TECH UPDATE
EXPERTENWISSEN FÜR IHRE IT-STRATEGIE

15 JAHRE braincon

braincon
IT-EXPERTS. NOTHING ELSE.

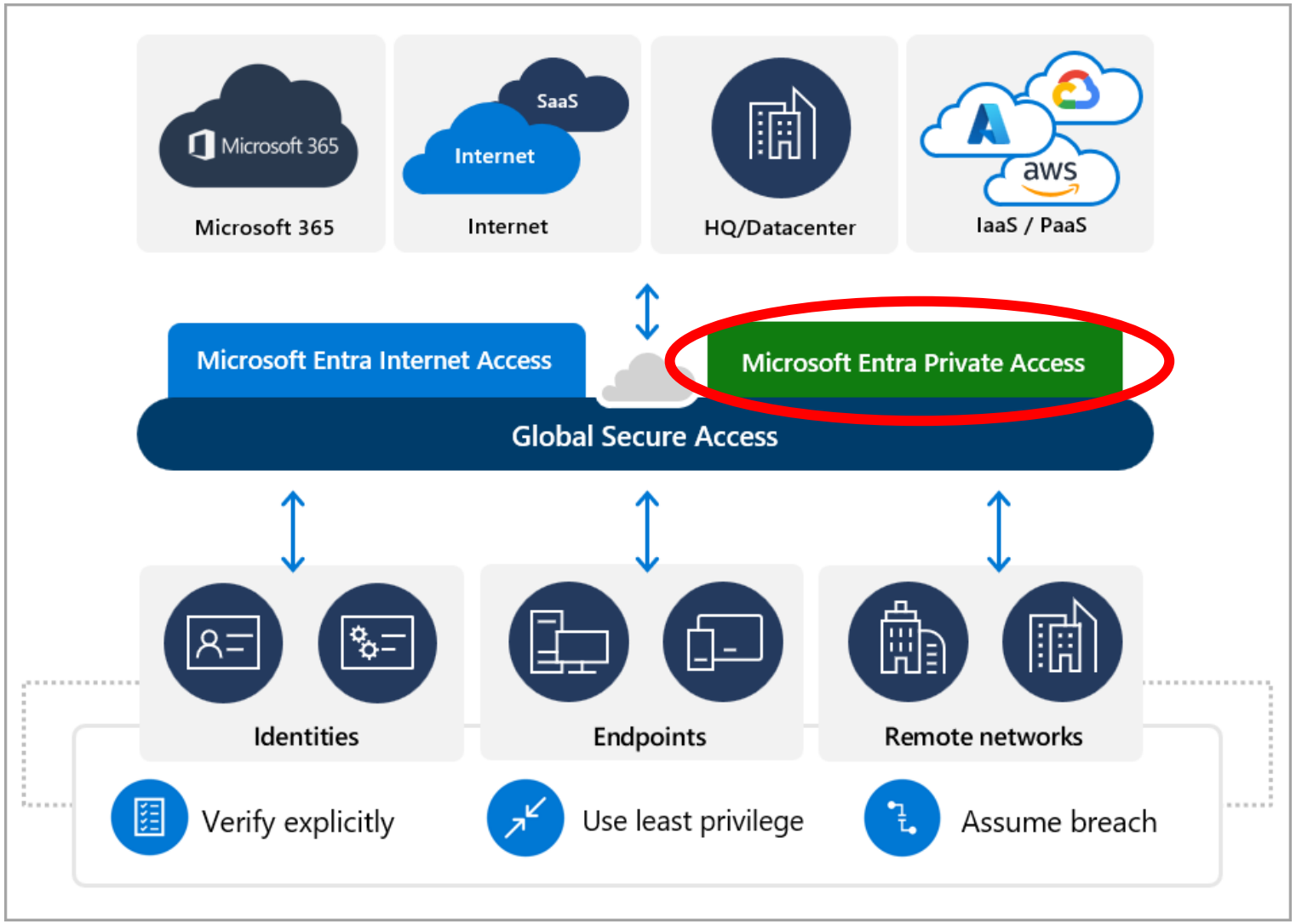
Microsoft Connectivity & Azure Governance

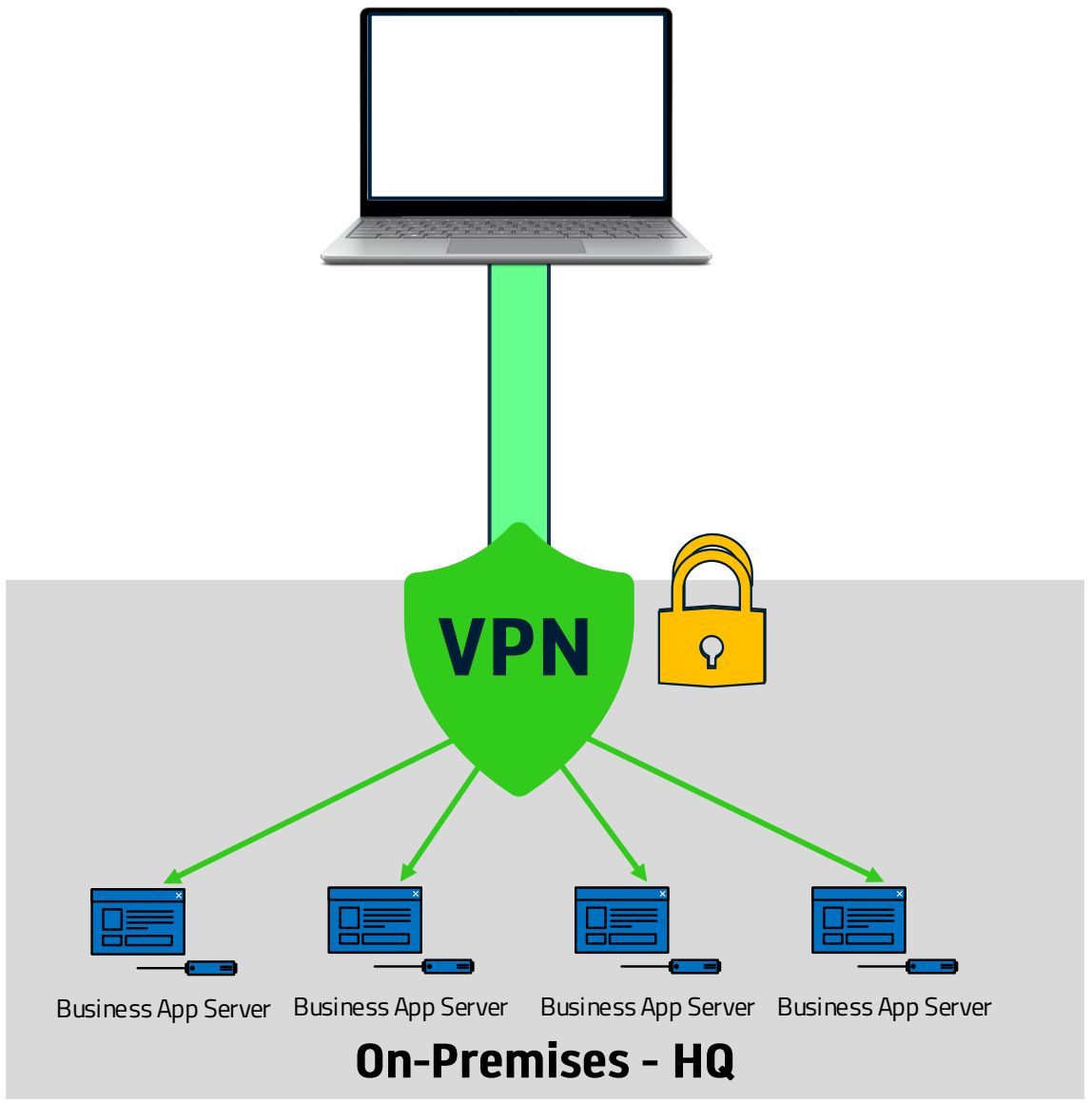
Kevin Pitschner
Teamlead Consulting

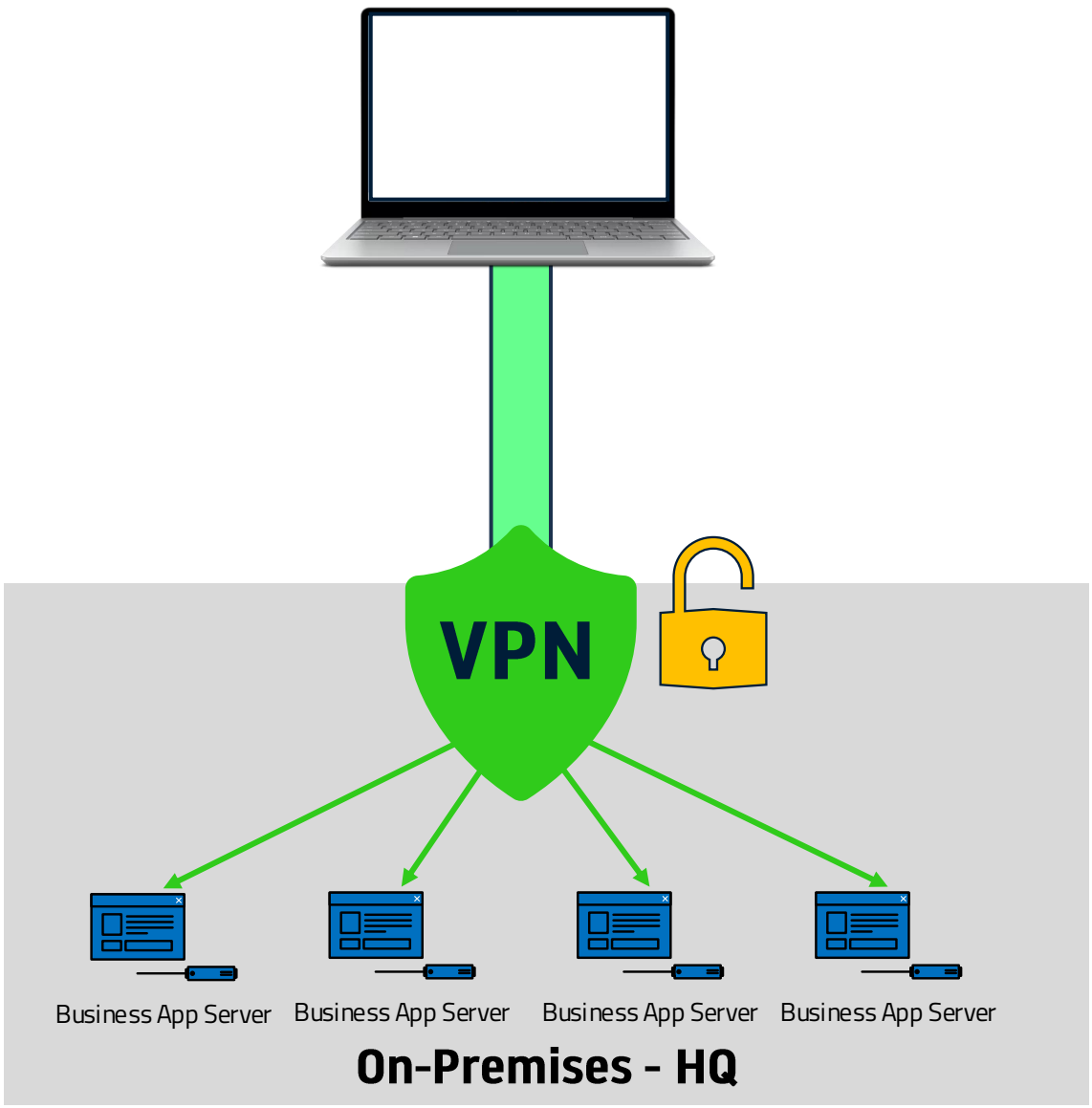
Christian Erwin
Lead Solution Expert

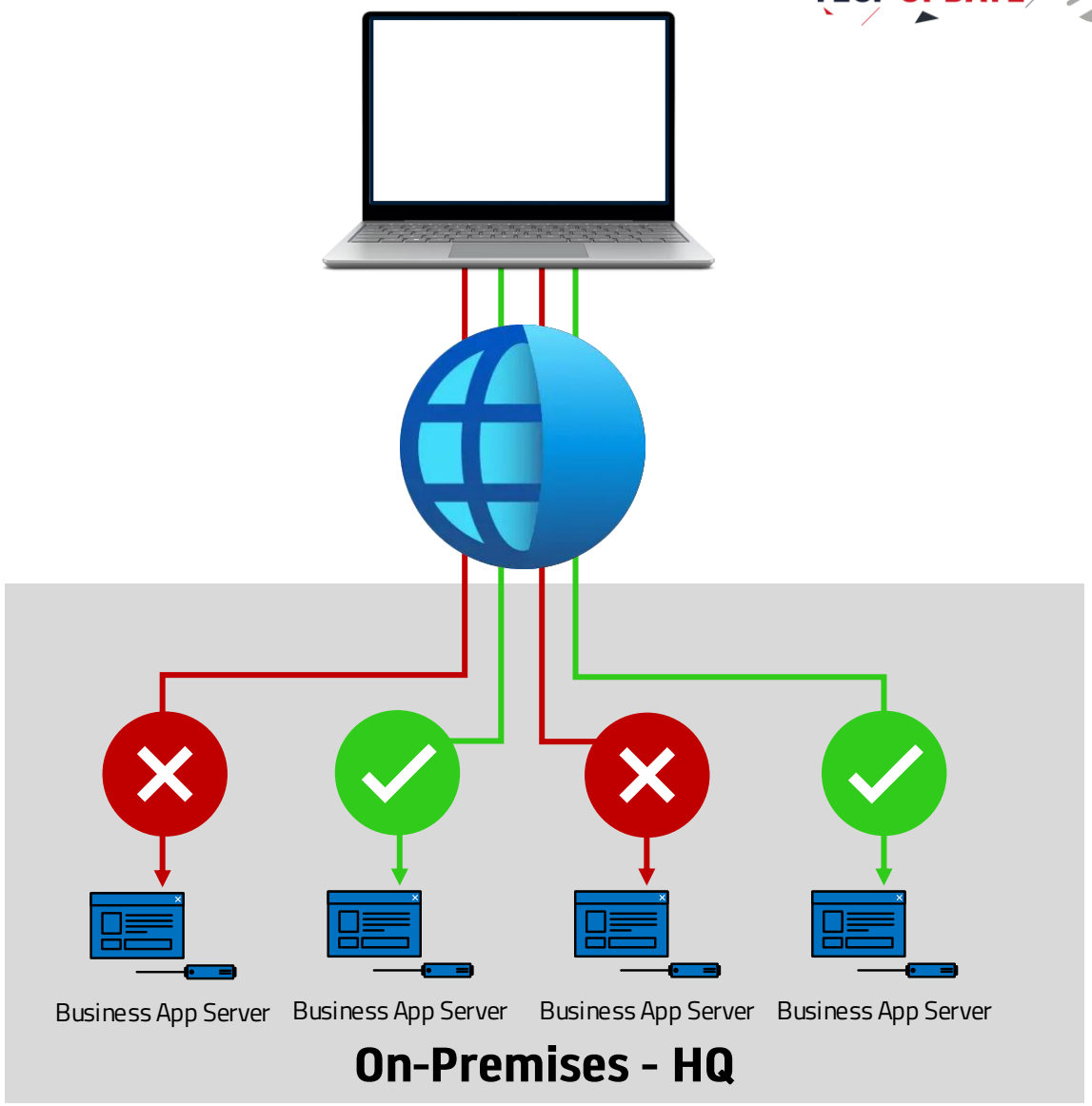
Global Secure Access

Wir erinnern uns...

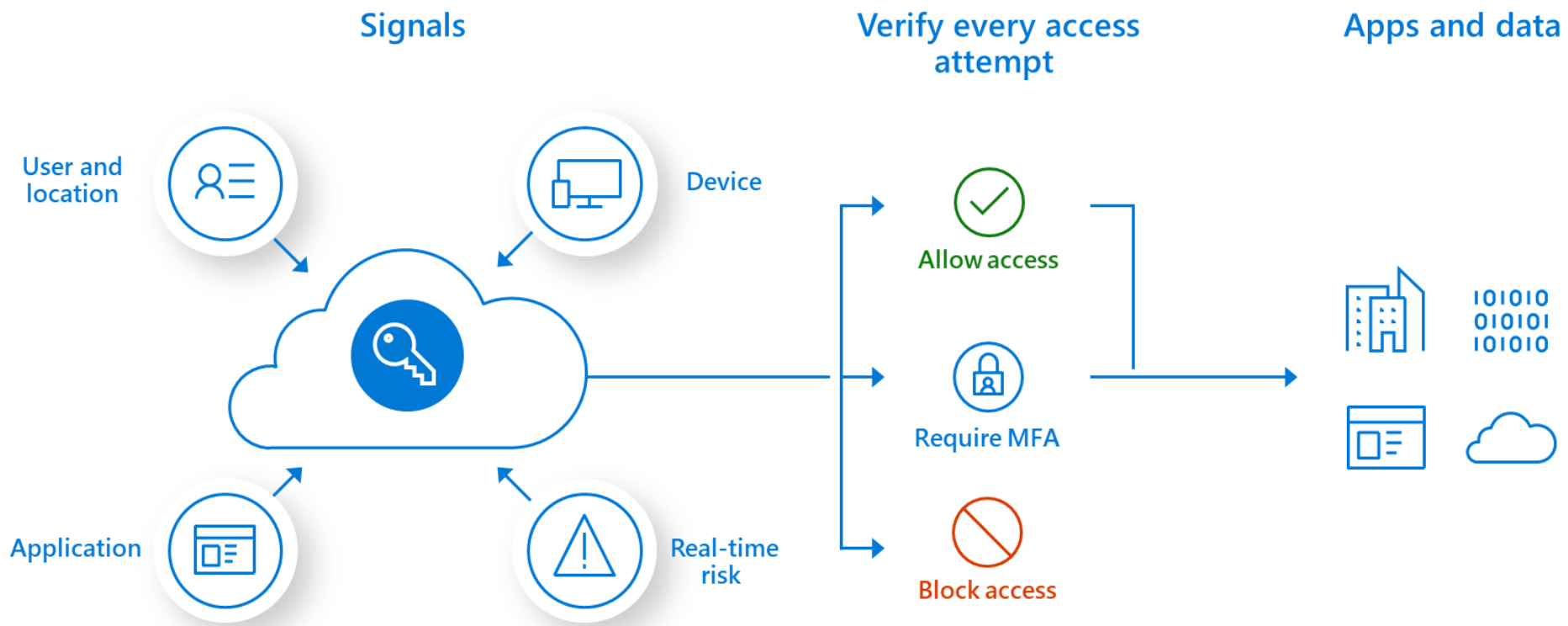


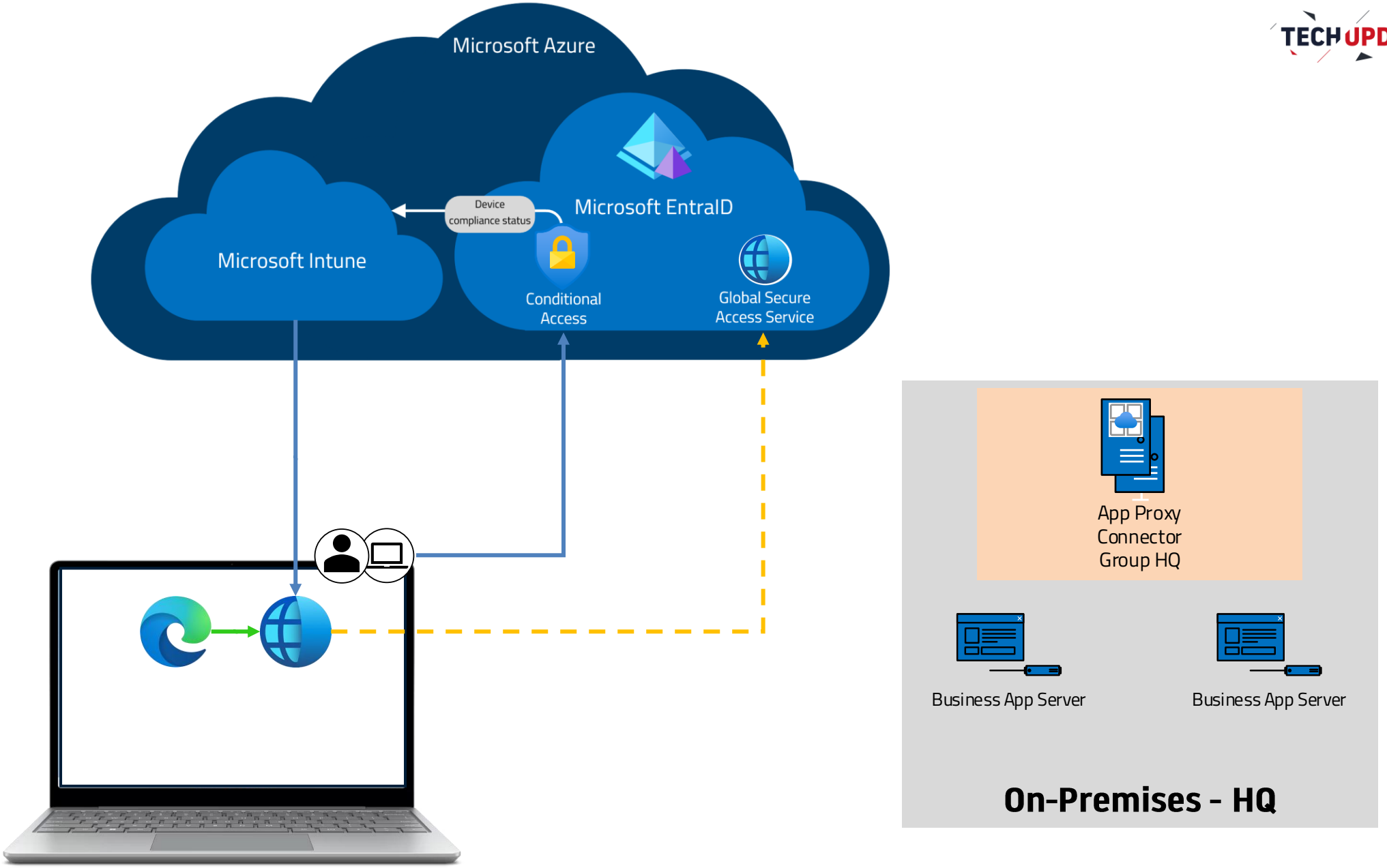

VPN
Business App Server
Business App Server
Business App Server
Business App Server
On-Premises - HQ

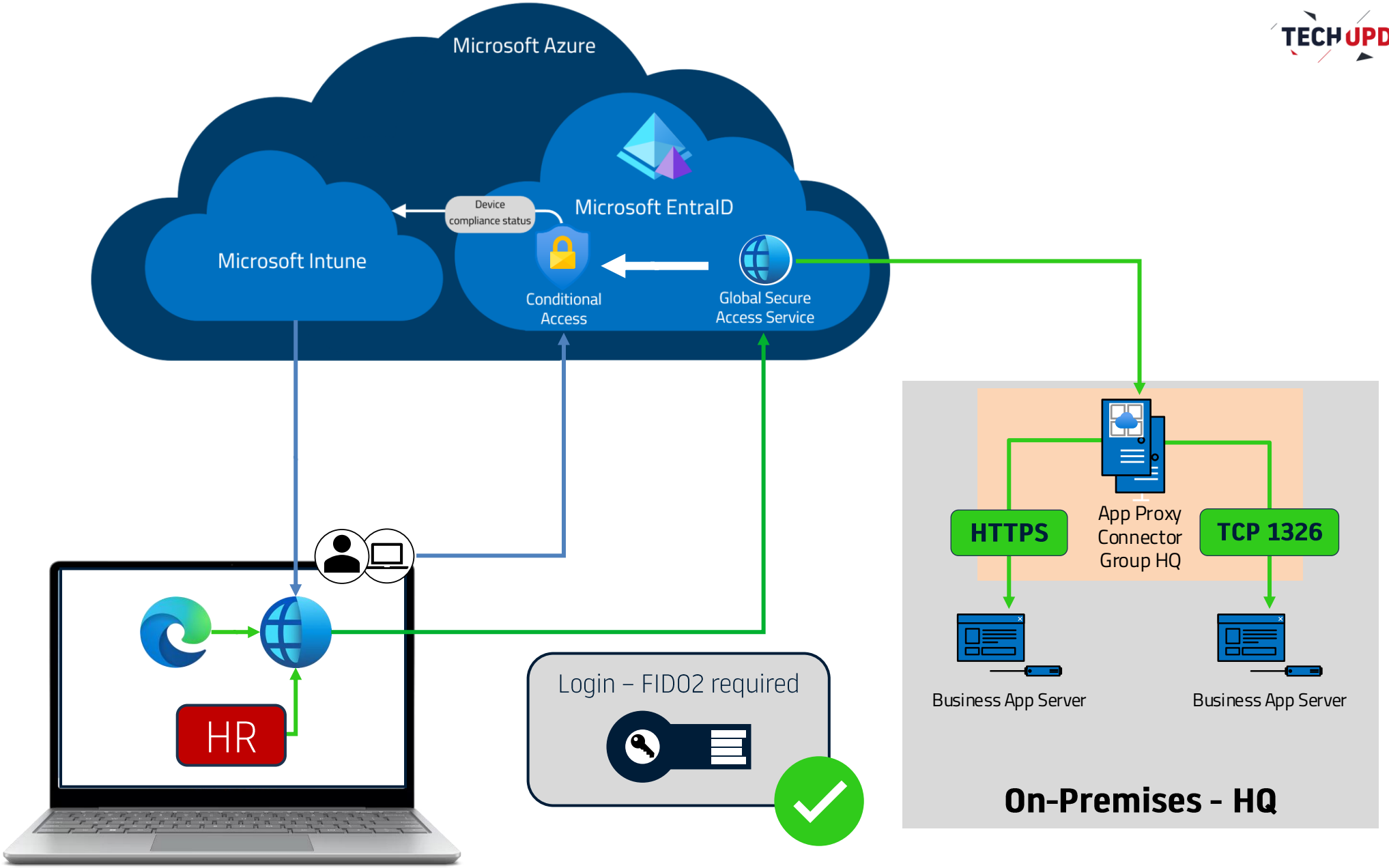

VPN
Business App Server
Business App Server
Business App Server
Business App Server
On-Premises - HQ

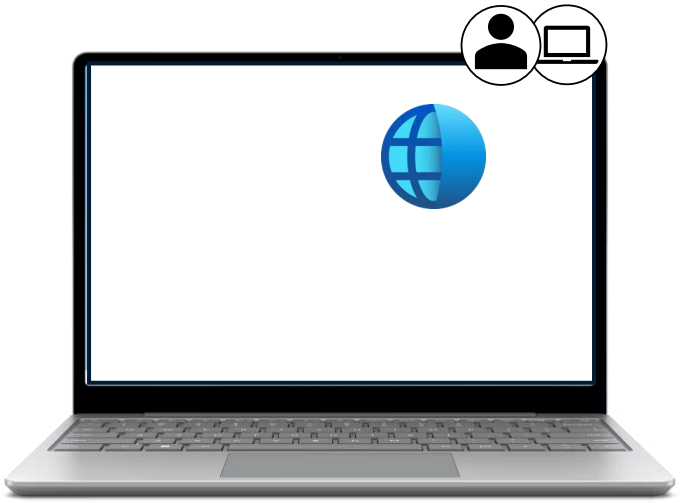

Business App Server
Business App Server
Business App Server
Business App Server
On-Premises - HQ

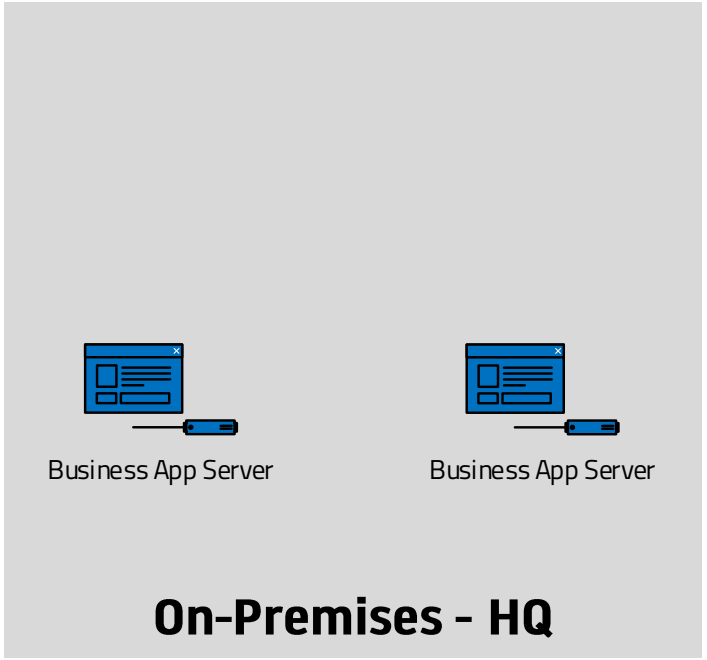
Zero-Trust-Strategie




Microsoft Azure
Microsoft Intune
Device compliance status
Microsoft EntraID
Conditional Access
Global Secure Access Service
App Proxy Connector Group HQ
Business App Server
Business App Server
On-Premises - HQ


Microsoft Azure
Microsoft Intune
Device compliance status
Microsoft EntraID
Conditional Access
Global Secure Access Service
HR
Login – FIDO2 required
HTTPS
App Proxy Connector Group HQ
TCP 1326
Business App Server
Business App Server
On-Premises - HQ

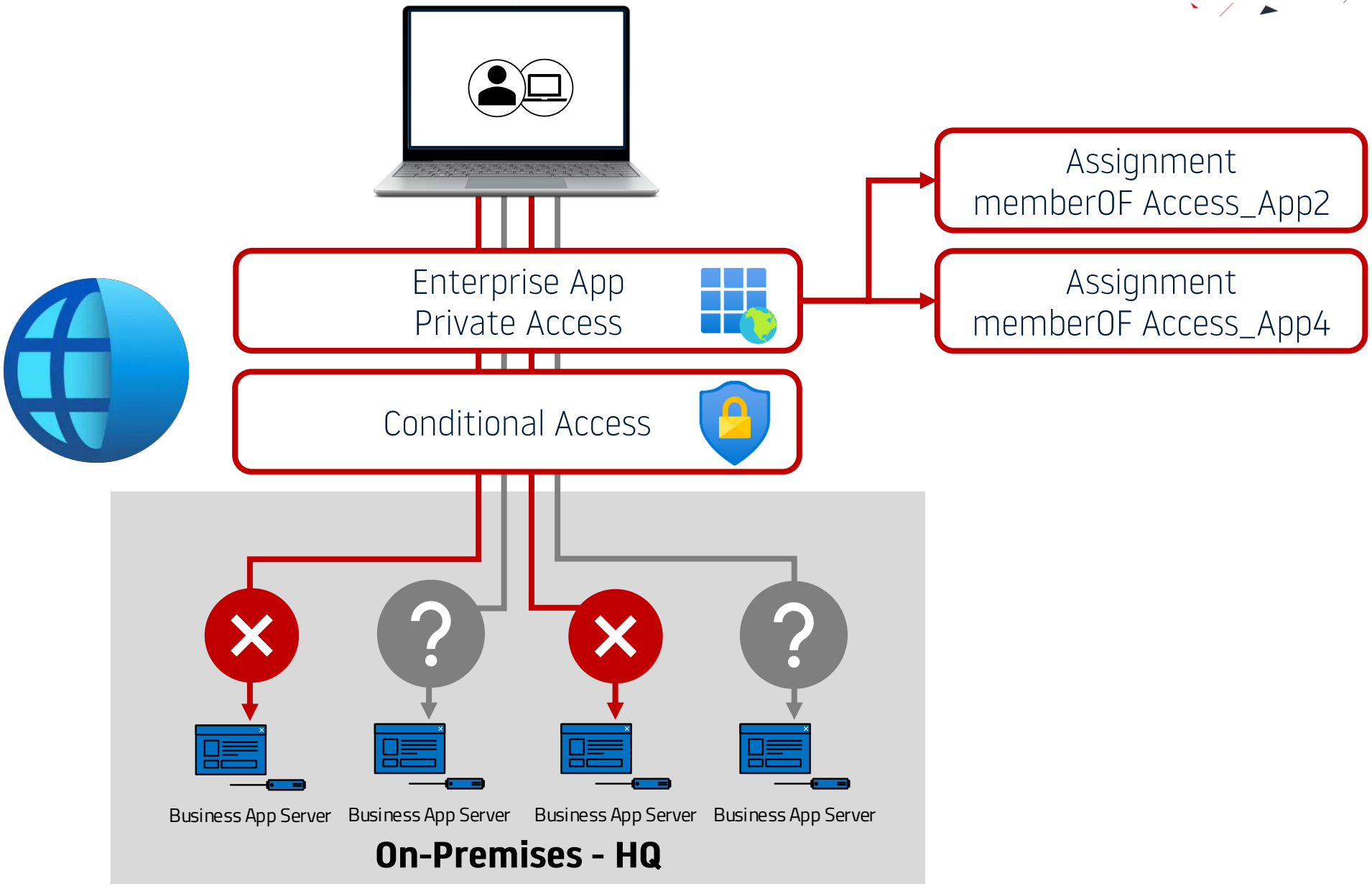


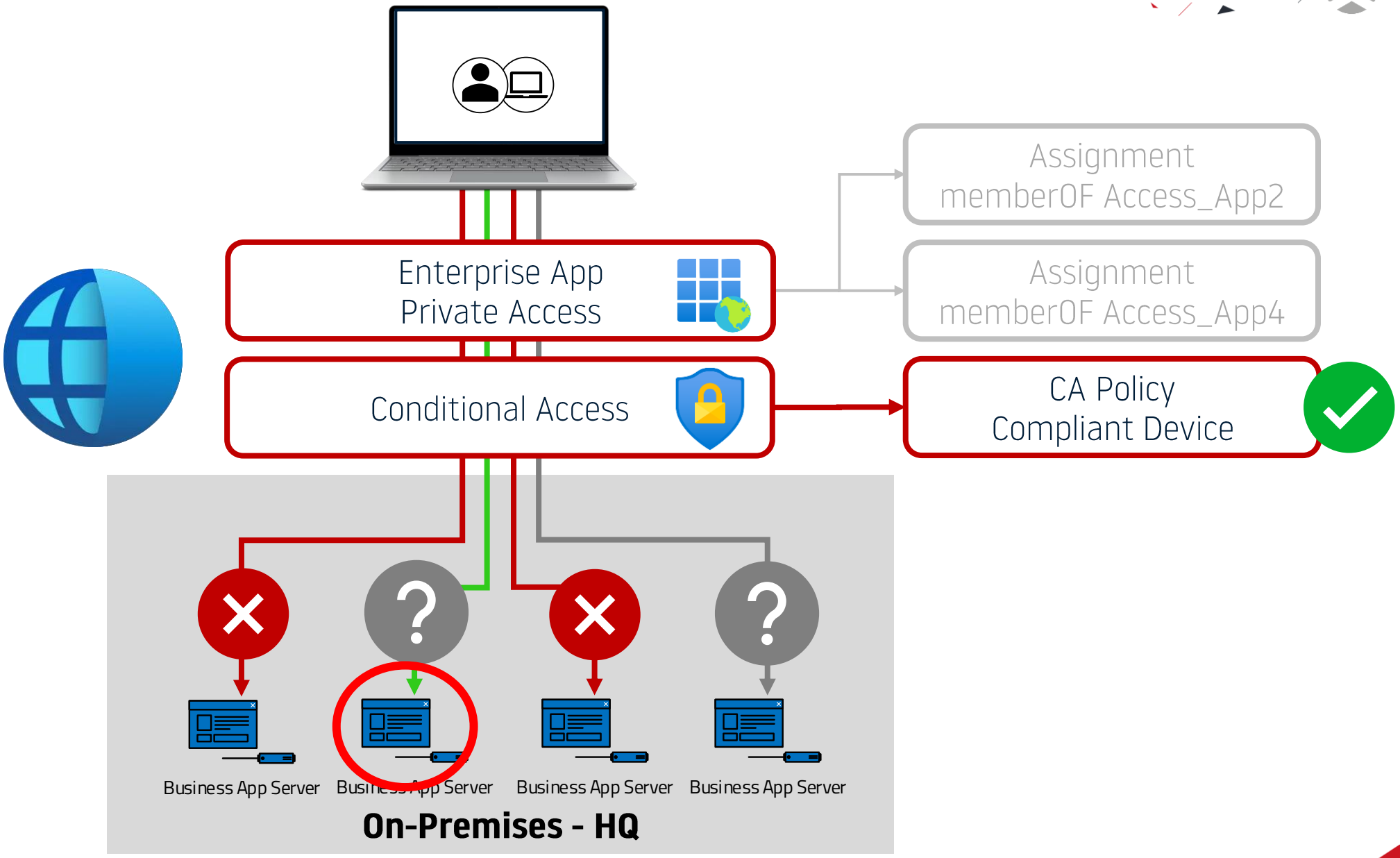

Business App Server
Business App Server
On-Premises - HQ

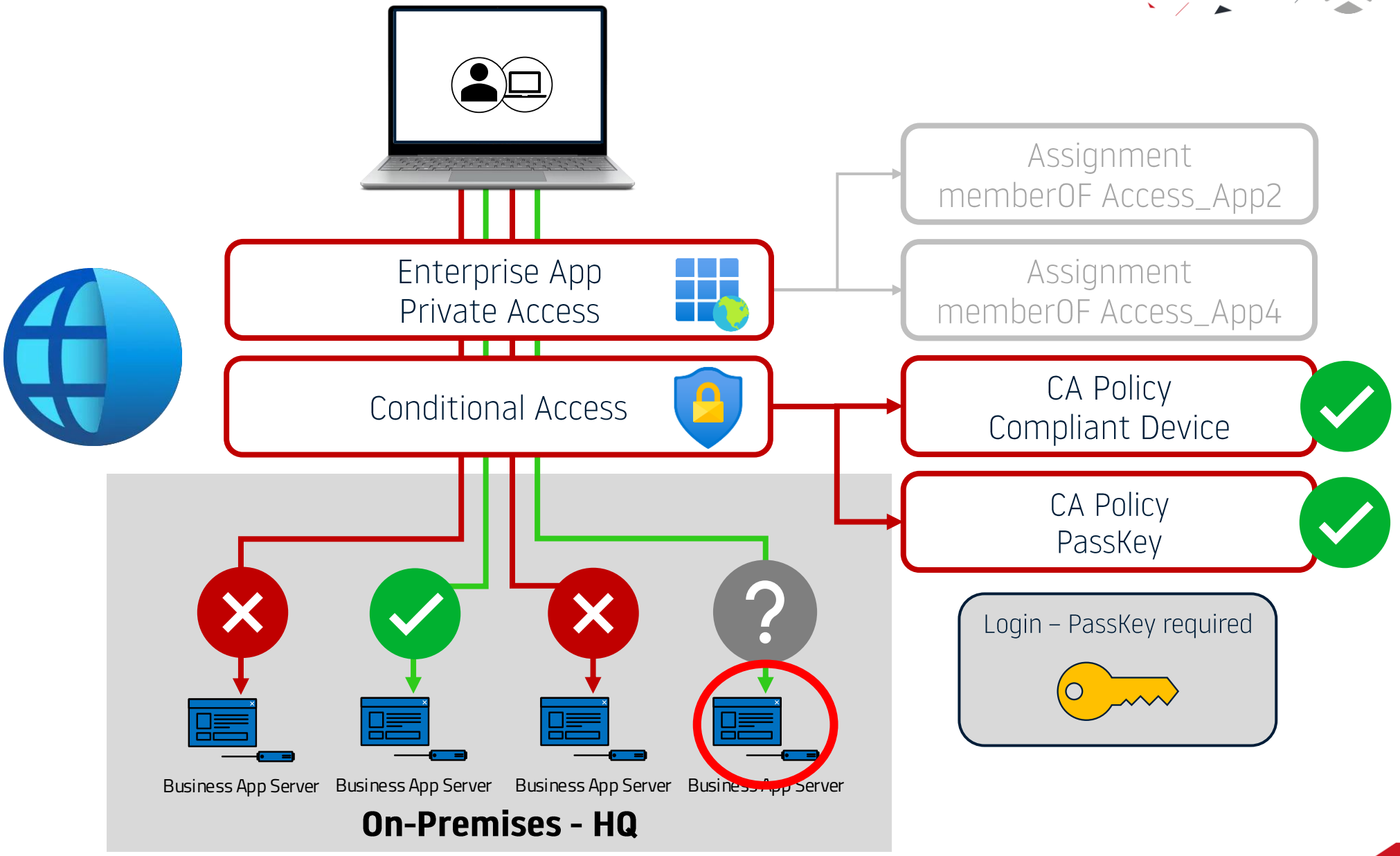
Enterprise App
Private Access

Conditional Access

On-Premises - HQ


Assignment
memberOF Access_App2
Assignment
memberOF Access_App4
Enterprise App
Private Access
Conditional Access
Business App Server
Business App Server
Business App Server
Business App Server
On-Premises - HQ

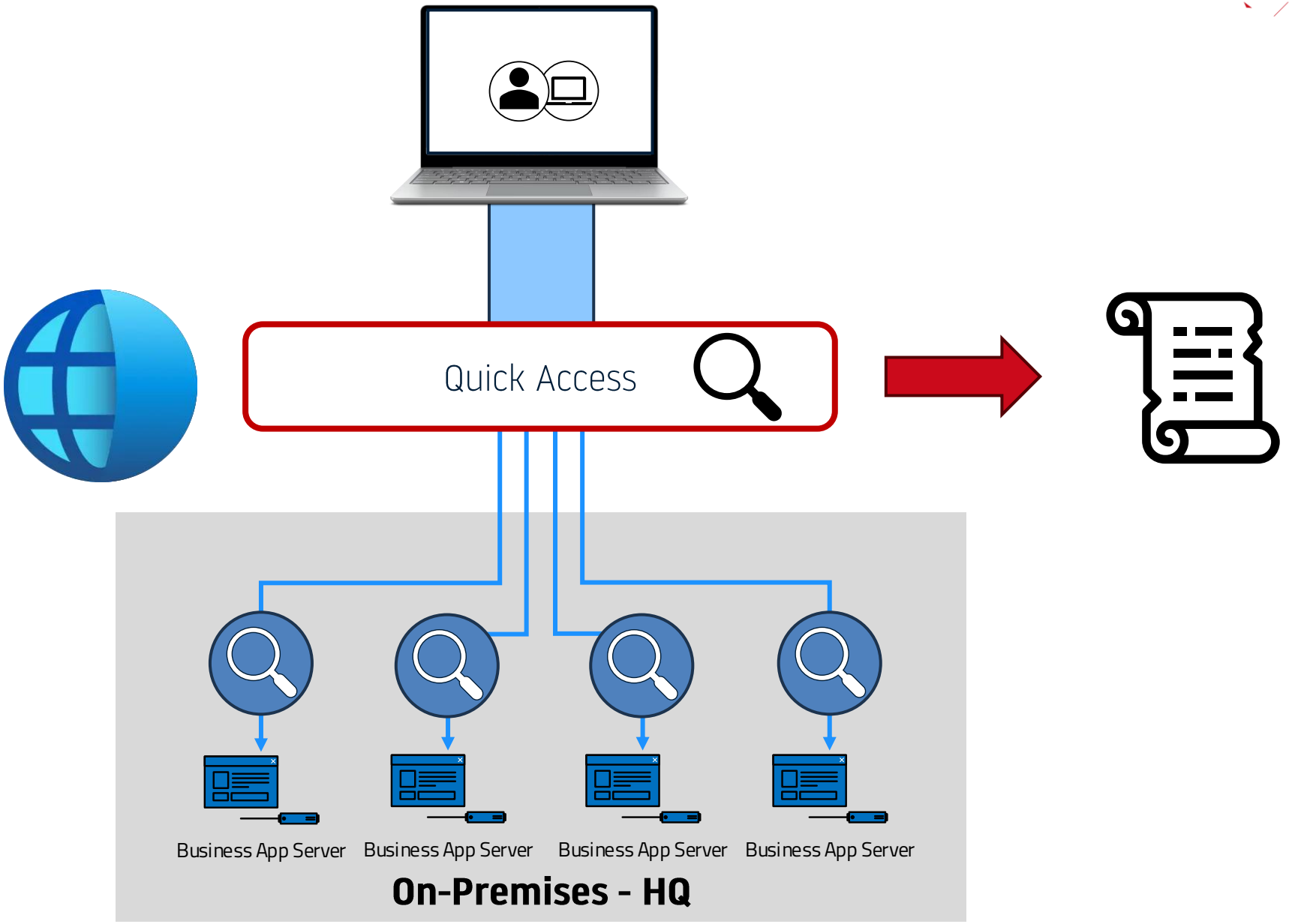

Assignment
memberOF Access_App2
Assignment
memberOF Access_App4
Enterprise App
Private Access
Conditional Access
CA Policy
Compliant Device
Business App Server
Business App Server
Business App Server
Business App Server
On-Premises - HQ


Assignment
memberOF Access_App2
Assignment
memberOF Access_App4
Enterprise App
Private Access
Conditional Access
CA Policy
Compliant Device
CA Policy
PassKey
Login – PassKey required
Business App Server
Business App Server
Business App Server
On-Premises - HQ

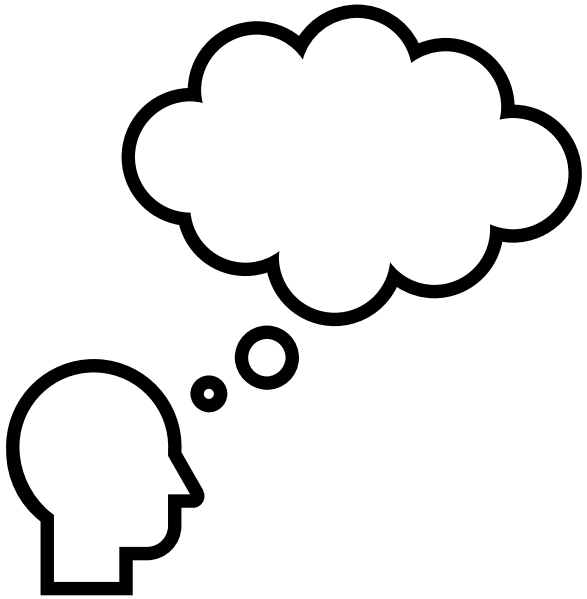
Enterprise App
Private Access

Conditional Access

On-Premises - HQ


Quick Access
Business App Server
Business App Server
Business App Server
Business App Server
On-Premises - HQ

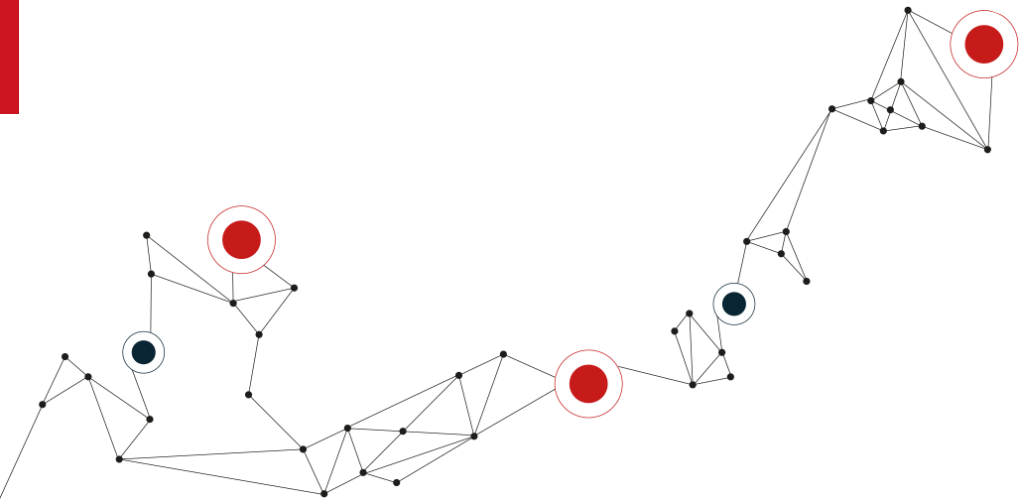
Gedankenspiel - Vision



Was wäre wenn?

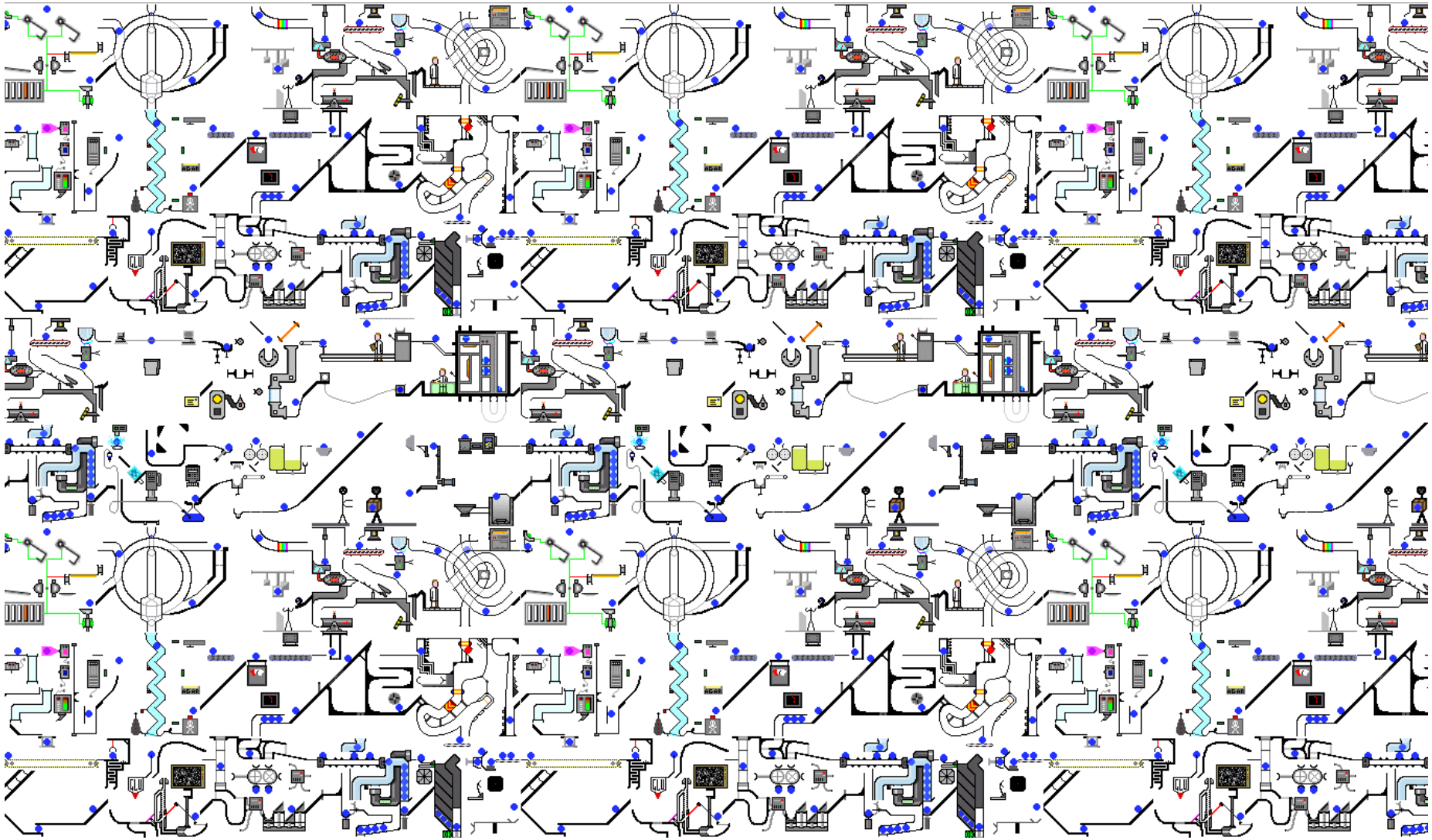
- Ihr Clientnetzwerk benötigt nur Internet…
- keine Zugriffe von der erstbesten Netzwerkdose…
- ein zentrales Regelwerk, unabhängig vom Standort des Clients…
- auch onPrem Netzwerkzugriffe per Gruppe geregelt…
- Strong Auth ins Server-Netzwerk für die Administration…
- nur compliant Clients erhalten Zugriff…
- Außenstandorte ohne Site-2-Site?


Global Secure Access

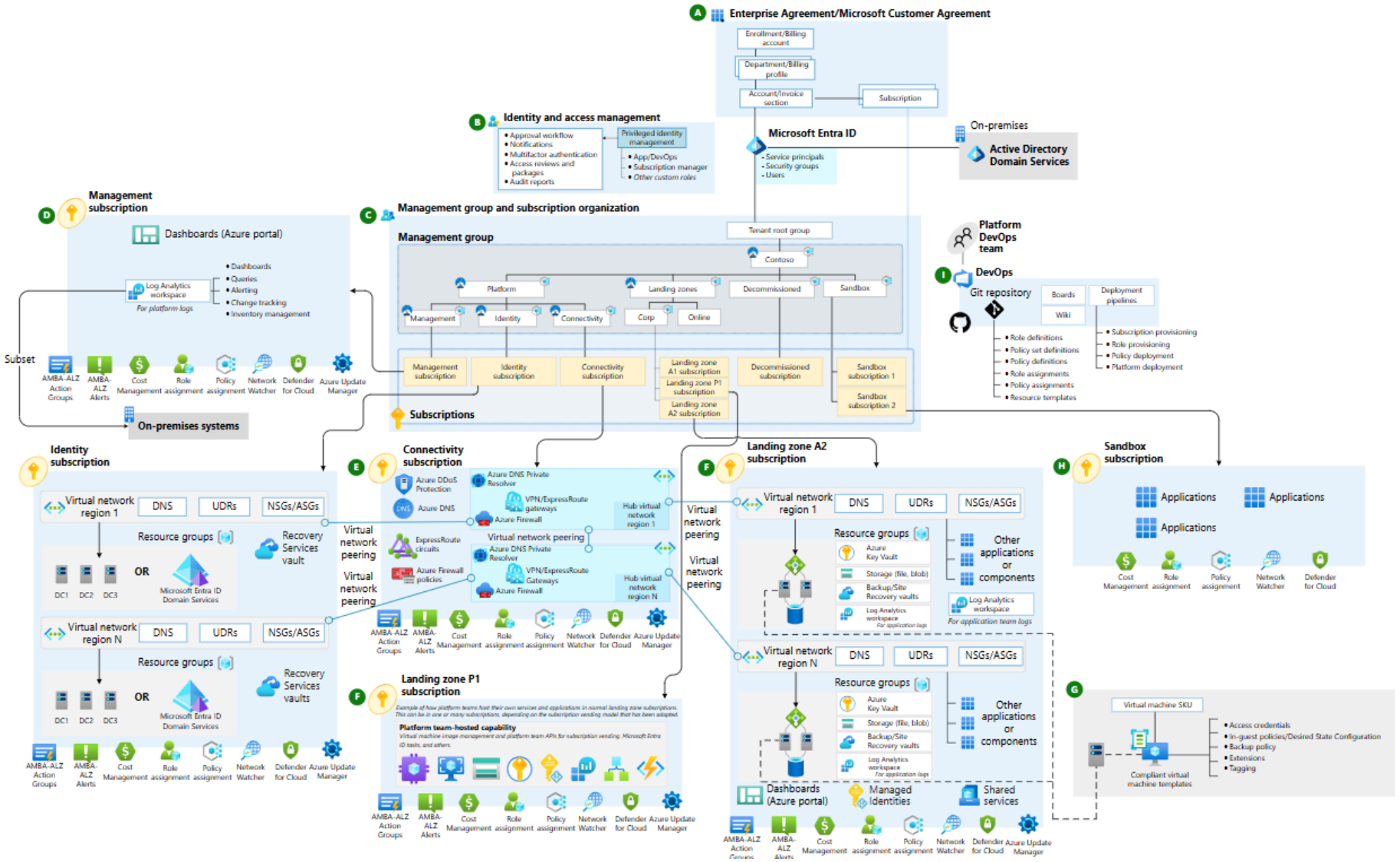


Azure Governance & Security

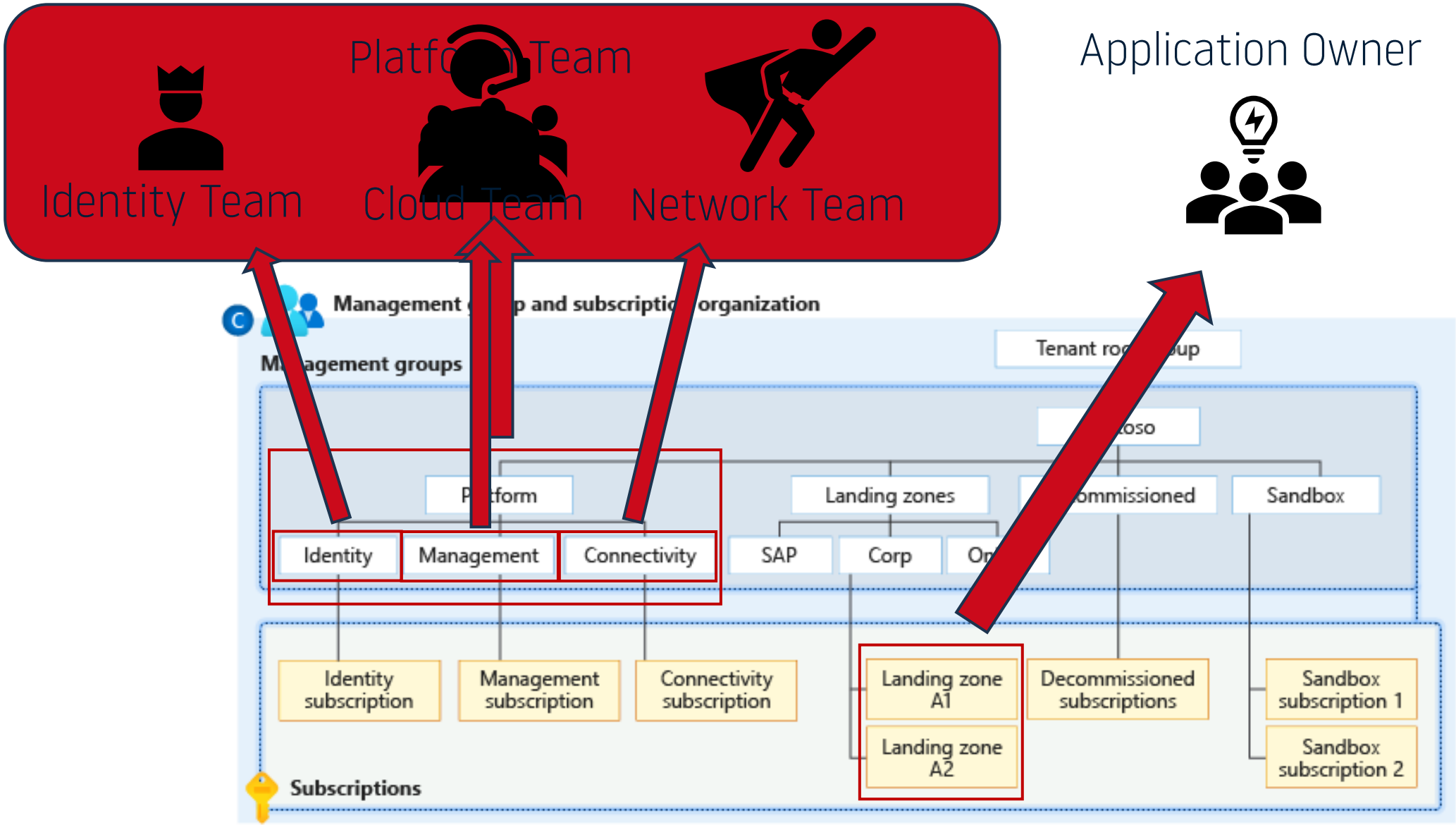
Wir erinnern uns...



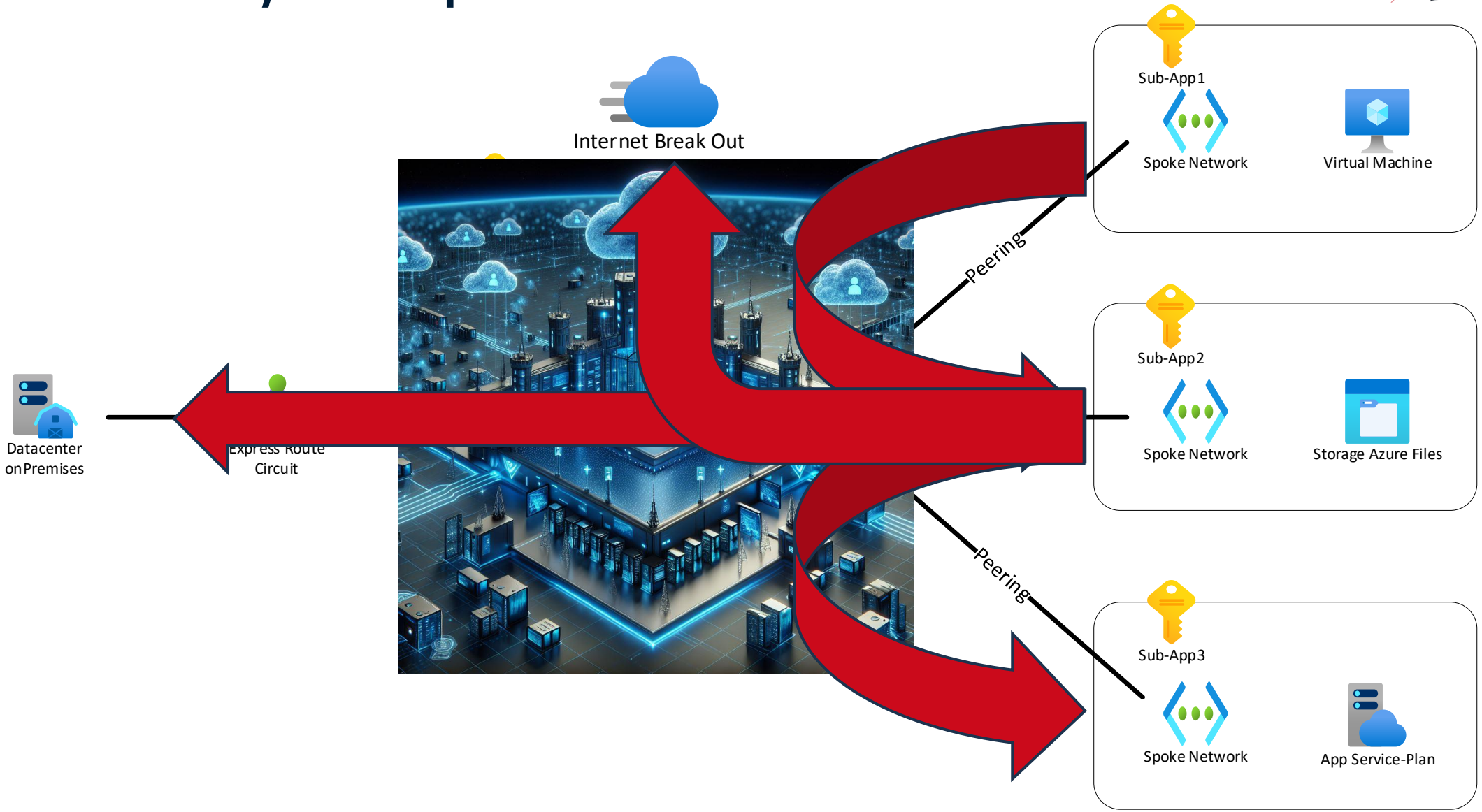
Microsofts Antwort: Azure Landing Zone Enterprise Scale



DIE eigentliche Azure Landing Zone



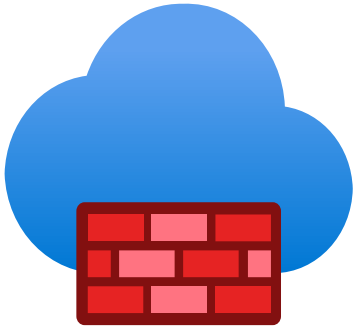
Die Connectivity Subscription



Firewall?

Azure Firewall

- Microsoft Managed Service
- Auto Scaling bis 100GBit
- HA integriert
- Einfacher Aufbau

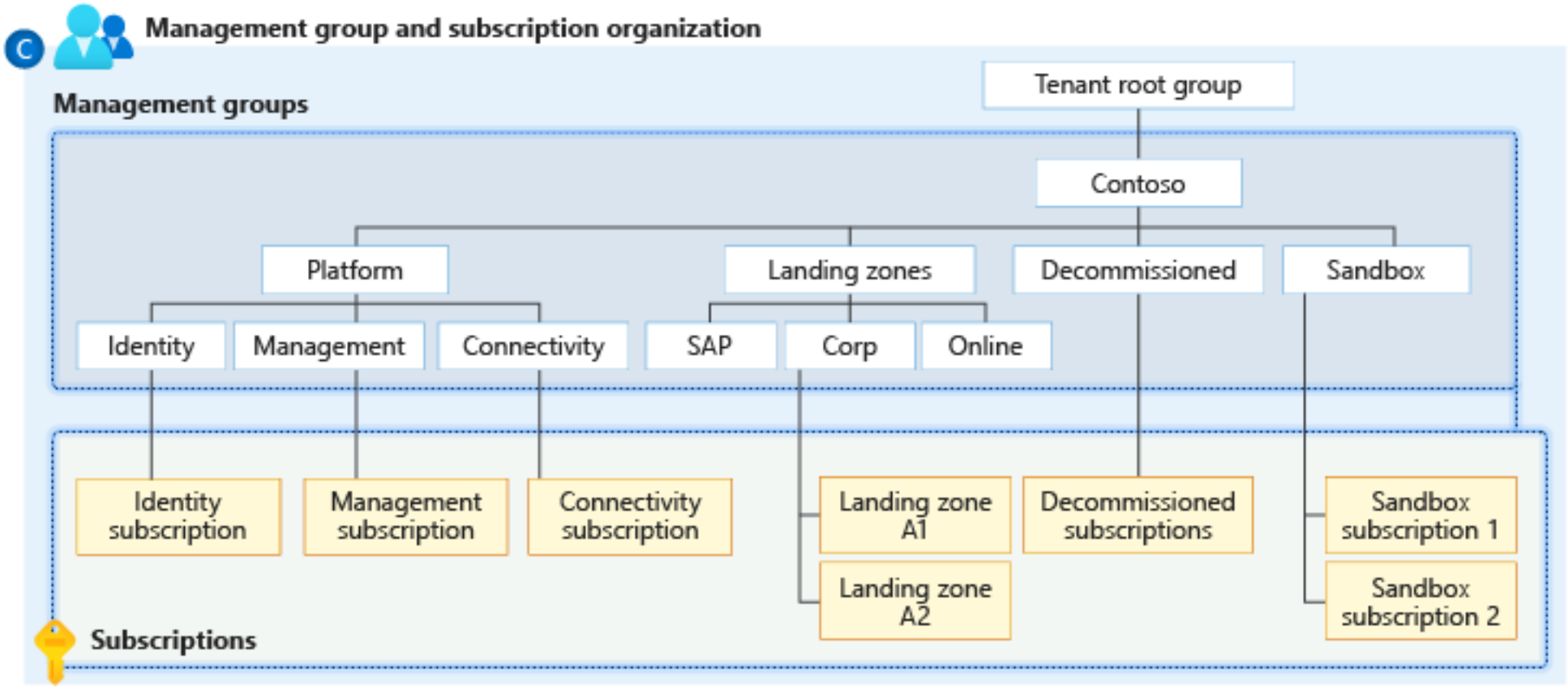


Ihre bevorzugte Firewall

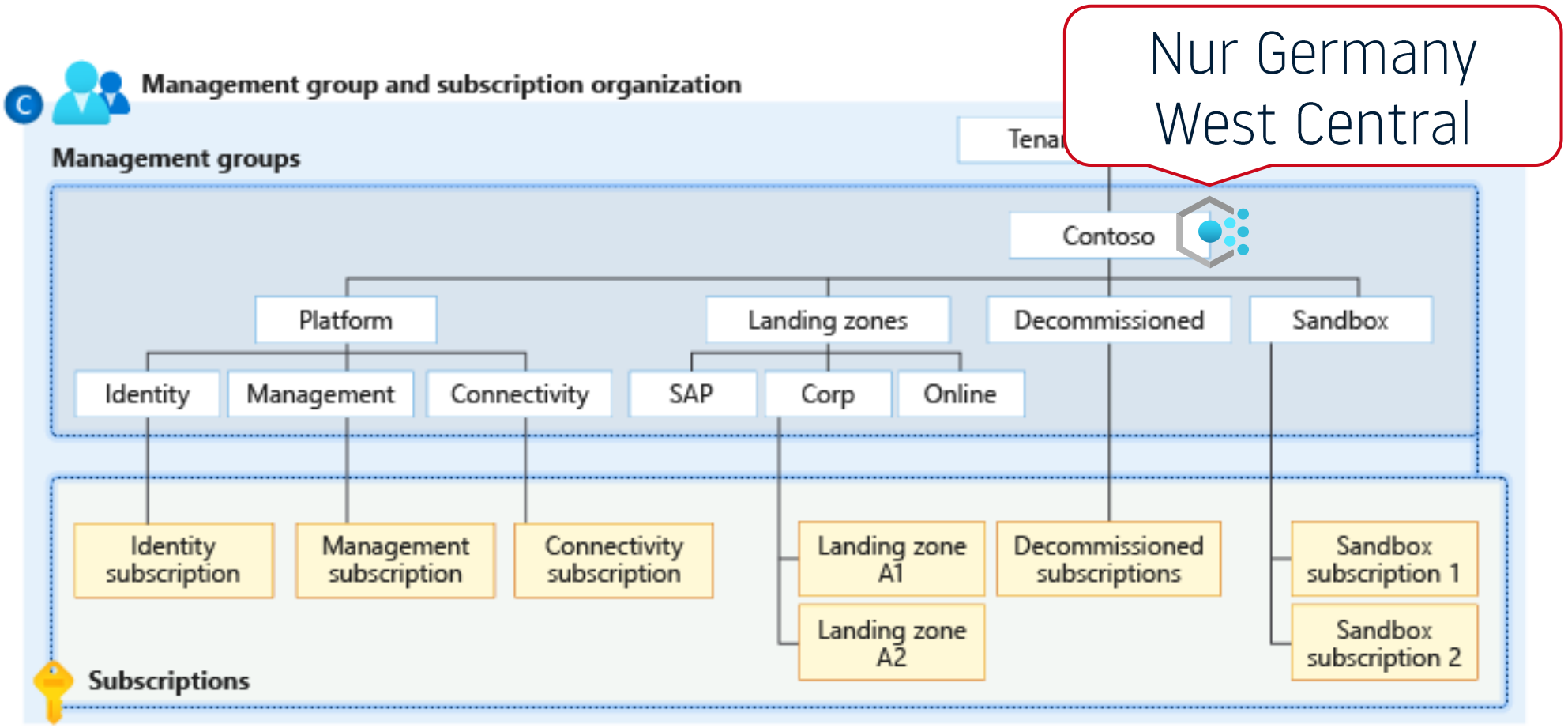
- Gängige Hersteller bieten Appliances
- Bekannte UI
- Integration in vorhandenes Mangement
- Komplexerer Aufbau

Lassen Sie uns gemeinsam evaluieren und entscheiden

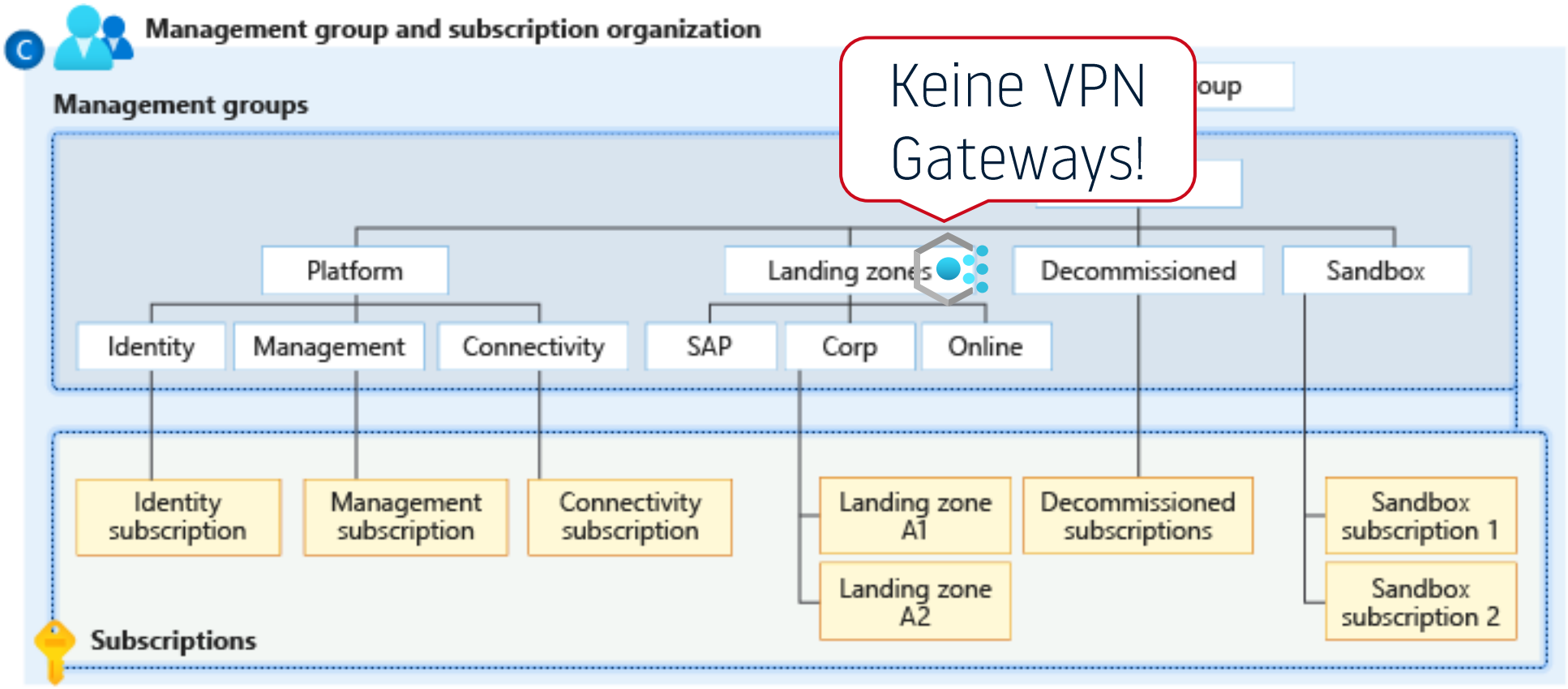
Azure - Governance



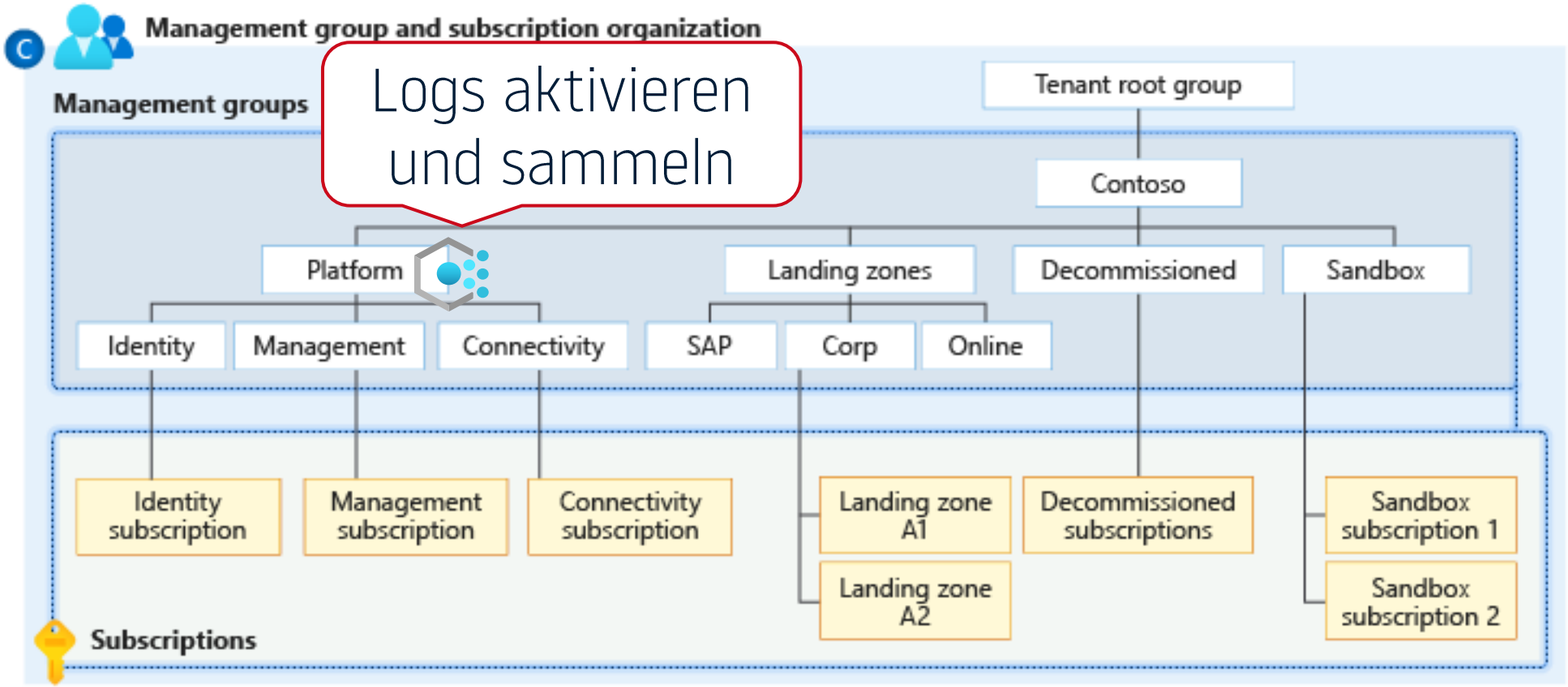
Azure - Governance



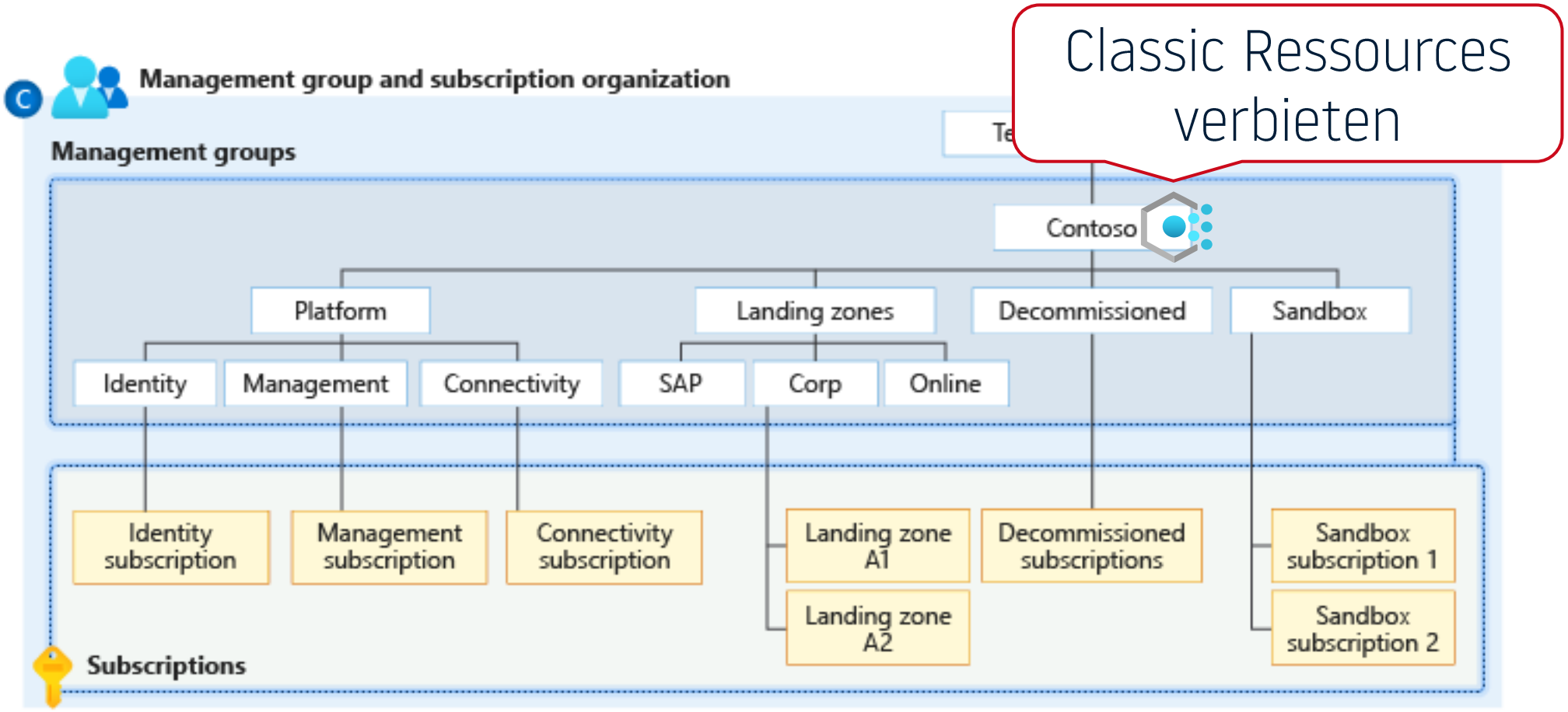
Azure - Governance



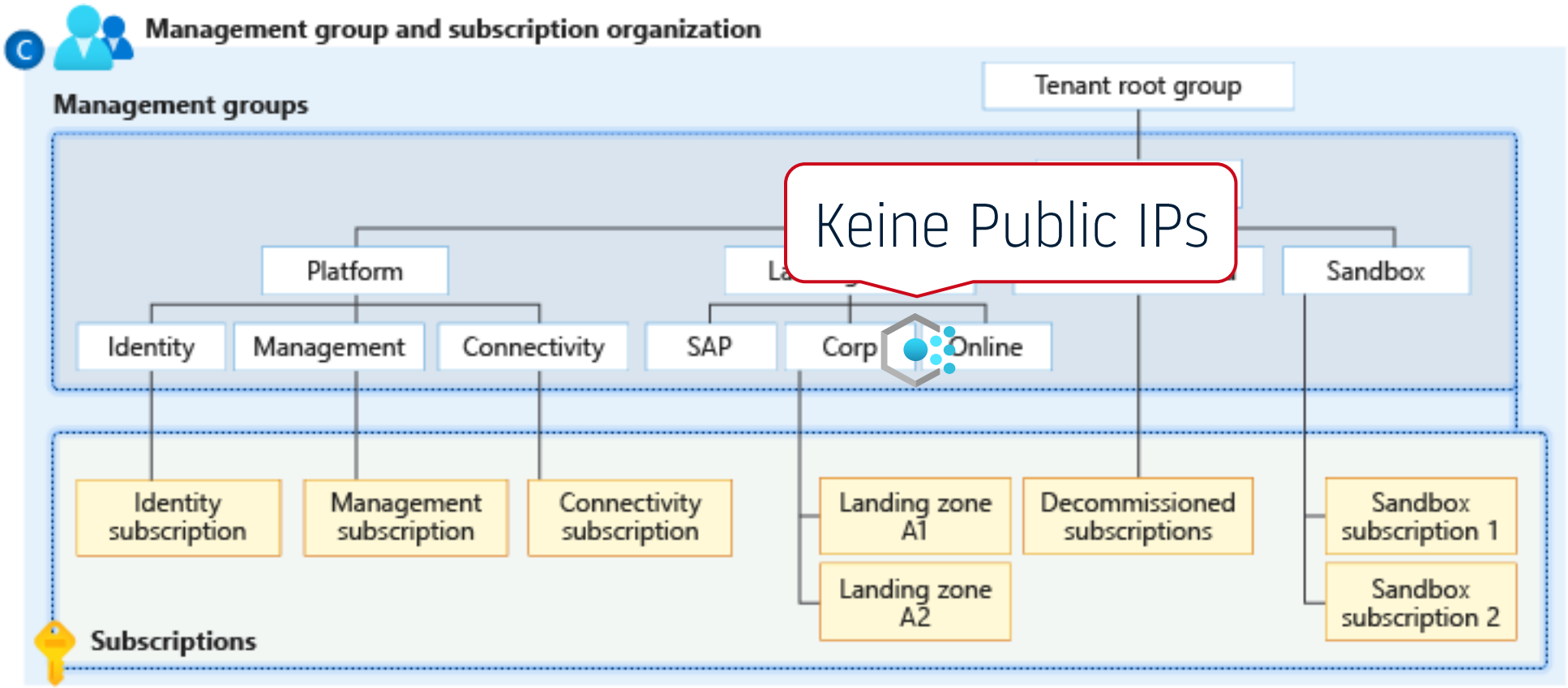
Azure - Governance



Azure - Governance



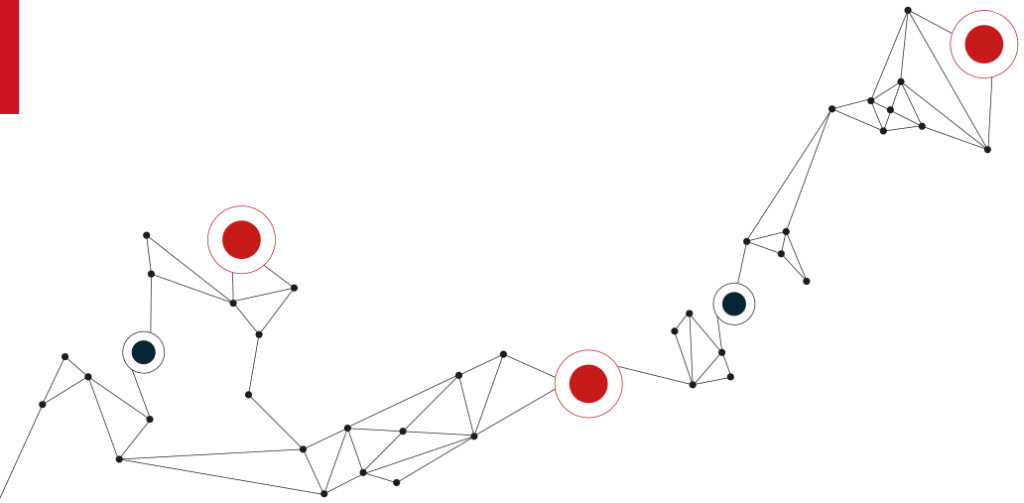
Azure - Governance



How to Azure Landing Zone?

Wir unterstützen Sie gerne!

- Konzept Erstellung der globalen „Leitplanken“
- Standarisiertes Deployment
  - Terraform
  - Azure DevOps
- Regelmäßiges Update auf aktuellen Definitionsstand



Surprise!?

Microsoft Azure

Default outbound access for VMs in Azure will be retired—transition existing VMs to a new method of internet access

You're receiving this notification because you are associated with one or more Azure

In Azure, VMs that are created in a virtual network without a defined explicit outbound method are assigned a default public IP address that enables internet connectivity. **On 30 September 2025, default outbound access connectivity for VMs in Azure will be retired.**

improve reliability.

Recommended action

To ensure more reliable internet connections, transition any existing VMs that rely on default outbound access to use an explicit method of connectivity. Please see here for more information.

If you deploy VMs on Azure Cloud Services (extended support), this retirement won't affect you and you don't need to take any action.

In order to determine which virtual machines for your subscription are in scope, please utilize Azure Advisor and look for the "Add explicit outbound method to disable default outbound" recommendation in the "Operational excellence" section to show the specific virtual machine NICs using default outbound.

Default outbound access for VMs in Azure will be retired— transition to a new method of internet access

RETIREMENT
September 2025

Conversational language understanding

On 30 September 2025, default outbound access connectivity for virtual machines in Azure will be retired. After this date, all new VMs that require internet access will need to use explicit outbound connectivity methods such as Azure NAT Gateway, Azure Load Balancer outbound rules, or a directly

In Azure, VMs that are created in a virtual network without a defined explicit outbound method are assigned a default public IP address that enables internet connectivity. Your existing VMs that use default outbound access will continue to work after this retirement, however, **we strongly recommend transitioning to an explicit outbound method so that:**

- Your VMs use traceable IP resources that you own.

If you deploy VMs on Azure Cloud Services (extended support), this retirement won't affect you and you don't need to take any action.

Recommended action

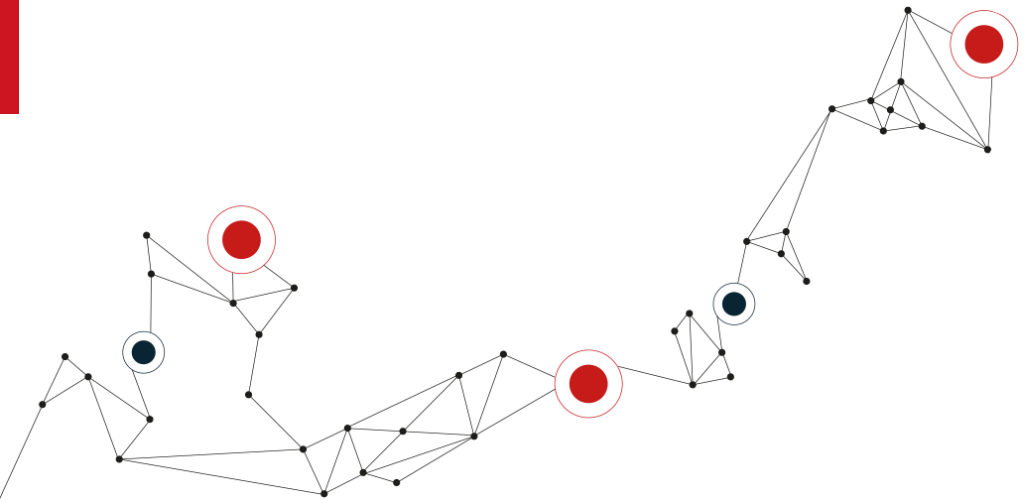
To ensure more controllable and traceable internet connections, **transition any existing VMs that rely on default outbound access to use an explicit method of connectivity**.

Help and support

If you have questions, get answers from community experts in Microsoft Q&A. If you have a support plan and you need technical help, create a support request.

Was heißt das für Sie?

- Ab 01. Oktober muss der Internet Break Out geklärt sein
- Nur alle neuen VMs benötigen diesen
- VORSICHT!
  - Auch (Re)Provisioning einer Remoting VM ist eine neue VM!



Nicht noch mehr Surprises?

Assessment Azure Infrastructure Security


braincon

Assessment Azure Infrastructure Security

Überprüfung der Zugriffssicherheit Ihrer Azure Infrastructure Komponenten

Die Herausforderung

Das Prinzip der geteilten Verantwortung ist eine grundlegende Festlegung in den Sicherheitsverpflichtungen für das Lösungsmodell Cloud. Dabei verantwortet der Anbieter primär die **„Sicherheit der Cloud"**.

Sie als Kunde sind für die **„Sicherheit in der Cloud"** verantwortlich. Dies inkludiert alle von Ihnen erstellten Elemente wie Daten, Endpunkte, Konten und die entsprechenden Zugriffsverwaltungen.

In der Konsequenz entstehen wichtige Aufgaben, wie die Identifizierung externer Angriffspunkte, die Analyse von möglichen Angriffspfaden sowie das Korrelieren und Analysieren der Daten in der gesamten Infrastruktur. Ergänzend zu unseren Leistungen für die Assessments von Microsoft Entra ID Connect-Cloudsynchronisierung und der Basis eines Microsoft Entra Tenant Assessments liegt der Fokus dieses Angebots auf einer Sicherheitsbewertung von Komponenten Ihrer Azure Infrastruktur.

Hervorzuheben sind folgende besonders kritische Erkennungen:

1. There are more than 3 owners designated on this Azure Subscription
2. Azure Storage Accounts allow public network access
3. Azure App Services Web App are not restricting access from the internet
4. Azure SQL server allows network access from internet

Übersicht 1: Kritische Erkennungen

Die Auflistung in Übersicht 1 bezieht sich auf Erkennungen mit der verhältnismäßig höchsten Kritikalität und konnte ggfs. mehrfach identifiziert werden. Details dokumentieren wir in den folgenden Abschnitten dieses Dokumentes.

Rule	Anzahl von Rule
Azure App Services are not enforcing HTTPS	2
Azure App Services does not have authentication enabled	8
Azure App Services does not have Client Cert Enabled	8
Azure App Services Functions are not restricting access from the internet.	14
Azure App Services is not using the latest .Net Framework version.	22
Azure App Services is not using the latest HTTP version	22
Azure App Services is not using the latest Python version	2
Azure App Services Web App are not restricting access from the internet.	22
Azure Functions does not have a TLS/SSL certificate associated	16
Azure Key Vault is not configured to be recoverable	2
Azure Resource Group does not have AAD Groups assigned for RBAC	8
Azure SQL databases do not have transparent data encryption enabled	1
Azure SQL server allows network access from internet	2
Azure SQL Server does not have AAD Admin configured	2
Azure SQL Server does not have Auditing enabled	1
Azure storage account is not using TLS 1.2 version	4
Azure Storage Accounts allow public network access	30
Azure Storage Accounts do not have infrastructure encryption enabled	33
Azure Storage Accounts do not have Trusted Microsoft Services access enabled	3
Azure Storage Accounts is not using Private Endpoint	3
Azure Subnet does not have an NSG associated	2
Azure Web App does not have a TLS/SSL certificate associated	24
SQL Server is missing BYOK encryption	2
There are more than 3 owners designated on this Azure Subscription	1

Übersicht 4: Auflistung Issues und Häufigkeit

Assessment Azure Infrastructure Security

braincon
IT-EXPERTS. NOTHING ELSE.

Jetzt auch für Entra ID!

Entra ID Healthcheck

6.7 Block Legacy Authentication in Entra ID Conditional Access Policies

Control Name	Detections Count
Block Legacy Authentication in Entra ID Conditional Access Policies	1

Beschreibung: Diese Regel stellt sicher, dass mindestens eine bedingte Zugriffsrichtlinie innerhalb von Entra ID konfiguriert ist, um Legacy-Authentifizierungsmethoden zu blockieren, die weniger sicher und anfälliger für Angriffe sind. Die Umsetzung dieser Regel verbessert die Sicherheitslage erheblich durch die Nutzung moderner Authentifizierungsprotokolle.

Begründung: Legacy-Authentifizierungsprotokolle unterstützen keine modernen Sicherheitsfunktionen wie die Multi-Faktor-Authentifizierung, wodurch sie anfällig für Brute-Force- und Passwort-Sprühangriffe sind. Durch das Blockieren der Legacy-Authentifizierung können Organisationen solche Schwachstellen schützen und sicherstellen, dass nur sichere, moderne Authentifizierungsmethoden verwendet werden.

Auswirkung: Das Blockieren der Legacy-Authentifizierung kann sich auf Clients und Geräte auswirken, die auf diese älteren Protokolle angewiesen sind. Es ist wichtig, die Kompatibilität Ihrer Umgebung zu bewerten und schrittweise auf moderne Authentifizierungsmechanismen umzustellen, um potenzielle Störungen zu minimieren.

6.8 User detected that is excluded from Conditional Access Policy

Control Name	Detections Count
User detected that is excluded from Conditional Access Policy	97

Beschreibung: Überprüft jeden Benutzer, um sicherzustellen, dass er in mindestens einer bedingten Zugriffsrichtlinie (CAP) enthalten ist. Benutzer, die durch keine CAP abgedeckt sind, könnten uneingeschränkten Zugriff haben und damit ein Sicherheitsrisiko darstellen.

Begründung: Bedingte Zugriffsrichtlinien (CAPs) sind entscheidend für die Sicherung des Zugriffs auf Ressourcen, indem Bedingungen durchgesetzt werden, die Benutzer erfüllen müssen, um auf Ressourcen zuzugreifen. Diese Regel identifiziert Benutzer, die durch keine CAPs abgedeckt sind, sei es aufgrund von Ausschluss oder fehlender Einbeziehung, und stellt sicher, dass alle Benutzer den notwendigen Sicherheitskontrollen unterliegen.

Auswirkung: Benutzer, die durch keine CAP abgedeckt sind, können möglicherweise uneingeschränkten Zugriff auf Ressourcen haben und wichtige Sicherheitsmaßnahmen umgehen, die zum Schutz vor unbefugtem Zugriff und Verstößen entwickelt wurden. Die Sicherstellung, dass alle Benutzer durch CAPs abgedeckt sind, mindert dieses Risiko.

6.9 Managed devices SHOULD be required for authentication

Control Name	Detections Count
Managed devices SHOULD be required for authentication	1

Beschreibung: Das Sicherheitsrisiko, dass ein Angreifer sich mit einem eigenen Gerät im Mandanten authentifiziert, wird dadurch reduziert, dass ein verwaltetes Gerät für die Authentifizierung erforderlich ist. Verwaltete Geräte stehen unter der Bereitstellung und Kontrolle der Organisation.

Begründung: Erstellen Sie eine Richtlinie für bedingten Zugriff, die erfordert, dass das Gerät eines Benutzers entweder Microsoft Entra hybrid registriert oder bei der Authentifizierung konform ist.

8 Entra ID Applications

8.1 Entra ID Application has dangerously extensive permissions

Control Name	Detections Count
Entra ID Application has dangerously extensive permissions	0

Beschreibung: Diese Regel überprüft Entra ID-Anwendungen, denen Berechtigungen gewährt wurden, die das für ihren Betrieb notwendige Minimum überschreiten. Insbesondere werden Anwendungen identifiziert, deren Berechtigungen potenziell eine Eskalation von Privilegien oder das Handeln im Namen anderer Entitäten innerhalb der Organisation ermöglichen könnten.

Begründung: Berechtigungen innerhalb von Entra ID sollten dem Prinzip der minimalen Rechtevergabe folgen und sicherstellen, dass Anwendungen nur so viel Zugriff haben, wie sie benötigen. Diese Regel identifiziert Anwendungen mit Berechtigungen, die für Privilegieneskalation missbraucht werden könnten, einschließlich, aber nicht beschränkt auf RoleManagement.ReadWrite.Directory, AppRoleAssignment.ReadWrite.All und Application.ReadWrite.All. Diese Berechtigungen ermöglichen es Anwendungen, Rollen zu ändern, App-Rollen zuzuweisen und als andere Entitäten zu handeln, was zu unbefugtem Zugriff oder Aktionen innerhalb der digitalen Umgebung der Organisation führen könnte.

Auswirkung: Anwendungen mit umfangreichen Berechtigungen stellen ein erhebliches Sicherheitsrisiko dar. Sie könnten von bösartigen Akteuren genutzt werden, um erhöhten Zugriff oder Kontrolle über organisatorische Ressourcen zu erlangen, was möglicherweise zu Datenverletzungen, unbefugtem Datenzugriff oder einer weiteren Kompromittierung der Sicherheit der Organisation führt. Die Identifizierung und Minderung solcher Berechtigungen ist entscheidend für die Aufrechterhaltung der Integrität und Sicherheit der digitalen Vermögenswerte der Organisation.

8.2 Entra ID Service Principal has dangerously extensive permissions

Control Name	Detections Count
Entra ID Service Principal has dangerously extensive permissions	0

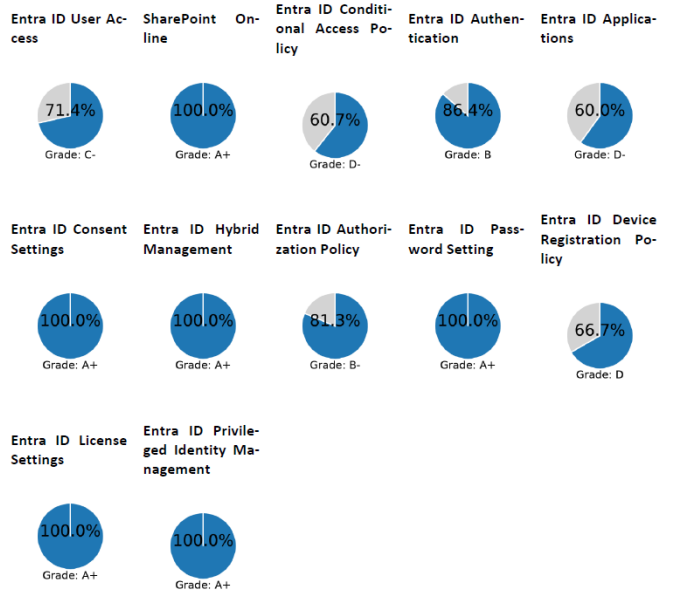
Beschreibung: Diese Regel überprüft Entra ID-Dienstprinzipale, denen Berechtigungen gewährt wurden, die das für ihren Betrieb notwendige Minimum überschreiten. Insbesondere werden Dienstprinzipale identifiziert, deren Berechtigungen potenziell eine Eskalation von Privilegien oder das Handeln im Namen anderer Entitäten innerhalb der Organisation ermöglichen könnten.

Begründung: Berechtigungen innerhalb von Entra ID sollten dem Prinzip der minimalen Rechtevergabe folgen und sicherstellen, dass Dienstprinzipale nur so viel Zugriff haben, wie sie benötigen. Diese Regel identifiziert Dienstprinzipale mit Berechtigungen, die für Privilegieneskalation missbraucht werden könnten, einschließlich, aber nicht beschränkt auf RoleManagement.ReadWrite.Directory, AppRoleAssignment.ReadWrite.All und Application.ReadWrite.All. Diese Berechtigungen ermöglichen es Anwendungen, Rollen zu ändern, App-Rollen zuzuweisen und als andere Entitäten zu handeln, was zu unbefugtem Zugriff oder Aktionen innerhalb der digitalen Umgebung der Organisation führen könnte.

Auswirkung: Dienstprinzipale mit umfangreichen Berechtigungen stellen ein erhebliches Sicherheitsrisiko dar. Sie könnten von bösartigen Akteuren genutzt werden, um erhöhten Zugriff oder Kontrolle über organisatorische Ressourcen zu erlangen, was möglicherweise zu Datenverletzungen, unbefugtem Datenzugriff oder einer weiteren Kompromittierung

3 Scoring

3.1 Environment Scoring



DANKE

Fragen? Gerne!

braincon
IT-EXPERTS. NOTHING ELSE.

15 JAHRE braincon

braincon GmbH

+49 6071 180 300
info@braincon.de
www.braincon.de

Region Rhein-Main

Altheimer Straße 4
64807 Dieburg

Region Rhein-Ruhr

Lise-Meitner-Straße 1-13
42119 Wuppertal

braincon
IT-EXPERTS. NOTHING ELSE.

15 JAHRE braincon

The Digital Workplace Experts!

Modern. Secured. Managed.