devoteam

M Cloud - Azure
Cloud Platform Accelerator

1 week implementation

Creative tech for Better Change

1

The right cloud foundation for your business

The enterprise-scale architecture represents the strategic design path and target technical state for your Azure environment.

It will continue to evolve alongside the Azure platform and is defined by the various design decisions that your organization must make to map your Azure journey.

Why our Platform Accelerator?

1

Speed of implementation
Pre-defined and code-based Cloud Platform components required for an enterprise scale landing zone support

2

Reduced costs
Cross company cloud Platform standards lowers cost of development and maintenance.

3

Secure & Compliant
Platform governance is security tested and are compliant with ISO 27001, CIS and NIST Frameworks.

Cloud Platform

The enterprise-scale architecture is modular by design and allow for a start with foundational landing zones that support application portfolios, regardless of whether the applications are being migrated or are newly developed and deployed to Azure.

M Cloud - Cloud Platform Overview:

Enterprise Enrollment

Management Group Hierarchy

Subscription Democratization

Identity and Access Management

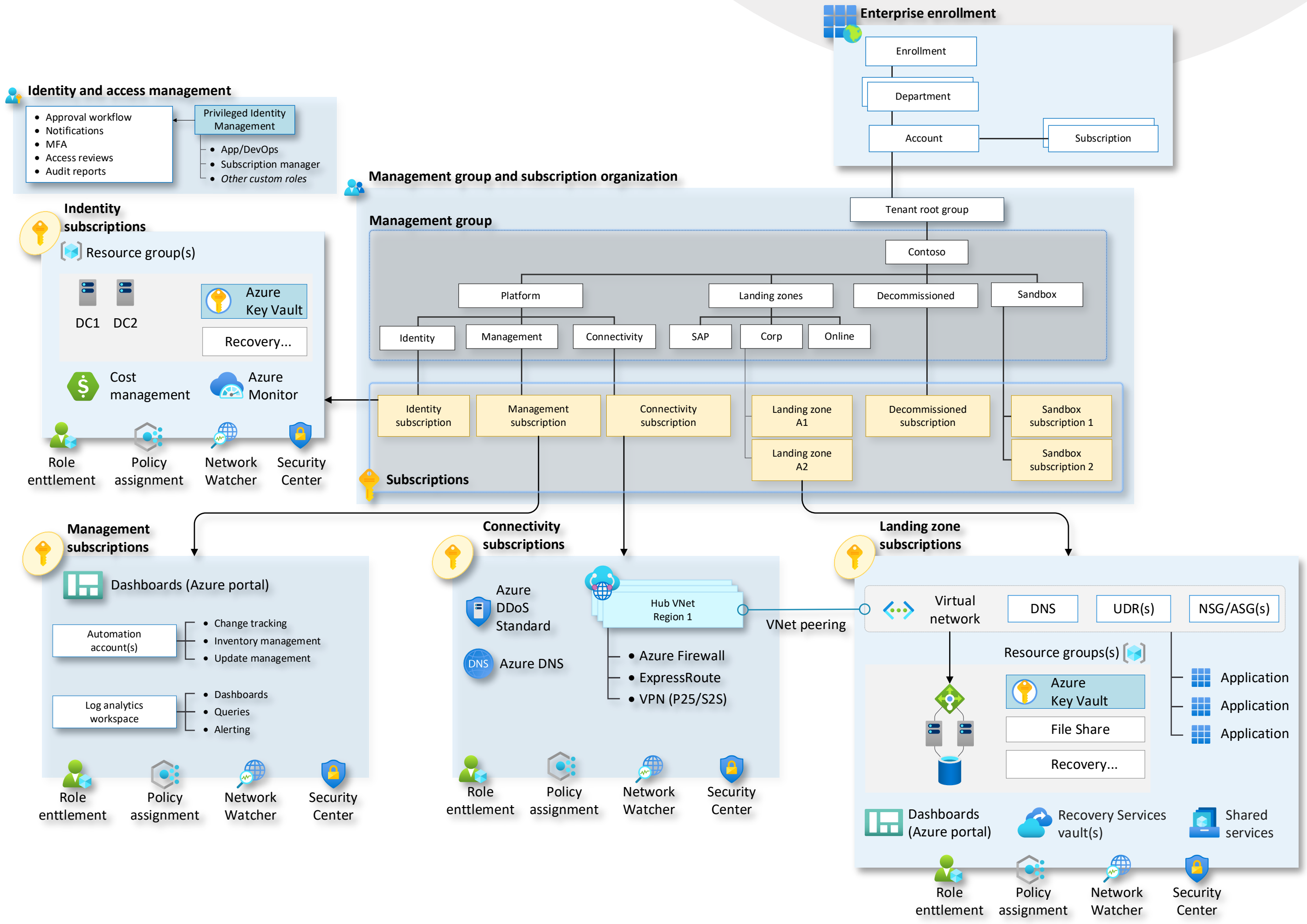
Management and Monitoring

Cloud Connectivity

Network Topology

Landing Zones

Security, Governance and Compliance



Enterprise enrollment

Enrollment

Department

Account

Subscription

Identity and access management

- Approval workflow
- Notifications
- MFA
- Access reviews
- Audit reports

Privileged Identity Management

- App/DevOps
- Subscription manager
- *Other custom roles*

Management group and subscription organization

Tenant root group

Management group

Contoso

Platform

Landing zones

Decommissioned

Sandbox

Identity

Management

Connectivity

SAP

Corp

Online

Identity subscription

Management subscription

Connectivity subscription

Landing zone A1

Landing zone A2

Decommissioned subscription

Sandbox subscription 1

Sandbox subscription 2

Subscriptions

Indentity subscriptions

Resource group(s)

DC1 DC2

Azure Key Vault

Recovery...

Cost management

Azure Monitor

Role enttlement

Policy assignment

Network Watcher

Security Center

Management subscriptions

Dashboards (Azure portal)

Automation account(s)

- Change tracking
- Inventory management
- Update management

Log analytics workspace

- Dashboards
- Queries
- Alerting

Role enttlement

Policy assignment

Network Watcher

Security Center

Connectivity subscriptions

Azure DDoS Standard

Azure DNS

Hub VNet Region 1

- Azure Firewall
- ExpressRoute
- VPN (P25/S2S)

VNet peering

Role enttlement

Policy assignment

Network Watcher

Security Center

Landing zone subscriptions

Virtual network

DNS

UDR(s)

NSG/ASG(s)

Resource groups(s)

Azure Key Vault

File Share

Recovery...

Application

Application

Application

Dashboards (Azure portal)

Recovery Services vault(s)

Shared services

Role enttlement

Policy assignment

Network Watcher

Security Center

2

Cloud Platform Overview

Enrollment and
Azure AD

Identity and Access
Management

Management Groups and
Subscriptions

Network Topology and
Connectivity

Management and
Monitoring

Business Continuity and
Disaster Recovery

Security, Governance and
Compliance

Platform Automation and
DevOps

Design Principles

Cloud is different than on-premise IT and needs to be managed differently. CLOUDEON builds and maintains your cloud platform based on the Cloud Adoption Framework (CAF) Enterprise-Scale design principles with additional ISO, CIS and NIST compliance policies.

Subscription Democratization
Subscriptions are used as a unit of management and scale aligned with business needs and priorities, to support business areas and portfolio owners to accelerate application migrations and new application development.

Policy Driven Governance
Azure Policy is used to provide the guard-rails and ensure the continued compliance of the platform and applications deployed onto it, whilst also providing application owners sufficient freedom and a secure unhindered path to cloud.

Single Control & Management Pane
The platform architecture should not consider any abstraction layers such as customer developed portals or tooling and should provide a consistent experience for both AppOps (centrally managed operation teams) and DevOps (dedicated application operation teams).

Application Centric and Archetype- Neutral
We focus on application centric migrations and development rather than a pure infrastructure "lift and shift" migration (i.e. movement of virtual machines) and do not differentiate between old/new applications or IaaS/PaaS applications.

Azure Native Design and Platform Roadmap Alignment
The Enterprise Scale platform architecture approach advocates the use of native platform services and capabilities whenever possible, which is aligned with Azure platform roadmaps to ensure new capabilities are made available within environments.

Enrollment and Azure AD

Enrollment represents the commercial relationship of how your organization uses Azure. It provides the basis for billing across all your subscriptions and affects administration of your digital estate. Your enrollment can be archived either CSP or EA.

Establish enrollment type:
Define the use of either CSP or EA to facilitate the Azure commercial relationship for your environment.

Planning topology:
Review topology model and confirm correct model against your environment and requirements.

Notification channel:
Define notification recipient of enrollment alerts and configure the group mailbox in Azure.

Emergency Access:
Create break glass account(s) for access to the tenant in case of loss of access from regular accounts.

Define account usage pattern:
Define and document the usage of types of Microsoft account options, MSA versus Work.

Tenant owner structure:
Identify model for tenant owner RBAC and document model for implementation.

Establish single-sign-on:
If not already in place for O365, customer domain must be made available in Azure for usage across the digital estate

Azure AD Connect:
Review of current sync if already in place for appropriate groups. If not in place, sync must be established

Identity and Access Management

Identity and access management (IAM) is boundary security in the public cloud. It must be treated as the foundation of any secure and fully compliant public cloud architecture. CLOUDEON uses a comprehensive set of services, tools, and reference architectures to enable organizations to make highly secure, operationally efficient environments

Data plane access:
Define and configure restrictions to data plane access to resources e.g. Key Vault, storage account or SQL.

Azure Lighthouse:
Implement lighthouse as the access layer for external users to cloud platform resources.

Central logging:
Configure policy driven platform-central logs to a log analytics workspace for log retention and monitoring for compliance.

Landing Zones:
Define and configure policies for RBAC in landing zones centrally. Ensuring consistent access patterns that are measurable and monitorable.

Privileged identity management:
Enable Azure PIM to facilitate zero standing access rights and least privilege across the Azure estate.

Multi-Factor:
Configure policy driven enforcement for MFA for all accounts accessing the Azure estate.

Custom roles:
Create necessary custom roles for the Azure estate across NetOps, SecOps, DevOps, AppOps and Owners.

Azure DevOps Access:
Configure required SPN (service accounts) for Azure DevOps project creation for new IT projects.

Management Group and Subscription

Management group structures within an Azure Active Directory (Azure AD) tenant support organizational mapping. We consider your management group structure thoroughly as your organization plans Azure adoption. Management groups are used to aggregate policy and initiative assignments via Azure Policy.

Management Groups:
Define MG structure in alignment with recommended practices and your specific organization.

Policy patterns:
Ensure alignment of hierarchical structures against policy and initiative assignment strategies.

SPN Requirements:
Document and implement required SPN's (service account) for the automated deployment of new MG and Subscriptions.

RBAC requirements:
Define and implement structure for access across MG and subscriptions in accordance with establish IAM.

Cloud Platform subscriptions:
Deploy platform subscriptions for Identity, Management, Connectivity, Landing Zones, Decommissioned and Sanbox.

Subscription transfer:
Configure policy driven enforcement the transfer of subscription to or from the Azure tenant.

Subscription quota´s:
Configure quotas of deployed subscriptions across the cloud platform and create automation for automatic quota support request for new subscriptions.

Dashboards:
Create dashboard to monitor capacity levels across the subscriptions and alerts for thresholds.

Network topology and Connectivity

Configuration and maintenance of network related components in Azure is critical to the enterprise landing zones and for the ability of application to communicate effectively across Azure regions.

IP Addressing:
Continuous management of assigned IP scopes to the Azure Cloud Platform for use in applications on the platform.

Azure DNS:
Configuration and management of the DNS within the Azure digital estate to facilitate in-cloud Domain Naming Services (DNS).

Private Link:
Configuration of private links across Azure services deployed to the cloud platform.

Network Topology:
Implementation of virtual WAN or hub-and-spoke topology model to facilitate secured scalable networks.

Azure Connectivity:
Configuration of Azure endpoints of hybrid connective through VPN, Express route or public internet.

Landing Zones:
Plan for and implementation of landing zones network segmentation across the digital estate.

Inbound and outbound:
Implementation of Azure-native network security services Azure Firewall, Web Application Firewall (WAF), Application Gateway and Azure Front Door.

Traffic inspection:
Evaluate native cloud options against inspection requirements and configure required models.

Management and Monitoring

Build and operationally maintain an Azure enterprise estate with centralized management and monitoring at a platform level.

Log Analytics:
Create log analytics workspace for central logging across the Azure estate. Configure storage account offload for long term retention.

Operational policies:
Create CLOUDEON recommended operational policies for the cloud platform Azure estate.

Azure Monitor:
Configure Azure Monitor for the digital estate across the cloud platform including Application Insights, VM insights, Container insights, Smart alerts and automated actions.

Security Center and Sentinel:
Enable Azure Security Center and Azure Sentinel to see and stop threat before they cause harm through cloud native SIEM.

Log Shipping:
Define policy driven log shipping for entire digital Azure estate to collect logs and metrics from IaaS and PaaS.

Dashboard and query:
Create operational dashboards with the cloud-native tools in use such as Azure Monitor logs, in-guest VM monitor and service and resource health events.

PIM automation:
Create central roles for controlling privileged activities across the digital estate, for both elevation and membership management.

Self-Service enablement:
Create/Configure self-service for new creation of new projects/landing zones on the cloud platform.

Business Continuity and Disaster Recovery

Enterprises needs to design suitable, platform-level capabilities that application workloads can consume to meet their specific requirements in form of specific recover time objective (RTO) and recovery point objective (RPO).

Multiregional:
Support application deployments that would require multiregional for failover purposes with component proximity for performance reasons

Workload RTO/RPO
Enable workloads to run active-active and active-passive availability patterns on the Cloud Platform

Native DR:
Support of business continuity for platform as a service (PaaS) services and the availability of native DR and high-availability features.

Availability Zones:
Configuration of AZ or availability sets for data sharing and dependencies between zones.

Consistent Backup:
Leverage Azure Backup and Recovery Services Vault along with VM snapshot to support your requirements.

Network connectivity:
Redundancy of networking through bandwidth capacity monitoring and traffic routing regional and zonal in case of cloud outage.

Failovers:
Planned and unplanned failovers are managed through consistency in requirements for IP address scopes and their failover along with DevOps capable engineering team

Dashboard:
Environmental overview of services health and platform metrics, ensures continuous insights into the Azure cloud platform.

Security, Governance and Compliance

Defining encryption and key management, governance support and reporting, defining security monitoring and the audit policy, and setting the level for platform security

Encryption:
Enforced and policy based Key Vaults to store secrets and certificates, including encryption at rest and in-transit and whole-disk encryption for Virtual machines.

Key Vault
Implement KV boundaries and policy assignment objectives to archived recommended state of isolation control for secrets.

Policy sets:
ISO, CIS and NIST policy frameworks are applied to support your internal governance requirements. Additional regulatory policies can be applied.

Tagging:
Apply recommended tags across the digital estate to support policy deployments, ownership of resources, cost allocations and many other elements.

SecOps:
Define retention periods, baseline security configuration and institute these in policies to ensures consistent security across the Azure services.

Financial transparency:
All resources on the cloud platform are tagged to ensure cost allocation across the entire digital estate.

Security Benchmark:
Review and improve Azure security benchmark across security controls and service recommendations.

Dashboards:
Create dashboards to view central security information as it related policy sets and compliance to these.

Platform Automation and DevOps

Building your Cloud Platform cloud-native using a DevOps approach for platform implementation and maintenance.

Azure DevOps:
Configure your Azure DevOps to host the Cloud Platform and facilitate new projects and release pipelines to deploy new landing zones for your projects.

Developer Guidance:
Build wiki-based guidance for your developers on how to interact with and leverage your new cloud platform optimally.

New Projects:
Build wiki-based guidance on how to request new projects, including landing zones and build test-driven deployment validations.

Landing Zone:
Build CLOUDEON recommended first landing zone template for use for new projects across your business.

Release Pipeline:
Build release pipeline for platform development and subsequent maintenance and testing.

Repositories:
Build and document repo structure based on GitHub and Azure DevOps, and provided usage guidance in Wiki.

3

Who are Devoteam

Devoteam who we are

Tech for people **unlocks the future.**

1 We believe technology with strong **human values** can actively **drive change for the better.**

2 We make sure **all our clients' employees are fully on board** with the transformation journey.

3 We **care about our people** and offer them a workplace that fuels **learning, innovation and engagement.**

25
years of passion for tech

8,000
devoteamers in 18 countries across EMEA

400+
devoteamers in Devoteam Denmark

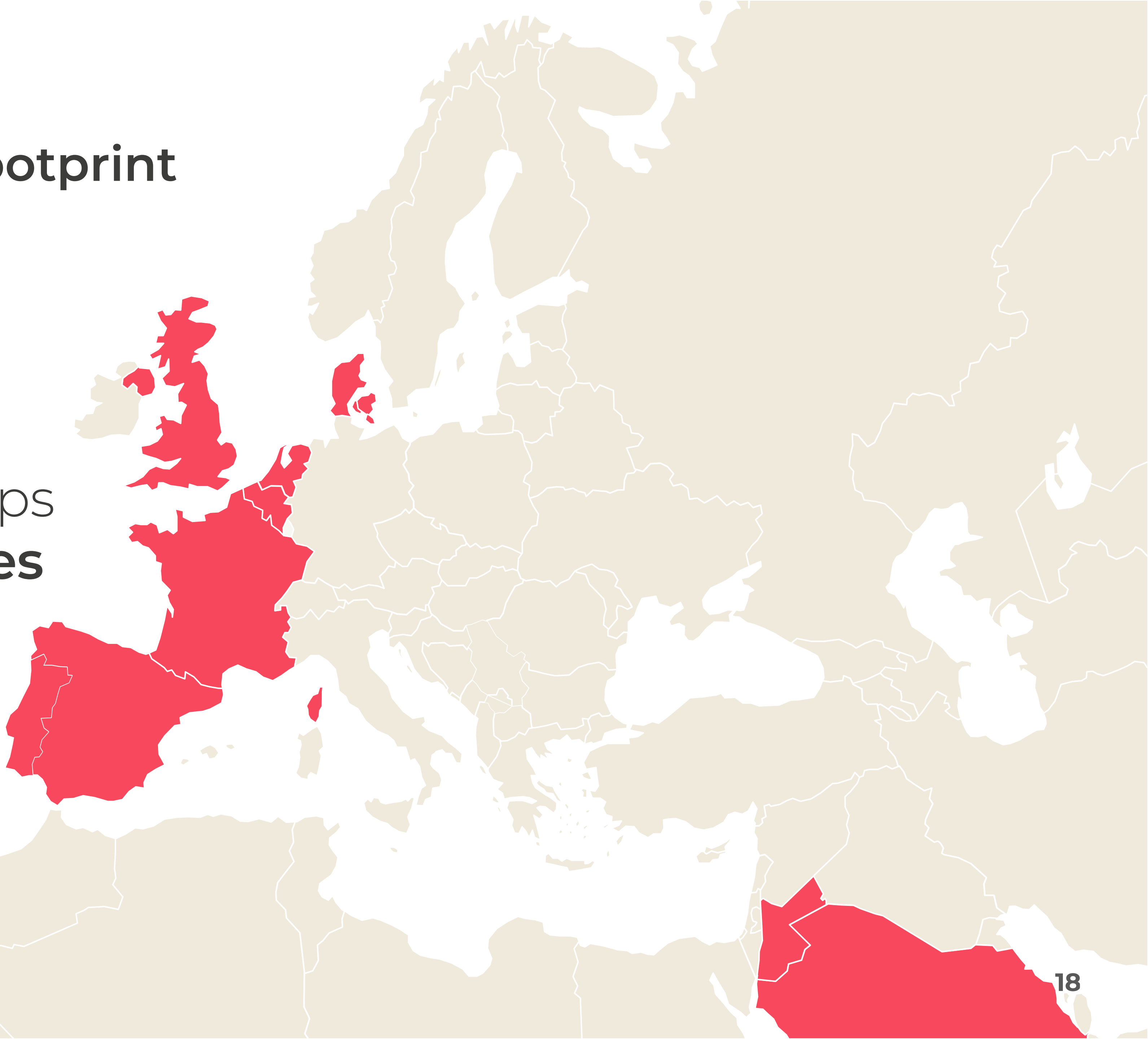
Devoteam Data Driven:
An established EMEA footprint

devoteam
Data Driven

- **800** consultants
- **8** countries

with strong partnerships in **leading technologies**

aws · Google Cloud · Microsoft · databricks · snowflake · alteryx · Collibra · dataiku · Qlik · Informatica · tableau · MicroStrategy



Devoteam M Cloud: **a preferred partner in EMEA**

Sized for agility and trust

Gold
Microsoft
Partner
Microsoft

Azure
Expert
MSP

+ 125 M€ | Revenue
+ 1000 | Experts
+ 1950 | Certifications

Our expertise

- 16 Gold competencies
- 9 Advanced specializations:

Change & Adoption

Low Code Development

Threat Protection

Windows and SQL migration

Calling for Teams

Application Modernisation

Kubernetes on Azure

Meetings and Rooms for Teams

Teamwork Deployment

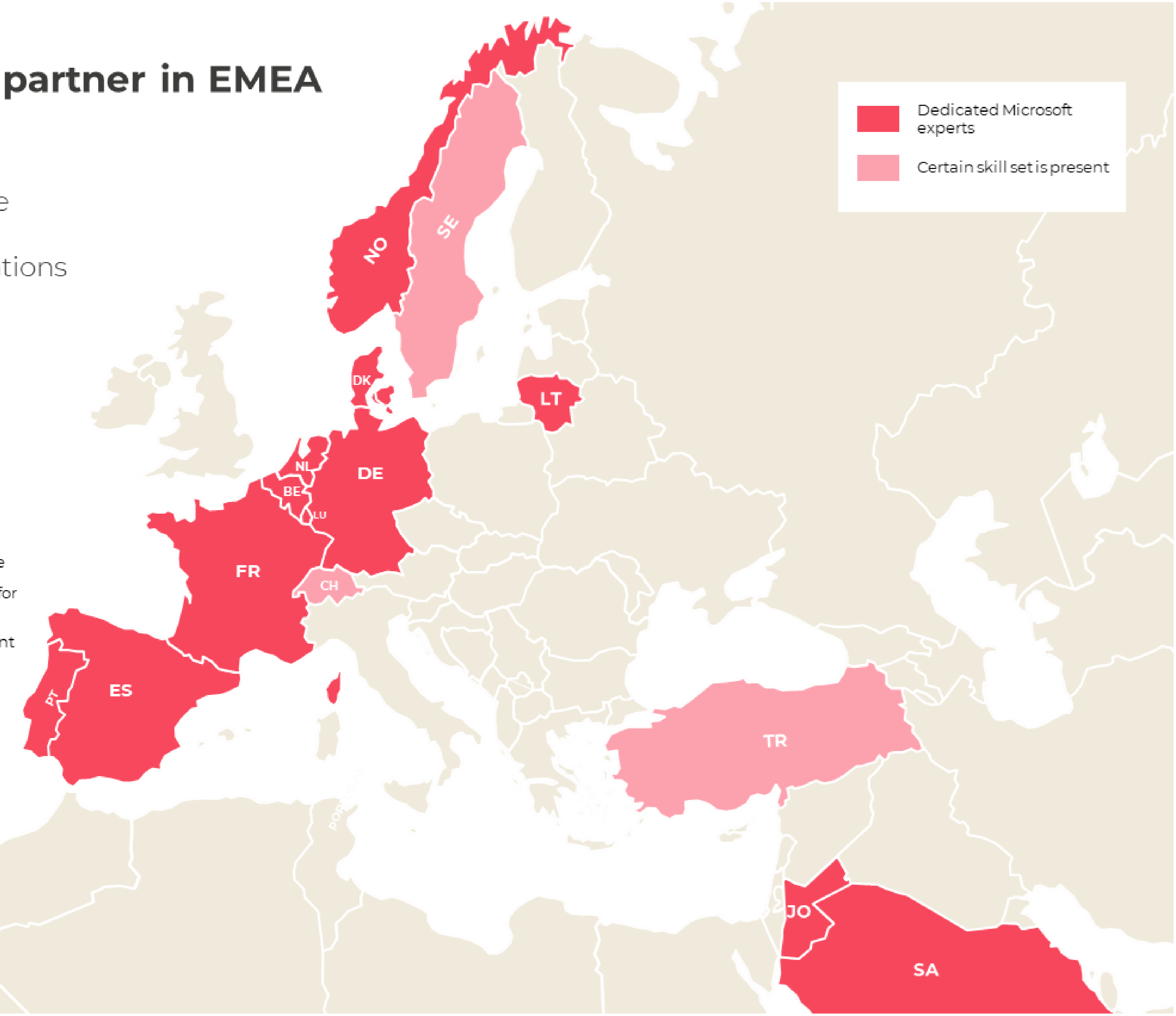
✓ FastTrack Ready

✓ Direct Reseller (CSP)

✓ Cloud and Hybrid Managed Services *with own IP*

✓ Authorized Training Partner

2019-2021
Partner of the Year Award



🟥 Dedicated Microsoft experts
▨ Certain skill set is present
NO
SE
DK
LT
NL
DE
BE
LU
FR
CH
ES
PT
TR
JO
SA