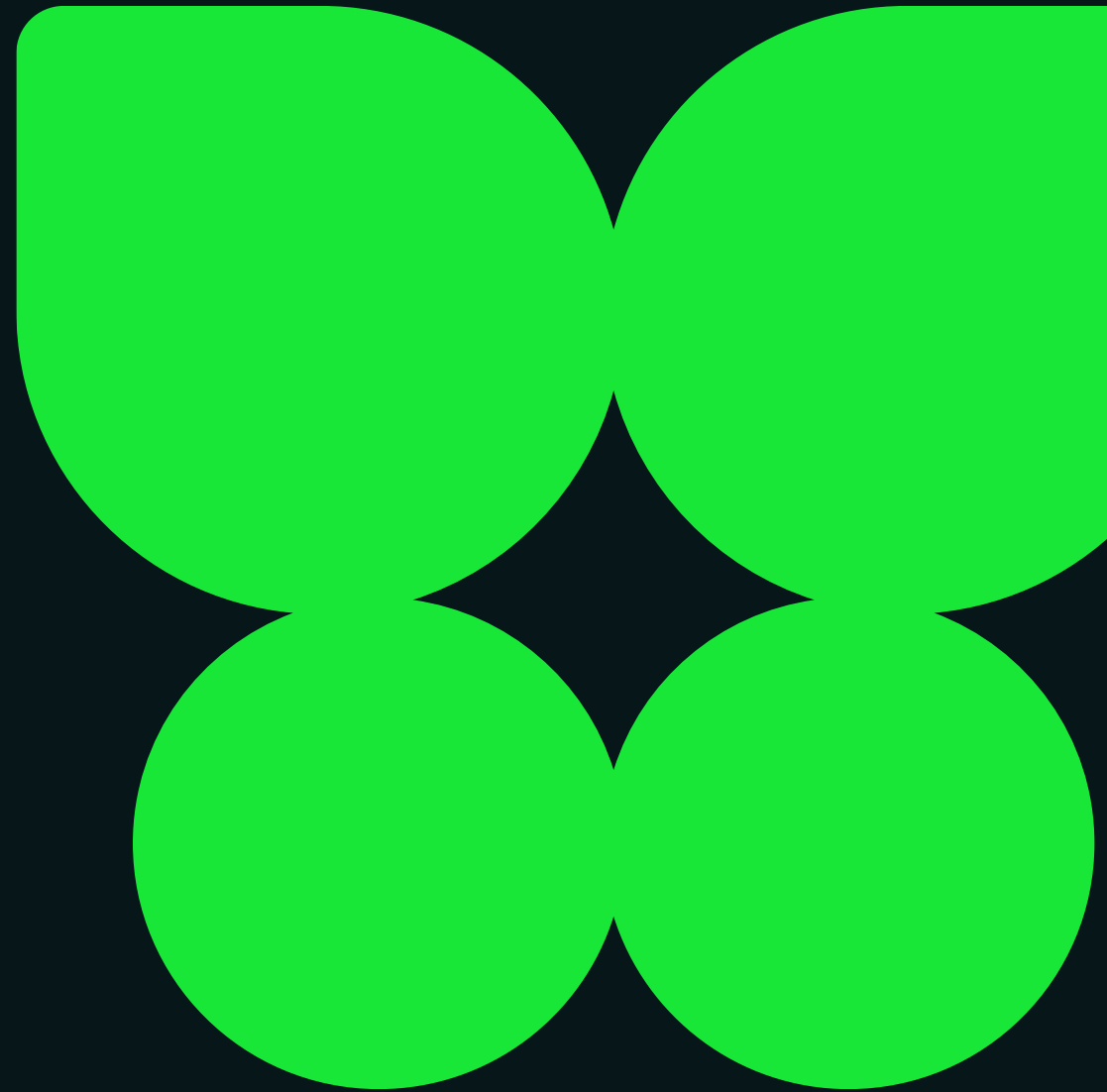


Entra ID Masterclass – Security and Governance Deep Dive

→ Tom Urwin | Senior Architect
Martyn Gill | Senior Architect & Team Lead

March 2024



Contents

- New Entra ID Governance
- Great possibilities with new features
- Modernisation strategy
- Deliver value through Kocho

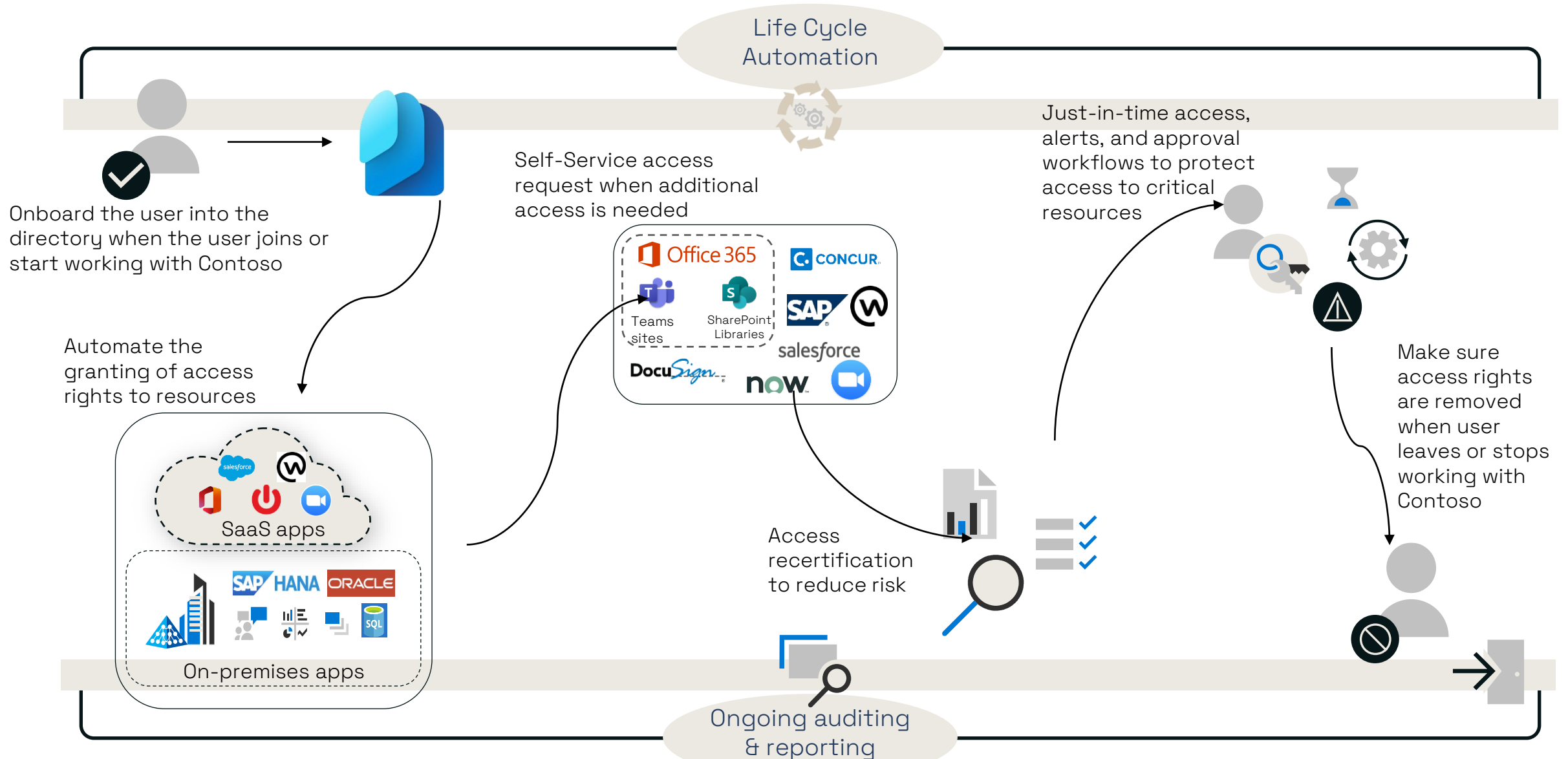
Azure AD
is now
Entra ID



NEW Microsoft Entra ID Governance

Utilise the best-in-class Identity and Access Management capabilities, using Microsoft Entra ID with its new Identity Governance features.

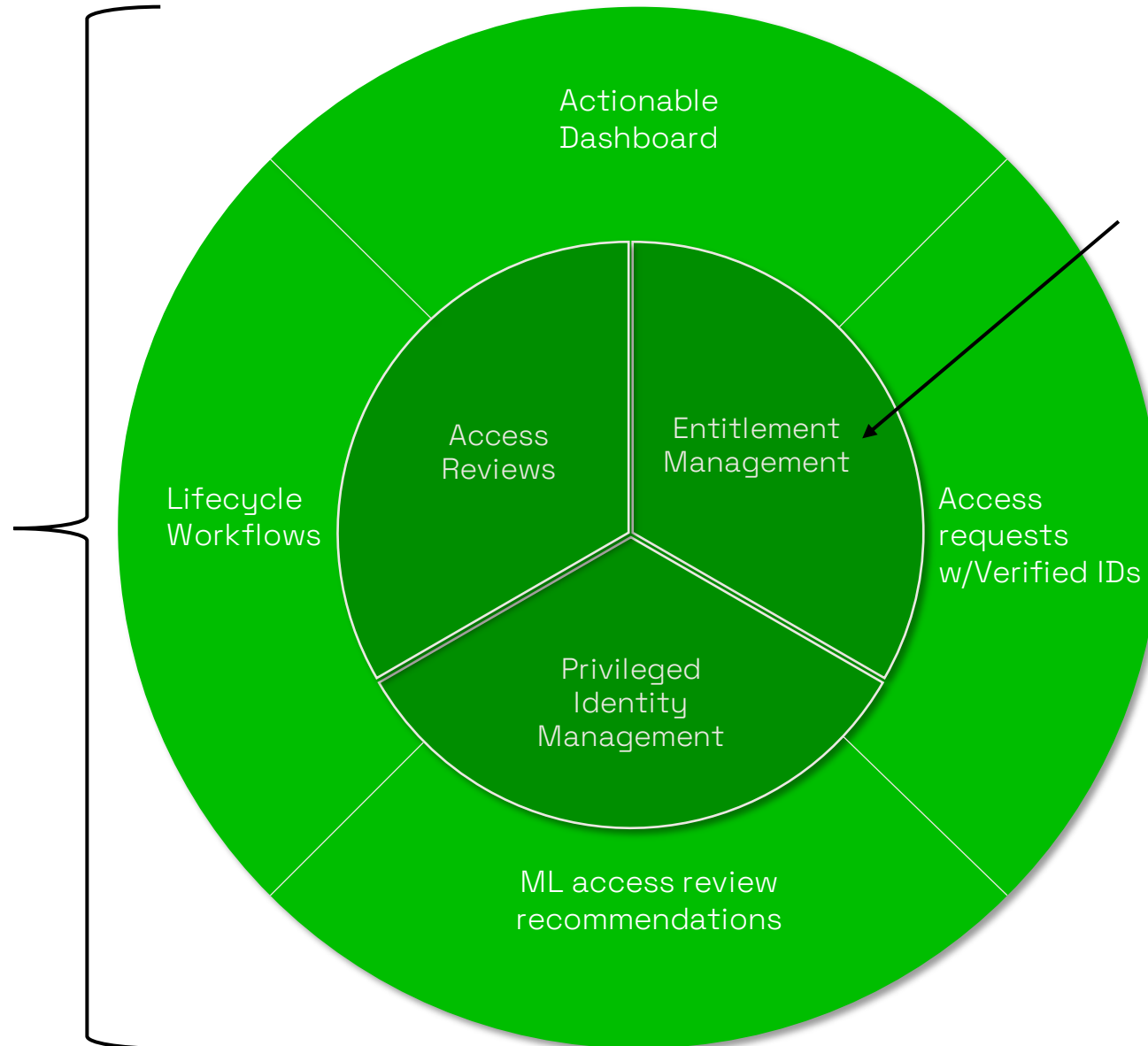
End-to-end user journey



A Premium Identity Governance product

Entra ID P1 /
P2 Add-On

Microsoft Entra
ID Governance
capabilities



Features now in Entra ID Governance

Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance
API-driven provisioning		✓	✓	✓
HR-driven provisioning				
Automated user provisioning to SaaS apps	✓			
Automated group provisioning to SaaS apps				
Automated provisioning to on-premises apps				
Conditional Access - Terms of use attestation				
Entitlement management - Basic entitlement management				
Entitlement management - Conditional Access Scoping				
Entitlement management MyAccess Search				
Entitlement management with Verified ID				
Entitlement management + Custom Extensions (Logic Apps)				
Entitlement management + Auto Assignment Policies				
Entitlement management - Directly Assign Any User(Preview)				
Entitlement management - Guest Conversion API				✓
Entitlement management - Grace		✓		✓

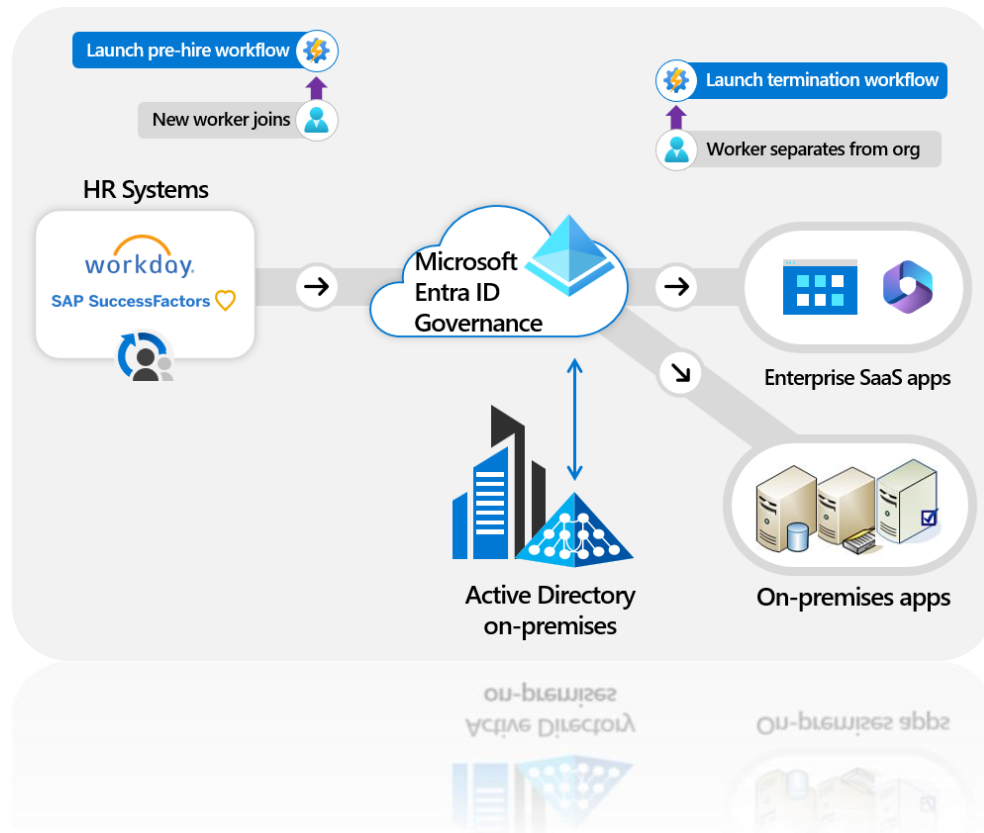
- Lifecycle Workflows
- Access Package Auto Assignment
- Access Package Logic App Integration
- Access Package with Verified ID
- Access Review User-to-Group Affiliation
- Clean-up stale / inactive accounts
- Access Review PIM for Groups
- And more!

Entra ID P2
Promo
Offer

Monthly
Active
Usage for
Guests

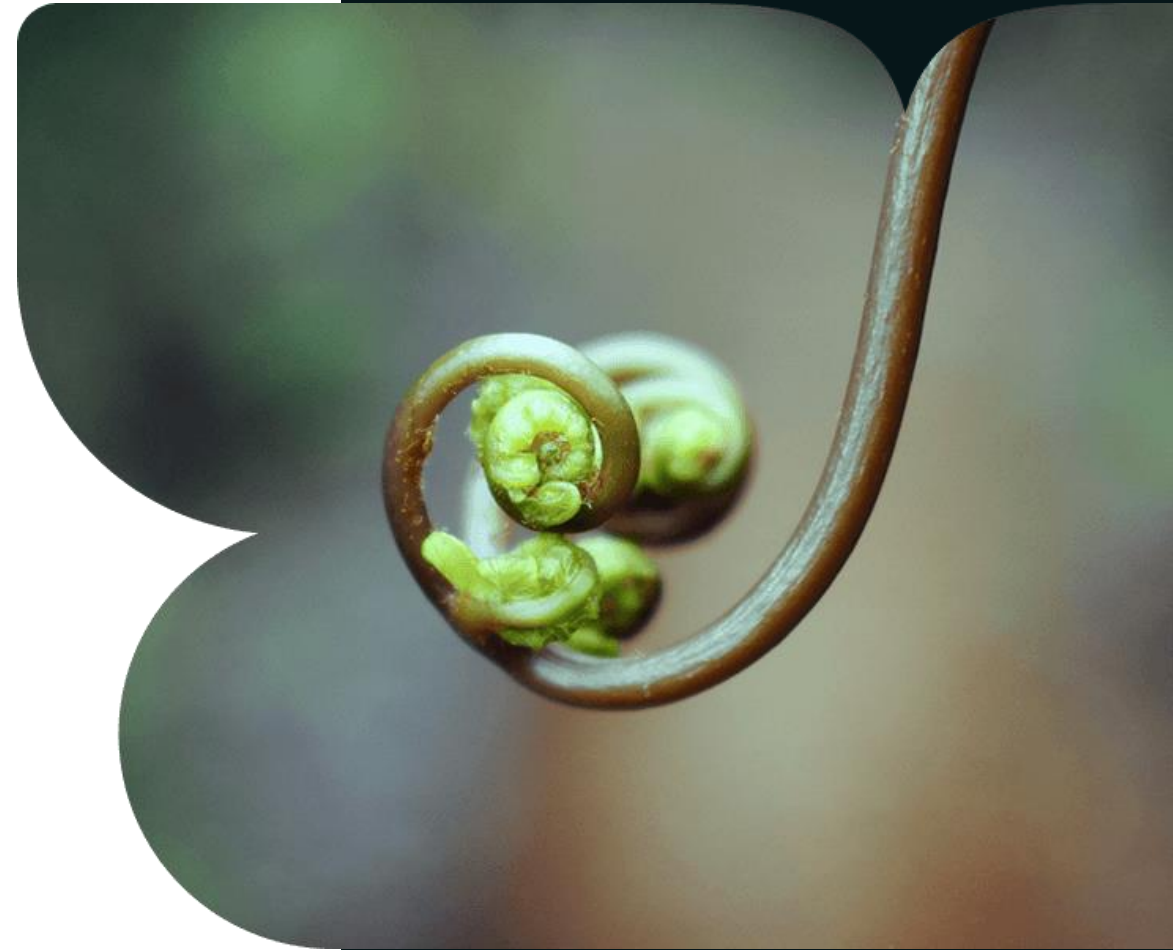
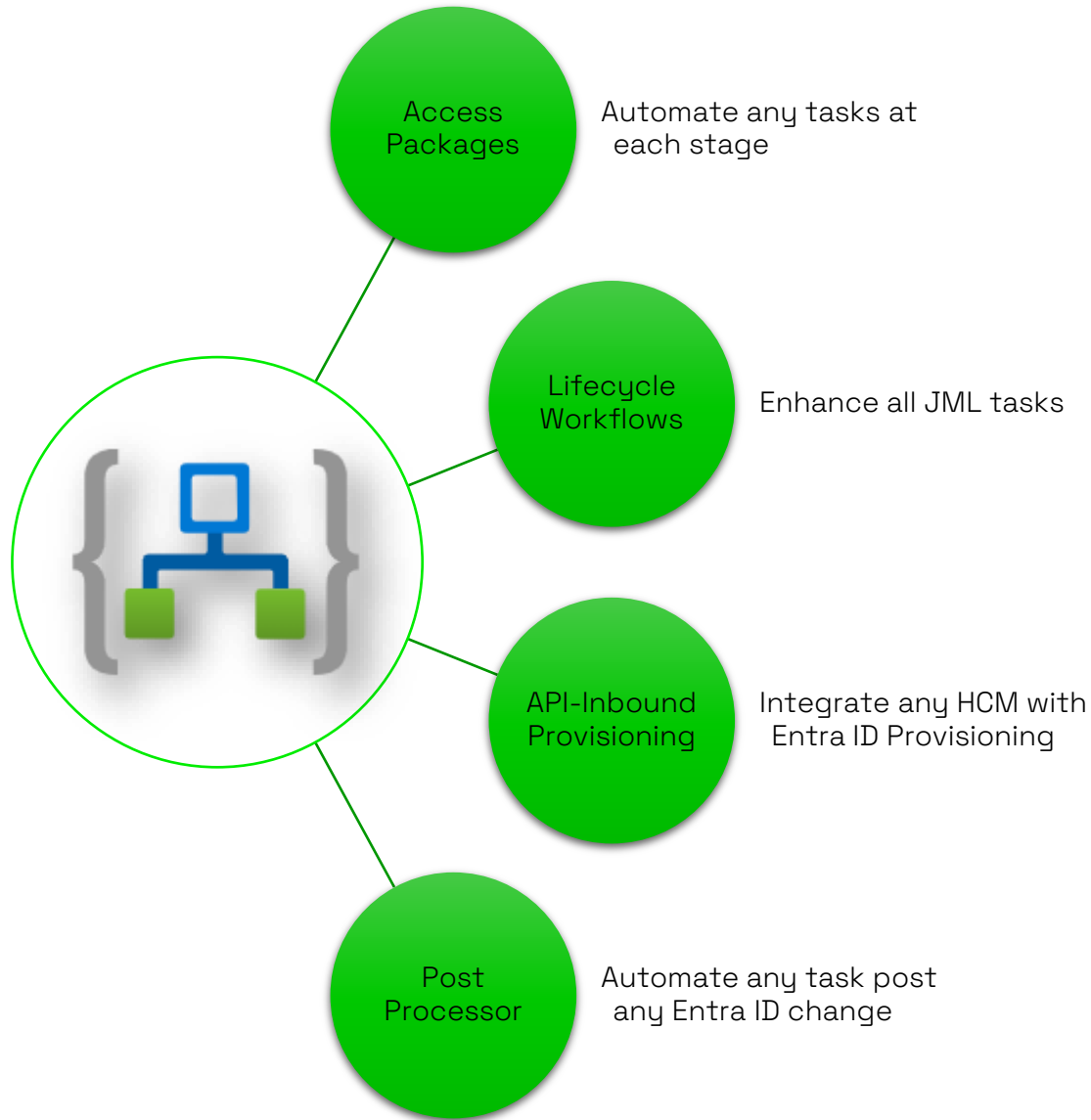
Lifecycle Workflows

Enhance the lifecycle by managing Entra ID accounts with automated processes



- Extending the lifecycle process by automating on/off-boarding tasks
- Centralise processes, create and manage in one place
- Enables scalability for organisation growth
- Reduce and potentially remove manual tasks
- Extensibility with Azure Logic App integration
- Lifecycle beyond attributes, 'X' days before the employeeHireDate
- Tasks, triggers (when) and scope (who) for each workflow

Compliment IAM with Azure Logic Apps



Are you licensed and
using these
capabilities yet?

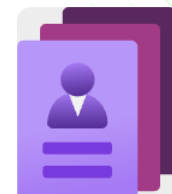
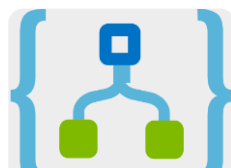


Great possibilities with new features

Using the best-in-class Microsoft services for your cloud-first hybrid Identity Governance & Access Lifecycle capabilities.

Any People Profile Data Source

- API interoperability
- Existing business applications
- Workflows and Automation
- Any system of record for digital identity



IT Service Management integration

→ Continue to use existing business processes and applications

The image shows two screenshots. The left screenshot is a ServiceNow 'New User Table' form with the following fields: Title (Mr), Start Date (2023-06-12), First Name (Martyn), Active (False), Last Name (Gill), UniqueID (09062023), Email (martyn.gill@corpdomain.com), and Type (Permanent). A 'Submit' button is highlighted with a green mouse cursor. The right screenshot shows the Azure AD 'Users' page for 'Kocho Identity Sandbox | Users', with a search filter for 'Employee ID == 09062023'.

ServiceNow

- New User Form

Azure Logic Apps

- HTTP Trigger
- API-Inbound Provisioning request

Entra ID

- User Account created pre-day-1

Self Service Account Activation

→ Enables new starters to self-activate their account on day-1

Kocho

Hi [redacted] Gill,

Today is your first day at Kocho, to get you started we would like you to fill out the below form so we can enable your account and send you the sign-in details.

Here is the link to the form: <https://forms.office.com>

Here is your One-Time-Passcode (OTP): 2541-[redacted]

Please contact Service Desk on 01223 456789 or [redacted]

Thank you, and have a lovely day.

Kocho

Hi [redacted] Gill,

Your account has been enabled and ready for you to use, please use the below to sign-in and set the password you'd like to use going forward.

Username: [redacted]

Password: [redacted]

URL: <https://portal.office365.com>

Please contact Service Desk on 01223 456789 or support@kocho.co.uk for any support queries.

Thank you, and have a lovely day.

Lifecycle Workflows

- Initiates process on day 1

Azure Logic Apps

- E-Mail One-Time-Passcode

Microsoft Forms

- Self-service activation

Azure Logic Apps

- Validation
- Account readiness
- E-Mail credentials

Lifecycle for LDAP

→ Near real-time lifecycle for on-premises LDAP

My Access

Access packages

Access packages

← Additional questions

Why do you require access to OpenLDAP? *

To support the integrated LDAP applications

What department do you work in?

IT Operations

Business justification

The perform day-to-day applications

```
dc=ldap,dc=kochoidentity,dc=onmicrosoft,dc=com
├── cn=admin,dc=ldap,dc=kochoidentity,dc=onmicrosoft,
│   ├── ou=groups,dc=ldap,dc=kochoidentity,dc=onmicrosoft
│   └── ou=people,dc=ldap,dc=kochoidentity,dc=onmicrosoft
│       └── uid=TomUrwin,ou=people,dc=ldap,dc=kochoidentity,dc=onmicrosoft
│           └── No children
```

Dn:
ou=people,dc=ldap,dc=kochoidentity,dc=onmicrosoft,dc=com
objectClass: organizationalUnit;
ou: people;

Expanding base
'uid=TomUrwin,ou=people,dc=ldap,dc=kochoidentity,dc=onmicrosoft,dc=com'...

Getting 1 entries:

Dn:
uid=TomUrwin,ou=people,dc=ldap,dc=kochoidentity,dc=onmicrosoft,dc=com

```
admin@AZ-UKS-LDAI x Windows PowerShell x Windows PowerShell x
dn: uid=TomUrwin,ou=people,dc=ldap,dc=kochoidentity,dc=onmicrosoft
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
```

Access Package

- Request Access
- Initiate Logic App

Azure Logic Apps

- Provision on-demand using the MS Graph API

On-Prem App Provisioning

- LDAP Connector
- Create, Update or Delete



Self Service Access for on-premises

→ Providing on-premises access lifecycle with Group writeback

The screenshot displays the Microsoft Access Packages console interface. At the top, a table lists access packages:

Name	Membership type	Source	Writeback enabled
OS On-premises SAP	Assigned	Cloud	Yes

Below the table, an 'Additional questions' dialog box is open, asking for justification for SAP access. The text input fields contain: 'To raise and approve invoices.' and 'Only access to the finance modules.'.

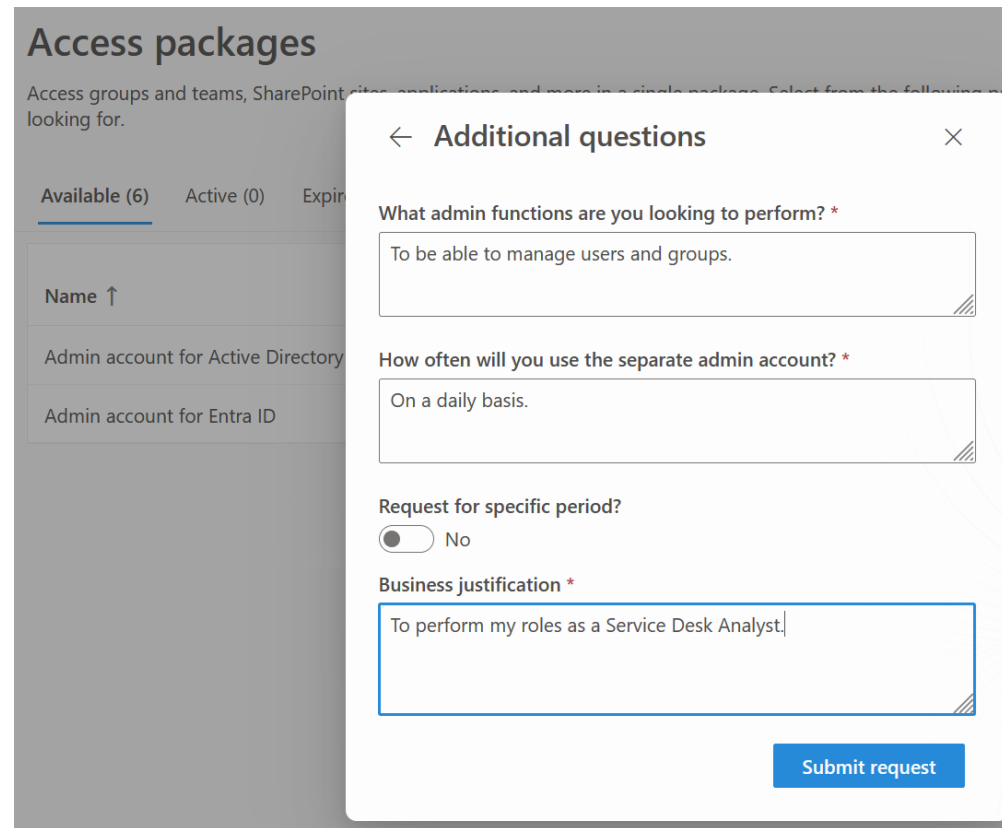
In the background, the 'Active Directory Users and Computers' window is open, showing the 'On-premises SAP_02bc385e9b50 Properties' dialog box. The 'Members' tab is selected, and the 'Writeback' checkbox is checked, indicating that group membership changes will be synchronized back to the cloud.

Three green callout boxes provide details about the configuration:

- Access Package**
 - Request Access
 - Approval Process
- Entra ID Group**
 - User is added to Group membership
 - Writeback enabled
- Cloud Sync**
 - Near real-time write-back of Group and membership updates

Lifecycle for multiple scenarios

- Separate Admin account lifecycle
- Any directory
- Non-synced accounts
- Access lifecycle
- Password lifecycle
- Self Service
- Test accounts



The screenshot shows the 'Access packages' interface with a modal dialog titled 'Additional questions'. The background interface includes a header 'Access packages', a sub-header 'Access groups and teams, SharePoint sites, applications, and more in a single package. Select from the following packages looking for.', and a table with columns 'Available (6)', 'Active (0)', and 'Expired'. The table lists 'Admin account for Active Directory' and 'Admin account for Entra ID'. The modal dialog contains the following fields:

- Question: 'What admin functions are you looking to perform? *' with the answer 'To be able to manage users and groups.'
- Question: 'How often will you use the separate admin account? *' with the answer 'On a daily basis.'
- Question: 'Request for specific period?' with a radio button selected for 'No'.
- Question: 'Business justification *' with the answer 'To perform my roles as a Service Desk Analyst.'

A 'Submit request' button is located at the bottom right of the modal dialog.

Great Capabilities

- Cloud-first hybrid automation
 - Azure Logic Apps
 - Hundreds of out-of-the-box connectors
 - Azure Automation Hybrid Worker for on-premises
- Verified ID
 - Proving who you are
 - Support helpdesk and onboarding
 - New Face Check for high-assurance verification



Cutting Edge

- Enrich with Power Platform
 - Low-code / no-code user interfaces
 - Power Pages - Advanced self-service portal
 - Dataverse - Metaverse of IAM data
 - Same Connectors as Azure Logic Apps
 - PowerApps
 - Embed in Teams and SharePoint Lists



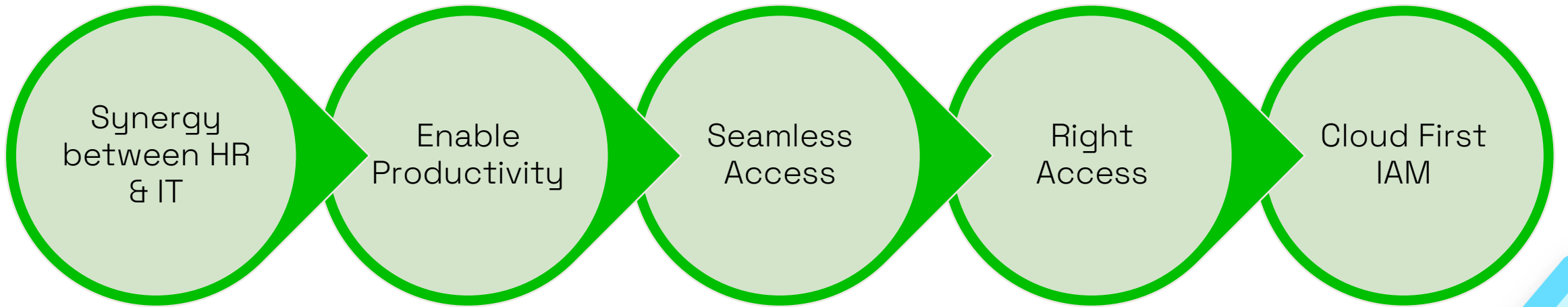
What capabilities are you looking for, to solve which business problems?



Modernisation strategy to Microsoft Entra ID

Begin the journey to move away from legacy on-premises IAM.

Start your IAM journey to the cloud today



→ Integrate HCM

→ Birth-rights Access

→ Single Sign-On Apps

→ Recertification

→ Entra ID &

→ Automate JML

→ RBAC Entitlements

→ Cloud & On-Prem

→ Separation of Duty

→ Entra ID Governance

→ Automate Tasks

→ Self-Service

→ Open Standards

→ Privileged Lifecycle



Cloud-first transformation to Entra ID

Full Discovery

- As-Is IAM features and capabilities
- Analysis of IAM usage
- Re-think IAM capabilities
- To-Be IAM requirements and solution

Cloud Transformation

- Quick-Win Parity Migrations
- Enable out-of-the-box Features
- Compliment with no-code
- Agile bitesize transitions

Legacy removal

- Less DIY by developers
- Leave technical debt behind
- Decommissioning on-premises IAM



Entra ID Future

- Evergreen SaaS
- Agile Feature releases
- Long-term support
- 99.9% SLA, mostly 99.999% performant
- Latest, modern, open standards
- Gartner Magic Quadrant Leaders



Design

Implementation

Support

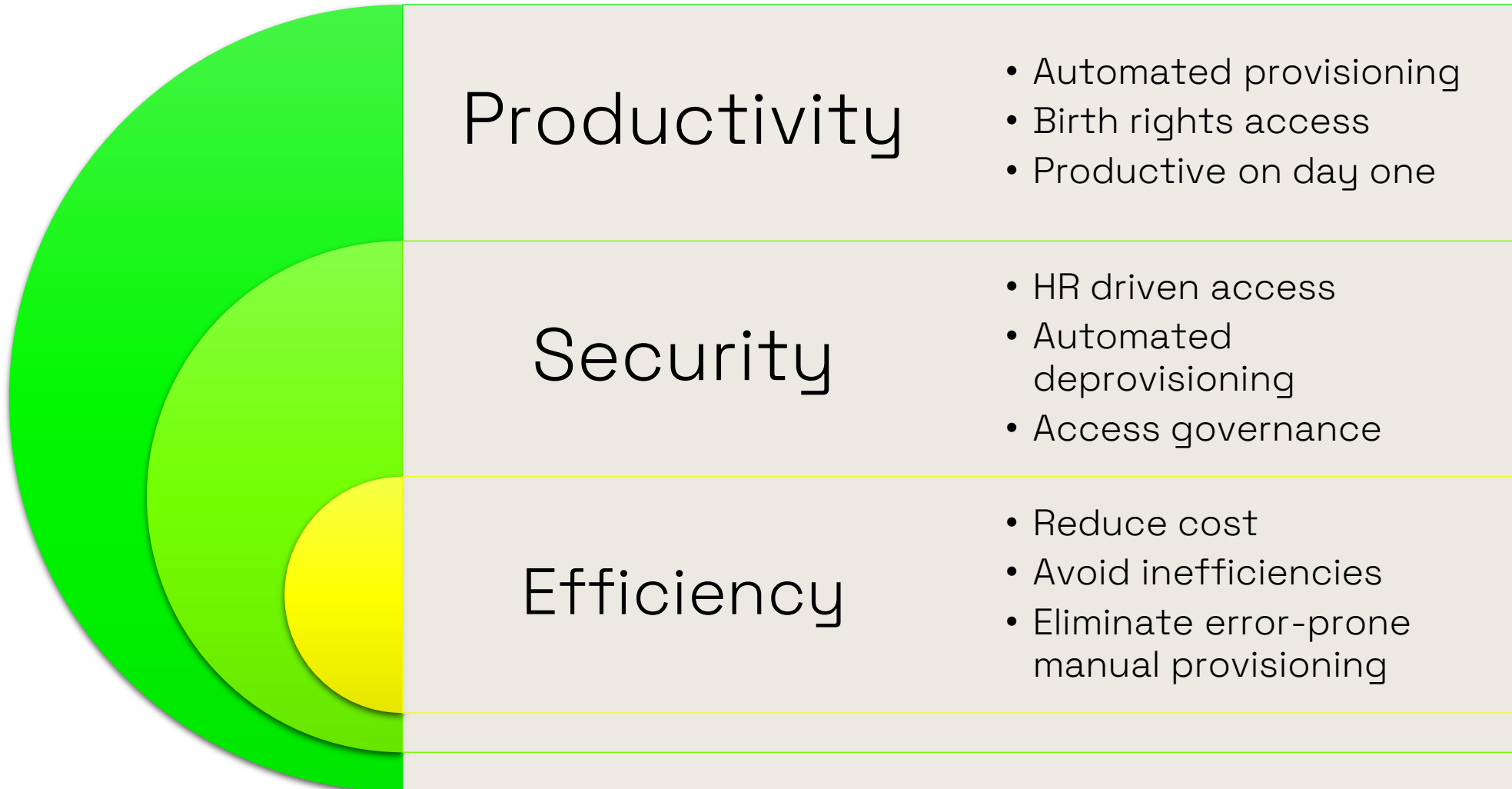
Kocho



Deliver value through Kocho with Microsoft Entra ID

Let us support you on your journey to greatness, by taking advantage of the benefits, and providing value to your business together.

Benefits realised



Summary



Top 3 Identity Partner
Worldwide

- Begin cloud first with Microsoft Entra ID
 - Start with Entra ID Provisioning New capabilities
 - Compliment with Azure Logic Apps
 - Try the New Microsoft Entra ID Governance
- Deliver capabilities that provide value
 - Quick wins
 - Agile delivery
- Let us support you in your journey
 - Begin Full Discovery and Roadmap to Success
 - 20+ years as a leader in identity management
 - Award winning Microsoft Partner in identity, security and compliance.



Entra ID Discovery and Roadmapping Workshop

Plan your roadmap to full cloud identity. And connect employees, customers, and partners seamlessly to apps, devices, and data.



Identify preferred implementation options

→ 5-day engagement

2 days on site

3 days report write-up and delivery



Explore potential cost savings and productivity gains



Uncover hidden challenges and best practice considerations

Want to find out more? [Get in touch](#)



Highlight proposed project timescales and indicate costs



hello@kocho.co.uk



0800 044 5009



Any questions?

Links and resources

→ <https://kocho.co.uk/blog/streamline-hr-driven-provisioning-microsoft-latest-api/>

→ <https://kocho.co.uk/blog/perfect-jml-process-azure-ad/>

→ <https://kocho.co.uk/blog/what-is-microsoft-entra-identity-governance/>



Thank you

Martyn Gill

Senior Architect & Team Lead

martyn.gill@kocho.co.uk

Tom Urwin

Senior Architect

tom.urwin@kocho.co.uk



More links

- Kocho News: [Microsoft rename Azure AD and introduce Security Service Edge](#)
- Microsoft Blog: [Azure AD is becoming Microsoft Entra ID](#)
- Microsoft Blog: [Entra ID Governance Dashboard](#)
- Microsoft Blog: [Entra ID Governance New Entitlement Management features](#)
- Microsoft Blog: [Entra ID Governance New Access Review features](#)
- Microsoft Doc's: [Entra ID Governance](#)
- Microsoft Licensing: [Entra Plans and Pricing](#)
- Microsoft Doc's: [API-Driven Inbound Provisioning Concepts](#)
- Microsoft Licensing: [Entra Plans and Pricing](#)



The Kocho Way.



Our values underpin how we do things at Kocho. They're a mindset, a way of working and when combined, make us a better workforce for good.



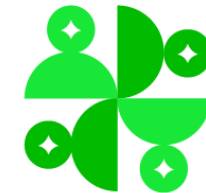
Do what's right.

- We believe that greatness thrives on doing the right thing. That's why we embrace each other's differences, celebrate honesty and respect every opinion.
- We stand up for what's important, always taking care of each other and the planet. And we know that life happens outside of work, so we encourage everyone to find a good balance.



Think greater.

- We're always striving to expand our minds and grow our expertise. No matter how high the bar, we can raise it. And we're not afraid to fail, every mistake is a lesson.
- Every day we challenge ourselves to find a better way of doing things. We're relentless in our quest to create great solutions and even greater careers.



Better together.

- We believe that solid teamwork leads to the best results. Collaboration isn't just a buzzword for us, it's our ethos.
- We're relationship people. We love to work in partnership at every step, sharing every challenge and learning, as well as celebrating every win. It's a one team thing.