AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

AGH UNIVERSITY OF SCIENCE
AND TECHNOLOGY

Chmury obliczeniowe

dr hab. inż. Piotr Boryło

12.03.2024

Agenda

- Wprowadzenie, pojęcia, zasady działania
  - Chmura blisko użytkowników
- Kto jest odpowiedzialny za bezpieczeństwo?
- Jak zapewniamy bezpieczeństwo
  - Dobre praktyki i zalecenia
  - Przykłady usług i aplikacji
- Dyskusja

Definicja

» Wszystko dotyczy jedzenia ☺

» W domu vs. w restauracji

http://www.telegraph.co.uk/travel/destinations/asia/india/articles/Indian-food-a-regional-tour-of-the-countrys-best-curries/

Infrastructure as a Service (IaaS)

- Samoobsługa
- Samemu trzeba zadbać o wszystkie komponenty
- Elastyczność

https://www.pinterest.com/pin/148196643961912589/

Platform as a Service (PaaS)

- Danie z menu
- Zestaw zintegrowanych komponentów
- Zależność od dostawcy

https://wall.alphacoders.com/big.php?i=327004

Software as a Service (SaaS)

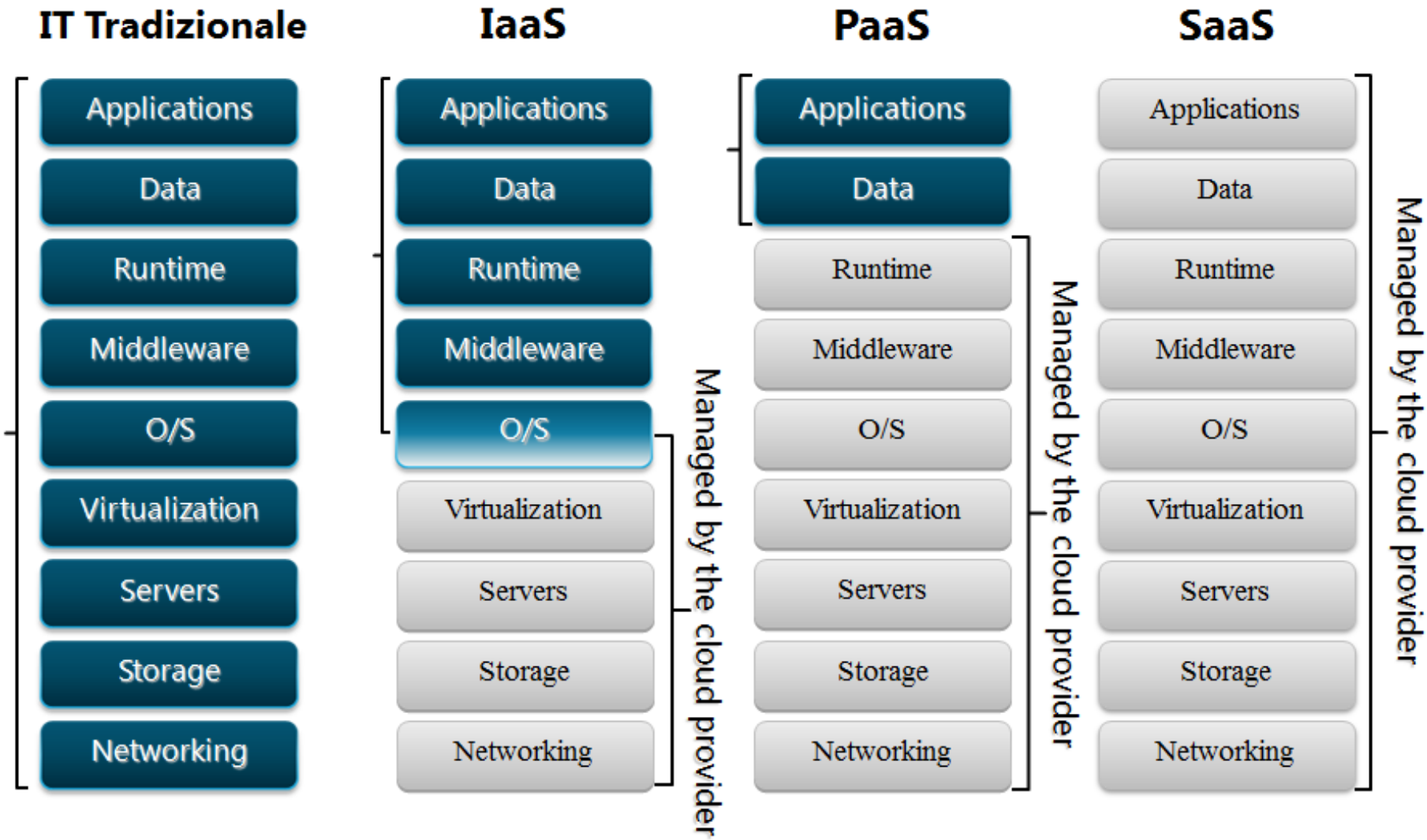
- Menu na zorganizowanym przyjęciu
- Rozwiązanie kompletne
- Ograniczony wybór

https://s-media-cache-ak0.pinimg.com/736x/9e/0a/fc/9e0afcf40afba074e7b0ff6859e01e70.jpg

Pizza as a Service

http://www.episerver.com/blog/blog-start/fred-bals/pizza-as-a-service/

Modele świadczenia usług



http://vinfrastructure.it/2013/07/iaas-vs-paas-vs-saas/

Rodzaje chmur obliczeniowych

- Prywatne
- Publiczne
- Hybrydowe

- Jak się mają rodzaje chmur do modeli świadczenia usług

Zalety

- Nie jest potrzebny know-how w zakresie budowania centrów danych
- Skalowalność i koszty proporcjonalne do zapotrzebowania
- Niezawodność
- Automatyzacja
- Efektywność kosztów… **na pewno?**

Wady

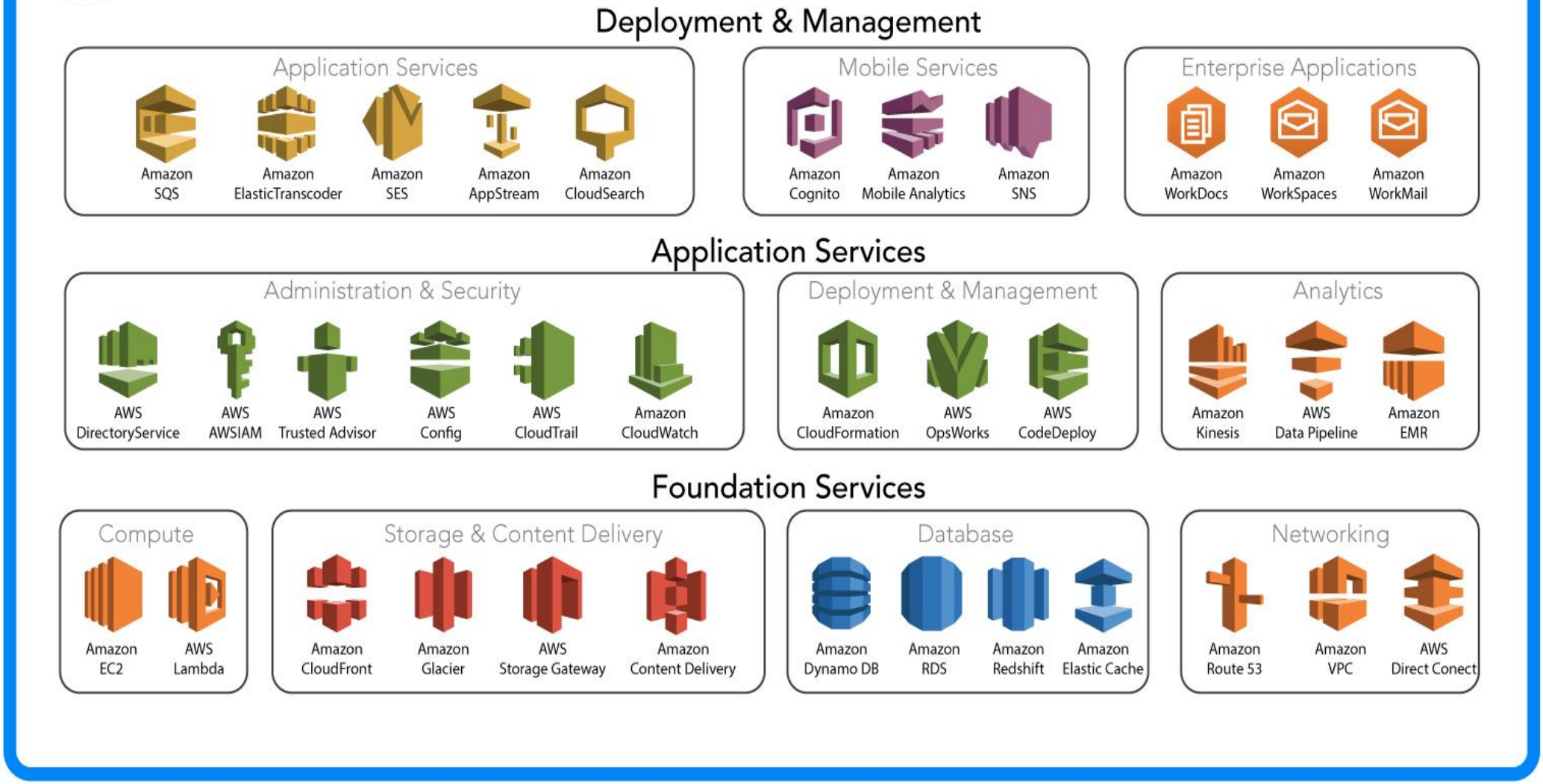
- Bezpieczeństwo
- Regulacje prawne
- Wydajność
  - Zdalny dostęp
  - Współdzielenie zasobów
  - Sprzęt ogólnego zastosowania

Operatorzy chmury publicznej

Google Cloud Platform

Microsoft Azure

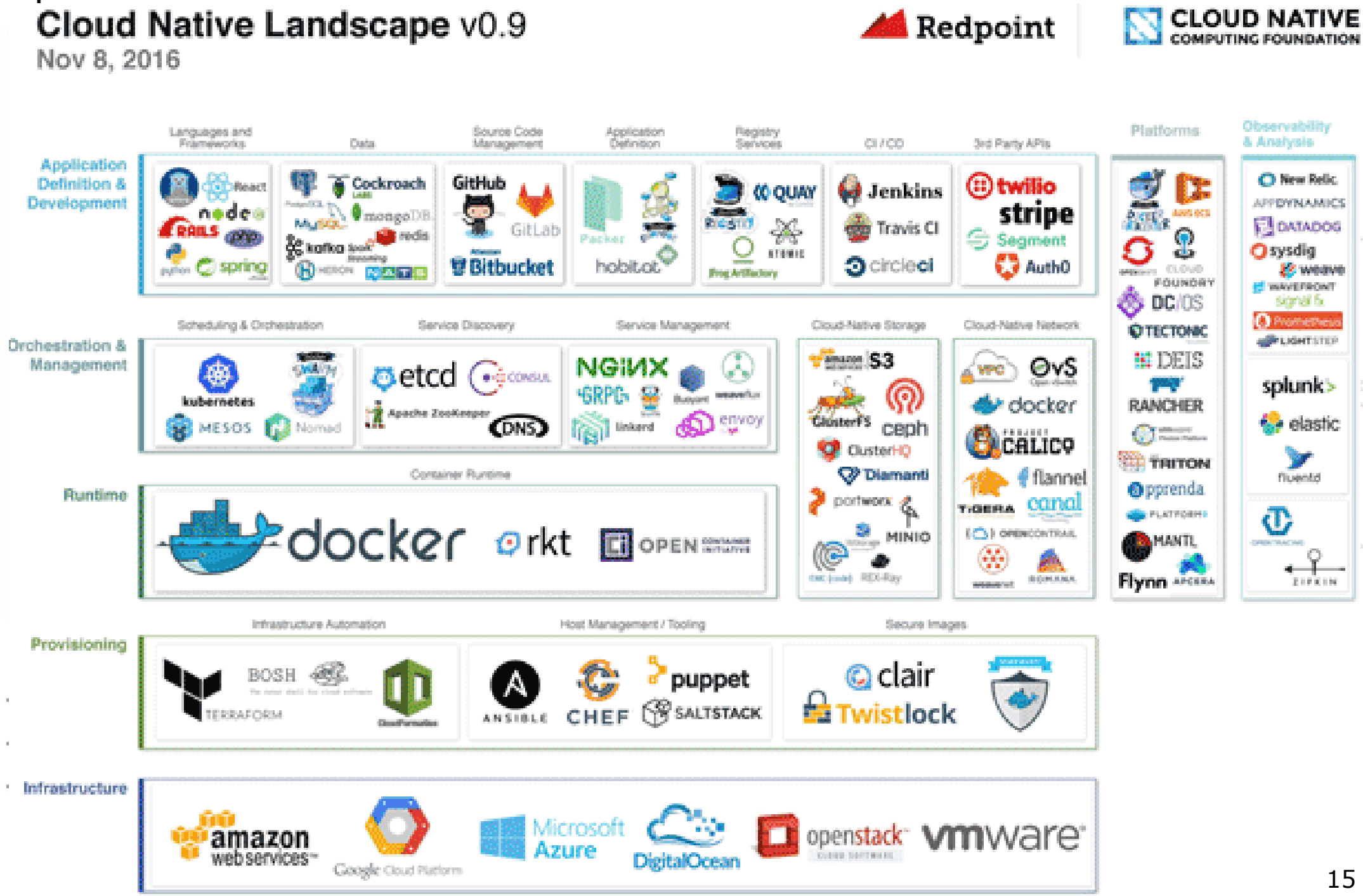
AWS Services



http://www.javamad.com/2021/03/amazon-web-services.html

Wirtualizacja vs. chmura

- Definicja wirtualizacji
- Co wirtualizujemy?
- Po co wirtualizujemy?
- Czy chmura może istnieć bez wirtualizacji?



https://www.quora.com/What-is-the-future-scope-of-Linux-Unix-administration-as-a-career-in-India-How-can-one-find-a-job-in-the-same-as-a-fresher-And-what-are-some-similar-alternate-domains

Chmura blisko użytkownika

- Mgła obliczeniowa
  - Fog Computing (Cisco)
  - EdgeComputing (Akamai)
  - Intel's Intelligent Edge
  - Microsoft's Cloudnet
- Zastosowania?
  - Inteligencja w usługach
  - Zależność od lokalizacji
  - Rozproszenie geograficzne
- Mgła vs. IoT

Mgła obliczeniowa – wyzwania

- Heterogeniczne zasoby
- Mobilność
- Chwilowa niedostępność zasobów
- Zachowanie złośliwe
- Drenaż baterii
- Unifikacja zarządzania
- Kwestie prawne

Bezpieczeństwo

- Trudno znaleźć pierwsze i wiarygodne źródło podające kompletna definicję
- Z syntezy wielu przyjmijmy

Bezpieczeństwo – zdolność do ochrony informacji, systemów i infrastruktury z równoczesnym dostarczaniem wartości biznesowej

Bezpieczeństwo

» Czy to jest definicja w jakiś sposób specyficzna dla chmury?

Bezpieczeństwo – zdolność do ochrony informacji, systemów i infrastruktury z równoczesnym dostarczaniem wartości biznesowej

Bezpieczeństwo chmury

Bezpieczeństwo **chmury** – zdolność do ochrony informacji **przechowywanych w chmurze**, systemów **uruchamianych w chmurze** i infrastruktury **chmury** z równoczesnym dostarczaniem wartości biznesowej **za pośrednictwem chmury**

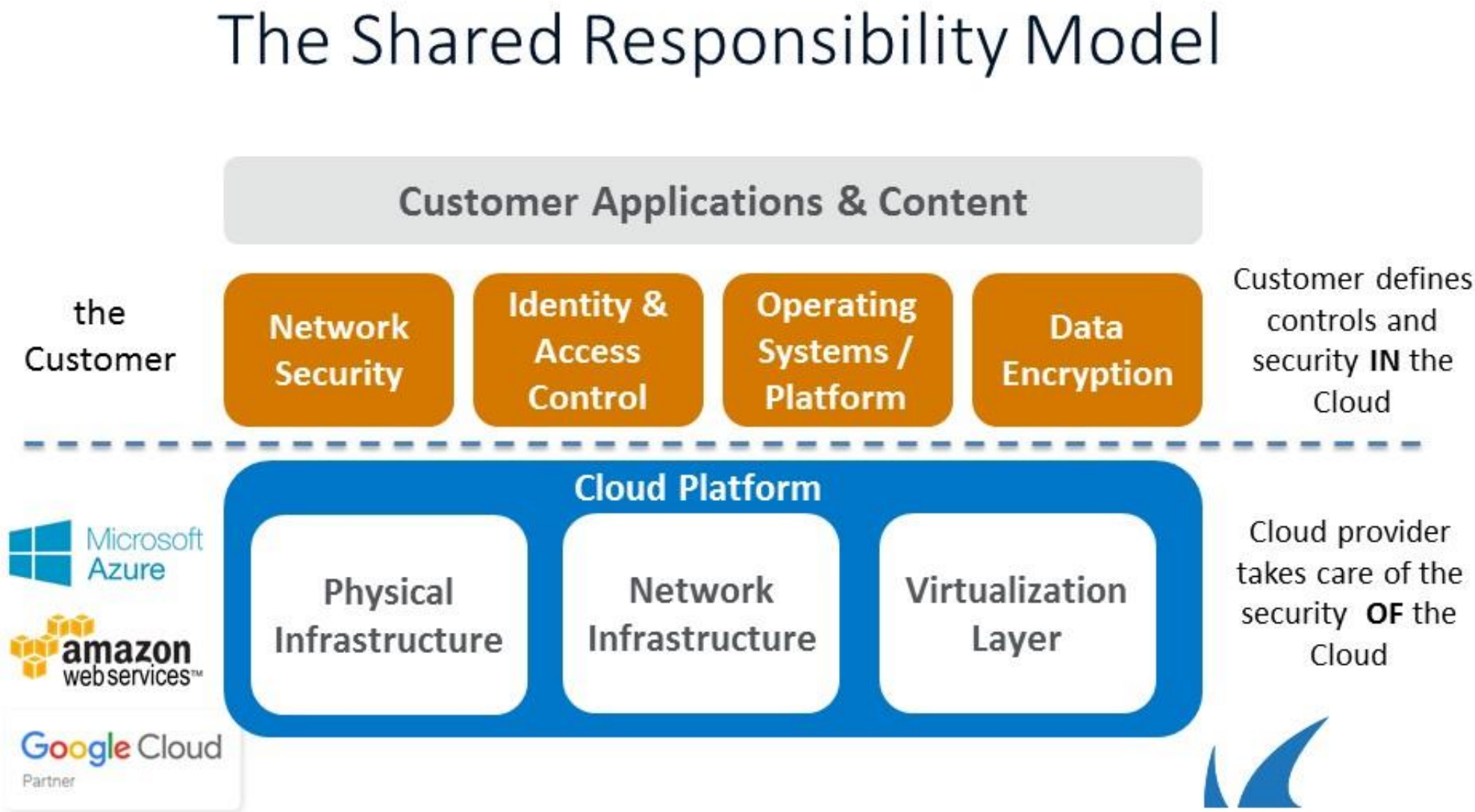
Kto jest odpowiedzialny?

- Kto może być odpowiedzialny?
  - Operator
  - Klient
- Kto jest odpowiedzialny?
- Jakie są wymiary bezpieczeństwa
  - Bezpieczeństwo chmury
  - Bezpieczeńtwo w chmurze

Kto jest odpowiedzialny?

- Jakie są wymiary bezpieczeństwa
  - Bezpieczeństwo chmury
  - Bezpieczeńtwo w chmurze
- Kto jest odpowiedzialny za który wymiar?
- Skupimy się przede wszystkim na wymiarze dotyczącym użytkownika
- Bepieczeństwo chmury poglądowo teraz

Kto jest odpowiedzialny?



https://smartermsp.com/ask-msp-expert-important-secure-public-cloud/

Bezpieczeństwo chmury

- Operator jest odpowiedzialny za wszystko co niezbędne by dostarczyć klientowi usługi w sposób bezpieczny
  - Infrastruktura fizyczna
  - Sprzęt
  - Oprogramowanie
  - Sieci

Bezpieczeństwo chmury

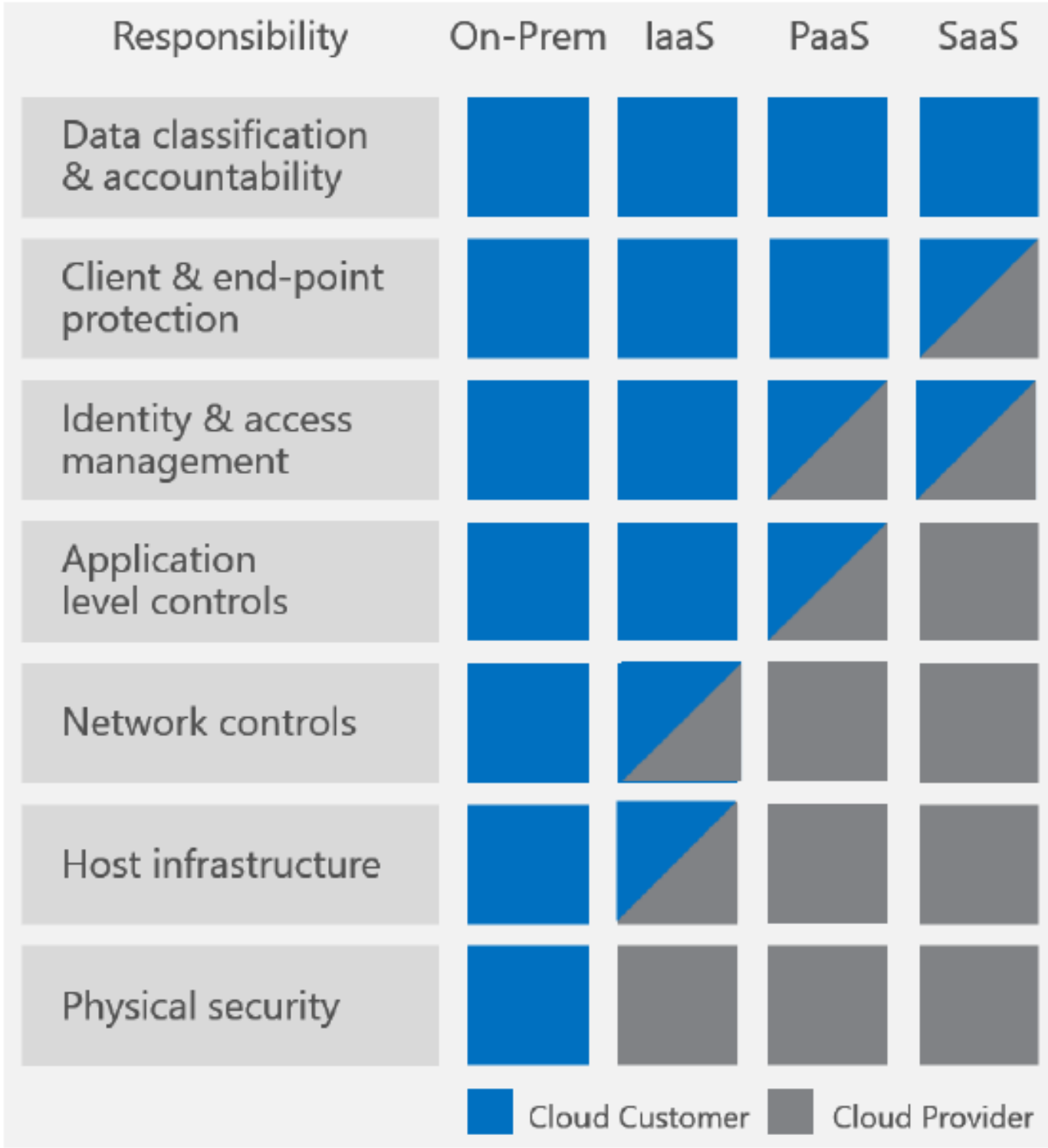
- Technicznie – wszystko co poniżej poziomu nadzorcy wirtualizacji
- Dodatkowo i opcjonalnie:
  - Certyfikacja i atesty pozyskiwane od zewnętrznych instytucji i urzędów
  - Poświadczenia dla użytkownika
  - Publikacje informacji na temat bezpieczeństwa

Bezpieczeństwo w chmurze

- Główna tematyka tego wykładu
- Użytkownik jest odpowiedzialny za swoje zasoby w chmurze, np.
  - Szyfrowanie danych
  - Systemy operacyjne
  - Sieć (zapory sieciowe)
  - Aplikacje
  - Konta użytkowników
  - Publikowane treści

Bezpieczeństwo w chmurze

- Poziom wymaganego zaangażowania zależy od model w jakim korzystamy z chmury
  - IaaS
  - PaaS
  - SaaS
- W którym modelu użytkownik ponosi największą odpowiedzialność?



https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

Najważniejsze komponenty i mechanizmy

- Ochrona infrastruktury
- Uwierzytelnianie i autoryzacja
- Bezpieczeństwo danych
  - Komunikacja
  - Przechowywanie
- Monitoring

Uwierzytelnianie i autoryzacja

- Metody uwierzytelniania w chmurze?
  - GUI: login i hasło
  - Konsola: klucze
  - SDK: klucze
- Słabe punkty każdej z metod?
- Możliwości dodatkowych zabezpieczeń?
- Czy któraś jest jedyną słuszną?

Uwierzytelnianie i autoryzacja

- Metody uwierzytelniania w chmurze?
- Słabe punkty każdej z metod?
  - GUI: człowiek
  - Klucze: kradzież, dobrowolne ujawnienie ☺
- Możliwości dodatkowych zabezpieczeń?
- Czy któraś jest jedyną słuszną?

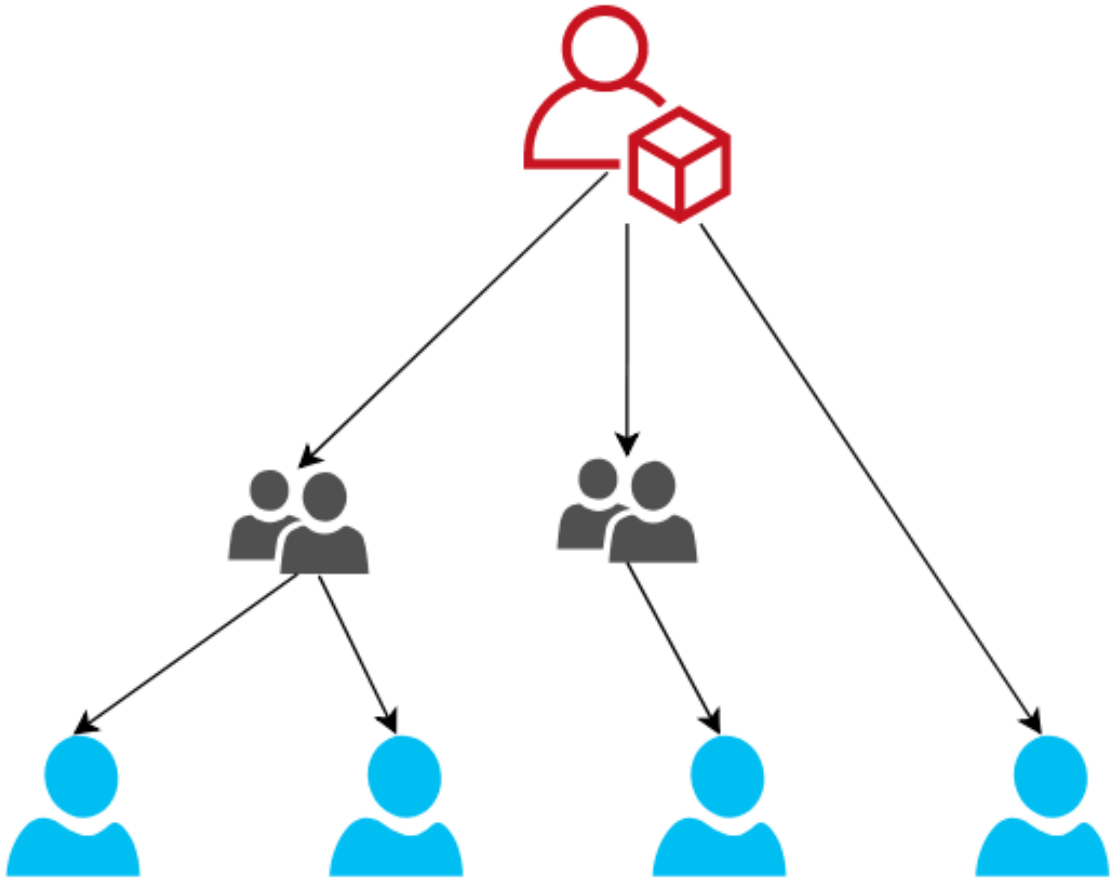
Uwierzytelnianie i autoryzacja

- Metody uwierzytelniania w chmurze?
- Słabe punkty każdej z metod?
- Możliwości dodatkowych zabezpieczeń?
  - MFA
  - Usługi zarządzania kluczami
  - Nadawanie uprawnień aplikacjom
- Czy któraś jest jedyną słuszną?

Uwierzytelnianie i autoryzacja

- *Identity and Access Management*
  - Konta
  - Użytkownicy
  - Grupy
  - Role i uprawnienia
  - Zasoby
- Drobne różnice w nomenklaturze pomiędzy operatorami + ikonografiki ☺

Uwierzytelnianie i autoryzacja

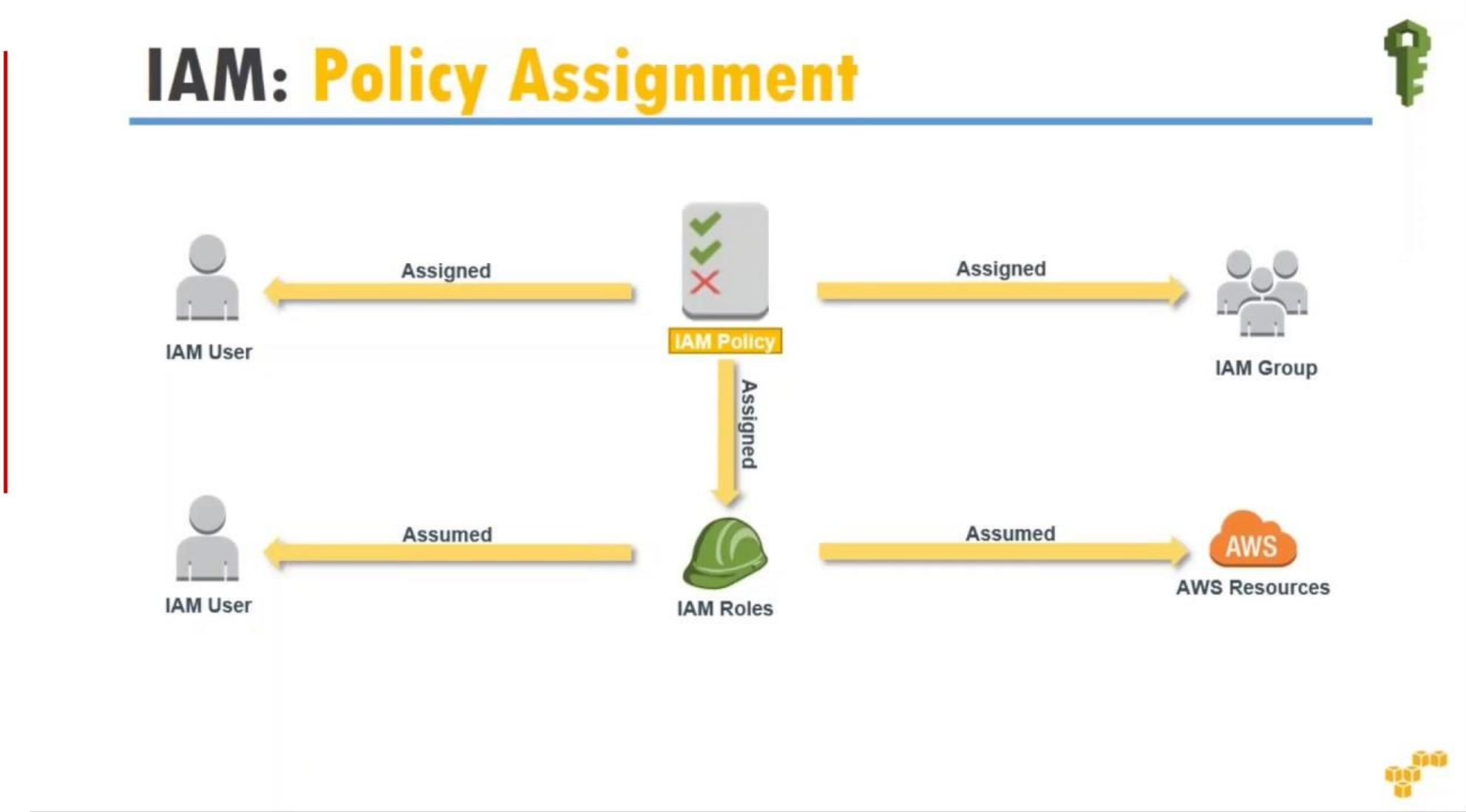


Konto

Grupy

Użytkownicy

Uwierzytelnianie i autoryzacja



https://scriptcrunch.com/aws-certification-iam-essentials-cheat-sheet/

Uwierzytelnianie i autoryzacja

- Dodatkowe ułatwienia w postaci gotowych zestawów uprawnień, np.
  - Dla serwera aplikacji do kontaktów z bazą danych
  - Pobieranie statycznych plików strony www
  - Dla systemu bazodanowego do tworzenia i przechowywania kopii zapasowych bazy

Uwierzytelnianie i autoryzacja

- Dodatkowe ułatwienia w zakresie dystrybucji kluczy i uprawnień
  - Nadanie uprawnień maszynie wirtualnej sprawia, że wszystkie aplikacje działają z takimi uprawnieniami (nie trzeba zapisywać kluczy w konfiguracji)
  - Możliwość tymczasowego przekazania uprawnień, np. admina, bez udostępniania hasła

Uwierzytelnianie i autoryzacja

- Ułatwienia w zakresie lokalnych katalogów użytkowników
  - Przenieś swój katalog do chmury
  - Używaj kont z lokalnego katalogu w chmurze
  - Synchronizuj katalog w chmurze i lokalny
- Uprawnienia tymczasowe per logowanie
- SSO, „zaufane” poświadczenie: FB, Google… ☺

Uwierzytelnianie i autoryzacja

- Dobre praktyki
  - Usunąć klucze dla konta admina
  - Jeden użytkownik – jedno konto
  - Korzystanie z grup
  - Nadawanie jak najmniej uprawnień
  - Wymuszenie silnych haseł + MFA
  - Korzystanie z ról i uprawnień
  - Rotowanie danych logowania
  - Sprzątanie (konta i uprawnienia)

Bezpieczeństwo danych

- W zakresie komunikacji (wymiany danych)
  - *Data in transit*
- W zakresie przechowywania danych
  - *Data in rest*

Bezpieczeństwo danych

- W zakresie komunikacji kwestie bezpieczeństwa rozwiązuje się na kilka sposobów
  - Konfiguracja sieci
  - Zapory sieciowe
  - Szyfrowanie transmisji

Bezpieczeństwo danych

- Konfiguracja sieci
  - Umieszczanie chronionego zasobu w prywatnej sieci
  - Network Address Translation
  - Virtual Private Network
  - Wysoka skuteczność
    - Szczególnie jeśli maszyna jest całkowicie nieosiągalna ☺
  - Niewielka elastyczność konfiguracji

Bezpieczeństwo danych

- Zapory sieciowe
  - Pozwalają filtrować ruch z dokładnością do poszczególnych portów i adresów IP
  - Pewien narzut wydajnościowy i konfiguracyjny
  - Dwa podejścia do realizacji:
    - Klasyczne (DMZ)
    - Zapora dedykowana dla maszyny

Bezpieczeństwo danych

- Szyfrowanie transmisji
  - Korzystanie z bezpiecznych punktów końcowych
  - Przede wszystkim HTTPS uniemożliwia przechwytywanie ruchu

Bezpieczeństwo danych

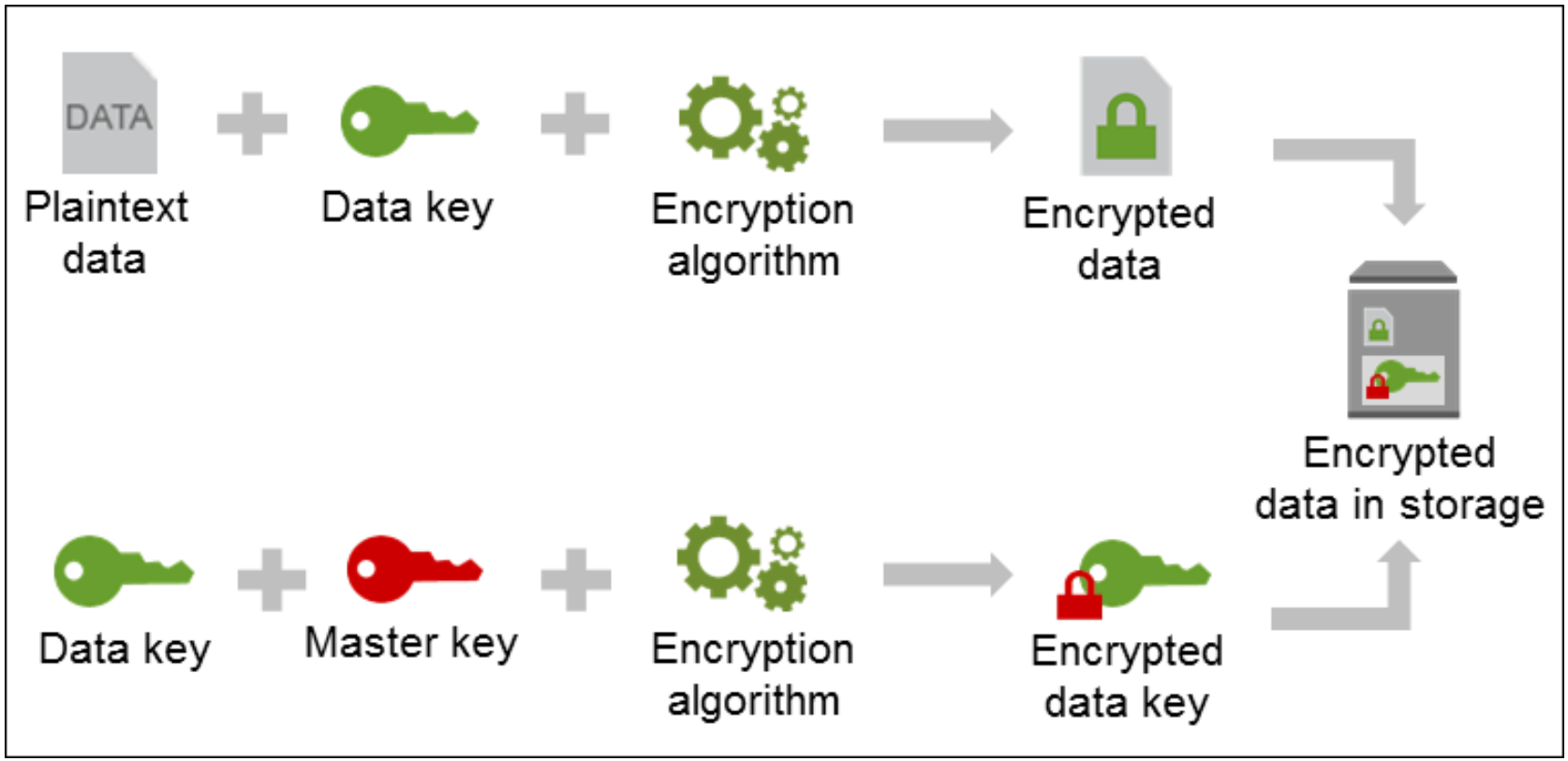
» W zakresie przechowywania danych
  – Klucze symetryczne
  – Hierarchiczne klucze symetryczne
  – Jeden wiodący model implementacji – czyli czym to się różni w chmurze

Bezpieczeństwo danych

- Klucze symetryczne
  - Jak działa klucz symetryczny?
  - Jakie są alternatywy?
  - Dlaczego akurat symetryczny?
  - Dlaczego wady symetrycznego klucza nie są tutaj aż tak istotne?

Bezpieczeństwo danych

» Ogólna zasada działania



https://cloudarchitectmusings.com/2018/03/09/data-encryption-in-the-cloud-part-4-aws-azure-and-google-cloud/

Bezpieczeństwo danych

- Potrzeba istnienia klucza nadrzędnego
- Ale klucz nadrzędny też trzeba bezpiecznie przechować
- Można tak w nieskończoność

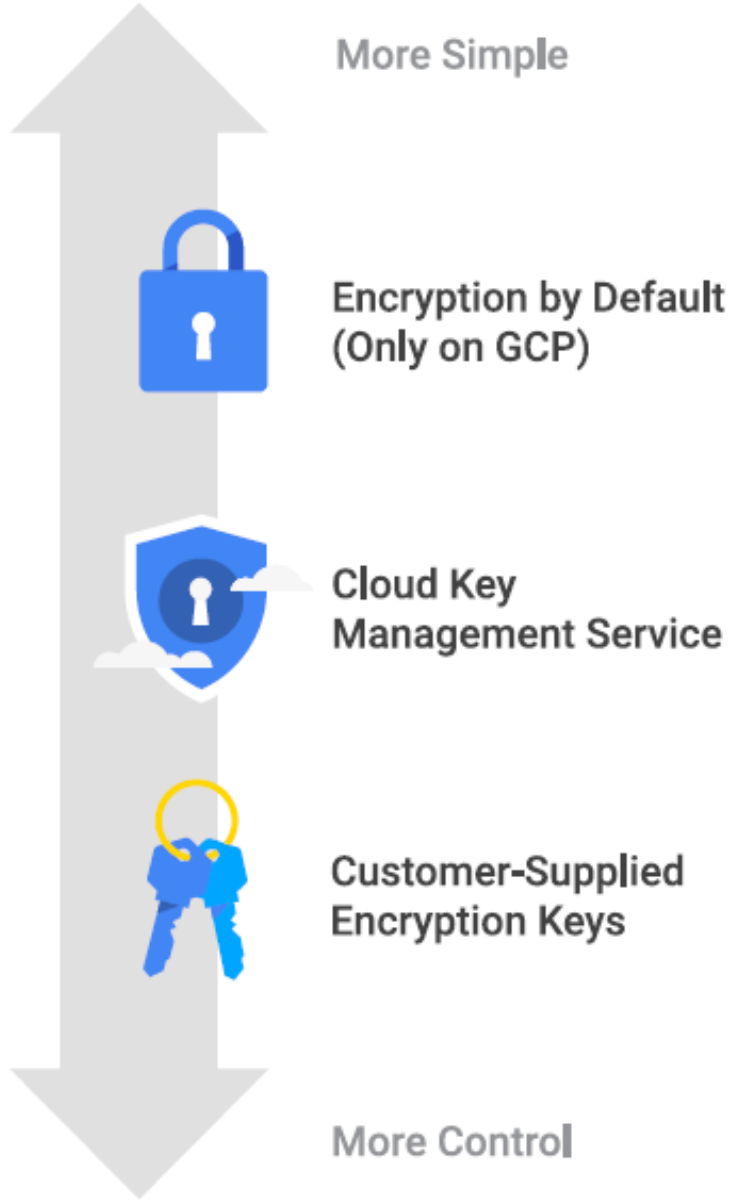
- Rotacja kluczy!

Bezpieczeństwo danych

- Zwykle tylko dwa poziomy zagnieżdżenia
- Klucz danych unikalny dla pojedynczego zasobu
- Klucz główny nigdy nie opuszcza systemu zarządzania kluczami zintegrowanego z innymi usługami

- Ale co to jest system zarządzania kluczami?!

Możliwe podejścia



https://cloud.google.com/security/encryption-at-rest/

Cloud HSM

- Dodatkowy poziom zabezpieczeń
- **Sprzętowe** repozytorium kluczy i prowadzenia operacji szyfrowania
- Odporność wynika z izolacji sprzętowej
- Pomaga spełnić wymagania i normy
- Powszechnie w ofercie dostawców z integracją z systemem zarządzania kluczami

Q&A
Dziękuję za uwagę!

piotr.borylo@agh.edu.pl

12.03.2024