

# AZURE MEETUP ROSTOCK

03.07.2024



# AGENDA

**01**

Azure Updates

**02**

Review zur European  
Cloud Summit 2024

# AZURE UPDATES (1/2)



- Azure Advisor will no longer display aggregated potential yearly savings beginning 30 September 2024: [View article...](#)
- General availability: Virtual network flow logs (jetzt auch ohne NSG): [View article...](#)
- Public preview: Azure Deployment Environments supports Bicep, Terraform, Pulumi [View article...](#)
- General Availability - Azure API Center [View article...](#)
- General availability: Customer-managed keys on existing accounts [View article...](#)
- Announcing the General Availability of GPT-4 Turbo with Vision on Azure OpenAI Service [View article...](#)
- General availability: Azure Bastion Developer SKU [View article...](#)
- Public preview: Azure Application Gateway v2 Basic SKU [View article...](#)
- Azure Front Door server variable enhancement generally available (Neue Routingmöglichkeiten) [View article...](#)
- Introducing GPT-4o: OpenAI's new flagship multimodal model now in preview on Azure [View article...](#)
- General Availability: Data API builder (GraphQL/REST für alle Azure DBs) [View article...](#)
- The availability of Azure compute reservations will continue until further notice [View article...](#)
- Update on Inter-Availability Zone Data Transfer Pricing [View article...](#)
- Public preview: KEDA in the Azure Portal (Kubernetes Event-Driven Autoscaler) [View article...](#)
- Generally Available: Azure Functions can now run on Azure Container Apps (inkl. KEDA, DAPR) [View article...](#)
- Public preview: Azure Functions extension for OpenAI [View article...](#)
- Public Preview: Azure Functions brings new flexibility with Azure Functions Flex Consumption [View article...](#)
- Generally Available: Azure Functions extension for Dapr (z.B. für PubSub, läuft auf AKS/ACA) [View article...](#)

## AZURE UPDATES (2/2)



- Public Preview: Monitor apps with Java metrics in Azure Container Apps [View article...](#)
- Public Preview: Next-Gen Dashboards Experience in Azure Portal [View article...](#)
- Public Preview Azure Integration Account Enhancements (AIA nur für Logic Apps) [View article...](#)
- Public Preview Azure Logic Apps Standard Deployment Scripting Tools in VS Code ("automated build and deployment processes using Azure DevOps and ARM templates") [View article...](#)
- GA Support for gRPC APIs in Azure API Management Self-hosted Gateway [View article...](#)
- Azure API Management hat jetzt Load Balancer ([View article...](#)), OData API ([View article...](#)) Circuite Breaker ([View article...](#))
- Public Preview - Azure Compute Fleet (bis zu 10T VMs (Standard & Spot) einfach starten/managen, für Bildgenerierung/Big Data) [View article...](#)
- Preview: Windows gRPC support is now available on App Service [View article...](#)
- Azure Deployment Environments (bisher Bicep, ARM, TF) unterstützen jetzt Pulumi [View article...](#)
- Public preview: Azure NetApp Files application volume group for Oracle [View article...](#)
- Visual Studio Code extension for Azure Web PubSub (Direktnachrichten bei WebSockets) now in preview [View article...](#)
- General Availability: VM Hibernation for General Purpose VMs [View article...](#)
- Public preview: Advanced Container Networking Services for Azure Kubernetes Services (AKS) [View article...](#)
- Azure Virtual Network Manager's virtual network verifier is now in public preview [View article...](#)
- Public preview: Azure Load Balancer now supports Admin State [View article...](#)



## 02 – Review zur European Cloud Summit



### Eckdaten:

- In Wiesbaden
- 14.05. – 16.05.
- Davon 1. Tag Workshops
- Zwei Konferenzen:
  - Cloud Summit
  - Collab Summit
- <https://cloudsummit.eu/>



## 02 – Review zur European Cloud Summit



### 👍 Gut

- Alle Vorträge mit sehr genauem Start-Stopp
- Viele Spannende Themen und breit gefächert (5 Tracks: Business, AI, Azure Security, Azure Infrastructure, Azure Development), es gab immer was zum Angucken
- Wein war lecker 🍷 😊
- Tolle Live Musik 🎸
- Hab alte Arvato-Kollegen getroffen

### 👎 Schlecht

- Keine Wissenslevel an den Vorträge und es gab verschiedene Detaillevel (Code, Übersicht)
- Einige Vortragende konnten das nicht so gut (zu schnell gesprochen)
- Manchmal fiel der Beamer aus
- Catering war chaotisch (kein Wasser, 4 Food Trucks für 3000 Leute, Abends gab es Wraps, ...)
- Ich warte noch auf einige Slides
- Es gab Coins, aber die wurden nicht immer gezählt und am Ende gab es keine Preise mehr
- Networking fällt alleine schwer
- Wohl wenig Interesse am Adesso Stand, ein paar Kundenanfragen ein paar Bewerber



26-28 May  
2025  
CCD / Messe  
Düsseldorf

Super Early Bird Discount  
Available in Limited Numbers!



## 02 – Review zur European Cloud Summit



- 👎 👁 • Lessons Learned in Migrating Legacy Apps to Azure
- 👎 👁 • Containers in multi-cloud world
- 👍 👁 • Implementing Event Sourcing Strategy on Azure
- 👍 👁 • Developing secure software with GitHub
- 👍 👁 • Serverless Actor Model with Durable Functions
- 👎 👁 • Cross-Tenant Collaboration with Entra External IDs
- ❌ • Azure Load Testing
- 👍 👁 • Protecting sensitive data in Azure SQL database
- ❌ • Protecting Your Kingdom with Azure Identity Platform v2
- ❌ • Mastering Resilience: Continuous Validation with Azure Chaos Studio and Azure Load Testing
- 👎 👁 • The Future of Network and Identity Security: Microsoft Entra SSE/SASE
- ❌ • Event Driven Communication with Azure Communication Services
- 👍 👁 • OAuth Flows in Microsoft Applications
- ❌ • Introducing Azure API Management
- 👍 👁 • Azure Container Apps and Dapr - Building Microservices State of the Art
- 👍 👁 • Unleashing the Power of Microsoft Semantic Kernel in API Communication - A Deep Dive into GPT-4



# LESSONS LEARNED IN MIGRATING LEGACY APPS TO AZURE 🙄



- Kurzüberblick 5Rs: Rehost, Refactor, Rearchitect, Rebuild, Replace
- Erfahrungsbericht mit alter Windows Server 2008 Anwendung
  - Lift&Shift zu teuer
  - Refactor zu schlechte Doku und 15 Jahre alter Code mit 20 verschiedenen Devs
  - Daher ReArchitecture und Rebuild in Kombi
  - Projekt wurde aber abgebrochen
- Typische Fehler:
  - Keine Cloud Strategie
  - Tech Depts
  - Zu wenig Cloud Knowledge
  - Vorgehen ist Big und Quick, aber nicht Smart
  - Kein Blick auf Compliance, Security, Privacy
  - Teams nicht synced
  - Keine Hilfe gesucht

- > [AppCAT Plugin für VS](#)
  - > Analysiert bestehenden Code
  - > Gibt es auch für Java
- > [AZD - Azure Developer CLI](#)
  - > Templates für Developer inkl. Infrastruktur etc.
- > [Azure Arc for Developers](#)
- > CAF, WAF, MS Assessments



# CONTAINERS IN MULTI-CLOUD WORLD 🙄



- 50% der Cloud Workloads weiterhin VMs
- K8s selbst betreiben ist schwer, besonders Updates bei Masternodes
- Alle 3 Hyperscaler haben managed K8s (mit verschiedenen Details in der GUI, mit verschiedenen Konfigurationen)
  - Am einfachsten und schnellsten ist GCP, dort wird auch nur für Nodes bezahlt, wenn genutzt
  - Am umständlichsten und längsten ist AWS
- Trend geht zu höherwertigen Containerdiensten: CaaS
  - AWS: Elastic Container Service (ECS)
  - Azure: Azure Container Service → arbeitet Serverless, erster Request hat 10 Sekunden gedauert
  - GCP: Google Cloud Run

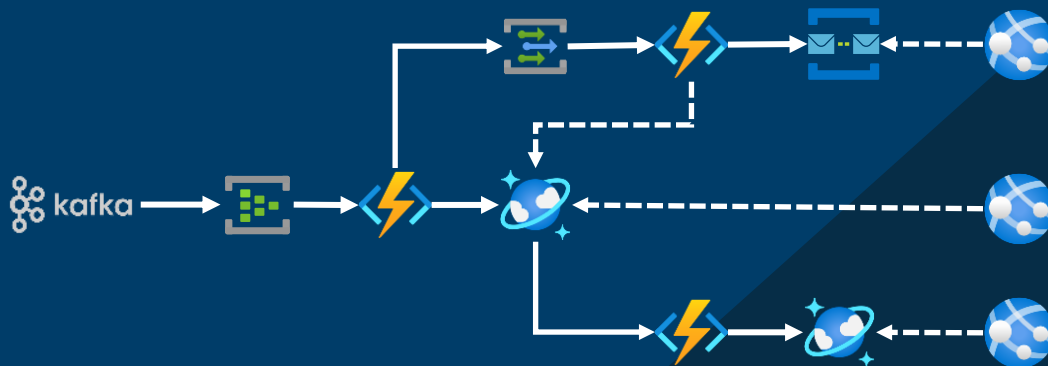
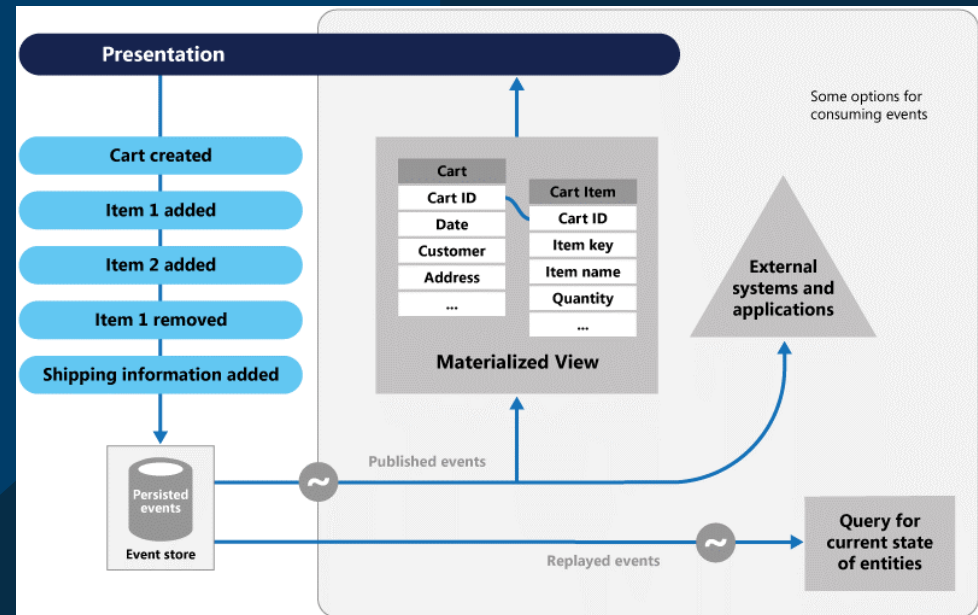
- > Alle Clouds haben höherwertige Containerdienste, die Mgmt vereinfachen
- > Höherwertige K8s-Dienste sind sinnvoll



# IMPLEMENTING EVENT SOURCING STRATEGY ON AZURE 👍



- Viele Vorteile von EventSourcing: Build-In Log, Keine Objekte, Einfache Benutzung, keine Locks und daher große Skalierung
  - Spiel HALO wurde daher auf EventSourcing umgestellt
- Gezeigtes Beispiel ist Flaschenpost.de entlehnt, dort ES für Bestellungen umgestellt → Materialized Views waren das Data Ware House
- CosmosDB als EventStore: Change Feed, Lease Container, wohl auch Immutable Container



- > [Code Repo](#)
- > [Slides](#)
- > CosmosDB ist guter EventStore
  - > PartitionKey ist wichtig für Kosten
  - > Mögl. keine DSGVO Daten in Events



# DEVELOPING SECURE SOFTWARE WITH GITHUB 👍



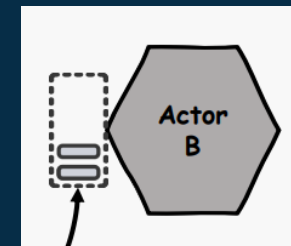
- Kurzinfo zu OWASP10, Secure Software Development Lifecycle
  - Vorteile: geringere Dev Kosten, weniger Security Fehler, bessere Compliance
  - Automatisierbar: Thread Modelling, Code Analysis, Security Tests, Config Scans, CI/CD, Incident Responses
- GitHub:
  - Secret Scan: free für public Proj., kann reporten, kann Push verhindern, auch als Pro mit mehr Features
  - Code Scan: free für pub., findet Errors/Secret Probl., basiert auf CodeQL, Pro Version hat „Autofix“ + AI
  - Dependencies: free, erzeugt Alerts bei nötigen Updates, kann Autoupdate und PR erzeugen
- Azure DevOps:
  - Hat auch diese Features, aber als „Advanced Security“ bei „Projekt Settings“ aktivieren
  - Kostet 50\$ pro user (für alle Orgs und alle Repos)
  - Nutzt auch CodeQL
  - Tools müssen manuell als Tasks eingebunden werden
- Empfehlungen für Alternativen: SonarQube, Snky

- > [Slides](#)
- > GitHub Commit mit [bfg Tool](#) bereinigen
- > Defender for Cloud kann GitHub, GitLab, AzDevOps [integrieren](#)
- > Langfristig (10+ Jahre) wird Azure DevOps verschwinden (neue Features in GitHub)
- > Snky hat auch [Freikontingent](#)



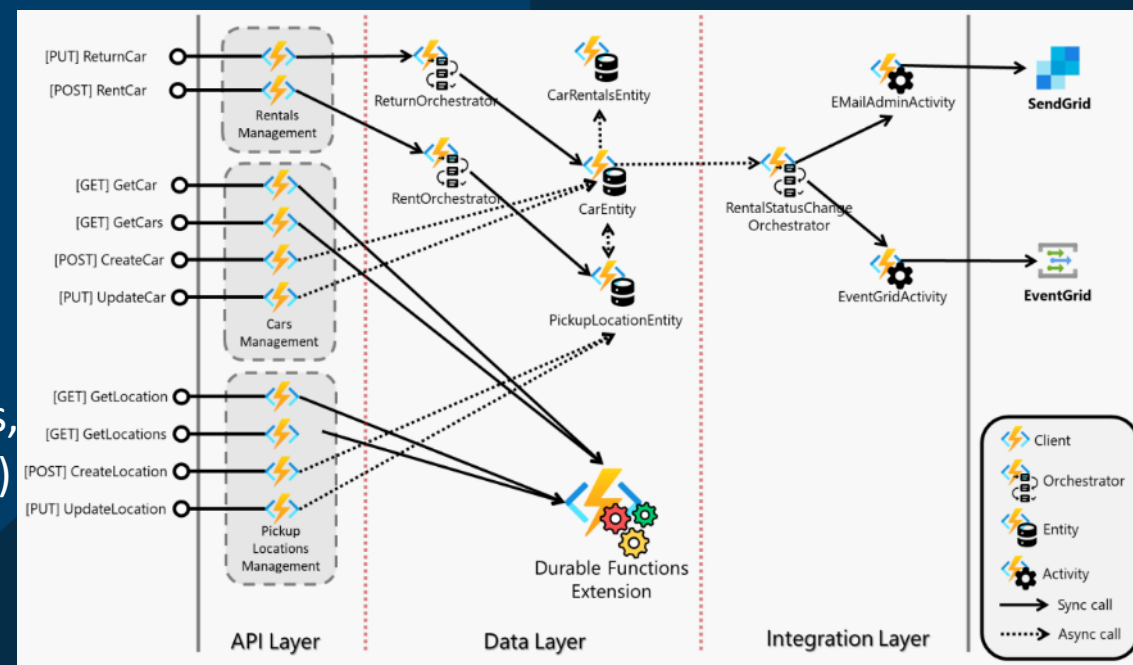


# SERVERLESS ACTOR MODEL WITH DURABLE FUNCTIONS 👍



a

- Actor Modell: für concurrent computing
  - alles ist ein Actor, Actor hat Speicher & Queue & Zustand, kann lange leben, schreibt Nachrichten in Queue der anderen Actors
  - Eintreffende Nachricht: ändert inneren Zustand, kann asynchrone Nachrichten schicken, kann Actors erschaffen
  - Keine Aufrufketten, keine Wartezeit, keine Deadlocks, keine Transaktionen (nur Kompensationsnachrichten)
- Entity Function:
  - Ist Durable Functions (Orchestrator, Action, Client)
  - Können read/update des Zustand, andere EF aufrufen
  - Am besten nutzen mit Basisklasse :TaskEntity<DATA>
  - Wohl keine Overloads und mind. 1 Argument
  - Zustand in Table Store



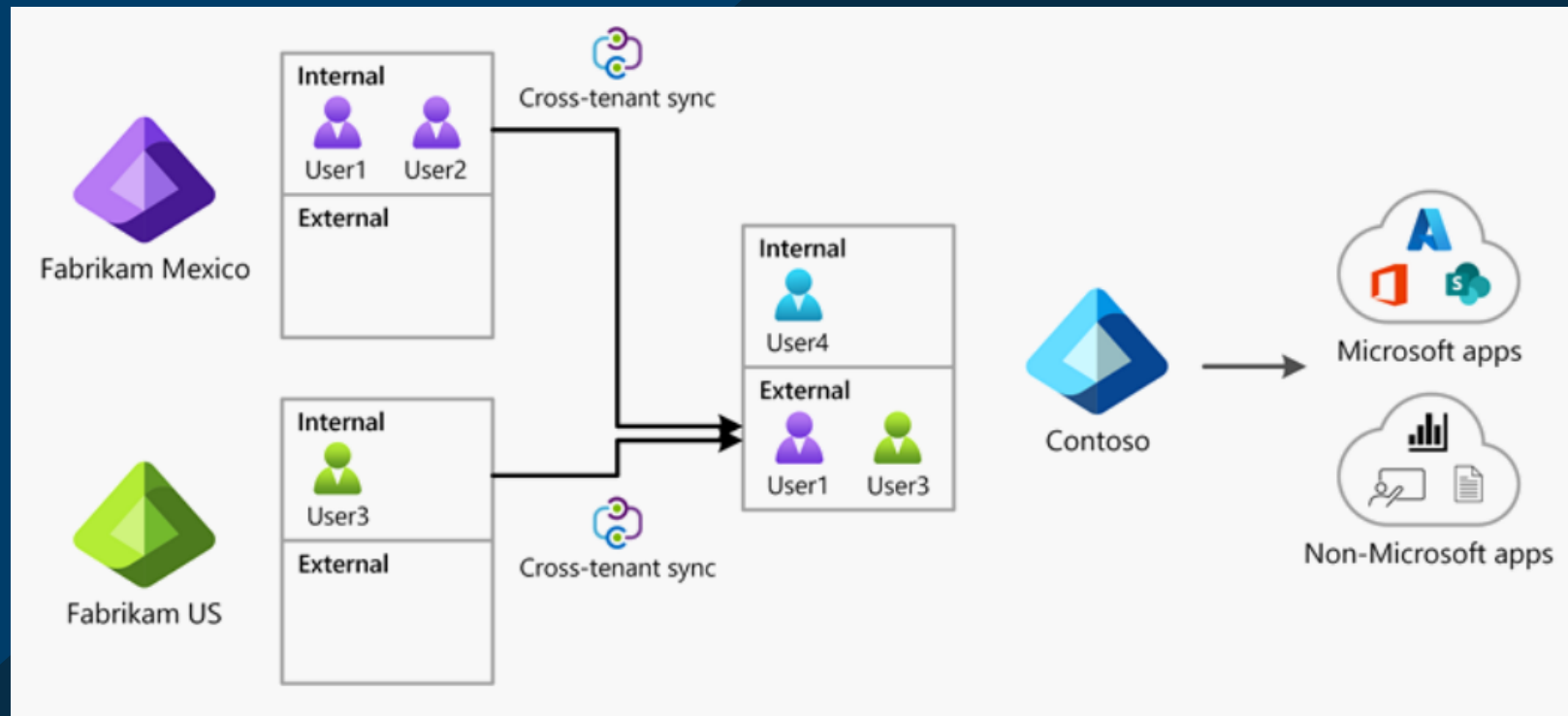
- > [Slides](#)
- > [CarShare Repo](#)
- > Table Store mit schlechter Performance
- > Fire&Forget bei Client, Orchestrator, Entity
- > Sync bei Orchestrator, Entity



# CROSS-TENANT COLLABORATION WITH ENTRA EXTERNAL IDS 🧠

- 3 Arten von External IDs
  - B2B Direct: Shared Channels, nur in Teams
  - B2B Collaboration: Guests im AAD
  - Cross Tenant Sync: Kopie und Update von User Objekten aus anderem AAD
    - nur für AADs aus eigener Organisation
    - Ist nur One Way
    - Users können als Guests oder Members ins Ziel

- > Quelle muss vertrauenswürdig sein
- > Quelle bestimmt Zielrolle!
- > [Slides](#)



# PROTECTING SENSITIVE DATA IN AZURE SQL DATABASE 👍




- Negativbeispiel Firma Vastaamo
- Angriffsmöglichkeiten: Backup-Datei → At-Rest, Übertragung → At-Transit, Verarbeitung → At-Process
- At-Rest:
  - MDF Dateien mit feste Struktur (8K mit Header), auslesen mit python table\_extractor
  - TDE verschlüsselt transparent, kann auch CMK und hat dann Server-Key in KV und pro DB ein Key in KV
- At-Transit:
  - Übertragung mit Tabular Data Stream Protokoll (TDS)
  - Version 7 hat Verschlüsselung optional, V8 mit Verschlüsselungspflicht
- At-Process:
  - Es können Dump-Files z.B. mit python page\_extractor ausgelesen werden
  - Einfachste Lösung ist transparente Verschl. "Always Encrypt" (auch als CMK) für einzelne Spalten
  - AE: Erzwingt Queries mit Parameter, Erfordert 2 Roundtrips, es geht nur Gleichheitsvergleich
  - AE mit Secure Enclave: Unterstützt alle Vergleiche, virtuell oder Chip

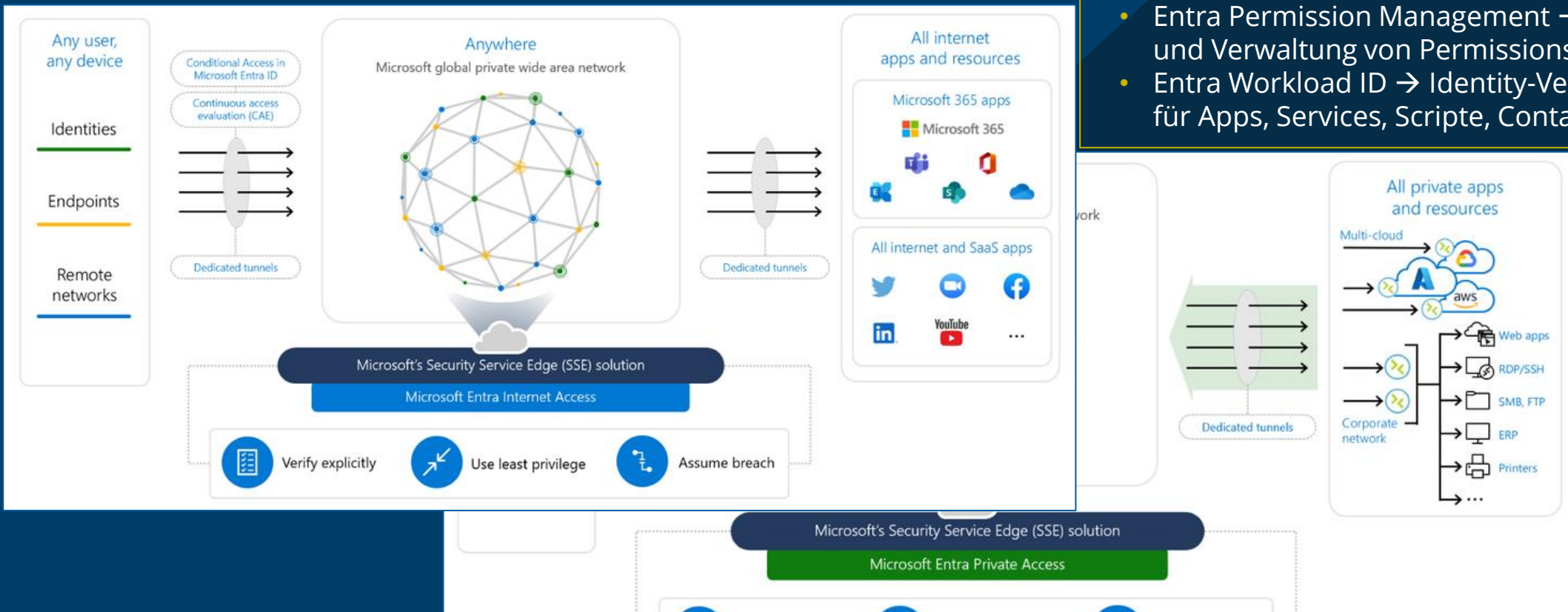
- > [Slides](#)
- > Immer TDE aktivieren
- > Immer TDS verschlüsseln
- > Wenn Always Encrypt, dann mit Secure Enclave



# FUTURE OF NETWORK & IDENTITY SECURITY: MICROSOFT ENTRA SSE/SASE

- SSE (Security Service Edge) ist Untermenge von SASE (Secure Access Service Edge)
  - SASE = Entra Internet Access & Entra Private Access
  - Client für Windows, Android, iOS, MacOS

- > Ersetzt VPN 
- > Client wird in Windows integriert
- > Andere Entra Services:
  - Entra ID Governance → SCL Prozess
  - Entra External IDs → Externe User
  - Entra Verified ID → User Nachweis für Dritte
  - Entra Permission Management → Report und Verwaltung von Permissions
  - Entra Workload ID → Identity-Verwaltung für Apps, Services, Scripte, Container, ...





# OAuth Flows in Microsoft Applications 👍



- OAuth für Access Token → Zugriff (beschrieben durch Scopes)
- OpenID als Aufsatz → ermöglicht ID Tokens
- Flows
  - Authorization Code Grant → für vertrauenswürdige Anwendungen da ID+Secret
  - Implicit Grant → ❌
  - Authorization Code with PKCE → SPA/Mobile App
  - Device Code → für Geräte ohne Browser (TV)
  - Client Credential Grant → für Anwendungen ohne User, benötigt aber ID+Secret (besser Zertifikate oder Azure Managed Identity)
  - Resource Owner Password → falls keine GUI, User+Password
  - On-Behalf-Of → Credentials an Downstream API durchreichen, Lib: Azure.Identity
  - Refresh Token Redemption → um neues Access Token zu bekommen
- Übersichtsslide und Code Snippets fehlen 😞

> Tokens sind schützenswert und nur httpS nutzen  
> ID Token & Access Token können nicht revoked werden, daher kurze Lebensdauer



# ACA AND DAPR - BUILDING MICROSERVICES STATE OF THE ART 👍



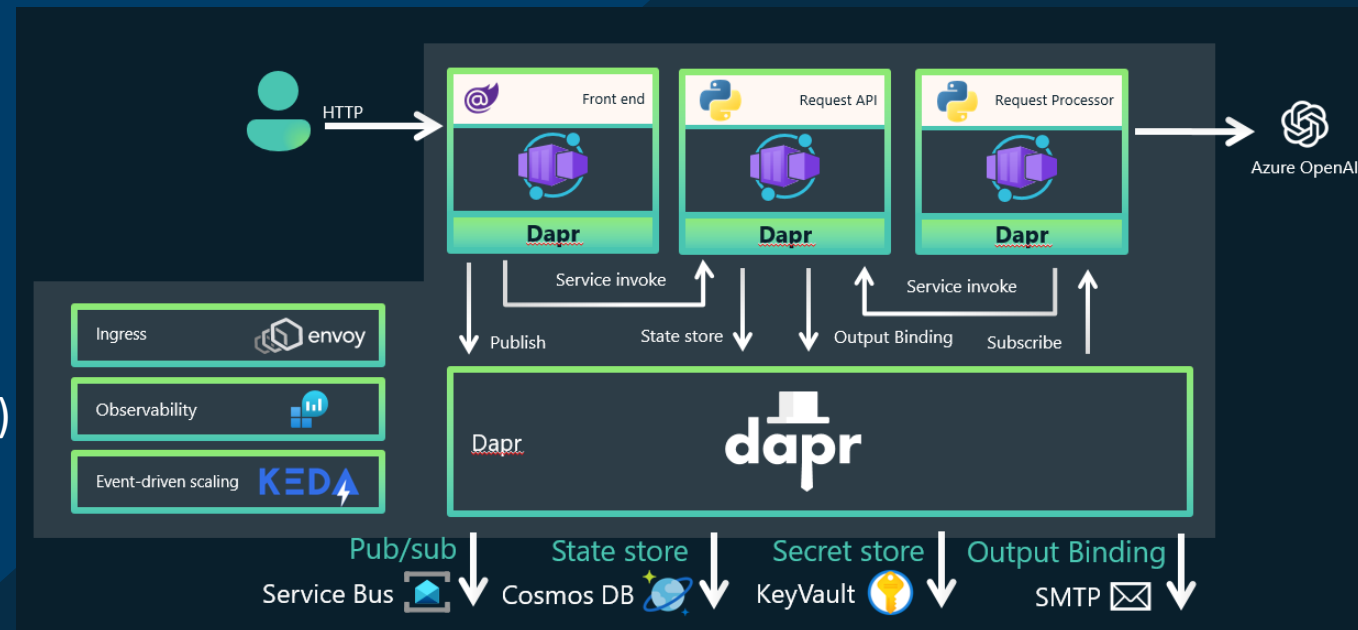
- Azure Container Apps:

- DAPR integriert
- Autoscale mit KEDA
- Price by Compute
- Hat Envoy als Ingress Controller
- Bis zu 100 Replicas

- Dapr

- Für jede Sprache geeignet (Go, C#, Java, ...)
- Setzt Regeln um, egal wie POD programmiert → durch Sidecar-Pattern
- Dapr kann komplett lokal laufen
- Input/Output Bindings sind inkludiert für viele Services und müssen nur einfach konfiguriert werden
- End2End Monitoring kann einfach mit Application Insights gemacht werden

- > [Beispielprojekt Repo](#)
- > [Quickstart Beispiele](#)
- > Erfolgreich bei 300K Requests/Sekunde
- > Wird ständig weiterentwickelt → im Auge behalten



# SEMANTIC KERNEL IN API COMMUNICATION - A DEEP DIVE INTO GPT-4 👍



- Semantic Kernel:
  - Integriert LLMs als SDK in konventionelle Sprachen (C#, Python, Java, ...)
  - Enthält zum Aufrufen: AutoInvoke, Function Calling, StepwisePlanner, Handlebars Planner
- Beispiel:
  - Anwendung ist ein Auto mit 5 Native Functions (vorwärts, rückwärts, links, rechts, stop)
  - erhält Text als Problem („Umfahre Hindernis“, „mache Moonwalk“)
  - Ausgabe ist passender Aufruf der Functions

- > [Slides](#)
- > [Beispielprojekt Repo](#)
- > [Doku zu Plugins](#)
- > AutoInvoke einfach, aber nur 5 calls



	Function calling w/ auto invoke	Function calling	Function calling stepwise planner	Handlebars planner
<b>Complexity</b>	easy	complex	easy	easy
<b>Speed</b>	fast	fast	slower	slow
<b>Cost</b>	cheap	cheap	expensive	expensive
<b>Features</b>	max 5 tool calls supports streaming	unlimited tool calls supports streaming	dynamic selection of tools user-defined calls limit user-defined calls interval	supports handlebars syntax review the plan before execution save the plan supports loops and statements