



#Milano



Security Copilot in Microsoft Entra

Michele Sensalari

CTO @ Overnet



#Milano

improve



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

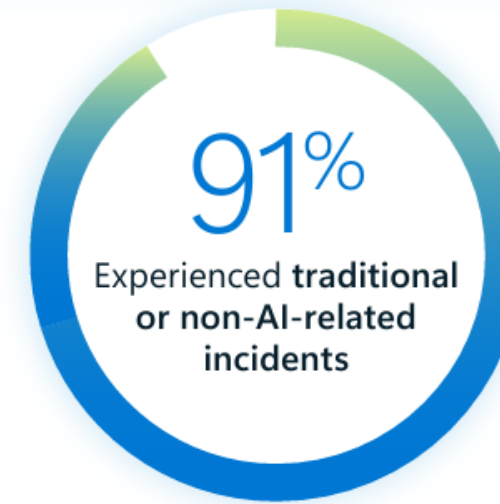
53%

vs

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Outdated or unpatched systems	24%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%

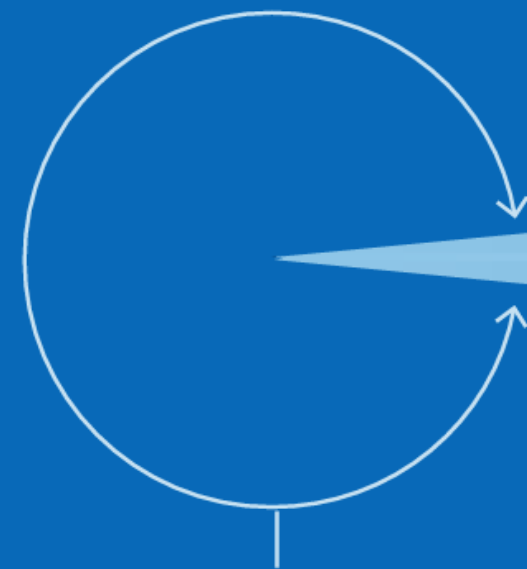


Identity, access, and the cybercrime economy

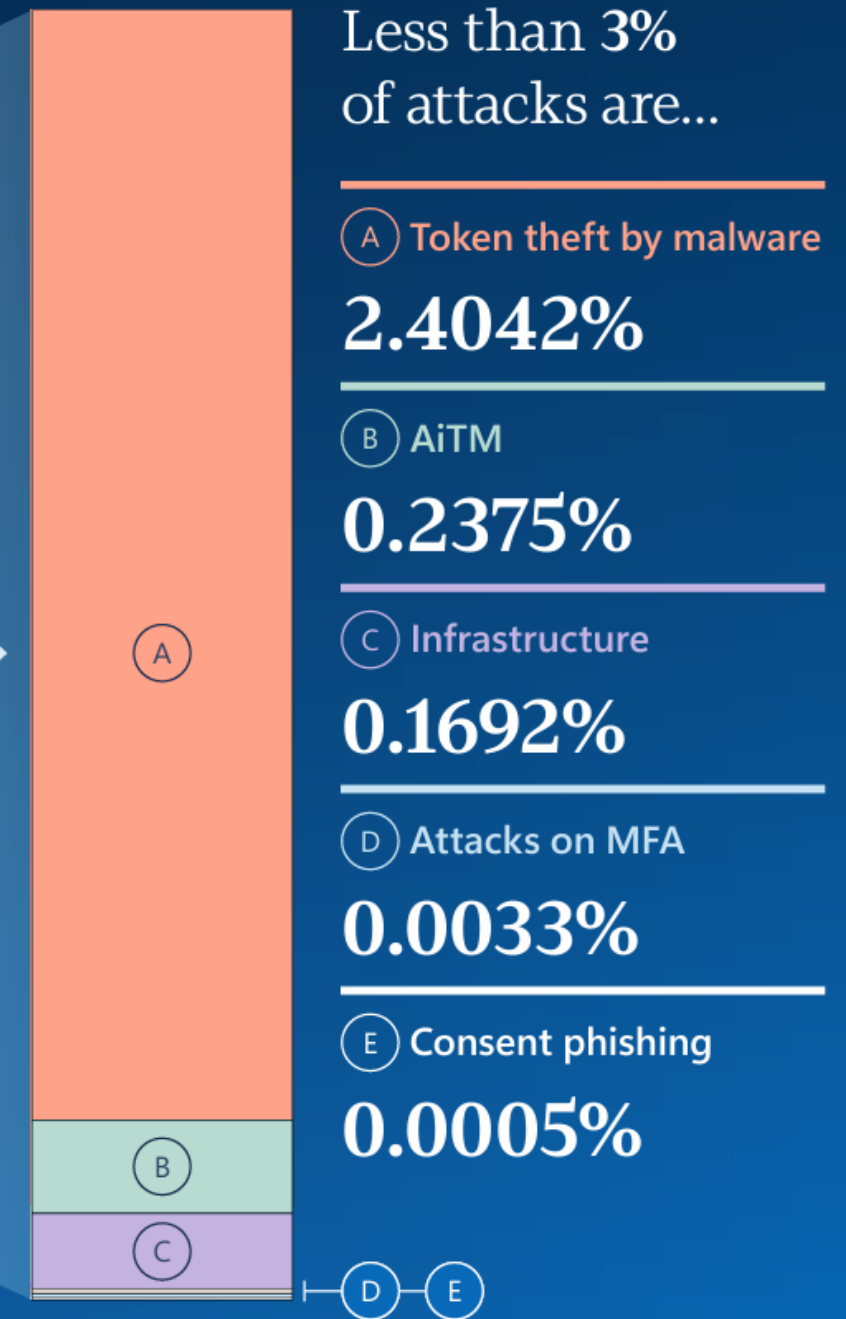
Identity attacks in perspective

Modern multifactor authentication still reduces the risk of identity compromise by more than **99%**.

While attacks against identity infrastructure (such as Microsoft Entra, Okta, Identity Provider (IdP), and hybrid components) are still limited in volume and are rare relative to other attacks, their variety is increasing. Novel attacks are continually being discovered, often targeting on-premises to cloud vertical attack paths.



More than **97%** of identity attacks are password spray or brute force attacks



Less than 3% of attacks are...

(A) Token theft by malware

2.4042%

(B) AiTM

0.2375%

(C) Infrastructure

0.1692%

(D) Attacks on MFA

0.0033%

(E) Consent phishing

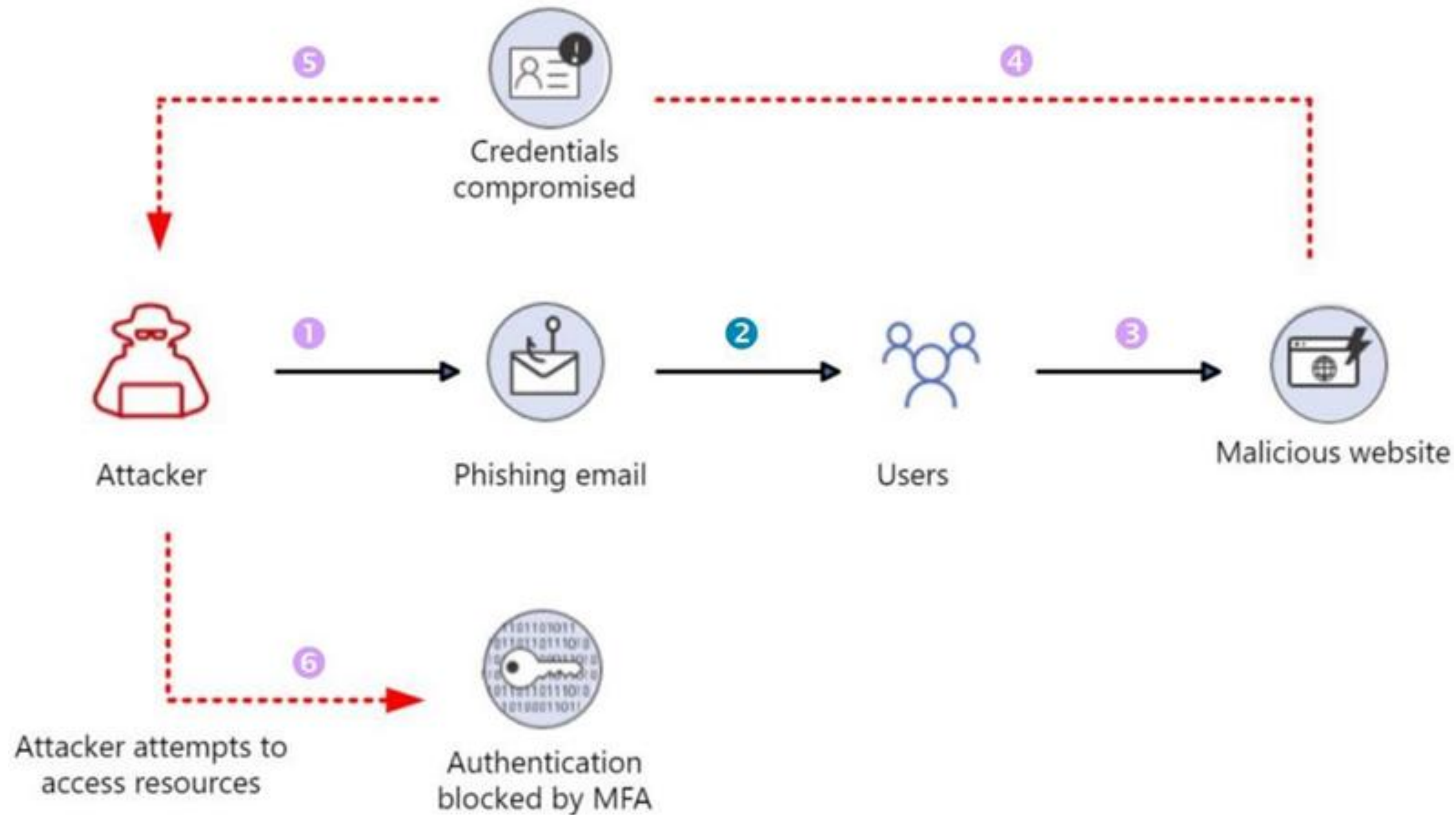
0.0005%

Source: Microsoft Defender XDR and Entra ID Protection alerts (April-June 2025)

Login compromise



Typical credential attacks happen before a token is issued



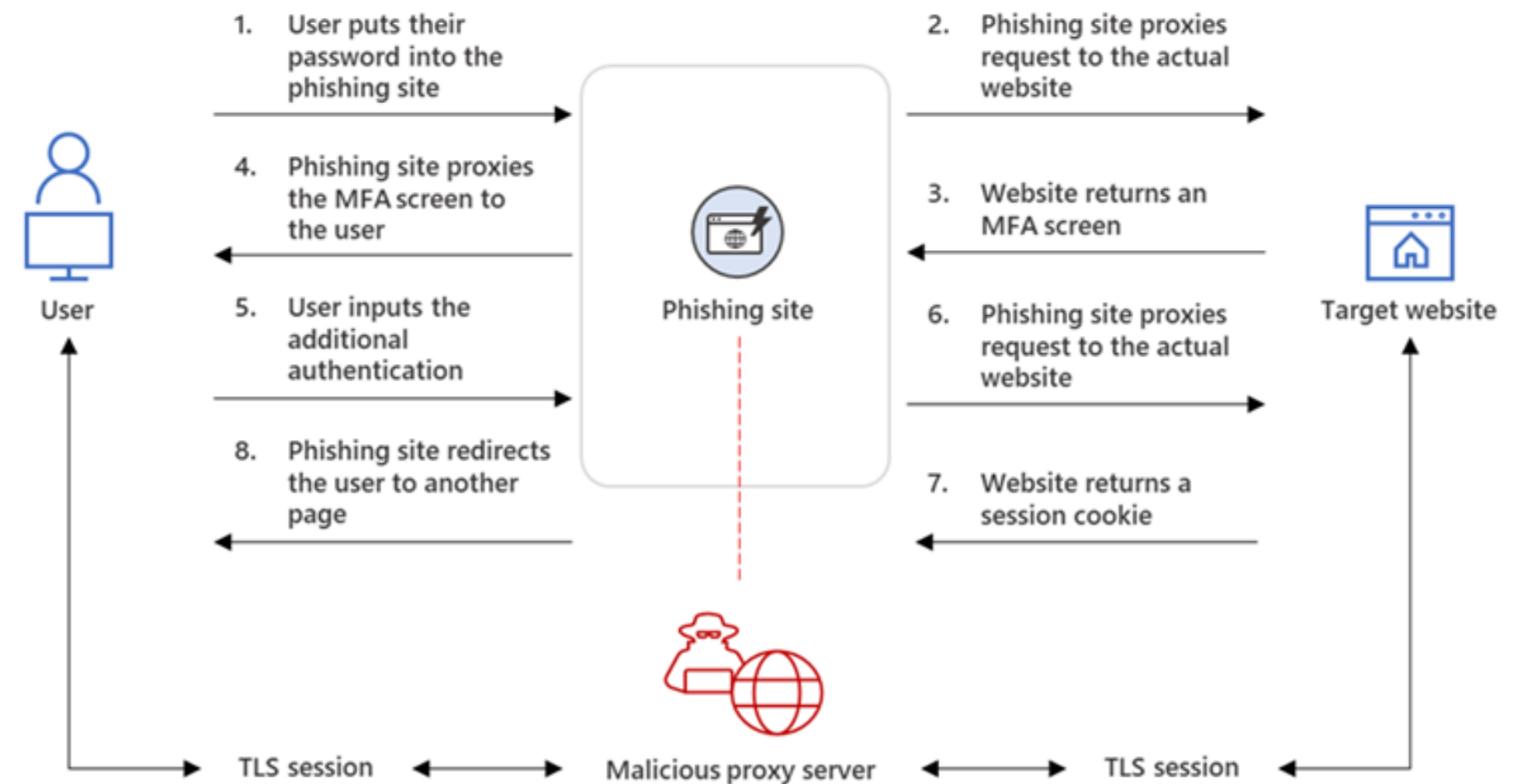
Enforce use of Conditional Access Policies



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

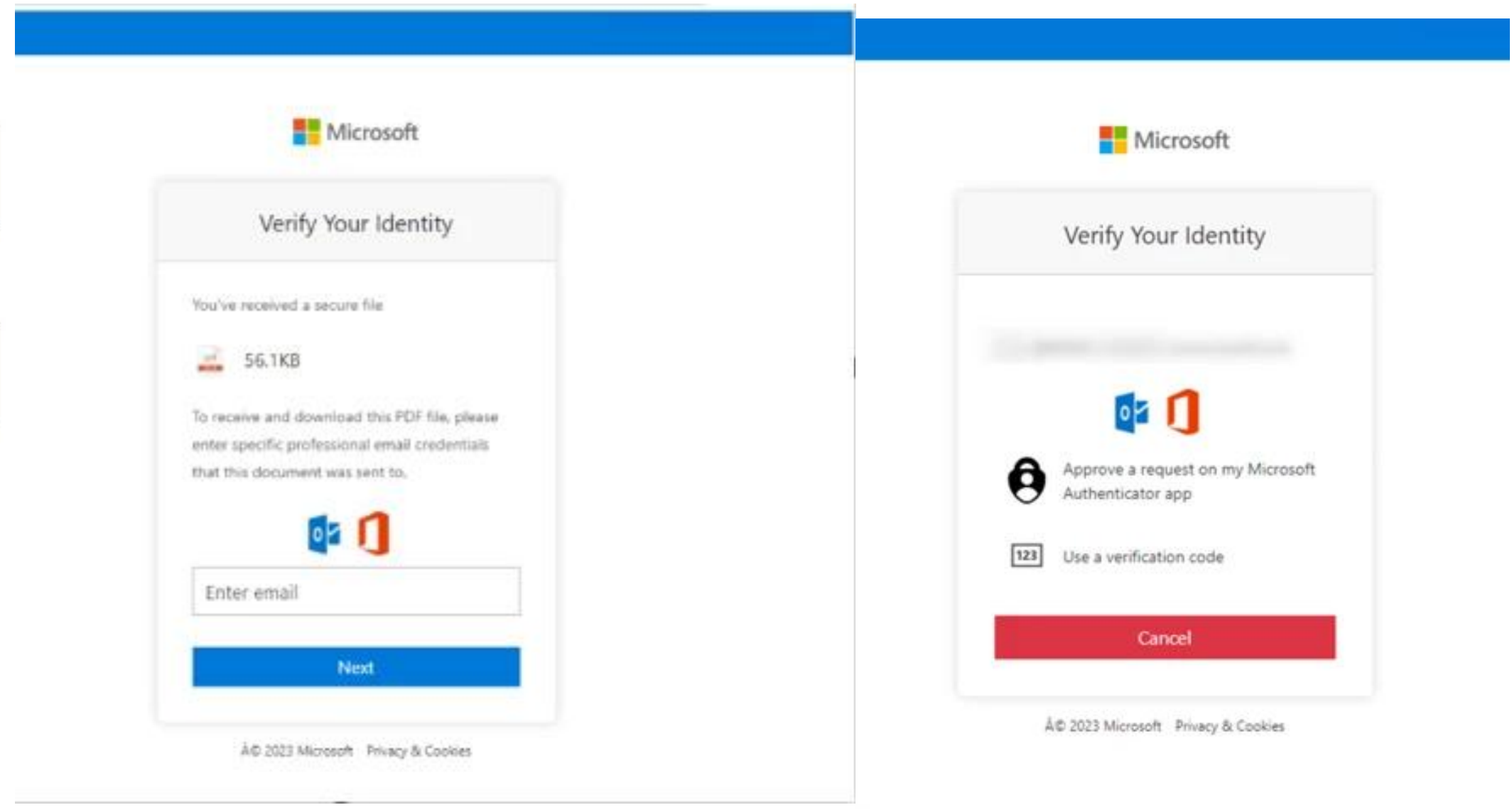
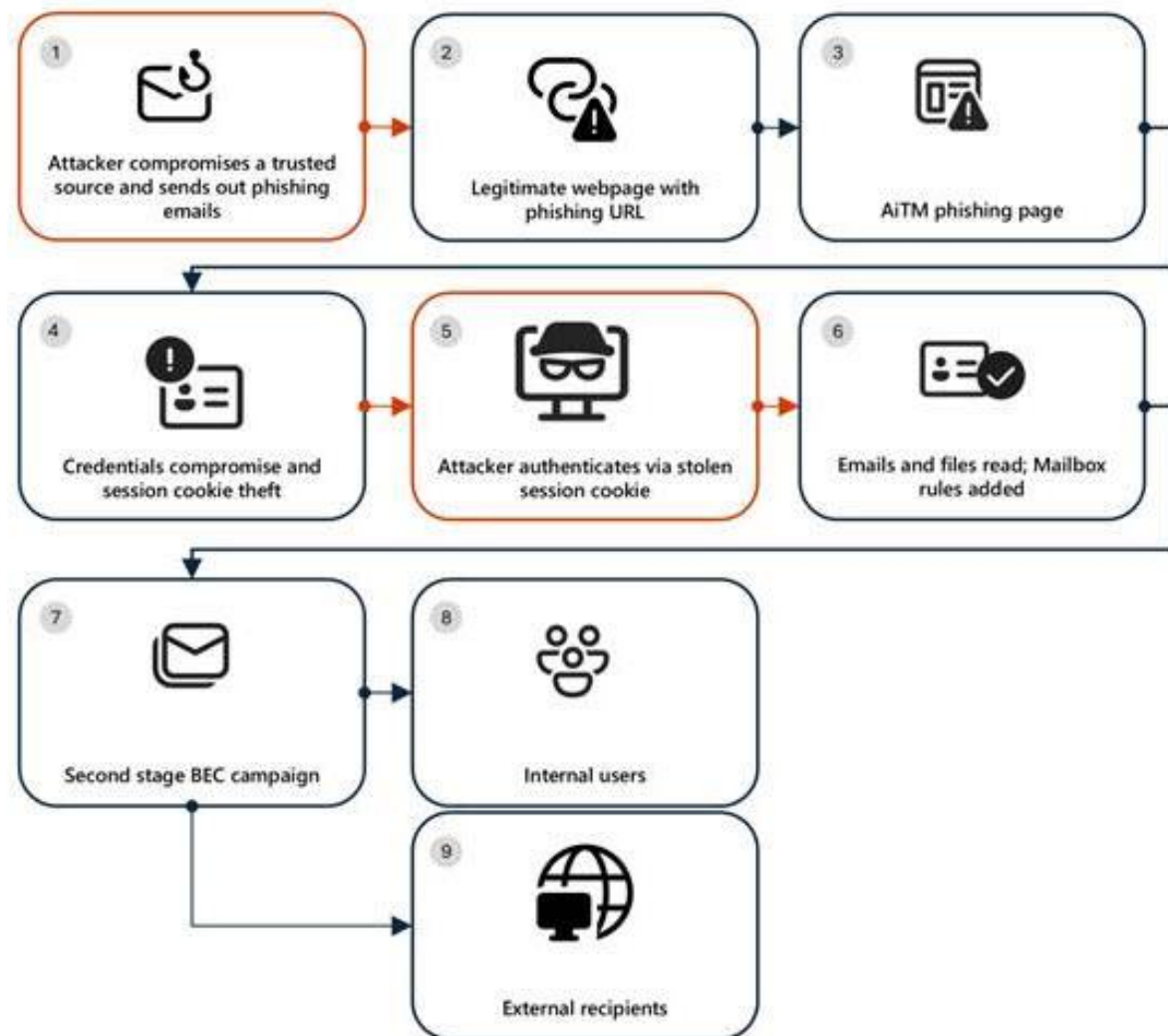


- Adversary in the middle phishing is an increasingly common tactic used by threat actors to steal both credentials and session cookies
- A user is sent a phishing link, when they click on the link, they are presented a website masquerading as a legitimate site. The user then enters their credentials, 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



Password to passkey



passkey

pass·key | \ 'pas-, kē \

A replacement for passwords that is a **more secure, easier, and a faster method** to sign in to websites and applications

A phishing resistant, WebAuthn credential, that is **usable across all your devices**

A **consumer-friendly and enterprise grade solution** that can be synced to allow secure passwordless sign-in across a device ecosystem, or be device-bound for access on a single machine

- **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

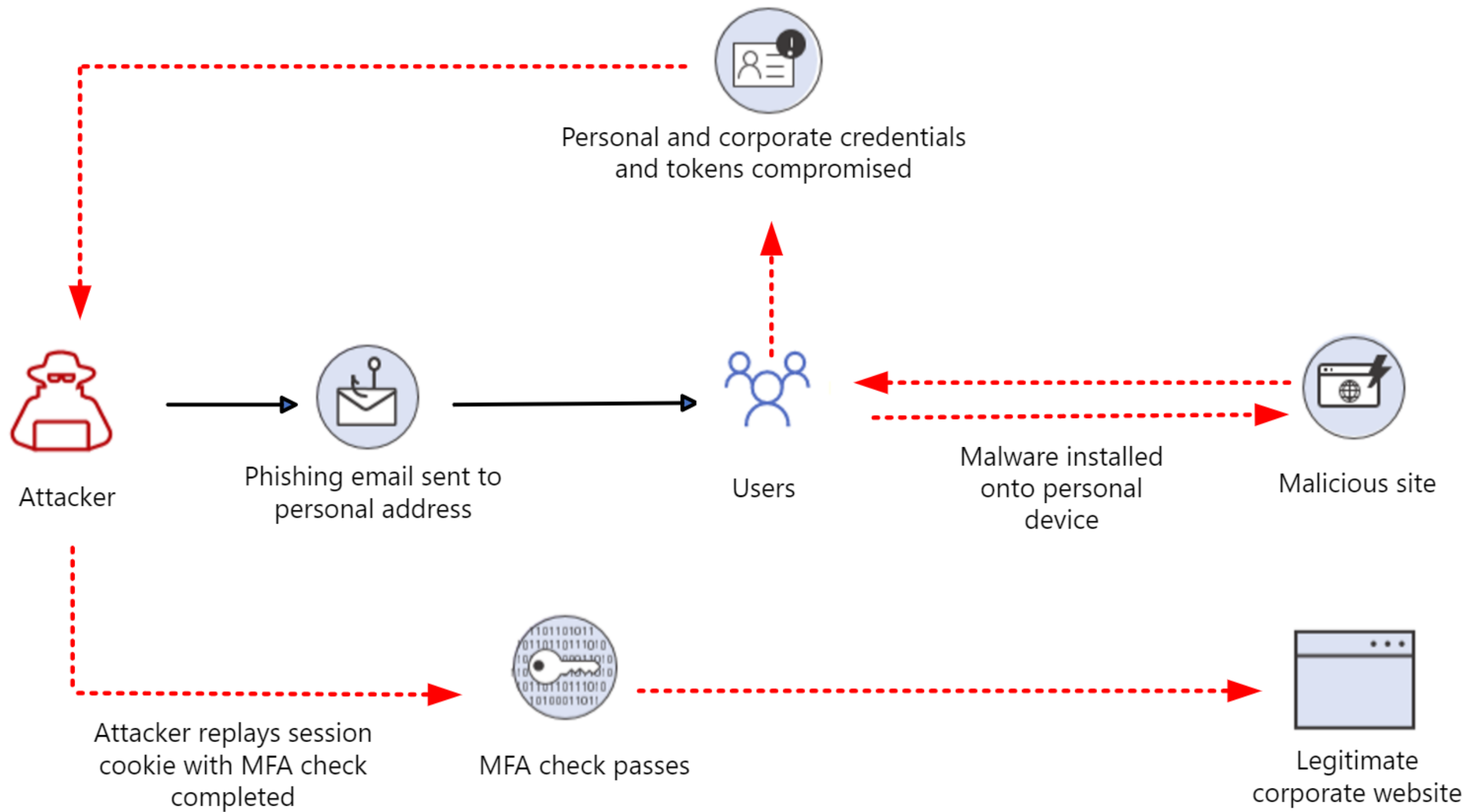
Each authentication is unique and non-replayable

Prevents interception and reuse


Token Theft



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

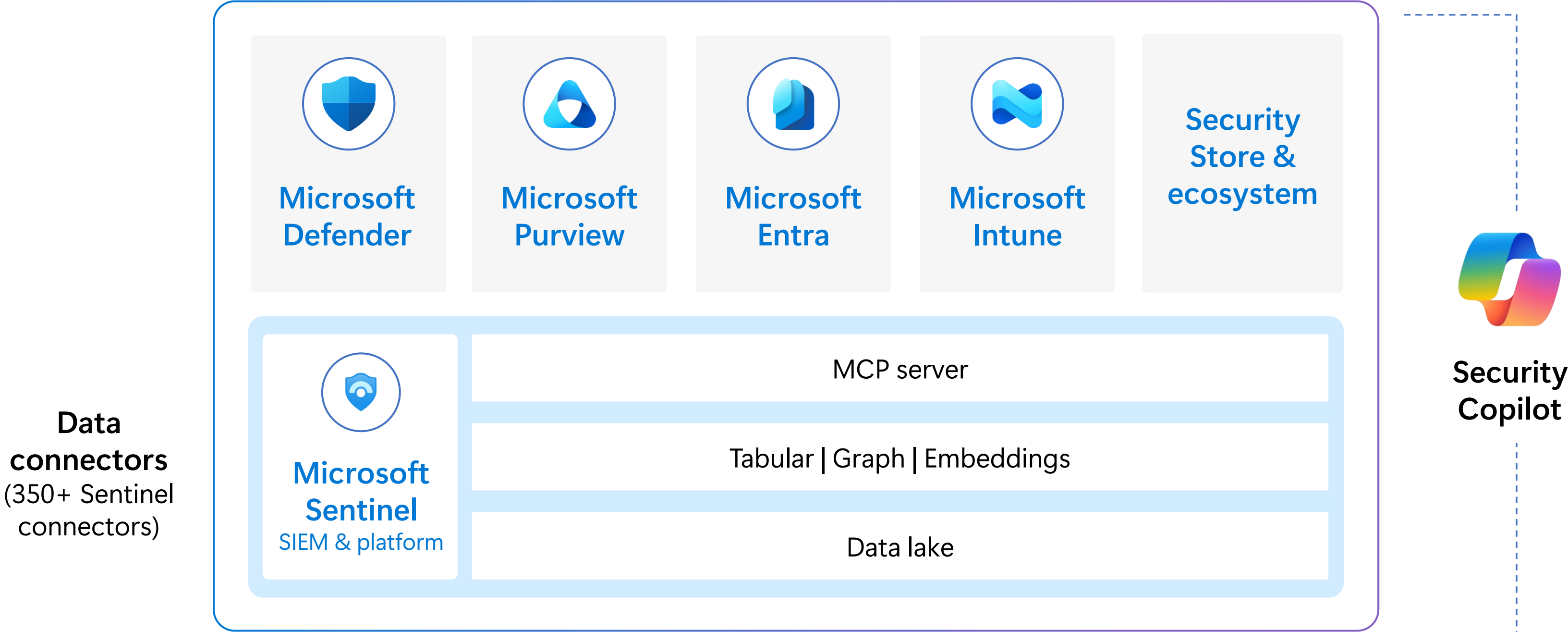
What is Security Copilot?



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



Microsoft Security Ecosystem



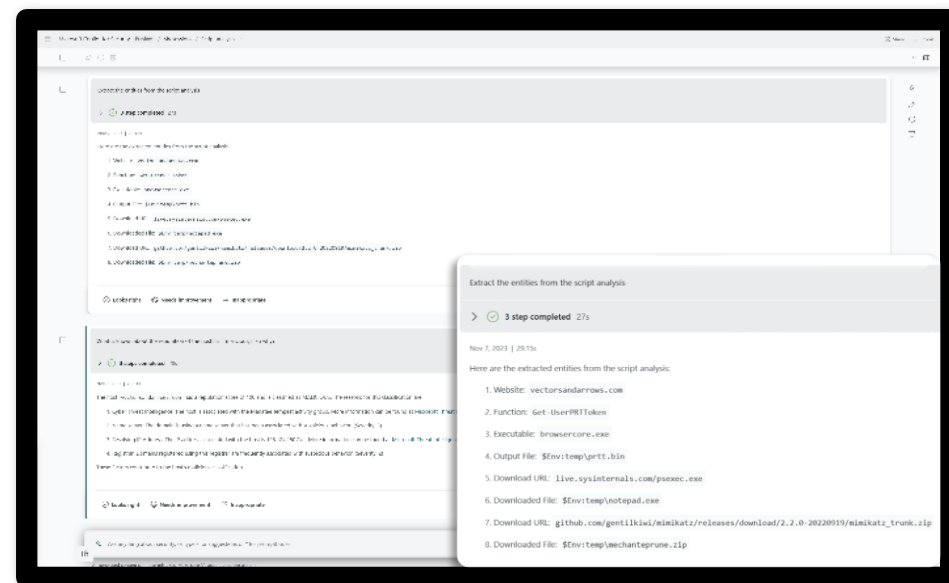
Multicloud and multiplatform

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.

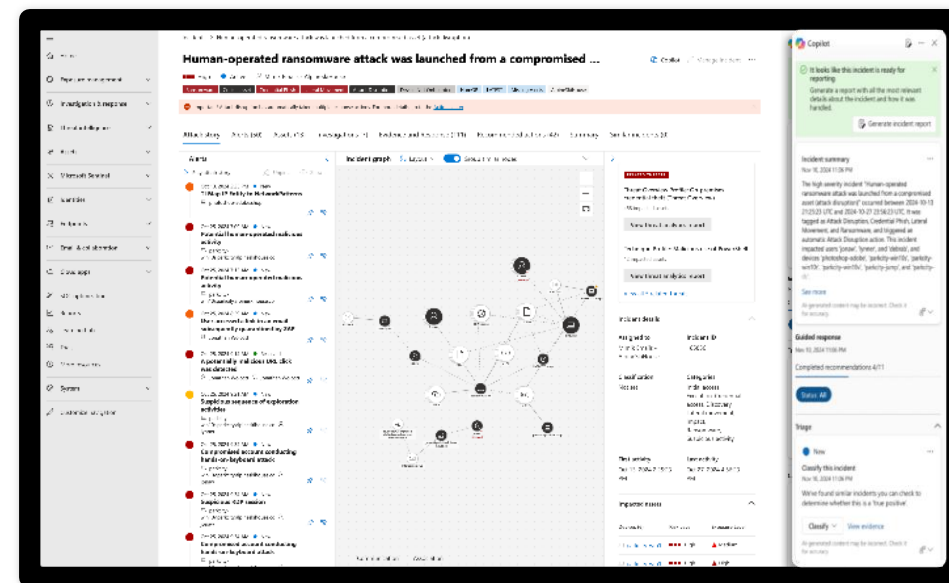
Standalone

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



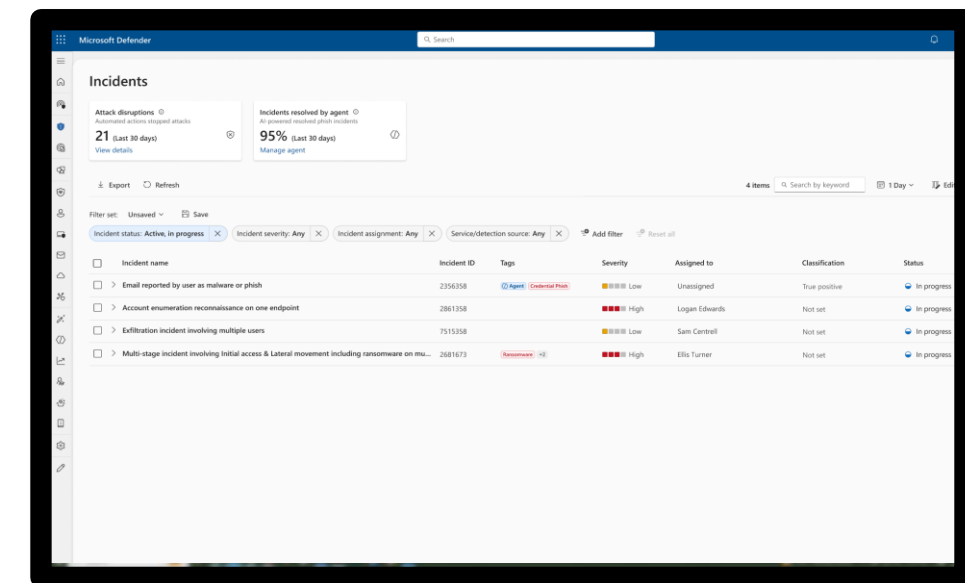
Embedded

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 scenarios in Entra ID - 1



Risky Users	Analyze risky users and query their detection type, risk state, risky level.		Audit Logs	Investigate audit logs for provisioning, creation, updating, deletion users/apps/groups.
Sign In Logs	Investigate sign in logs for failed/interrupted/successful sign ins and query the auth methods, CA policies applied during sign ins.	+	Lifecycle Workflows	Investigate about joiner/leaver lifecycle workflows.
Access Reviews	Monitor access reviews.	+	Groups	Analyze group information like members, owners, security enabled, etc.
Entra ID Recommendations	Review security and health recommendations across Secure Score, apps, Conditional Access, and configurations.	+	Users	Investigate user information like their manager details, office location, groups, etc.
License Usage	Check assigned licenses and roles and investigate overall license usage across your tenant.	+	App Risk	Check for unused/risky service principals.

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

Security Copilot scenarios in Entra ID - 2



Security Copilot in Microsoft Entra



The screenshot displays the Microsoft Entra admin center interface. The main content area is divided into several sections:

- Your Security Copilot agents trial is active:** A blue banner with the text "Experience the benefits of agent-powered automation. Learn more about agents" and a "Go to agents" button.
- Zava - Private:** A summary card for the tenant. It includes:
 - Tenant ID: 536279f6-15cc-45f2-be2d-61e352b51eef
 - Primary domain: zava-private.com
 - Metrics: 2,100 users (View users), 1,290 groups (View groups), 2,242 devices (View devices), and 544 apps (View apps).
- Sandeep Benarjee:** A user profile card with ID 98c361a5-62ad-4c61-871e-0a8ecb7e42ba, a "View user profile" link, and a "My role assignments" section showing 3 assignments (3 high privileged, 0 other). A "Manage my roles" button is at the bottom.
- Users at high risk:** A card indicating "41 user detections with risk level 'high' in the last 12 months." It features a line graph showing a 200% increase in the last 30 days and a "View high risk users" button.
- Shortcuts:** A grid of buttons for quick navigation: User sign-ins, Audit logs, Authentication Methods, Blocked users, Domain names, Unused service principals, Manage tenants, Named locations, Cross-tenant Access Policies, Tenant restrictions, Risk Based Conditional Access policies, Risky sign-ins, and Lifecycle workflows.
- Deployment guides:** A section titled "Get the most out of your licenses and subscriptions" with a "Deployment guides" link.

On the right side, a **Copilot** chat window is open. It contains the following text and suggestions:













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?

At the bottom of the Copilot window, there is a text input field with the placeholder "List all global admins" and a blue arrow button.

Prompt examples in Microsoft Entra



Troubleshoot sign-ins	Find risky groups
 Why was Adriana Smith prompted for MFA 	 Which groups have no owners in my tenant? 
Investigate risky users	Find audit log anomalies
 Show me risky users in my tenant 	 Show me all audit logs for [app] in my tenant 
Investigate risky apps	Look up user details
 Show me unused apps with high permissions in my tenant 	 Who is [username]? 

Enhanced data protection



The screenshot displays the Microsoft Entra admin center interface. The main dashboard includes several key sections:

- Your Security Copilot agents trial is active:** A notification box with a "Go to agents" button.
- Zava - Private:** Tenant information including Tenant ID (536279f6-15cc-45f2-b...) and Primary domain (zava-private.com). Metrics show 2,002 users, 1,268 groups, 2,235 devices, and 516 apps.
- Sandeep Benarjee:** User profile card showing role assignments, including high privileged role assignments.
- Users at high risk:** A chart showing 45 user detections with a risk level of "high" in the last 12 months, with a 200% increase in the last 30 days.
- Shortcuts:** A row of navigation buttons for User sign-ins, Audit logs, Authentication Methods, Blocked users, Domain names, Unused service principals, Manage tenants, and Named locations.
- Deployment guides:** A section for planning, configuring, and deploying Microsoft Entra capabilities.
- Microsoft Entra plan:** Information about the current plan (Entra Suite) and standalone products (Entra Workload ID).
- Tenant status:** A card showing the Identity Secure Score (77.43%) and the status of Microsoft Entra Connect (Enabled).
- Knowledge center:** A grid of links to Microsoft Learn for Entra, Microsoft Mechanics, support and troubleshooting, and change announcements.

On the right side, the Copilot interface is visible, providing suggestions for actions such as "Summarize", "Analyze", "Troubleshoot", and "Learn". At the bottom right, there is a text input field with the prompt "Give me a list of users in the human resources department." and a "SUBSCRIBE" button.

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

mamta@ztatest10.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...

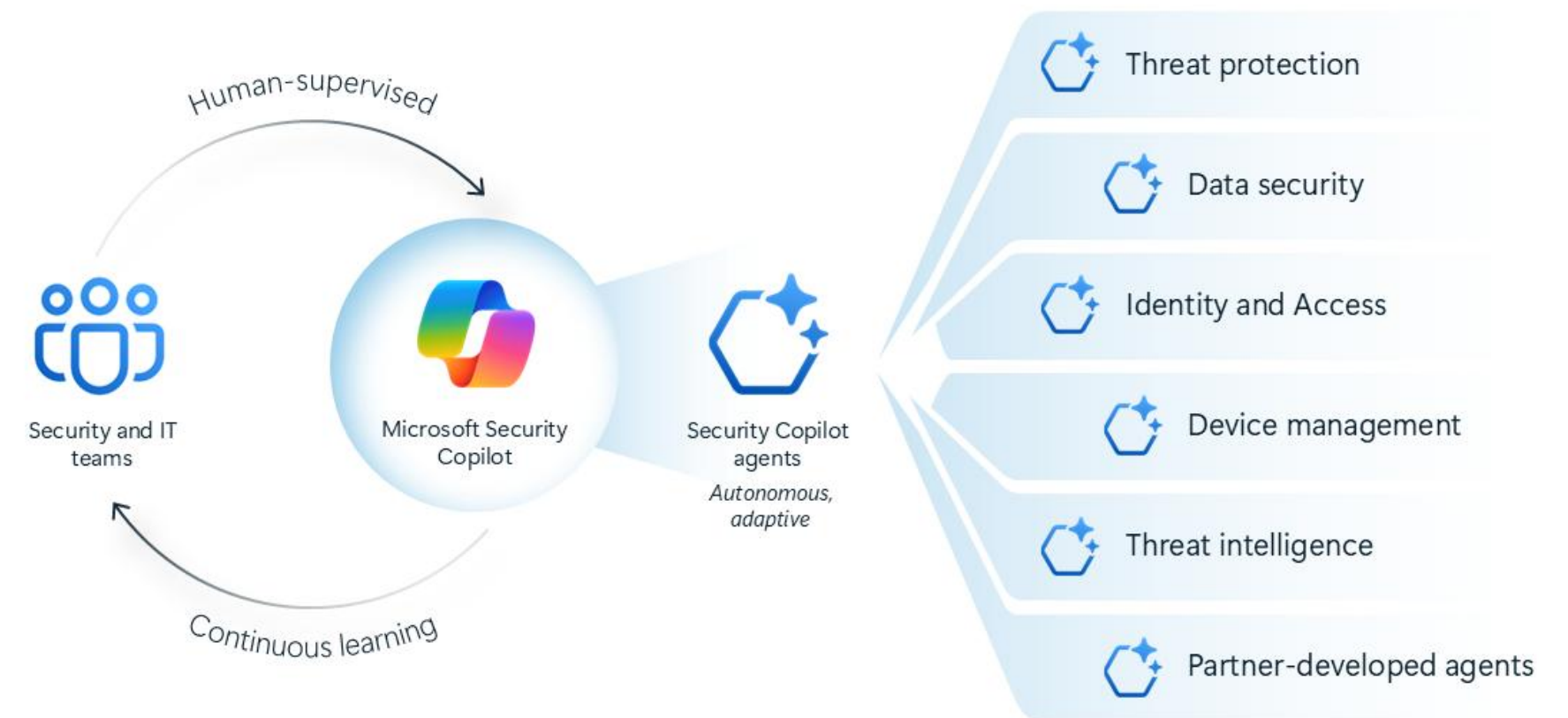


Security Copilot AI Agent in Entra

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

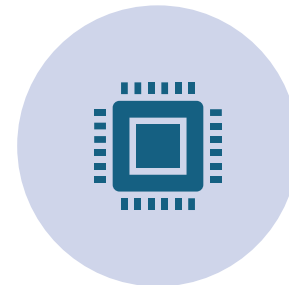


Challenge area



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 prioritizes 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

The screenshot shows the Microsoft Entra Conditional Access Optimization Agent dashboard. At the top, there are navigation options: 'Analyze my tenant', 'Remove agent', 'Chat with agent', and 'Give Microsoft feedback'. Below this is a navigation menu with 'Overview', 'Activities', 'Suggestions', and 'Settings'. The main content area is titled 'Agent summary' and covers the period from Feb 9, 2026 to Mar 11, 2026. It states: 'In the past 30 days, 0 suggestions have been applied to protect 0 users and 0 applications. Conditional Access Optimization Agent has analyzed a total of 27 new users and 28 new applications.' Below this, there are four metrics: 'Unprotected users discovered' (47), 'Unprotected apps discovered' (237), 'Sign-ins protected' (0), and 'Security compute units used' (3.46). There are also sections for 'Agent is active' (showing analysis on March 10, 2026) and 'Recent suggestions' (listing various policy updates and actions taken by the agent).

Suggested next steps	Actions taken by agent	Last updated ↓	Status
Conditional Access Policy Naming Standardization	Suggested new policy	3/10/26, 2:21:58 PM	<input type="radio"/> Not applied Review suggestion
Turn on policy: new policy to require Microsoft-managed remediation for high-risk users. (Preview)	Created new report-only policy	3/10/26, 9:16:19 AM	<input type="radio"/> Not applied Review suggestion
Add 2 users to existing policy: NonAdmins_DeviceCompliance_AdminPortals.	Suggested policy update	3/10/26, 9:16:10 AM	<input type="radio"/> Not applied Review suggestion
Add 2 users to existing policy: Admins_DeviceCompliance_AllApps.	Suggested policy update	3/10/26, 8:59:14 AM	<input type="radio"/> Not applied Review suggestion
Review policy with no break-glass accounts: Block			

Microsoft Entra Conditional Access Optimization Agent - Demo



Home > Security Copilot agents > Conditional Access Optimization Agent > Conditional Access | Policies > Security Copilot agents > Conditional Access Optimization Agent > Security Copilot agents

Security Copilot agents

Show me users with both risky sign-ins and expiring app credentials. List guest users who have directory role assignments. +1

Explore Security Copilot agents that use generative AI and your security tools to perform critical tasks autonomously.
[Learn more about agents](#)

Microsoft agents

Conditional Access Optimization Agent
Microsoft
Active
This agent finds new users and apps in your tenant and makes sure they're covered by policies.
[View details](#)

Identity Risk Management Agent Preview
Microsoft
Available
The Identity Risk Management Agent investigates and remediates identity risks in Microsoft Entra, helping ensure secure access...
[View details](#)

Conditional Access Agent Activity

Monday

Conditional Access Agent AI generated Monday 23:49

I've analyzed your Conditional Access (CA) policies and identified new opportunities to improve security and reduce complexity.

Conditional Access Optimization Agent
Review policy suggestions

- Enable report-only policies

[Review suggestions](#)

Passkey adaption campaign for administrators



Microsoft Entra admin center Search resources, services, and docs (G+/f)

Home > Conditional Access Optimization Agent

Passkey adoption campaign for administrators

Last updated on 3/13/26, 2:34:02 PM

Passkey adoption campaign for administrators

The Conditional Access Optimization campaign has created a passkey adoption plan for your admin users. Execution will begin once you approve the suggestion. All parts of the campaign will execute consecutively and apply to your users depending on what part of the process they are currently on. [Learn more about passkey adoption campaigns](#).

Campaign summary

All generated content may be incorrect. Check it for accuracy.

The campaign is ready to launch, with 47 users currently on devices compatible with passkeys. All active devices are Windows-based and fully compatible, which bodes well for a smooth rollout. No users are flagged as needing device upgrades or overdue for action, indicating a favorable starting point. The absence of passkey registrations so far is expected at this stage. With a planned duration of 7 days and clear grace periods, the timeline appears realistic for this user group. The main early challenge will be ensuring that all users move promptly from compatibility to actual passkey registration once the campaign begins. Overall, the risk profile is low given the strong device readiness, but close monitoring will be important to catch any unexpected delays in user adoption.

Before starting the campaign, turn on passkeys (FIDO2) in the authentication method policy. [Go to passkey \(FIDO2\)](#)

Campaign Stages

- 1 Target users for passkey campaign** 88 47 users targeted

The system found admin users in your organizations that should be using device-bound passkeys. [Learn which administrator roles were selected.](#)

Users targeted: 47 [Edit users targeted](#)



Phishing Resistant Adoption Agent

Upcoming Change: Passkey Enforcement

Hello Michele Sensalari,

As part of your organization's rollout of phishing-resistant authentication, you have already registered a passkey on your device.

Beginning on 2025-09-27 UTC, you will be required to use this passkey to sign in.

Why this change? Cyber threats continue to evolve, and passkeys provide stronger protection against phishing than passwords or text codes.

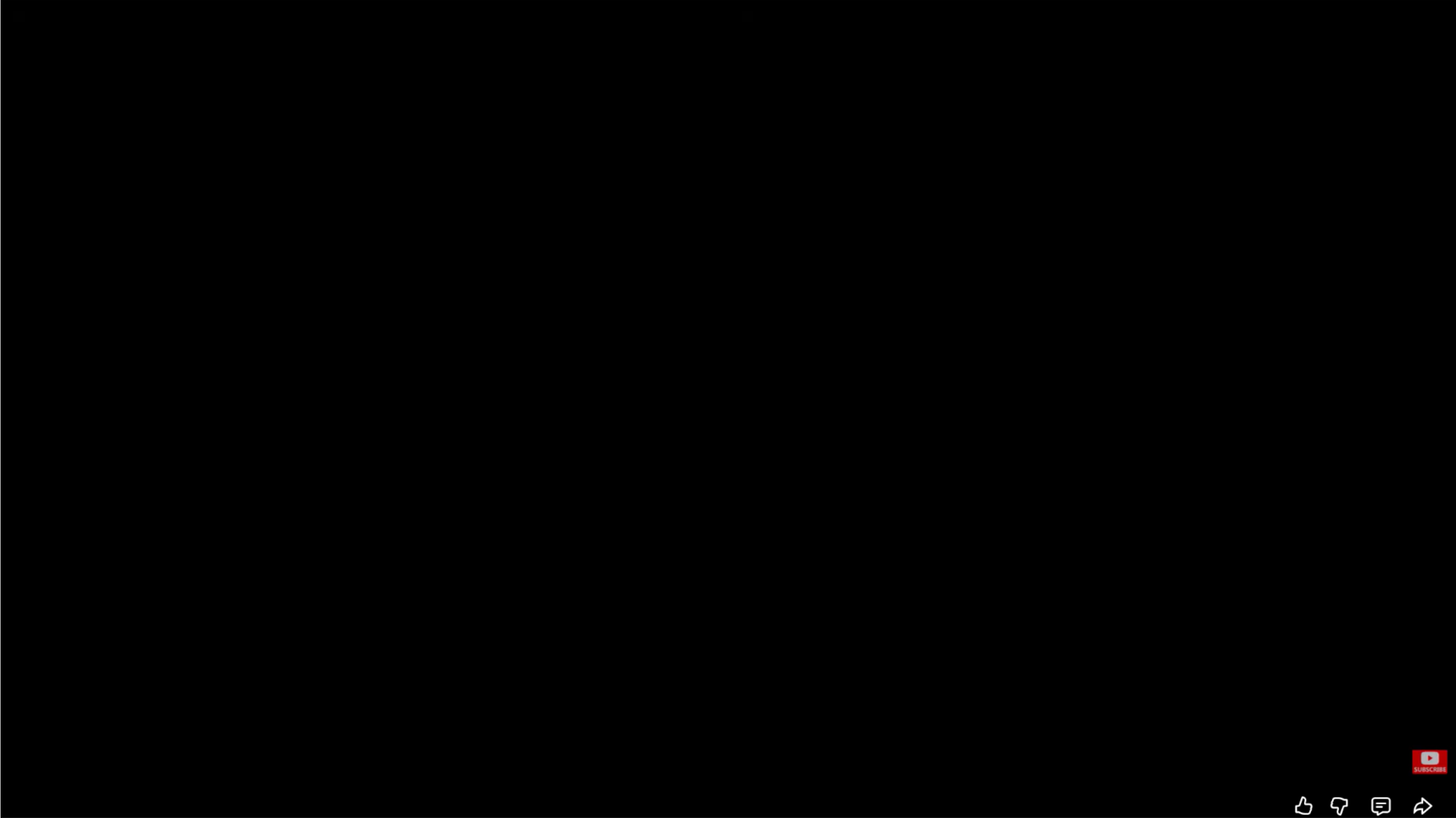
What to expect: After this date, your account will be secured with passkey-based authentication as part of the organization-wide enforcement.

Need help? Contact your IT support team with any questions.

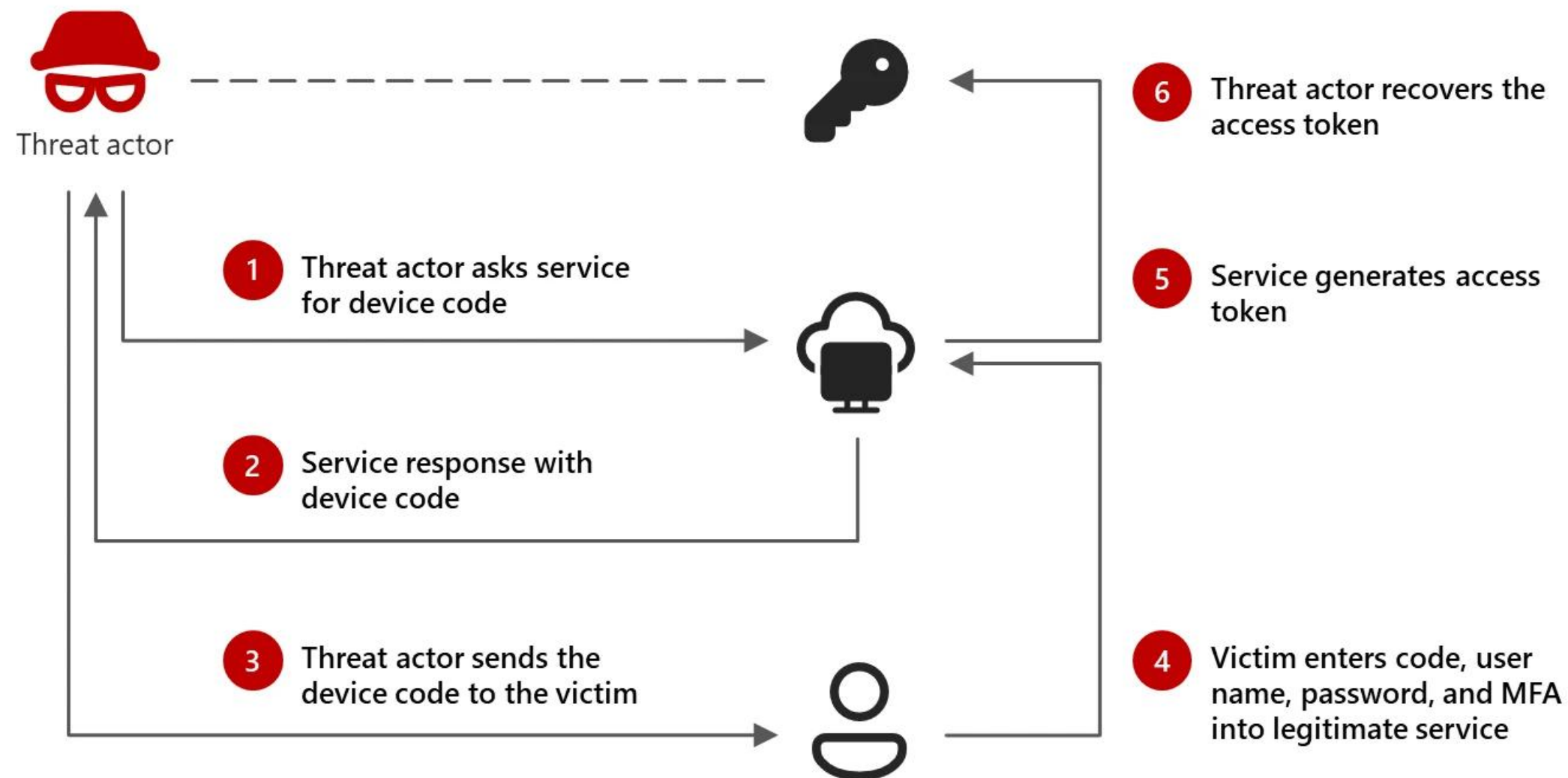
Thank you for supporting this important security initiative.

[Learn more about passkeys](#)

Phased rollout



Device Code Flow



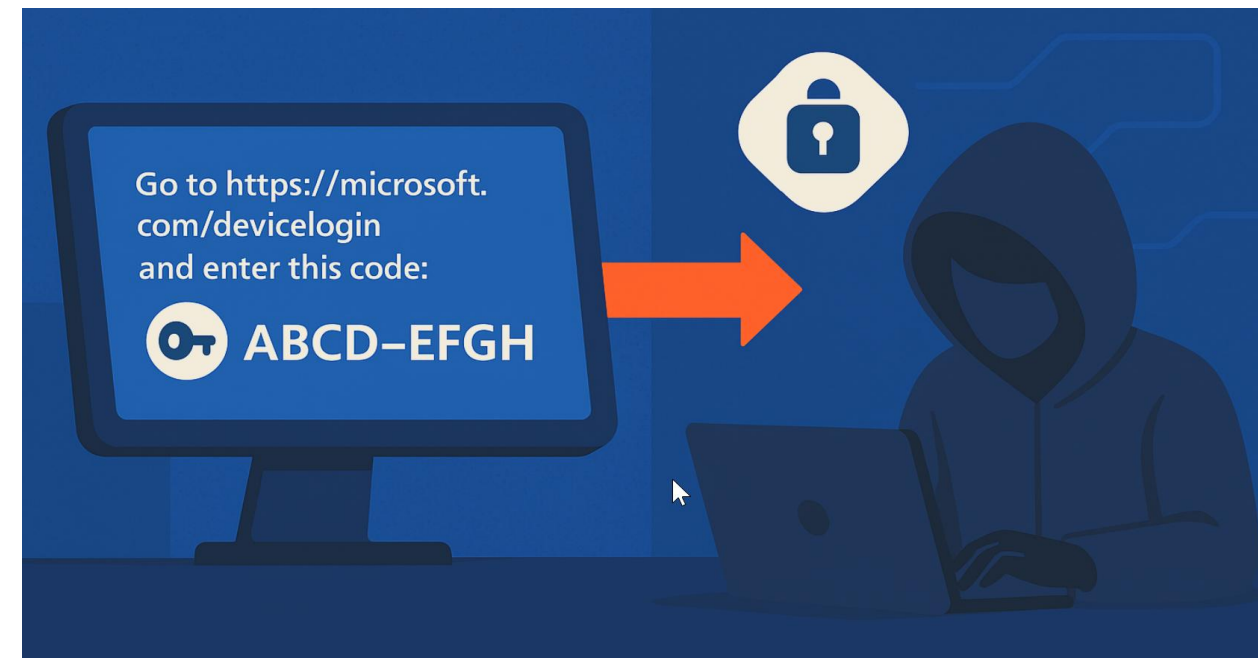
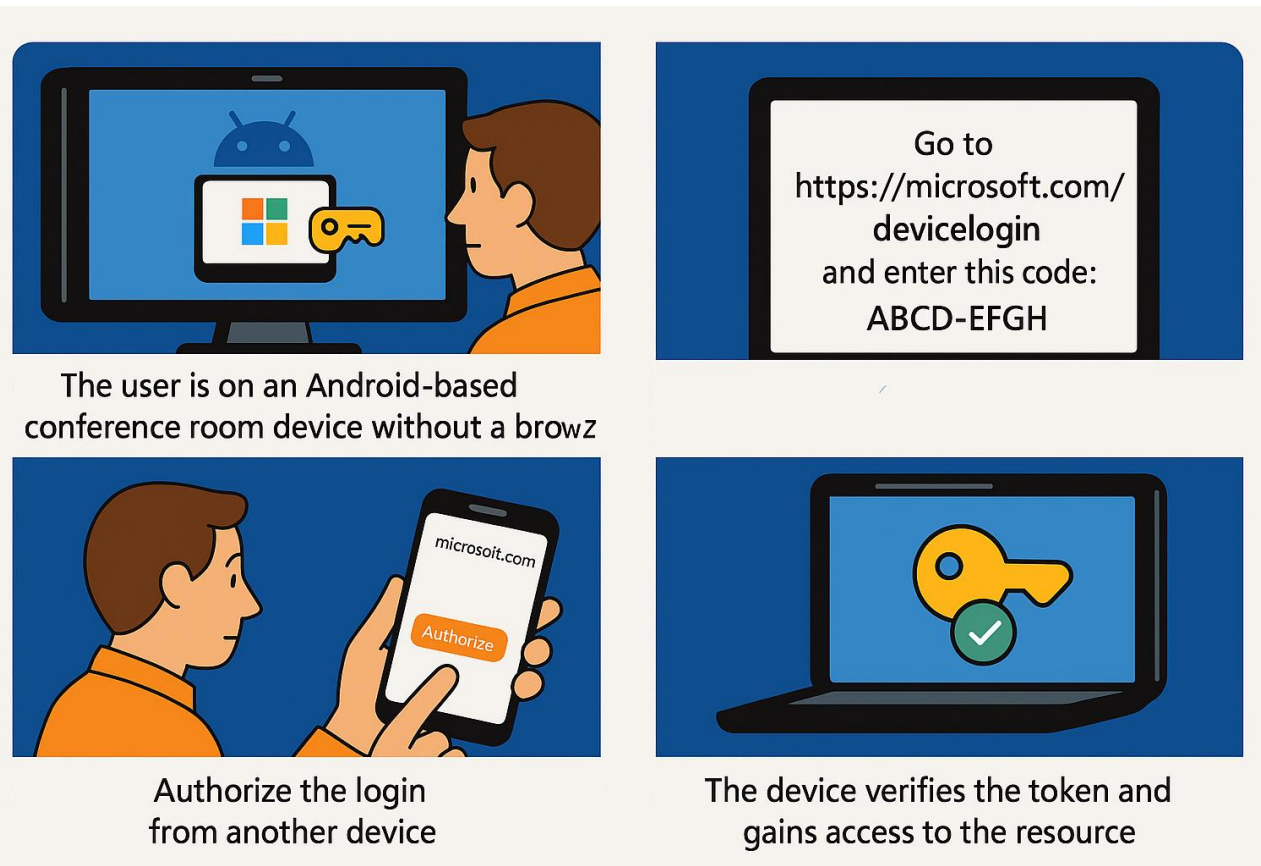
This is an OAuth flow designed for browser-less devices (TV, IoT, CLI):

- 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

Block device code flow

Policy details Policy impact

Edit Duplicate Download JSON Delete

Policy details

Summary

This policy was created in report-only mode by the Conditional Access Optimization Agent at 10 agosto 2025 alle ore 12:10. [Manage agent](#)

Name

Block device code flow

State

Report-only (policy is evaluated but not enforced)

Included identities

All users

Included cloud apps

All apps

Requirements for access

Block access

Created by

CONDITIONAL ACCESS OPTIMIZATION AGENT

Excluded identities

1 user, 0 groups, 0 roles

Conditions

Device Code Flow Authentication

Created date

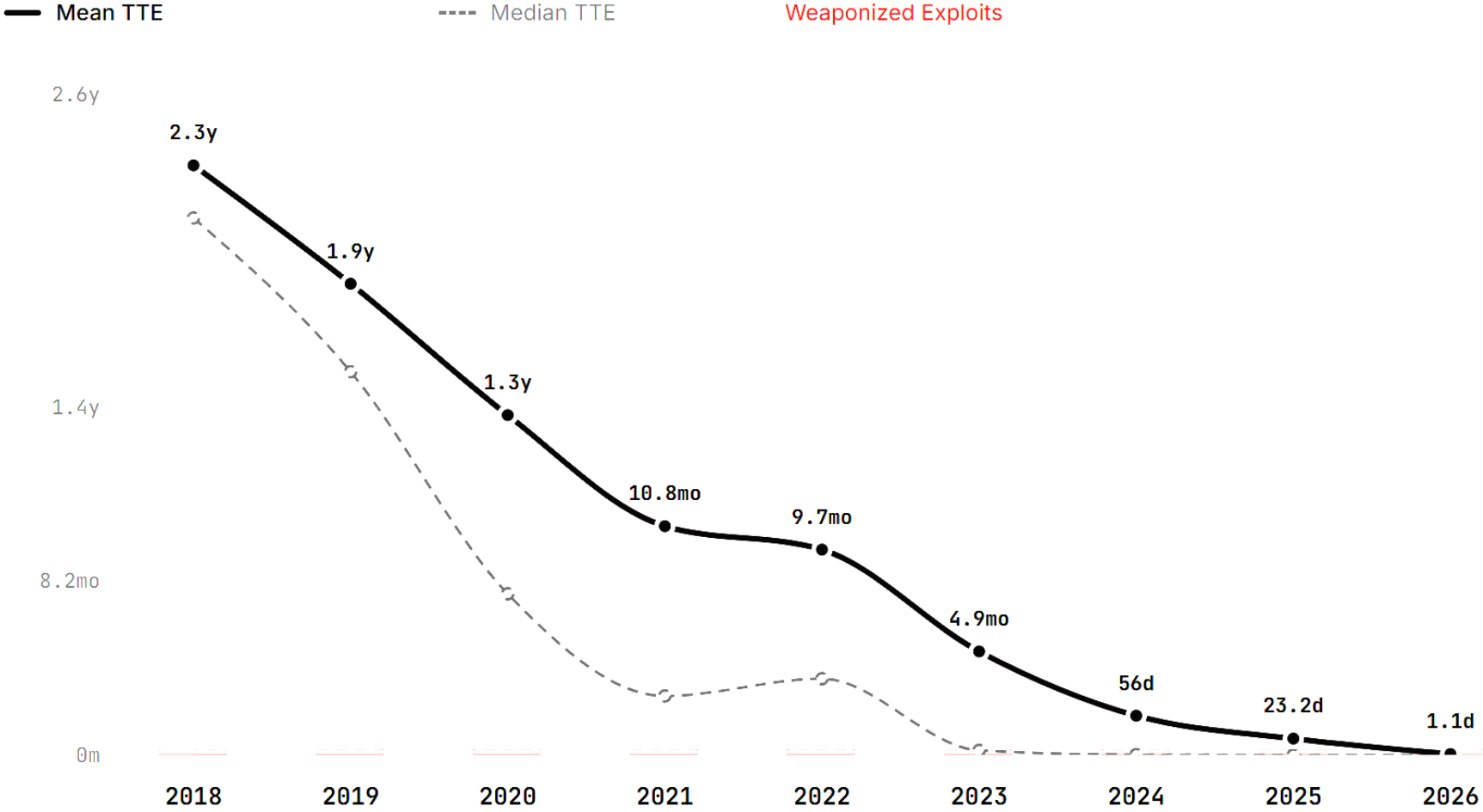
10/08/25, 12:10:54

Threat evolution



From Vulnerability to Exploitation

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



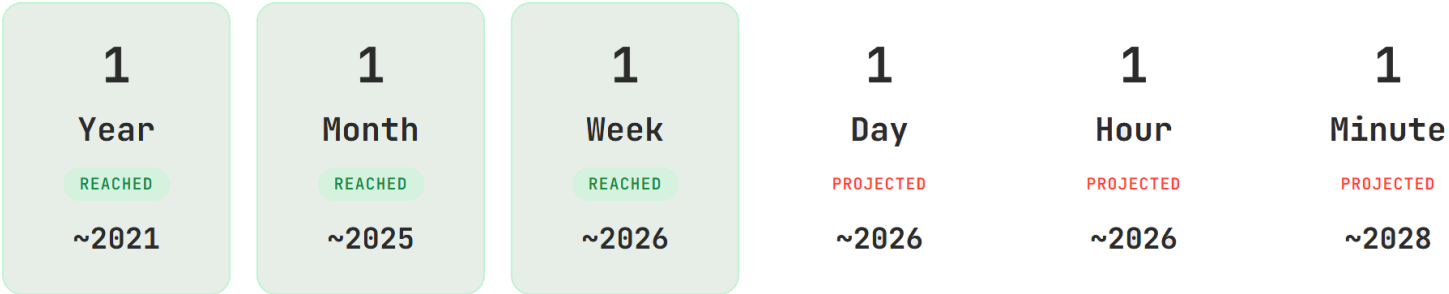
Based on 3,521 CVE-exploit pairs from trusted sources (CISA KEV, VulnCheck KEV & XDB)

zerodaycLock.com

618

Time-to-Exploit Milestones

When mean time-to-exploit crosses each threshold





#Milano

Slide e video:

<https://www.globalazuremilano.it>