Walk the walk – explore ways to ensure strong authentication in real life scenarios

Christopher Brumm

Christopher Brumm (he/him)

Cyber Security Architect @ glueckkanja, DE

I am a big fan of Microsoft Cloud Security products because there my two favorite topics Identity and Security work together in a unique way. I've been working in IT for quite a while and have almost 15 years of experience in IT security in various roles.

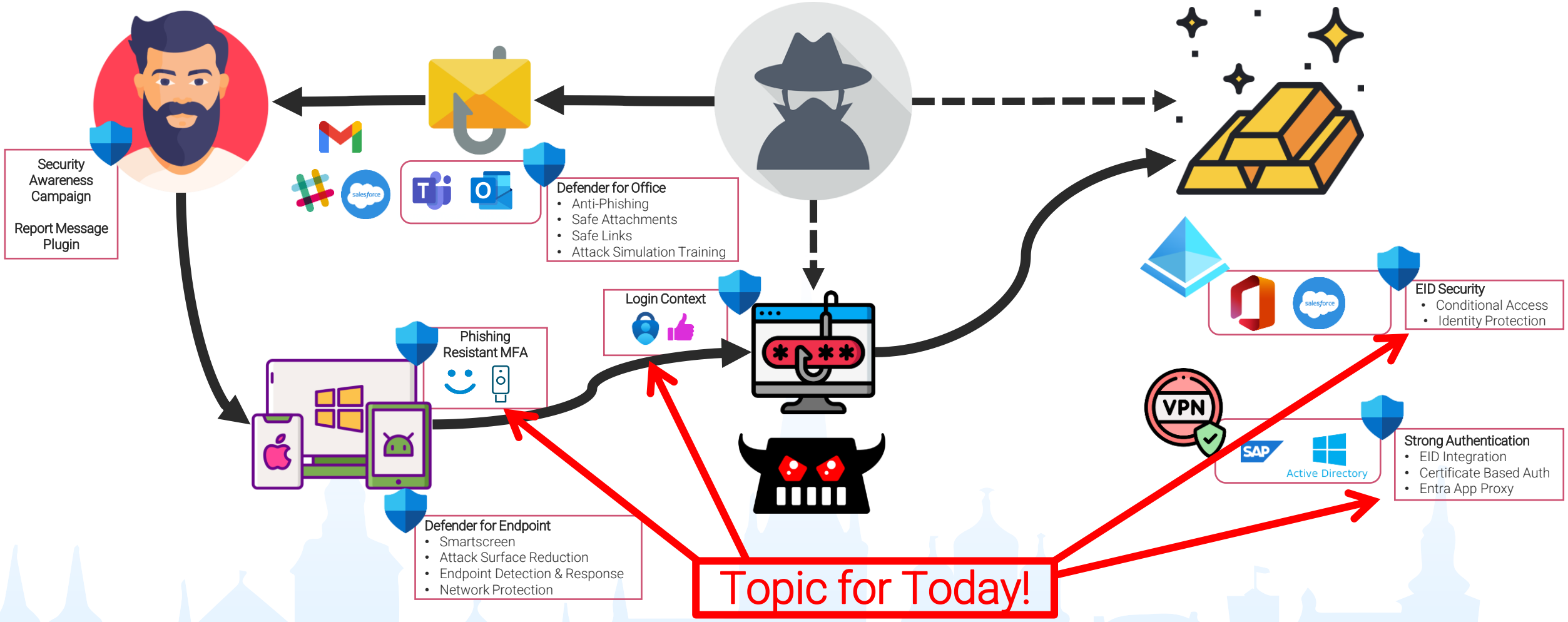
chris@brumm.cc

chris-brumm.medium.com

@cbrhh

/in/christopherbrumm

Let‘s start with a common Attack Scenario



images: Flaticon.com

The golden ruleset

The All Users + All Apps goal

OAuth2 & MSAL everywhere

Phishing Resistant Authentication

Risk Based Access Control

Strong Registration Controls

The main access path

Compliance Policies

- Require BitLocker
- Require Secure Boot
- Require Code Integrity
- Require TPM
- Require Defender
- Require Real Time Protection
- Require device under machine risk score Low
- Min OS Version

Azure AD joined
Windows Hello for Business

Risk-based Access Control

Conditional Access Policies

- All Users, All Cloud Apps
- Require compliant device
- Require **strong** MFA
- Check User Risk
- Check Session Risk

All Cloud Apps

Office 365

Azure Active Directory

The status quo in many environments

1. None or Phone-based MFA and no registration restrictions
2. No restriction on trusted devices
3. Massive use of Trusted Locations in CA
4. Usage of "or" instead of "and“ in CA policies
5. Only some/licensed user in scope of CA

User Authentication

Picture: Flaticon.com

How to rollout MFA

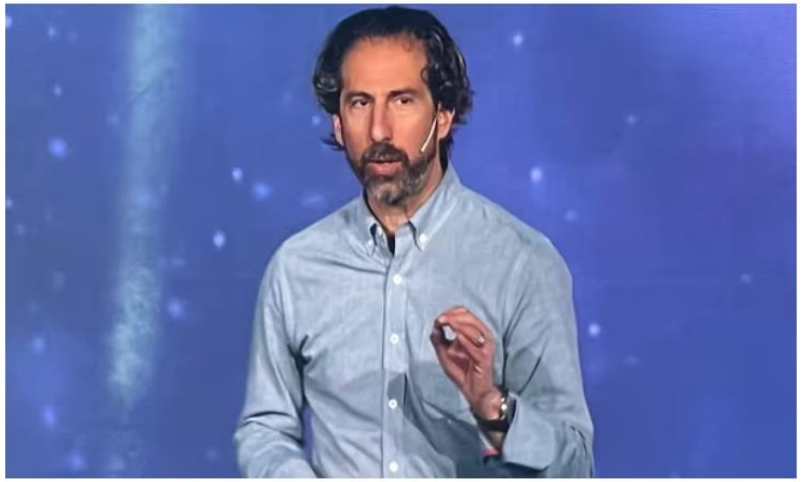
You need:

1. Management Commitment
2. User communication
3. Defined goals
4. measurement tools

Identity and access, Strategy

Customer communications key to Salesforce's mandatory MFA edict

Bradley Barth June 22, 2022



Ian Glazer, senior vice president of identity product management at Salesforce. (Bradley Barth/SC Media)

By the end of its fiscal year last Jan. 31, Salesforce managed to convert approximately 80% of its monthly active users — about 14 million in total — to multi-factor authentication (MFA) or single sign-on (SSO) for all of its login activity.

It's a feat that Ian Glazer, Salesforce's SVP of identity product management, credits in part to a strong internal and external communications strategy that set clear expectations for future identity and access management adoption while building trust among involved stakeholders.

Options for MFA Rollout / Improvement

Conditional Access Policy

Multifactor Authentication Registration Policy

Authentication Method Policy

Authentication Strength Policy

Manual registration by users

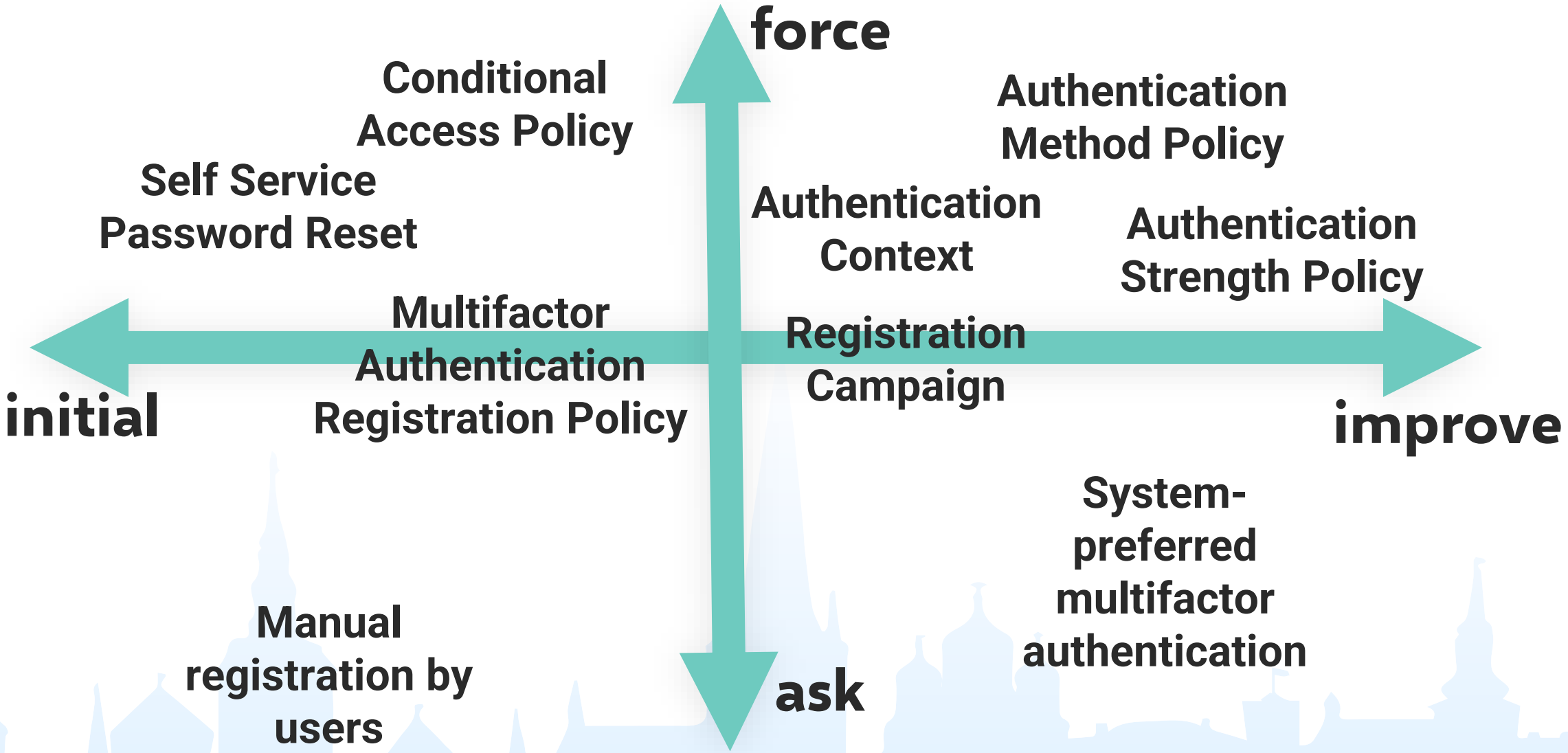
Registration Campaign

Authentication Context

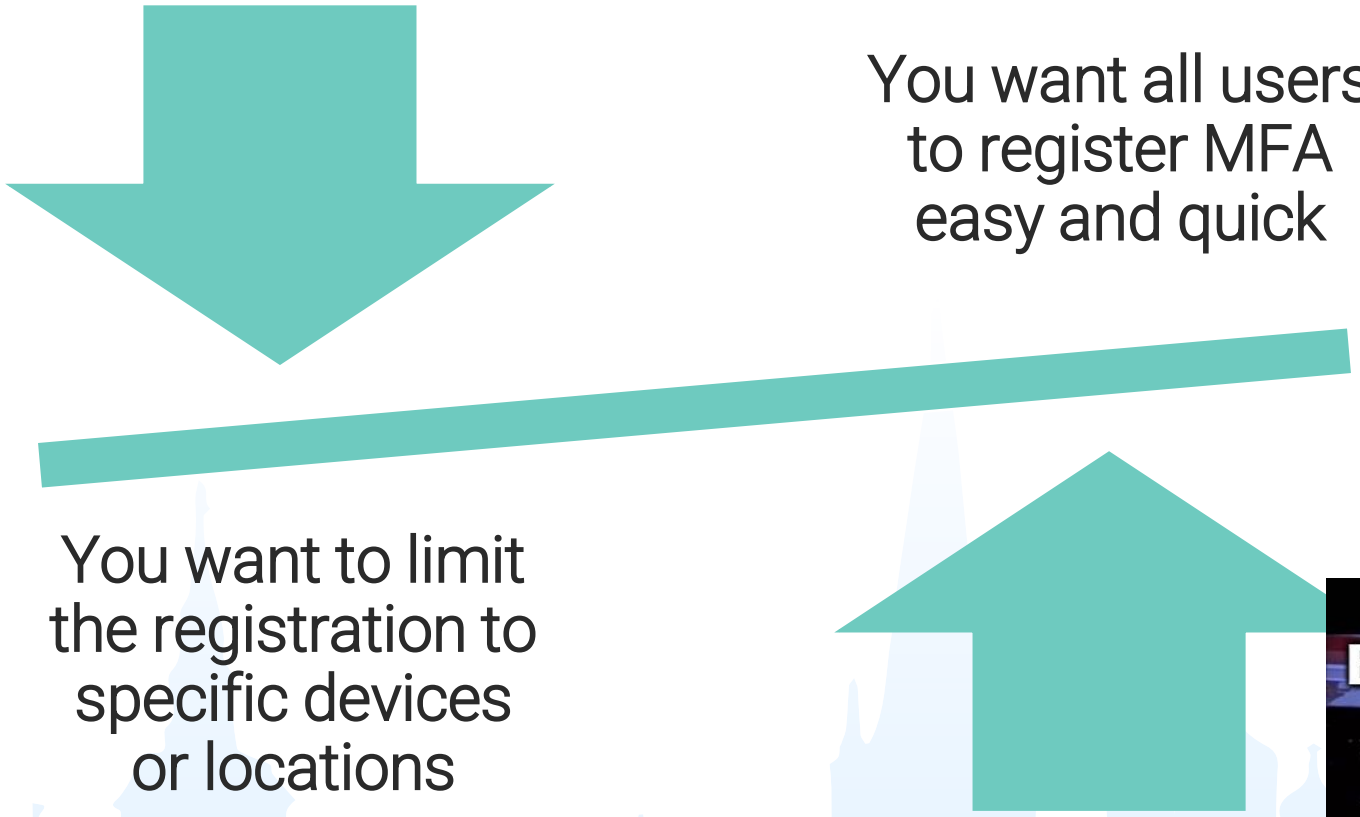
Self Service Password Reset

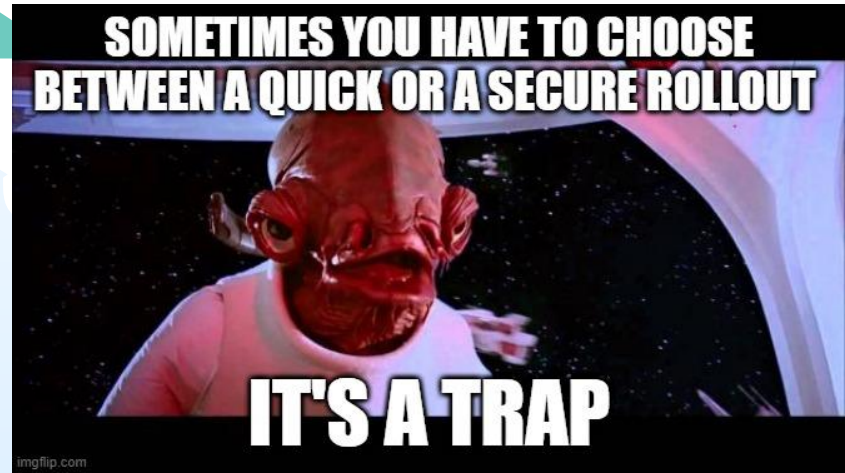
System-preferred multifactor authentication

Options for MFA Rollout / Improvement

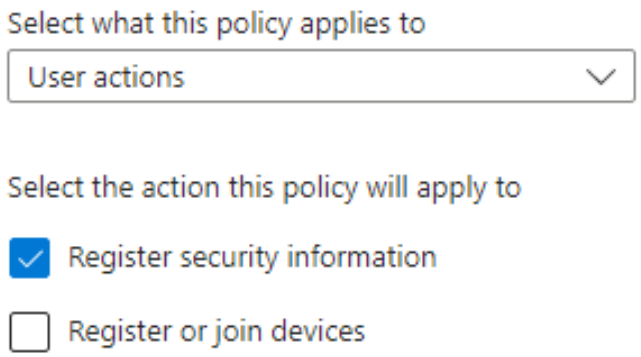


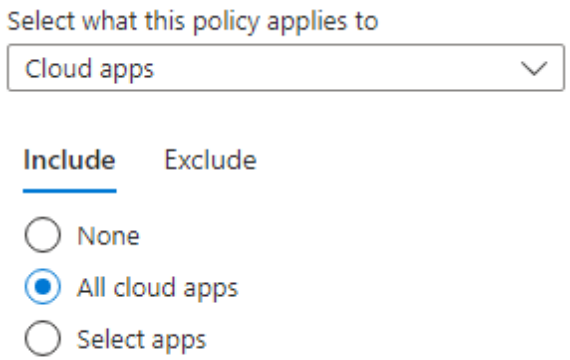
The Security Info Registration Dilemma
(in an early phase)





Security Information Registration





- ☑ Create a dedicated CA policy for the User Action
- ☑ Enforce Trusted Device or MFA (or Location)
- ☑ Use TAP for onboarding

- ☑ Security Info Page is part of All Cloud Apps
- ☑ Security Info Page can‘t be targeted as a single App
- ☑ Only the interrupt mode is bypassed

A typical MFA rollout

Enable Tooling

Define allowed Auth Method

Contact your users on all available channels

Provide all needed informations and inform about goals and timelines

Ask for their support!

Show an optional setup dialog as often as possible

Let the user choose the best moment for setup

First: **Enforce MFA Registration**

Then: **Enforce MFA Usage**

In previous projects I've used Logic Apps to build dynamic groups based on registered Auth Methods

Allow Users to Opt-Out

In most companies only a subset of the users have a corporate mobile device and not everybody is willing to use a private device

Prepare | Ask | Nudge | Force | Optimize and Operate

Authentication Method Policy

Manual Registration

Multifactor Authentication Registration Policy

Conditional Access Policy

Handling the „Opt-Out“-Users

Step 1:

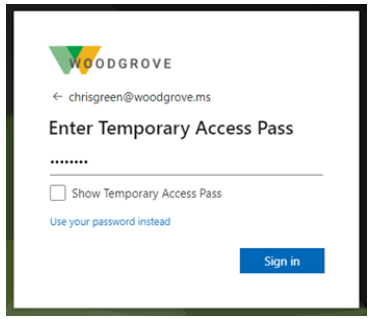
- Use an Access Package with a group as ressource. (Optional: Configure an approval.)
- Exclude this group from MFA Registration Policy and Registration Campaign
- Include the link to the Access Package in your communication and assign permissions to your supporters

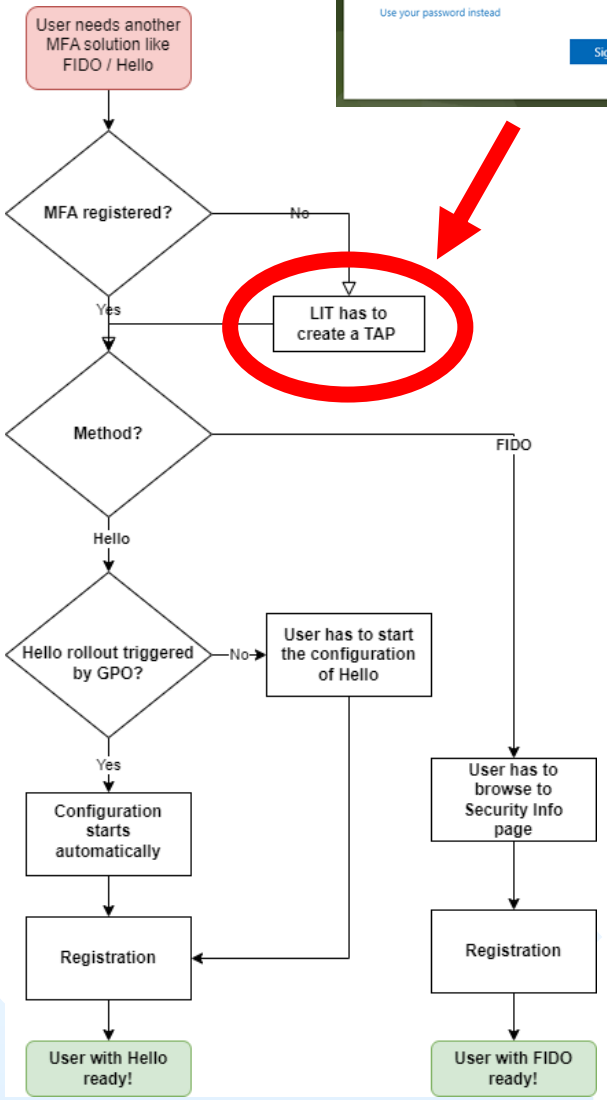
Step 2:

- Establish a dedicated reporting for the „Opt-Out“-Users and assign the task to take care of them.
- They need to be onboarded to WH4B/ FIDO2 with a Temporary Access Pass
- Enforce MFA for all enrolled WH4B/FIDO2 users with Conditional Access

**Side note: Imo there is no use case for access from Mobile Devices without the Authenticator App (and I‘ve never seen a MAC user without an iPhone)* 😉

Enable your support!



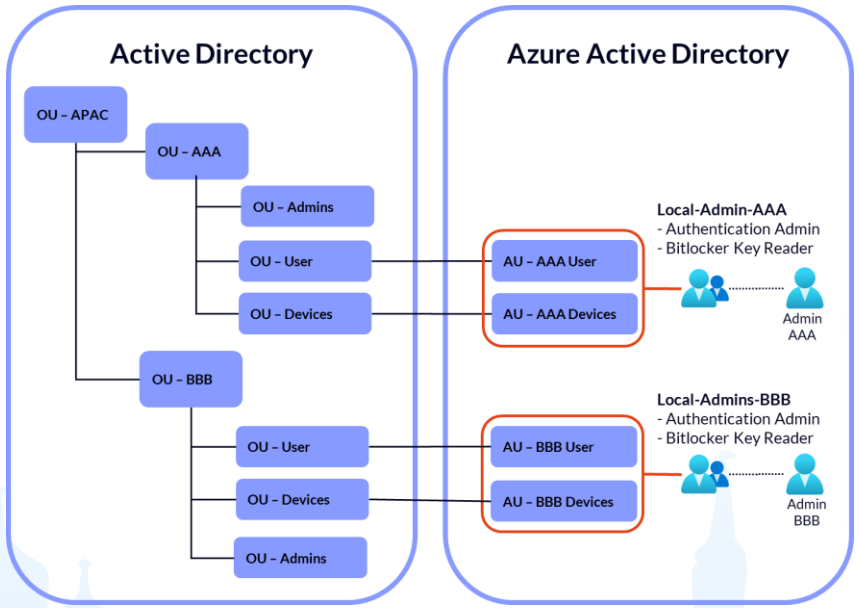


It's useful if your local Admins are able to:

- ☑ Support users while setup
- ☑ See and understand the Sign-In Logs
- ☑ Create Temporary Access Passes
- ☑ See registered methods and Reset MFA

for the users in their responsibility.

Use Administrative Units for e.g. locations



Better Together

device independent

Use Cases:
- Shared PCs
- Admin Accounts
- Unmanaged Devices
- AVD / Win365

Win+Mac+iOS (+more to come)

Standard - Works with every major identity provider

manual rollout by user with hardware and no automation

phishing-resistant

passwordless

Requires MFA for setup

No SSPR method

integrated in device

Win10/11 (+Mac)

Use Case:
- Personal Devices

Propriety - works only with EID*

lightweight automated rollout on new or old clients

*Windows Hello can now also be used as a Passkey

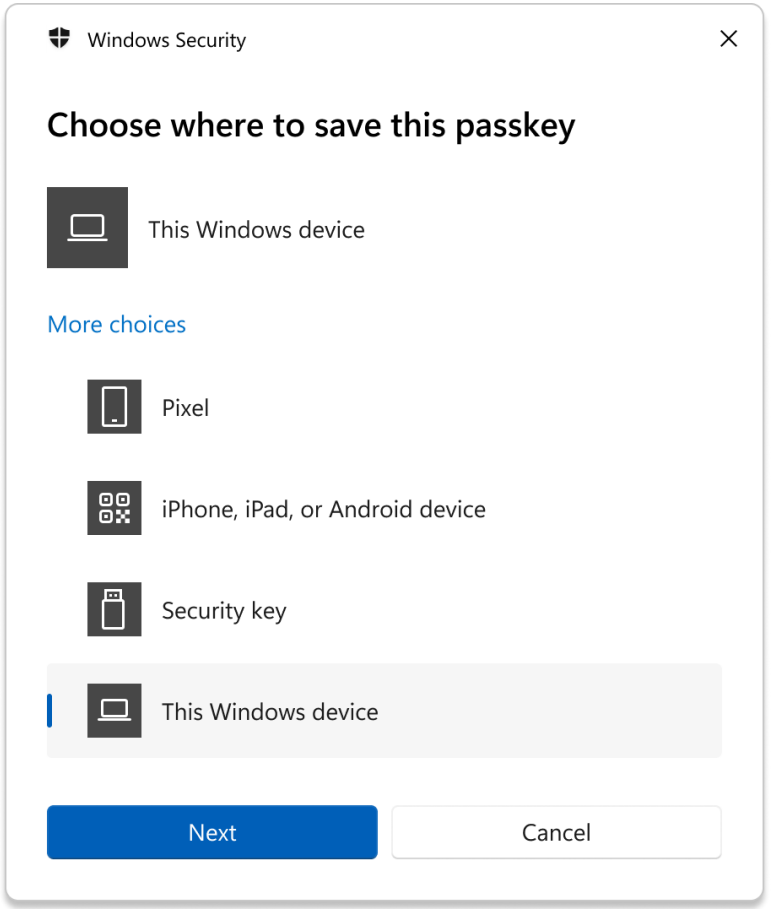
What about passkeys?

Learn more

2024 will be the year of the passkey

FIDO keys can already be used as a passkey
Windows Hello can already be used as a passkey
Android and iOS can already be used as a passkey

Microsoft Authenticator will be soon usable as passkey
Login to Entra ID with (devicebound) passkeys will be soon possible



This will change a lot but it is not already there and I can‘t share rollout experience with you so far!

A typical FIDO rollout

Enable Tooling

Define User groups
- With registered MFA method
- Without registered MFA method

Contact your users on all available channels

Provide all needed informations and inform about goals and timelines

Ask for their support!

Distribute Hardware

- For Users with MFA you can send the HW eg. by mail
- For User without MFA an OnSite appointment at the local IT is often necessary

Enforce MFA Usage
-> For users without other registered MFA method

Enforce FIDO Usage (optional)
-> Depends on your Use Case

Take care for the other lifecycle processes

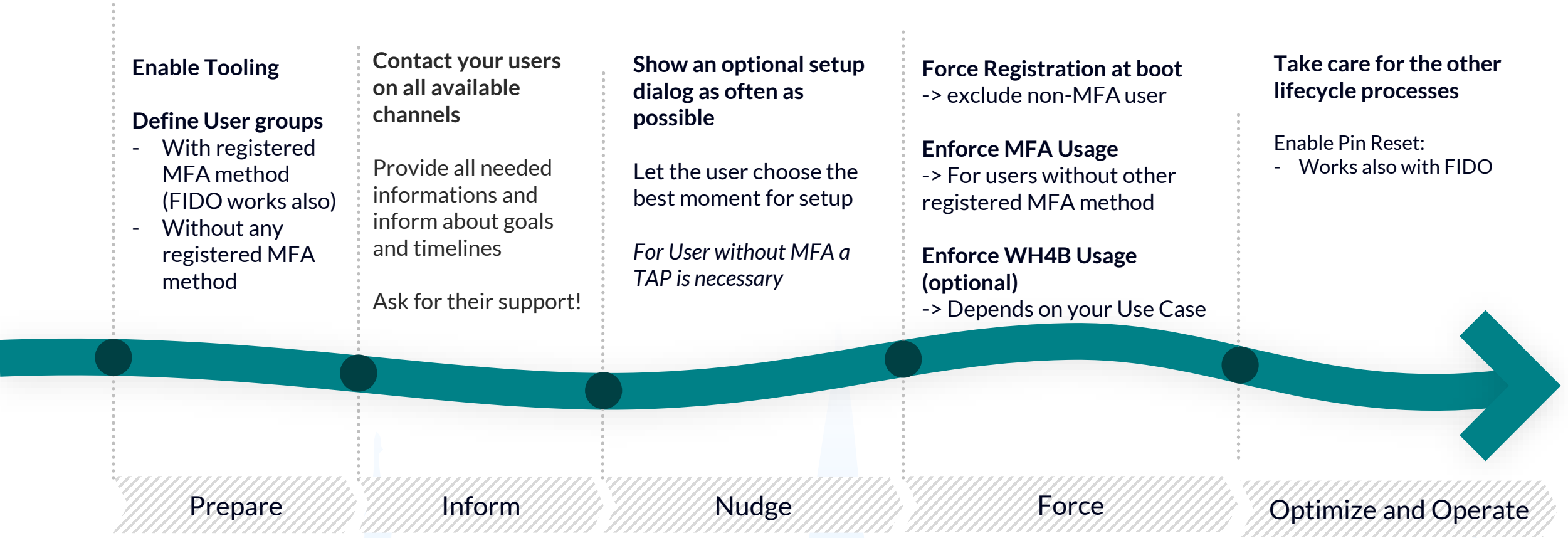
Keys can be:
- lost/stolen
- Forgotten
- ...

Users can:
- Leave the company
- ...

Prepare | Inform | HW-Handover | Force | Optimize and Operate

Conditional Access Policy with Authentication Strength

A typical WH4B rollout (on existing clients)



WH4B config enforced

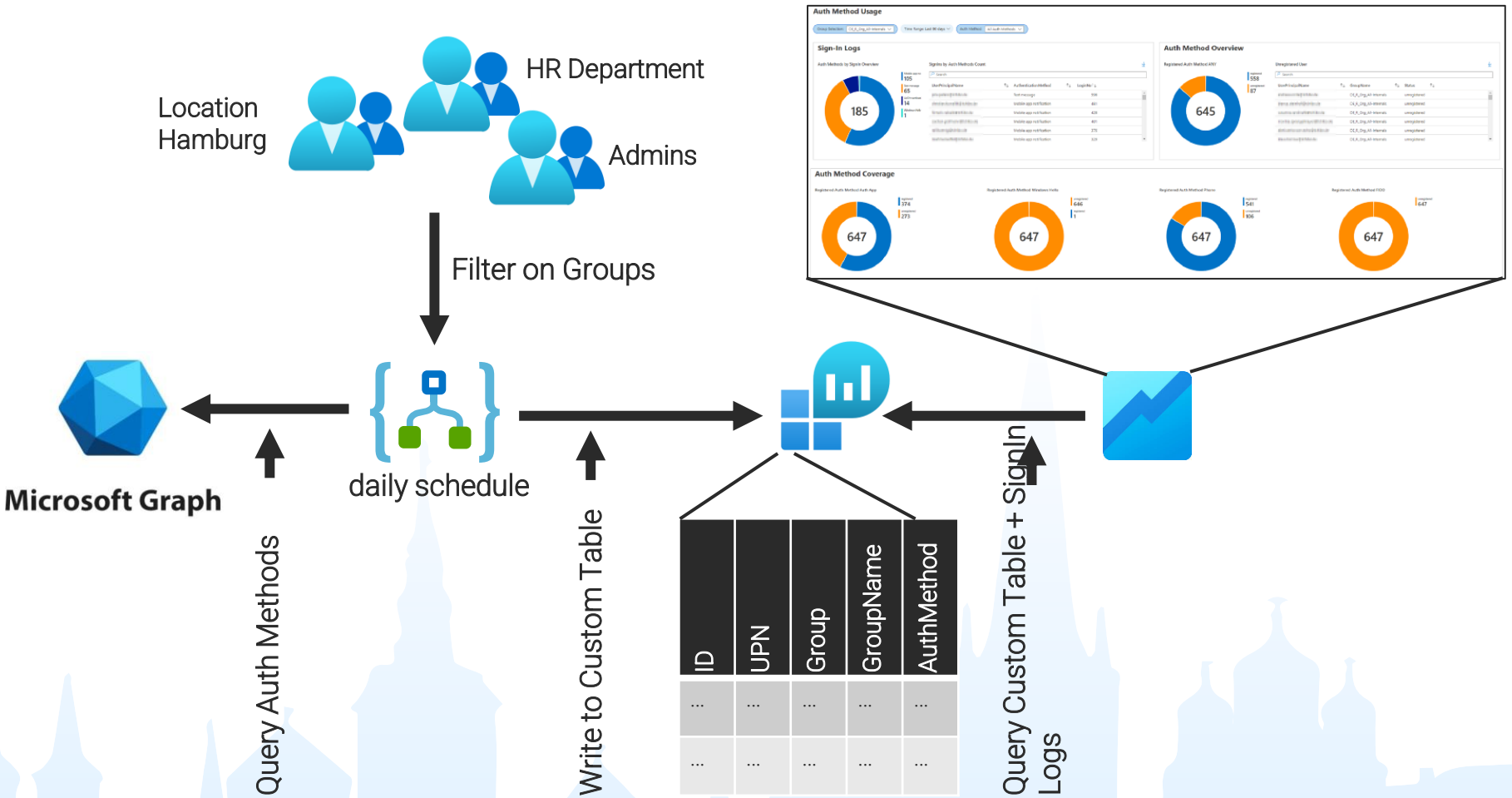
DisablePostLogonProvisioning

Conditional Access Policy

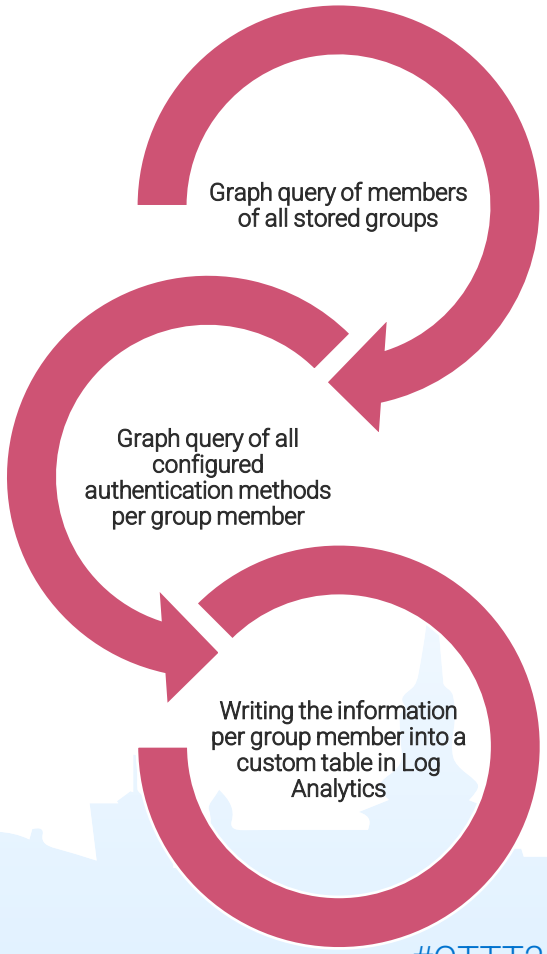
Challenges while WH4B Enrollment

Sometimes user register their office phone as MFA method and Admins migrate PSTN to MS Teams…

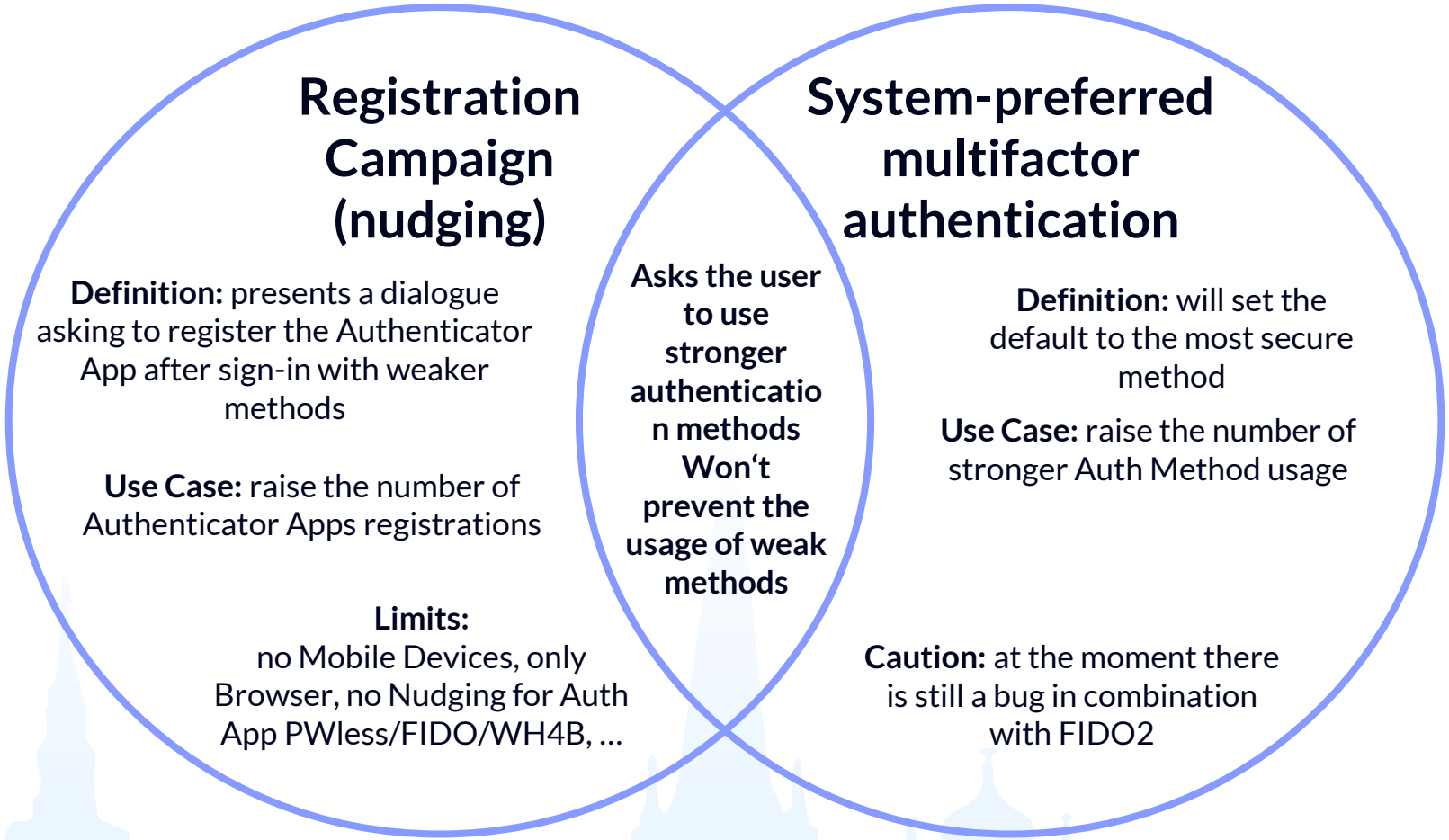
Strong Authentication Dashboard



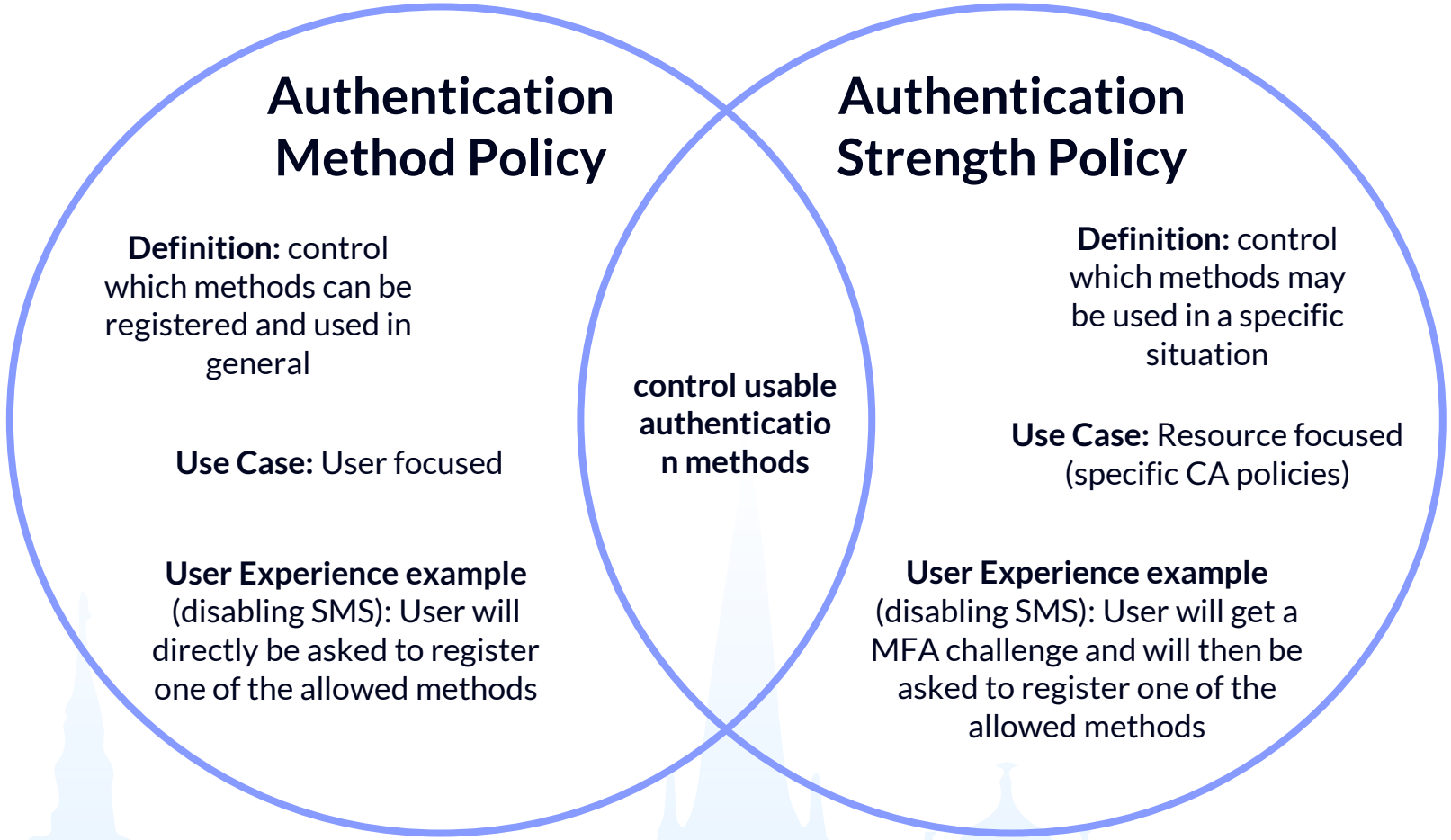
Structural flow of the required Logic App



Improve Auth Methods – the soft way!

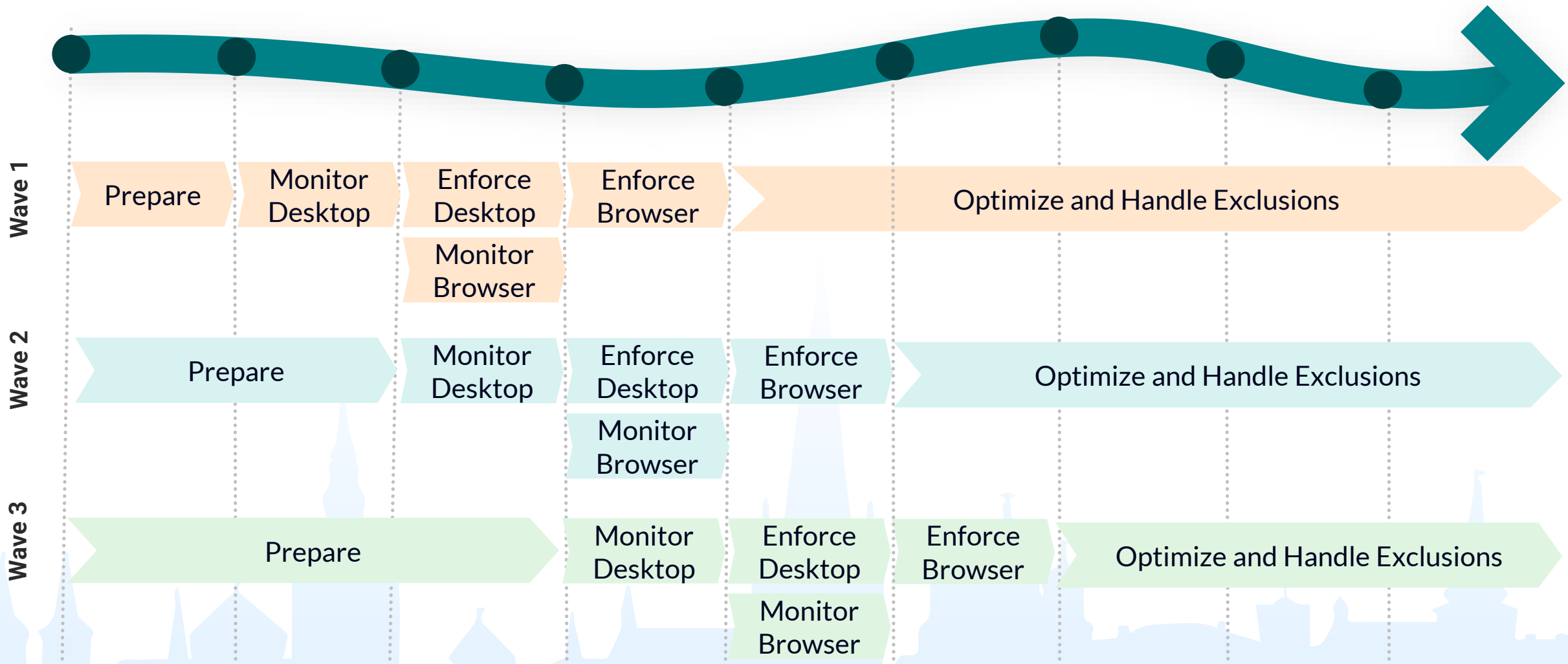


Improve Auth Methods – the effective way!



Device Authentication

A typical Managed Device Enforcement rollout



BuiltIn Conditional Access Reporting

Conditional Access insights and reporting

For tenants with high volume of sign-ins, this workbook may not support filtering by time ranges longer than 24 hours. Microsoft recommends using the Conditional Access overview dashboard instead.

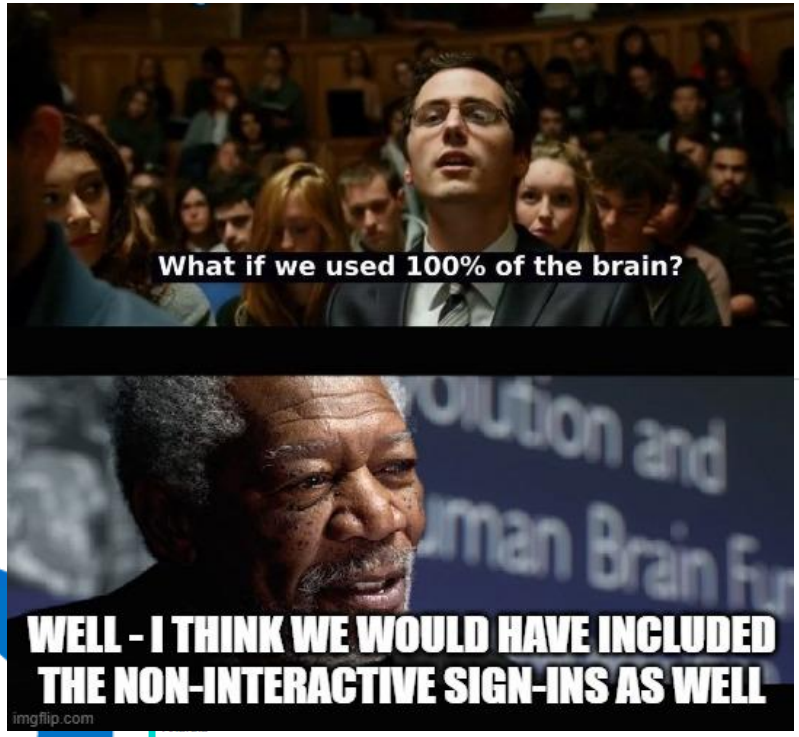
User sign-ins | Service principal sign-ins

Conditional Access policy: Select all enabled policies - All ... | Time range: Last 24 hours | User: All users | App: All apps | Data view: users

Impact summary

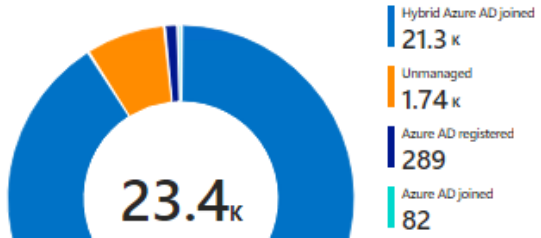
Click on the tiles below to filter the report by the selected Conditional Access result.

Total	Success	Failure	Not applied
22.6K users	17.6K users	1.39K users	21.8K users



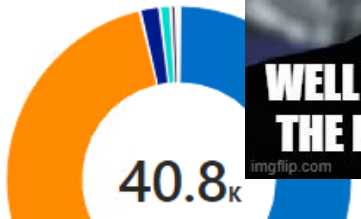
Breakdown per condition and sign-in status

Device State - Total



Hybrid Azure AD joined 21.3K
Unmanaged 1.74K
Azure AD registered 289
Azure AD joined 82

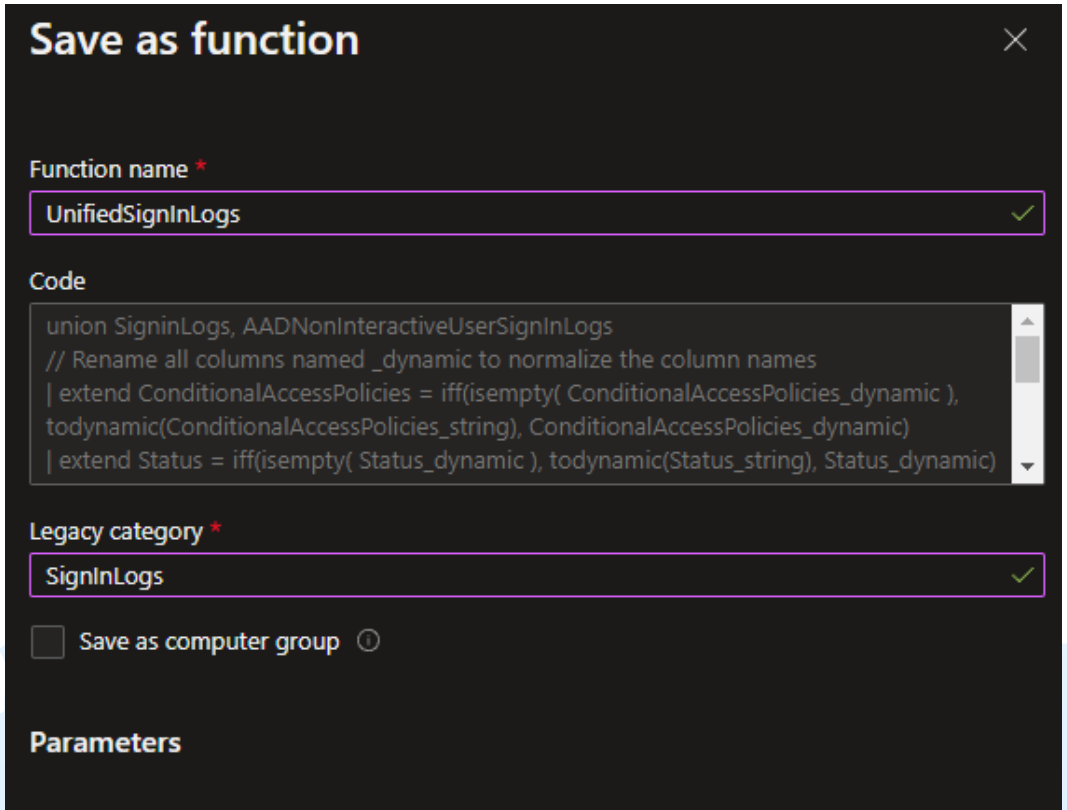
Device platform - Total



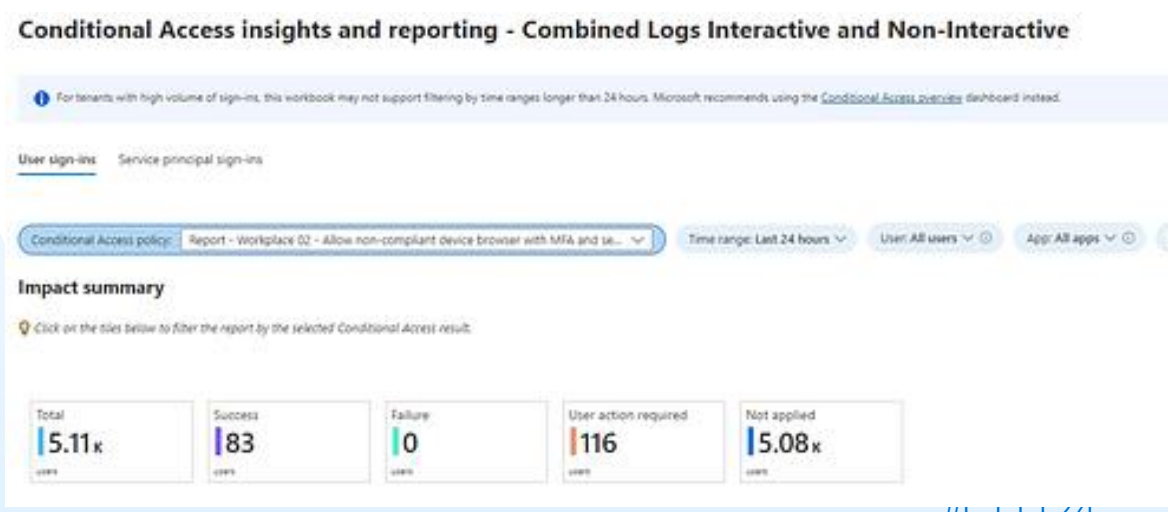
415

Combined Sign-in Logs

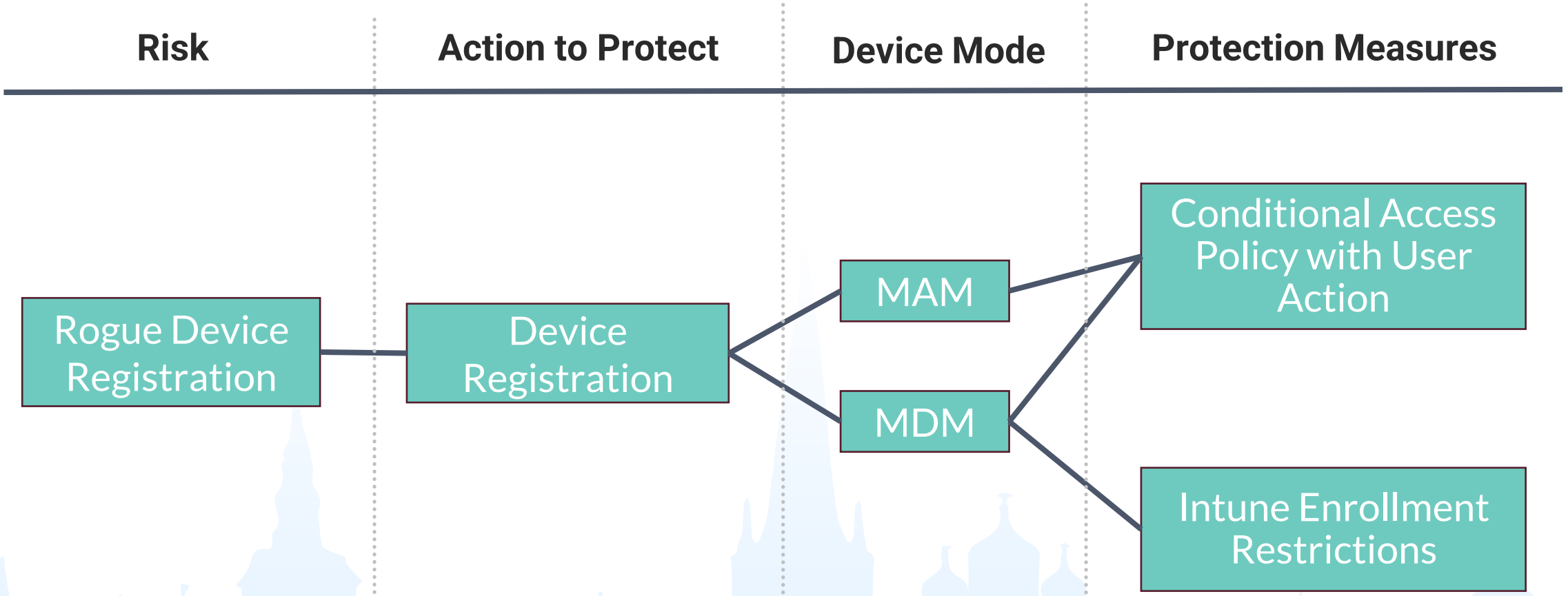
Use Fabians UnifiedSignInLogs function!



Use my extended Workbooks!



The Rogue Device Threat




To Do List
1. Rollout and enforce MFA
2. Improve used methods
3. Enforce the usage of trusted devices
4. Protect the Registration of Methods and Devices

Thank you!

PLATINUM

resco

AvePoint

SILVER

PROMISE
GRUPA APN PROMISE

502nm

WORKSHOPS

ARROW

COMMUNITY

EUROPEAN CLOUD SUMMIT

GOLD

pax8

Visit Tallinn

Sparkle

BRONZE

NORDIC KOOLITUS

ESPC

FORCEWORKS GLOBAL

QUBIX

OIXIO Digital

CRMK

DYNAMICS MINDS

netspore

ColorCloud HAMBURG

cloudtechtallinn.com

CTTT

#CTTT24

Session No. 43

Please rate this session!

Your feedback will help with

- speaker evaluation
- content relevance
- decision making for future events
- quality improvement

Q&A