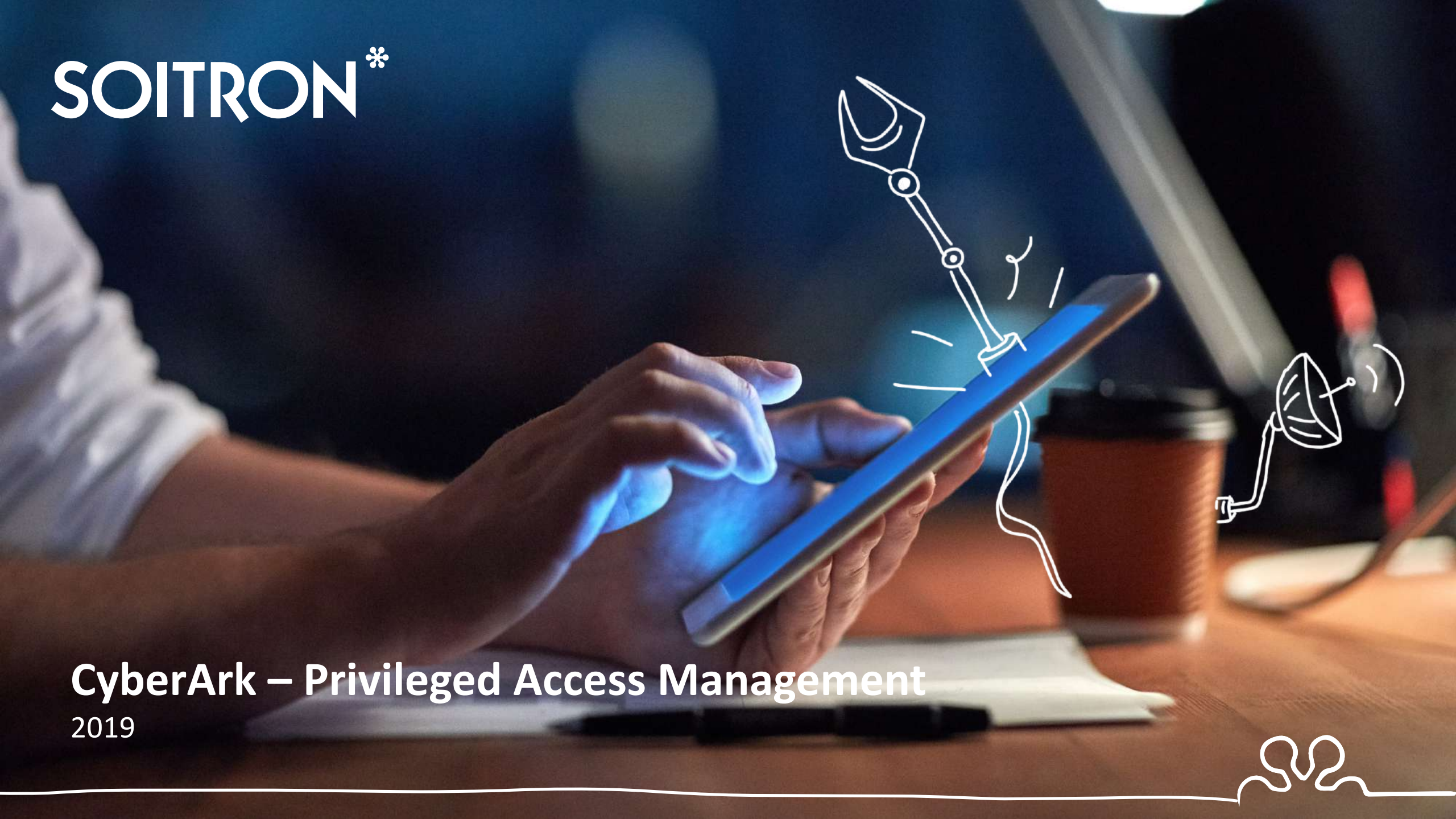
SOITRON



# 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)

## 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

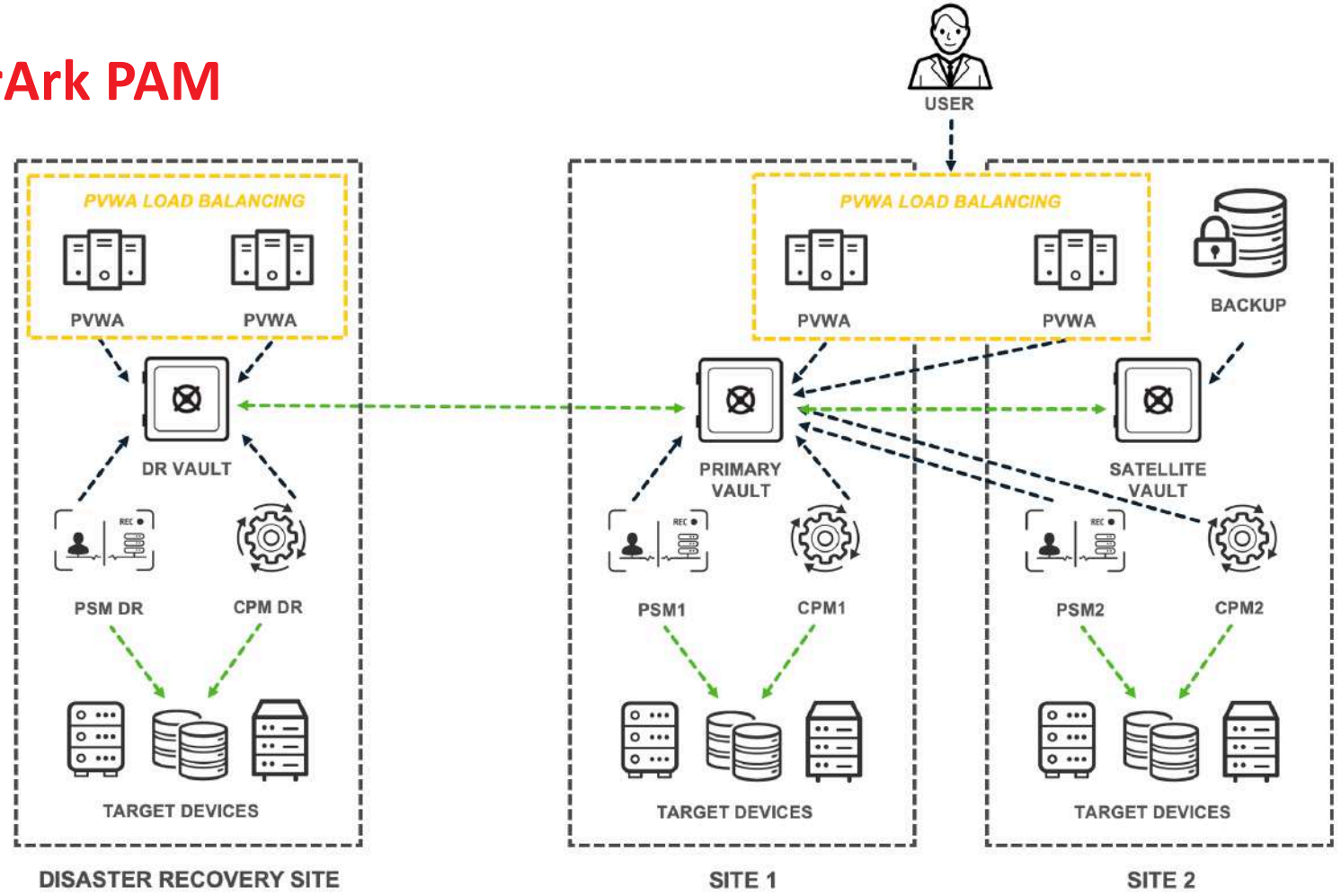
- “zero day leavers“

- 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

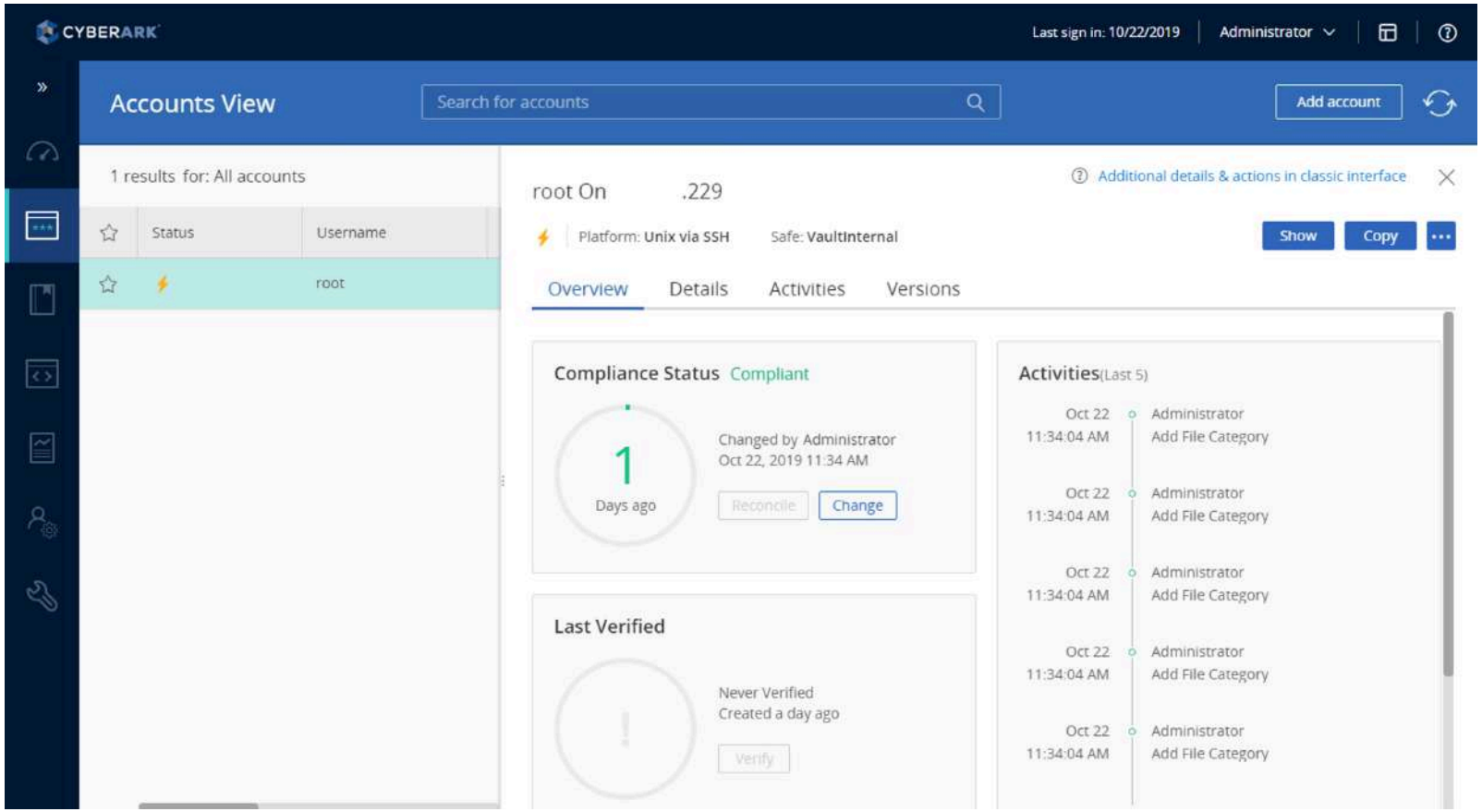


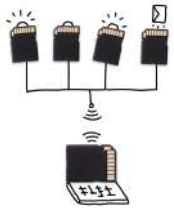
# Enterprise Password Vault

- 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

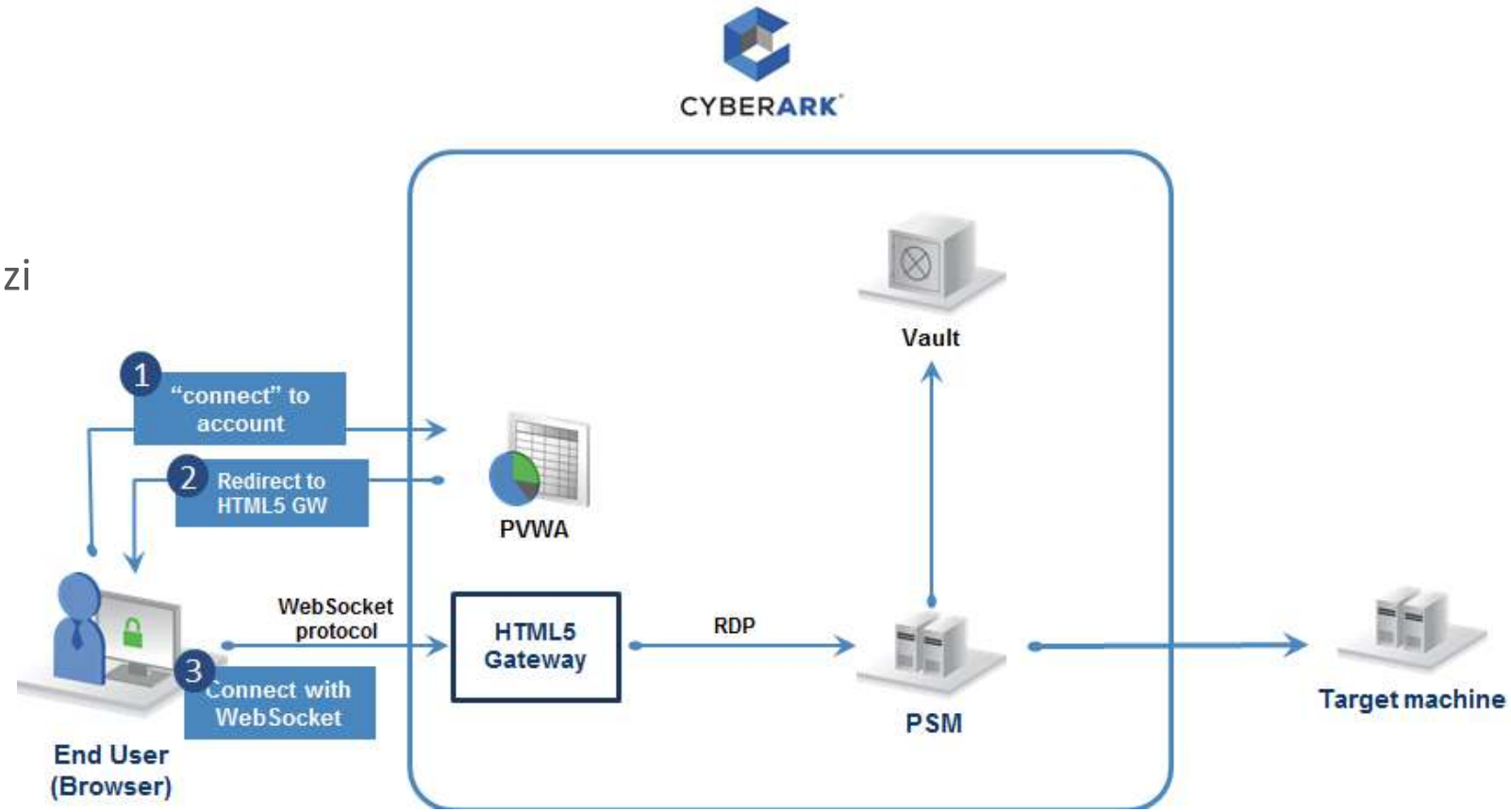
- Prístup k účtom cez webový portál
- Správa účtov, sejfov a politík
- Auditovanie prístupov
- Možnosť pripojenia relácie cez web
- Prístup pre externistov





# Privileged Session Manager

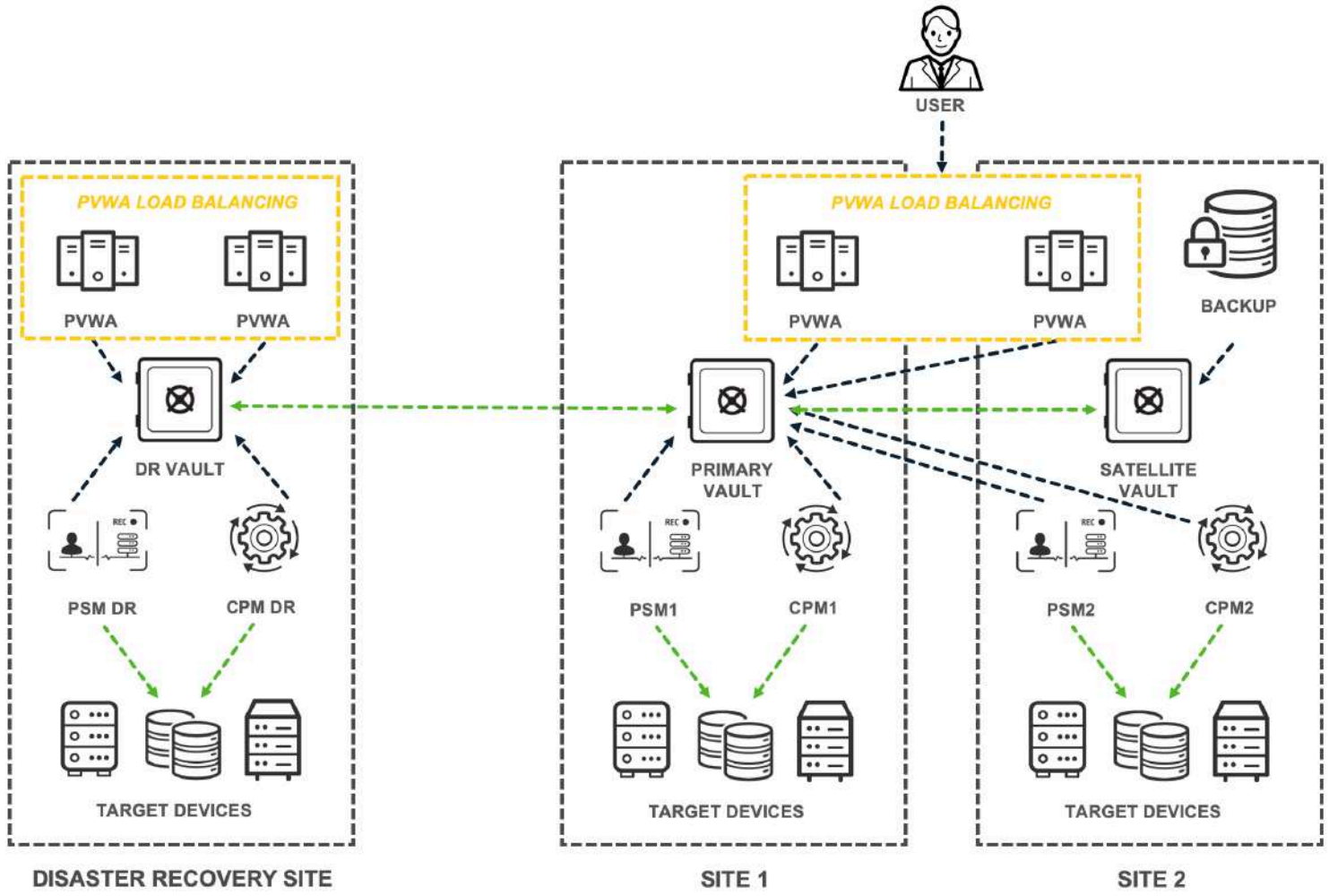
- Nahrávanie relácii
- Bez nutnosti sieťových prestupov medzi používateľom a cieľovým systémom
- Okrem prístupu cez web podporuje aj putty a RDP




- 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



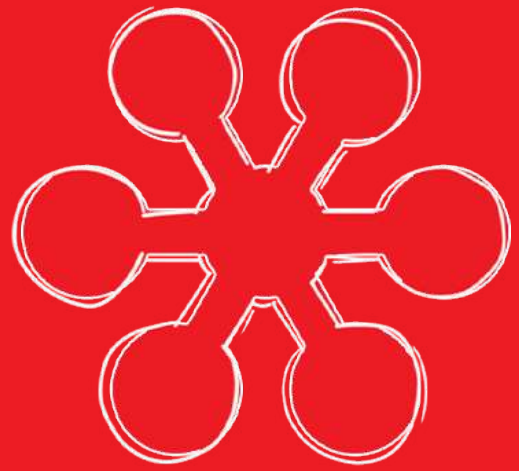

# CyberArk Discovery & Audit™

- 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 zaznámenávanie relácii a nástrojov pre jednoduchý prístup a správu k produktu



# ĎAKUJEME