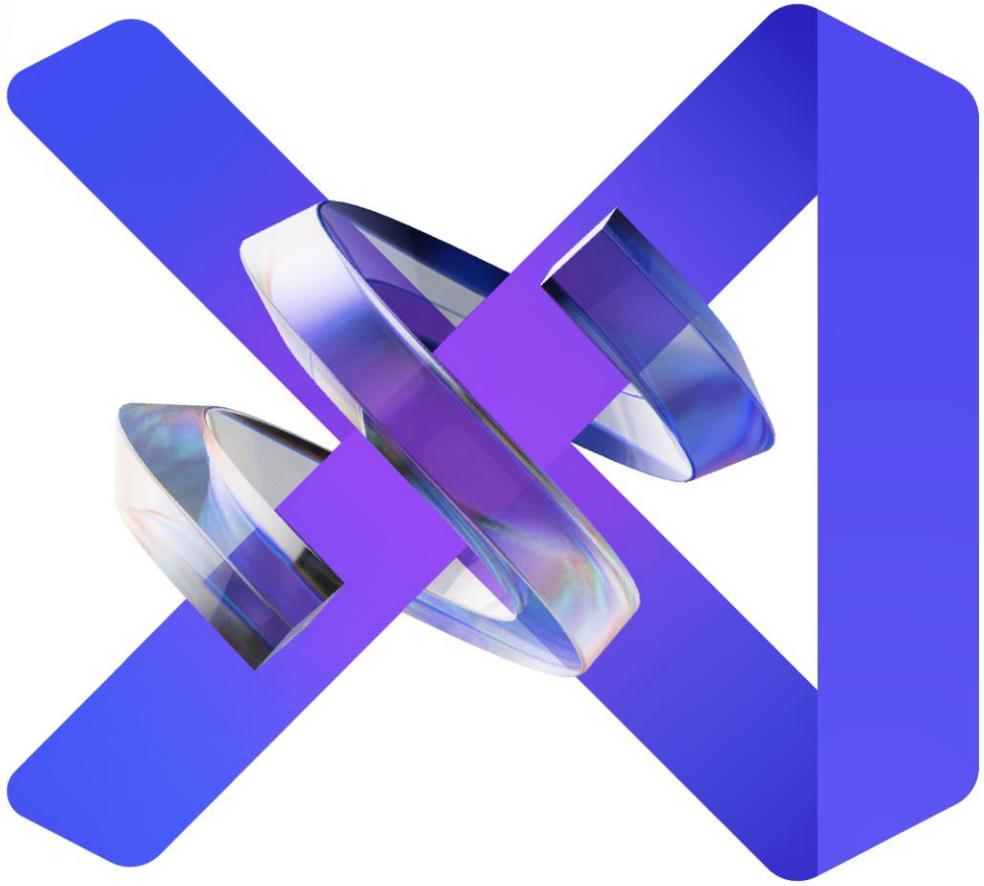
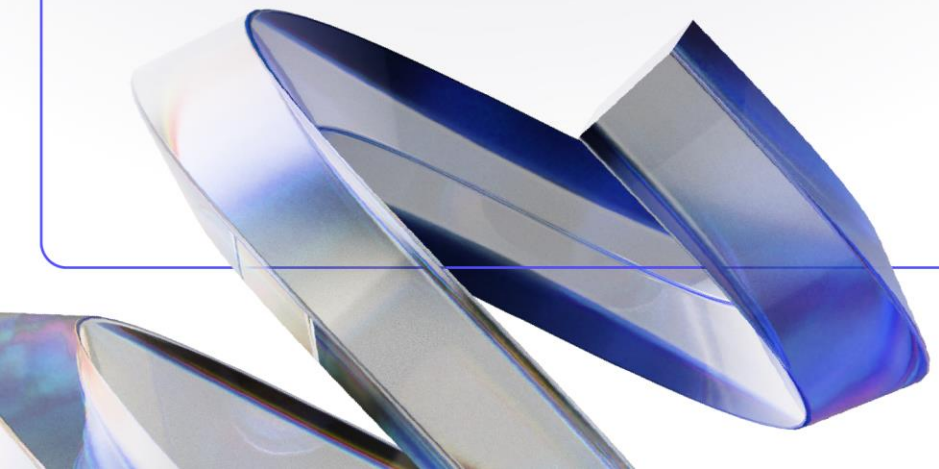
//MSTS/ MS TECH SUMMIT

Czy da się chronić serwer Linuxowy narzędziami Microsoft?

Konrad Sagała
Cloud Security Architect, Alior Bank





Organizatorem wydarzenia jest Fundacja Academic Partners

ACADEMIC PARTNERS

Trochę o sobie

- Cloud Security Architect – Azure/M365
- Microsoft Certified Trainer since 2007
- Microsoft MVP since 2007 – M365 Apps & Services
- Twitter - @sagus
- LinkedIn - @konradsagala
- Github - https://github.com/ksagala
- Blog – https://pepugmaster.blogspot.com
- Hobby – Podróże, Śpiew, Taniec

Agenda

- Wprowadzenie
- SELinux
- Dobre praktyki
- CNAPP, CSPM, CWP
- Defender for Endpoint i Defender for Servers

Wprowadzenie

- „Linux jest bezpieczny”
- „Takie same zabezpieczenie jak w on-prem”
- „Microsoft nie zabezpieczy linuxa”
- „Klucz SSH jest nie do złamania”
- ...

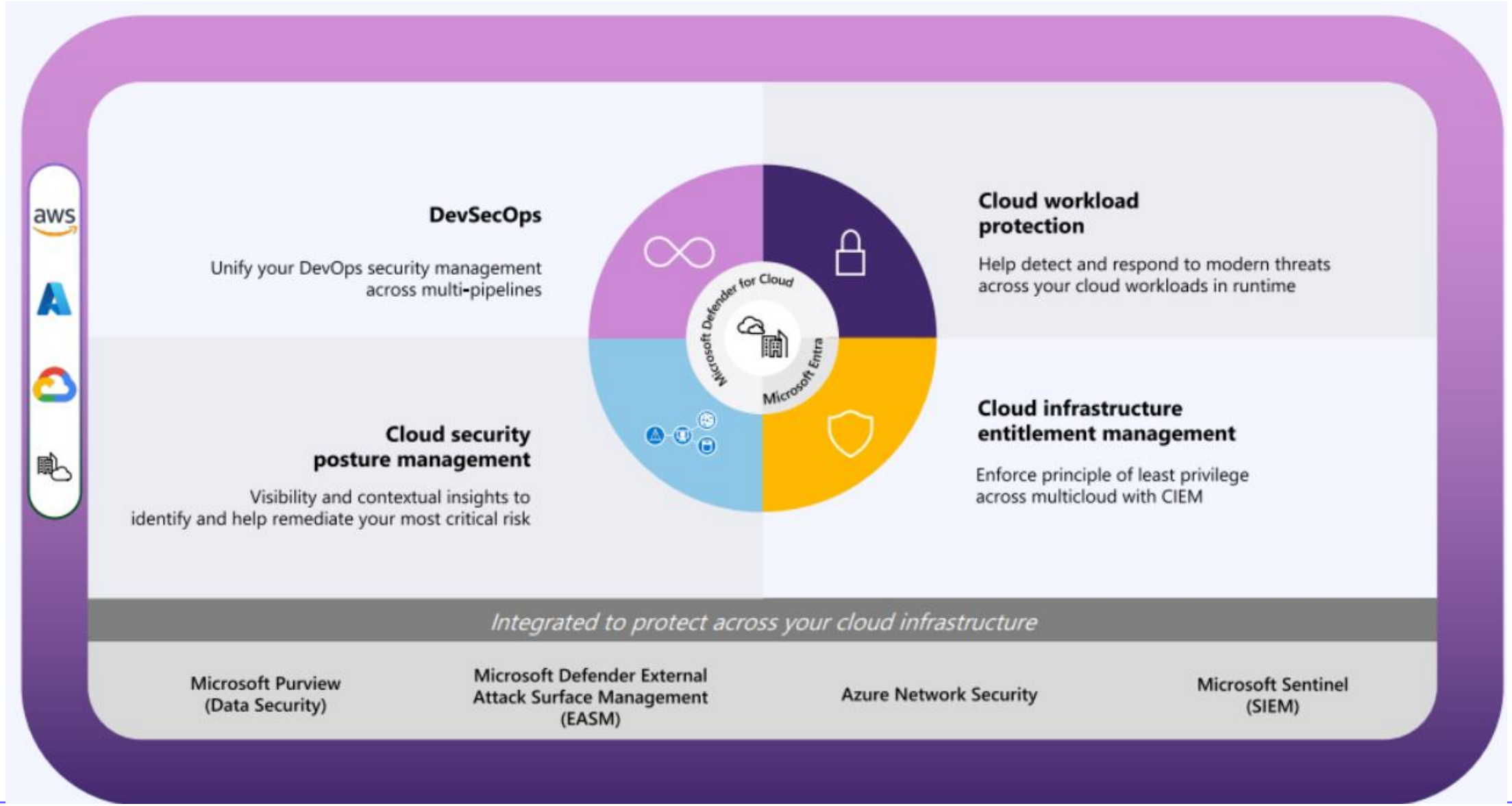
SELinux

- Wiele usług działa w kontekście roota, SELinux kontroluje dostęp nawet roota do naszego systemu
- Początkowo przygotowany przez NSA, jest częścią Red Hata od RHEL 4
- 3 tryby operacyjne:
  - Enforcing (reguły wymuszane, naruszenia logowane)
  - Permissive (bez wymuszenia reguł, naruszenia logowane)
  - Disabled (SELinux wyłaczony, brak logowania)

Dobre praktyki chmurowe

- Minimalizacja uprawnień i regularna ich weryfikacja
- MFA/Just-in-time Access
- Regularne audyty i monitorowanie
- Szyfrowanie danych w ruchu oraz w spoczynku
- Stosowanie dobrych praktyk bezpieczeństwa dla kontenerów
- Monitorowanie podejrzanych zachowań i reagowanie na incydenty
- Regularna aktualizacja systemu i aplikacji
- Ochrona sieciowa

CNAPP = CSPM, CWP, ...



Cloud Workload Protection

Compute: Any server, Azure VMSS, Azure K8s, App Services, Unmanaged K8s

Service layer: Azure DNS, Key Vault, Network Layer V1, Resource Management

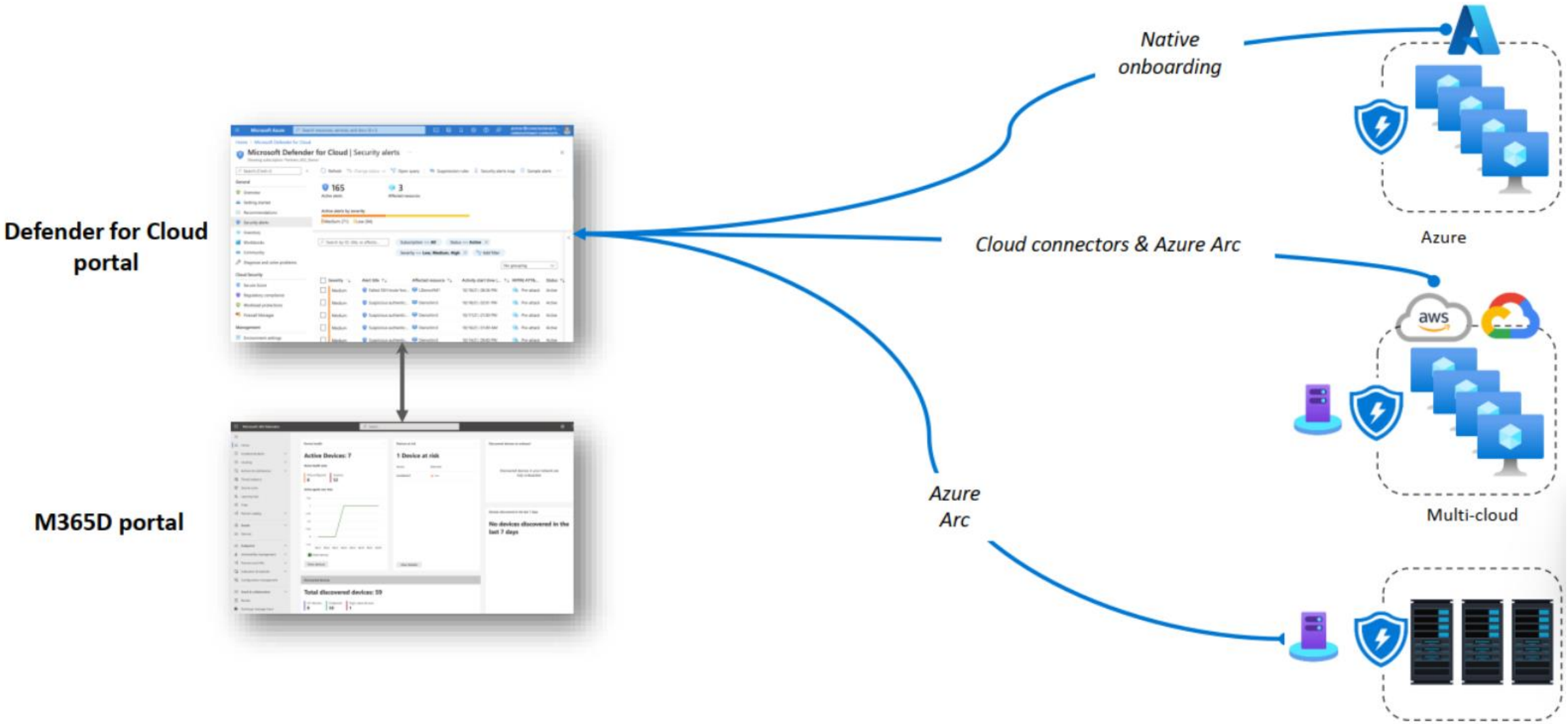
Databases and storage: Blob storage, File storage, Maria DB, Cosmos DB, Azure SQL, MySQL, Postgres SQL, SQL on VM

AWS workloads: Amazon EKS, Amazon EC2, SQL on VM, Unmanaged Kubernetes

GCP workloads: GKE clusters, Google Compute, SQL on VM, Unmanaged Kubernetes

On-premises workloads: Kubernetes, SQL on VM, Servers

Defender for Servers onboarding

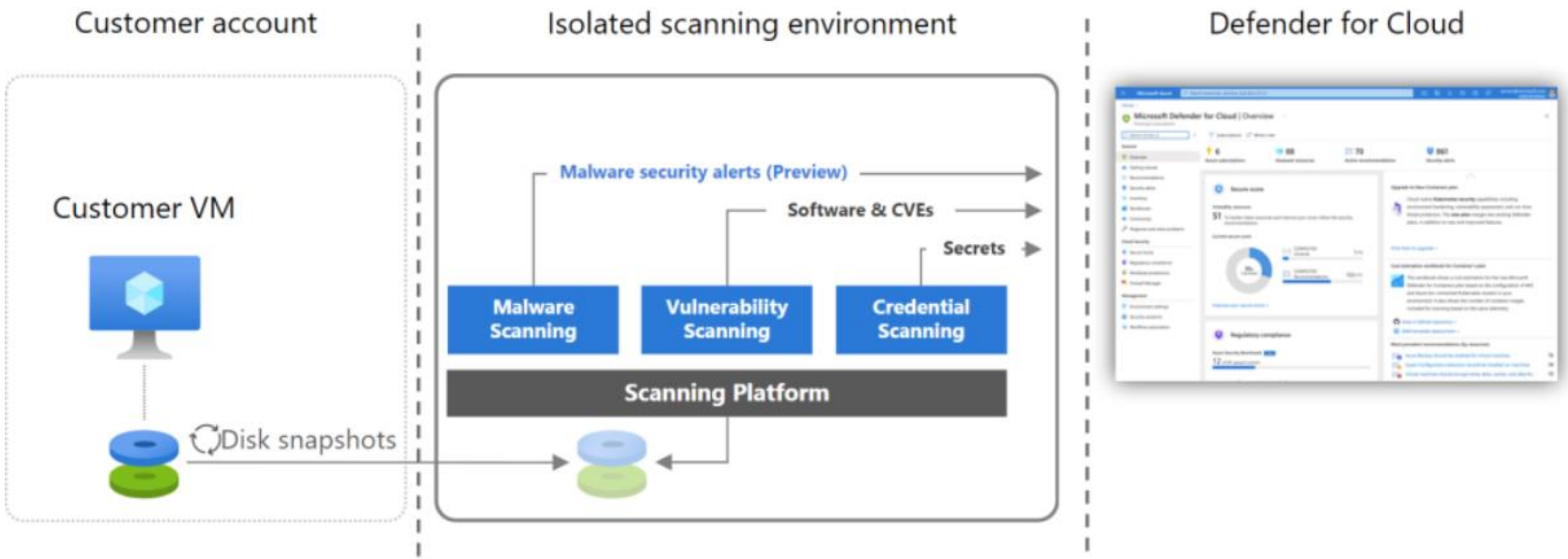


Defender for Servers – wsparcie linuxowe

- Red Hat Enterprise Linux 6.7 or higher (In preview)
- Red Hat Enterprise Linux 7.2 or higher
- Red Hat Enterprise Linux 8.x
- Red Hat Enterprise Linux 9.x
- CentOS 6.7 or higher (In preview)
- CentOS 7.2 or higher
- Ubuntu 16.04 LTS
- Ubuntu 18.04 LTS
- Ubuntu 20.04 LTS
- Ubuntu 22.04 LTS
- Debian 9 - 12
- SUSE Linux Enterprise Server 12 or higher
- SUSE Linux Enterprise Server 15 or higher
- Oracle Linux 7.2 or higher
- Oracle Linux 8.x
- Oracle Linux 9.x
- Amazon Linux 2
- Amazon Linux 2023
- Fedora 33 or higher
- Rocky 8.7 and higher
- Alma 8.4 and higher
- Mariner 2

https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint-linux

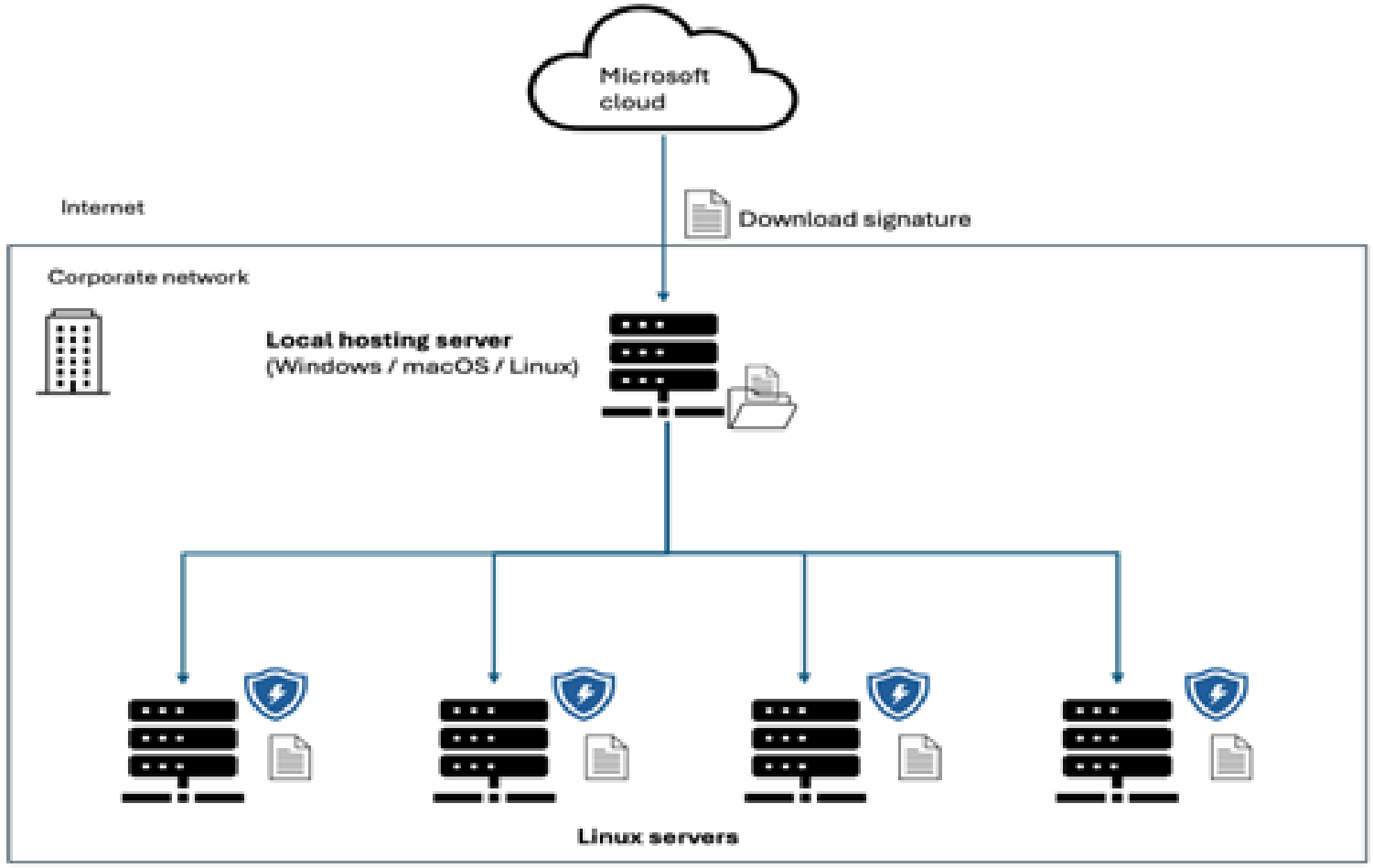
Skanowanie bezagentowe



Ciągły proces usprawniania

- Maj 2023 - MDE direct onboarding
- Lipiec 2023 – informacja o wycofywaniu agenta Log Analytics
- Listopad 2023 – rekomendacje systemowe w ramach Azure Update Managera wchodzą w GA
- Grudzień 2023 – możliwość właczenia Defendera for Servers na pojedynczych VM
- Styczeń 2024 – wycofywanie się z integracji z Qualysem,
- Maj 2024 – zablokowanie możliwości wdrażania Qualysa, przełączenie maszyn na MDVM
- Koniec maja 2024 – preview File Integrity Monitoring
- Koniec czerwca 2024 – FIM w GA, Agentless EDR Discovery również w GA

Aktualizacje offline MDE dla Linuxa



https://learn.microsoft.com/en-us/defender-endpoint/linux-support-offline-security-intelligence-update

//MSTS/ MS TECH SUMMIT

Dziękujemy za uwagę

Zapraszamy do zadawania pytań
oraz oceny wystąpienia pod nagraniem.

//MSTS/ MS TECH SUMMIT

FEEDBACK

Czy da się chronić serwer linuxowy narzędziami Microsoft?

Konrad Sagała

https://mstechsummit.pl/user.html#!/lecture/MSTS24-ba7d/rate