#Milano

Security Copilot in Microsoft Entra

Michele Sensalari

CTO @ Overnet

#GLOBALAZURE 2026

#Milano

improove

TD SYNNEX

Grazie ai nostri sponsor 🙏

Agenda

- Why needs Security Copilot in Entra?
  - Threats to identities
  - Protection and remediation
- What is Security Copilot?
  - Standalone vs Embedded
- What are the advantages of Security Copilot in Entra?
- Security Copilot AI Agent in Entra
  - Microsoft Entra Conditional Access Optimization Agent

Why needs Security Copilot in Entra?

Threats to identities

Every breach has one thing in common:

An identity was exploited!

Access incidents remain widespread, spanning human error, malicious attacks, and AI-driven threats

Malicious	Accidental
53%	47%

Top causes of identity and network access incidents

Weak authentication mechanisms	29%
Lack of employee awareness	29%
Weak credentials	28%
Network access vulnerabilities	27%
Misuse or abuse of access privileges (excessive access permissions)	24%
Outdated or unpatched systems	24%
Inadequate monitoring & auditing	23%
Gaps or seams between different tools/vendors	22%

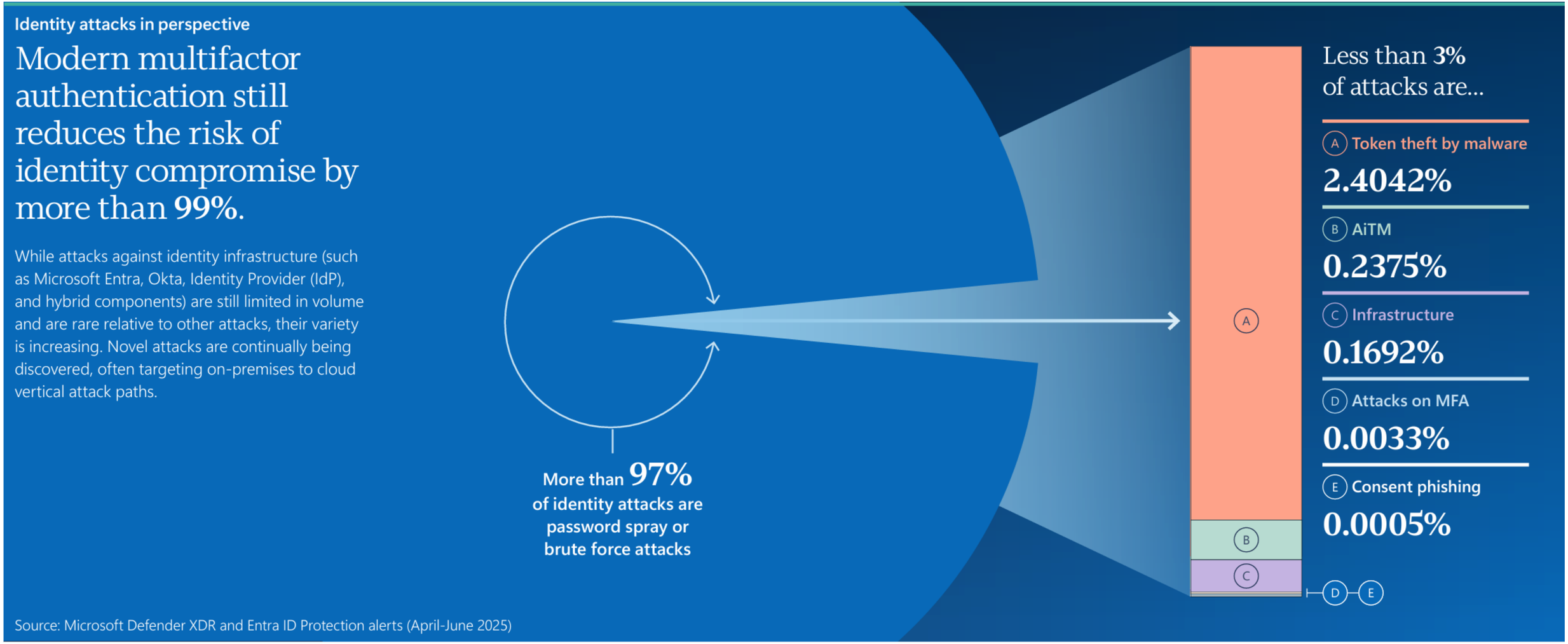
TOP TRADITIONAL / NON-AI INCIDENTS

Password attacks	43%
MFA attacks	29%
Post-authentication attacks	28%

TOP AI INCIDENTS

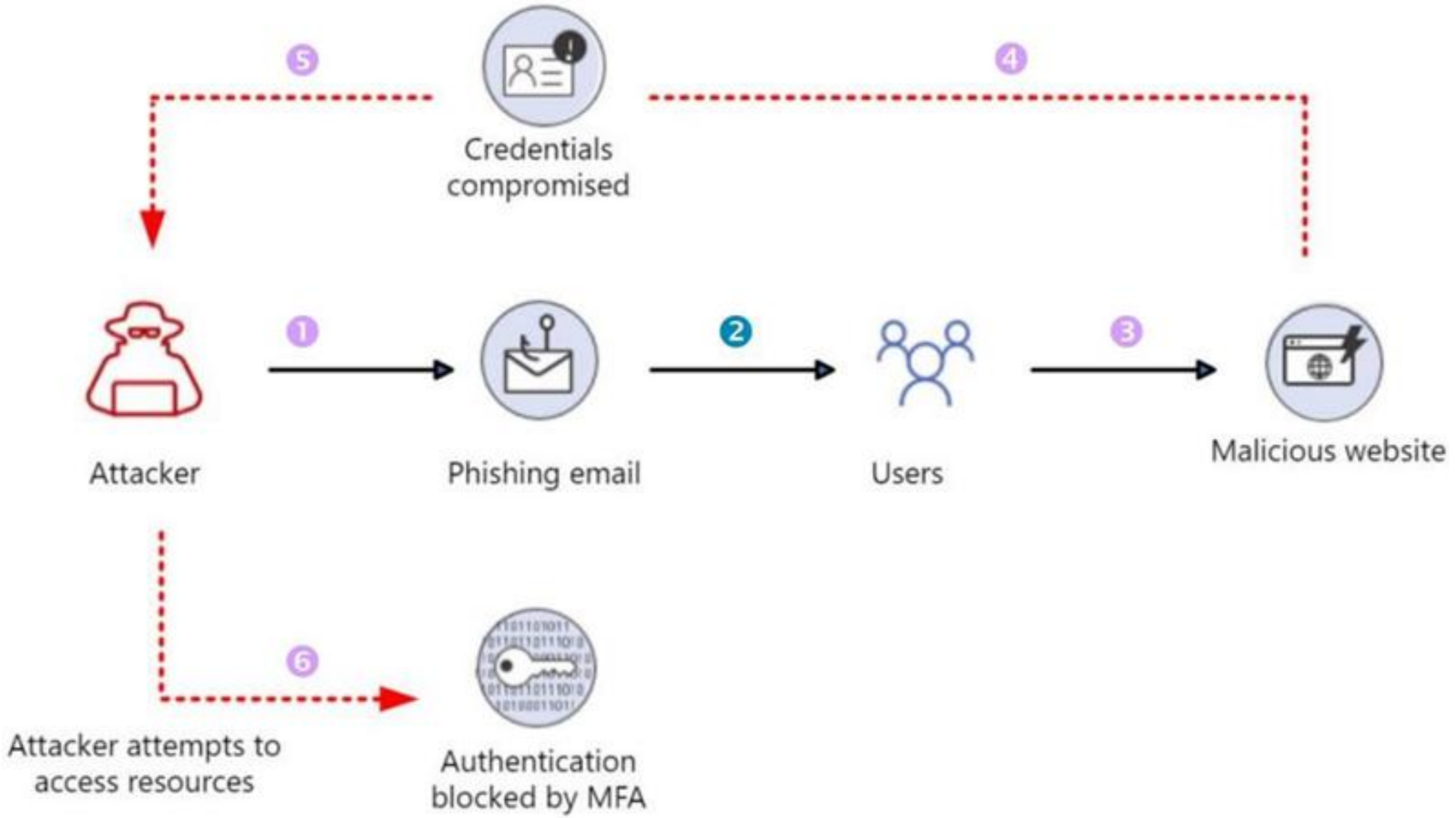
AI-assisted phishing	32%
AI agent privilege escalation	28%
Data exfiltration via AI models	21%
Prompt injection attacks	13%

Identity, access, and the cybercrime economy



Login compromise

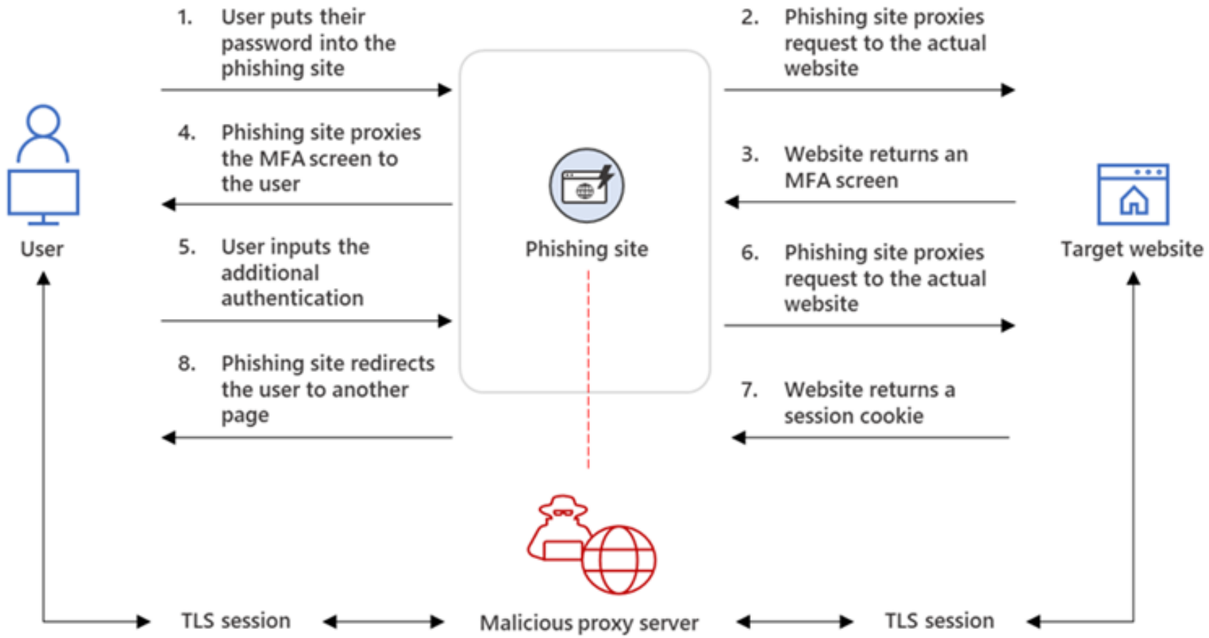
Typical credential attacks happen before a token is issued



Enforce use of Conditional Access Policies

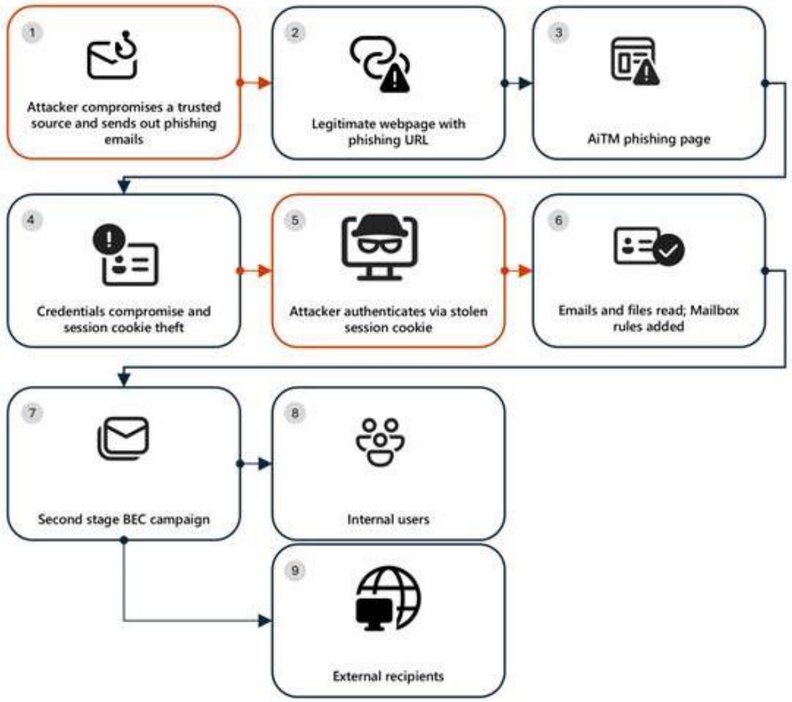
Adversary-in-the-middle (AitM) phishing attack

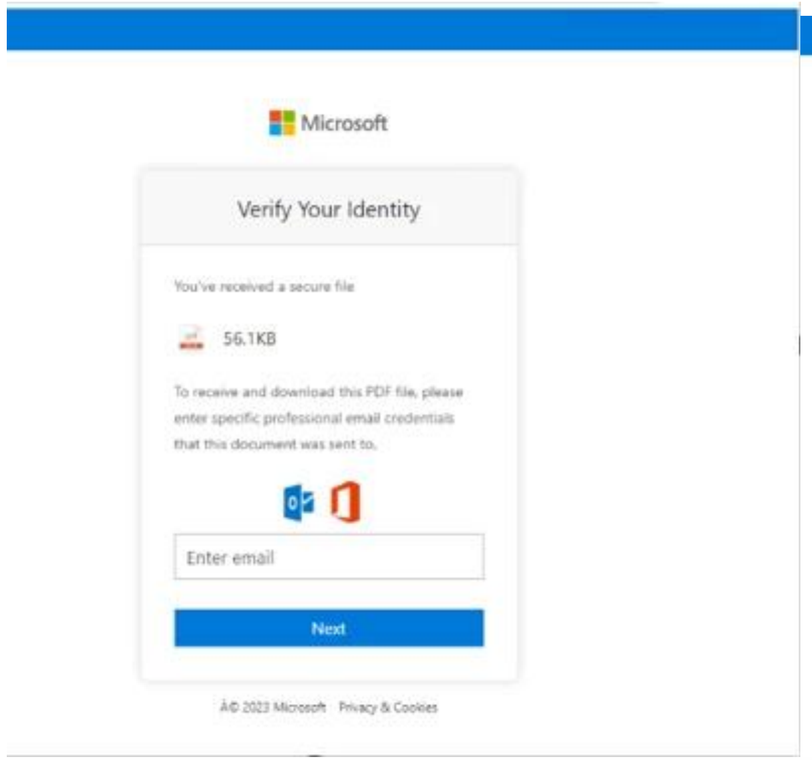
- Adversary in the middle phishing is an increasingly common tactic used by threat actors to steal both credentials and session cookies
- A user is sent a phishing link, when they click on the link, they are presented a website masquerading as a legitimate site. The user then enters their credentials, at that point the AiTM infrastructure proxies a connection to the legitimate site, in this case office.com.
  Open source AiTM toolkits such as **Evilginx2 & Modlishka** help facilitate this. **Phishing as a service** platforms can also include AiTM capability
- The user is prompted for MFA as usual, the **AiTM infrastructure then steals both the credentials and a session cookie** that has satisfied MFA
- The threat actor can then import that cookie into their own browser, when they refresh their browser, they can then logon as the user

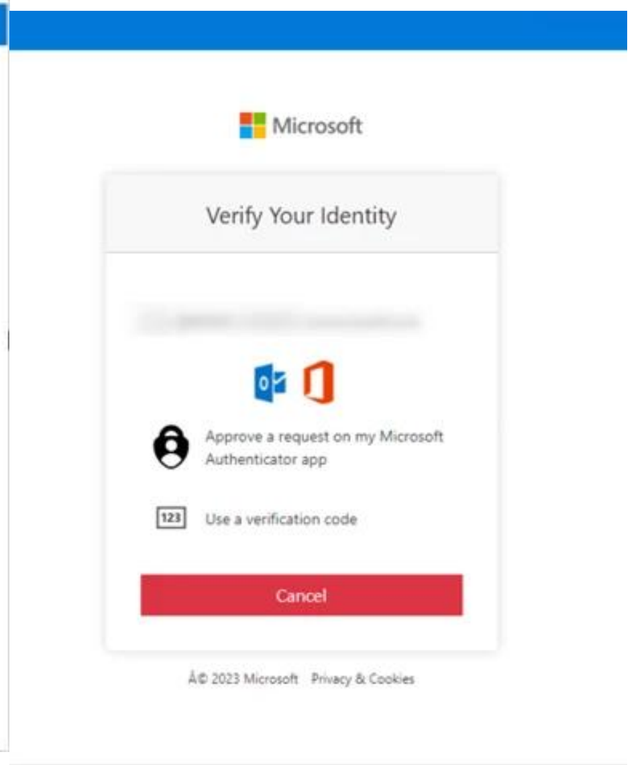


Multi-stage AiTM phishing and BEC campaign abusing SharePoint

The campaign abused SharePoint file-sharing services to deliver phishing payloads and relied on inbox rule creation to maintain persistence and evade user awareness. The attack transitioned into a series of AiTM attacks and follow-on BEC activity spanning multiple organizations.







The message is unmistakable

Traditional MFA based on TOTP, push notifications, and SMS is obsolete as a defense against motivated attackers. This isn't because MFA is useless; it's because attackers have solved the problem elegantly, without even breaking it.

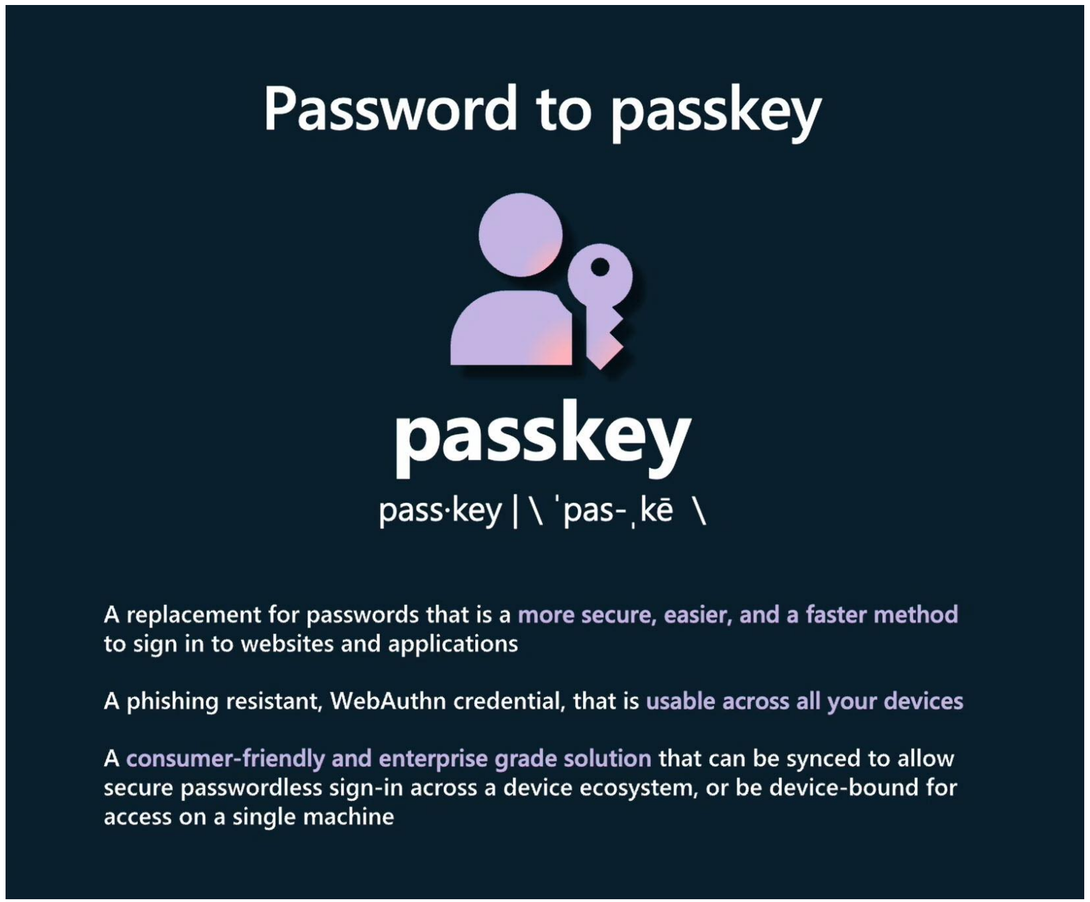
Protection and remediation for login compromise

Protections/ mitigations against AiTM phishing in Microsoft Entra

- Phish-resistant MFA solutions (FIDO/Certificate-based authentication)
  - FIDO2 security keys
  - Windows Hello for Business
  - Certificate-based authentication
- Protect attacks using Conditional Access

Method	Protected (mitigation) against AiTM
Passkey (FIDO2)	Yes
Windows Hello for Business	Yes
Certificate-based authentication	Yes
Passwordless phone sign-in	No
Phone number and SMS	No
Username and password	No

Passkey



- **Device-bound passkeys**: The private key is created and stored on a single physical device and never leaves it. Examples:
  - Microsoft Authenticator
  - FIDO2 Security keys
- **Synced passkeys**: The private key is created by the hardware security module (HSM) and encrypted on the local device. This encrypted key is then synced and stored in the cloud passkey provider. Other devices authenticated with the passkey provider may then use the passkey. This may differ depending on the provider. Synced passkeys do not support attestation. Examples:
  - Apple iCloud Keychain
  - Google Password Manager

Why Passkeys Stop AiTM Attacks

Origin Binding (WebAuthn)

- Passkeys are cryptographically tied to the real domain
- Authentication works only on the legitimate website

No Shared Secrets

- No passwords transmitted or stored server-side
- Private key never leaves the user device

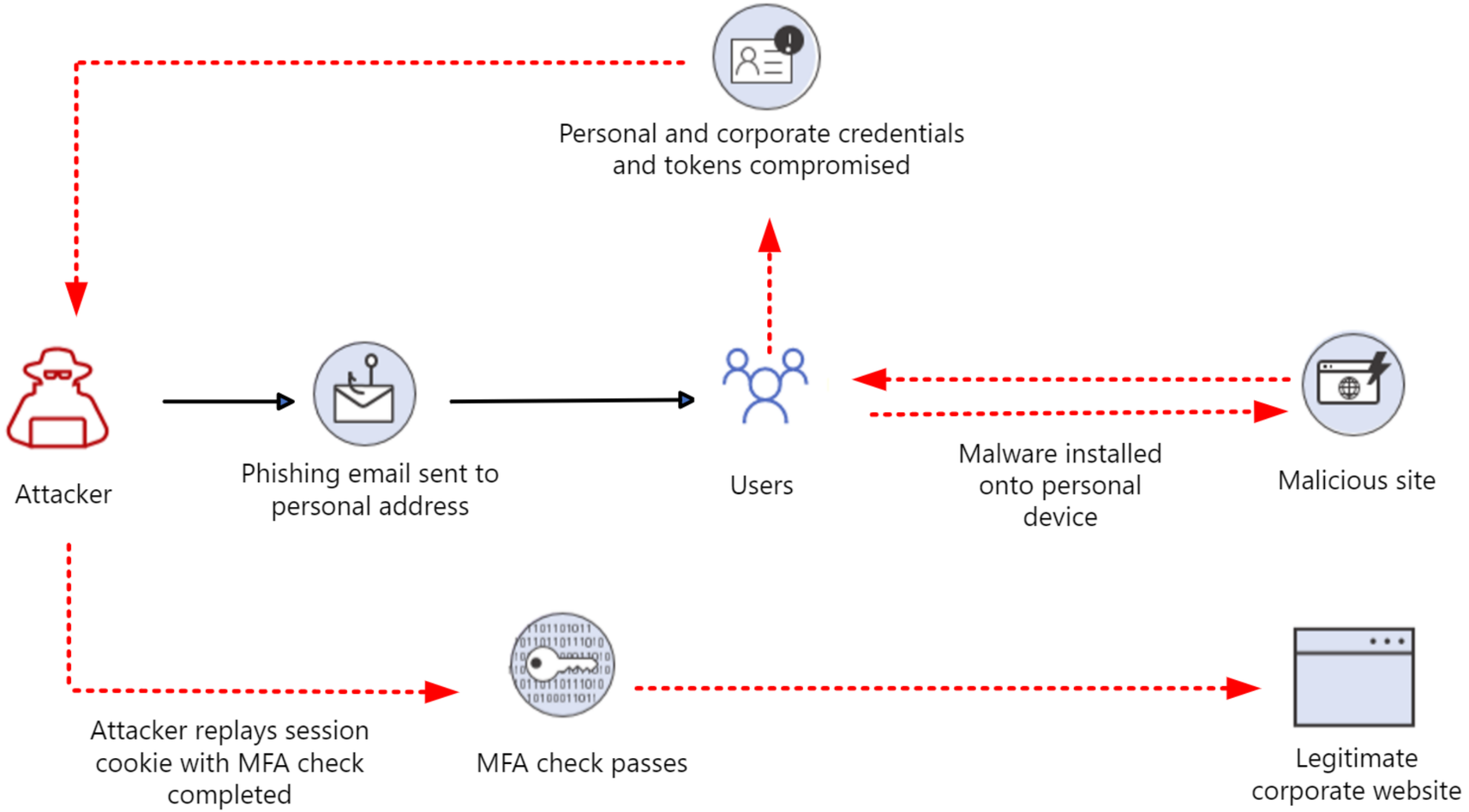
Challenge–Response Mechanism

- Each authentication is unique and non-replayable
- Prevents interception and reuse

Token Theft


Token Theft
Stolen Token Used
Access Token
TOKEN
Sensitive Data
Logged In as:
user@example.com
Access Granted
Fake ID
Bypassing MFA
MFA
2FA
Identity Spoofing
Fake ID
Full Access

Pass-the-cookie attack



Protection and remediation for token theft

Protections/ mitigations against pass-the-cookie in Microsoft Entra

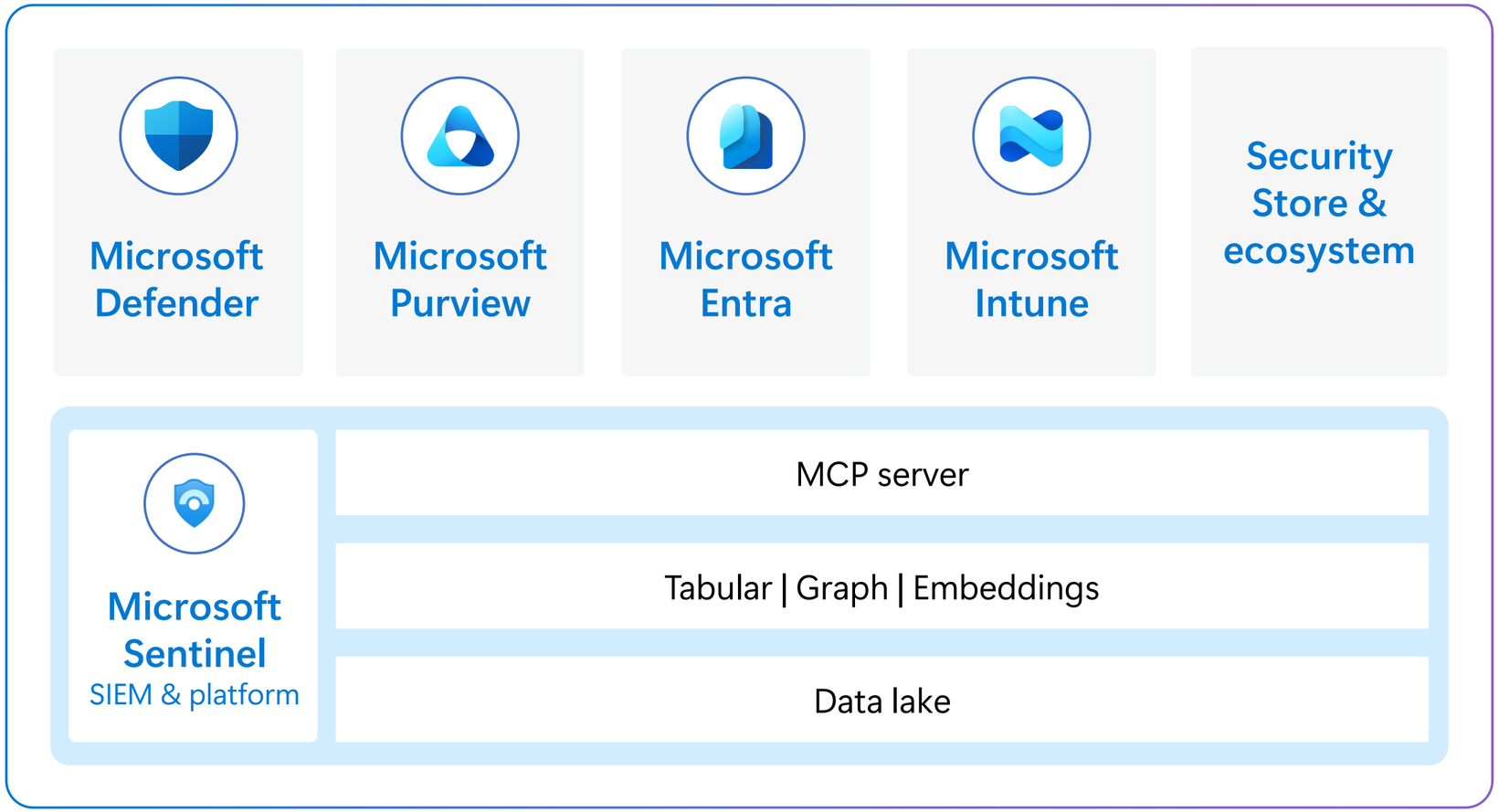
Microsoft Entra ID and other modern identity systems use several mechanisms to protect against token theft and replay attacks

Mechanism	Protection provided
Conditional Access	Requires MFA or triggers additional checks when risk or context changes.
Short Token Lifetime	Limits the usefulness of a stolen token by making it expire quickly.
Continuous Access Evaluation (CAE)	Instantly revokes or re-evaluates tokens when risk is detected or conditions change.
Token Protection (Device Binding)	Ensures a token is valid only on the original device, preventing replay on others.
Device-based access	Ensures device compliant and Hybrid or Entra Joined

What is Security Copilot?

The evolution of phishing: from spam to AI-driven identity attacks

Microsoft Security Ecosystem



Data connectors
(350+ Sentinel connectors)

Security Copilot

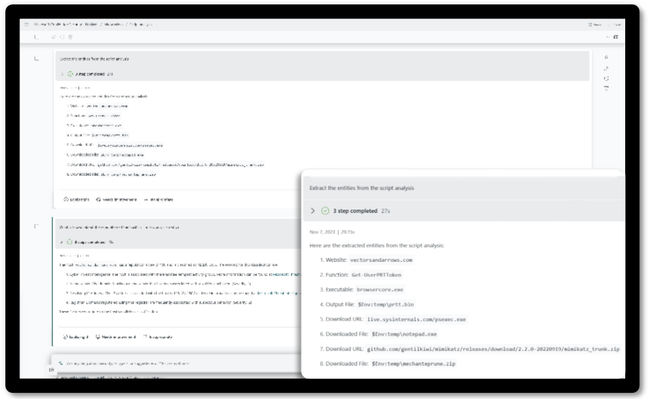
Multicloud and multiplatform

Security Copilot

An AI-powered, cloud-based security analysis tool that enables analysts to respond to threats quickly, process signals at machine speed, and assess risk exposure more quickly than may otherwise be possible.

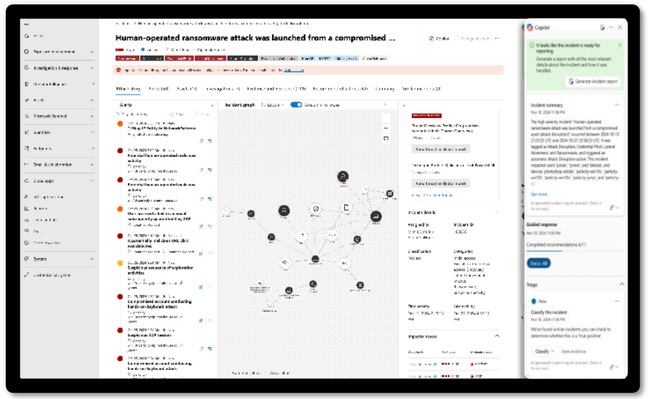
Standalone

Helps teams gain a broader context to troubleshoot and remediate incidents faster within Copilot itself, with many use cases in one place, enabling enriched cross-product guidance



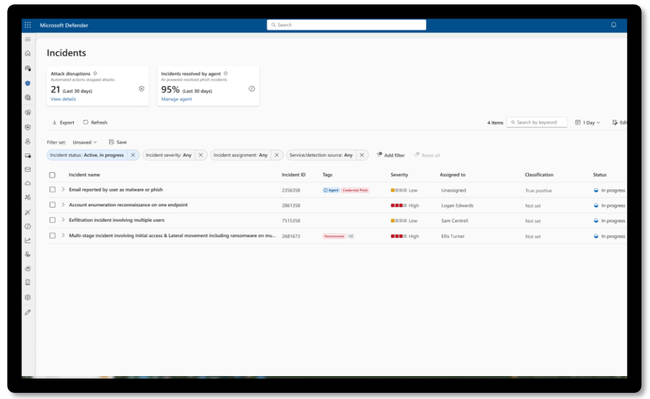
Embedded

Offers the intuitive experience of getting Copilot guidance natively within the products that your team members already work from and are familiar with



Automation and agents

Helps teams accelerate response with built-in agents and custom promptbooks as well as integration with Logic Apps



Security Copilot - Use Cases

Incident summarization.

Distil complex security alerts into concise actional summaries.

Impact analysis.

Assess the potential impact of security incidents to enable quicker response times and streamlined decision-making.

Reverse engineering of scripts.

Analyze complex command line scripts and translate them into natural language with clear explanations of actions.

Guided responses.

Actionable step-by-step guidance for incident response, including directions for triage, investigation, containment, and remediation.

What are the advantages of Security Copilot in Entra?

With Security Copilot in Entra

1

Understand identity in natural language

2

Investigate identity risks with built-in reasoning

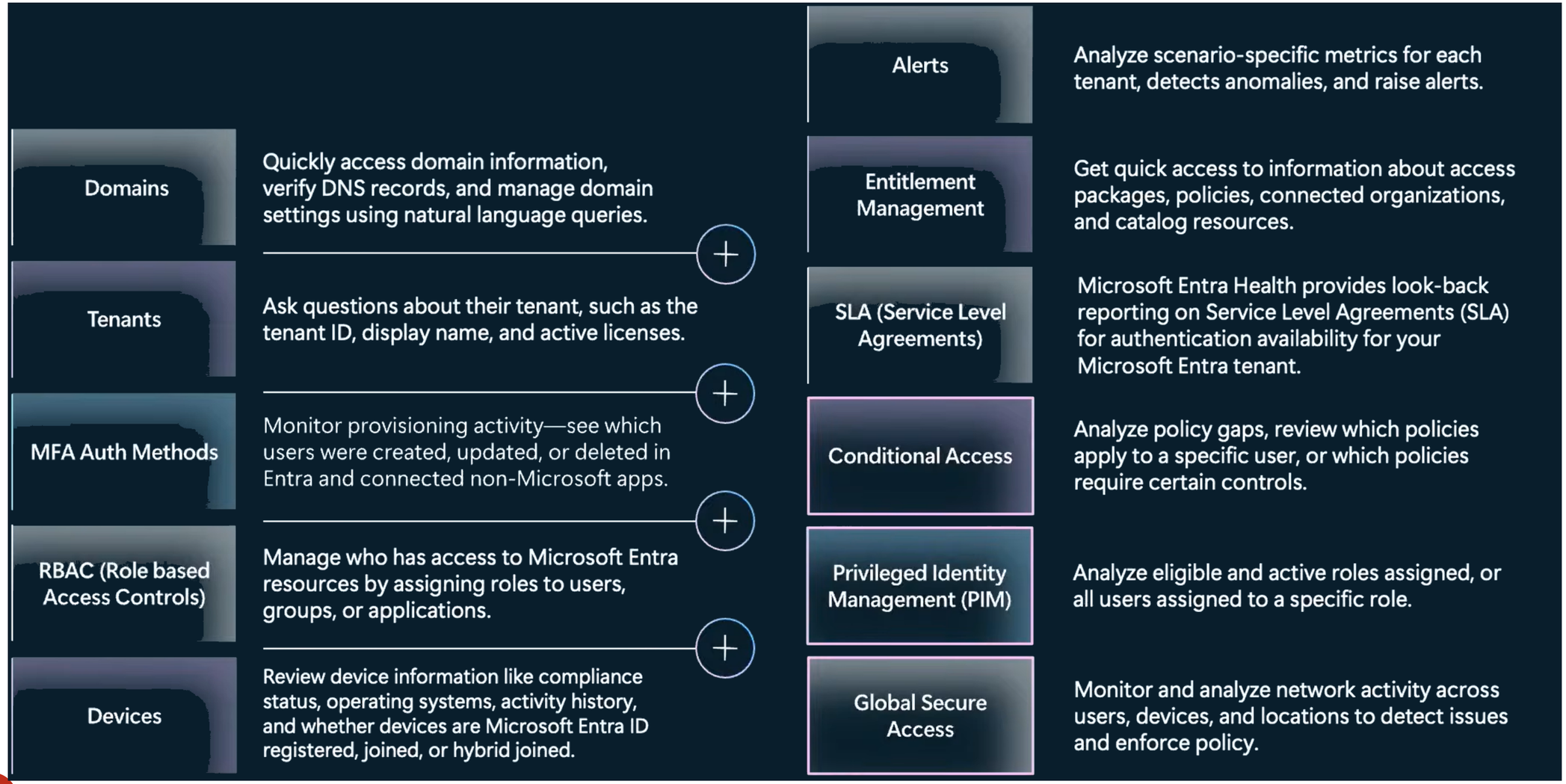
3

Execute at scale with AI agents

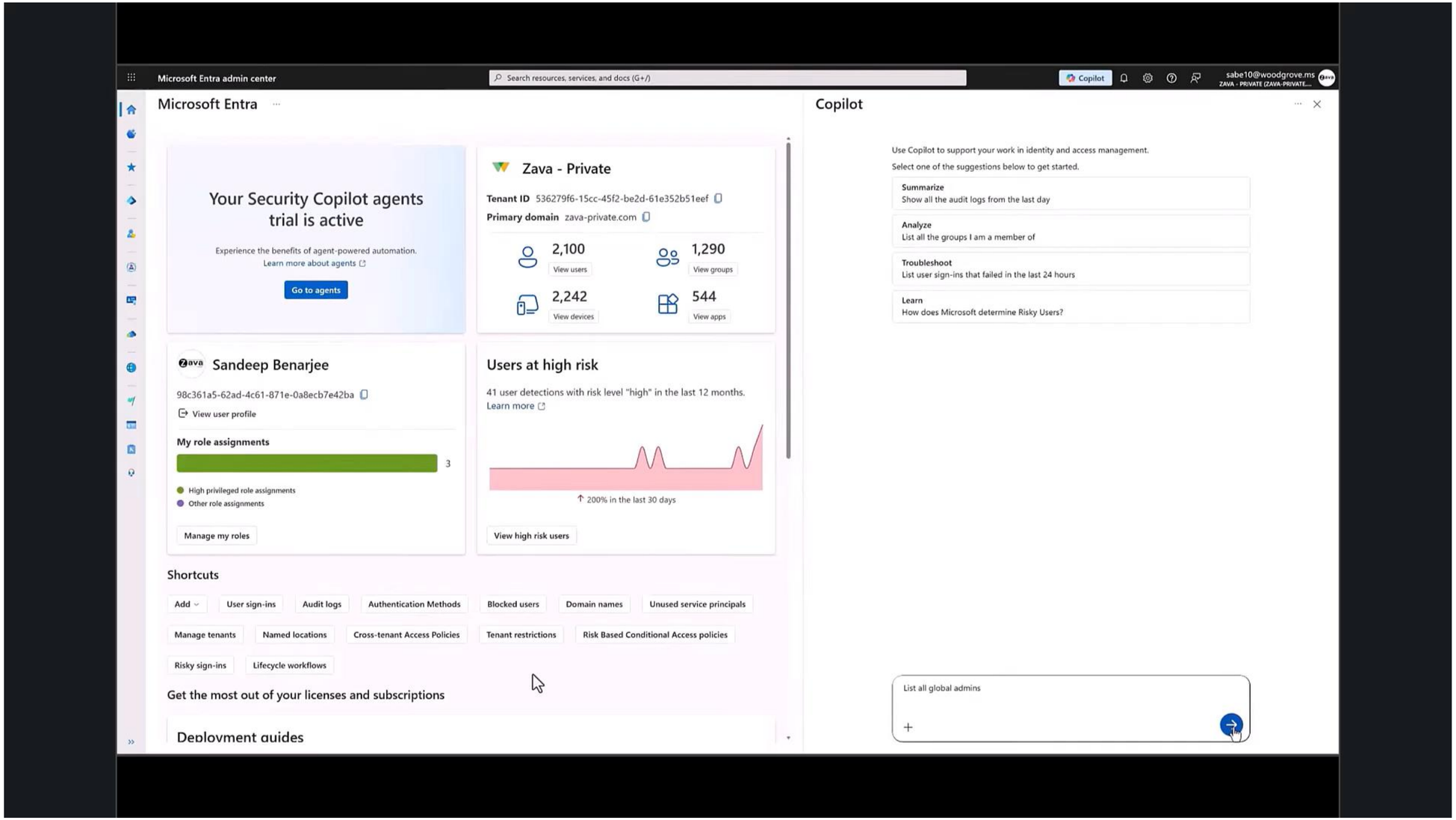
Security Copilot scenarions in Entra ID - 1

https://learn.microsoft.com/en-us/entra/security-copilot/entra-security-scenarios

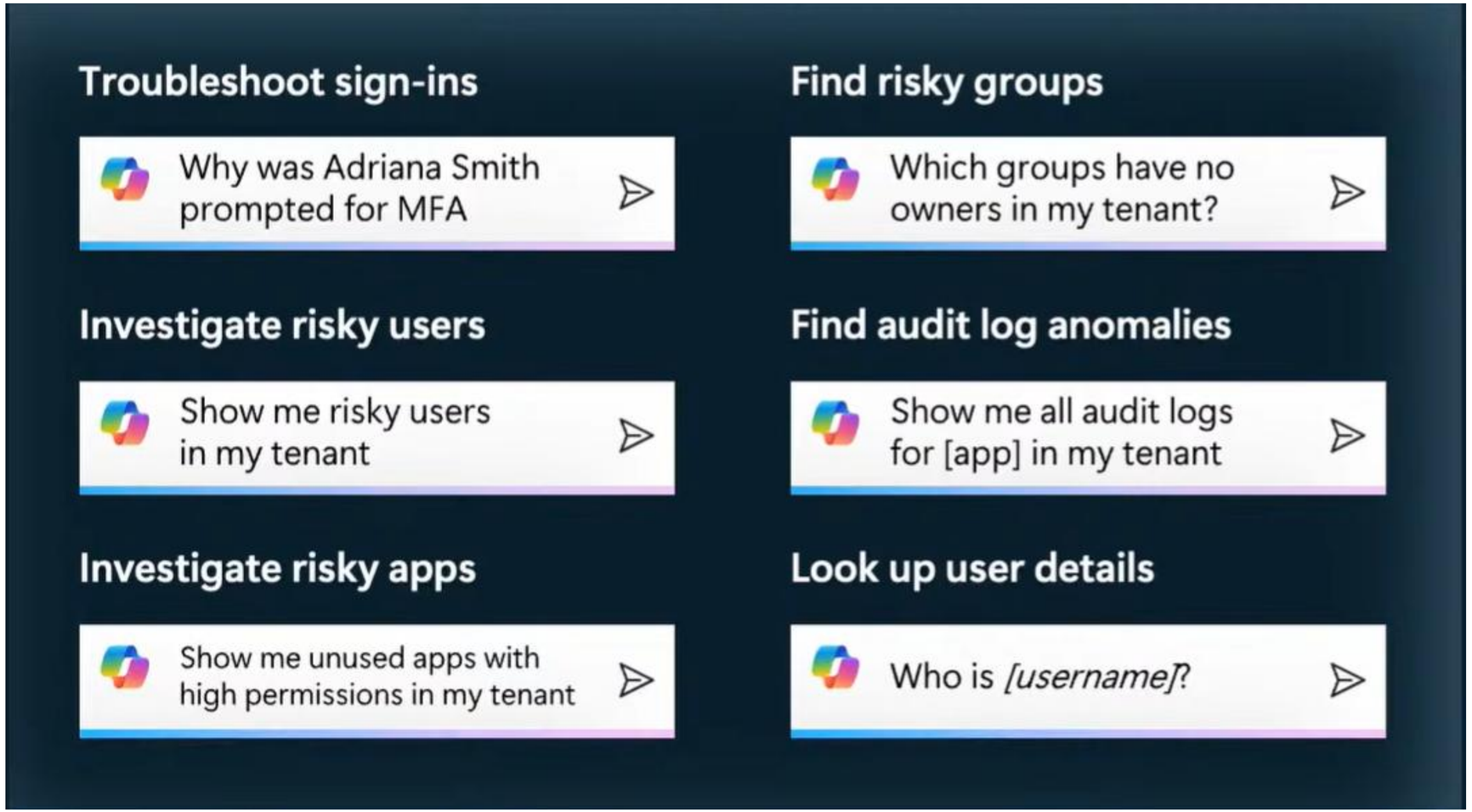
Security Copilot scenarions in Entra ID - 2



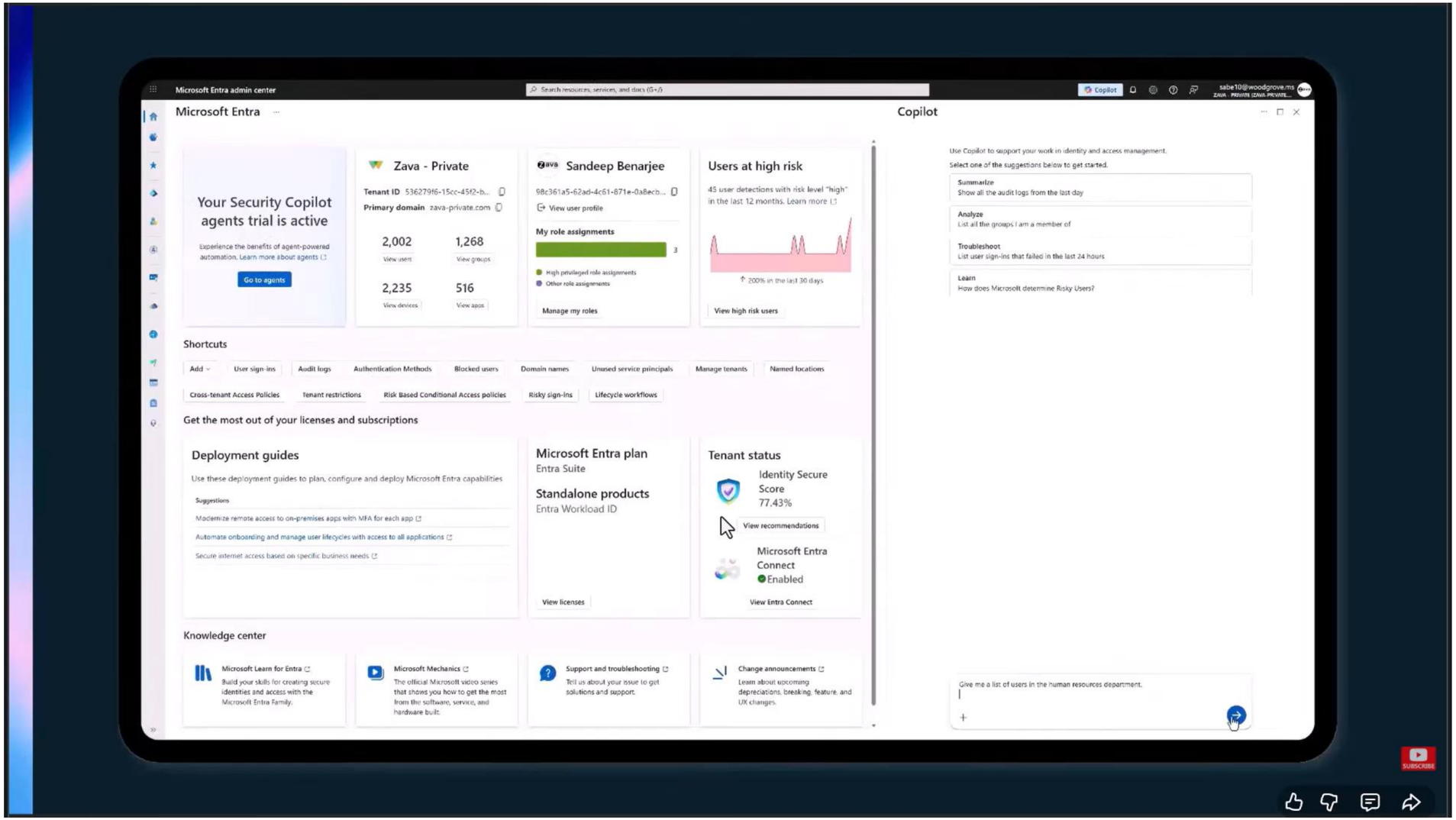
Security Copilot in Microsoft Entra

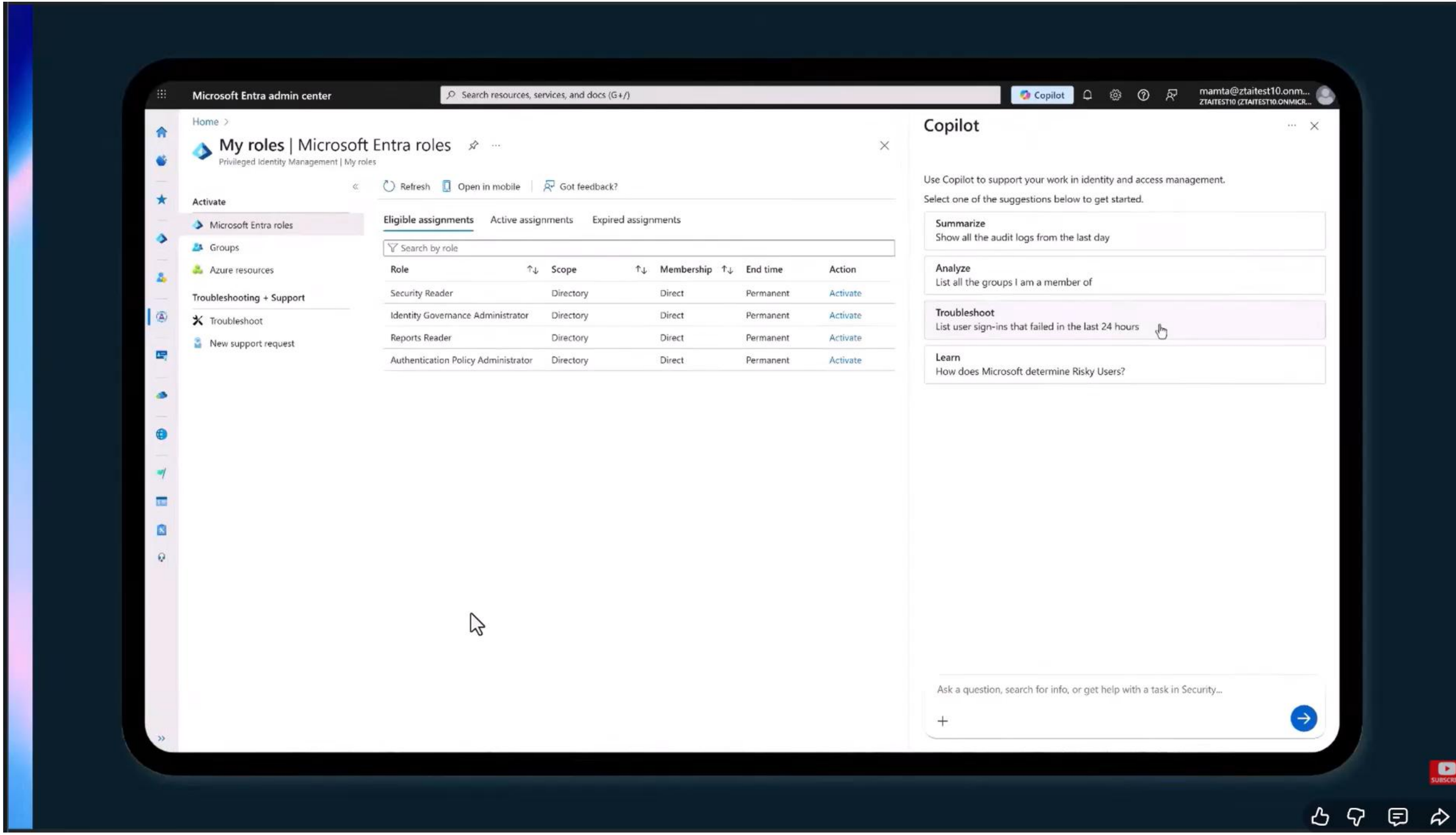


Prompt examples in Microsoft Entra



Enhanced data protection

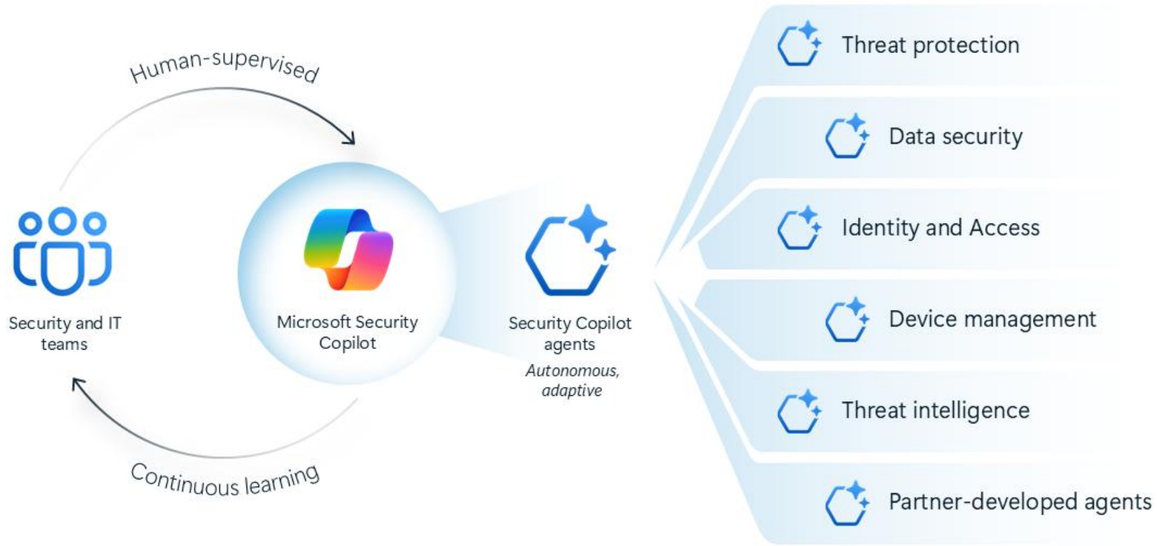



Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
mamta@ztaitest10.onm...
ZTAITEST10 (ZTAITEST10.ONMICR...
Home
My roles | Microsoft Entra roles
Privileged Identity Management | My roles
Refresh
Open in mobile
Got feedback?
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Eligible assignments
Active assignments
Expired assignments
Search by role
Role
Scope
Membership
End time
Action
Security Reader
Directory
Direct
Permanent
Activate
Identity Governance Administrator
Directory
Direct
Permanent
Activate
Reports Reader
Directory
Direct
Permanent
Activate
Authentication Policy Administrator
Directory
Direct
Permanent
Activate
Copilot
Use Copilot to support your work in identity and access management.
Select one of the suggestions below to get started.
Summarize
Show all the audit logs from the last day
Analyze
List all the groups I am a member of
Troubleshoot
List user sign-ins that failed in the last 24 hours
Learn
How does Microsoft determine Risky Users?
Ask a question, search for info, or get help with a task in Security...

Security Copilot AI Agent in Entra

Security Copilots AI Agents

- AI-powered assistants built into Microsoft Security Copilot
- Automate repetitive tasks, reduce manual workloads, and optimize security operations.
- Agents learn based on feedback and keep you in control on the actions it takes.
- Agents are available in the standalone and embedded experiences.
- Integrate seamlessly with Microsoft Security solutions and the broader supported partner ecosystem.
- Utilize security compute units (SCUs) to operate.



As organizations grow, CA policies must stay up to date

Challenge area

Identity administrators face significant challenge in designing effective access control policies to enforce least privilege at scale

Customer pain

Admins struggle to identify security gaps because of the scale and complexity of their Entra environment and Conditional Access policy set

Solution

Automatically identify new objects (users/apps) creation; analyzes CA policies to identify gaps where new objects are not protected by CA

Productivity

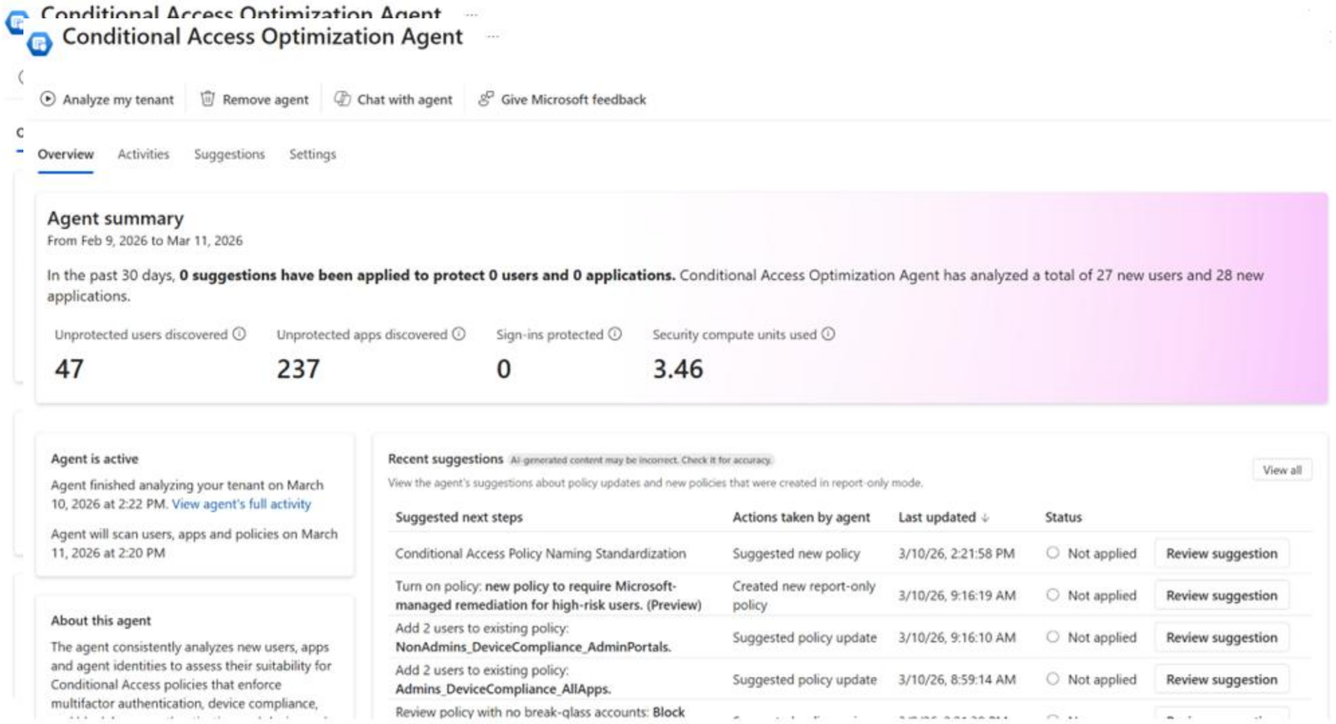
The agent priorities action to close gaps, supports snooze workflows, offers safe rollout via report-only simulation

How it’s different

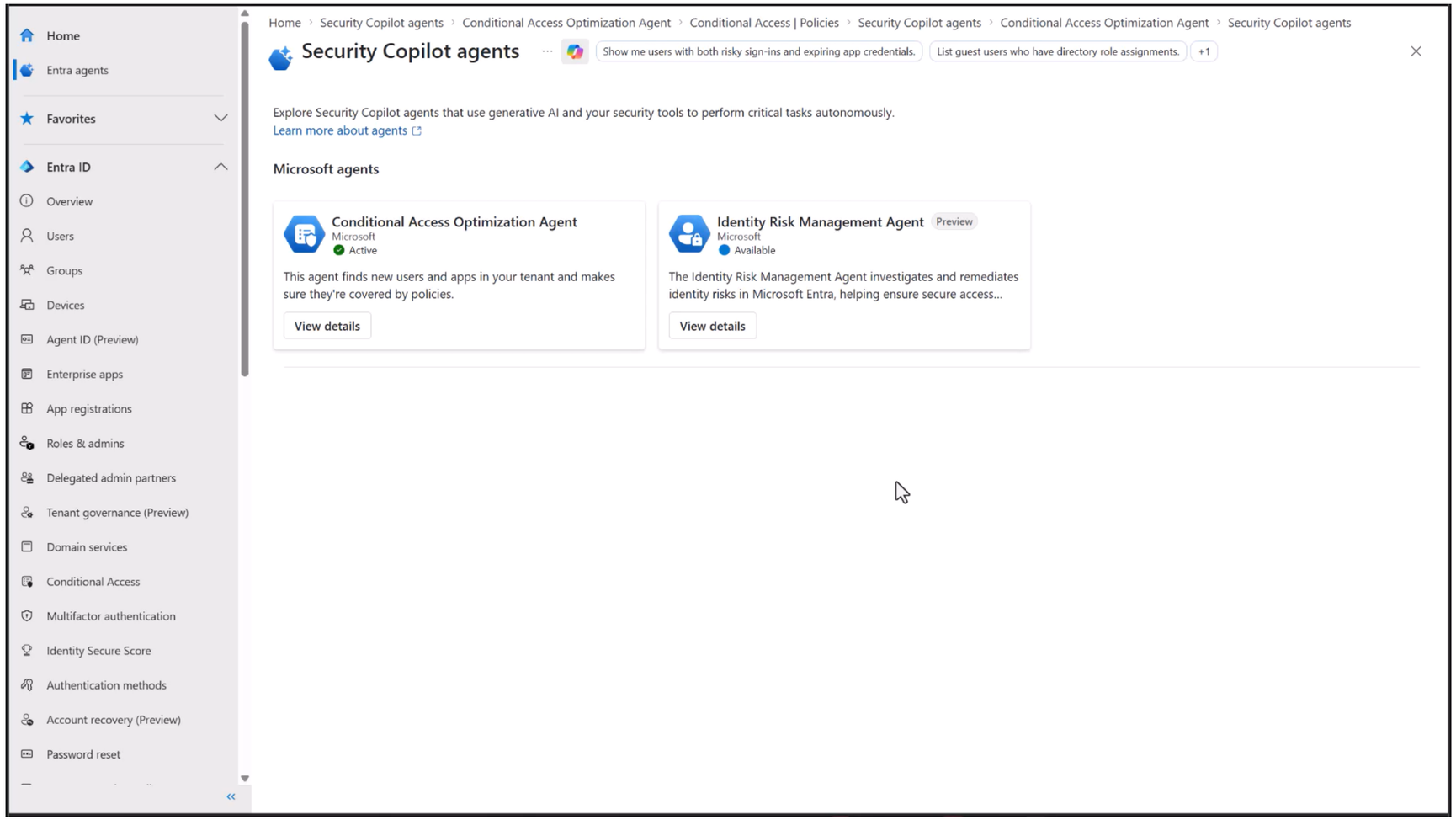
Eliminates manual cross-referencing, adds proactive drift detection, Intune-aware policy suggestions and automation to maintain

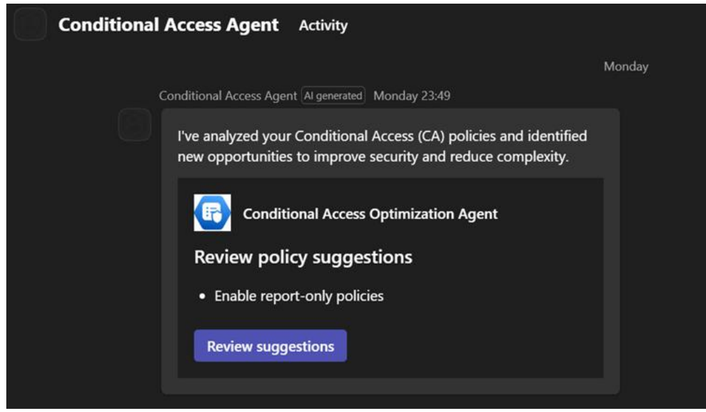
Microsoft Entra
Conditional Access Optimization Agent

- The Conditional Access optimization agent ensures all users are protected by policy.
- Autonomously identify security gaps before attacker do
- It recommends policies and changes based on best practices aligned with Zero Trust and Microsoft's learnings.
  - The agent evaluates policies requiring multifactor authentication (MFA), enforces device-based controls (device compliance, app protection policies, and Domain Joined Devices), and blocks legacy authentication and device code flow.
  - Policy consolidation.
- Scanning is limited to a 24 hour period
- The agent runs every 24 hours but can also run manually.
- Learns with customer feedback
- The agent explains every recommendation in clear and natural language
- Visual activity map

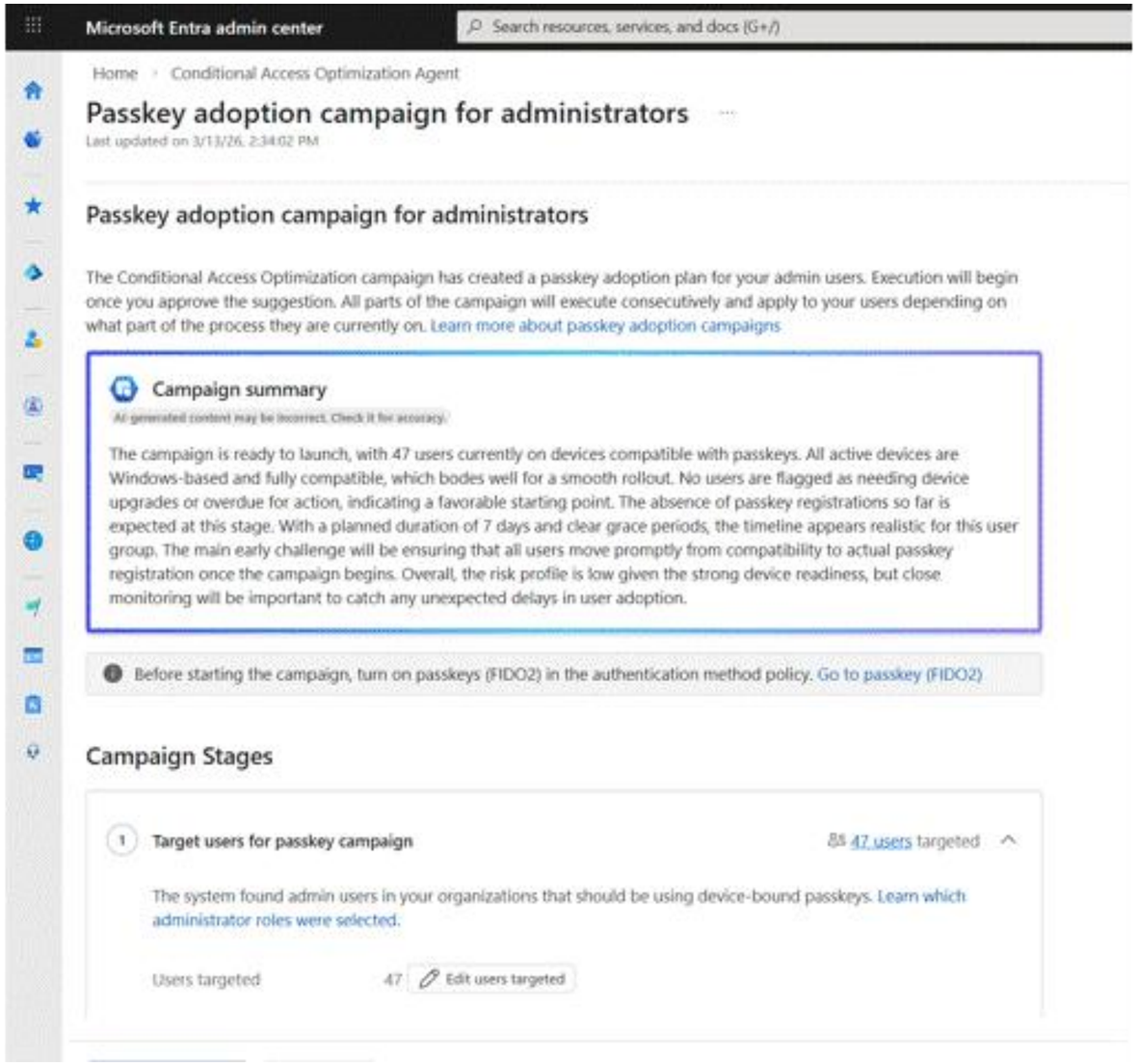


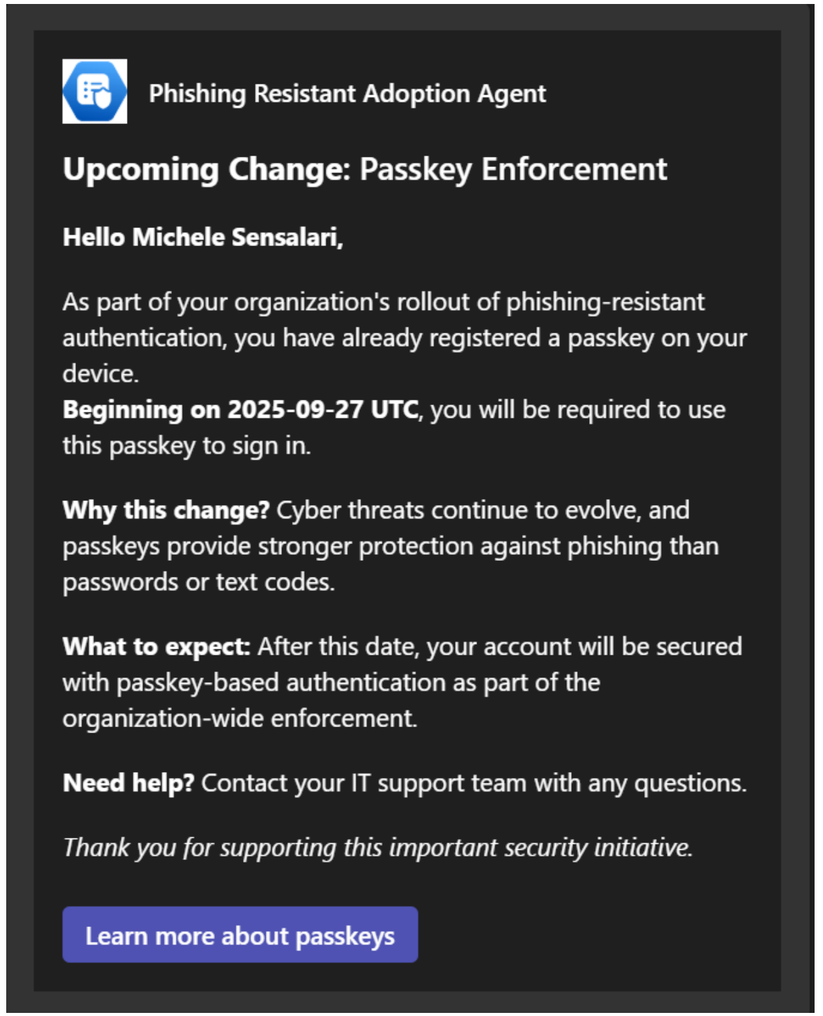
Microsoft Entra Conditional Access Optimization Agent - Demo





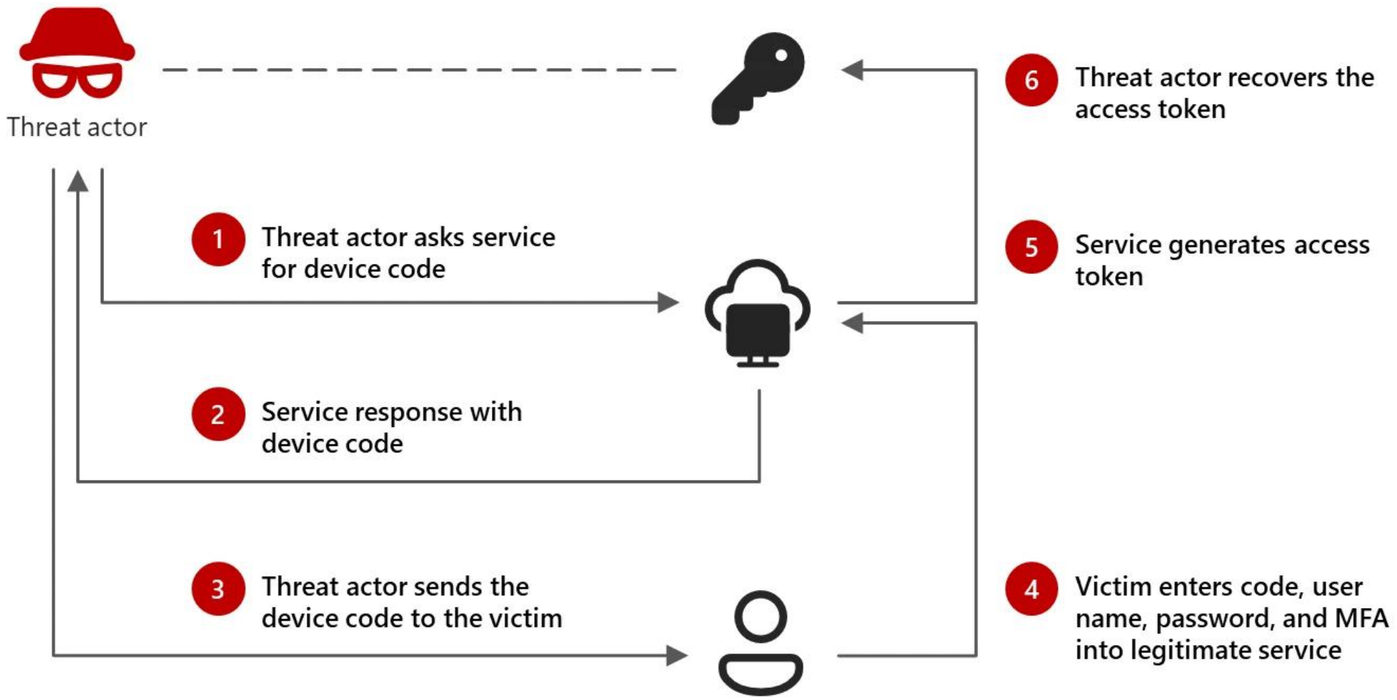
Passkey adaption campaign for administators





Phased rollout

Device Code Flow

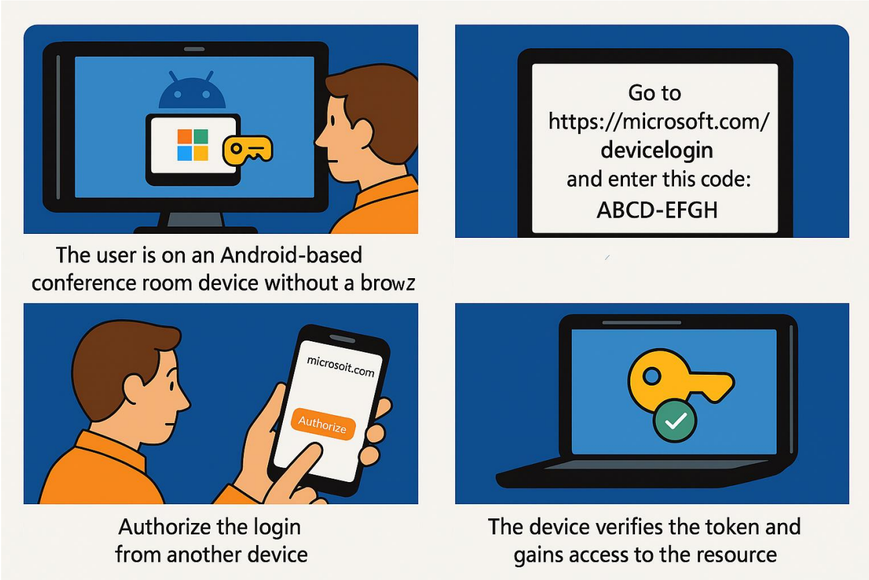


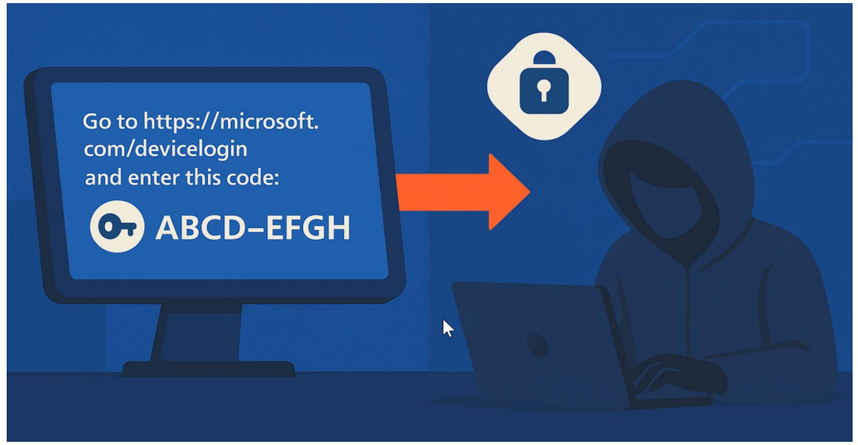
This is an OAuth flow designed for browser-less devices (TV, IoT, CLI):

- The user enters a code on a website (e.g., microsoft.com/devicelogin)
- Authentication occurs normally (MFA, passkey, etc.)
- The device receives the token

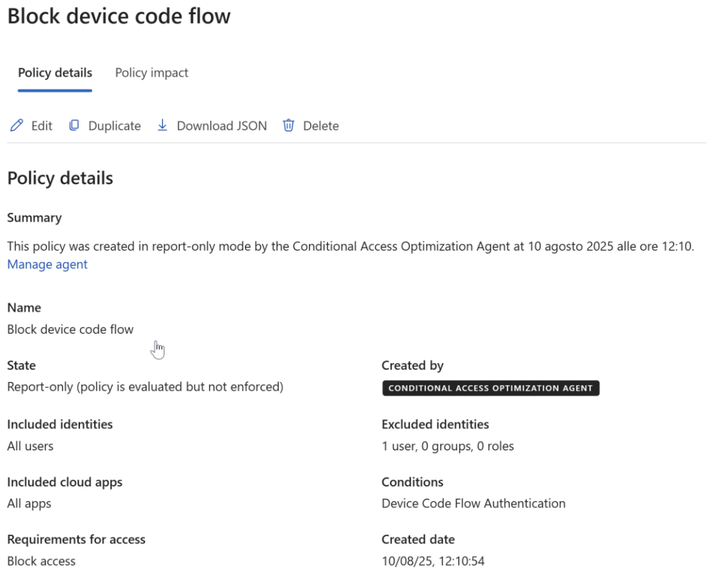
Agent AI Suggestion

Device code flow is a high-risk authentication method that can be part of a phishing attack or used to access corporate resources on unmanaged devices.





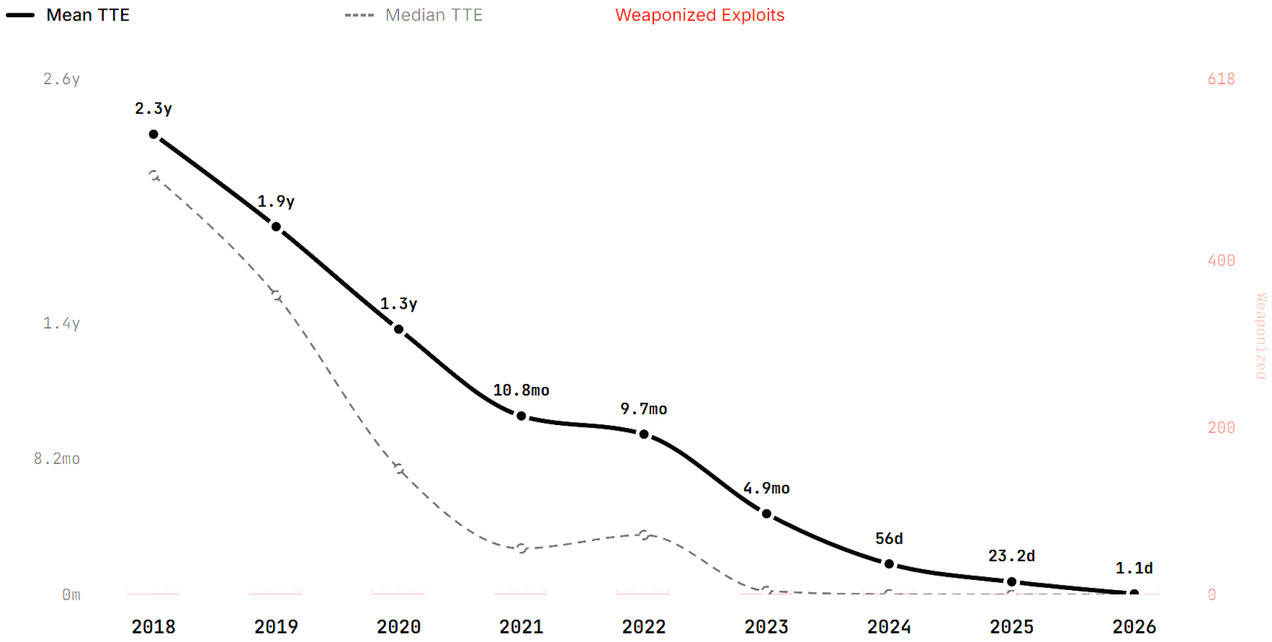
Security Copilot Agent AI Suggestion



Threat evolution

From Vulnerability to Exploitation

TTE (Time-to-Exploit) measures the gap between CVE disclosure and confirmed exploitation



Time-to-Exploit Milestones

When mean time-to-exploit crosses each threshold

1 Year	1 Month	1 Week	1 Day	1 Hour	1 Minute
REACHED	REACHED	REACHED	PROJECTED	PROJECTED	PROJECTED
~2021	~2025	~2026	~2026	~2026	~2028

Based on 3,521 CVE-exploit pairs from trusted sources (CISA KEV, VulnCheck KEV & XDB)

zerodayclock.com

#Milano

Slide e video:
https://www.globalazuremilano.it