

ACCELER8IT

by Conlea

Hostowanie MCP na Azure

Kolejna aplikacja czy warstwa platformy?

Michał Smyk

DevOps Cluster Lead



WWW.ACCELER8.IT

ACCELER8IT

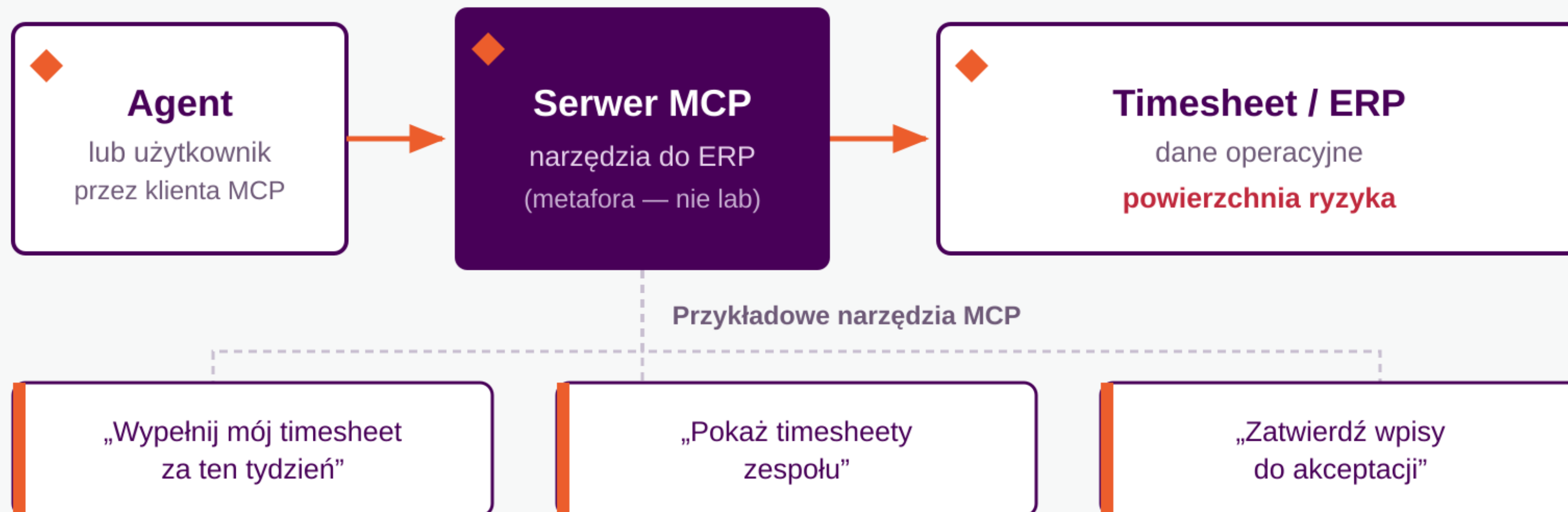
by Conlea

Opowiadane case study jest
wypadkową kilku różnych
wdrożeń - fabuła została trochę
uproszczona.



WWW.ACCELER8.IT

Co robi nasz serwer?



Różnica między API a MCP

API

- Oparte na protokole (zwykle REST)
- Definicje wystawione np. przez Swagger/OpenAPI
- Wiele endpointów HTTP
- Logika biznesowa decyduje, które endpointy wybrać
- Obszar działania = zaplanowane endpointy

MCP

- Wiele opcji wdrożenia (HTTP, ale też stdio, npx)
- Definicje dostępne jako narzędzia (Tools)
- Pojedynczy endpoint do połączenia
- Agent wybiera, czego użyć
- Obszar działania = narzędzia, które agent może złożyć

Rodzeństwo — nie zamiennik

Agent za Ciebie wybiera, co zrobić



PoC vs Produkcja



W ramach prelekcji skupimy się na poniższej konfiguracji

Azure Container Apps + Entra



Pułapki w drodze na produkcję

Wyzwanie

AuthN - kim jesteś?

Czyje uprawnienia wykorzystują narzędzia?

Sieć - dostęp do serwera MCP i serwera do innych zasobów

Rozwiązanie (na Azure)

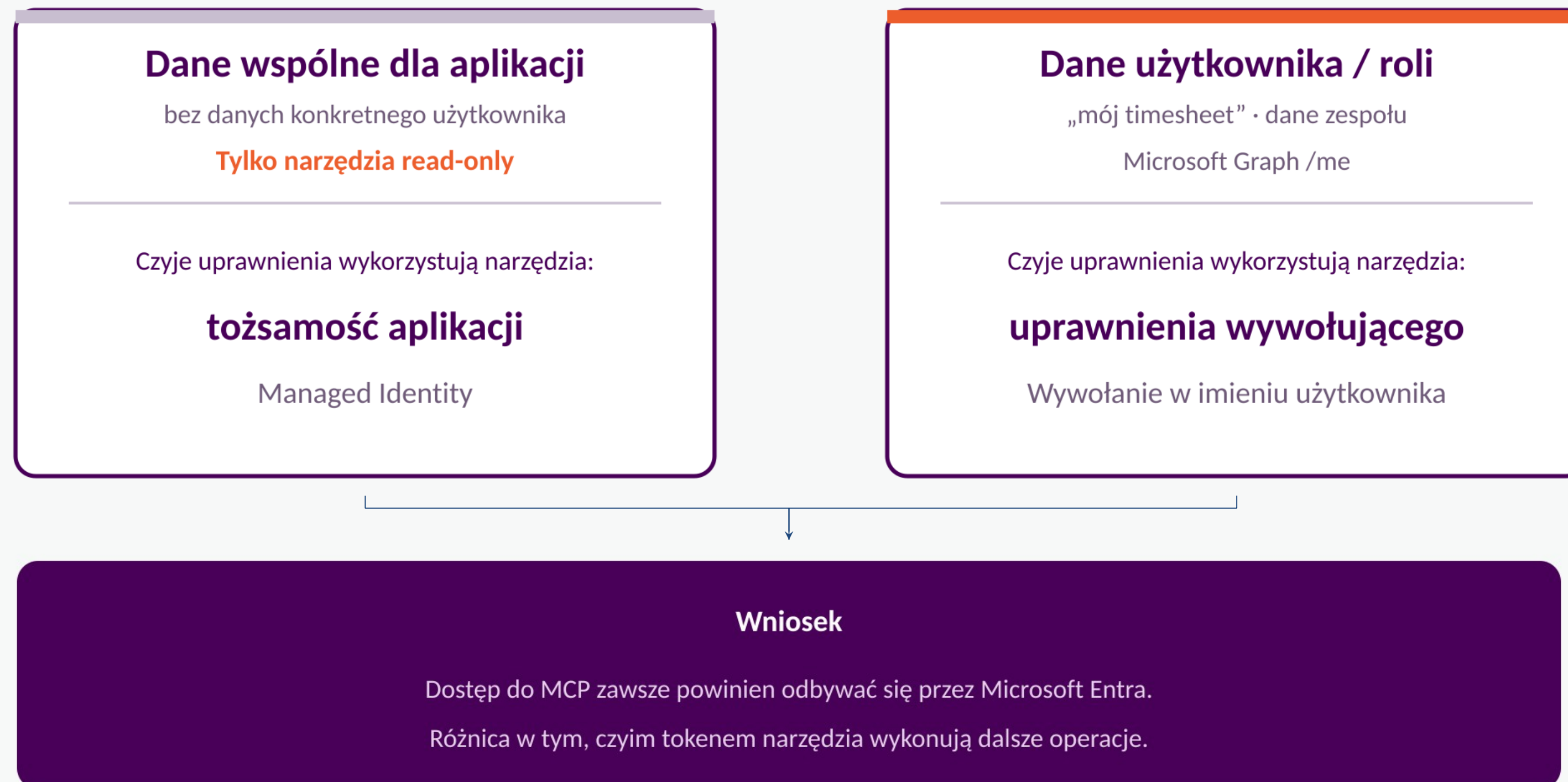
Microsoft Entra ID

Managed Identity, App Registration, RBAC, MS Graph

Virtual Network, Private Endpoint, Inne zasoby sieciowe



Dwa typy narzędzi ≠ te same uprawnienia



Dopasuj tożsamość do zadania

PoC wspólna tożsamość

wszystkie narzędzia
jedna tożsamość na wszystkie wywołania

OK na PoC

Produkcja tożsamość aplikacji + tożsamość użytkownika

narzędzia publiczne + wymagające użytkownika z uprawnieniami
bez tego — aplikacja widzi dane wszystkich
token użytkownika musi dojść do zasobów



Klient

użytkownik + token Entra



MCP na Container Apps

Obsługa uwierzytelnienia i autoryzacji
Logowanie audytowe



Graph / ERP

w imieniu tego użytkownika
On-Behalf-Of (OBO)

Wniosek

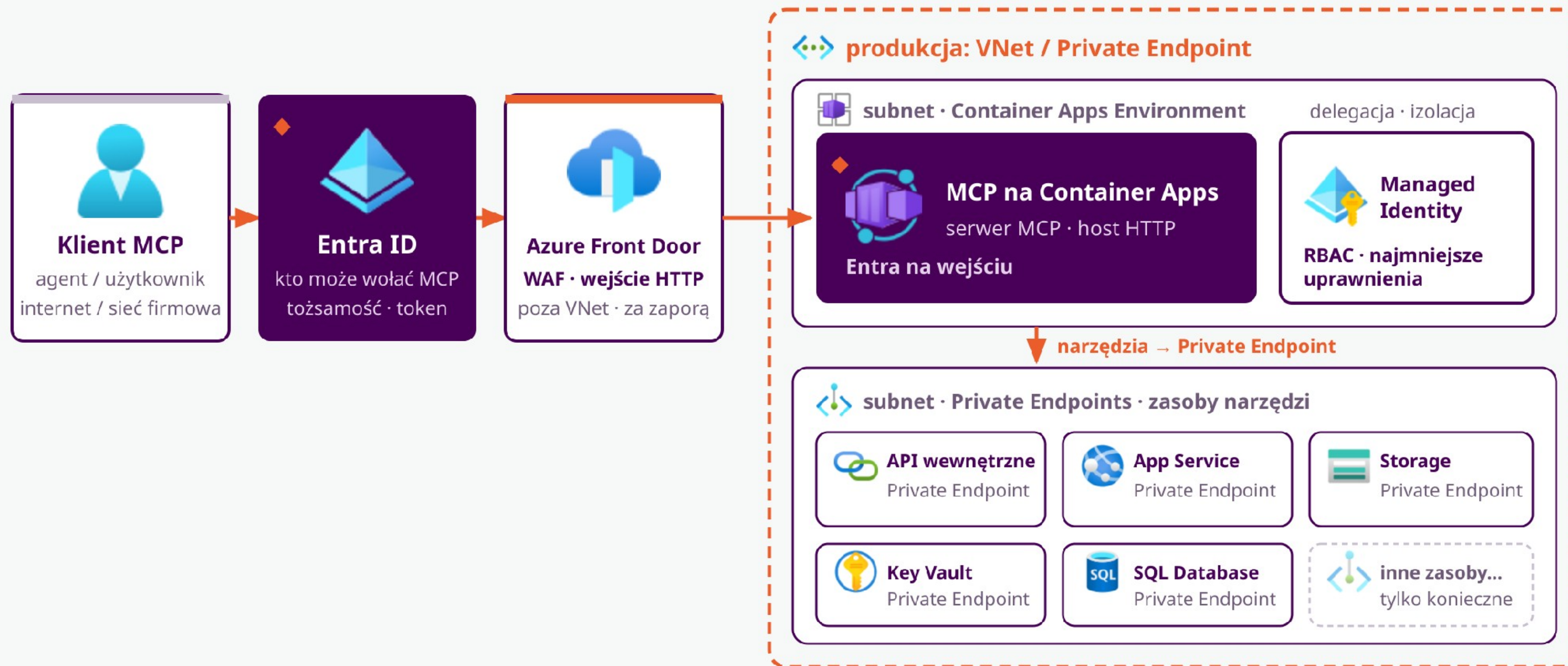
Pass-through = czy użytkownik może użyć danego narzędzia · i kto / kiedy je wywołał (audyt).
Bez tego — stop przed produkcją. Azure: Entra + uprawnienia delegowane



Sieć i dostęp do danych



Całość na Azure



Więc - aplikacja czy warstwa platformy?

Aplikacja

Warstwa platformy

Tożsamość

implementacja w ramach aplikacji

spójna wewnątrz całego produktu

Kontekst

wyizolowany byt + jego bezpośrednie zasoby

cały ekosystem: sieć, inne usługi, izolacja danych i granice dostępu

Odpowiedzialność

zespół zajmujący się aplikacją

wszyscy, którzy dostarczają tooling pod MCP - **także inne usługi**

Zbyt wiele decyzji wychodzi poza pojedynczą aplikację — to warstwa platformy.

O czym nie powiedziałem?

1 Azure API Management

Kiedy MCP stoi za APIM: polityki, limity, ekspozycja narzędzi.

2 Pass-through / On-Behalf-Of

Jak każde narzędzie używa tokenu użytkownika — pełne scenariusze OBO.

3 Observability

Co logujemy i gdzie trzymamy telemetry? Alerty i kiedy odcinać dostęp.

4 Protokół / SDK MCP

Transport, sesje, wersje SDK — jak klient i serwer się dogadują.

5 Łańcuchy agentów

Agent woła agenta (lub narzędzie tworzy kolejnego): czyja tożsamość, czyj token, jak śledzić wywołania.

6 Zaufanie do bibliotek

Skąd biorą się zależności; allowlista; kto odpowiada za kod pod spodem.



Check-lista przed produkcją

1 AuthN / AuthZ
Kto wchodzi do MCP i z jakimi uprawnieniami?
np. Microsoft Entra ID

2 Hosting
MCP u nas — nie na maszynie klienta
np. Container Apps

3 Narzędzia
Jak dzielisz narzędzia — i czyje uprawnienia każde z nich potrzebuje?
np. wspólne vs dane użytkownika

4 Pass-through
Czy token użytkownika dochodzi do zasobów?
np. uprawnienia delegowane / OBO

5 Sieć
Gdzie w ekosystemie stoi MCP i jak sięga do innych zasobów?
np. VNet / Private Endpoint

6 Izolacja
Czy izolujesz tenantów i dostęp do danych?
np. granice Entra + izolacja w systemie

7 Audyt
Kto / co / kiedy przy wywołaniu narzędzia?
np. Azure Monitor (App Insights / Log Analytics)

8 Platforma
Aplikacja czy wspólna warstwa platformy?
np. tożsamość · kontekst · odpowiedzialność



Dodatkowe materiały

Przykłady: github.com/Azkel/azure-ai-platform/



Slajdy: smyk.it/mcp.pdf



Blog: smyk.it



Zachęcam do zadawania pytań - po sesji lub na LinkedInie



ACCELER8IT

by Conlea

Dziękuję za uwagę!

Michał Smyk

smyk.it



WWW.ACCELER8.IT