Bezpieczny dostęp do danych wrażliwych w środowiskach hybrydowych i multi-cloud

Radosław Piedziuk

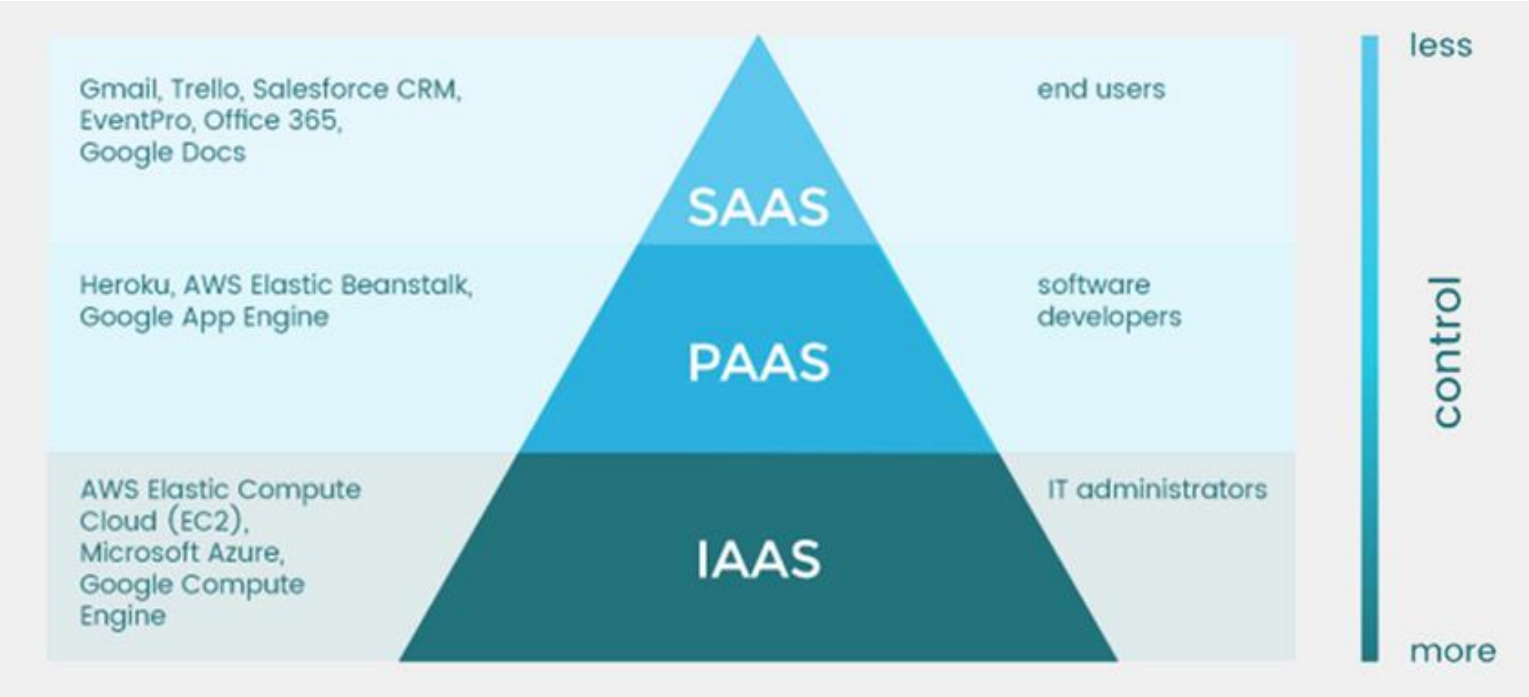
DELL Technologies

Multicloud – wybór tego co najlepsze

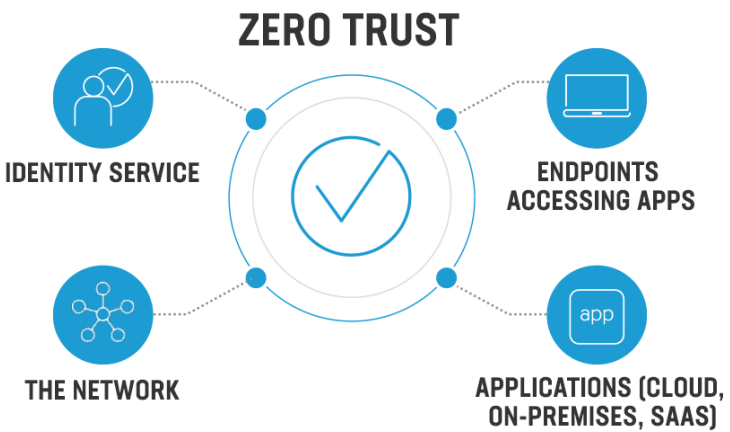
- **Multicloud**

  zakłada wykorzystanie różnych usług/platform zewnętrznych i tworzenie środowiska heterogicznego, żeby zwiększyć możliwości środowiska IT oraz obniżyć koszty.

Multicloud – wiele modeli usług



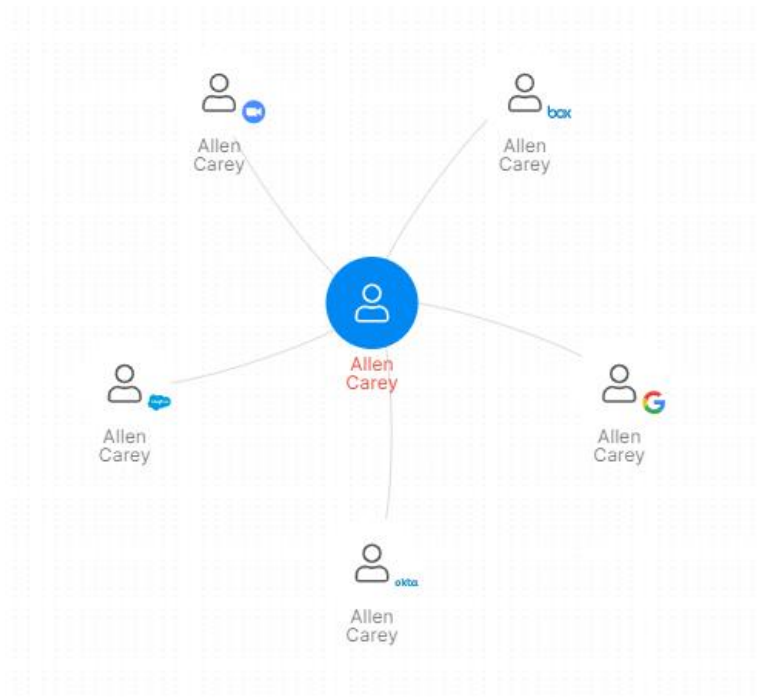
Zero Trust: skuteczna strategia bezpieczeństwa



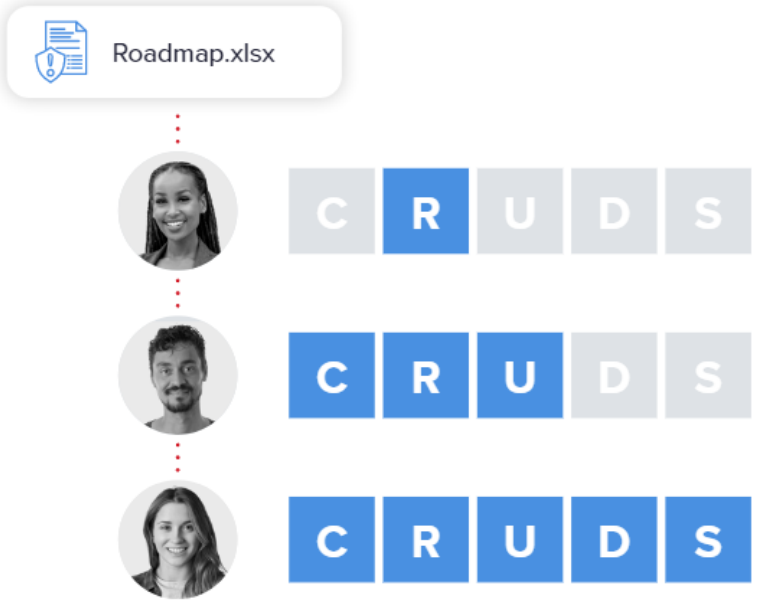
- **Zero Trust:** uprawnienia użytkownika (zaufanie) to najsłabszy element bezpieczeństwa.
- **Dane i cyfrowa tożsamość użytkowników** są w centrum zainteresowania.
- **Kluczowe elementy:**
  1. Chroń dane wrażliwe: zidentyfikuj i ogranicz do nich dostęp
  2. Podziel sieć na segmenty: żeby ograniczyć rozprzeestrzenianie się ataków;
  3. Ogranicz uprawnienia użytkowników;
  4. Zabezpiecz stos aplikacji;
  5. Zarządzaj urządzeniami w sieci.

Mapa powiązań: użytkownicy i usługi

- Powiązanie różnych **kont użytkówników** w ramach usług w **pojedynczą tożsamość cyfrową**
- Ujawnienie kont-cieni (**shadow identities**) wysokiego ryzyka i nadmiernych uprawnieniach
- Bezpieczne **dołączanie** (onboarding) i **odłączanie** (offboarding) użytkowników

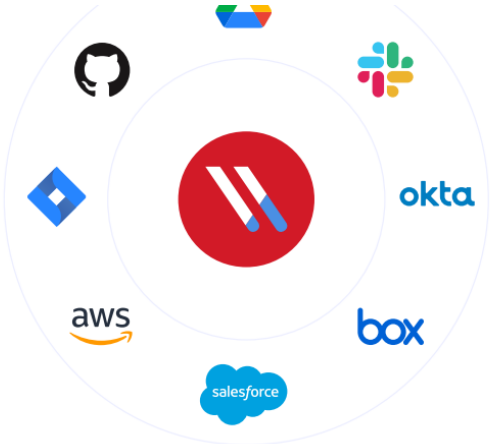


Mapa powiązań: użytkownicy i dane wrażliwe



- Model CRUDS (Create, Read, Update, Delete, Share) pozwala **zwizualizować uprawnienia i ograniczyć ryzyko**.
- Odpowiedzi:
  - Kto ma dostęp do danych wrażliwych?
  - Jaki jest dostęp do danych?
  - Co się dzieje z danymi?
  - Jak były udostępniane?

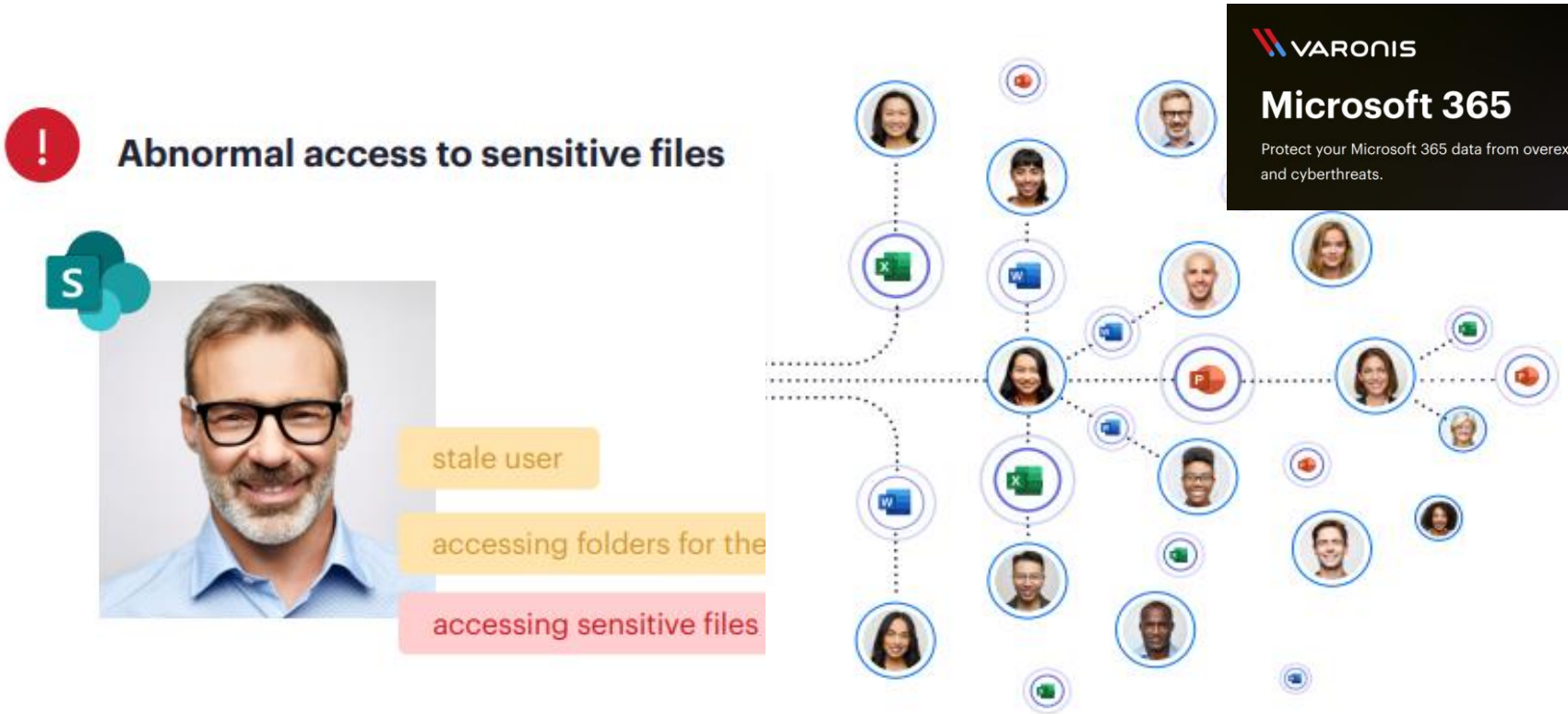
Mapa powiązań: użytkownicy i aktywność



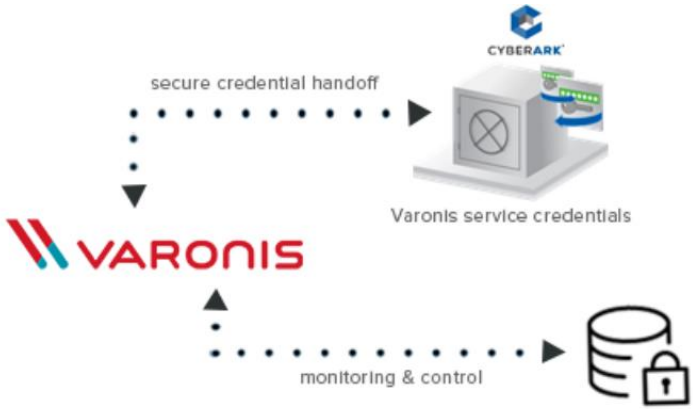
Actor	Service	Type
	Jira	authentication
	aws	access
	okta	user manageme

Insider threat indication: Anomalous number of account records accessed

Mapa powiązań: użytkownicy i aktywność



Zero Trust: bezpieczeństwo jest procesem



- Zasoby lokalne i w chmurze;
- Filtrowanie alarmów (korelacja AI);
- Integracja z ekosystemem bezpieczeństwa SIEM i IM;
- **Realizacja wymogów formalnych: KNF, ISO27001, RODO, itp.**

LogRhythm ArcSight splunk> FireEye Radar


DELL Technologies