Entra ID Protection and Conditional Access

Real World Best Practices

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

About me

8 years

Product Management in Entra ID

6 years

Microsoft partner leading customer success

4 years

Licensed corporate attorney

in linkedin.com/in/basseri

2Pint

PATCH MY PC

robopack

wortell

INGRAM MICRO®

The Collective

bechtle

lebon.IT

ConXioN
The new style of IT

VirtualMetric

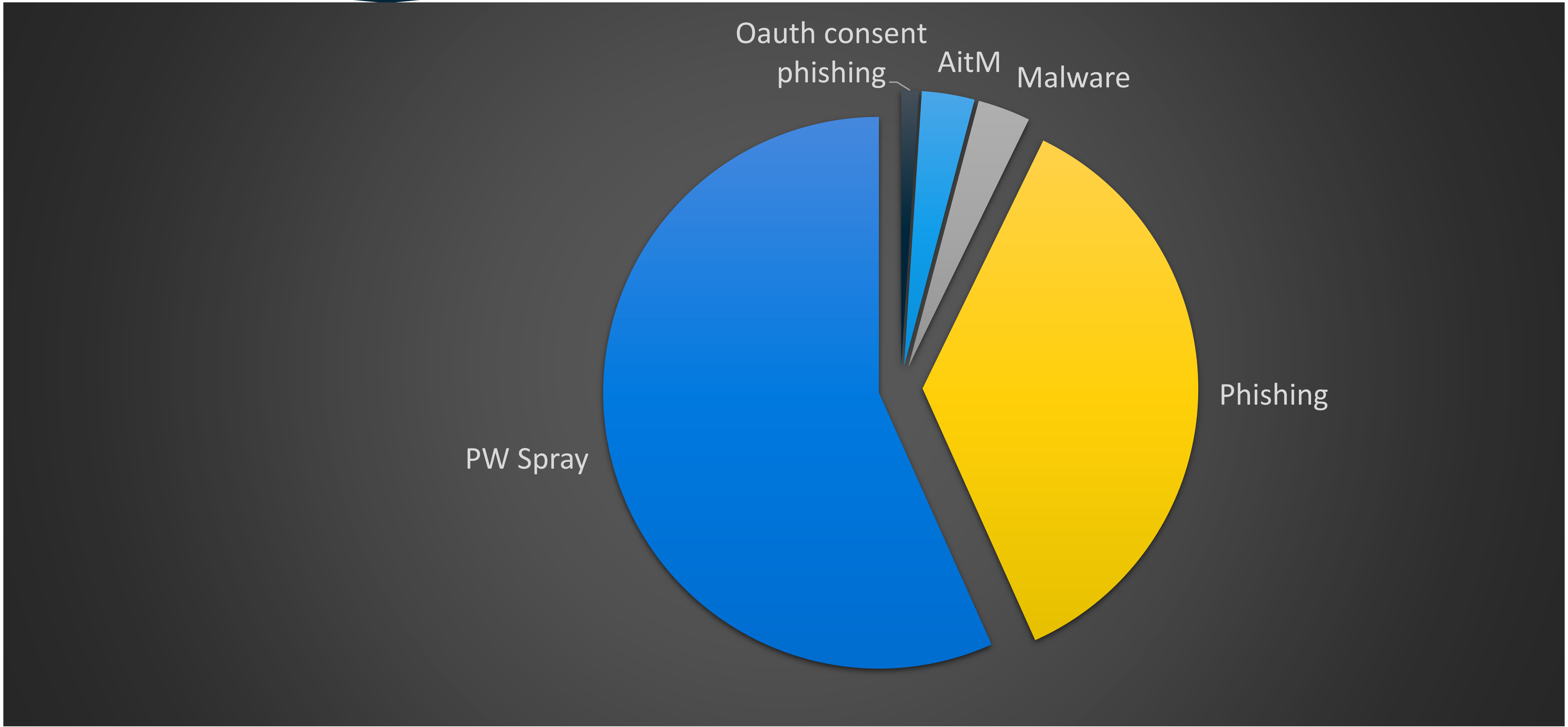
veeam

evri

Agenda

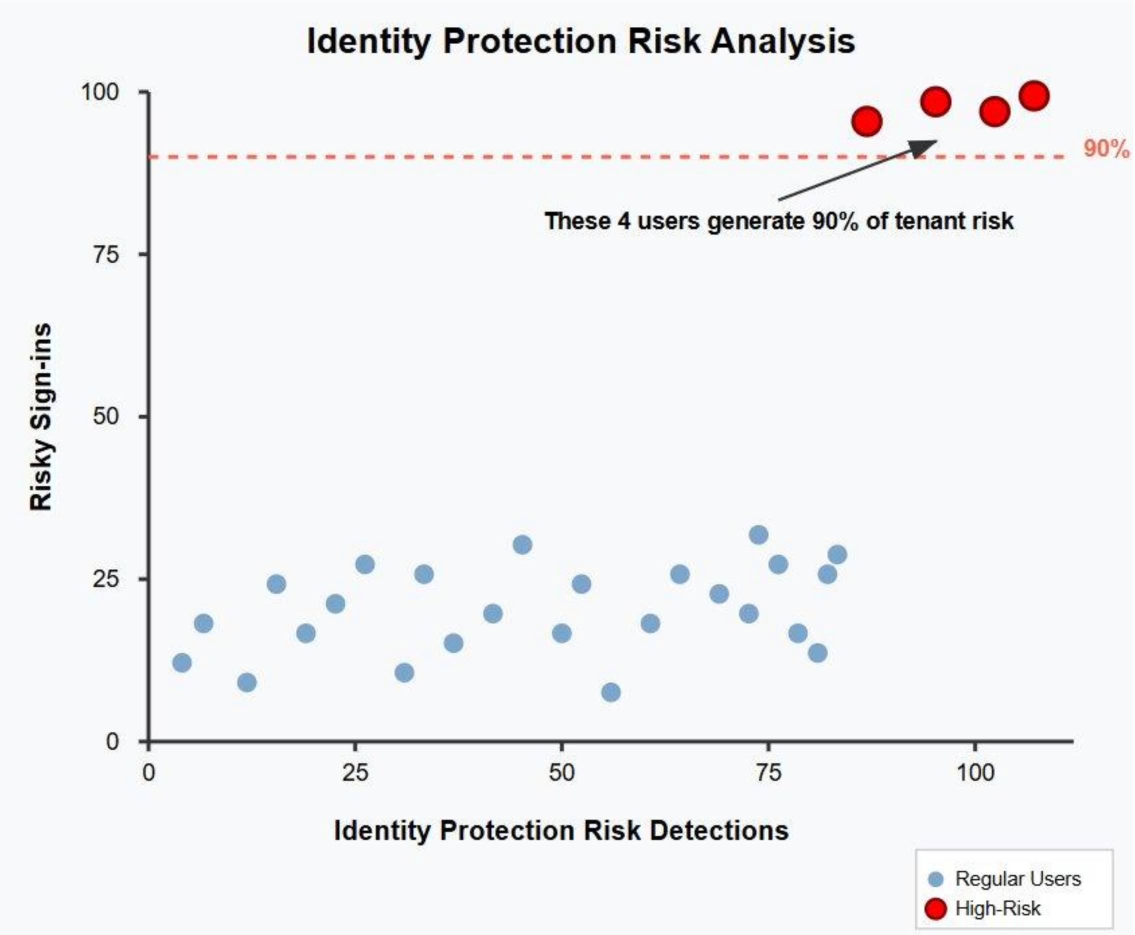
1. Introduction / Overview
2. Customer examples
3. Best Practices
4. How risk works
5. Q&A

Initial access techniques in Entra ID



Customer examples

Story: Global commercial retailer


Identity Protection Risk Analysis
100
75
50
25
0
Risky Sign-ins
0
25
50
75
100
Identity Protection Risk Detections
90%
These 4 users generate 90% of tenant risk
● Regular Users
● High-Risk

Story: US federal agency

MS.AAD.2.

Users detec

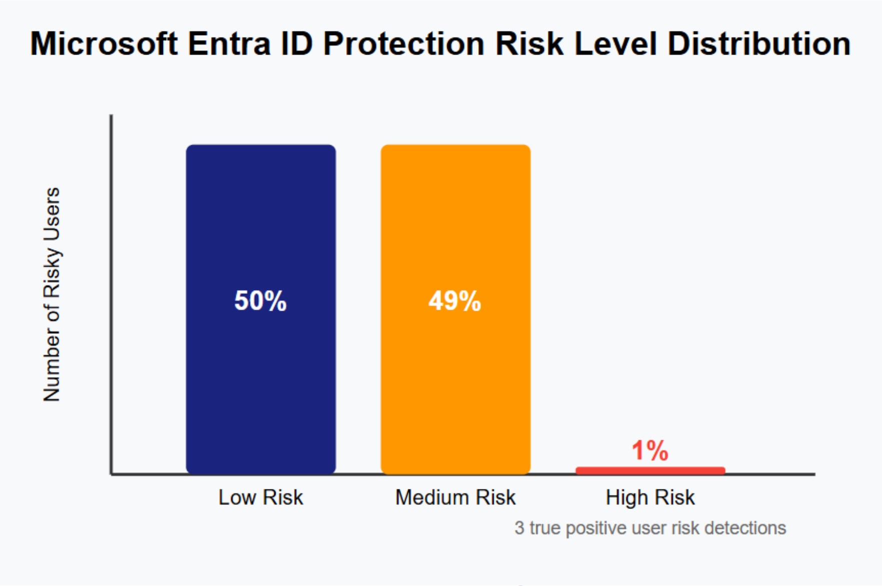
- *Rationa*
- *Last mo*
- Note: U Microso account

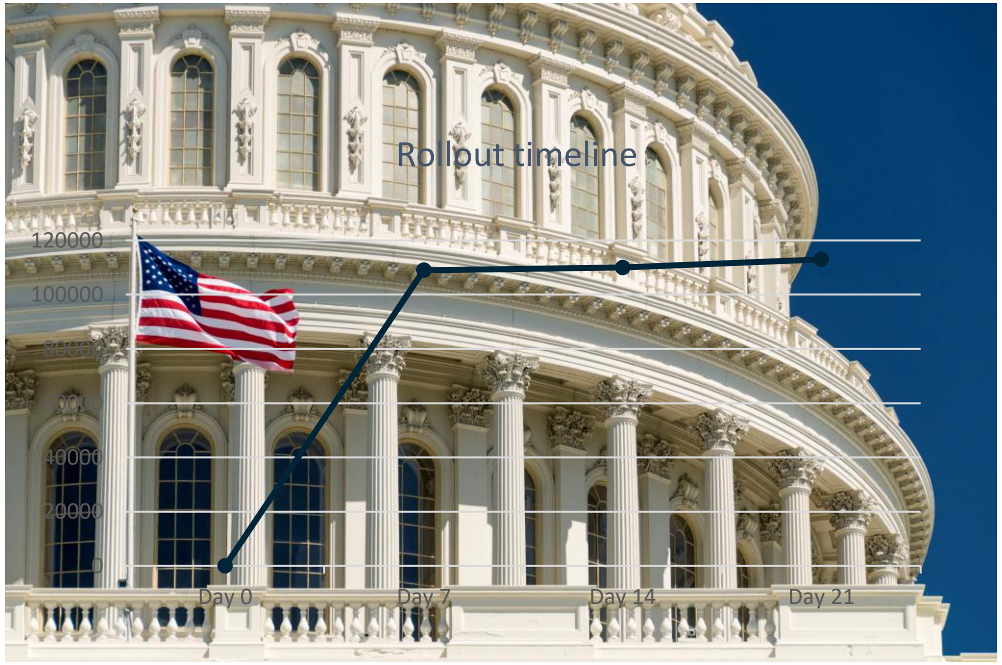
MS.AAD.2.:

Sign-ins de

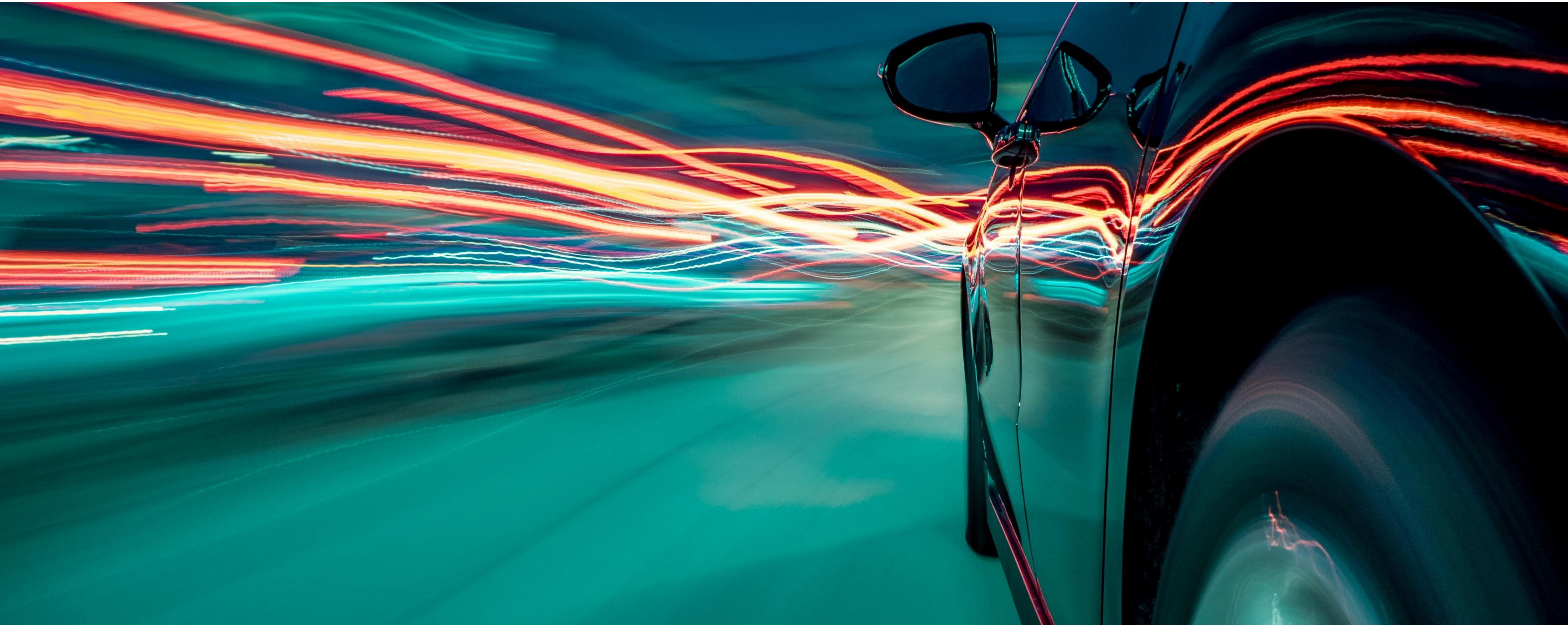
- *Rationa*

sing the system via a nediates their


Microsoft Entra ID Protection Risk Level Distribution



Story: European Automaker



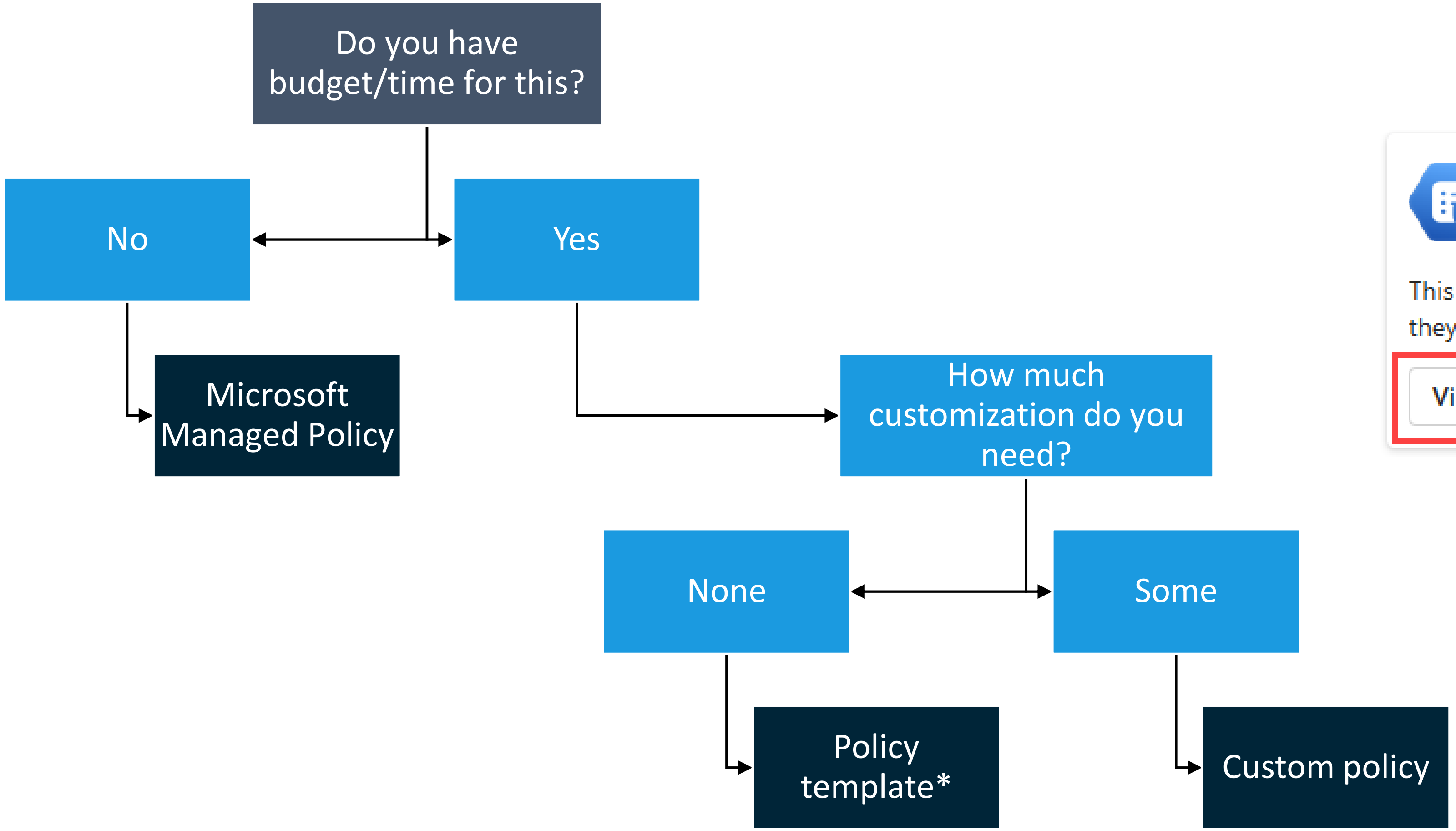
Best practices: Planning

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Which approach is right for you?



Do you have budget/time for this?

No

Yes

Microsoft Managed Policy

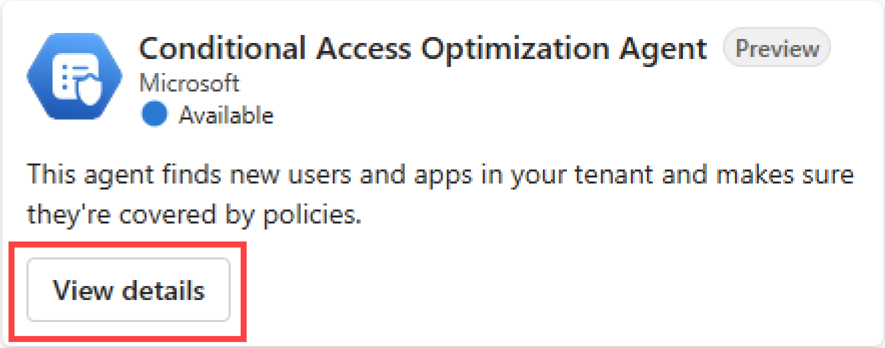
How much customization do you need?

None

Some

Policy template*

Custom policy



Conditional Access Optimization Agent Preview

Microsoft

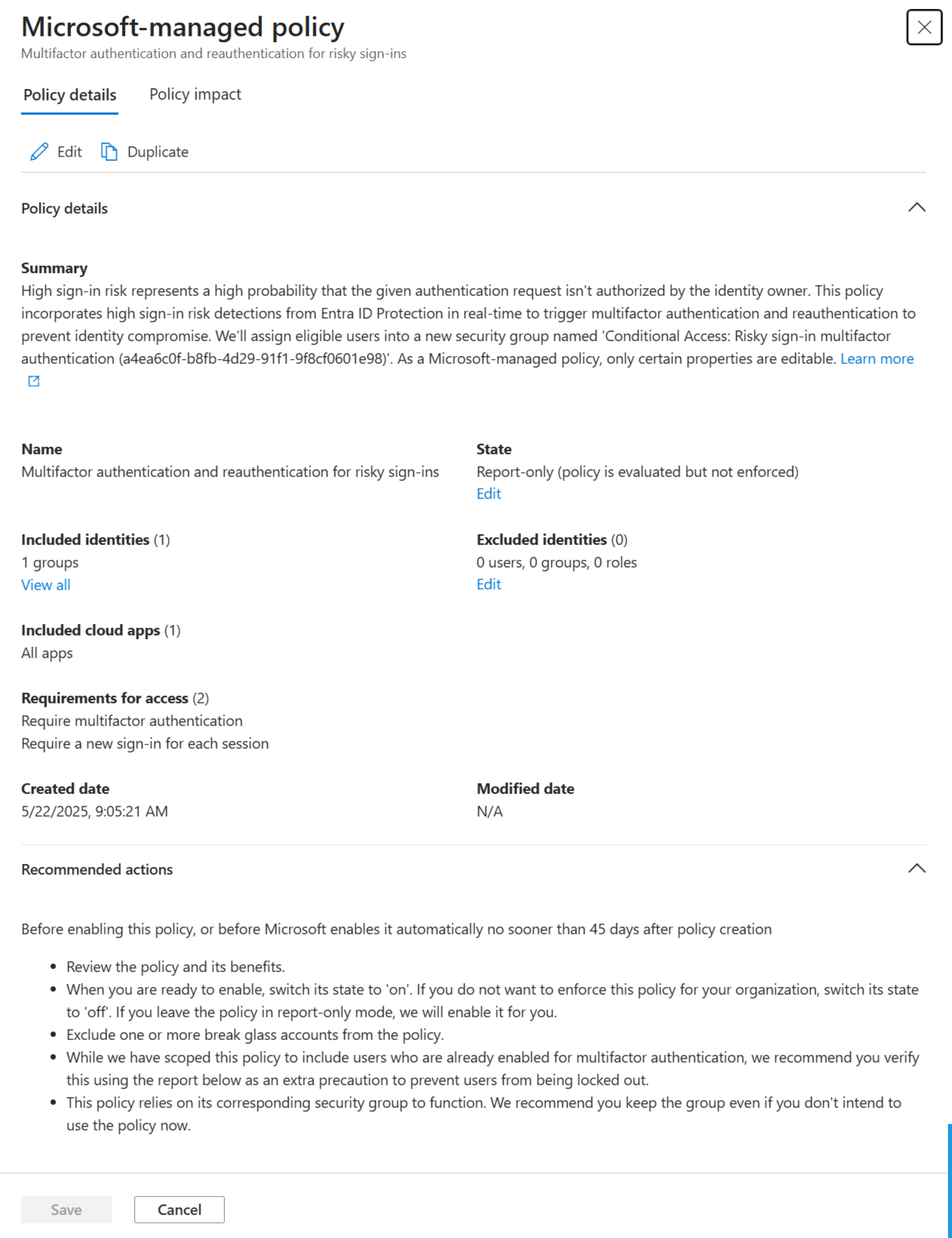
● Available

This agent finds new users and apps in your tenant and makes sure they're covered by policies.

Microsoft-managed policies

- Benefits
  - ✓ Adheres to best practice
  - ✓ Maximizes utilization
  - ✓ No one gets blocked
  - ✓ License-compliant
  - ✓ Updated by Microsoft
  - ✓ Admin no-op

- Process
  - Notify
  - Create group and policy
  - Wait 45+ days
  - Enforce policy
  - Update policy



Summary

High sign-in risk represents a high probability that the given authentication request isn't authorized by the identity owner. This policy incorporates high sign-in risk detections from Entra ID Protection in real-time to trigger multifactor authentication and reauthentication to prevent identity compromise. We'll assign eligible users into a new security group named 'Conditional Access: Risky sign-in multifactor authentication (a4ea6c0f-b8fb-4d29-91f1-9f8cf0601e98)'. As a Microsoft-managed policy, only certain properties are editable. Learn more

Name
Multifactor authentication and reauthentication for risky sign-ins

State
Report-only (policy is evaluated but not enforced)
Edit

Included identities (1)
1 groups
View all

Excluded identities (0)
0 users, 0 groups, 0 roles
Edit

Included cloud apps (1)
All apps

Requirements for access (2)
Require multifactor authentication
Require a new sign-in for each session

Created date
5/22/2025, 9:05:21 AM

Modified date
N/A

Recommended actions

Before enabling this policy, or before Microsoft enables it automatically no sooner than 45 days after policy creation

- Review the policy and its benefits.
- When you are ready to enable, switch its state to 'on'. If you do not want to enforce this policy for your organization, switch its state to 'off'. If you leave the policy in report-only mode, we will enable it for you.
- Exclude one or more break glass accounts from the policy.
- While we have scoped this policy to include users who are already enabled for multifactor authentication, we recommend you verify this using the report below as an extra precaution to prevent users from being locked out.
- This policy relies on its corresponding security group to function. We recommend you keep the group even if you don't intend to use the policy now.

Policy templates

- Benefits
  - ✓Adheres to best practice
  - ✓Updated by you when needed

- Process
  - Meet pre-reqs
  - Create group and policy
  - Wait
  - Enforce policy
  - Update policy

Custom policies

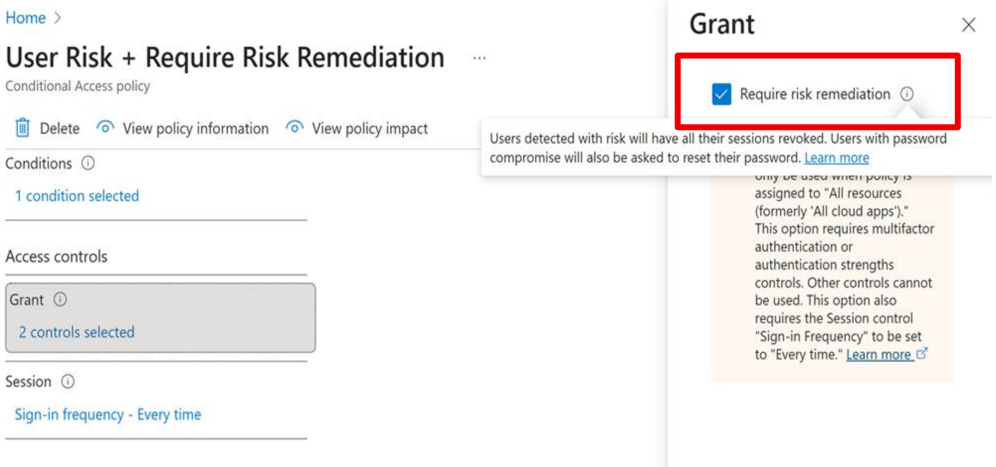
- Benefits
  - ✓Tailored for your organization
  - ✓Fully customizable
  - ✓Updated by you when needed

- Process
  - Meet pre-reqs
  - Create group and policy
  - Wait
  - Enforce policy
  - Update policy

Note: Passwordless users

Challenge

I want to auto-remediate compromised users but don’t want to force a password reset on a passwordless user!



Home >

User Risk + Require Risk Remediation ...

Conditional Access policy

Delete · View policy information · View policy impact

Conditions

1 condition selected

Access controls

Grant

2 controls selected

Session

Sign-in frequency - Every time

Grant

☑ Require risk remediation

Users detected with risk will have all their sessions revoked. Users with password compromise will also be asked to reset their password. Learn more

only be used when policy is assigned to "All resources (formerly 'All cloud apps')." This option requires multifactor authentication or authentication strengths controls. Other controls cannot be used. This option also requires the Session control "Sign-in Frequency" to be set to "Every time." Learn more

Solution (public preview)

A User Risk policy that accommodates **all authentication methods**, ID Protection manages the appropriate remediation flow:

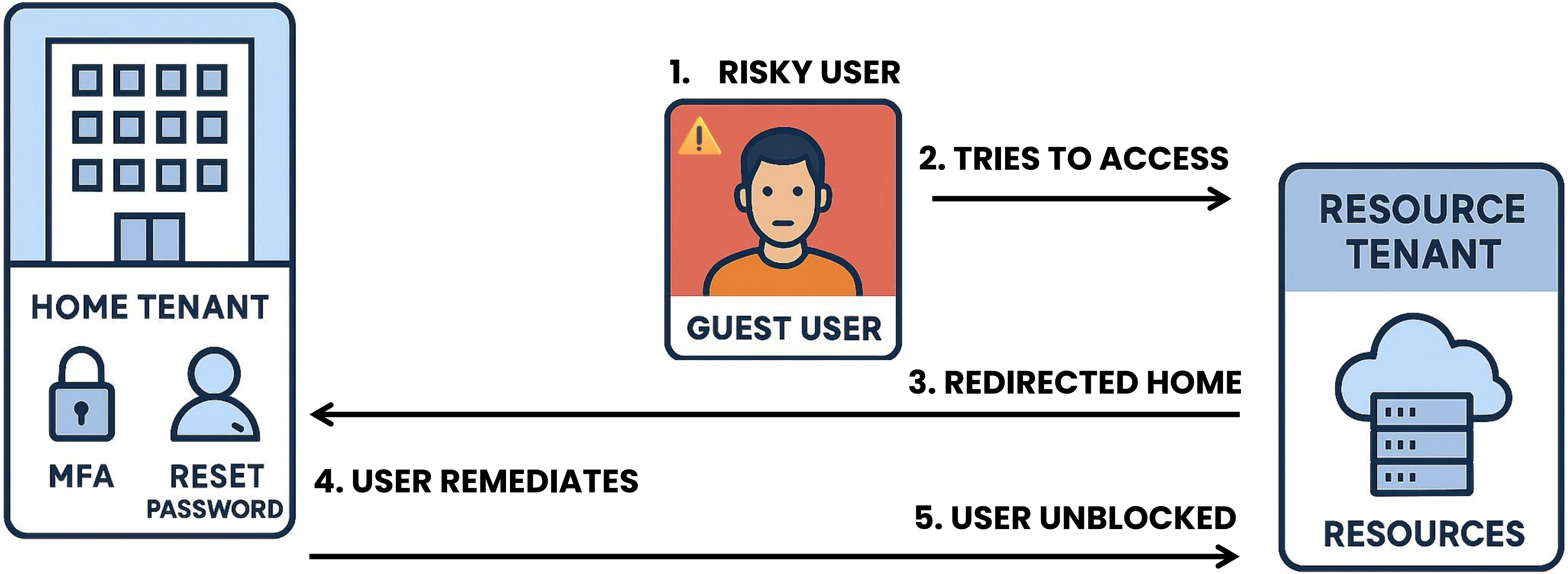
Path 1 - Password and session compromise: Active risk detection (e.g. leaked credential, password spray, or session history involving a compromised password). Entra ID forces secure password change and revokes sessions.

Path 2 – Session compromise only: Active risk detection that doesn't involve a compromised password (e.g. anomalous token, impossible travel, unfamiliar sign-in properties). Entra ID revokes sessions.

Instead of “require password change” choose “**require risk remediation**”

Note: Guest users

- Evaluated for risk and remediated in the guest's home



Note: Policy exclusions

- Emergency/break-glass accounts (HW backed)

- Service accounts

Best practices: Deployment

Prerequisites

Review reports

Plan for change

Deploy policies

Monitor and adapt

- Ensure Microsoft Entra ID P2 or trial license is active
- Required roles: Security Reader, Security Admin, Conditional Access Admin
- Ensure users are registered for MFA and password reset (if still on passwords)
- Create test users and groups for validation
- Engage stakeholders early and define responsibilities

Prerequisites

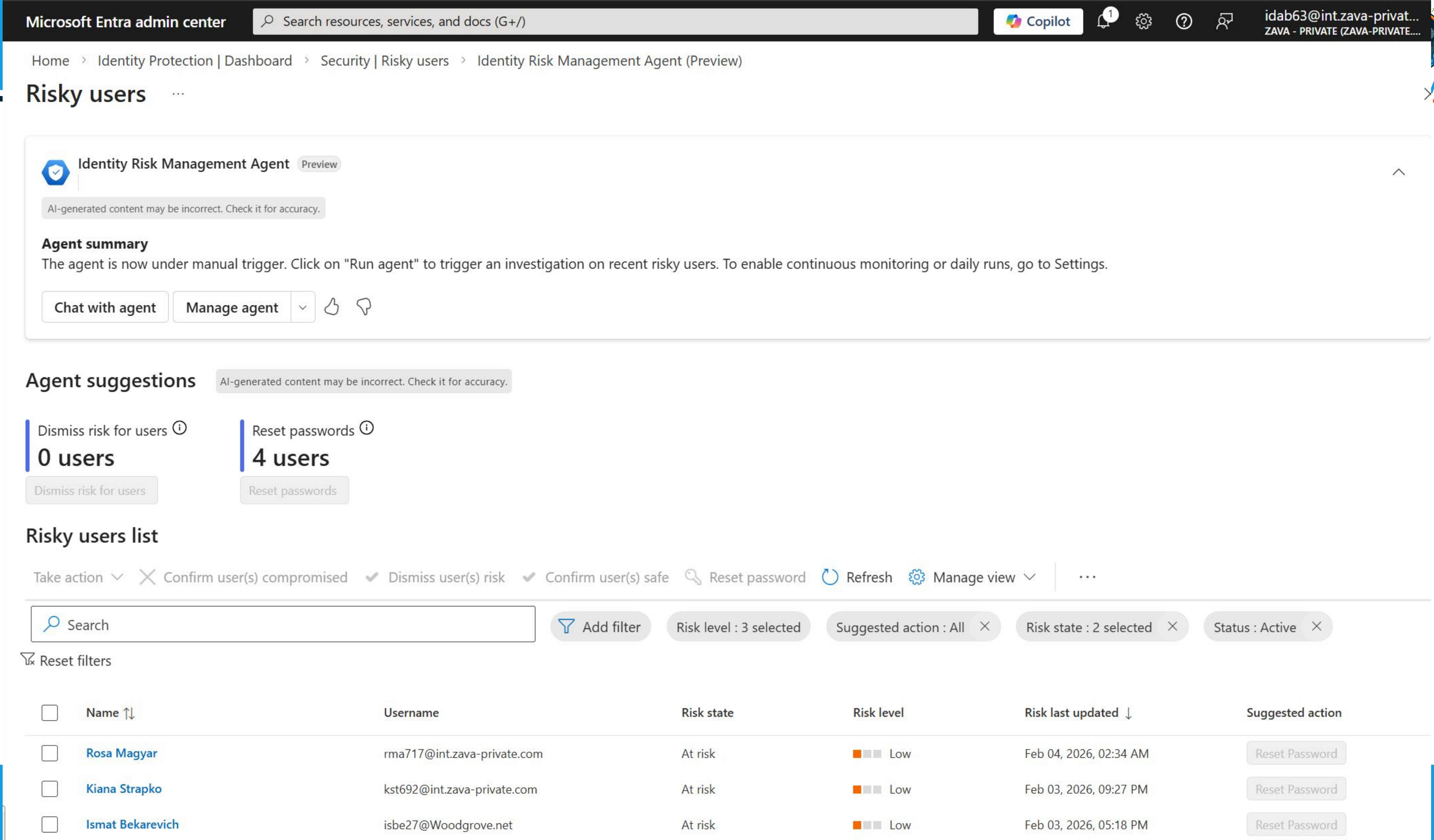
Review reports

Plan for change

Deploy policies

Monitor and adapt

- Review ID Protection reports for suspicious activity
- Investigate and remediate risky users
- Use the Risk Management Agent or Microsoft Graph PowerShell for bulk actions
- Use the Impact analysis workbook to understand user impact before creating risk policies



Risky users

Identity Risk Management Agent Preview

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

Agent summary

The agent is now under manual trigger. Click on "Run agent" to trigger an investigation on recent risky users. To enable continuous monitoring or daily runs, go to Settings.

Agent suggestions

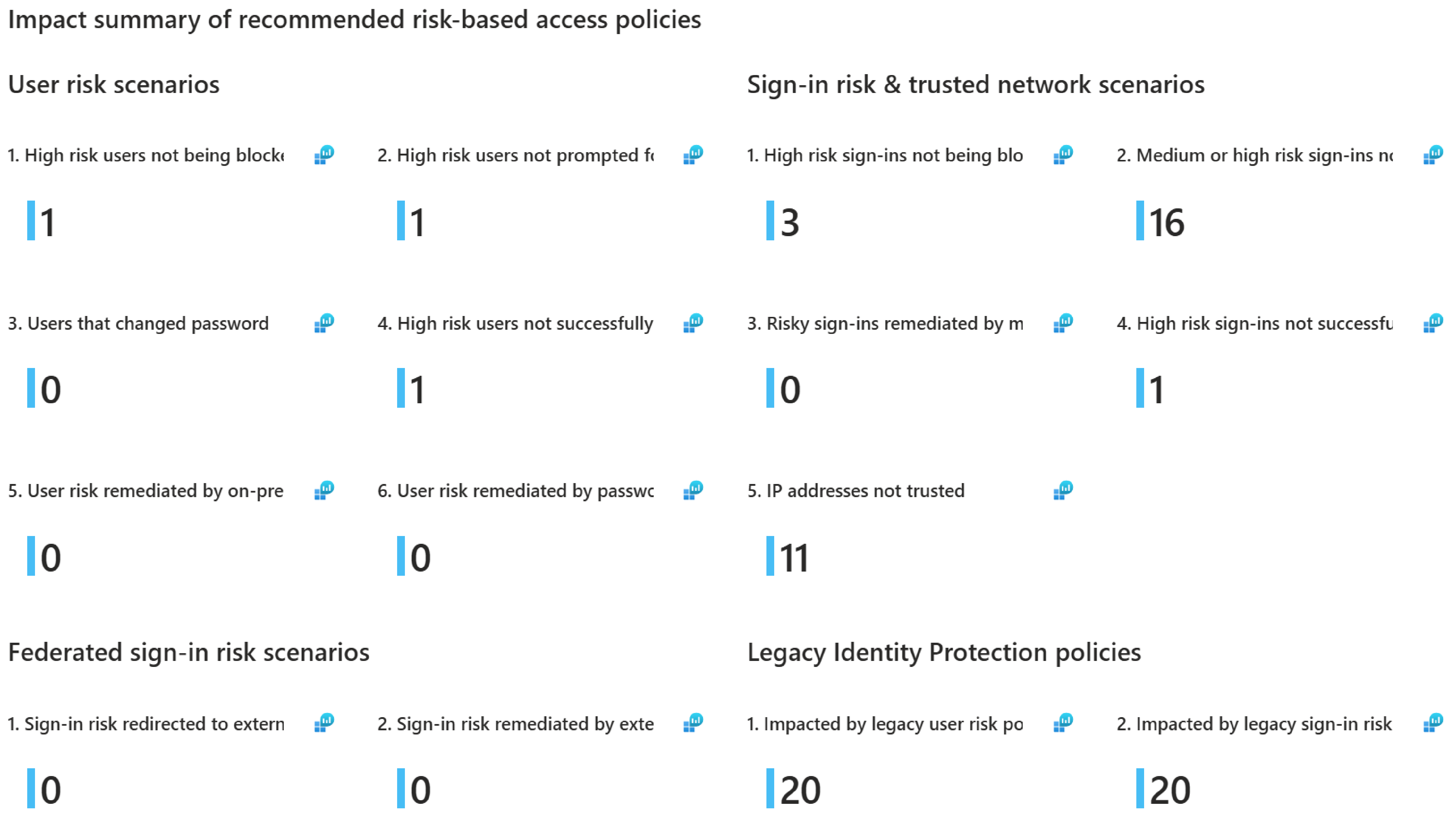
AI-generated content may be incorrect. Check it for accuracy.

Dismiss risk for users
0 users

Reset passwords
4 users

Risky users list

☐	Name	Username	Risk state	Risk level	Risk last updated	Suggested action
☐	Rosa Magyar	rma717@int.zava-private.com	At risk	Low	Feb 04, 2026, 02:34 AM	Reset Password
☐	Kiana Strapko	kst692@int.zava-private.com	At risk	Low	Feb 03, 2026, 09:27 PM	Reset Password
☐	Ismat Bekarevich	isbe27@Woodgrove.net	At risk	Low	Feb 03, 2026, 05:18 PM	Reset Password



Impact summary of recommended risk-based access policies

User risk scenarios

1. High risk users not being block

1

2. High risk users not prompted f

1

3. Users that changed password

0

4. High risk users not successfully

1

5. User risk remediated by on-pre

0

6. User risk remediated by passwc

0

Sign-in risk & trusted network scenarios

1. High risk sign-ins not being blo

3

2. Medium or high risk sign-ins n

16

3. Risky sign-ins remediated by m

0

4. High risk sign-ins not successfu

1

5. IP addresses not trusted

11

Federated sign-in risk scenarios

1. Sign-in risk redirected to extern

0

2. Sign-in risk remediated by exte

0

Legacy Identity Protection policies

1. Impacted by legacy user risk po

20

2. Impacted by legacy sign-in risk

20

Prerequisites

Review reports

Plan for change

Deploy policies

Monitor and adapt

- Define Conditional Access policies for sign-in and user risk based on your risk tolerance
  - 2 separate policies
- Exclude emergency and service accounts to prevent lockouts
- Configure Named Locations as trusted to reduce false positives and define your VPN ranges in Defender for Cloud Apps
- Proactively inform users to prepare them for change and enhance deployment success

Prerequisites

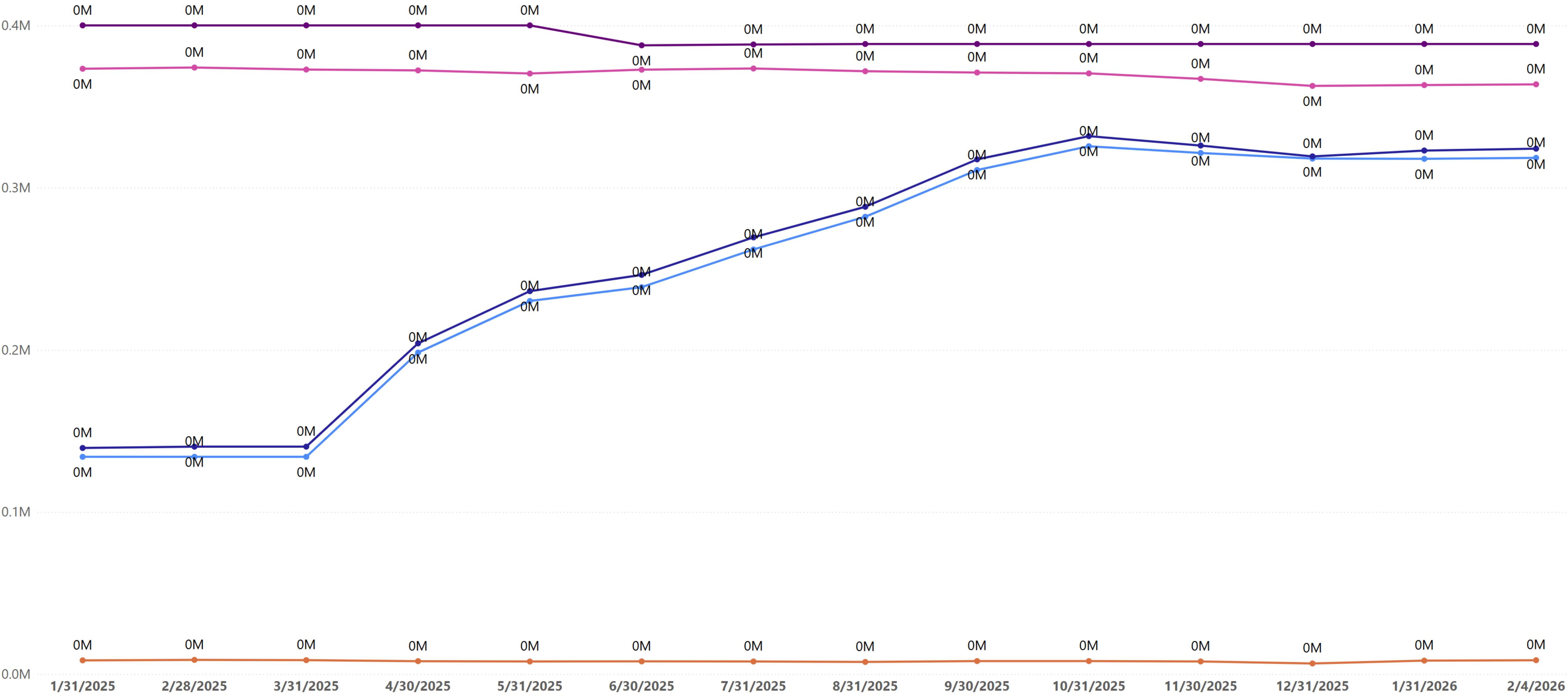
Review reports

Plan for change

Deploy policies

Monitor and adapt

- Enable MFA registration policy first (if needed)
- Use Report-only mode to test policies before enforcement
  - First: Sign-in risk
  - Next: User risk
- Validate policy behavior with test users
- Rollout enforcement gradually
  - Ring 1 (Identity team)
  - Ring 2 (InfoSec)
  - Ring 3 (Corp. HQ)
  - Ring 4 (everyone else)


0M
0.4M
0.3M
0.2M
0.1M
0.0M
1/31/2025
2/28/2025
3/31/2025
4/30/2025
5/31/2025
6/30/2025
7/31/2025
8/31/2025
9/30/2025
10/31/2025
11/30/2025
12/31/2025
1/31/2026
2/4/2026

Prerequisites

Review reports

Plan for change

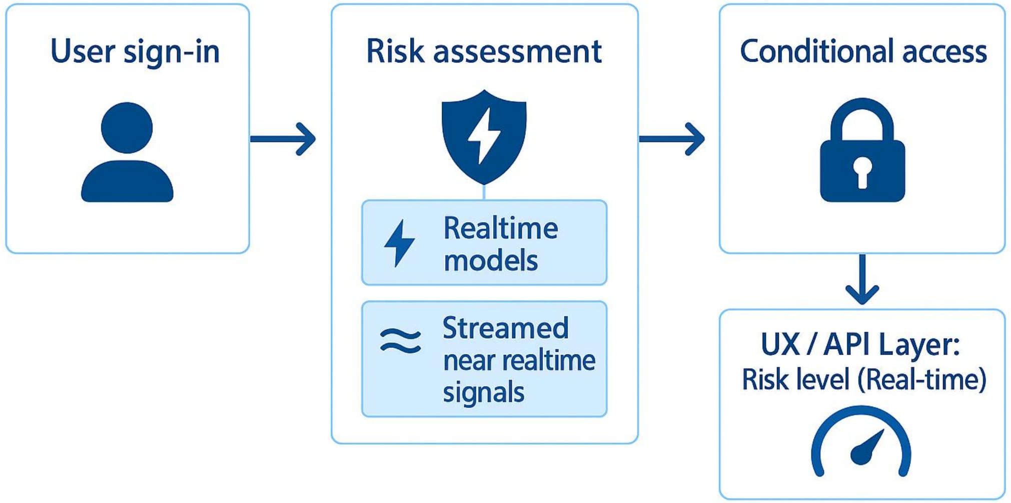
Deploy policies

Monitor and adapt

- Monitor by enabling alerts, using workbooks, or exporting risk data.
- Exclude additional accounts as appropriate
- Revisit policy coverage gaps to ensure all users are protected*

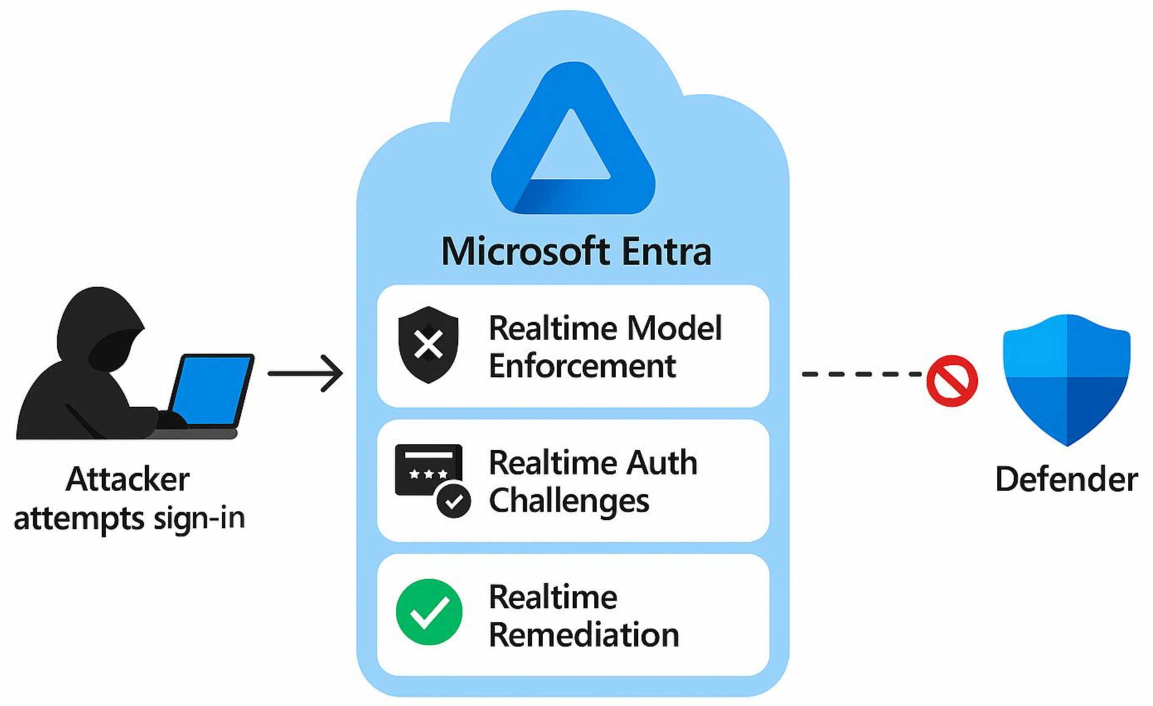
How risk works

How Entra Computes Realtime Risk


User sign-in
Risk assessment
Realtime models
Streamed near realtime signals
Conditional access
UX / API Layer: Risk level (Real-time)

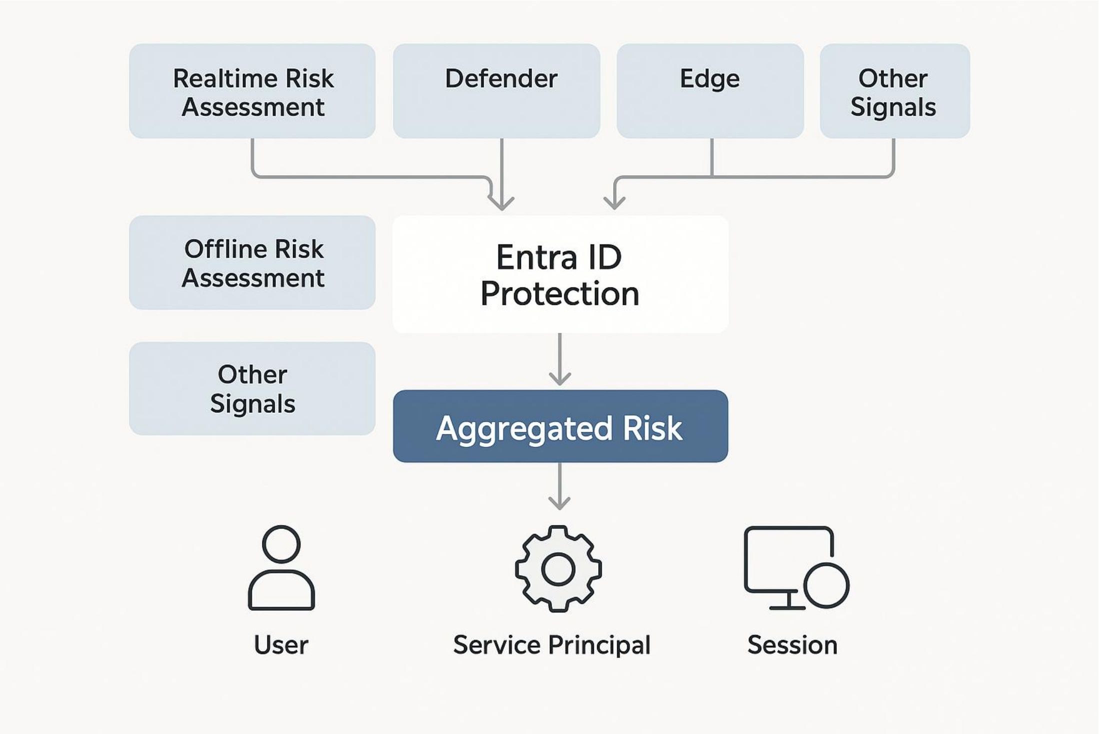
- Entra ID Protection takes a multifaceted approach to risk analysis.
- Leveraging real-time models to quickly assess risk during authentication time
- Stream near-real-time signals like aggregate risk and Microsoft Defender Alerts to the evaluation engine.

Realtime Enforcement and Remediation



- Realtime Model Enforcement means pre-token issuance – so we can stop the attacker very early in the kill chain.
- Realtime Auth Challenges means we can disrupt the attacker early and give legit users an opportunity to self-remediate.
- Realtime Remediation means if the user passes the challenges, we can close the risk and reduce SOC overhead and investigation time.

How Entra Computes Aggregated Risk



- Entra ID Protection Aggregated Risk is the most comprehensive authority for an Entra Accounts Risk
- Entra ID Protection Aggregated Risk can change over time as Entra learns more about the Account and Remediations occur like TAP Generation or a Credential Change.

Anomalous Token

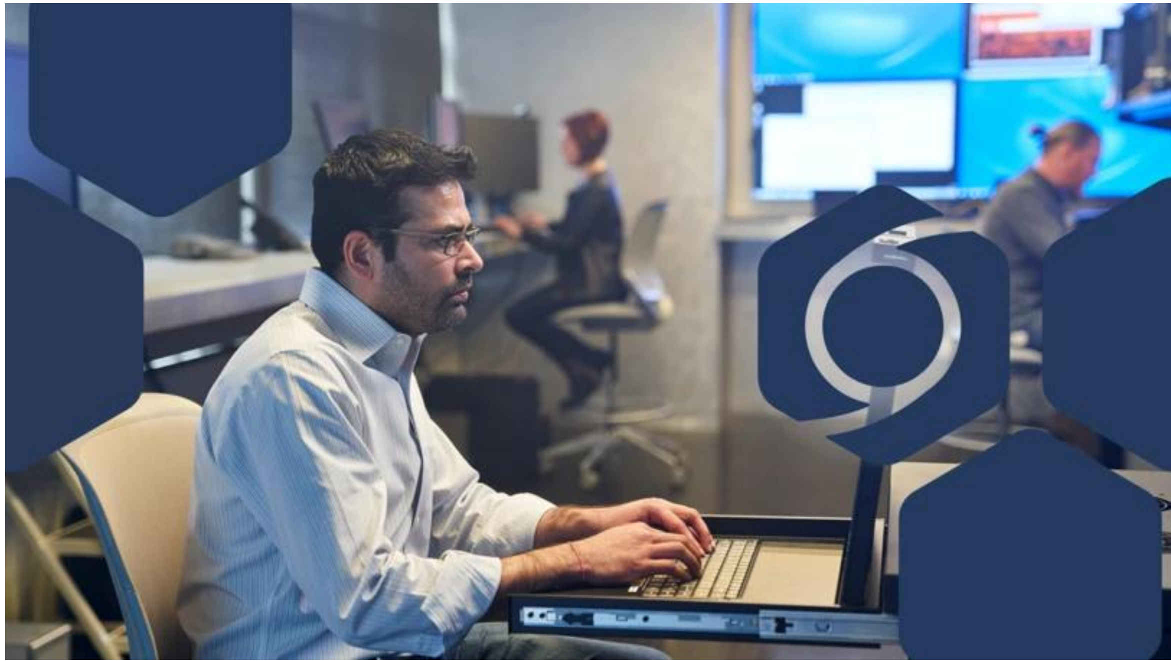
- Attackers are increasing leveraging token theft attacks to bypass MFA Protections.
- Anomalous Token detection helps catch and stop these attacks by evaluating risks real-time and offline.

Realtime Password Spray

- Still the most common attack
- Real-time version

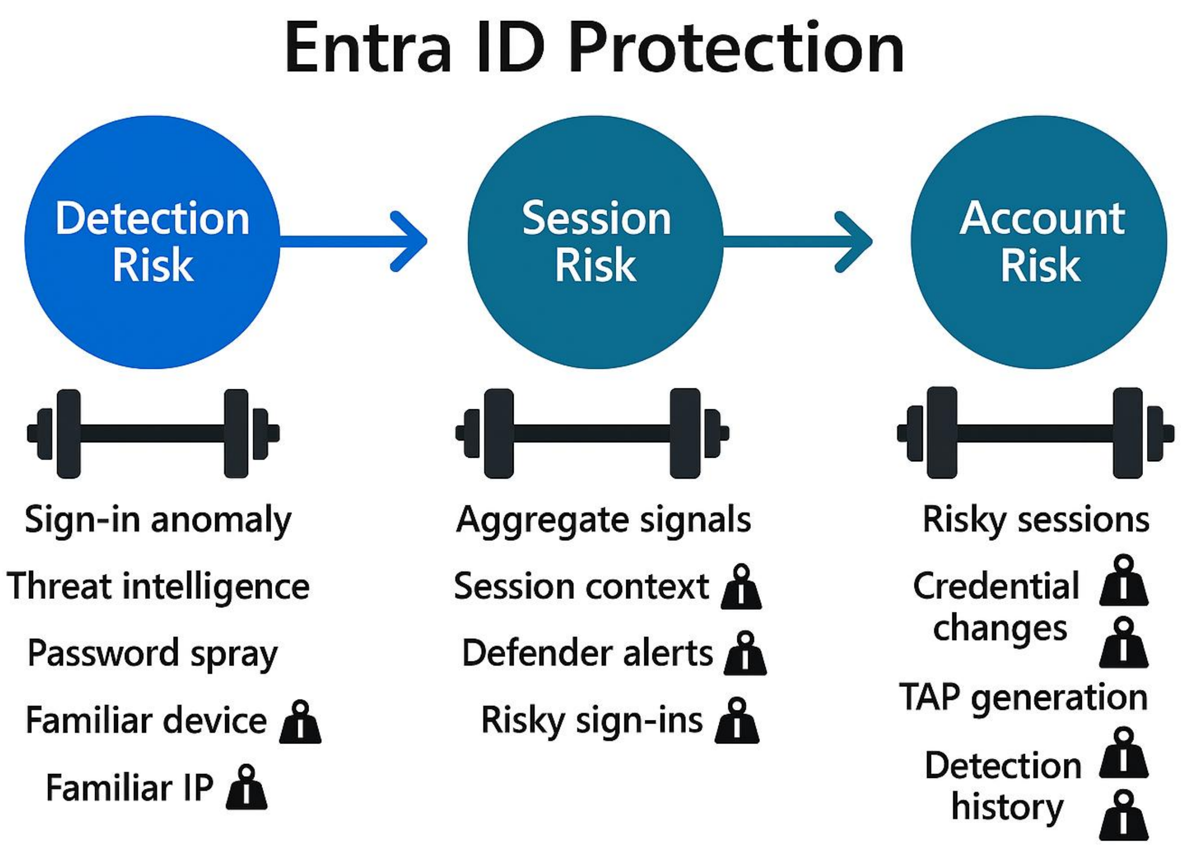
Verified Threat Actor IP / Threat Intelligence

- Verified Threat Actor IP
- Entra Threat Intelligence



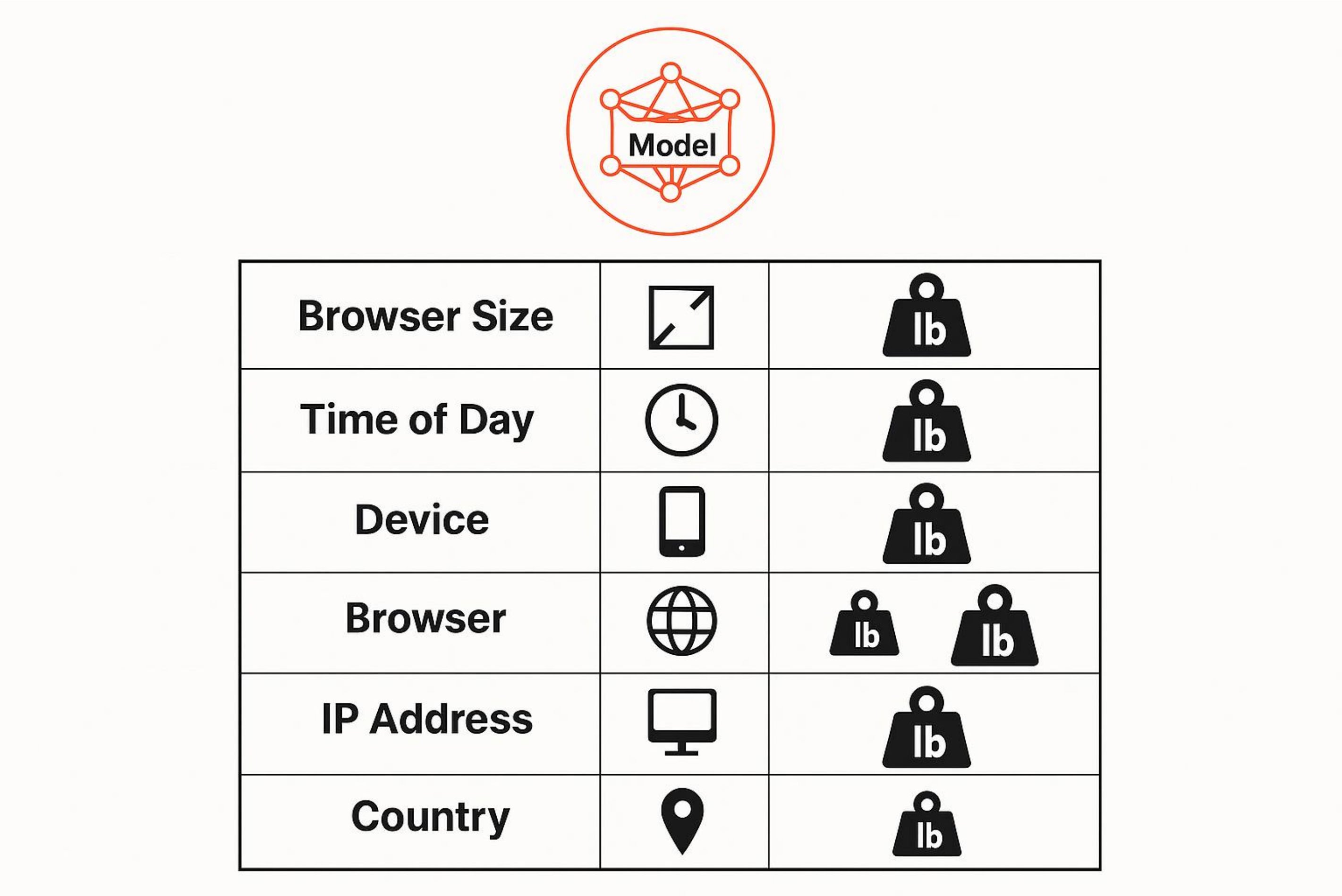
Risk Thresholds and Scoring

Entra ID Protection communicates risk as Risk Levels i.e Low, Medium, and High. These risk levels are decided by real-time and offline models depending on the weights.



Example: A Deeper Look at Unfamiliar Location

Some of the feature set used by a real-time model for the Unfamiliar Location detection base.



Model

Browser Size	⤢	lb
Time of Day	🕒	lb
Device	📱	lb
Browser	🌐	lb lb
IP Address	🖥	lb
Country	📍	lb

Closing

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Go-do's

- Check to see if you have a Microsoft-Managed policy available
- Review the Policy Impact workbook or the policy blade report
- AI for Security: Try out our agents
  - Conditional Access Optimization Agent
  - Risk Management Agent
- Security for AI: Check out ID Protection and Conditional Access for Agents

Trivia question:
This new CA grant control will allow a passwordless risky user to self-remediate.

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Discussion / Q&A

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Session feedback available in home feed of the app after the session

run
events

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT