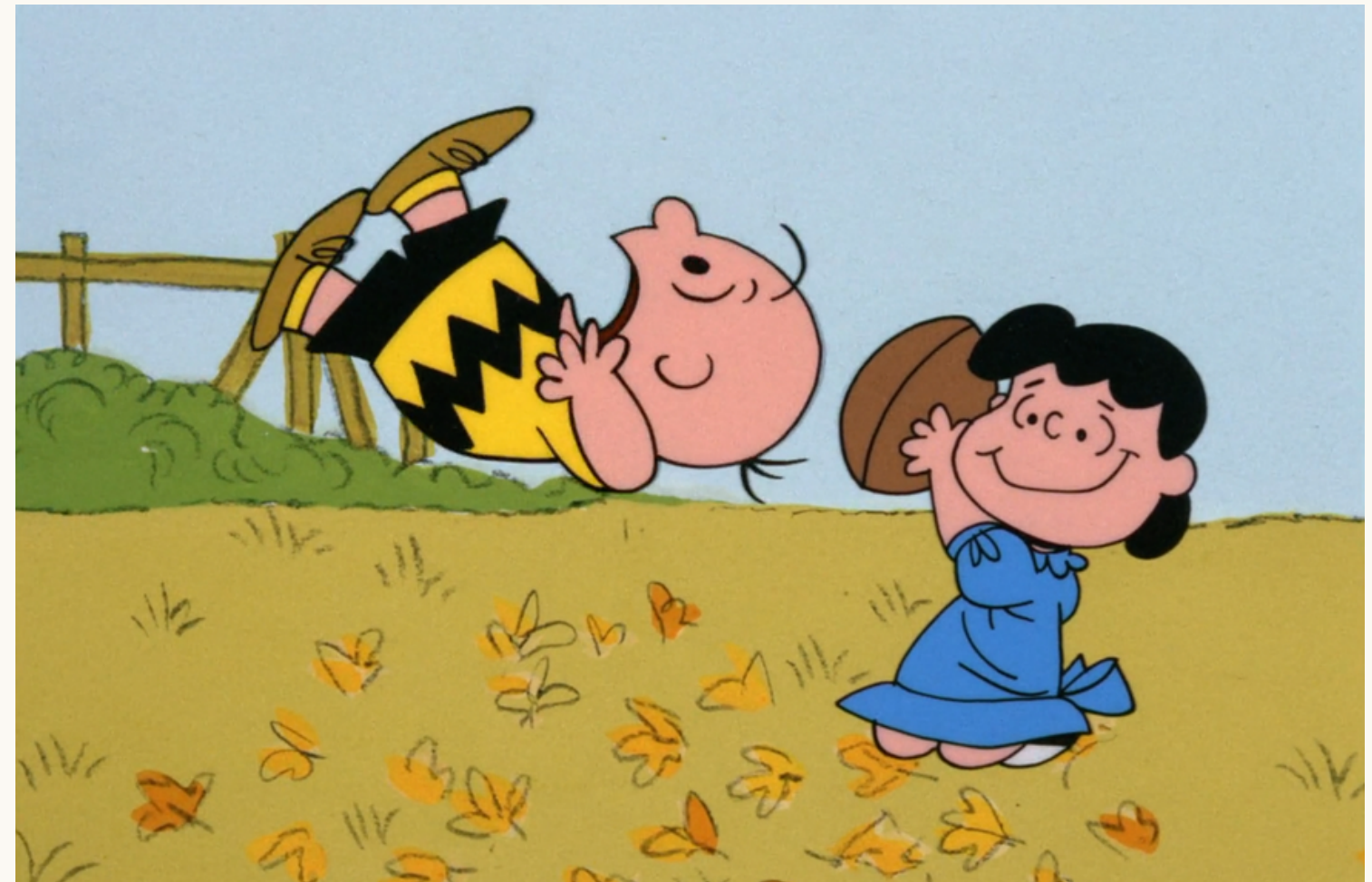
Moved abroad for a year for my Master's.

Microsoft · UX Engineer

Code + design in one seat across teams.

What is trust?

Trust is the willingness to rely on someone, something, or a system when the outcome matters and there is risk involved.



Every act of trust is composed of three things



Reliance



Risk



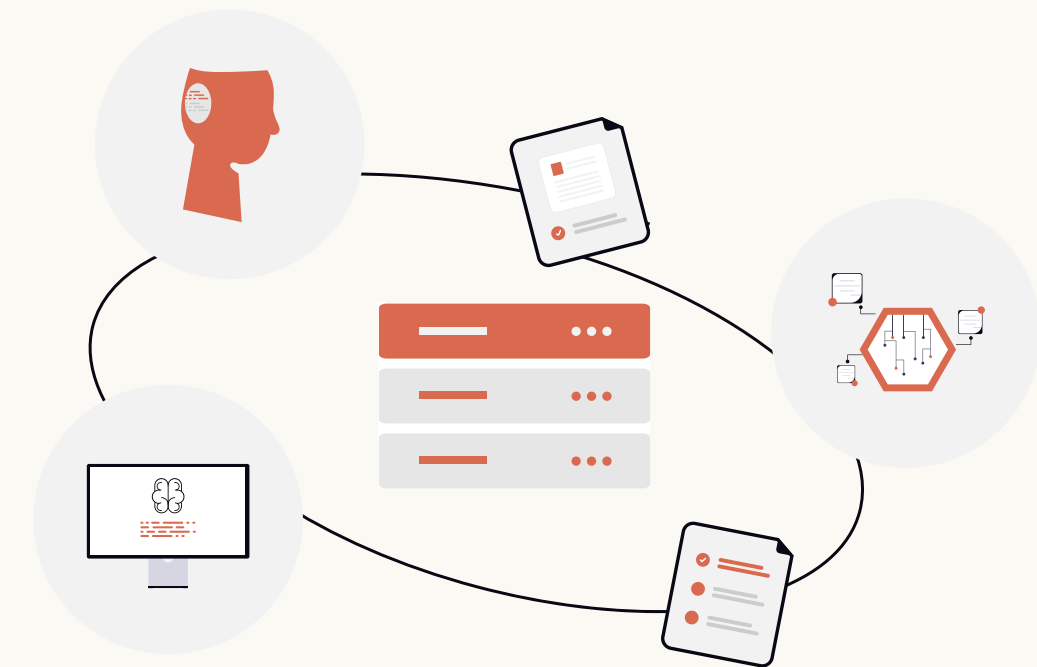
Vulnerability

Defining the AI Partner

Generative AI systems, AI assistants and copilots, Human-AI decision making, Enterprise AI experiences

AI systems are software that can generate, reason, predict, recommend, or act based on patterns learned from **data**.

Unlike traditional software, modern AI operates as a probabilistic reasoning engine, creating outcomes that are inherently dynamic and unpredictable.



78%

Organizations using AI

35–40%

Users trust AI decisions

Adoption is growing faster than trust.

Organizations are rapidly integrating AI into products, workflows, and decision-making. AI is no longer an emerging technology. It's becoming a core part of how work gets done.

SOURCE: MCKINSEY GLOBAL SURVEY ON AI (2025)

The goal isn't total trust, it's appropriate trust.

Successful AI systems don't maximize trust. They help users understand when to trust, when to verify, and when to intervene. Trust should be earned through evidence, transparency, and control.



Trustworthy experiences start with trustworthy systems

Microsoft's Responsible AI principles define what trustworthy systems should do. UX patterns determine whether users experience them as trustworthy.

Reliability & safety

Can users predict and safely manage impact?

Transparency

Can users understand what's happening?

Accountability

Who remains responsible for outcomes?

Meet Maya

Maya Patel
"The Guardian"

Senior IT Administrator

Identity & Security

Global Enterprise (50,000 employees)



About Maya

Maya is an IT administrator responsible for protecting access across thousands of employees, applications, and devices. She needs AI she can understand, trust, and control.

Goals

- Keep the organization secure
- Reduce administrative burden
- Respond quickly to security incidents

Challenges

- Too many alerts
- Limited time
- Fear of unintended impact

Key Motivation

"I need to move faster without losing control."

Admin portal entry

USERS STARTS THEIR DAY WITH HUNDREDS OF SIGNALS
COMPETING FOR ATTENTION.

Microsoft Entra admin center

Search resources, services and docs

Copilot

Connie Wilson
CONTOSO

Home

Security Copilot

Dashboard

Chat

Projects

Agent library

Favorites

Entra ID

ID Protection

ID governance

Verified ID

Global Secure Access

Permissions Management

What's new

Billing

Diagnose & solve problems

New support request

New project

Welcome back, Maya

Needs your attention (3)

View all activity

25 users impacted by an anomalous spike in MFA sign-in failures

High severity

Last updated: 2/16/26, 12:10 PM

Anomalous spikes may indicate an MFA service disruption, brute-force attacks, or misconfigured Conditional Access policies that require immediate review. Review sign-in activity and MFA policy health.

Y-axis title

100K

80K

60K

40K

20K

0

Feb 1

Feb 2

Feb 3

Feb 4

Feb 5

Feb 6

Feb 7

Day

View sign-in logs

Review with Copilot

54 admin users don't have MFA set up

Last updated: 2/16/26, 12:10 PM

Require MFA for admin roles. Review affected users to complete registration.

Resource	Status	First detected
adelev@woodgrove.ms	Active	Apr 15, 2025, 4:17 AM
johnw@woodgrove.ms	Active	May 10, 2025, 5:28 PM...
ronhd@woodgrove.ms	Active	May 17, 2025, 2:24 PM

Showing 3 of 54 impacted resources

View all

Review users

Review with Copilot

Recommendations (5)

2 of 54 admin users don't have MFA set up

Last updated: 2/16/26, 12:10 PM

Require MFA for admin roles. Review affected users to complete registration.

Resource	Status	First detected
adelev@woodgrove.ms	Active	Apr 15, 2025, 4:17 AM
johnw@woodgrove.ms	Active	May 10, 2025, 5:28 PM...

433 of 2503 users don't have MFA set up

Last updated: 2/16/26, 12:10 PM

Require MFA for these users. Review affected users to complete registration.

Resource	Status	First detected
adelev@woodgrove.ms	Active	Apr 15, 2025, 4:17 AM
johnw@woodgrove.ms	Active	May 10, 2025, 5:28 PM...

Reliability & Safety

USERS NOW VIEW A PREVIEW OF AN AI GENERATED SUMMARY OF ALL THE SIGNAL AND NOISE IN THEIR ENVIROMENT.

Microsoft Entra admin center

Search resources, services and docs

Copilot

Connie Wilson
CONTOSO

Home

Security Copilot

Dashboard

Chat

Projects

Agent library

Favorites

Entra ID

ID Protection

ID governance

Verified ID

Global Secure Access

Permissions Management

What's new

Billing

Diagnose & solve problems

New support request

New project

Welcome back, Maya

Copilot summary

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

Unusual spike detected in sign-ins were detected +64% in the last hour. Recommendation: Block IP range via Named Locations + Conditional Access. Lorem ipsum dolor

Needs your attention (3)

View all activity

25 users impacted by an anomalous spike in MFA sign-in failures

High severity

Last updated: 2/16/26, 12:10 PM

Anomalous spikes may indicate an MFA service disruption, brute-force attacks, or misconfigured Conditional Access policies that require immediate review. Review sign-in activity and MFA policy health.

Y-axis title

100K

80K

60K

40K

20K

0

Feb 1

Feb 2

Feb 3

Feb 4

Feb 5

Feb 6

Feb 7

Day

View sign-in logs

Review with Copilot

54 admin users don't have MFA set up

Last updated: 2/16/26, 12:10 PM

Require MFA for admin roles. Review affected users to complete registration.

Resource	Status	First detected
adelev@woodgrove.ms	Active	Apr 15, 2025, 4:17 AM
johnw@woodgrove.ms	Active	May 10, 2025, 5:28 PM...
ronhd@woodgrove.ms	Active	May 17, 2025, 2:24 PM

Showing 3 of 54 impacted resources

View all

Review users

Review with Copilot

Recommendations (5)

2 of 54 admin users don't have MFA set up

Last updated: 2/16/26, 12:10 PM

Require MFA for admin roles. Review affected users to complete registration.

433 of 2503 users don't have MFA set up

Last updated: 2/16/26, 12:10 PM

Require MFA for these users. Review affected users to complete registration.

Resource	Status	First detected
----------	--------	----------------

Confidence signals

USERS GAIN CONFIDENCE WHEN THE SYSTEM DEMONSTRATES IT CAN SEPARATE SIGNAL FROM NOISE, ACCURATELY AND CORRECTLY.

Welcome back, Maya

 **Copilot summary**

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

Last updated: 3 hours ago

I've been monitoring your tenant activity. **An unusual spike detected in sign-ins were detected +64% in the last hour. I recommend blocking the IP range and strengthening Conditional Access policies to reduce risk.** Over the last 24 hours, I've identified **1 critical issue** and **1 medium-severity item** requiring your attention, and resolved **3 low-severity items** automatically.

- 30 high-risk users were identified with privileged role assignments. [Investigate with copilot](#)
- Unfamiliar IP ranges associated with recent access attempts, not previously seen in your tenant's activity baseline. [Investigate with copilot](#)
- Policy gaps identified in Conditional Access coverage, leaving some sign-in scenarios without enforced protections. [Review audit logs](#)
- Repeated failed sign-ins from a single region, indicating potential brute-force or credential stuffing attempts. [Review audit logs](#)

What do I need to know?

What changed since yesterday?

Improve my tenant's security



Needs your attention (3)

[View all activity](#)



25 users impacted by an anomalous spike in MFA sign-in failures

High severity

Last updated: 2/16/26, 12:10 PM

Anomalous spikes may indicate an MFA service disruption, brute-force attacks, or misconfigured Conditional Access policies that require immediate review. Review sign-in activity and MFA policy health.

100K

80K



54 admin users don't have MFA set up

Last updated: 2/16/26, 12:10 PM

Require MFA for admin roles. Review affected users to complete registration.

Resource	Status	First detected
adelev@woodgrove.ms	Active	Apr 15, 2025, 4:17 AM
johnw@woodgrove.ms	Active	May 10, 2025, 5:28 PM...

Disclosure

USERS SHOULD ALWAYS KNOW WHEN CONTENT IS AI-GENERATED. MAYA KNOWS THIS SUMMARY WAS GENERATED BY AI.

CLEAR DISCLOSURE

Welcome back, Maya



Copilot summary

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

Last updated: 3 hours ago



I've been monitoring your tenant activity. **An unusual spike detected in sign-ins were detected +64% in the last hour. I recommend blocking the IP range and strengthening Conditional Access policies to reduce risk.** Over the last 24 hours, I've identified **1 critical issue** and **1 medium-severity item** requiring your attention, and resolved **3 low-severity items** automatically.

- 30 high-risk users were identified with privileged role assignments. [Investigate with copilot](#)
- Unfamiliar IP ranges associated with recent access attempts, not previously seen in your tenant's activity baseline. [Investigate with copilot](#)
- Policy gaps identified in Conditional Access coverage, leaving some sign-in scenarios without enforced protections. [Review audit logs](#)
- Repeated failed sign-ins from a single region, indicating potential brute-force or credential stuffing attempts. [Review audit logs](#)

What do I need to know?

What changed since yesterday?

Improve my tenant's security



Reliability & safety

Freshness

SECURITY POSTURE CHANGES CONSTANTLY. SHOWING WHEN INSIGHTS WERE GENERATED HELPS MAYA DETERMINE WHETHER THE RECOMMENDATION IS STILL RELEVANT BEFORE ACTING.

FRESHNESS OF DATA

Welcome back, Maya

 **Copilot summary** AI-generated content may be incorrect. Check for accuracy.

🕒 Last updated: 3 hours ago

I've been monitoring your tenant activity. **An unusual spike detected in sign-ins were detected +64% in the last hour. I recommend blocking the IP range and strengthening Conditional Access policies to reduce risk.** Over the last 24 hours, I've identified **1 critical issue** and **1 medium-severity item** requiring your attention, and resolved **3 low-severity items** automatically.

- 30 high-risk users were identified with privileged role assignments. [Investigate with copilot](#) 
- Unfamiliar IP ranges associated with recent access attempts, not previously seen in your tenant's activity baseline. [Investigate with copilot](#) 
- Policy gaps identified in Conditional Access coverage, leaving some sign-in scenarios without enforced protections. [Review audit logs](#) 
- Repeated failed sign-ins from a single region, indicating potential brute-force or credential stuffing attempts. [Review audit logs](#) 

What do I need to know?

What changed since yesterday?

Improve my tenant's security



Feedback

FEEDBACK MECHANISMS CREATE A LEARNING LOOP BETWEEN USERS AND THE SYSTEM, HELPING IMPROVE FUTURE RECOMMENDATIONS WHILE GIVING MAYA A VOICE WHEN SOMETHING FEELS INCORRECT.

Welcome back, Maya



Copilot summary

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

Last updated: 3 hours ago



I've been monitoring your tenant activity. **An unusual spike detected in sign-ins were detected +64% in the last hour. I recommend blocking the IP range and strengthening Conditional Access policies to reduce risk.** Over the last 24 hours, I've identified **1 critical issue** and **1 medium-severity item** requiring your attention, and resolved **3 low-severity items** automatically.

- 30 high-risk users were identified with privileged role assignments. [Investigate with copilot](#)
- Unfamiliar IP ranges associated with recent access attempts, not previously seen in your tenant's activity baseline. [Investigate with copilot](#)
- Policy gaps identified in Conditional Access coverage, leaving some sign-in scenarios without enforced protections. [Review audit logs](#)
- Repeated failed sign-ins from a single region, indicating potential brute-force or credential stuffing attempts. [Review audit logs](#)

What do I need to know?

What changed since yesterday?

Improve my tenant's security



CONTINUOUS IMPROVEMENT

Guidance

FOLLOW-UP PROMPTS REDUCE AMBIGUITY BY HELPING MAYA INVESTIGATE, VALIDATE, AND ACT WITHOUT NEEDING TO FORMULATE THE NEXT QUESTION HERSELF.

Welcome back, Maya



Copilot summary

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

Last updated: 3 hours ago



I've been monitoring your tenant activity. **An unusual spike detected in sign-ins were detected +64% in the last hour. I recommend blocking the IP range and strengthening Conditional Access policies to reduce risk.** Over the last 24 hours, I've identified 1 **critical issue** and 1 **medium-severity item** requiring your attention, and resolved 3 **low-severity items** automatically.

- 30 high-risk users were identified with privileged role assignments. [Investigate with copilot](#)
- Unfamiliar IP ranges associated with recent access attempts, not previously seen in your tenant's activity baseline. [Investigate with copilot](#)
- Policy gaps identified in Conditional Access coverage, leaving some sign-in scenarios without enforced protections. [Review audit logs](#)
- Repeated failed sign-ins from a single region, indicating potential brute-force or credential stuffing attempts. [Review audit logs](#)

What do I need to know?

What changed since yesterday?

Improve my tenant's security



GUIDED EXPLORATION

Verification

TRUST GROWS WHEN RECOMMENDATIONS CAN BE INSPECTED.
DIRECT LINKS TO SUPPORTING EVIDENCE ALLOW MAYA TO
VALIDATE FINDINGS BEFORE TAKING ACTION.

VERIFIABLE EVIDENCE

Welcome back, Maya



Copilot summary

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

Last updated: 3 hours ago



I've been monitoring your tenant activity. **An unusual spike detected in sign-ins were detected +64% in the last hour. I recommend blocking the IP range and strengthening Conditional Access policies to reduce risk.** Over the last 24 hours, I've identified **1 critical issue** and **1 medium-severity item** requiring your attention, and resolved **3 low-severity items** automatically.

- 30 high-risk users were identified with privileged role assignments. [Investigate with copilot](#)
- Unfamiliar IP ranges associated with recent access attempts, not previously seen in your tenant's activity baseline. [Investigate with copilot](#)
- Policy gaps identified in Conditional Access coverage, leaving some sign-in scenarios without enforced protections. [Review audit logs](#)
- Repeated failed sign-ins from a single region, indicating potential brute-force or credential stuffing attempts. [Review audit logs](#)

What do I need to know?

What changed since yesterday?

Improve my tenant's security





“I want to understand how and why these users are high risk”

Maya Patel

Confidence signals

MAYA WANTS TO UNDERSTAND WHY THERE ARE HIGH RISK USERS IN HER TENANT. LETS DIG IN.

Welcome back, Maya

 **Copilot summary**

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

Last updated: 3 hours ago

I've been monitoring your tenant activity. An unusual spike detected in sign-ins were detected +64% in the last hour. I recommend blocking the IP range and strengthening Conditional Access policies to reduce risk. Over the last 24 hours, I've identified 1 critical issue and 1 medium-severity item requiring your attention, and resolved 3 low-severity items automatically.

- 30 high-risk users were identified with privileged role assignments. [Investigate with copilot](#)
- Unfamiliar IP ranges associated with recent access attempts, not previously seen in your tenant's activity baseline. [Investigate with copilot](#)
- Policy gaps identified in Conditional Access coverage, leaving some sign-in scenarios without enforced protections. [Review audit logs](#)
- Repeated failed sign-ins from a single region, indicating potential brute-force or credential stuffing attempts. [Review audit logs](#)

What do I need to know?

What changed since yesterday?

Improve my tenant's security



Needs your attention (3)

[View all activity](#)

 **25 users impacted by an anomalous spike in MFA sign-in failures**

High severity

Last updated: 2/16/26, 12:10 PM

Anomalous spikes may indicate an MFA service disruption, brute-force attacks, or misconfigured Conditional Access policies that require immediate review. Review sign-in activity and MFA policy health.

100K

80K

 **54 admin users don't have MFA set up**

Last updated: 2/16/26, 12:10 PM

Require MFA for admin roles. Review affected users to complete registration.

Resource	Status	First detected
adelev@woodgrove.ms	Active	Apr 15, 2025, 4:17 AM
johnw@woodgrove.ms	Active	May 10, 2025, 5:28 PM...

Confidence signals

SHE CLICKS INVESTIGATE WITH COPILOT TO START AN INVESTIGATION

Search resources, services and docs

Copilot

Connie Wilson
CONTOSO

New project

6/21, 9:15 AM

Further investigate 30 high-risk users were identified with privileged role assignments.

Welcome back, Maya

Copilot summary

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

Last updated: 3 hours ago

I've been monitoring your tenant activity. An unusual spike detected in sign-ins were detected +64% in the last hour. I recommend blocking the IP range and strengthening Conditional Access policies to reduce risk. Over the last 24 hours, I've identified 1 critical issue and 1 medium-severity item requiring your attention, and resolved 3 low-severity items automatically.

- 30 high-risk users were identified with privileged role assignments. [Investigate with copilot](#)
- Unfamiliar IP ranges associated with recent access attempts, not previously seen in your tenant's activity baseline. [Investigate with copilot](#)
- Policy gaps identified in Conditional Access coverage, leaving some sign-in scenarios without enforced protections. [Review audit logs](#)
- Repeated failed sign-ins from a single region, indicating potential brute-force or credential stuffing attempts. [Review audit logs](#)

What do I need to know?

What changed since yesterday?

Improve my tenant's security

Needs your attention (3)

25 users impacted by an anomalous spike in MFA sign-in failures

High severity

Last updated: 2/16/26, 12:10 PM

Anomalous spikes may indicate an MFA service disruption, brute-force attacks, or misconfigured Conditional Access policies that require immediate review. Review sign-in activity and MFA policy health.

54 admin users don't have MFA set up

Last updated: 2/16/26, 12:10 PM

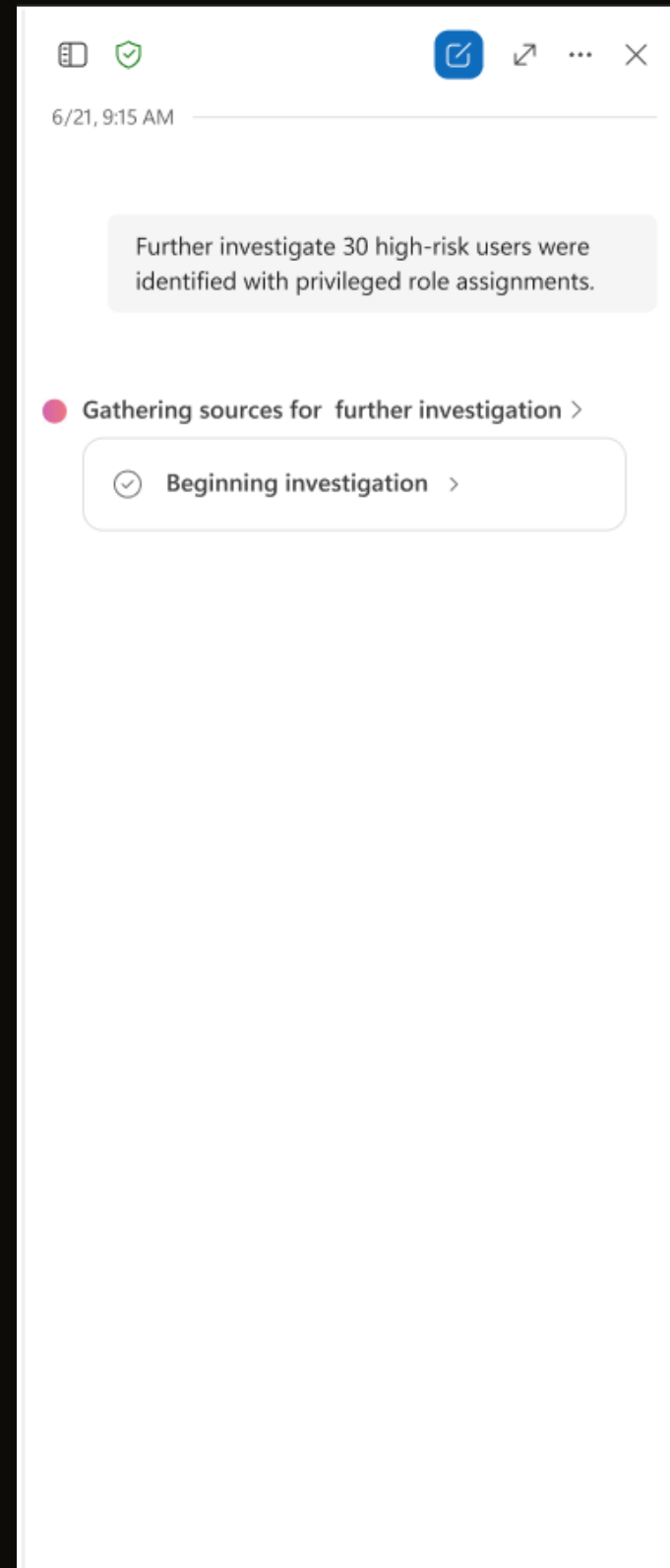
Require MFA for admin roles. Review affected users to complete registration.

Resource	Status	First detected
adelev@woodgrove.ms	Active	Apr 15, 2025, 4:17 AM
johnw@woodgrove.ms	Active	May 10, 2025, 5:28 PM...
ronhd@woodgrove.ms	Active	May 17, 2025, 2:24 PM

Transparency

Guided investigation

USERS WANT CONFIDENCE THAT THE SYSTEM FOLLOWED A REASONABLE PROCESS. TRANSPARENCY DOES NOT REQUIRE EXPOSING EVERY DETAIL ALL THE TIME.

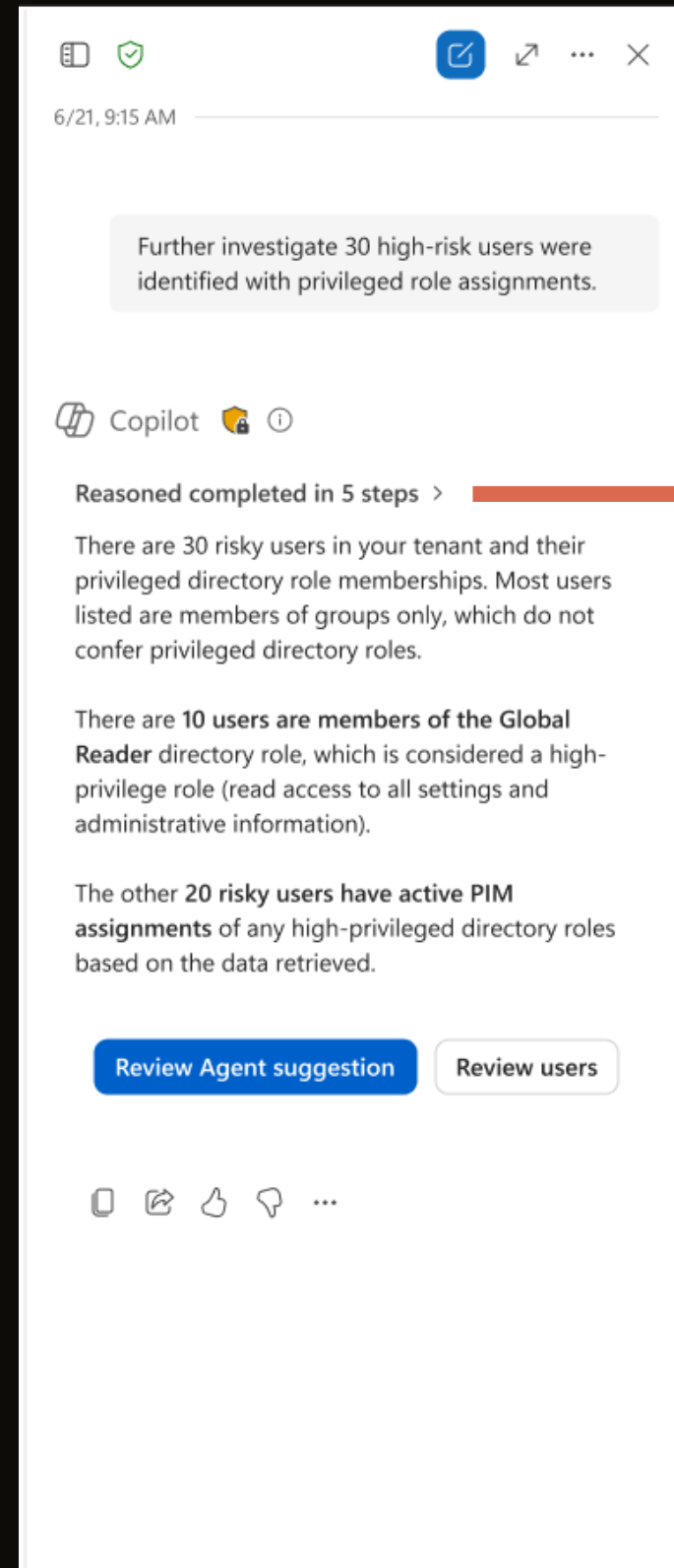
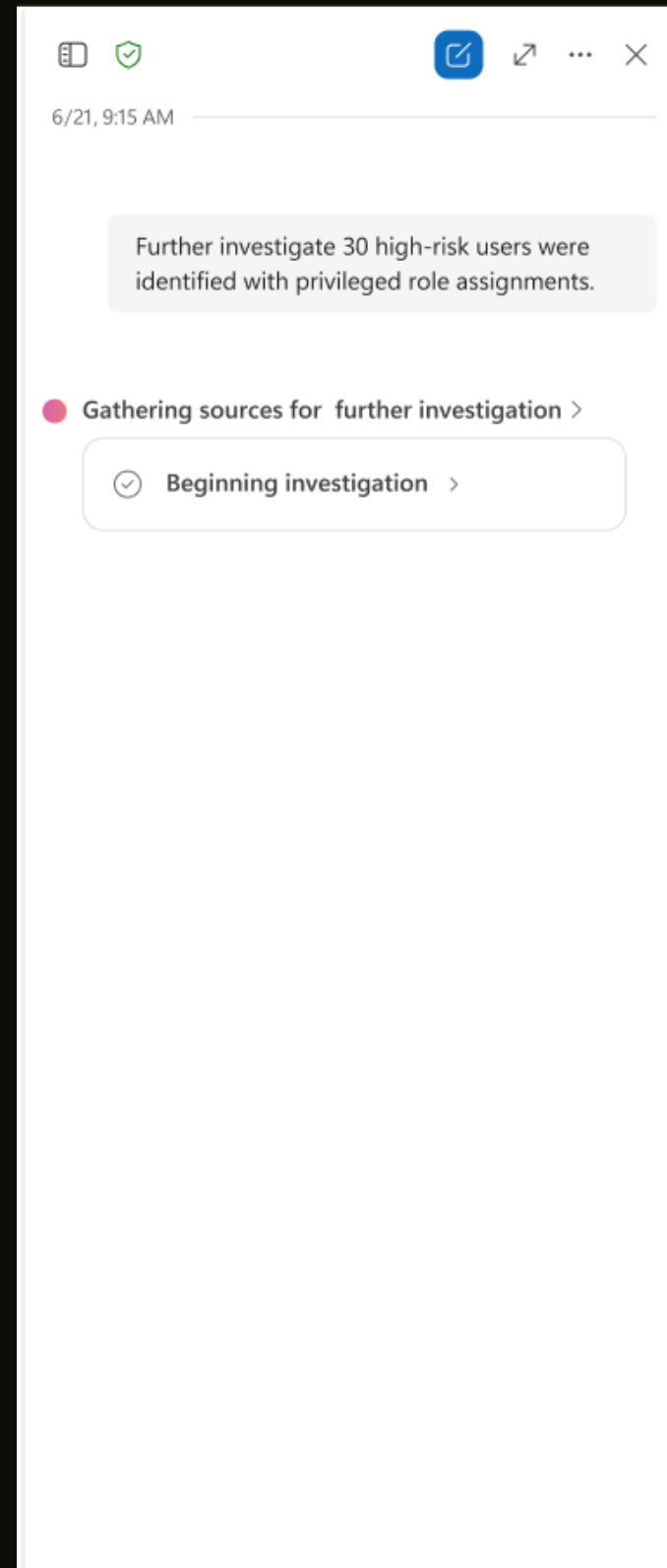


INVESTIGATE

Transparency

Show your work

BEFORE ASKING THE USER TO ACT, THE SYSTEM SUMMARIZES THE FINDINGS THAT LED TO ITS RECOMMENDATION.



REASONING SUMMARY

Transparency

Show your work

USERS CAN INSPECT HOW INFORMATION WAS GATHERED AND EVALUATED WITHOUT NEEDING TO UNDERSTAND EVERY TECHNICAL DETAIL.

REASONING STEPS

Copilot

Reasoned completed in 5 steps

Beginning research

Started to pull together relevant sources.

Sign-in-logs-06-07-2026

Researching knowledge base

Naming convention matches tenant standards in knowledge base.

Sign-in-logs-06-07-2026

Retrieved the privileged roles assigned to...

Looked for the roles that those users have assigned to them. Filtered into each role to find high privileged roles belonging to those users.

Sign-in-logs-06-07-2026

Correlated risk signals with role assignme...

Correlated the user's risk signals with their role assignments to produce a consolidated result set.

Sign-in-logs-06-07-2026

There are 30 risky users in your tenant and their privileged directory role memberships. Most users listed are members of groups only, which do not confer privileged directory roles.

There are 10 users are members of the Global Reader directory role, which is considered a high-privilege role (read access to all settings and administrative information).

The other 20 risky users have active PIM assignments of any high-privileged directory roles based on the data retrieved.

Review Agent suggestion

Review users

Transparency

Show your sources

EXPANDING THE REASONING ALLOWS USERS TO INSPECT THE STEPS TAKEN, UNDERSTAND HOW INFORMATION WAS GATHERED, AND EVALUATE WHETHER THE APPROACH WAS APPROPRIATE.

 Copilot  

Reasoned completed in 5 steps ▾

✓ Beginning research

Started to pull together relevant sources.

 Sign-in-logs-06-07-2026

✓ Researching knowledge base

Naming convention matches tenant standards in knowledge base.

 Sign-in-logs-06-07-2026

✓ Retrieved the privileged roles assigned to...

Looked for the roles that those users have assigned to them. Filtered into each role to find high privileged roles belonging to those users.

 Sign-in-logs-06-07-2026

✓ Correlated risk signals with role assignme...

Correlated the user's risk signals with their role assignments to produce a consolidated result set.

 Sign-in-logs-06-07-2026

There are 30 risky users in your tenant and their privileged directory role memberships. Most users listed are members of groups only, which do not confer privileged directory roles.

There are 10 users are members of the Global Reader directory role, which is considered a high-privilege role (read access to all settings and administrative information).

The other 20 risky users have active PIM assignments of any high-privileged directory roles based on the data retrieved.

Review Agent suggestion

Review users

INVESTIGATION STEPS

SOURCE DATA

TRUST INCREASES WHEN USERS CAN SEE BOTH THE PROCESS AND THE INFORMATION USED TO REACH A CONCLUSION.

Transparency

Show options to go deeper

EXPANDING THE REASONING ALLOWS USERS TO INSPECT THE STEPS TAKEN, UNDERSTAND HOW INFORMATION WAS GATHERED, AND EVALUATE WHETHER THE APPROACH WAS APPROPRIATE.

 Copilot  

Reasoned completed in 5 steps ▾

✓ Beginning research

Started to pull together relevant sources.

 Sign-in-logs-06-07-2026

✓ Researching knowledge base

Naming convention matches tenant standards in knowledge base.

 Sign-in-logs-06-07-2026

✓ Retrieved the privileged roles assigned to...

Looked for the roles that those users have assigned to them. Filtered into each role to find high privileged roles belonging to those users.

 Sign-in-logs-06-07-2026

✓ Correlated risk signals with role assignme...

Correlated the user's risk signals with their role assignments to produce a consolidated result set.

 Sign-in-logs-06-07-2026

There are 30 risky users in your tenant and their privileged directory role memberships. Most users listed are members of groups only, which do not confer privileged directory roles.

There are 10 users are members of the **Global Reader** directory role, which is considered a high-privilege role (read access to all settings and administrative information).

The other 20 risky users have active PIM assignments of any high-privileged directory roles based on the data retrieved.

Review Agent suggestion

Review users

INVESTIGATION STEPS

SOURCE DATA

TAKE ACTION

Transparency

Explore further

DIFFERENT USERS NEED DIFFERENT LEVELS OF
DETAIL. TRANSPARENCY SHOULD SUPPORT BOTH
QUICK DECISIONS AND DEEPER
INVESTIGATION.

✓ Retrieved the privileged roles assigned to...

Looked for the roles that those users have assigned to them. Filtered into each role to find high privileged roles belonging to those users. [↔ Sign-in-logs-06-07-2026](#)

✓ Correlated risk signals with role assignme...

Correlated the user's risk signals with their role assignments to produce a consolidated result set. [↔ Sign-in-logs-06-07-2026](#)

There are 30 risky users in your tenant and their privileged directory role memberships. Most users listed are members of groups only, which do not confer privileged directory roles.

There are 10 users are members of the **Global Reader** directory role, which is considered a high-privilege role (read access to all settings and administrative information).

The other 20 risky users have active PIM assignments of any high-privileged directory roles based on the data retrieved.

Review Agent suggestion

Review users

📄

🔗

👍

👎

...

Ask me anything

+

🎤

Review the evidence

THE STRONGEST FORMS OF TRANSPARENCY
ALLOW USERS TO MOVE FROM:
ANSWER → REASONING → EVIDENCE.

Microsoft Entra admin center

Search

Copilot

Home

Users

Show risky users most recent sign-in

Show sign-in failures from the last 24 hours

Show users flagged for review

2 more

Copilot summary

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

Investigate sign-in failures

Unusual spike detected in sign-ins were detected +64% in the last hour. Recommendation: Block IP range via Named Locations + Conditional Access. Lorem ipsum dolor sit amet consectetur. Sem eget sed at quam

Download

Data export settings

Troubleshoot

Refresh

Columns

Feedback

Add filter

Date range : Last 3 hours

Sign-in error code : 50126; 50053; 50074

Flagged for review : Yes

User display name	Risk level	Risk state	High Privileged Role(s)	Risk last updated
Sally Sparks	high	atRisk	Global Reader	6/18/2026, 3:59:26 PM
Louise Smithson	high	confirmedCompromized	Global Reader	6/18/2026, 3:59:26 PM
Rianna Keosanah	high	atRisk	Global Reader	6/18/2026, 3:59:26 PM
Tammy Braun	high	atRisk	Global Reader	6/18/2026, 3:59:26 PM
Aadi Kapoor	high	confirmedCompromized	Global Reader	6/18/2026, 3:59:26 PM
Aaron Voski	high	confirmedCompromized	Global Reader	6/18/2026, 3:59:26 PM
Dabir Uwimana	high	atRisk	Global Reader	6/18/2026, 3:59:26 PM
Billie Borbely	high	confirmedCompromized	Global Reader	6/18/2026, 3:59:26 PM
Camille San	high	atRisk	Global Reader	6/18/2026, 3:59:26 PM
Gabriel Moeller	high	confirmedCompromized	Global Reader	6/18/2026, 3:59:26 PM
Karin Blair	high	confirmedCompromized	Global Reader	6/18/2026, 3:59:26 PM
Jarmila Sima	high	atRisk	Global Reader	6/18/2026, 3:59:26 PM
Bothilde Davydenko	high	confirmedCompromized	Global Reader	6/18/2026, 3:59:26 PM
Ijaodola Kamangar	high	confirmedCompromized	None	6/18/2026, 3:59:26 PM

Retrieved the privileged roles assigned to...

Looked for the roles that those users have assigned to them. Filtered into each role to find high privileged roles belonging to those users. [Sign-in-logs-06-07-2026](#)

Correlated risk signals with role assignme...

Correlated the user's risk signals with their role assignments to produce a consolidated result set. [Sign-in-logs-06-07-2026](#)

There are 30 risky users in your tenant and their privileged directory role memberships. Most users listed are members of groups only, which do not confer privileged directory roles.

There are 10 users are members of the Global Reader directory role, which is considered a high-privilege role (read access to all settings and administrative information).

The other 20 risky users have active PIM assignments of any high-privileged directory roles based on the data retrieved.

Review Agent suggestion

Review users

Here is a prefiltered view of the 30 risky users in your tenant and their privileged directory role memberships. Most users listed are members of groups only, which do not confer privileged directory roles.

Would you like to review the agent suggestion?

📄

🔗

👍

👎

...

Ask me anything

+

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

Human review required

RECOMMENDATIONS ARE PROPOSED BY THE SYSTEM, BUT RESPONSIBILITY FOR THE FINAL DECISION REMAINS WITH THE USER.

✓ Retrieved the privileged roles assigned to...

Looked for the roles that those users have assigned to them. Filtered into each role to find high privileged roles belonging to those users. [↔ Sign-in-logs-06-07-2026](#)

✓ Correlated risk signals with role assignme...

Correlated the user's risk signals with their role assignments to produce a consolidated result set. [↔ Sign-in-logs-06-07-2026](#)

There are 30 risky users in your tenant and their privileged directory role memberships. Most users listed are members of groups only, which do not confer privileged directory roles.

There are 10 users are members of the **Global Reader** directory role, which is considered a high-privilege role (read access to all settings and administrative information).

The other 20 risky users have active PIM assignments of any high-privileged directory roles based on the data retrieved.

Review Agent suggestion

Review users

Ask me anything

+



Agent suggests, human acts

THE AGENT PERFORMS ANALYSIS AND PREPARES RECOMMENDATIONS. MAYA REVIEWS THE EVIDENCE, EVALUATES THE IMPACT, AND DECIDES WHETHER TO TAKE ACTION.

Home > Conditional Access

Conditional Access | Policies

Microsoft Entra ID

Overview

Policies

Deleted policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication contexts

Authentication strengths

Classic policies

Monitoring

Sign-in logs

Audit logs

Troubleshooting + Support

New support request

+ New policy

+ New policy from template

Upload policy

Microsoft Entra Conditional Access policies are used to apply e

Conditional Access Optimization Agent

Policies created 2

Policy suggestions 1

Manage agent

Search

Add filter

59 out of 59 policies found

Policy name

Multifactor authentication for 16 users

Device compliance for 47 new users

CA4: MFA for corporate

Enforce MFA

High risk user policy

Hr app access policy

MFA

MFA compliance for Fabrikam guests

MFA for admins

Contoso Terms of Use

CA4: MFA for corporate

Conditional Access policy

Policy details

Policy impact (Preview)

Edit

Duplicate

Download JSON

Delete

Suggestion: Remediate 30 high-risk users privileged access

Not applied

Generated on 6/16/26, 1:07 PM

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

The agent identified 30 high-risk users with privileged permissions that may increase organizational risk. The 29 Conditional Access policies that require MFA do not cover them.

How it will affect users

The agent created a new policy in report-only mode on 6/16/26, 1:27PM. If you turn it on:

5 confirmed compromised users will have privileged access removed

8 privileged users will be required to register for MFA

17 high-risk privileged accounts will be submitted for access review

Reasoning complete in 5 steps

Beginning research

Identified users that are currently classified risky in Contoso

Retrieved the privileged roles assigned to those users

Correlated risk signals with role assignments to produce a consolidated result set

Gathered information in a list

Review policy changes

Apply suggestion

View agent's full activity

Policy details

Name

CA4: MFA for corporate

State

Report only

Created by

Sign-in-logs-06-07-2026

Retrieved the privileged roles assigned to...

Looked for the roles that those users have assigned to them. Filtered into each role to find high privileged roles belonging to those users.

Sign-in-logs-06-07-2026

Correlated risk signals with role assignme...

Correlated the user's risk signals with their role assignments to produce a consolidated result set.

Sign-in-logs-06-07-2026

There are 30 risky users in your tenant and their privileged directory role memberships. Most users listed are members of groups only, which do not confer privileged directory roles.

There are 10 users are members of the Global Reader directory role, which is considered a high-privilege role (read access to all settings and administrative information).

The other 20 risky users have active PIM assignments of any high-privileged directory roles based on the data retrieved.

Review Agent suggestion

Review users

Here is a Agent suggestion of of the 30 risky users in your tenant and their privileged directory role memberships. Most users listed are members of groups only, which do not confer privileged directory roles.

Would you like to review the users in detail?

Copy

Share

Like

Dislike

More

Ask me anything

Accountability

ACCOUNTABILITY ENSURES PEOPLE REMAIN RESPONSIBLE FOR OUTCOMES, EVEN WHEN AI ASSISTS WITH ANALYSIS, RECOMMENDATIONS, OR AUTOMATION.

 **Suggestion: Remediate 30 high-risk users privileged access** ... ^

☐ Not applied | Generated on 6/16/26, 1:07 PM

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

The agent identified [30 high-risk users](#) with privileged permissions that may increase organizational risk. The [29 Conditional Access policies that require MFA](#) do not cover them.

How it will affect users

The agent created a new policy in report-only mode on 6/16/26, 1:27PM. If you turn it on:

- 5 confirmed compromised users will have privileged access removed
- 8 privileged users will be required to register for MFA
- 17 high-risk privileged accounts will be submitted for access review

Reasoning complete in 5 steps ▼

☒ Beginning research ➤

☒ Identified users that are currently classified risky in Contoso ▼
Looked for the roles that those users have assigned to them. Filtered into each role to find high privileged roles belonging to those users. ↔ Sign-in-logs-06-07-2026

☒ Retrieved the privileged roles assigned to those users ➤

☒ Correlated risk signals with role assignments to produce a consolidated result set ➤

☒ Gathered information in a list ➤

Review policy changes

☒ Apply suggestion ▼ View agent's full activity   



Human in the loop

HUMAN-IN-THE-LOOP WORKFLOWS CREATE DELIBERATE MOMENTS FOR REVIEW, APPROVAL, AND INTERVENTION BEFORE CONSEQUENTIAL ACTIONS ARE TAKEN.

Suggestion: Remediate 30 high-risk users privileged access

Not applied

Generated on 6/16/26, 1:07 PM

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

The agent identified [30 high-risk users](#) with privileged permissions that may increase organizational risk. The [29 Conditional Access policies that require MFA](#) do not cover them.

How it will affect users

The agent created a new policy in report-only mode on 6/16/26, 1:27PM. If you turn it on:

- 5 confirmed compromised users will have privileged access removed
- 8 privileged users will be required to register for MFA
- 17 high-risk privileged accounts will be submitted for access review

Reasoning complete in 5 steps

Beginning research

Identified users that are currently classified risky in Contoso

Retrieved the privileged roles assigned to those users

Correlated risk signals with role assignments to produce a consolidated result set

Gathered information in a list

Review policy changes

✓ Apply suggestion

View agent's full activity

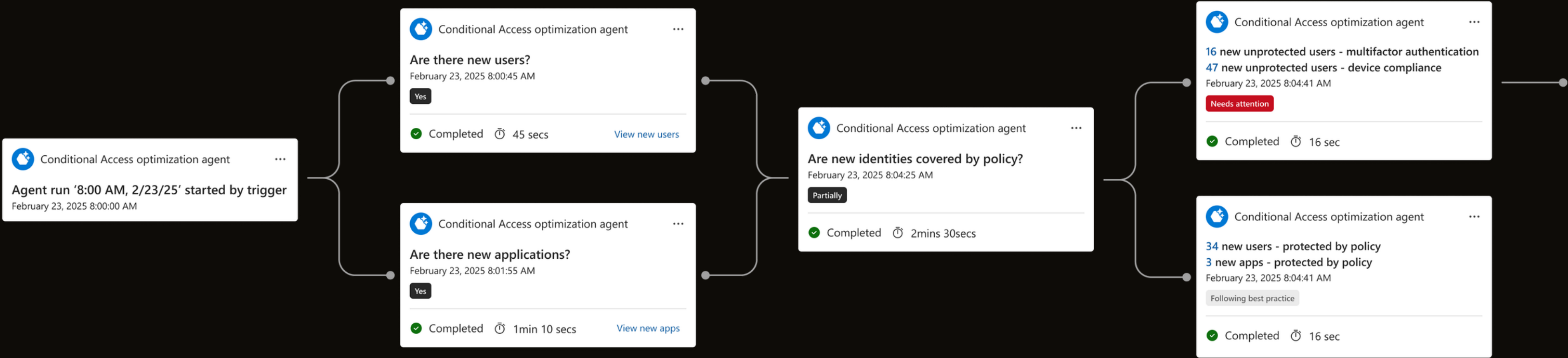
✓ Apply suggestion

Dismiss

Snooze for 14 days

Audit trail

AUDIT TRAILS HELP USERS UNDERSTAND WHAT HAPPENED, WHY IT HAPPENED, AND HOW THE OUTCOME WAS REACHED.



Accountability + Reliability & safety

Accountability at scale

ORGANIZATIONS CANNOT MANAGE WHAT THEY CANNOT SEE. ACCOUNTABILITY BEGINS WITH VISIBILITY.

Agent Observability

Full visibility into every agent across platforms — see their risks, risky activities, and protection status over the last 30 days.

Total 321 agents across your organization

↑ 3% (last 7 days)

View all agents

9 high risk agents

↑ 3% (last 7 days)

View risky agents

37 agents with oversharing risks

↑ 3% (last 7 days)

View oversharing agents

15 Agents with regulatory risks

↑ 3% (last 7 days)

View regulatory risky agents

Group & filters Refresh Export 321 items Search

Agent	Status	Risk level	Risk types	Risky activity trend	Knowledge & Tools	Data protection	Data compliance
 Sam (AI Sales Agent) Agent 365	Sanctioned	High	Oversharing Exfiltration		SharePoint CRM- Connector +3 more	12 Policies	18 Policies
 InsightSynth Agent Azure AI Foundry	Sanctioned	High	Oversharing Exfiltration		SharePoint Dataverse MCP +1 more	4 Policies	6 Policies
 Campaign Agent Agent 365	Sanctioned	High	Unethical		SharePoint	7 Policies	12 Policies
 Data Analysis Agent Salesforce	Unsanctioned	N/A					
 Visual Creator Copilot Studio	Quarantined	N/A					
 Supply Chain Agent Copilot Studio	Sanctioned	Medium	Exfiltration		Outlook CRM- Connector +3 more	12 Policies	15 Policies
 FinanceOps Agent Cloud	Sanctioned	Medium	Oversharing		SharePoint Ally- Connector +3 more	4 Policies	1 Policy

Additional patterns, outside of this flow

Design for choice

Accountability

AI CAN NARROW THE POSSIBILITIES, BUT USERS SHOULD ALWAYS BE ABLE TO STEER THE FINAL DECISION. CUSTOM INPUT PRESERVES AGENCY.

(MICROSOFT PATTERN IN VSCODE)

What should the badge be updated to? ✕ ✓

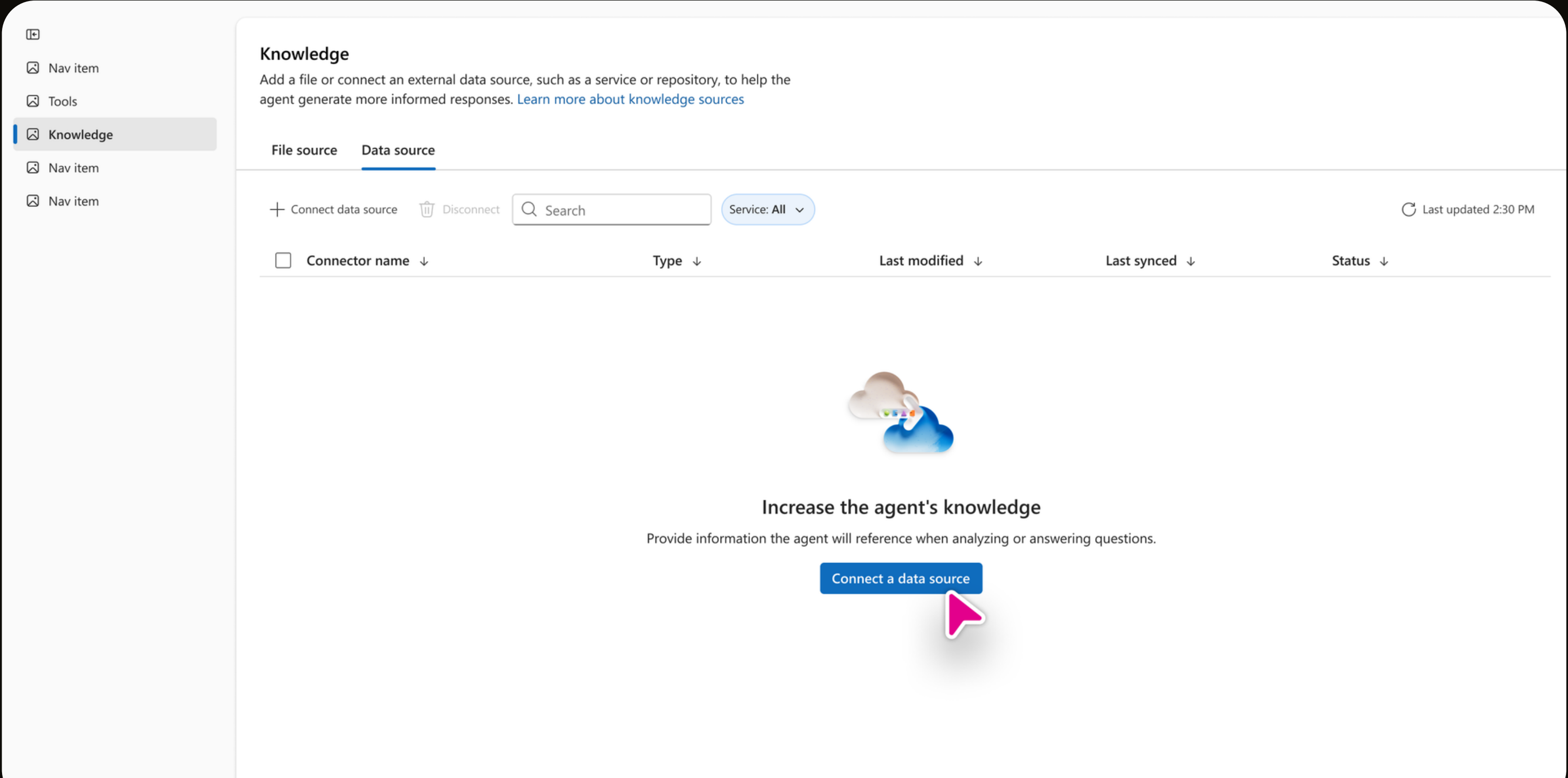
Current badge text is "Needs review".

- 1 Needs approval ✓
- 2 Pending approval
- 3 Awaiting review
- 4 Custom text (type it)
- 5

< > 1/2

Steering with context

TRUST IS EARNED GRADUALLY. AS CONFIDENCE GROWS, USERS OFTEN CHOOSE TO DELEGATE MORE RESPONSIBILITY TO AI SYSTEMS, THAT REQUIRES MORE CONTEXT.



Transparency

Contextually relevant disclaimers

EXPECTATION-SETTING DOESN'T HAPPEN ONCE.
IT APPEARS THROUGHOUT THE EXPERIENCE.

This is for informational purposes only. For medical advice or diagnosis, consult a professional. AI responses may include mistakes. [Learn more](#)



Responsible AI principles



Transparency



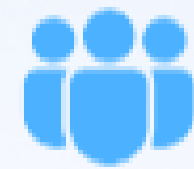
Fairness



Reliability & Safety



Privacy & Security



Inclusiveness



Accountability

Trust must be *continuously* earned.

As AI becomes more capable, trust isn't a milestone. It's an ongoing design responsibility.

Transparency

Keep users informed.

Ground AI in trusted data, monitor performance, and adapt as context changes.

Reliability & Safety

Keep systems dependable.

Ground AI in current context, measure outcomes, and reduce mistakes over time.

Accountability

Keep humans in control.

Give users meaningful oversight, review points, and the ability to intervene.

”

The most profound technologies are those that *disappear*. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

— MARK WEISER • FATHER OF UBIQUITOUS COMPUTING

What we trust, we trust *quietly*.

Questions?

Questions or ideas? Let's connect!

EMAIL

• mary.gansallo@gmail.com

LINKEDIN

• [in/mary-gansallo](https://www.linkedin.com/in/mary-gansallo)

