

Session B2

wie baut man eine sichere Datenplattform in der Cloud unter Berücksichtigung strenger Datenschutzrichtlinien



Patrick Vogler

Senior Consultant Data & Analytics
Cloud Solution Architect
Associate Partner
pvogler@it-logix.ch



Elgar Brunott

Principal Consultant Data & Analytics
Associate Partner
ebrunott@it-logix.ch

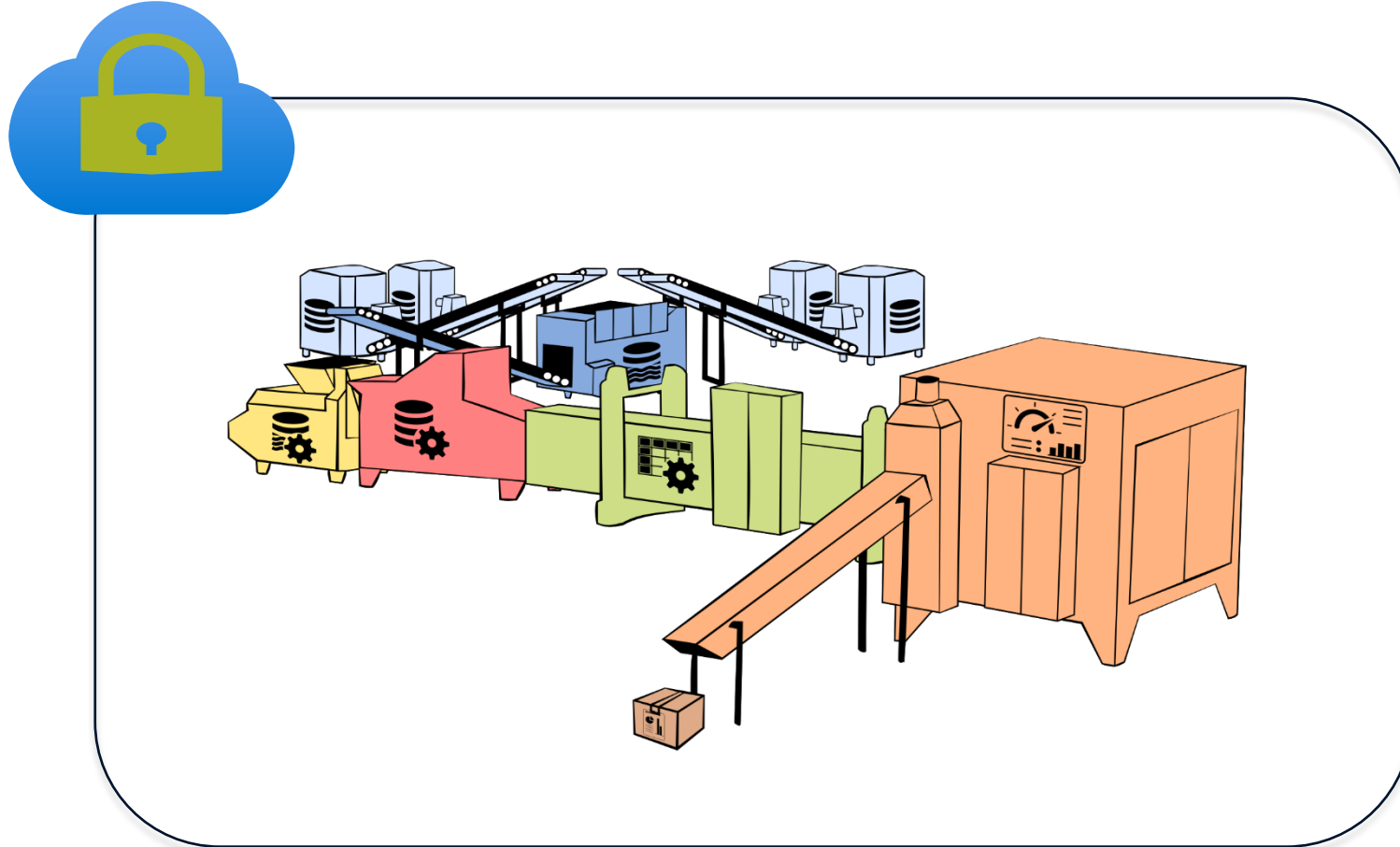
Stellen Sie Fragen in der virtuellen Plattform

- 1 Loggen Sie sich auf der virtuellen Plattform mit **Ihrem persönlichen Link** ein (aus Bestätigungs-Mail MAKE BI)
- 2 Kicken Sie in der Lobby auf der **Session B2** auf den Button „**Teilnehmen**“

- 3 Kicken Sie in der **Session B2** auf der rechten Seite in der Navigation auf „**Q&A**“
MOBILE: Klicken Sie der Navigation unten zuerst auf „**Interaktion**“, danach auf das **Sprechblasen-Symbol**


- 4 Geben Sie im entsprechenden Feld Ihre Frage ein und schicken Sie diese ab, indem Sie auf das **Pfeil-Symbol** klicken

Die Referenten werden am Ende Ihrer Präsentation vereinzelt auf Fragen eingehen. Nicht beantwortete Fragen können gerne bei den diversen Networking-Möglichkeiten mit den entsprechenden Referenten aufgegriffen werden.





Agenda

- › Systemarchitektur
- › Authentifizierung in der Cloud
- › Datenschutz und Datensicherheit
- › Verfügbarkeit und Skalierbarkeit

Systemarchitektur

Wie unterstützt Microsoft Unternehmen bei der “Cloud Journey”

- › Cloud Adoption Framework
- › Microsoft Cloud Reference Architecture (MCRA)
- › Microsoft Well Architected Framework
- › Microsoft Cloud Security Benchmark (MCSB)
- › Rapid Modernization Plan (RaMP) für Zero Trust

Cloud Adoption Framework

Paradigmen:

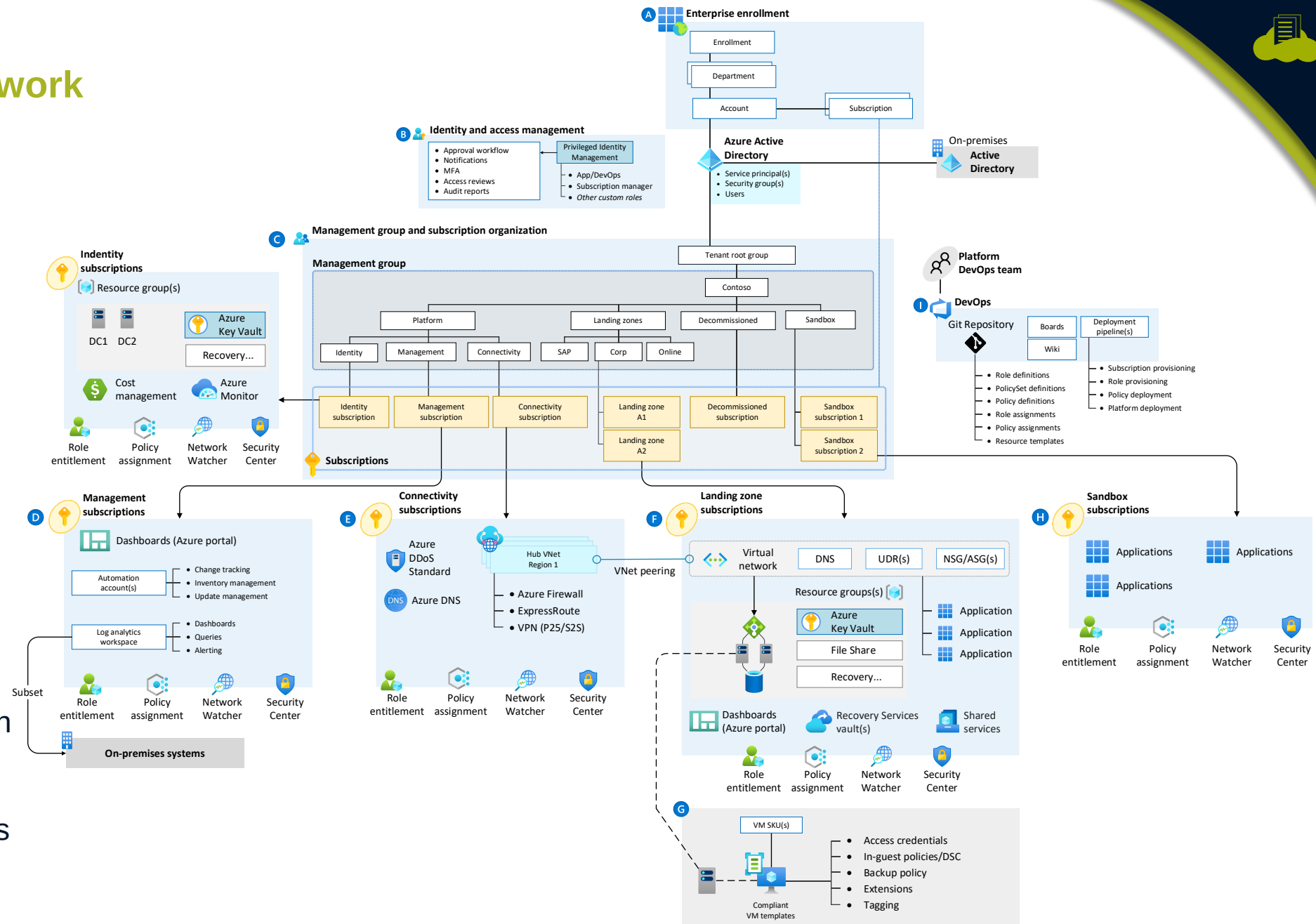
- Start Small and Expand
- Enterprise Scale

Abhängig von:

- Fokus
- Cloud-Organisation
- Cloud-Buchhaltung
- Workloads zu migrieren
- Workloads zukünftig

Kernthemen:

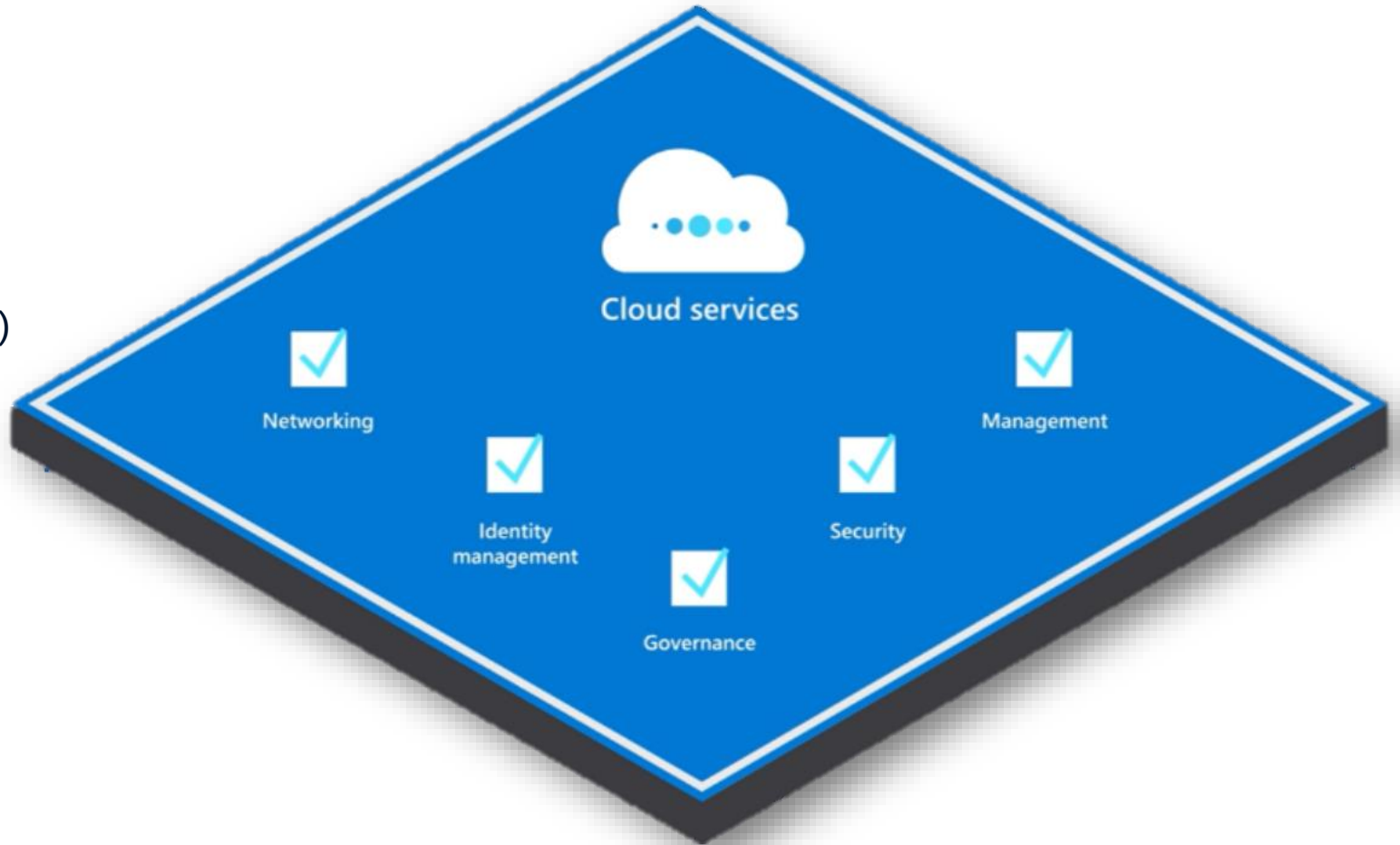
- Enterprise Enrollment
- IAM
- Management groups
- Subscription Organisation
- DevOps
- Platform Landingzones
- Application Landingzones
- Sandbox Landingzones





Azure Landingzone

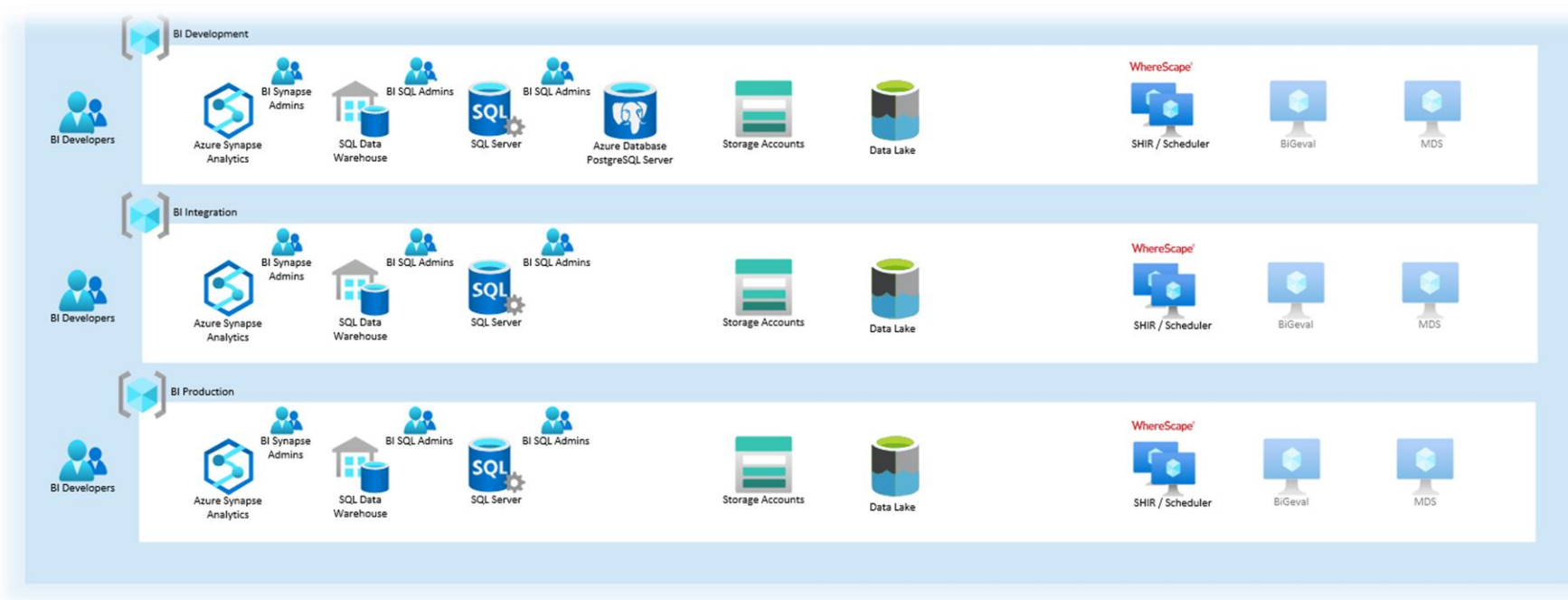
- › Was ist eine Landingzone?
- › Besteht aus (nicht abschliessend):
 - › Subscription als logische Gliederung und Abrechnungsbereich
 - › Netzwerkanbindung
 - › Angewendete Richtlinien (Azure Policies)
 - › Monitoring und Auditierungskonzept
 - › Backupstrategie und Ressourcen
 - › Vorkonfigurierte Sicherheitsfeatures





Umgebungen

- › Verschiedene Ansätze
- › Abhängig von der Datenplattform und Grösse
- › Gemäss Standardkonzept IT-Logix 1 dedizierte Landingzone



Zero Trust Einführung

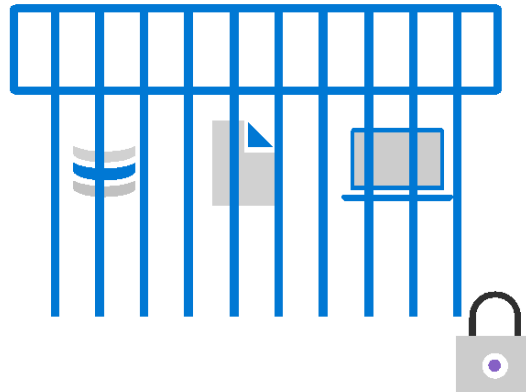


Secure Assets where they are with Zero Trust
Simplify security and make it more effective

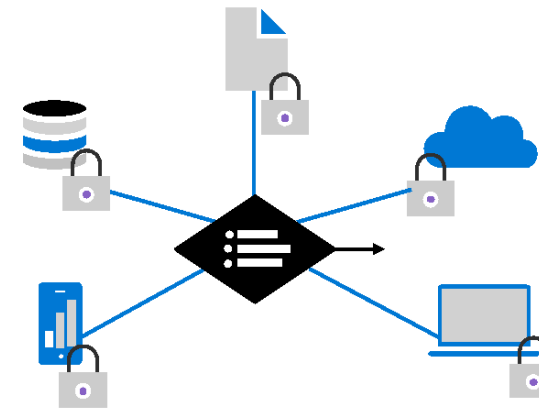
Perimeter based

Restricted access

Trusted Assets



Classic Approach
Restrict everything to a 'secure' network



Zero Trust
Protect assets anywhere with central policy

Verify explicitly

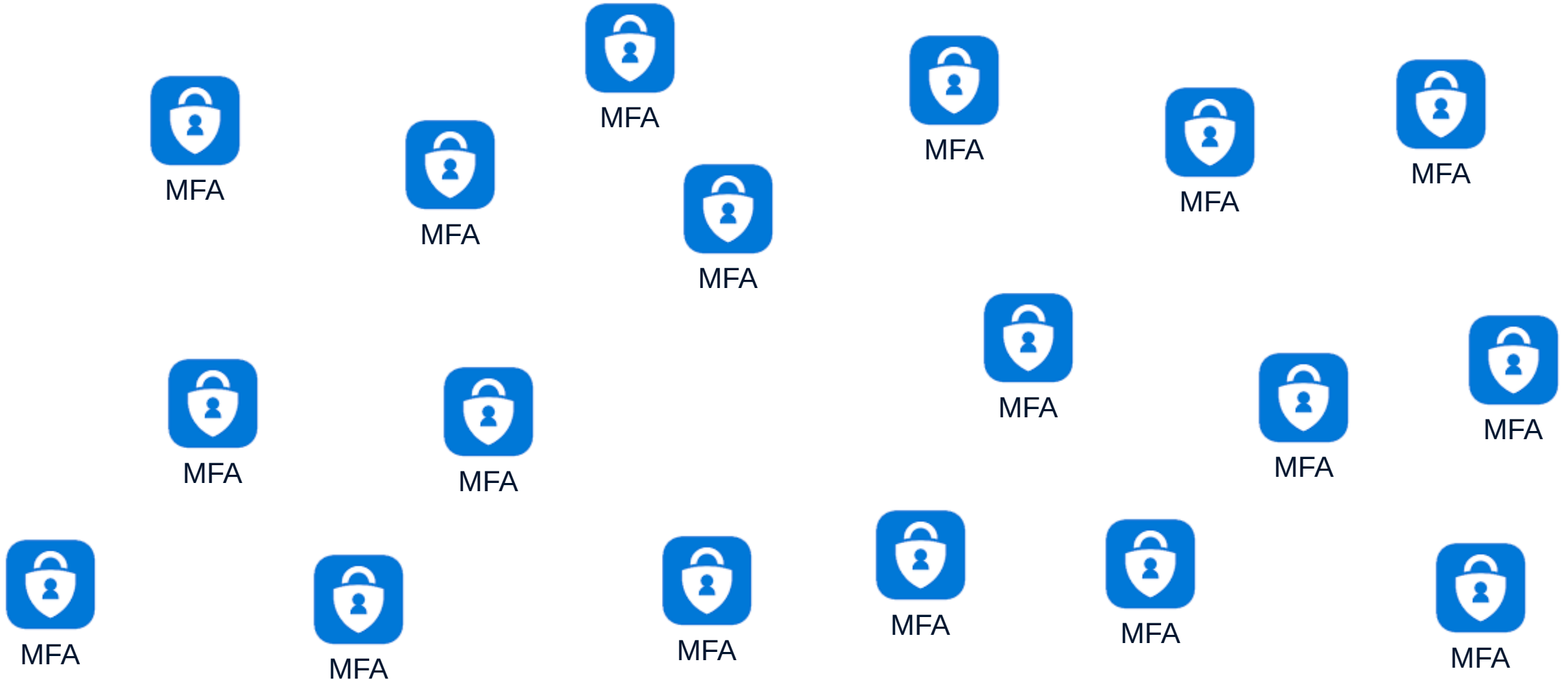
Least privilege access

Assume breach

Authentifizierung in der Cloud



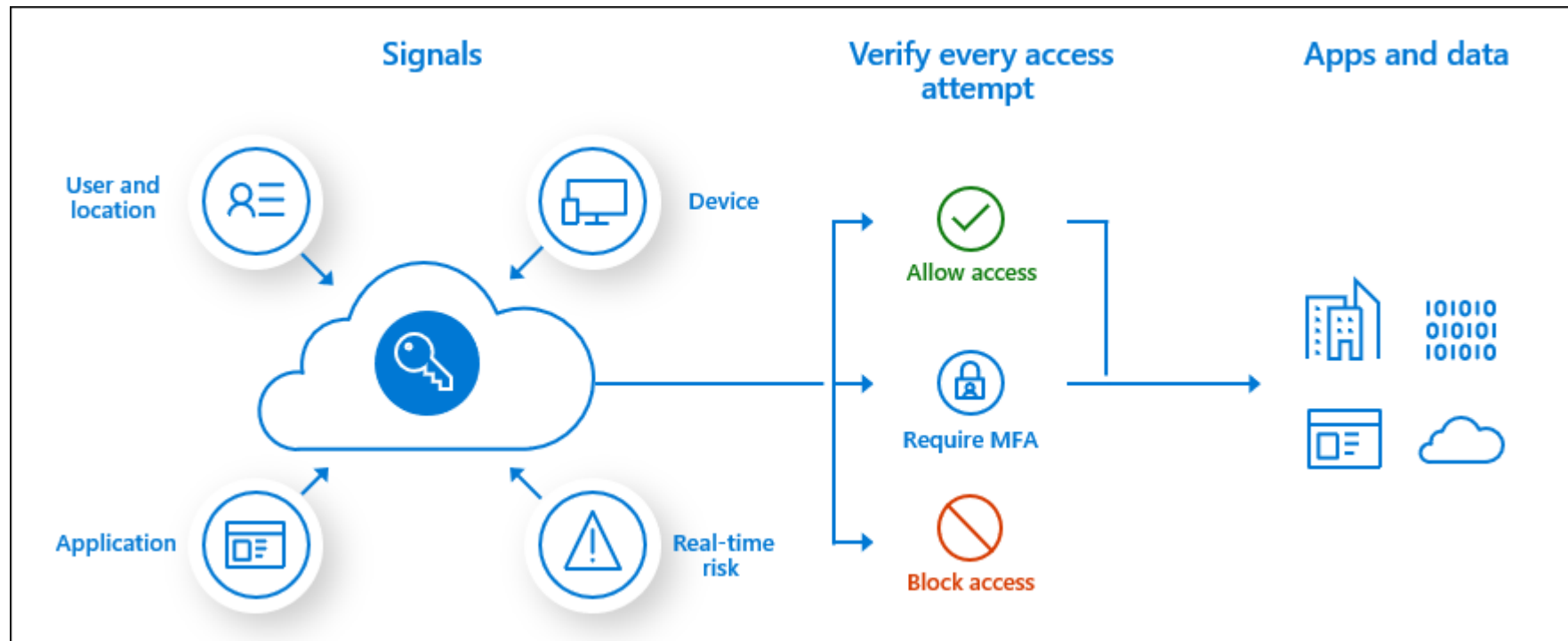
Wichtigstes Authentifizierungsmerkmal





Authentifizierungsmethoden

- › Fokus moderne Authentifizierungsmethoden (Entra ID) und Monitoring (Identity Protection) – Zero Trust
- › Lokale Authentifizierungsmethoden (SQL-Authentifizierung, lokale Windows Authentifizierung) möglichst vermeiden
- › Einbindung von legacy Applikationen über Entra ID App Proxy



Azure Conditional Access



Bewertung und Umsetzung von Sicherheitsmassnahmen

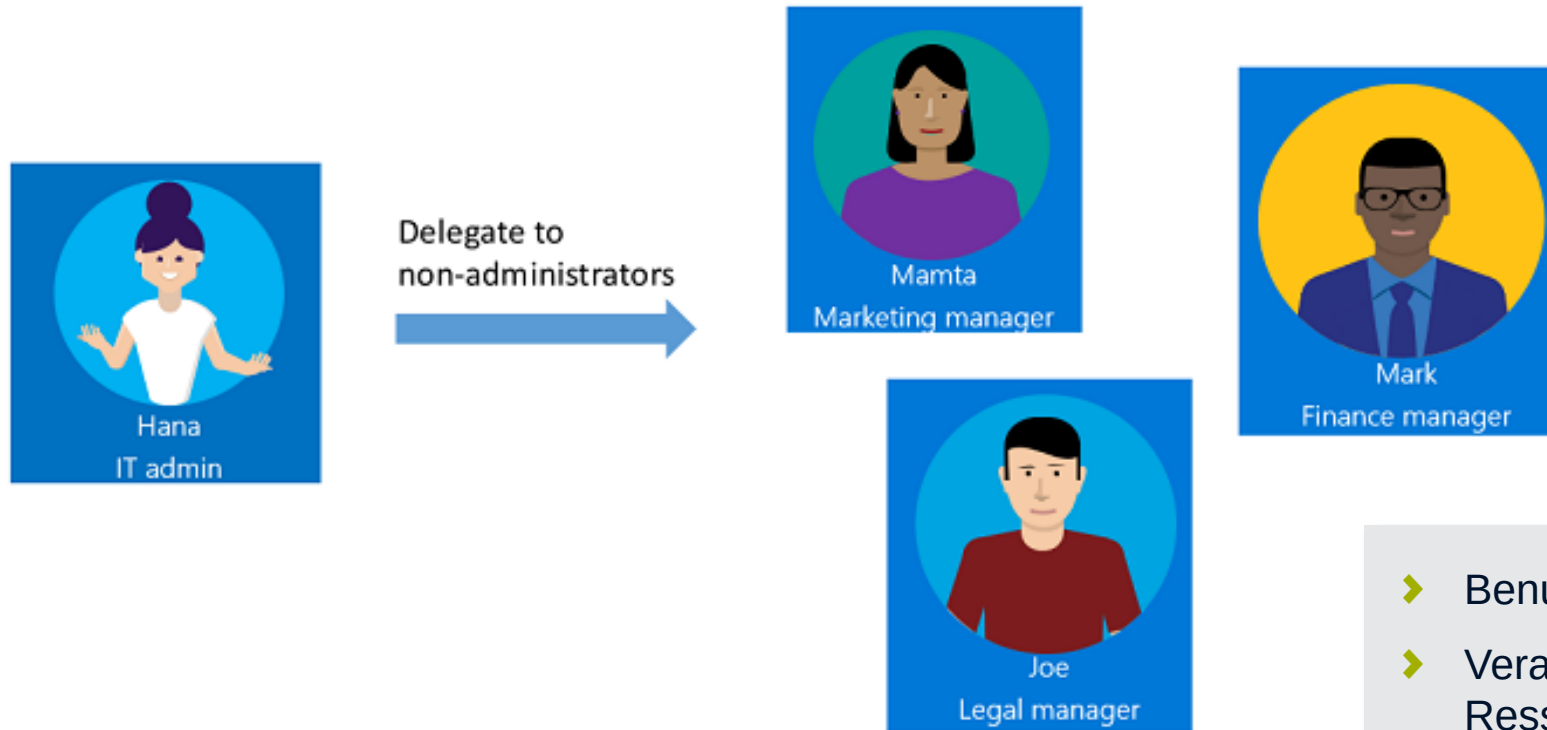
Measure	Security Impact	User Impact	Implementation Costs
MFA	High	Low	Low
Enable Entra ID Identity Protection	High	Moderate	Moderate
Use least privileged Access administrative Roles	Low	Low	Low
Expiring passwords	Low	High	Low
Low Refresh Token Lifetime	Low	High	Moderate
User consent to apps not allowed	Moderate	Moderate	Low

Umsetzen

Von Fall zu Fall

Weglassen

Delegierte Administration



- Benutzer kann Zugang selbst anfordern
- Verantwortliche Person kann Rolle / Ressourcen selbst verwalten

Beispiele:

- Product Owner und BI Administrator verwaltet BI Rollen
- Application Owner verwaltet Landingzone

Datensicherheit und Datenschutz



Verschlüsselung

- › Data-at-rest (TDE, Bitlocker)
- › Data-in-transit (TLS, VPN, Expressroute)
- › Data-in-use
 - › Daten müssen entschlüsselt werden, um verarbeiten werden zu können
 - › Clientseitige Verschlüsselung



Datenschutzmassnahmen

› Pseudonymisierung

- › Ersetzen von Personendaten durch ein Pseudonym oder eine eindeutige Identifikation. Die hersteller von die daten kann immer noch Rückschlüsse auf die ursprüngliche Person.



› Anonymisierung

- › Entfernt oder verändert alle persönlich identifizierbaren Information (PII)
- › Rückschlüsse sind ausgeschlossen

› Maskierung

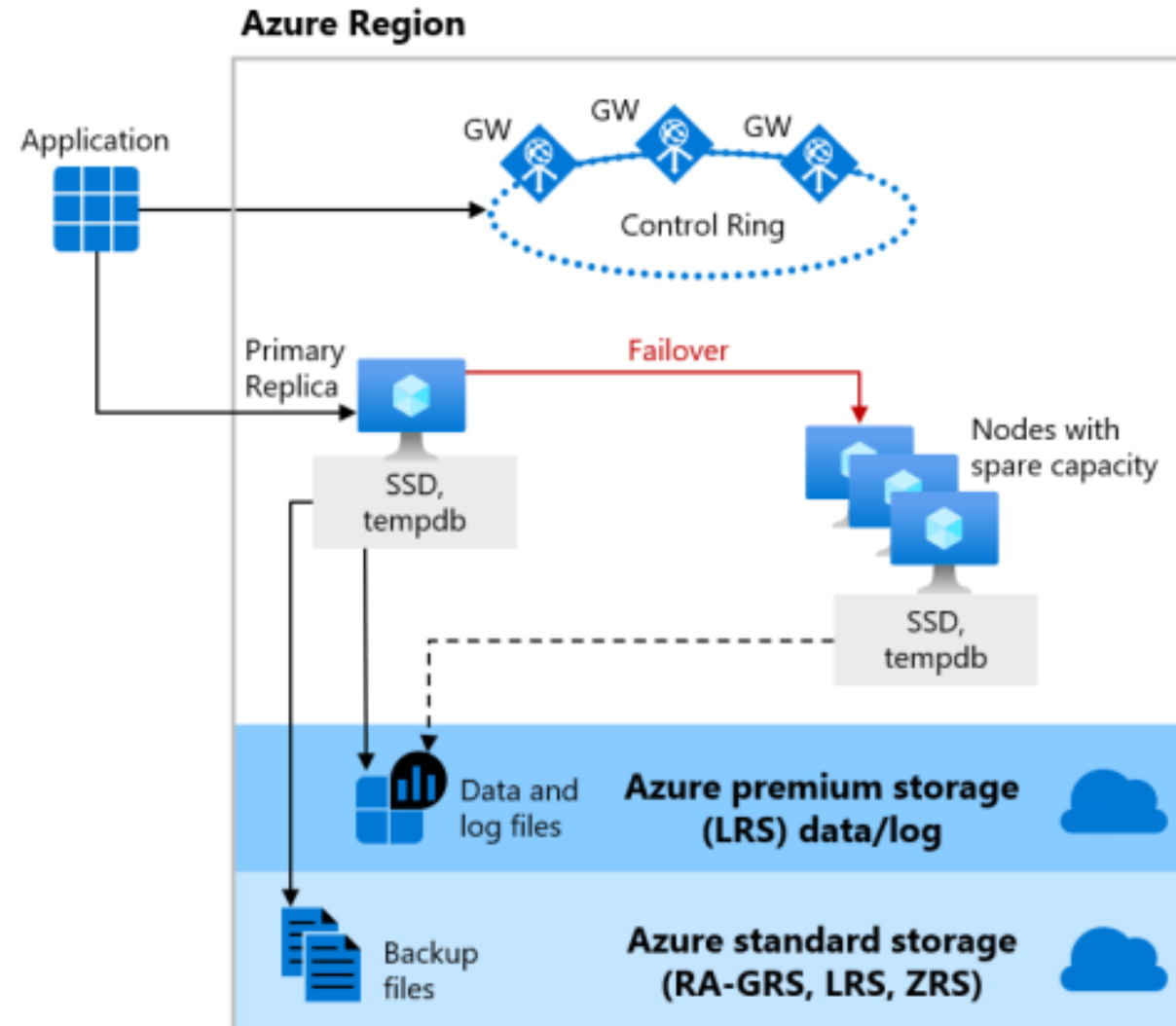
- › Datenfelder werden für bestimmte Benutzergruppen maskiert
- › Die ursprünglichen Daten bleiben erhalten und werden nicht verändert



Verfügbarkeit und Skalierbarkeit

Verfügbarkeit und Skalierbarkeit

Beispiel Azure SQL Database
SLA 99.99%





Kostenoptimierung

- › Nutzungsbasierte Modelle erfordern Kostenoptimierung
- › Grünere IT durch Kostenoptimierung (Emission Impact Dashboard)

Massnahmen

- › Nach Bedarf Skalieren
- › Ressourcen herunterfahren oder pausieren
- › Reservationen verwenden
- › Kosten- und Ressourcenmonitoring (Budgets)



Pitfalls und Antipattern

- › Verwendung von On-Premise Konzepten (Perimeter)
- › Nicht nach Standards aufgebaut (Cloud Adoption Framework)
- › Cloud Konzept entspricht nicht den Anforderungen des Unternehmens (Cloud Operating Model)
- › IT will alle Verantwortung bei sich behalten (keine Delegierte Administration, dämpft Innovation)
- › Keine Kostenkontrolle während Entwicklungsphase



Q&A



Bewerten Sie diese Session jetzt in der virtuellen Plattform

- 1 Loggen Sie sich auf der virtuellen Plattform mit **Ihrem persönlichen Link** ein (aus Bestätigungs-Mail MAKE BI)
- 2 Kicken Sie in der Lobby auf der **Session B2** auf den Button „**Teilnehmen**“

- 3 Kicken Sie in der **Session B2** auf der rechten Seite in der Navigation auf „**Umfragen**“
MOBILE: Klicken Sie der Navigation unten zuerst auf „**Interaktion**“, danach auf das **Umfragen-Symbol**

- 4 Beantworten Sie die vier Fragen, indem Sie pro Frage auf das zutreffende Feld klicken und Ihre Auswahl anschliessend mit einem Klick auf den Button „**Abstimmen**“ bestätigen

Die von Ihnen ausgewählten Bewertungen werden weder für die anderen Teilnehmenden noch für die Referenten ersichtlich sein. Das Ergebnis der Auswertung wird nach dem Event in aggregierter und anonymisierter Form an die jeweiligen Referenten kommuniziert werden.



Twitter



LinkedIn



Xing



YouTube



Blog