

# SOITRON\*

## CyberArk – Privileged Access Management

2019



## História firmy CyberArk

- Založená v roku 1999 v Izraeli – Alon N. Cohen
- Vynašli a patentovali si technológiu digitálneho trezoru
- Najzaujímavejší zákazníci
  - Adobe, Barclays, Deloitte, Duracell, Motorola, Pfizer
- Momentálne zamestnáva približne 1200 ľudí
- Ročná revenue je cca 343 miliónov dolárov (2018)



**CYBERARK**<sup>®</sup>







## Najväčšie riziká:

- neauditovaný prístup k heslám
- používanie rovnakých hesiel  
pre viacero systémov
- nezaznamenávané aktivity
- social engineering
- hackerské útoky



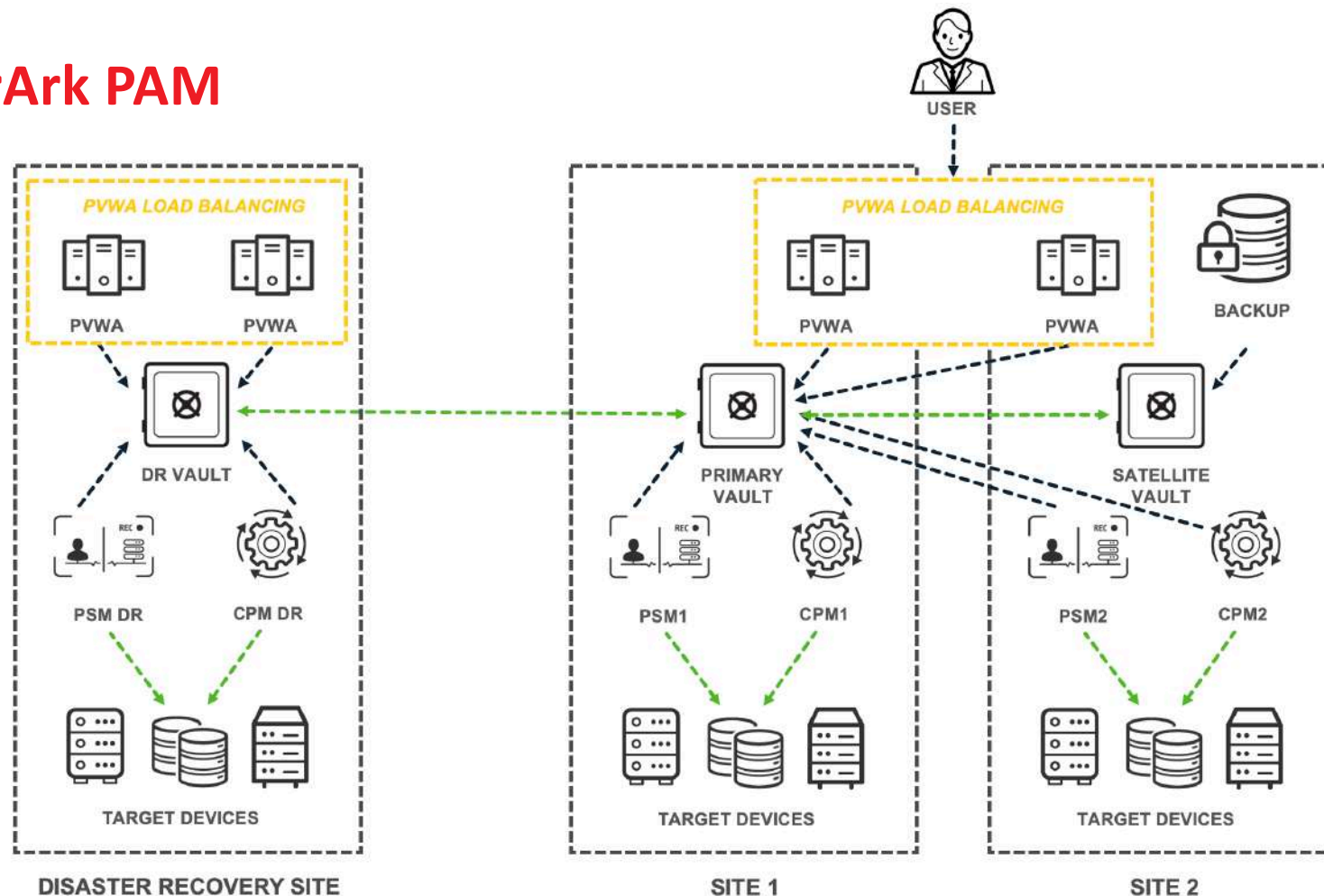
## Najväčšie výzvy:

- bezpečný prístup k heslám 24/7
- prístup offline aj online
- rotácia hesiel
- heterogénne prostredia
- “zero day leavers“
- nájsť to, čo treba naozaj chrániť

# Architektúra riešenia CyberArk PAM

Hlavné komponenty:

- Enterprise Password Vault (HW)
- Password Vault Web Access
- Privileged session manager
- Central policy manager
- Privileged Threat Analytics







## Enterprise Password Vault

- Hardware slúžiaci na ukladanie hesiel, kľúčov a citlivých dát
- Zabezpečený od BIOSu až po aplikáciu
- Proprietárny komunikačný protokol
- Vysoká miera sieťovej izolácie
- Šifrovanie všetkých údajov
- Viacstupňová administrácia (Master, Administrator)
- Privátne kľúče potrebné k chodu systému a správe

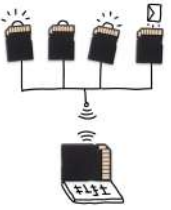


## Password Vault Web Access

- Prístup k účtom cez webový portál
- Správa účtov, sejfov a politik
- Auditovanie prístupov
- Možnosť pripojenia relácie cez web
- Prístup pre externistov

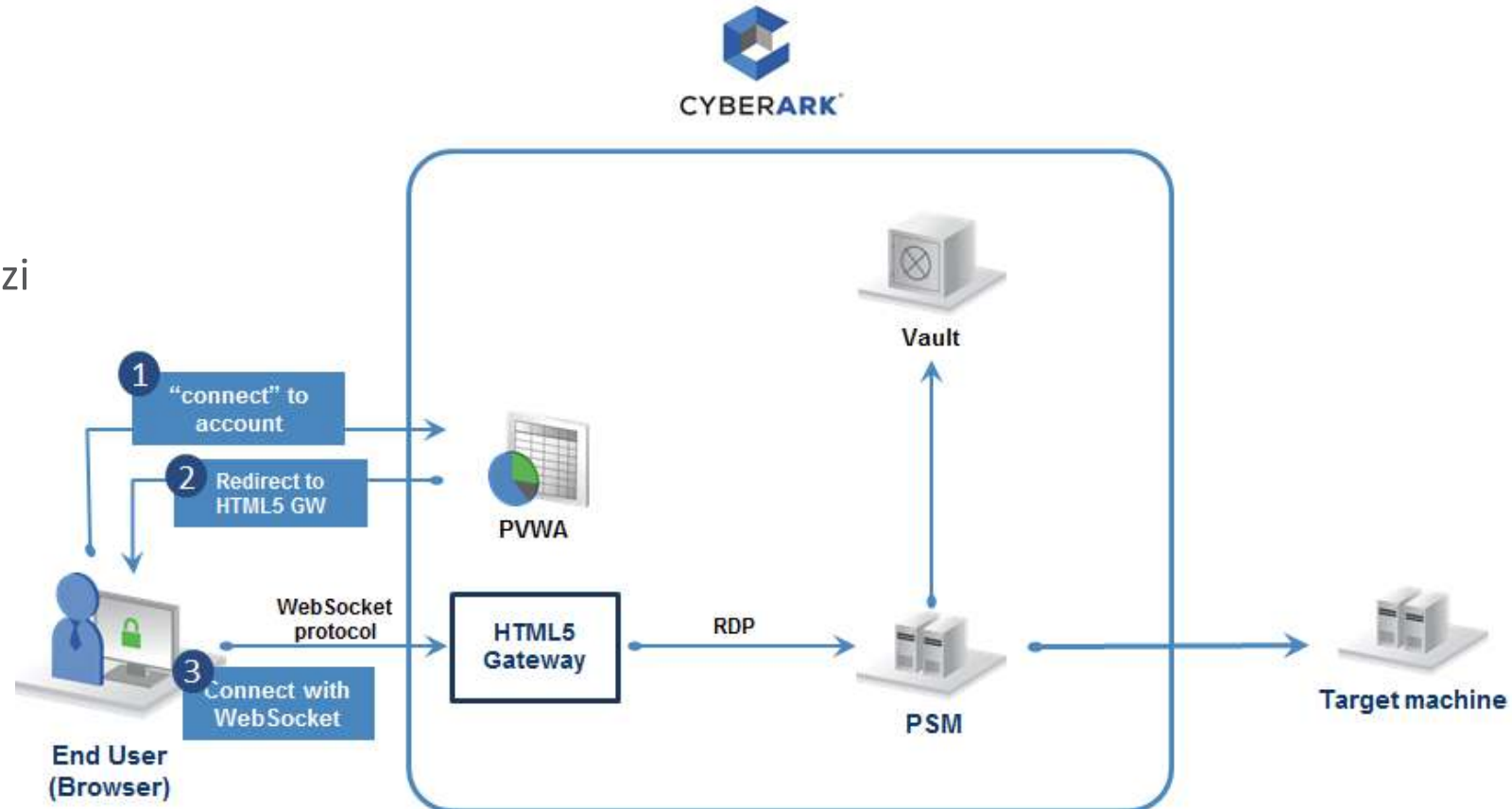
The screenshot displays the CyberArk Password Vault web interface. At the top, the header shows 'CYBERARK' on the left, 'Last sign in: 10/22/2019 | Administrator' in the center, and navigation icons on the right. Below the header is a blue navigation bar with 'Accounts View' and a search box. A table on the left shows search results for 'All accounts' with one entry: 'root' with a status of 'On' and a lightning bolt icon. The main content area shows details for the 'root' account, including 'Platform: Unix via SSH' and 'Safe: VaultInternal'. Below this are tabs for 'Overview', 'Details', 'Activities', and 'Versions'. The 'Overview' tab is active, showing a 'Compliance Status' of 'Compliant' with a '1 Days ago' indicator and a 'Last Verified' status of 'Never Verified Created a day ago'. An 'Activities' section on the right lists five recent actions: 'Administrator Add File Category' on Oct 22, 11:34:04 AM.





## Privileged Session Manager

- Nahrávanie relácií
- Bez nutnosti sieťových prestupov medzi používateľom a cieľovým systémom
- Okrem prístupu cez web podporuje aj putty a RDP



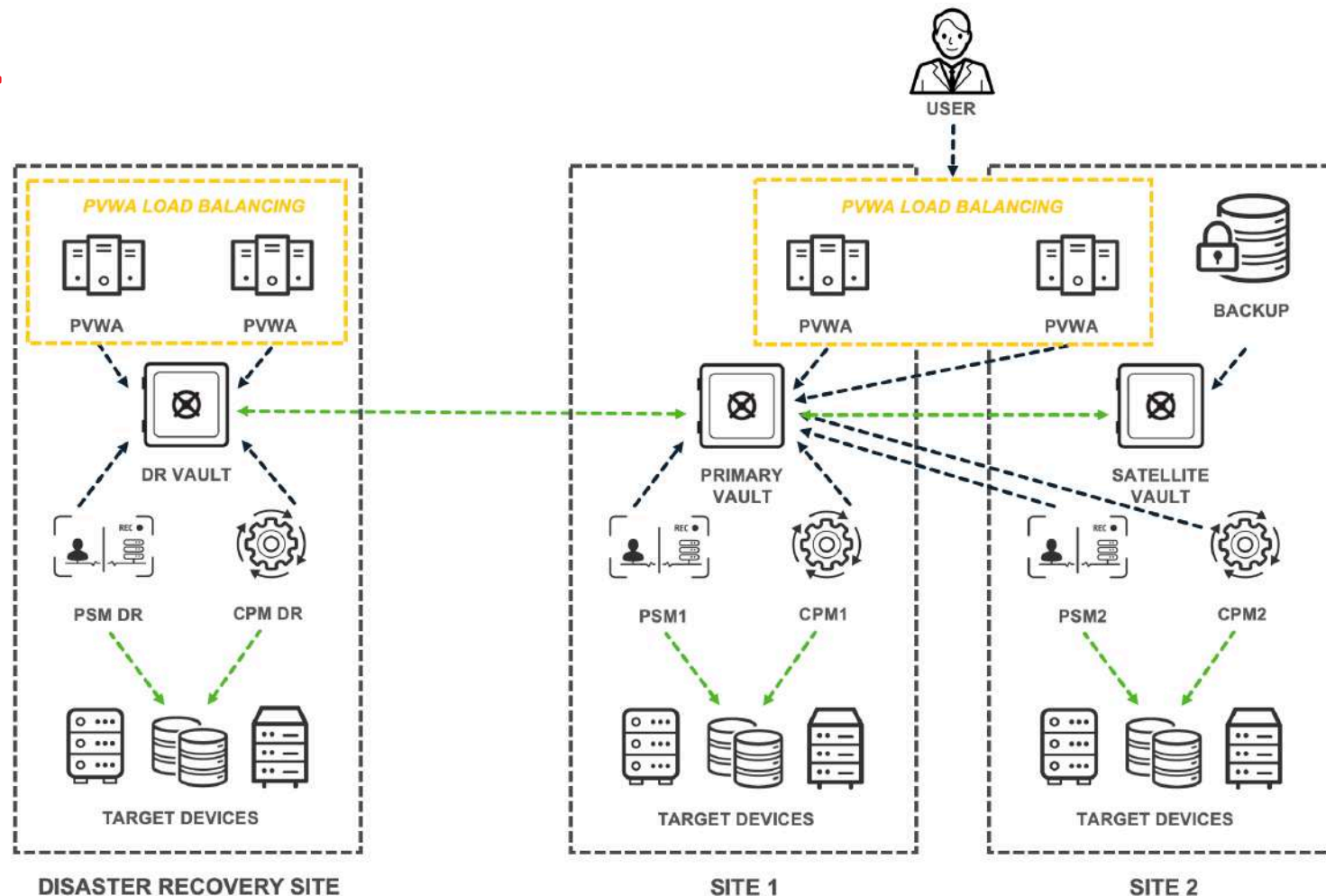
- Možnosť inštalácie viacerých inštancií pre dodávateľov a interných adminov





## Central Policy Manager

- Automatizácia zmeny hesiel
- Prehľad o využití hesiel
- Detekcia rovnakých hesiel
- Aplikovanie bezpečnostných politík pre heslá, a prehľad o ich plnení





## CyberArk Discovery & Audit™

- Identifikácia systémov
- Vyhľadávanie účtov
- Onboarding účtov
- Pravidelné skenovanie nových účtov

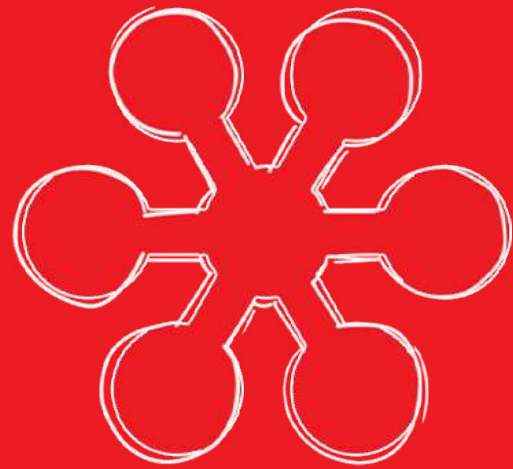


## Implementácia

- Identifikácia cieľov a hlavných požiadaviek
  - Identifikácia kritických systémov s citlivými informáciami
  - Vyhľadávanie privilegovaných účtov a ich kategorizácia
  - Nastavenie priorít na základe DNA a analýzy prostredia
- 
- Na základe predošlých krokov sa vypracuje plán projektu a určí sa potrebná spolupráca od klienta
  - Vypracuje sa architektúra riešenia vzhľadom na požiadavky systému a zákazníka
  - Do systému sú importované konkrétne heslá, do maximálnej možnej miery automatizujeme ich rotáciu a vynucujeme ich bezpečnostnú politiku
  - Nasadia sa nástroje pre zabezpečenie a zaznamenávanie relácii a nástrojov pre jednoduchý prístup a správu k produktu







**ĎAKUJEME**