Compliance mit IT

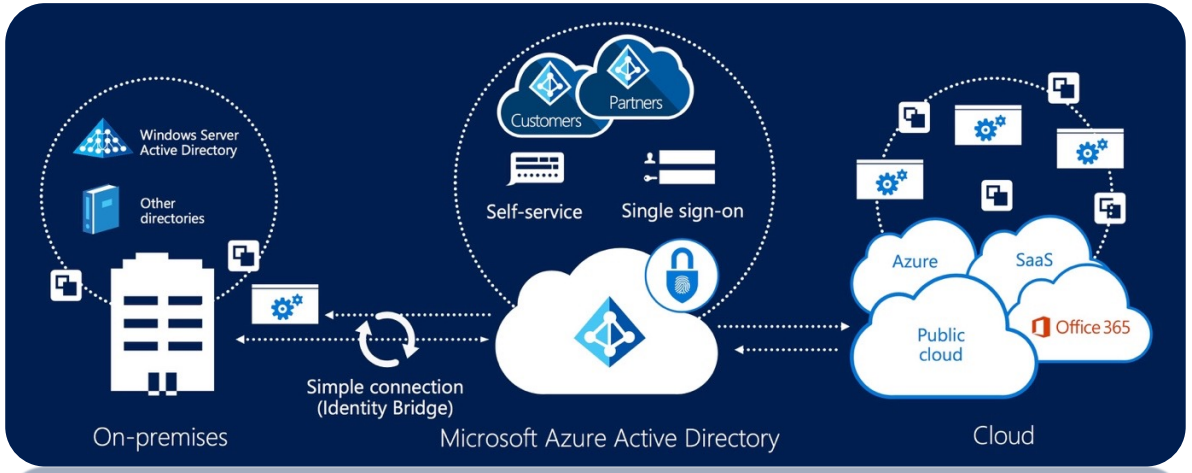
Identity Governance & Administration (IGA) im Kontext Compliance

Jens Lorenz
Strategic Consultant, CISSP, CCSP, CIPT
Swiss IT Security Deutschland GmbH

Azure AD - Identity as a Service

Zentraler Cloud-basierter Identitäts-Provider

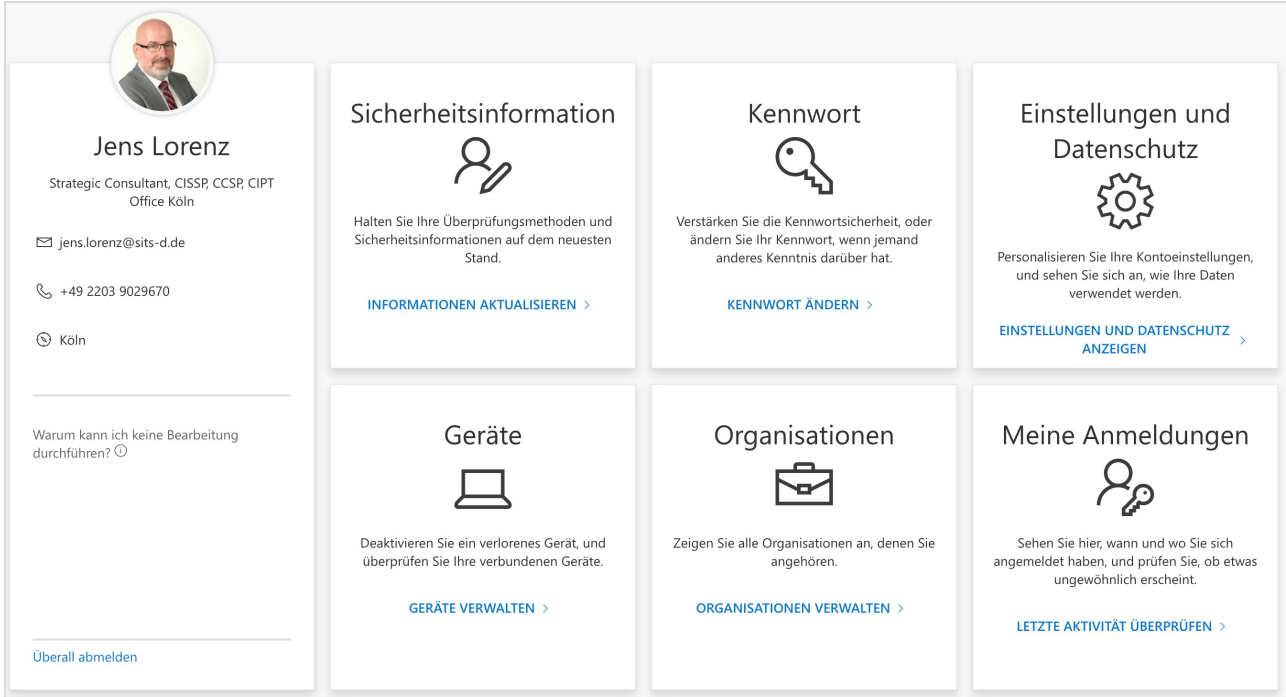
- Bereitstellen von hybriden Identitäten
  - Integration von dezentralen Identitätsquellen
- Zentrale Authentifizierung und Autorisierung
  - Single Sign-On für angebundene Applikationen



Azure AD - Identity as a Service

Zentraler Cloud-basierter Identitäts-Provider

- Self-Service Funktionalitäten
  - Kennwort ändern / zurücksetzen
  - Delegation von Gruppenverwaltung
  - Geräte und Anmeldungen
  - Sicherheitsinformationen
  - Datenschutzinformationen und Einstellungen



Bring Your Own Identity

Azure AD Externe Identitäten

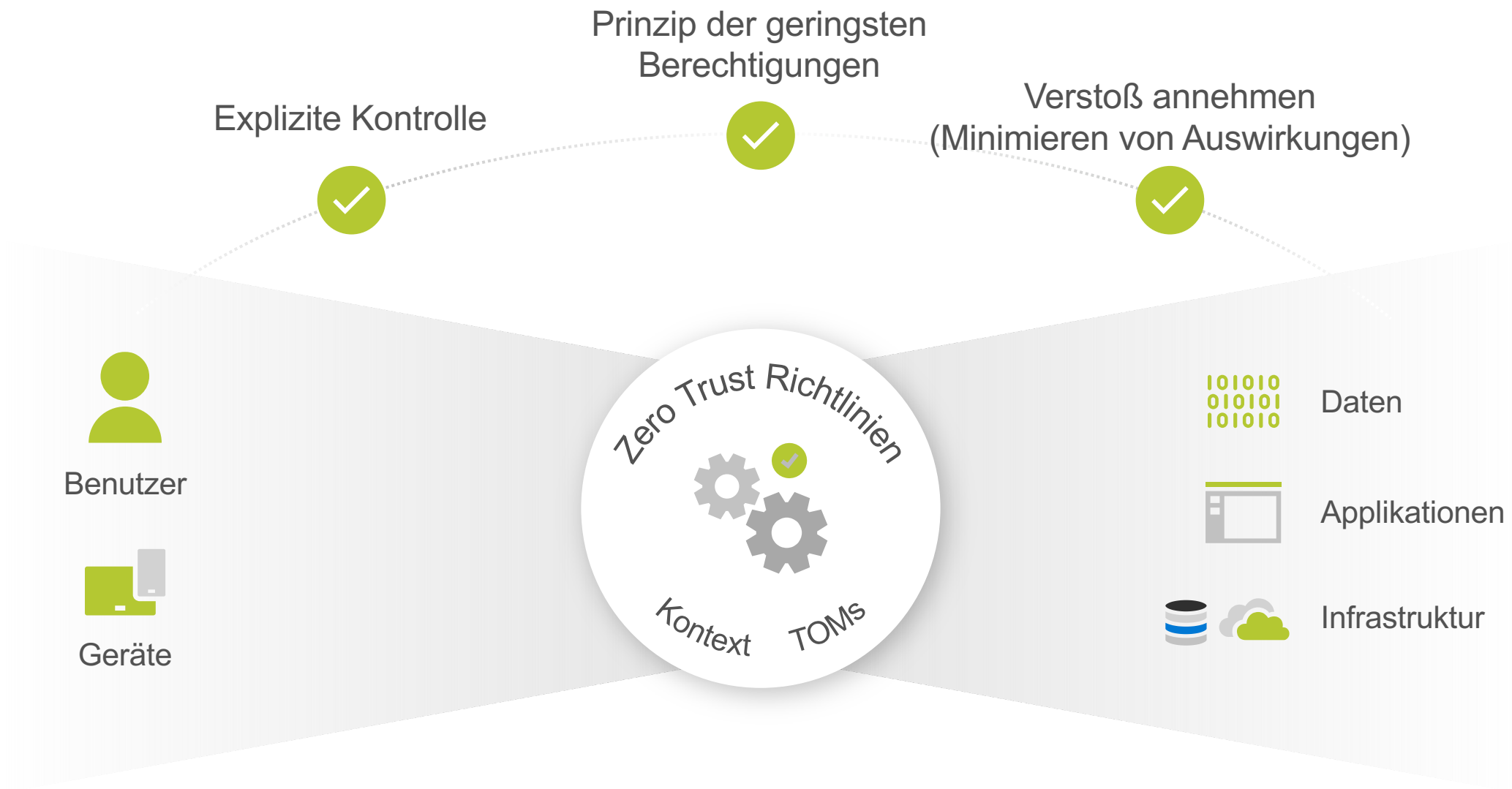
- Authentifizierung von externen Konten in der eigenen Organisation, Autorisierung der Zugriffe in der Ziel-Organisation
  - Azure Active Directory
  - Microsoft Konto
  - Einmalpasscode (OTP)
  - SAML/WS-Fed IdP
  - Social Identities
    - Google (gmail)
    - Facebook

User type	Source
Guest	Microsoft Account
Guest	External Azure Active Directory
Guest	External Azure Active Directory
Guest	OTP
Guest	OTP

Das „Zero-Trust“ Modell


Cloud-Dienste
Home Office
IoT Device
SaaS-Apps
Firmengeräte
Partner
Kunden
Dienstleister
On-Premises
Mobile
Mitarbeiter
Persönliche Geräte

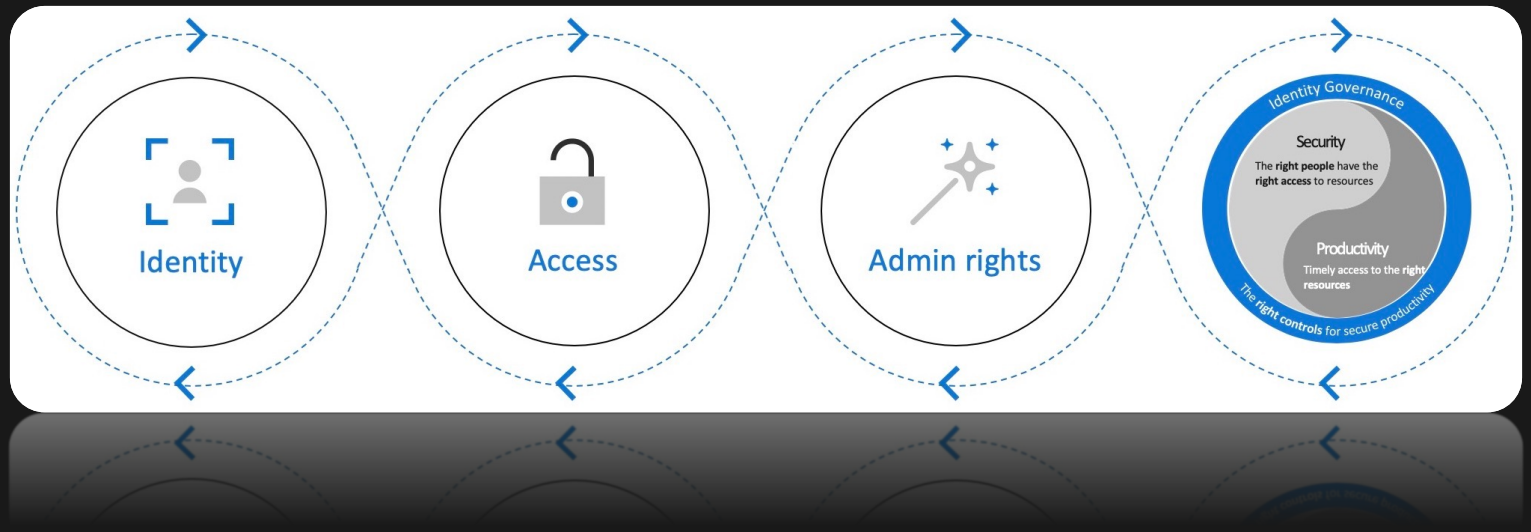
Zero-Trust Prinzipien



https://aka.ms/Zero-Trust-Vision

Azure AD Bedingter Zugriff

Azure AD Identity Governance

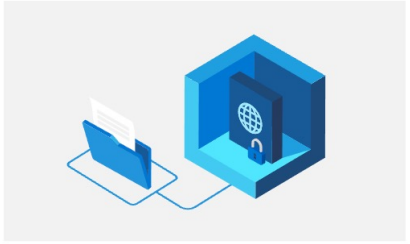


Azure AD Identity Governance

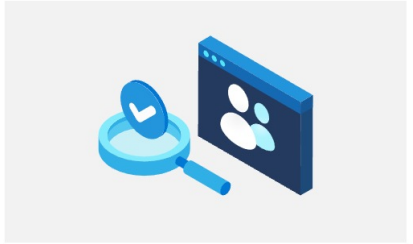
Rollen- und Rechtemanagement, Delegation, Prüfung und Re-Zertifizierung

- Lebenszyklus einer Identität
- Zugriffslebenszyklus
- Privilegierter Zugriffslebenszyklus

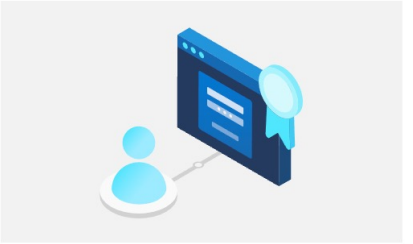
Für Interne und externe Identitäten



Entitlement management



Access reviews

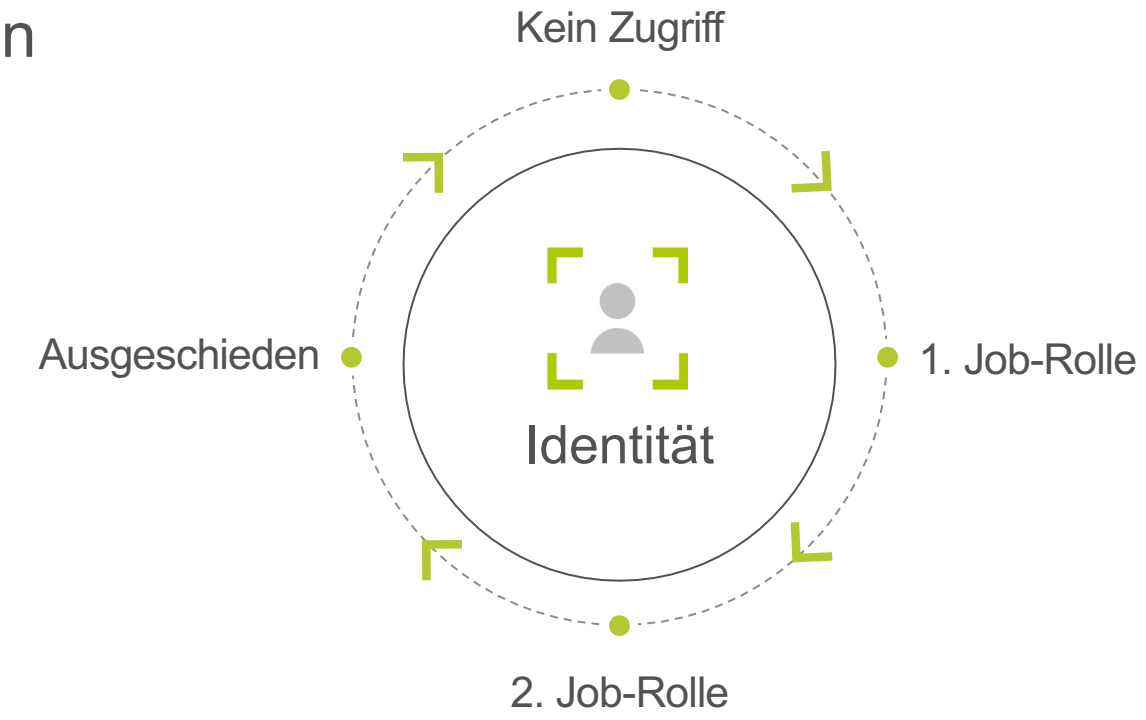


Privileged Identity Management

Azure AD Identity Governance

Lebenszyklus einer Identität

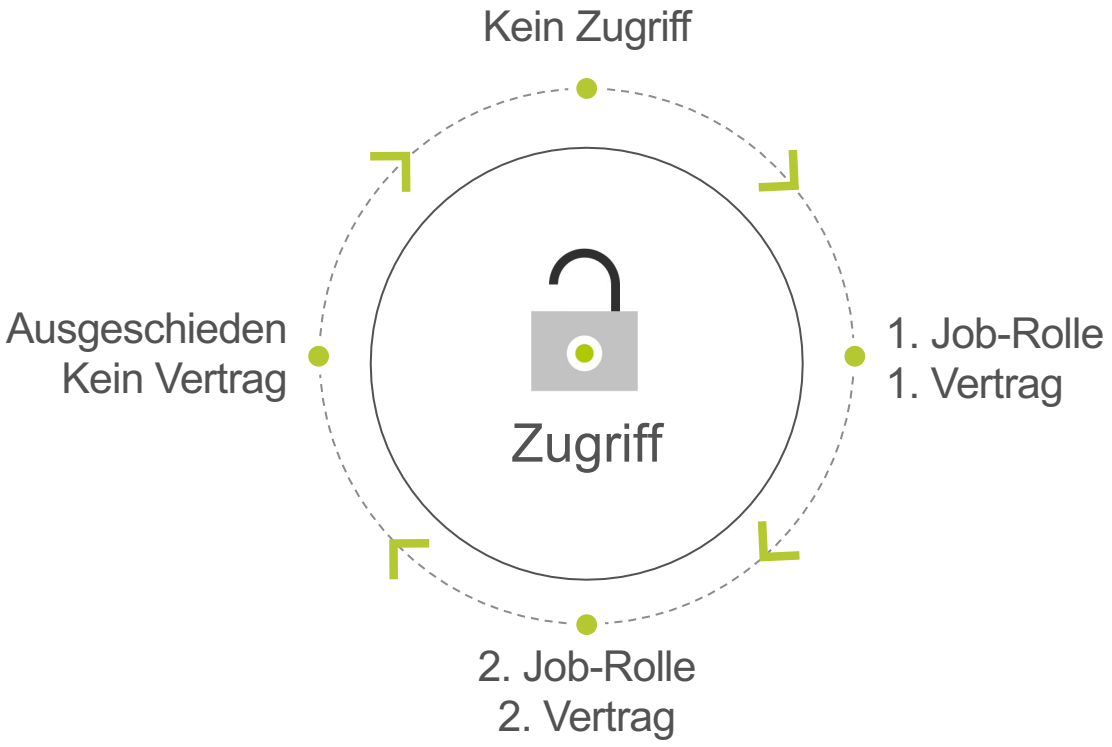
- Benutzer-Provisionierung/Deprovisionierung
- Zeitgerechte Zugriffe auf Ressourcen
- Zugriffsänderungen über die Zeit



Azure AD Identity Governance

Zugriffslebenszyklus

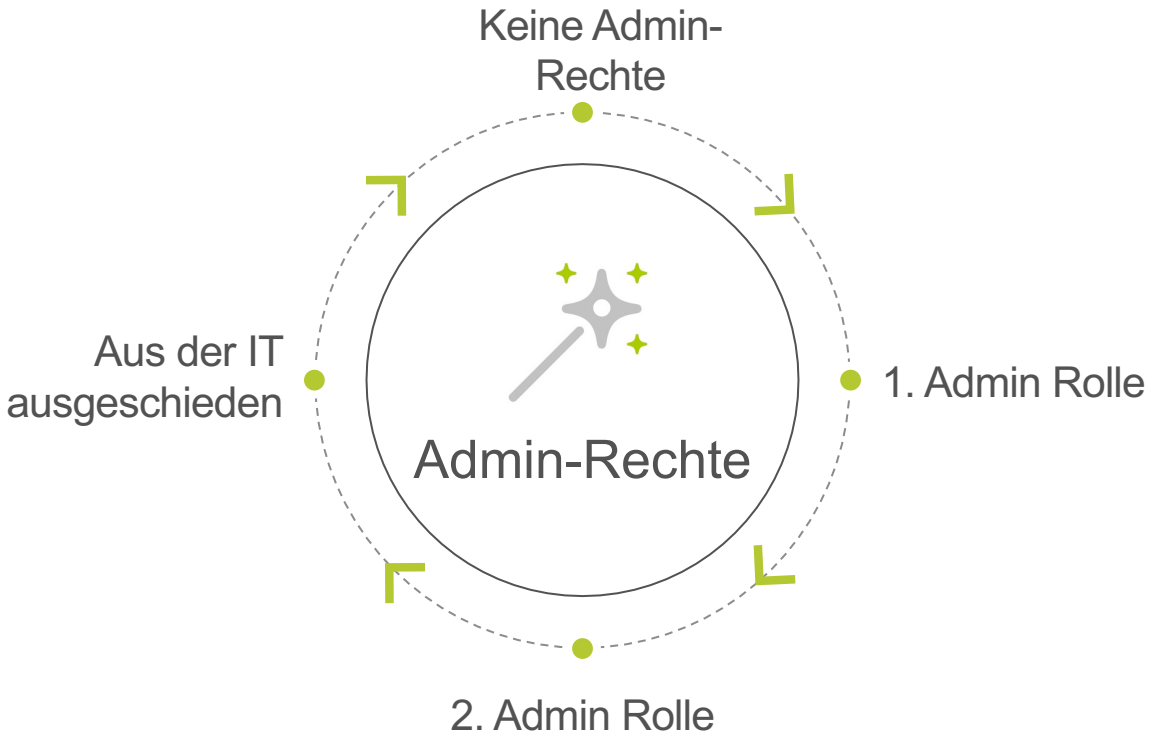
- Verwalten von Zugriffsänderungen über die Zeit
- Delegation von Genehmigungs-Workflows für Zugriffe
- Re-Zertifizierungen
- Prozess-Automatisierung



Azure AD Identity Governance

Priviligierter Zugriffslebenszyklus

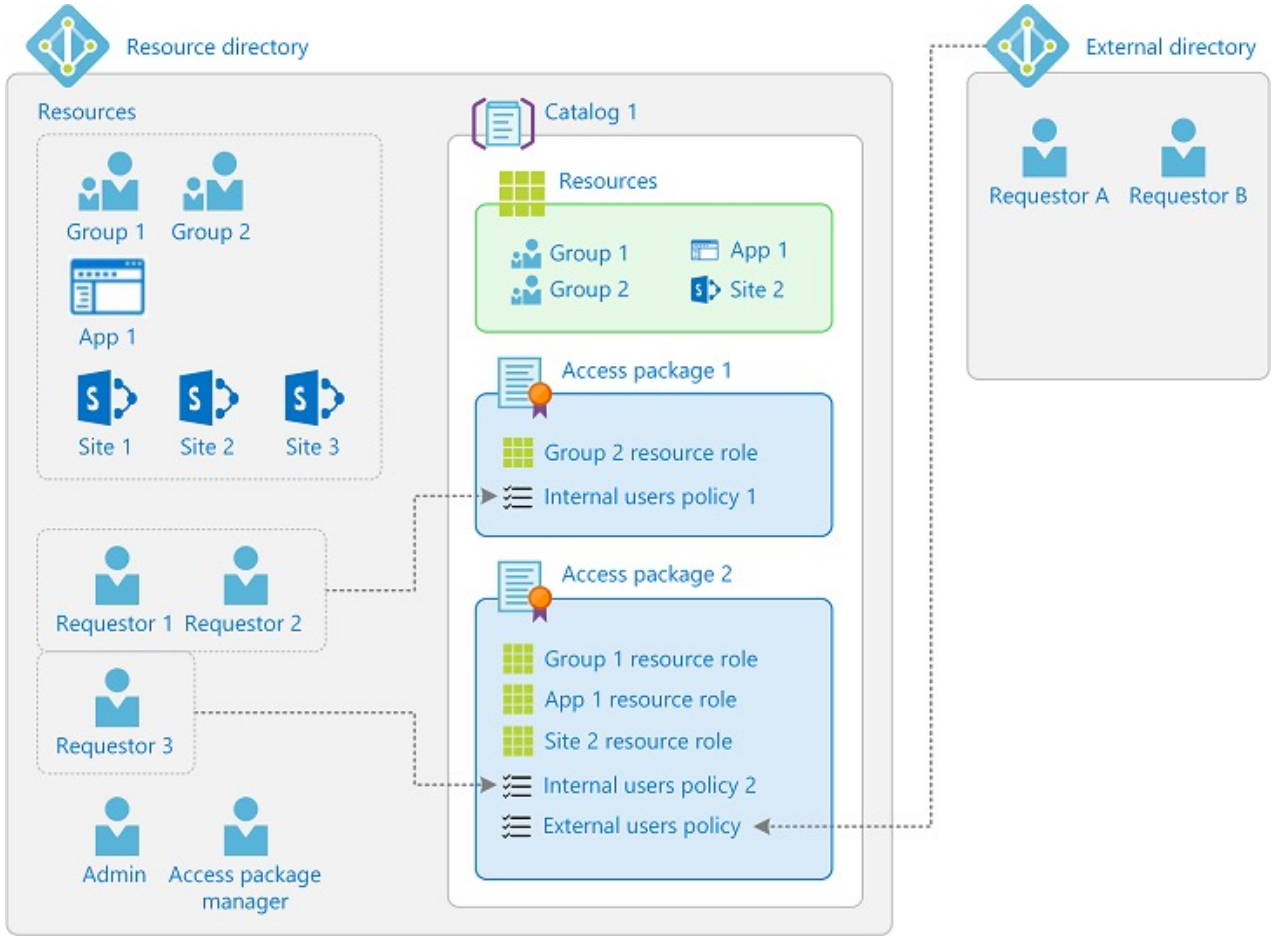
- „Just-in-Time“-Zugriff
- Zeitgebundener Zugriff
- Genehmigungsprozesse
- Re-Zertifizierungen
- Mehrstufige Authentifizierung
- Überwachung und Alarmierung
- Bedingter Zugriff



Azure AD Identity Governance

Entitlement Management

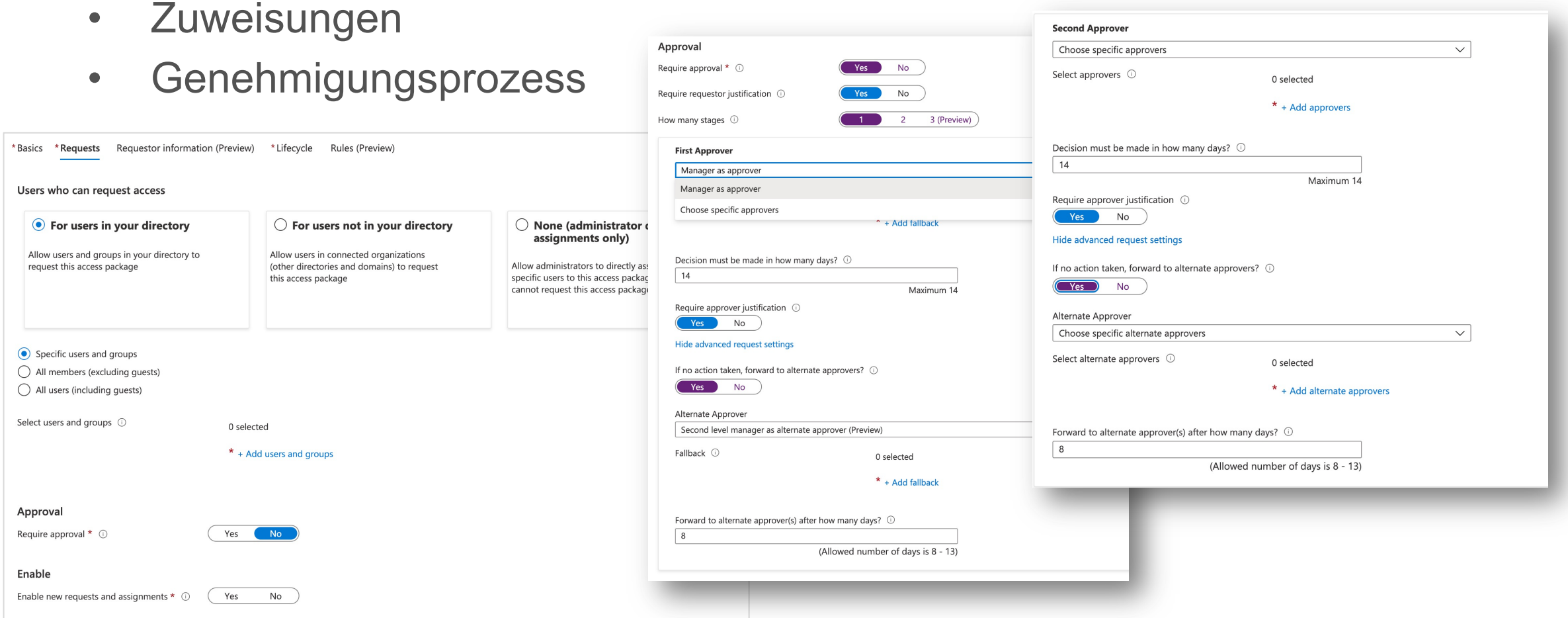
- Ressourcen
- Kataloge
- Zugriffspakete
- Ressourcen Rollen
- Benutzer-Richtlinien
- Anforderer (Intern/Extern)
- Genehmigungsprozesse (Einfach oder Mehrstufig)
- Genehmigende Person/en



Azure AD Identity Governance

Entitlement Management

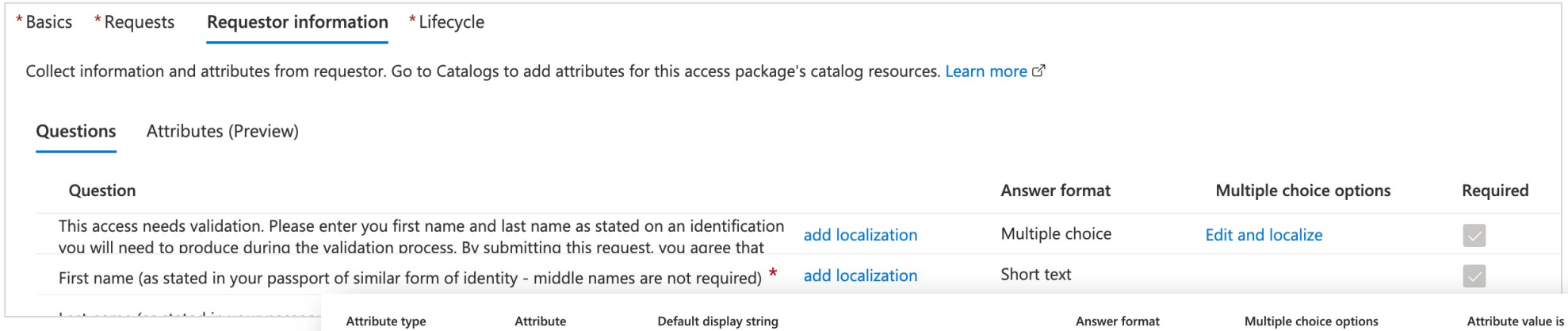
- Richtlinien für Zugriffspakete
  - Zuweisungen
  - Genehmigungsprozess

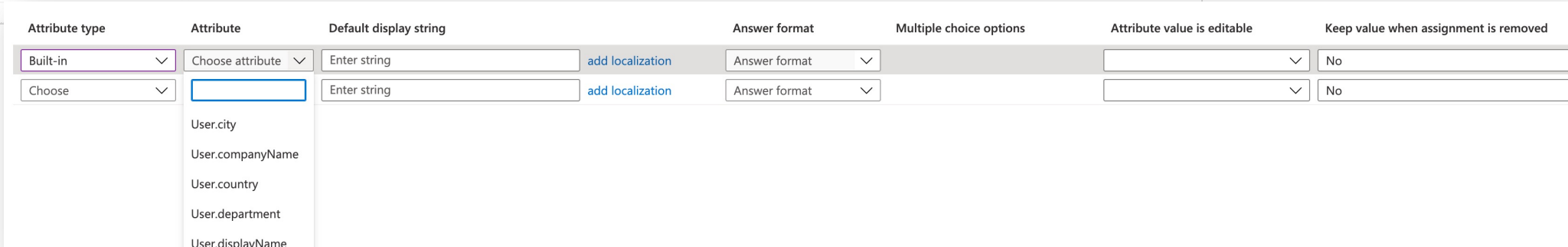


Azure AD Identity Governance

Entitlement Management

- Informationen zum Antragsteller
  - Fragen, z.B. zur Unterstützung des Genehmigers
  - Attribute – Verzeichnis-Schema oder Schema-Erweiterung

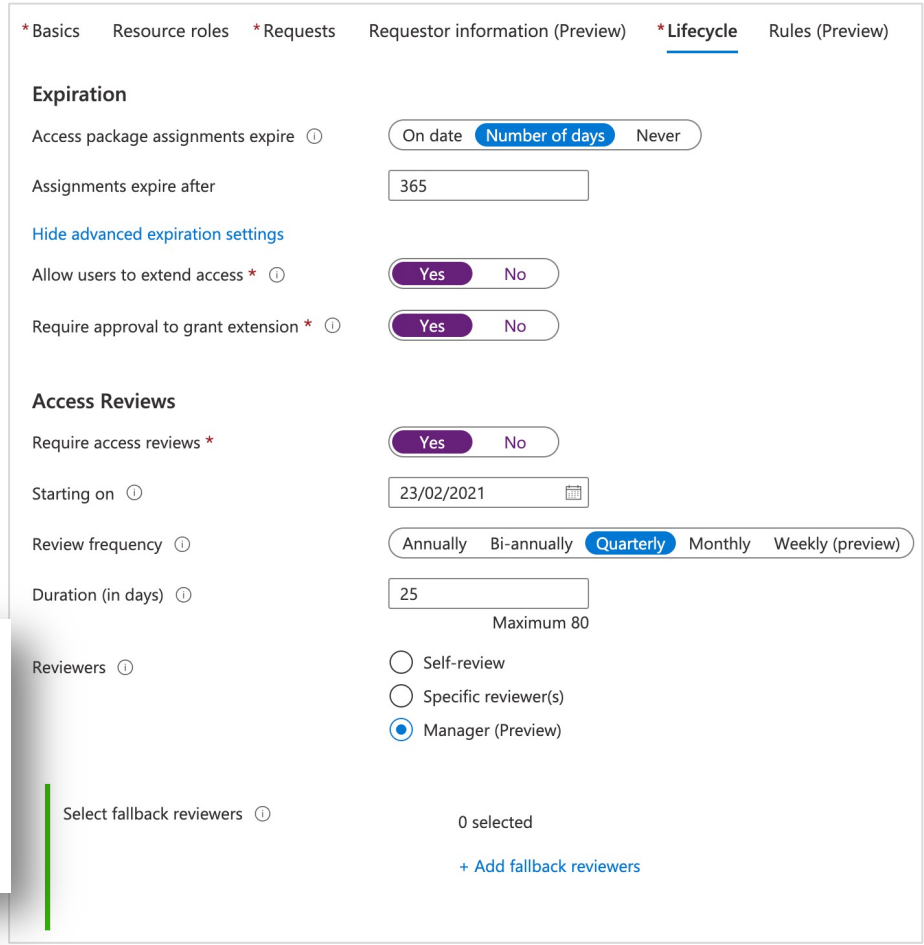


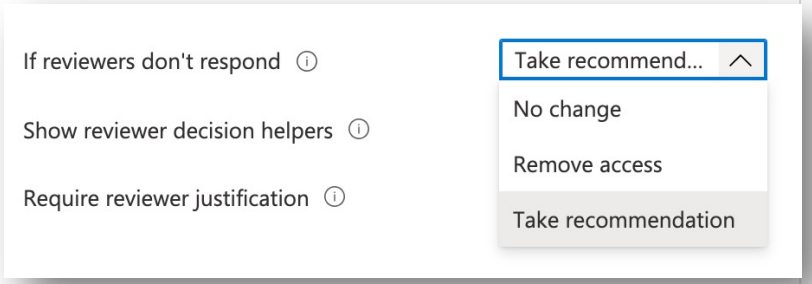


Azure AD Identity Governance

Entitlement Management

- Zugriffslebenszyklus
  - Ablauf von Zuweisungen
  - Re-Zertifizierung
  - Automatisierung

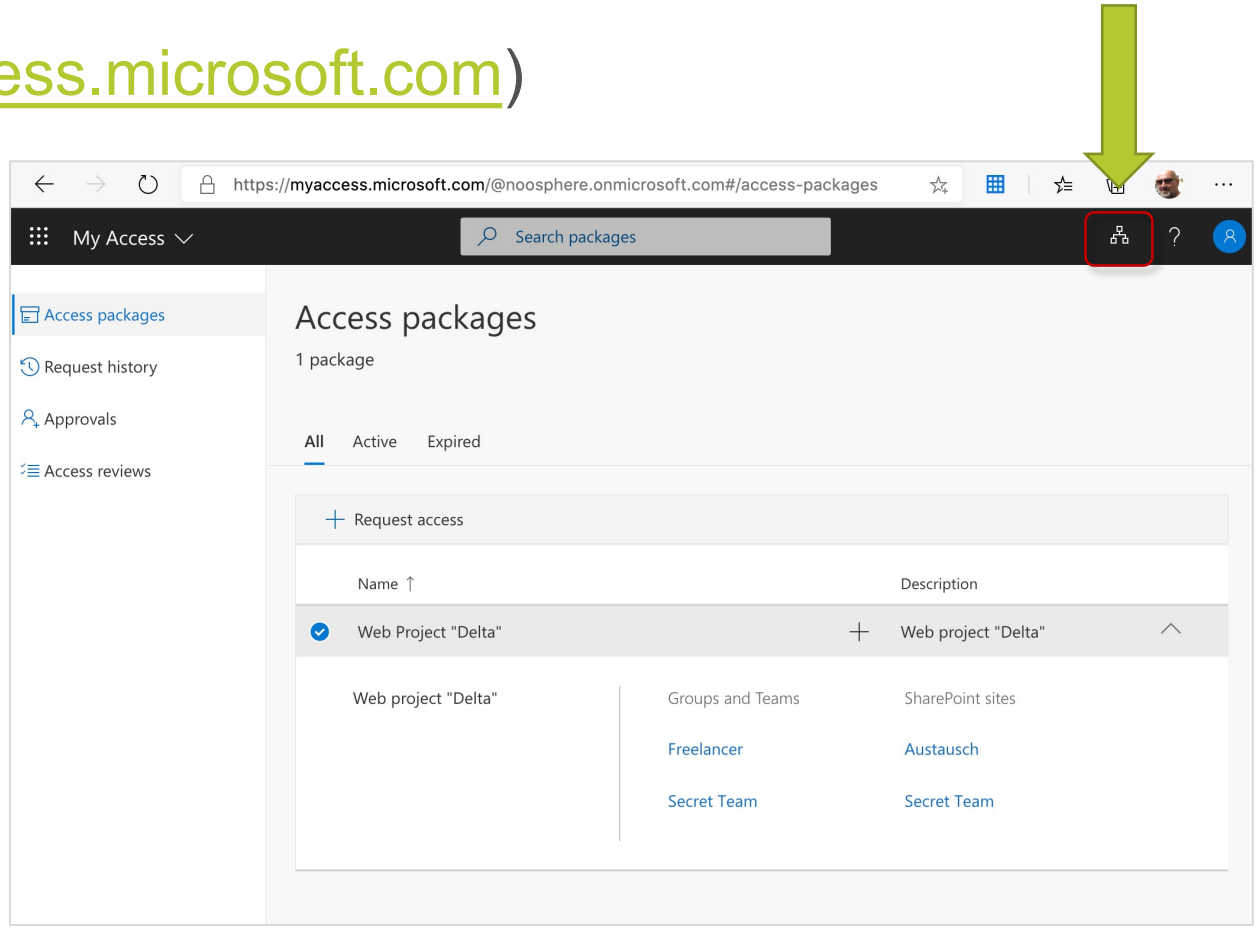




Azure AD Identity Governance

Entitlement Management

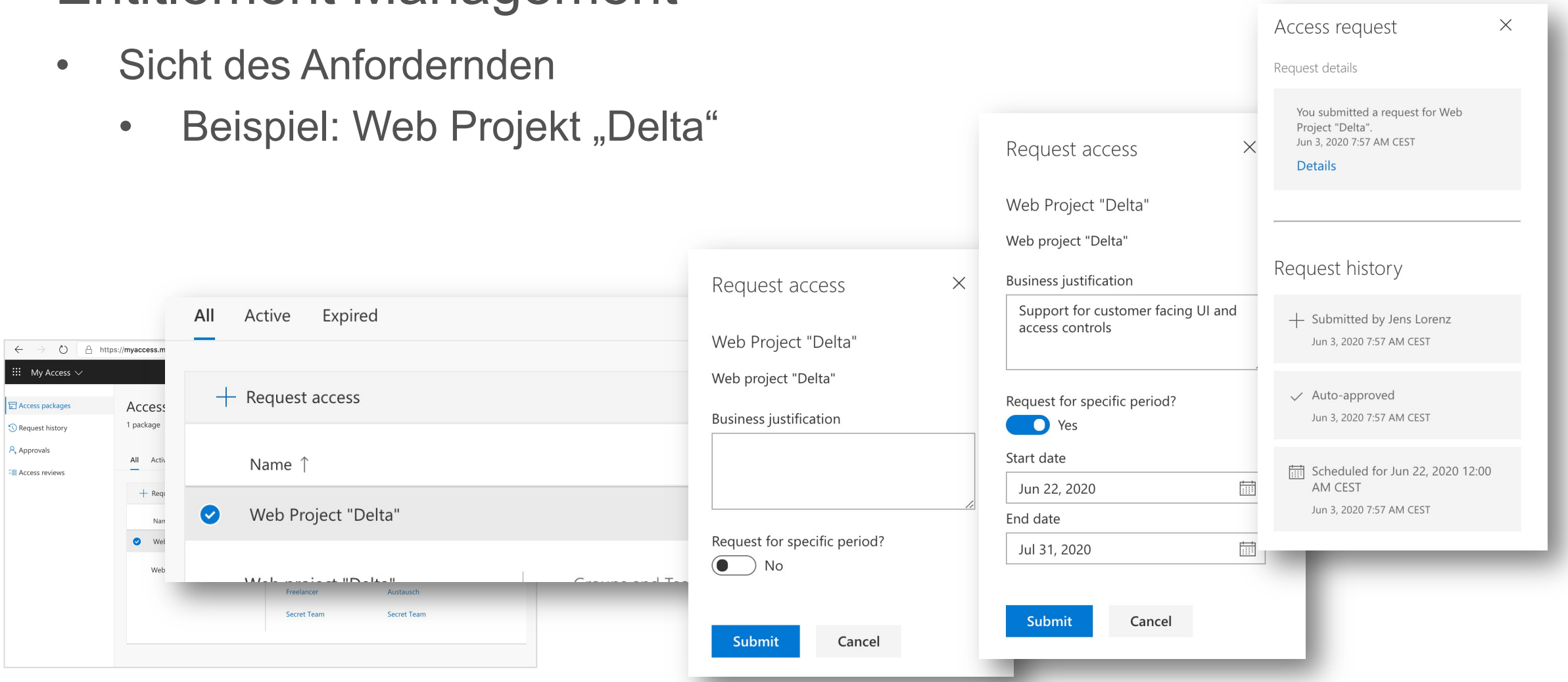
- Sicht des Anfordernden
  - My Access Portal (https://myaccess.microsoft.com)
    - Zugriffspakete
    - Historie
    - Genehmigungen
    - Re-Zertifizierungen
    - Organisations-übergreifend
    - Multi-Lingual



Azure AD Identity Governance

Entitlement Management

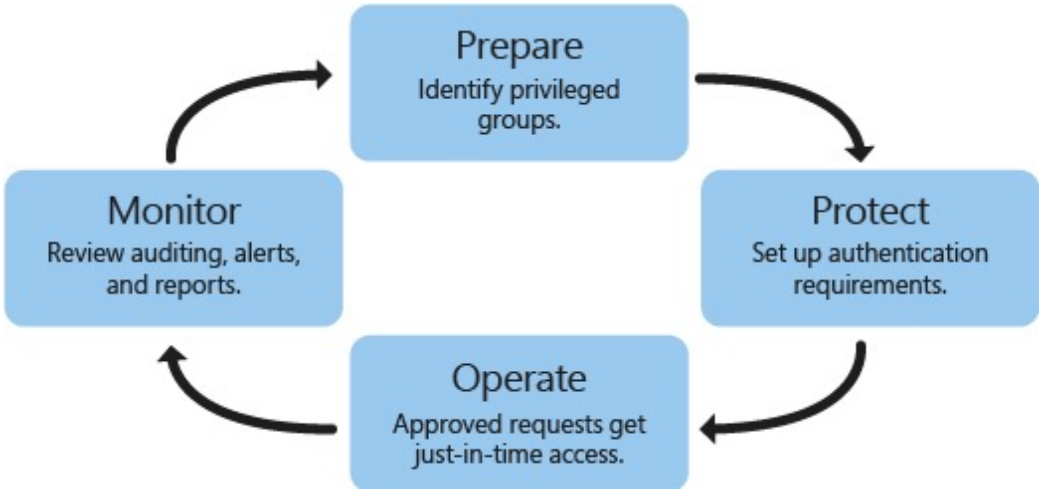
- Sicht des Anfordernden
  - Beispiel: Web Projekt „Delta“



Azure AD Identity Governance

Privileged Identity Managenent

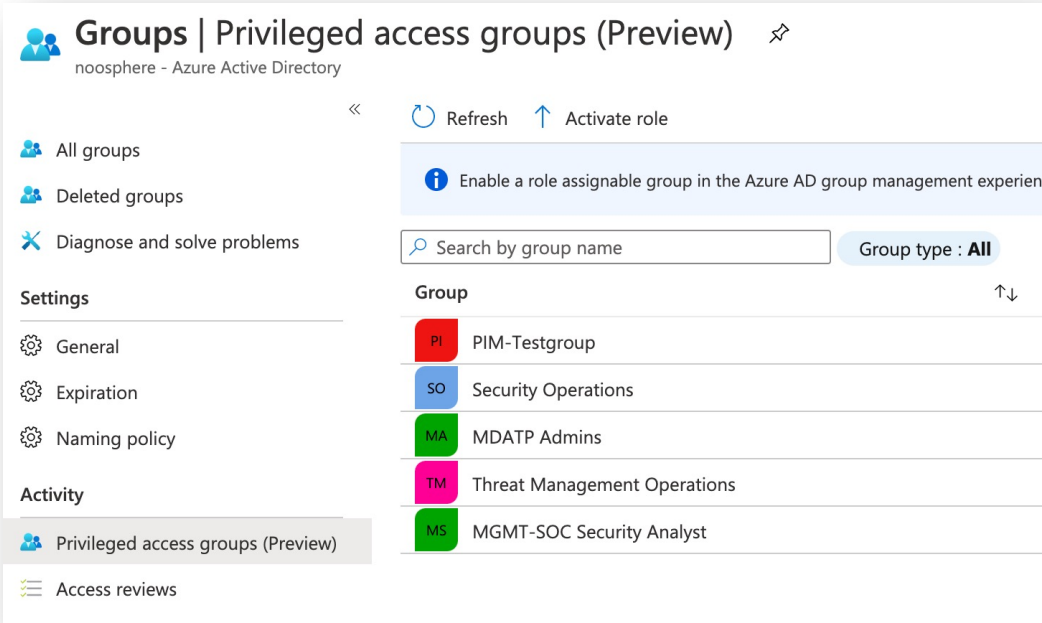
- „Just-enough-Administration“ (Least Privilege)
  - Dedizierte RBAC Rollen mit definierten Privilegien
- „Just-in-time-Administration“ (Need to Know)
  - Zeitbasierte Zuweisung von privilegierten Rollen
- Genehmigungsprozesse
  - Z.B. „Peer-Review“
- Nachverfolgbarkeit
- Re-Zertifizierung von privilegierten Rollenzuweisungen



Azure AD Identity Governance

Privileged Identity Managenent

- Privileged Access Groups
  - Definition von privilegierten operativen Rollen in der Organisation
  - Zuweisung von Rollen und Rechten über PAG
  - „Just-in-Time“- und zeitgebundene Zuweisungen
  - Integration in Entitlement Management

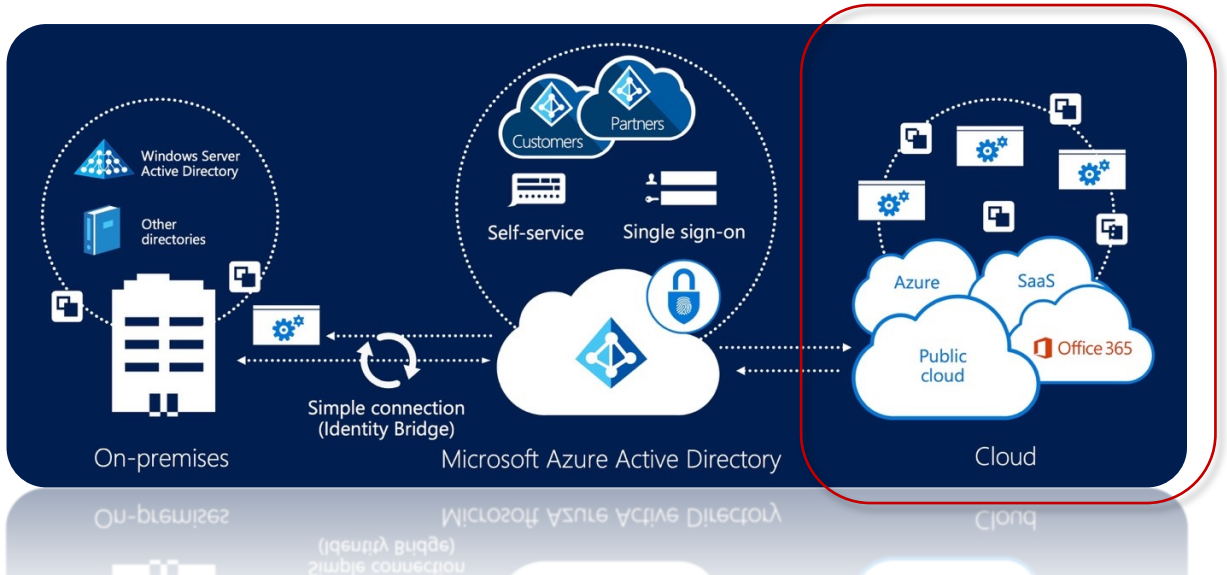


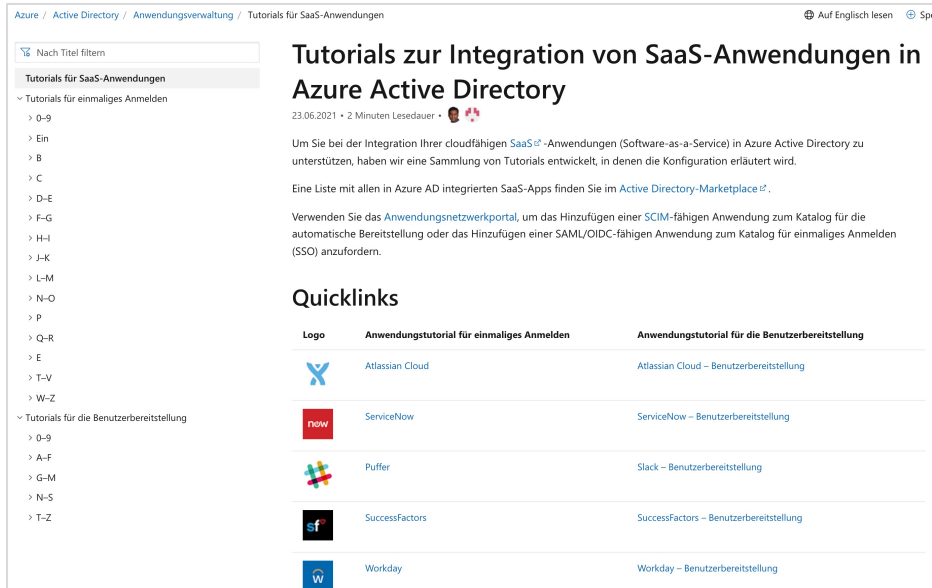
Azure AD Cloud App Discovery mit Microsoft Cloud App Security

Azure AD Cloud App Discovery

Azure AD als zentraler Identity Provider

- Integration von Cloud Apps
  - Microsoft und Drittanbieter
  - Zentrale Authentifizierung und Autorisierung
  - Integration in Azure AD Conditional Access (Zero-Trust)

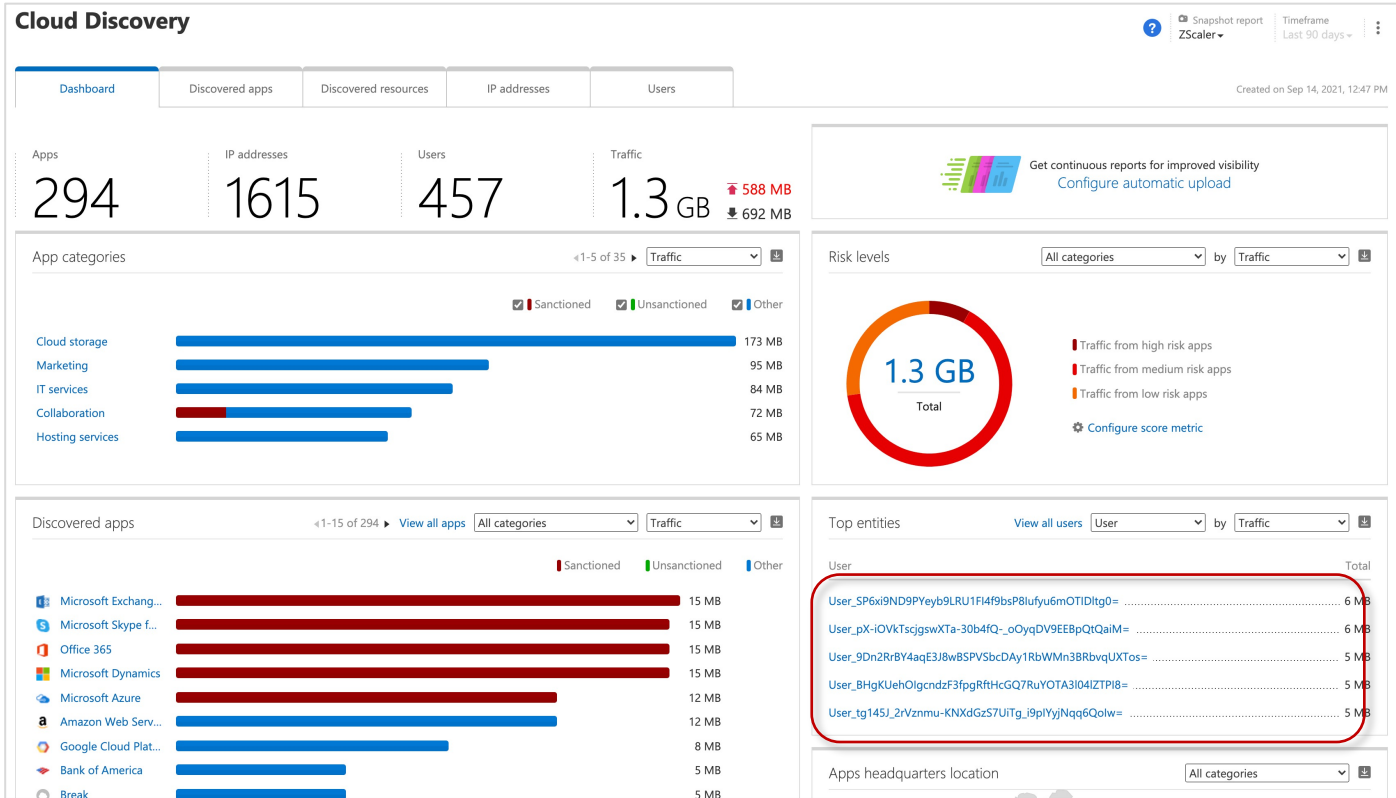




Azure AD Cloud App Discovery

Erfassen und Bewerten von Cloud Apps

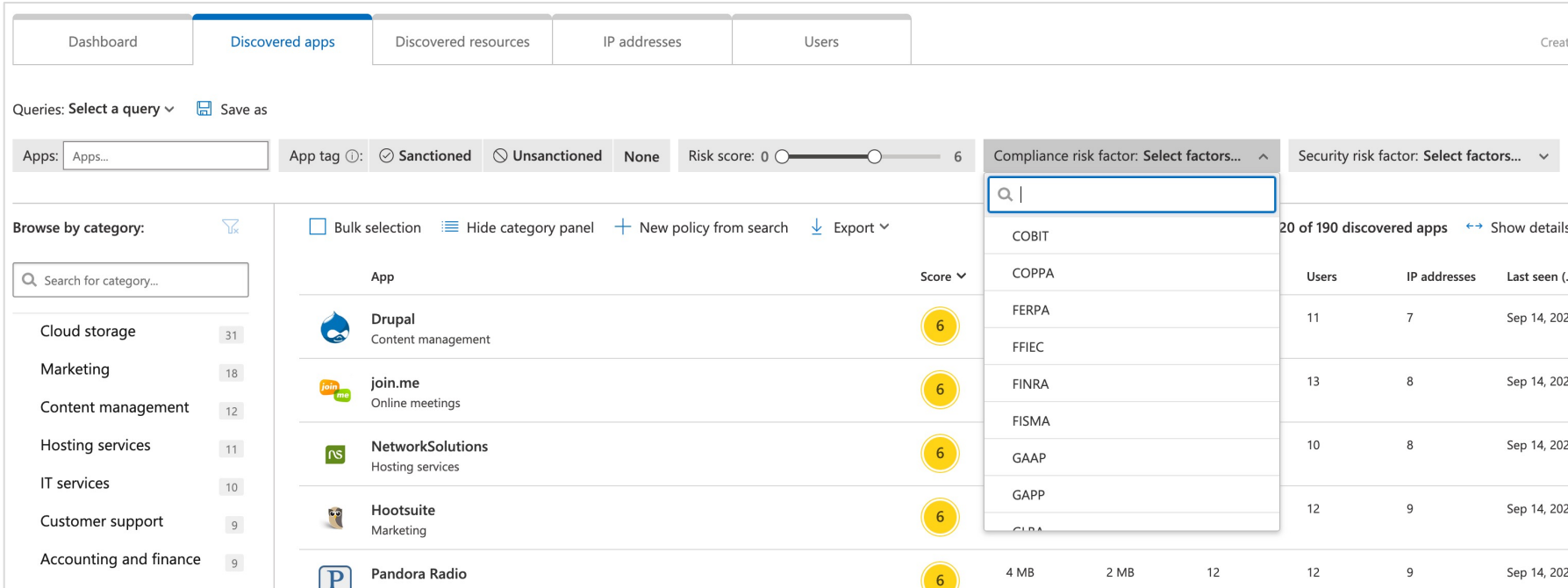
- Integration mit Proxy Anbietern
- Integration mit Microsoft Defender for Endpoint
  - Kategorisierung
  - Risikobewertung
- Pseudonomisierung von Benutzerinformationen



Azure AD Cloud App Discovery

Bewertung nach Compliance und Security

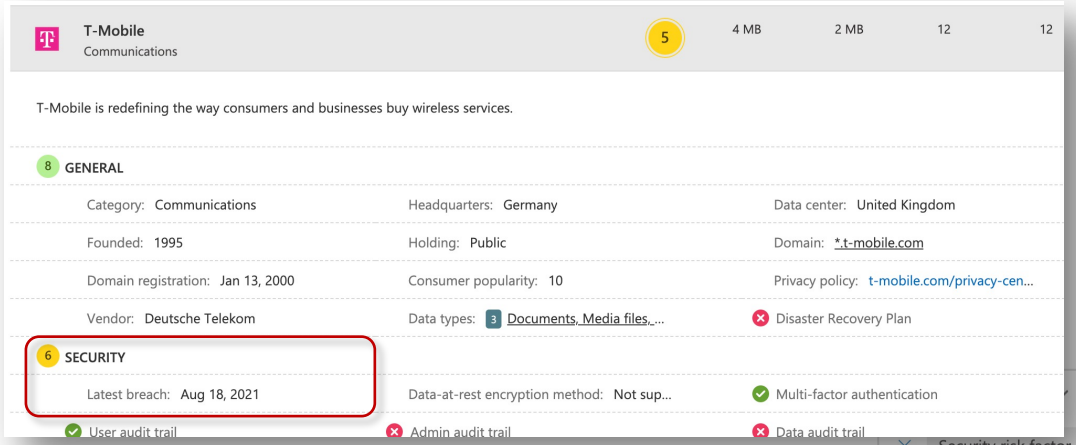
- Filtern nach Risiko-Bewertung, Compliance oder Security Faktoren
- Sanktionieren von Apps
  - Verwenden für Data Loss Prevention Funktionen (Microsoft 365 DLP)

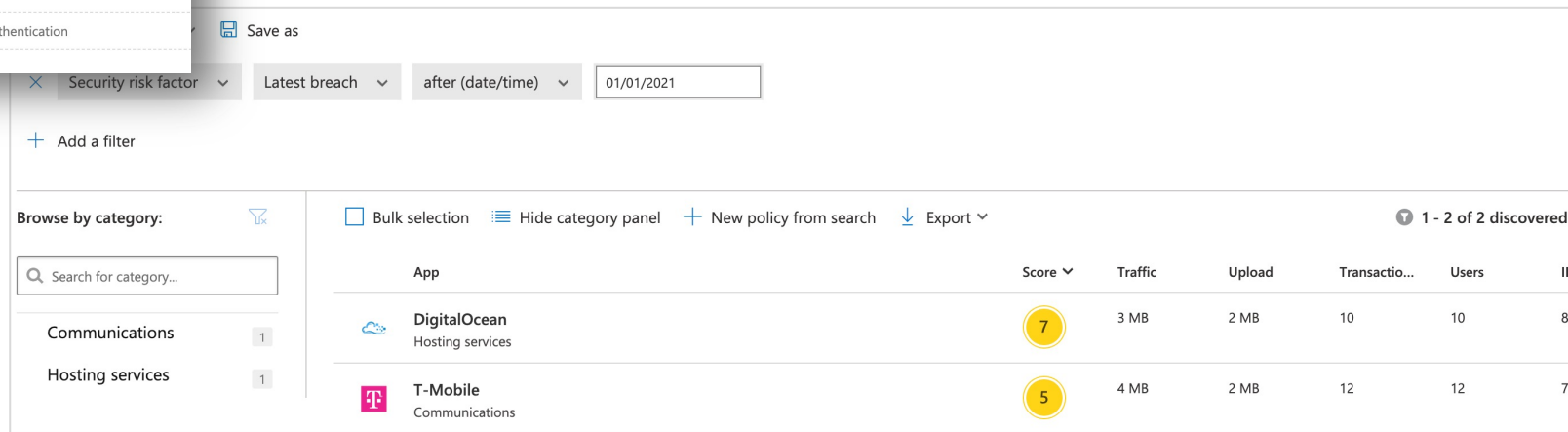


Azure AD Cloud App Discovery

Bewertung nach Compliance und Security

- Filtern nach spezifischen Risiken (z.B. Datenpannen)
  - Automatische Alarmierungen

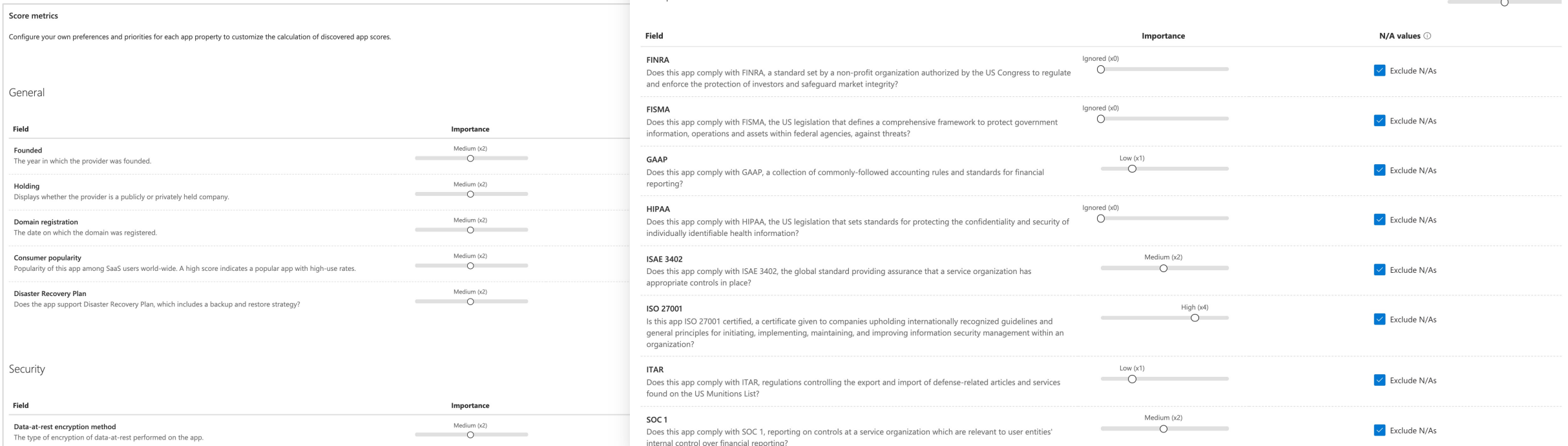




Azure AD Cloud App Discovery

Anpassung an die Anforderungen der Organisation

- Gewichtung in den Bewertungen
- Relevanz von Compliance Anforderungen



Webinar-Reihe „Compliance mit IT“

Nachfolgende Webinare:

- Mittwoch, 27.10.2021: *Datenmanagement im Kontext Compliance* (Anmelden)
- Mittwoch, 24.11.2021: *Adressieren von Insider-Risiken* (Anmelden)

Vielen Dank!

Jens Lorenz
Strategic Consultant, CISSP, CSSP, CIPT

mail: jens.lorenz@sits-d.de
fon: +49-170-4516565

LinkedIn: https://de.linkedin.com/in/jenslorenz