



# Microsoft Ignite



# Pre-Day: Raising your organization's security posture with Microsoft's cloud

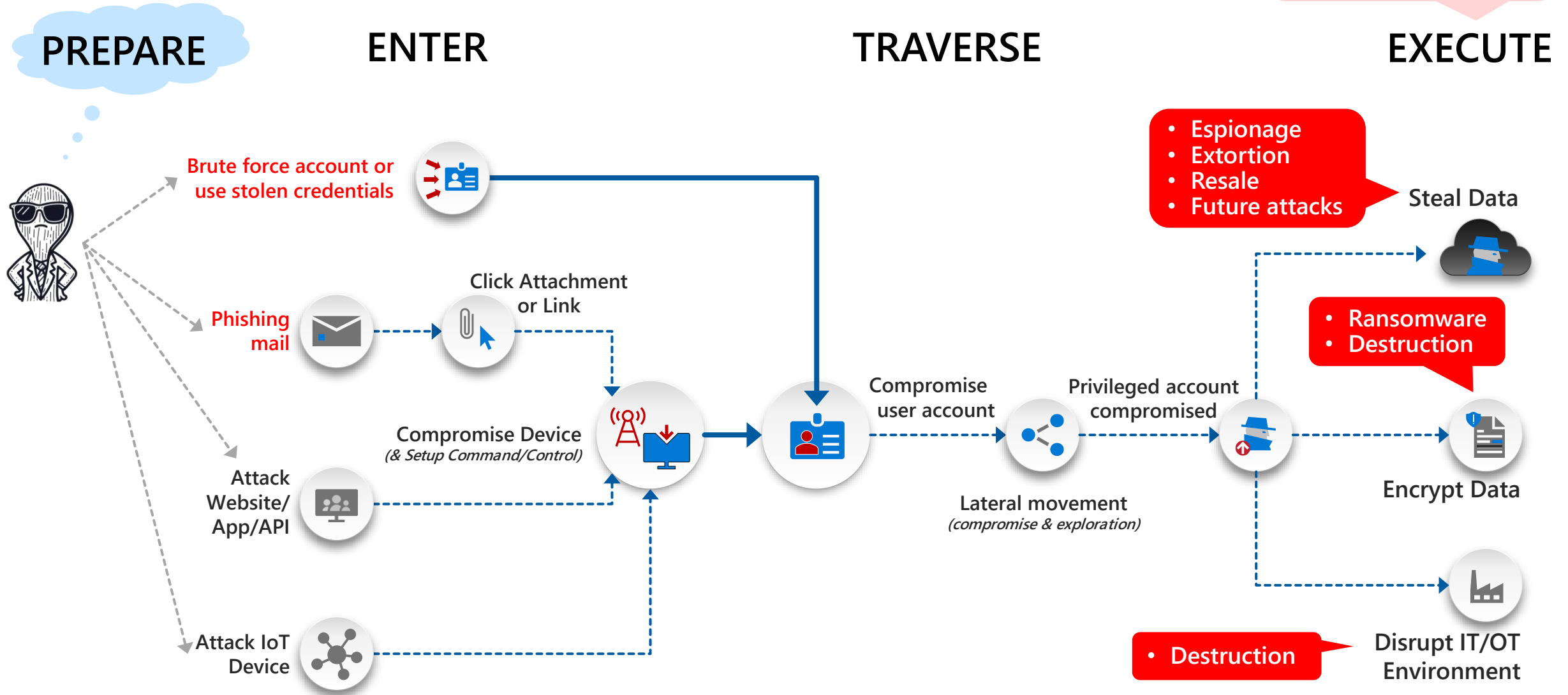
Janice Ricketts  
David Hoerster

# Microsoft Entra ID

# What are bad actors trying to do?

*Potential Payoff:*

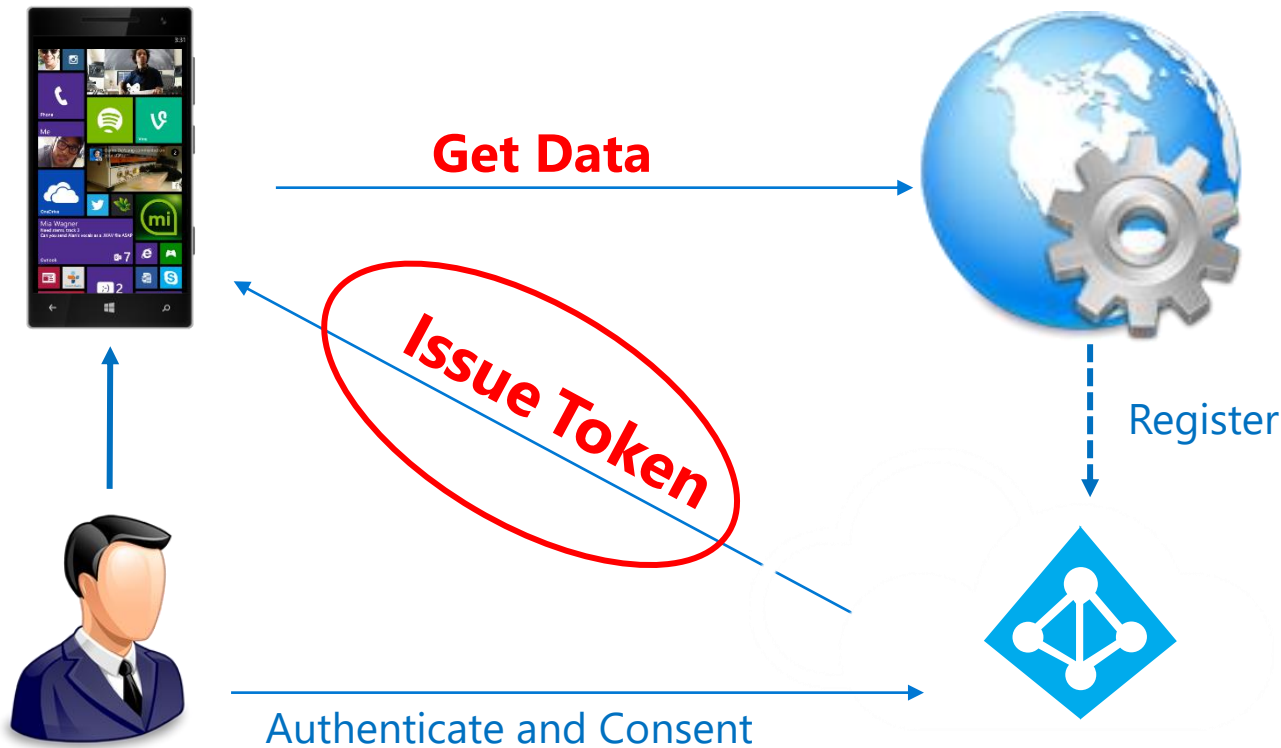
- Profit
- Further a Mission



# Entra ID AuthZ

Client Device

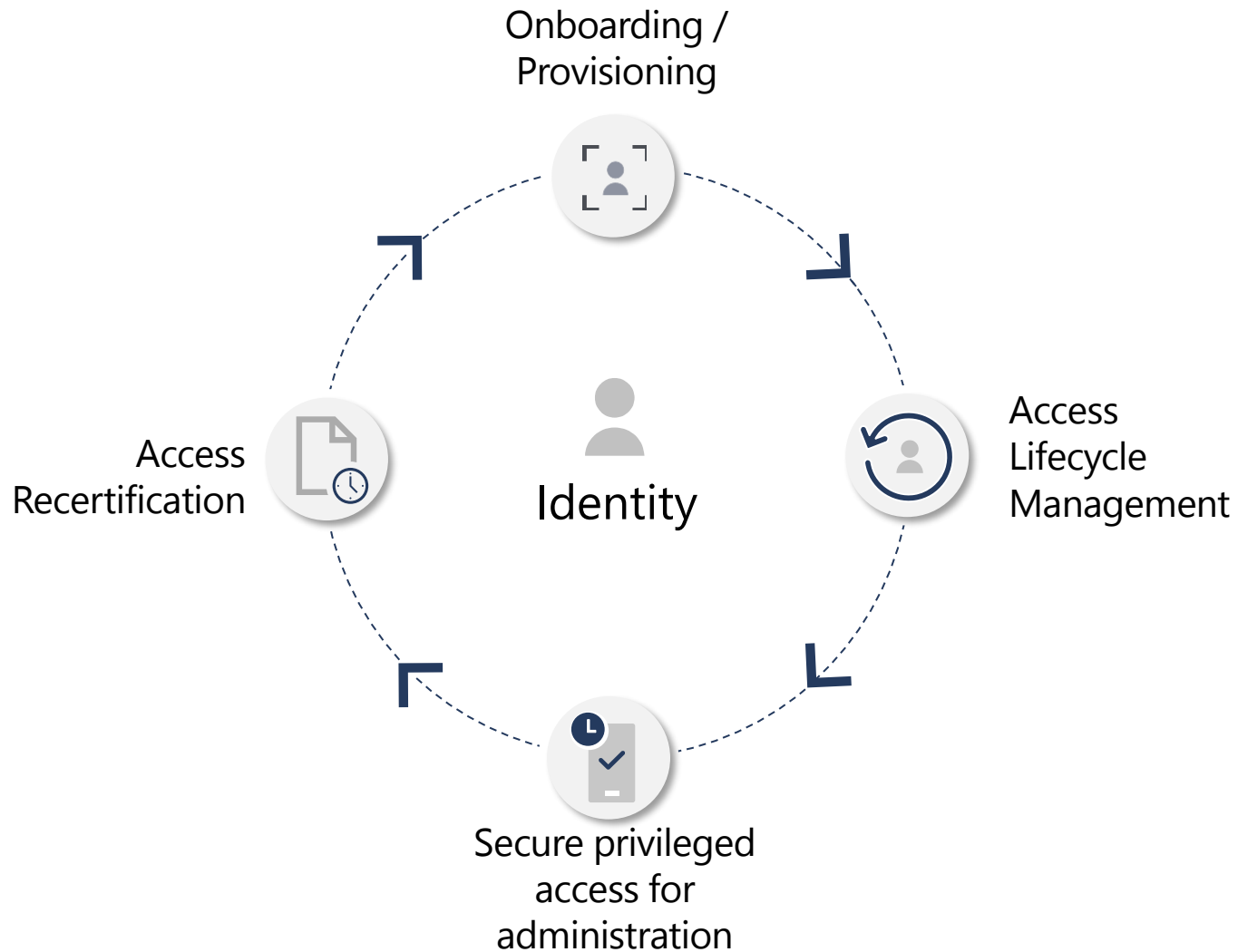
Resource Server



Resource Owner (User)

Entra ID

# Entra ID



01

Who has/should have access to which resources?

02

What are they doing with that access?

03

Are there effective organizational controls for managing access?

04

Can auditors verify that the controls are working?

# It's bad out there!

*For sale in "bad neighborhoods" on the internet*

Attacker techniques,  
business models, and  
skills/technology, are  
continuously evolving

## Other Services

Continuous attack  
supply chain innovation

## Attacker for hire (per job)

\$250 per job (and up)

## Ransomware Kits

\$66 upfront  
(or 30% of the profit / affiliate model)

## Compromised PCs / Devices

PC: \$0.13 to \$0.89  
Mobile: \$0.82 to \$2.78

## Spearphishing for hire

\$100 to \$1,000  
(per successful account takeover)

## Stolen Passwords

\$0.97 per 1,000 (average)  
(Bulk: \$150 for 400M)

## Denial of Service

\$766.67 per month

**Attackers**

Many attack tools and  
tutorials/videos available  
for free on internet

The odds are  
**against** today's  
security analysts



**4,000**

Password attacks per second



**72 mins**

Median time for an attacker to access your private data if you fall victim to a phishing email



**3.5M**

Global shortage of skilled cybersecurity professionals




# Turn on MFA!

Better yet – go

Passwordless!

## Reduces attack risk by

99.9%



# Even better than MFA - Passwordless

(Nobody likes passwords!)

## Value to the User

*Your users never need to remember their passwords*

## Value to the Organization

*User credentials cannot be broken, stolen, or violated*

Windows 10 device, Phone, or Security key  
And  
Biometric gesture or PIN

Windows Hello for Business  
Microsoft Authenticator  
FIDO2 security keys  
Certificate-based authentication

# Self Service Password Reset - benefits



MFA and passwordless means users forget their passwords...

## Save money

- \$ spend on password reset ticket volume
- Not uncommon for companies to spend \$100K per month, average, for calls to the helpdesk

## Save time

- **For users** – ability to reset their password saves time and increases productivity
- **For IT teams** – helpdesk and IT admin do not have to get involved

## Increase security

- Make the password reset process more secure
- Reduce calls to the helpdesk, which reduces opportunities for social engineering

# Self Service Password Reset (SSPR)

Self-service password reset includes:

- **Password change:** I know my old password but want to change it to something new.
- **Password reset:** I can't sign in and want to reset my password using one or more approved authentication methods.
- **Account unlock:** I can't sign in because my account is locked out and I want to unlock using one or more approved authentication methods.

\*Users can only reset their password if they have data present in the authentication methods that the administrator has enabled.

# What is conditional access?



Conditional access capability of Azure Active Directory enables you to enforce controls on the access to applications in your environment based on specific conditions from a central location.



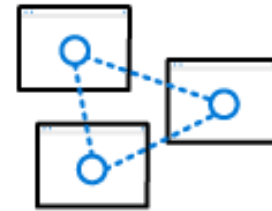
User- and location-based conditional access

Keep sensitive data protected by limiting user access based on geo-location or IP address with [location-based conditional access policies](#).



Device-based conditional access

Ensure that only enrolled and approved devices can access corporate data with [device-based conditional access](#).



Application-based conditional access

Work doesn't have to stop when a user is not on the corporate network. [Secure access to corporate cloud and on-premises apps](#) and maintain control with conditional access.



Risk-based conditional access

Protect your data from hackers with a [risk-based conditional access policy](#) that can be applied to all apps and all users, whether on-premises or in the cloud.

# Conditional access features: Conditions

Conditional access policy triggers controls when all conditions are met.  
Conditions are logically 'ANDed'.

"**When this happens**" is called a **condition**.  
"**Then do this**" is called an **access control**.

Conditions available:

- Users and groups
- Cloud apps OR Actions
- User Risk
- Sign-in risk
- Device platforms
- Locations
- Client apps
- Filter for devices

Users and groups

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest and external users ⓘ

☒ Directory roles ⓘ

Global administrator

☐ Users and groups

Cloud apps

Include Exclude

☐ None

☐ All cloud apps

☒ Select apps

Select

Office 365

## User risk level

Configure ⓘ

Yes No

Configure user risk levels needed for policy to be enforced

- ☐ High
- ☐ Medium
- ☐ Low

## Sign-in risk level

Control user access to respond to specific sign-in risk levels. [Learn more](#)

Configure ⓘ

Yes No

Sign-in risk level is generated based on all real-time risk detections.

Select the sign-in risk level this policy will apply to

- ☐ High
- ☐ Medium
- ☐ Low
- ☐ No risk

## Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure ⓘ

Yes No

Include Exclude

- ☒ Any device
- ☐ Select device platforms
- ☐ Android
- ☐ iOS
- ☐ Windows Phone
- ☐ Windows
- ☐ macOS
- ☐ Linux

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

Yes No

Include Exclude

- ☐ Any location
- ☒ All trusted locations
- ☐ Selected locations

## Client apps

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ

Yes No

Select the client apps this policy will apply to

Modern authentication clients

- ☒ Browser
- ☒ Mobile apps and desktop clients

Legacy authentication clients

- ☒ Exchange ActiveSync clients
- ☒ Other clients ⓘ

## Filter for devices

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure ⓘ

Yes No

- Devices matching the rule:
- ☒ Include filtered devices in policy
- ☐ Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
--------	----------	----------	-------

# Conditions: When does this policy apply?

## Users and groups

Include or exclude specific users and/or groups, directory roles, guest and external users

## Cloud Apps

Include or exclude specific AAD apps or apply to all apps.

## Actions

Registering user security information or devices.

## How to use

These filters support both including and excluding. This allows a policy to focus on a group or on apps, or it allows other apps or users to be exempted from this policy.

Users and groups

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest and external users ⓘ

☒ Directory roles ⓘ

Global administrator

☐ Users and groups

Cloud apps

Include Exclude

☐ None

☐ All cloud apps

☒ Select apps

Select

Office 365

Select what this policy applies to

User actions

Select the action this policy will apply to

☐ Register security information

☐ Register or join devices

Name \*

CA004: Require multifactor authentication f ...

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

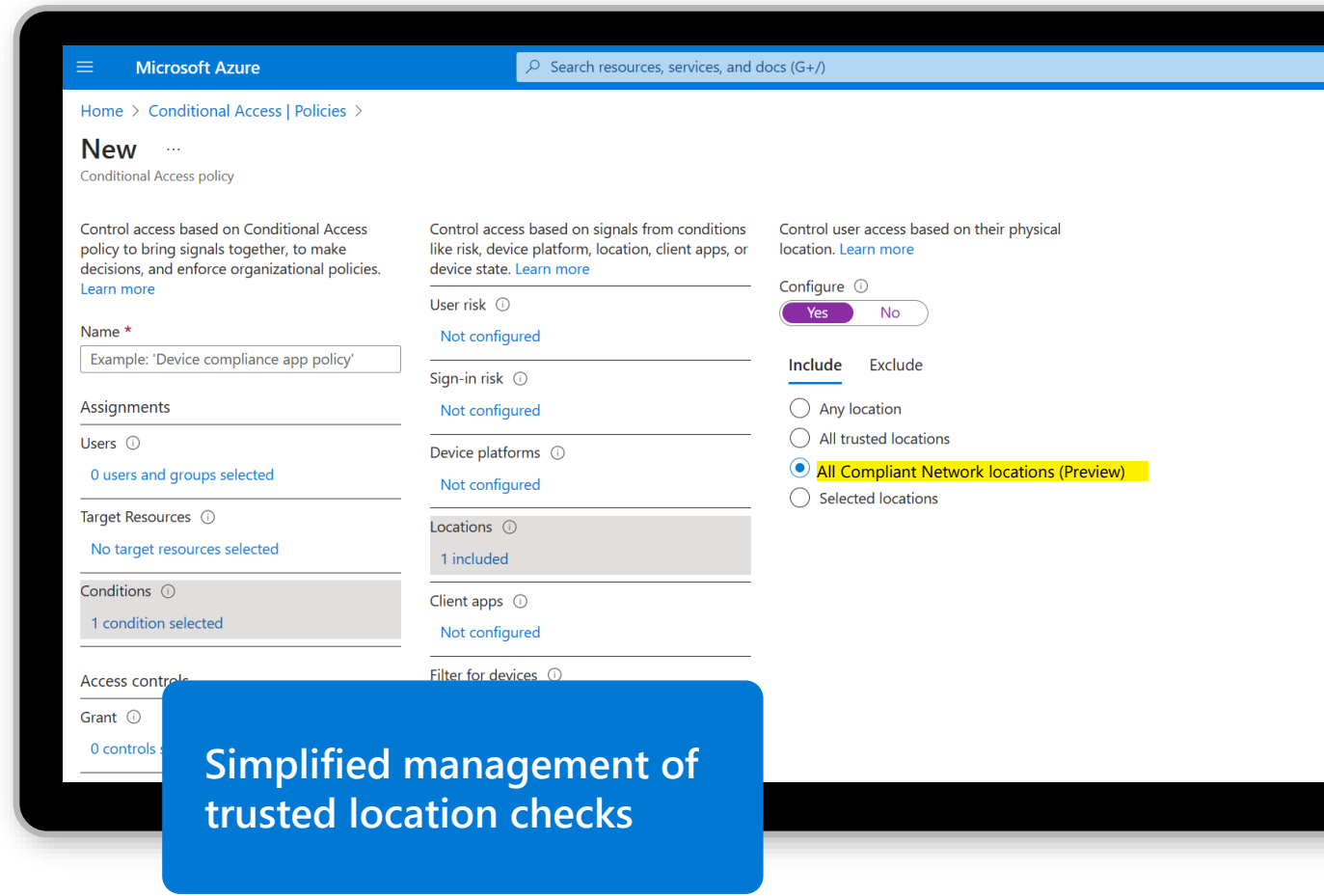
Enable policy

Report-only On Off

# Compliant network check – SSE Public Preview

Stop user bypass of edge security stack and protect against token theft

- » Validates user is connecting from verified device/network of your tenant
- » Ensures that user has not bypassed underlying security **controls**: Universal Conditional Access and continuous access evaluation policies at network access gate, network firewall/filtering, DLP, CASB, IDPS, etc., while accessing cloud apps
- » **Enhanced user productivity**: No need to hairpin remote users to central egress points to enforce compliance checks
- » **Continuous access evaluation integrated for instantaneous access revocation**
- » **Built-in support for tenant level granularity**
- » **All the security, without any of the Src IP management overheads**
- » **Helps with seamless transition to IPv6 when IPs become even more cumbersome to manage**
- » **Integrated with trusted location construct**





# Microsoft Entra ID Labs

---

Task 1 – Create a Microsoft Entra ID Account

Task 2 – Sign in with the new account

**Task 3 - Enable passwordless phone sign-in authentication methods**

**Task 4 – Configuration of SSPR**

Task 5 – Managing the SSPR Security Group

Task 6 – Auditing Password Reset

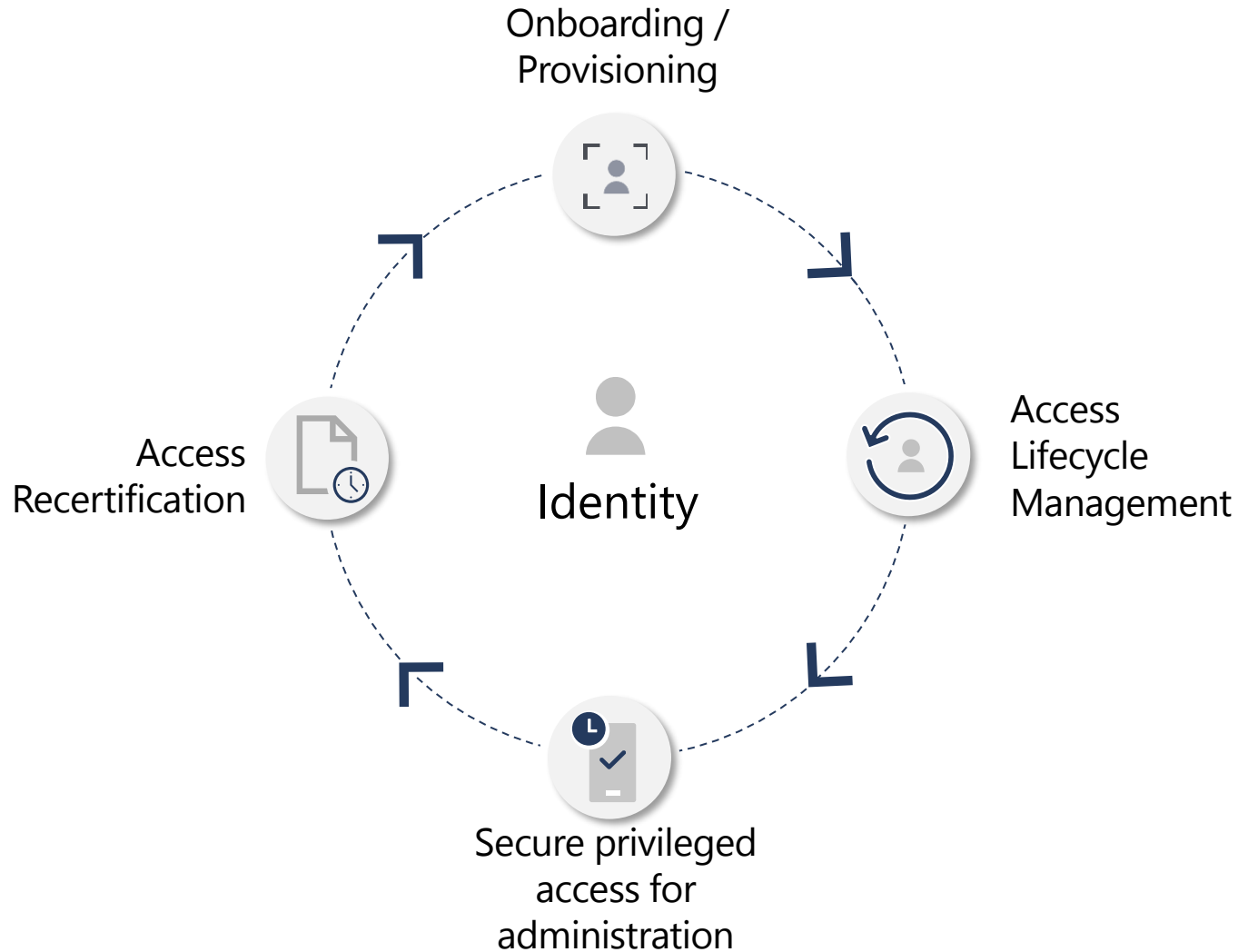
Task 7 – Reset a Password

**Task 8 – Creating Conditional Access Policies**

Task 9 – The Conditional Access What If tool

# Microsoft Entra ID Governance

# What is Microsoft Entra Identity Governance?



01

Who has/should have access to which resources?

02

What are they doing with that access?

03

Are there effective organizational controls for managing access?

04

Can auditors verify that the controls are working?

# Access requests, workflow and approvals

## Entitlement management

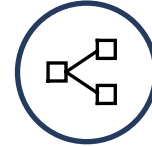
---



Let users request access (to any connected app, group, Teams site and more) while automating access assignments, approval, workflows, reviews and expiration for all human identity types (users, guests, etc.)



Self-service policy and workflow can be defined by app, group or site owners



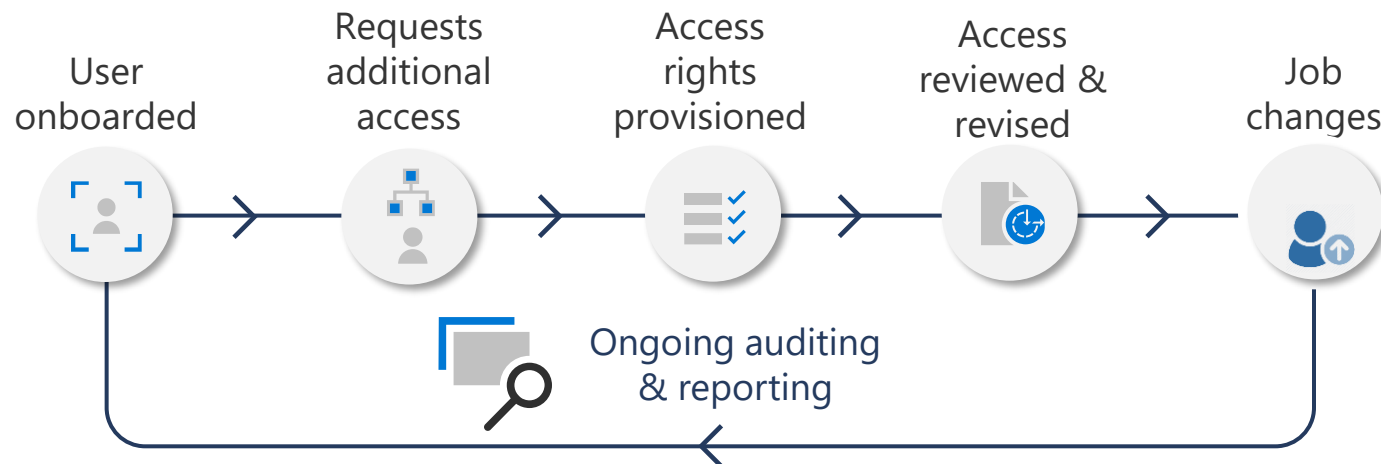
Supports multi-stage approval workflow, separation of duties enforcement and recurring access recertification



Supports custom workflows for access lifecycle (through Logic Apps integration)



Access time-limited, guests removed when last access expires



# Guest attribute management

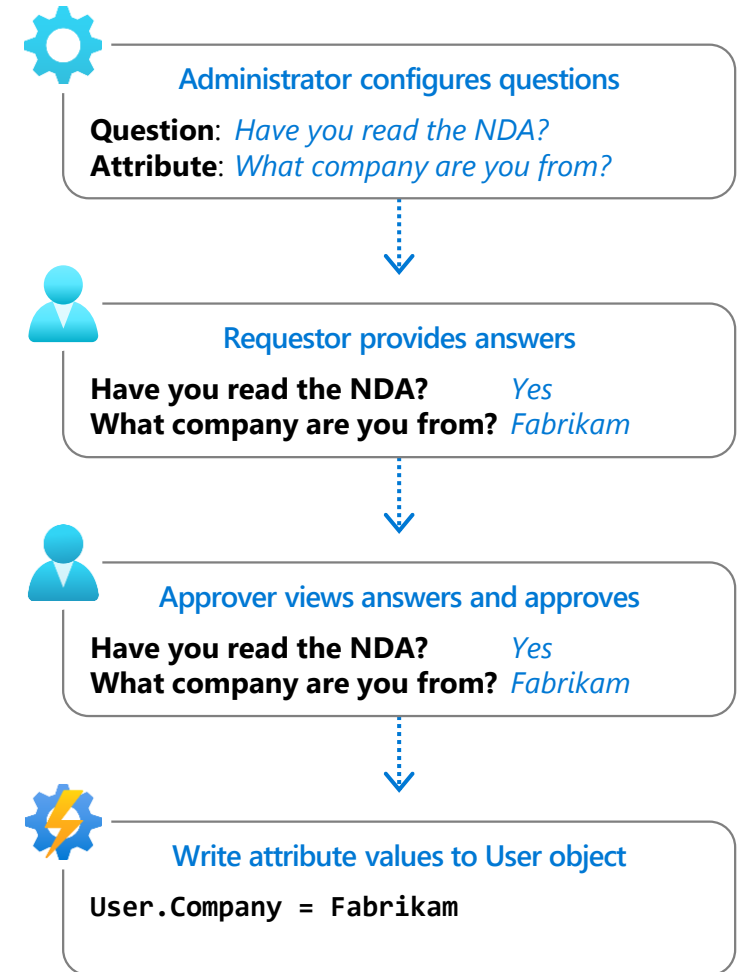
---

## Collect additional information from requestors

- Include custom questions that are surfaced within the request flow.
- Approvers are shown the information as part of the request so they can make better decisions.

## Store provided information in User attributes

- If your apps or processes need to reference it later, you can also store requestor information in attributes automatically.
- Especially useful for onboarding external users.



# Access recertification to reduce risk

## Access Reviews

---



---

Natively built-in to Entra  
ID

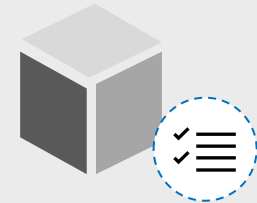
---



---

Manage risk and meet  
compliance for users,  
guests and workload  
identities

---



---

Ensure access to  
sensitive Teams, Groups,  
Apps, Roles is reviewed  
periodically

---

# Access recertification to reduce risk

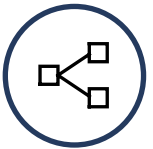
## Access Reviews



**Policy-based** access certification for automation



**Intelligent recommendations** based on sign-in history



**Multi-stage** reviews



**Audit history** for compliance reviews



Native support for **B2B guest** users, privileged roles, non-human workload identities



**Customizable notifications** to reviewers



**Downloadable reports** to see how reviewers are performing



**Out-of-the-box integration** with Microsoft Teams

← Access reviews

FY22 Quarterly review

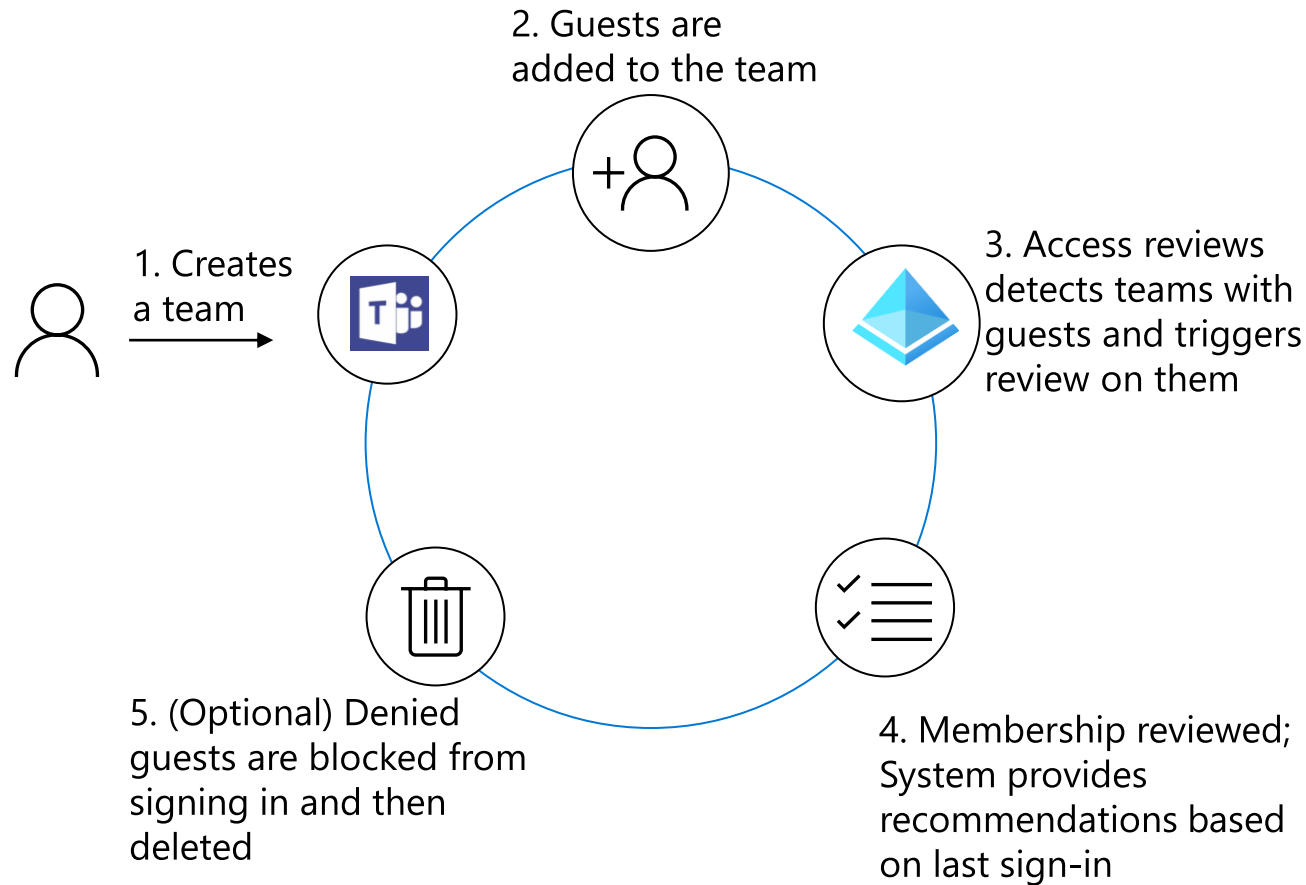
Please review members of 'FY22 Planning' [See details](#)

✓ Approve ✗ Deny ? Don't know ↺ Reset decisions 🗒 Accept recommendations

Name ↑	Recommendation	Decision
<input checked="" type="checkbox"/> abhijeet sinha absinh@fimdev.net	Approve Last signed in (Jul 1, 2021) less than 30 days before review began	
<input checked="" type="checkbox"/> Barclay Neira barclayn@fimdev.net	Deny Last sign-in date unknown	
<input checked="" type="checkbox"/> Bhaskar Kamasani vikama@microsoft.com	Deny Last signed in (May 6, 2021) more than 30 days before review began	
<input type="checkbox"/> Bhavesh Patel bpatel@microsoft.com	Approve Last signed in (Jun 30, 2021) less than 30 days before review began	
<input type="checkbox"/> Blake Nelson Blake.Nelson@microsoft.com	Approve Last signed in (Jun 21, 2021) less than 30 days before review began	
<input type="checkbox"/> Bob Grumpy bobgrumpy@fimdev.net	Deny Last signed in (Apr 5, 2021) more than 30 days before review began	
<input type="checkbox"/> Cassie King cassie@fimdev.net	Deny Last signed in (May 8, 2020) more than 30 days before review began	
<input type="checkbox"/> Chris Griffiths chgriff@fimdev.net	Deny Last signed in (May 12, 2020) more than 30 days before review began	
<input type="checkbox"/> Chris Wood chrwood@microsoft.com	Deny Last signed in (Nov 19, 2020) more than 30 days before review began	
<input type="checkbox"/> ChrisGreenUAA ChrisGreenUAA@fimdev.net	Deny Last sign-in date unknown	
<input type="checkbox"/> Dalki	Approve	

# Reduce risk of guest users in Teams and Microsoft 365 groups

---



**Newly created groups** that have guests, and **existing groups** that have newly added guests are automatically included in the review

Designate **group owners** or **guests themselves** to be the reviewer

Ensure that guest users retain only the **access they need** to Teams and Microsoft 365 groups



# Access Review history report

- Downloadable review history to gain more insight on Access Reviews
- Download results for audit and compliance needs, or to integrate with other solutions
- Reports can be constructed to include specific access reviews, for a specific time frame, and can be filtered to include different review types and review result

Home > Identity Governance

Identity Governance | Review History

« + New report Refresh

Date: Last 1 month

Search by name or owner

Name	Created By	Created Time
No access review reports to display		

Create Review History Report

Select filters for selecting history data

Report Name: \* Last Month's Reviews ✓

Reviews starting and ending in period:

Starting \* 02/16/2021 to Ending \* 03/16/2021

Review Type: \* ⓘ 5 selected

Review Result: \* 5 selected

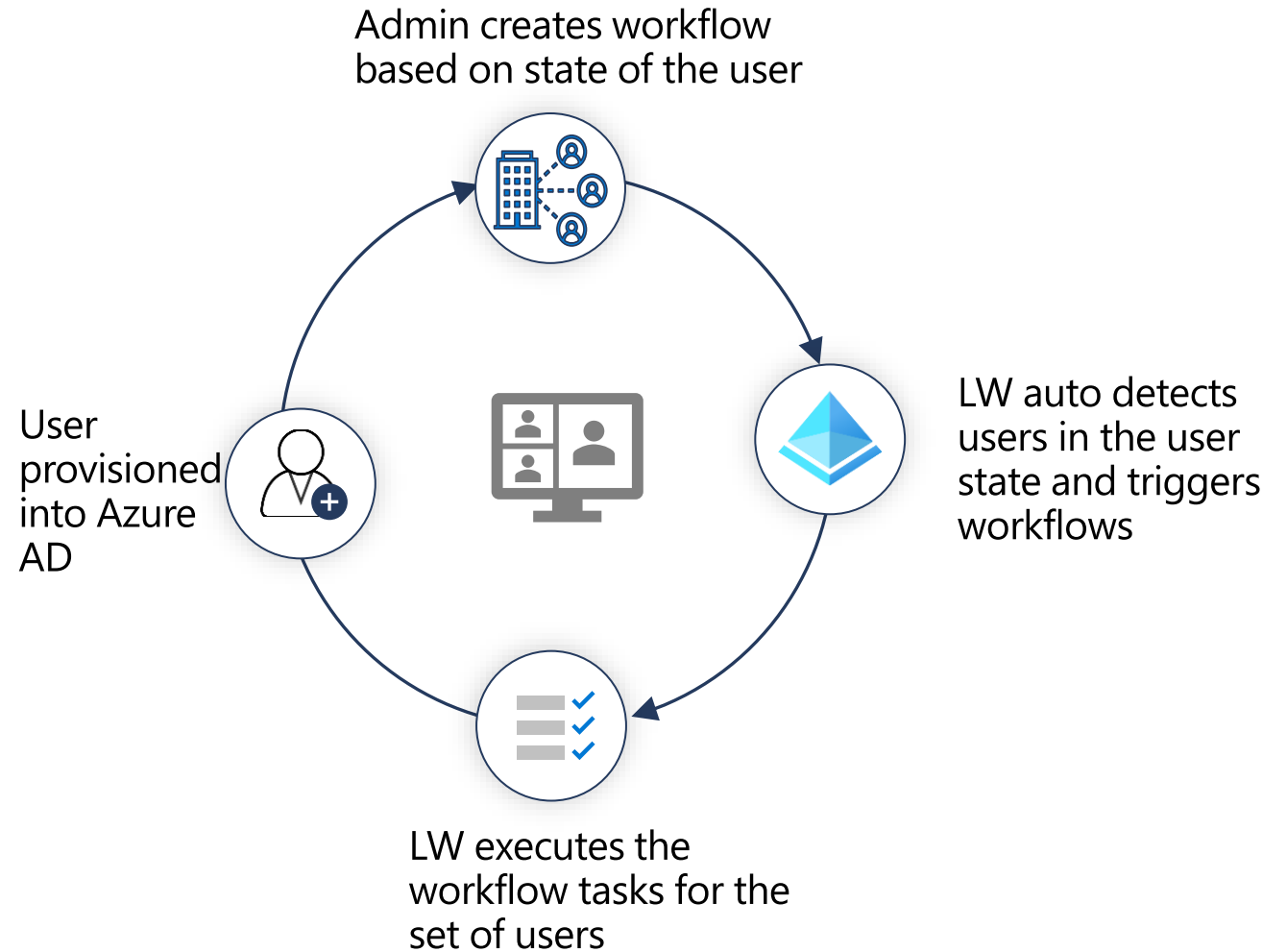
Create

# Lifecycle Workflows

Manage users by automating Joiner/Mover\*/Leaver processes

---

- **Pre-defined workflow templates** for most **common** user **tasks**.
- **Automatic trigger** based on **attribute state changes** of user.
- Custom policies for triggering **workflows based** on pre-defined or custom **user states**.
- **Extensibility** and **flexibility** with Logic Apps



# Microsoft Entra ID Governance Labs

---

- Task 1 – Configure basics for your access package
- Task 2 – Configure the resources for your access package
- Task 3 – Configure requests for your access package
- Task 4 – Configure requestor information for your access package
- Task 5 – Configure the lifecycle for your access package
- Task 6 – Review and create your access package
- Task 7 – Clean up resources

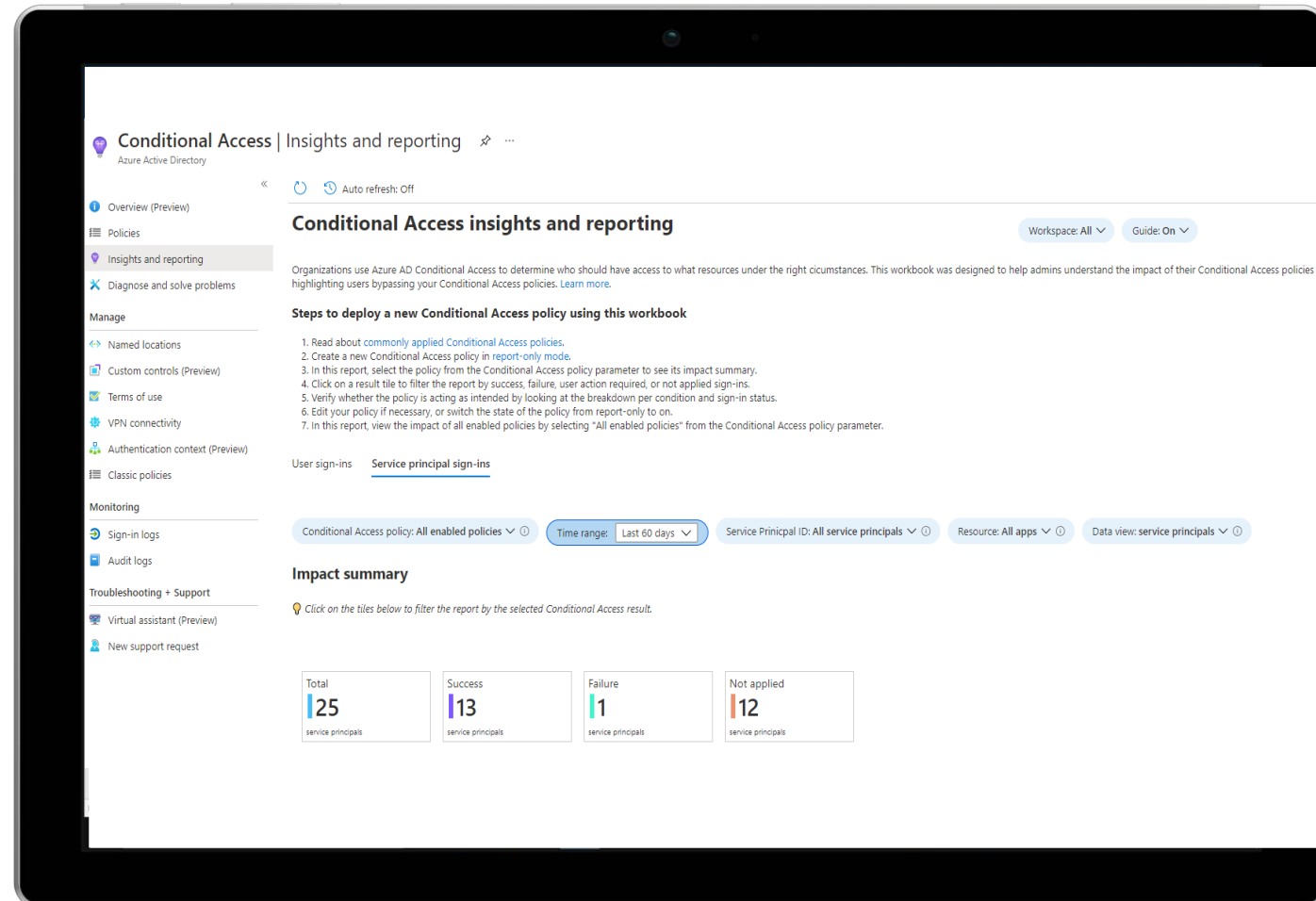
# Microsoft Entra Workload ID



# Conditional Access for workload identities

Protect access to resources by enforcing access control

- **Support for Conditional Access** policies applied to workload identities.
- **Define the conditions** under which a workload may access a resource.
- **Enables blocking** workload identities from outside of trusted IP ranges, such as a corporate network public IP ranges.

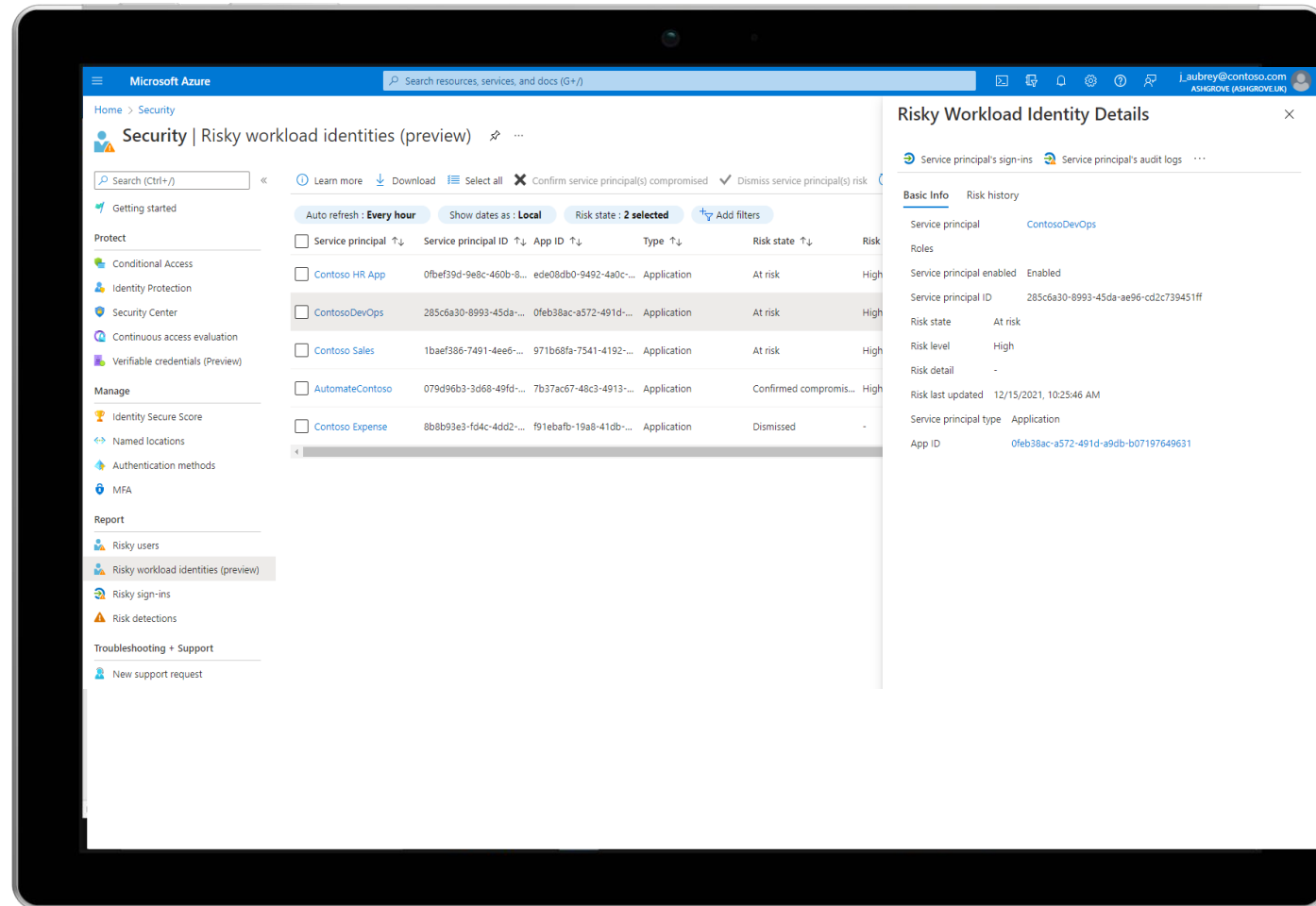




# Identity protection for workload identities

Detect compromised workload identities and block access

- Support identity protection capabilities, such as detecting, investigating and remediating, to workload identities.
- Detect risk on workload identities across sign-in behavior and offline indicators of compromise.
- Enable applying risk-based conditional access to workload identities.

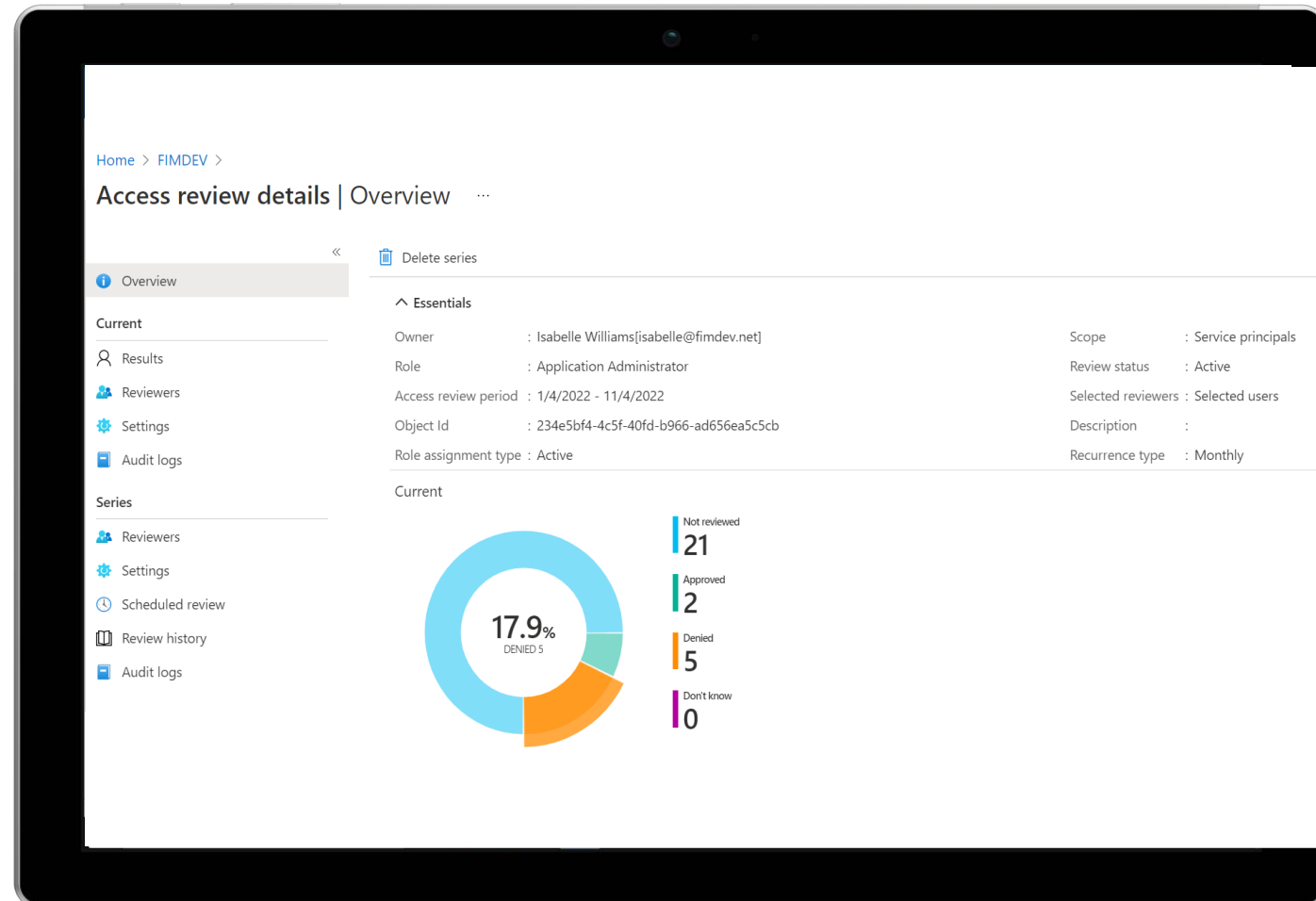




# Access reviews for workload identities

## Workload identities assigned to privileged roles

- Reduce the risk associated with stale role assignment by configuring recurring reviews of workload identities
- Delegate the reviews to the right people, then automatically revoke access of the denied workload identities.



# Microsoft Entra Workload ID Labs

---

Task 1 – Create access reviews