

Azure

User group

Norway

Guest user governance

Automatically review your guest accounts using Azure AD Identity governance

What to learn?

- Azure AD Premium features
- Configure External Collaboration Settings
- Govern your guest users with Entitlement Management





POINT : TAKEN

Julian Rasmussen

Azure & Microsoft 365 consultant

 @JulianRasmussen

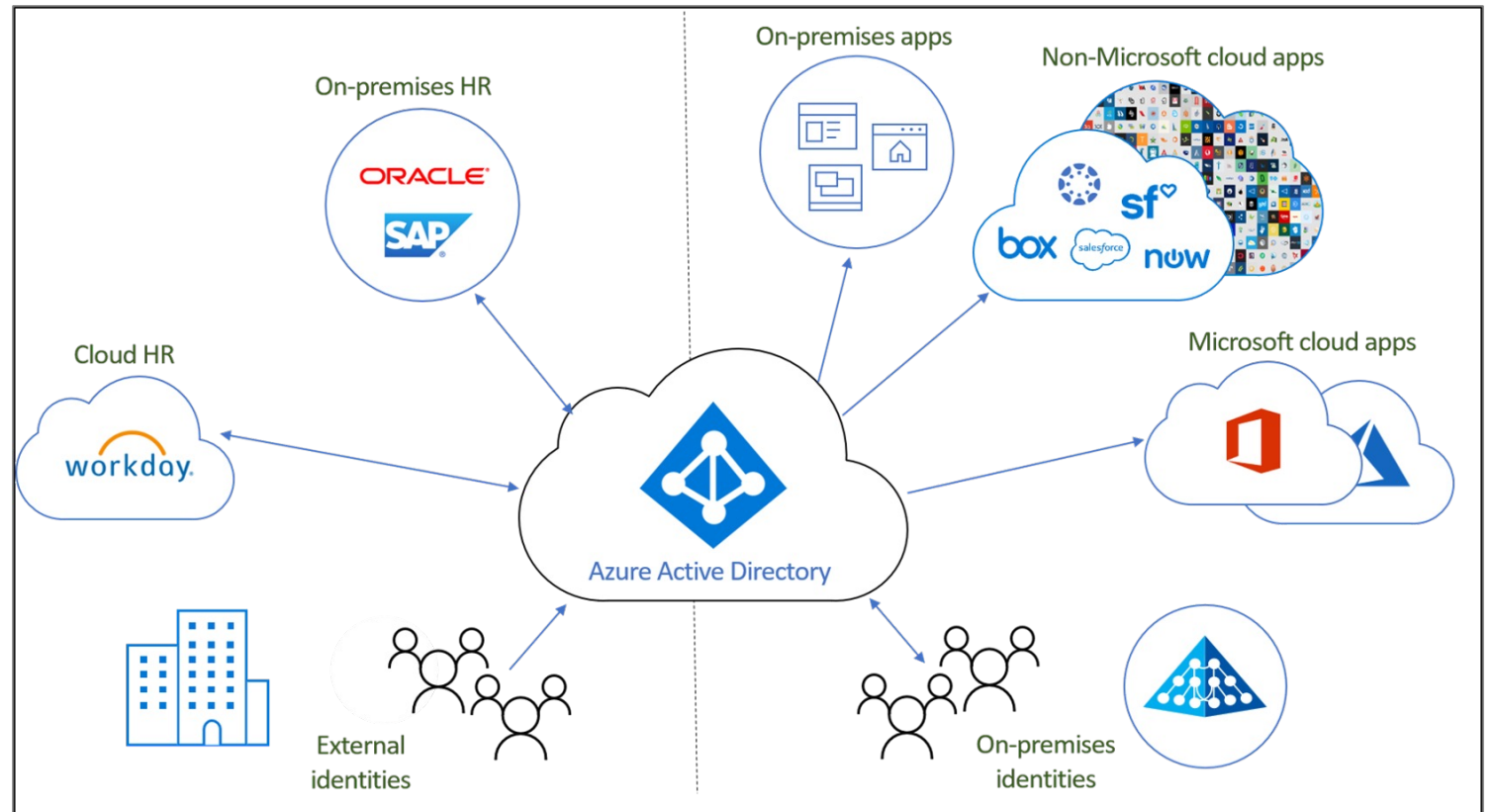
 JulianRasmussen

 www.idefixwiki.no



Challenges

- Why do we have 800 guest accounts?
- Are the guest user in-use anymore?
- How can we review the guest users?
- Who should take decision on guest users?
- Are there effective organizational controls for managing access?
- Can auditors verify that the controls are working?

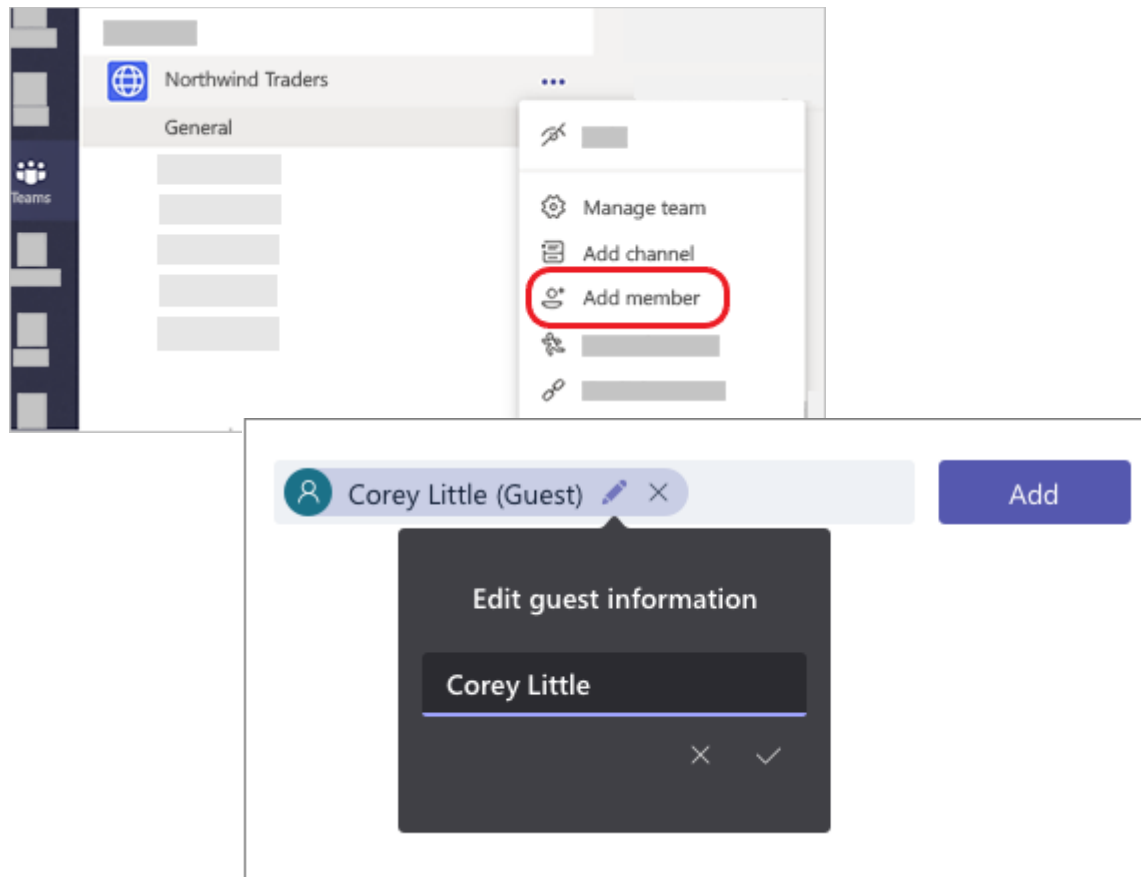


How does Azure AD automate identity lifecycle management?

Azure AD currently provides these features:

- Users can be automatically created and updated in Azure AD and Active Directory using [HR-driven provisioning](#)
- Existing users in Active Directory can be automatically created and maintained in Azure AD using [inter-directory provisioning](#)
- Users can be automatically assigned to groups based on their properties, using [dynamic groups](#) and can, upon request, be assigned to groups, Teams, Azure AD roles, Azure resource roles, and SharePoint Online sites, using [entitlement management](#) and [Privileged Identity Management](#)

Users added as guests by Microsoft Teams



Users added as guests by SharePoint Online

The image shows a SharePoint Online interface. On the left, a file explorer view displays a folder named 'test'. A context menu is open over the folder, with the 'Share' option highlighted. The menu includes options like 'Copy link', 'Manage access', 'Download', 'Add shortcut to OneDrive', 'Delete', 'Automate', 'Rename', 'Pin to top', 'Move to', 'Copy to', 'Alert me', 'More', and 'Details'.

On the right, a 'Send link' dialog box is open for the 'test' folder. It shows a list of people you specify can edit, with 'julian.rasmussen' selected. Below this, there is a section 'Add another' with a search bar. A message indicates 'julian.rasmussen is outside of your organization.' There is a 'Message...' field and a 'Send' button.

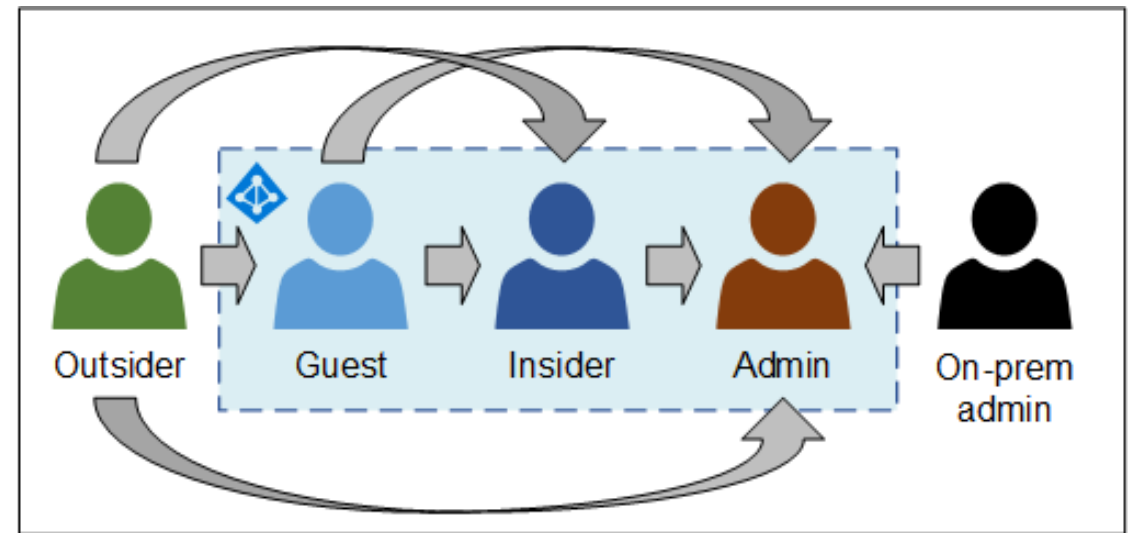
Below the 'Send link' section, there is a 'Copy link' section with a 'Copy' button. At the bottom, it shows 'Shared with:' followed by several user avatars.

Users added as guests by Azure AD

The screenshot displays the Microsoft Azure portal interface for managing users. The top navigation bar shows 'Microsoft Azure' and a search bar. The breadcrumb trail indicates the path: Home > Idefix | Users > Users > New user. The main content area is titled 'New user' and includes a 'Got feedback?' link. A blue banner below the title states: 'Bulk invite and create are now located under the 'Bulk operations' menu item on the 'All users' view. [View all users](#)'. The 'Select template' section offers two options: 'Create user' (Create a new user in your organization) and 'Invite user' (Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating. [Help me decide](#)). The 'Identity' section contains fields for Name (Example: 'Chris Green'), Email address (julian.rasmussen@pointtaken.no), First name, and Last name. The 'Personal message' section has a text area. The 'Groups and roles' section shows '0 groups selected' and 'User' role. The 'Settings' section includes 'Block sign in' (Yes/No) and 'Usage location' (dropdown). A blue 'Invite' button is at the bottom. On the left, a sidebar shows 'Home > Idefix | Users > Users' and a 'Users' section with a search bar and a '+ New user' button. Below this, a list of users is shown, including 'All users (preview)', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage', and 'Deleted users (preview)'. A dropdown menu is open from the '+ New user' button, showing 'Create new user' (Create a new internal user in your organization) and 'Invite external user' (Invite an external user to collaborate with your organization). Below the dropdown, two users are listed: '7L 701 Lava lamp' and '7L 702 Lava lamp'.

Guests – Why restrict it?

- Azure AD guest users have access to properties and memberships of directory objects and can read the members of the groups they are assigned to
- We need to train our personell before they are allowed to invite guests



External collaboration settings

Save Discard

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☒ Guest users have limited access to properties and memberships of directory objects
- ☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- ☐ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- ☐ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ☒ Only users assigned to specific admin roles can invite guest users
- ☐ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

[Learn more](#)

Yes No

Collaboration restrictions

- ☐ Allow invitations to be sent to any domain (most inclusive)
- ☒ Deny invitations to the specified domains
- ☐ Allow invitations only to the specified domains (most restrictive)

Delete


☐ Target domains

☐ vipps.no

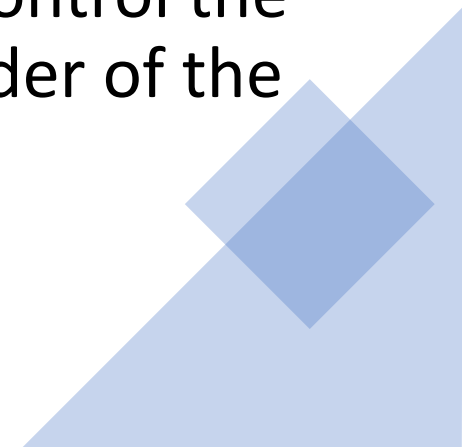
Demo

- External Collaboration settings





Why do we have 800 guest accounts?

- The creation of guest identities is very simple and uncontrolled (no identity manager, no traceability, no restrictions etc.)
 - The number of guest identities may increase in an uncontrolled manner, which makes managing their lifecycles difficult.
 - The company does not control the security of the initial holder of the “guest” identity
- 




Compromised?

Two threat scenarios:

- A **malicious** “guest” identity
- A “guest” identity **compromised** by an attacker.


An attacker would then have the opportunity to:

- **Retrieve confidential data** that the identity has access to
 - **Destroy all data** accessible by this identity
 - **Compromise AD** by assigning roles to this identity
 - **Perform social engineering** through their access to all user data.
- 



Azure AD Identity Governance

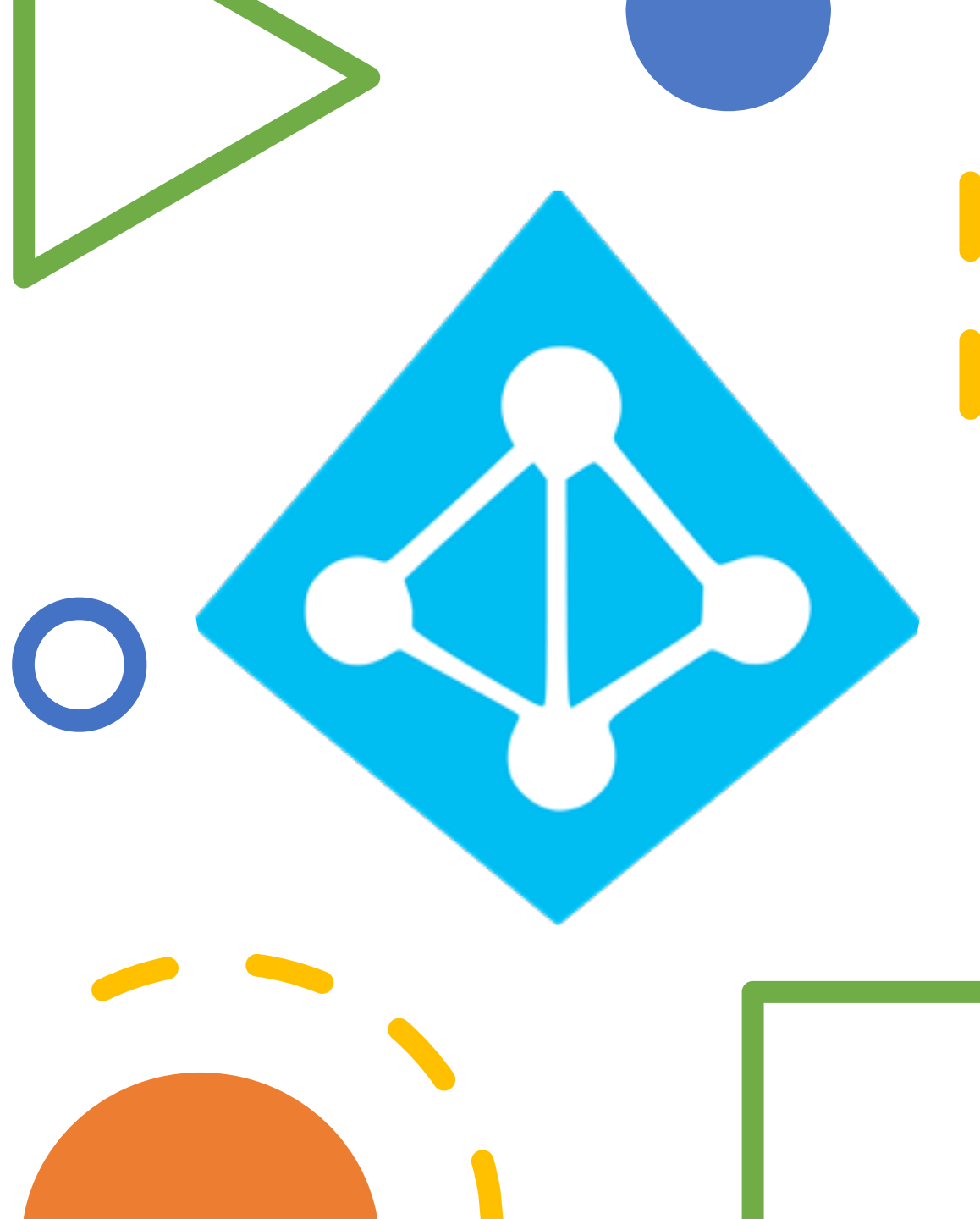
Identity Governance gives organizations the ability to do the following tasks across employees, business partners and vendors, and across services and applications both on-premises and in clouds

- Govern the identity lifecycle
 - Govern access lifecycle
 - Secure privileged access for administration
- 

Azure AD Premium P1

\$6 / 62 NOK

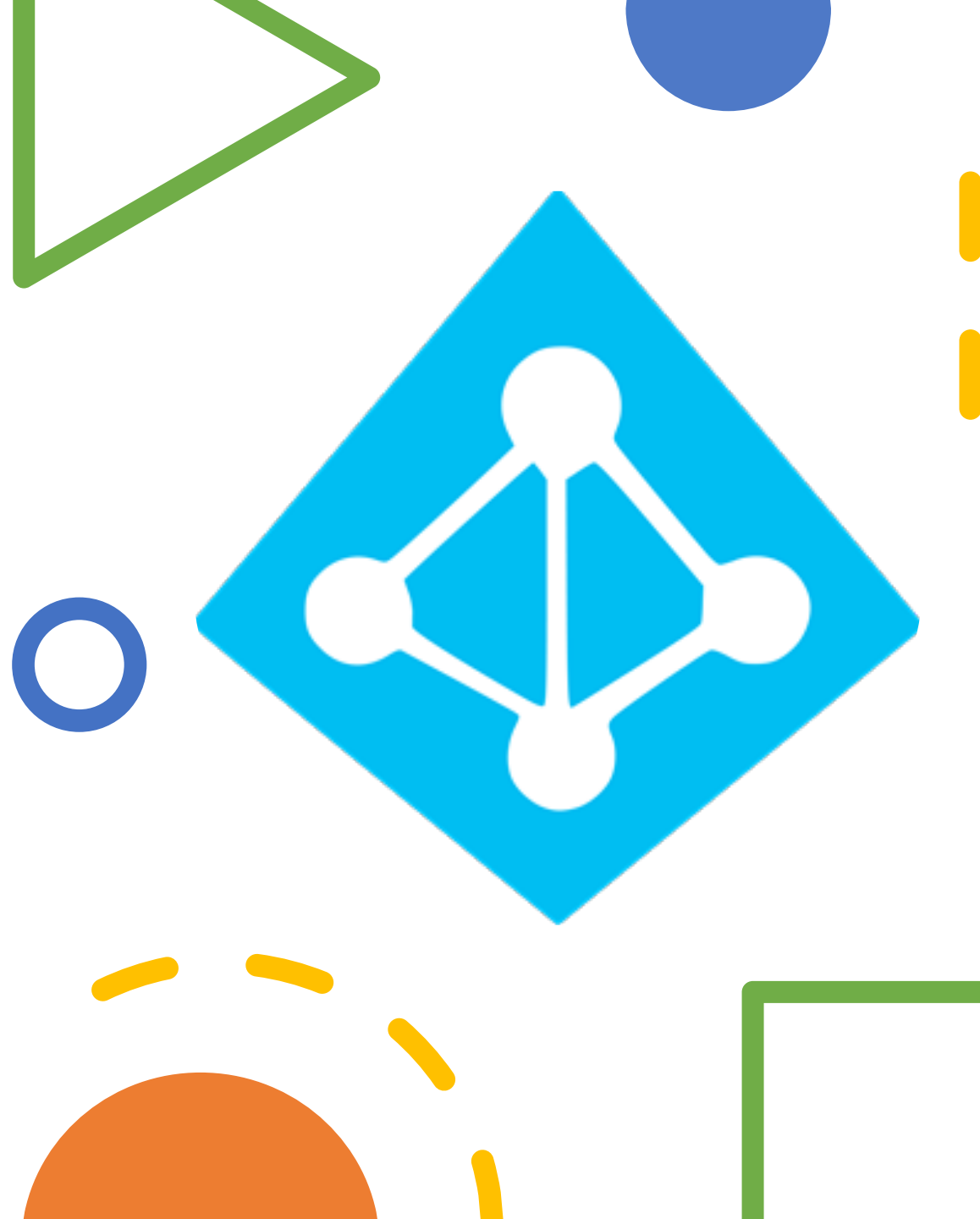
- SLA
- Advanced Group Management
- Advanced security & usage reports
- Password Protection
- Self Service Password reset
- Defender for Cloud apps
- MFA Fraud alert, Usage reports
++
- Conditional access



Azure AD Premium P2

\$9 / 93 NOK

- Risk-based conditional access
- Identity Protection (Risky sign-ins, risky users)
- Access Reviews
- Entitlements Management
- Privileged Identity Management (PIM), just-in-time access



Demo

- Azure AD – Access Review





There are PowerShell options

- Tony Redmond's Powershell / Graph script to find old Guest users

<https://github.com/12Knocksinna/Office365itpros/blob/master/FindOldGuestUsers.ps1>



Wrap-up

- Always remove unused accounts!
- Harden your default Azure AD configuration
- Utilize your license if you have AAD Premium P2
- Use PowerShell / Graph scripts to automate it your own way



HAVE ANY QUESTIONS



DO YOU?