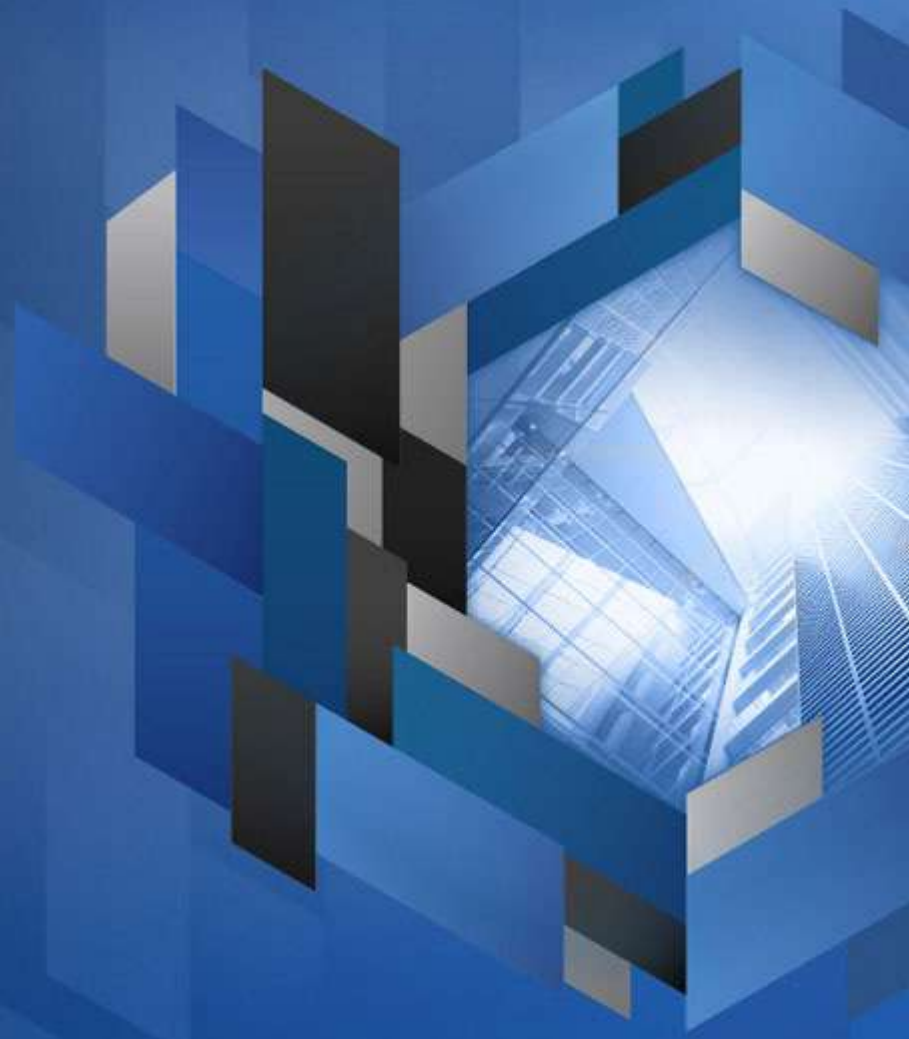
CYBERARK

Prečo chrániť privilegované účty?

Daniel.Hetenyi@cyberark.com



Gartner Security & Risk Management Summit 2018

TOP 10 SECURITY PROJECTS

No. 1: Privileged access management

No. 2: CARTA-inspired vulnerability management

No. 3: Active anti-phishing

No. 4: Application control on server workloads

No. 5: Microsegmentation and flow visibility

No. 6: Detection and response

No. 7: Cloud security posture management

No. 8: Automated security scanning

No. 9: Cloud access security broker

No. 10: Software-defined perimeter

Source: Top 10 Security Projects for 2018, Neil MacDonald, Gartner Security and Risk Summit 2018

Hlavný Hacker NSA – ako ma udržíte mimo vašu sieť?

Rob Joyce - šéf NSA Tailored Access Operations:

- “V dnešnom svete APT hráčov (ako aj NSA), sú privilegované účty kráľom v možnostiach získania prístupu k systémom”
- “Nie účty VIP zamestnancov, ale účty sieťových/doménových/systémových administrátorov otvárajú útočníkom cestu k útoku.”
- “NSA tiež často potešia hard-coded heslá v aplikáciách alebo heslá, ktoré sú prenášané v čitateľnej podobe – napr. použitím starších protokolov – a tak ľahko dostupné.”

CYBERARK

CYBERARK


CIO Journal.

Malware Targets Vulnerable Admin Accounts

Many a CIO has warned employees about malicious links in e-mail that potentially give hackers an entry into corporate networks. Increasingly, so cated cyber attacks are us so-called privileged accou s.


SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Privileged Accounts Play Key Role in Advanced Cyber Attacks

Malware and attackers are increasingly targeting privileged accounts as part of multi-stage operations where they breach networks, gath


SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Privileged Account Details Are Often Shared and Can Be a Weak Entry Point for Attackers

Privileged user accounts


info security
STRATEGY | INSIGHT | TECHNOLOGY

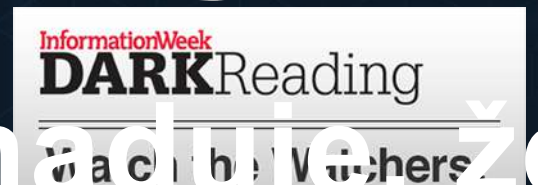
Privileged Accounts at Root of Most Data Breaches

If enterprises ever were given wake-up call, it should be this: stealing and exploiting privileged accounts is a critical success factor for attackers in 100% of all


Forbes

Grasping the Problem with Privileged Accounts

Many in the security industry tend to focus on authentication strength a

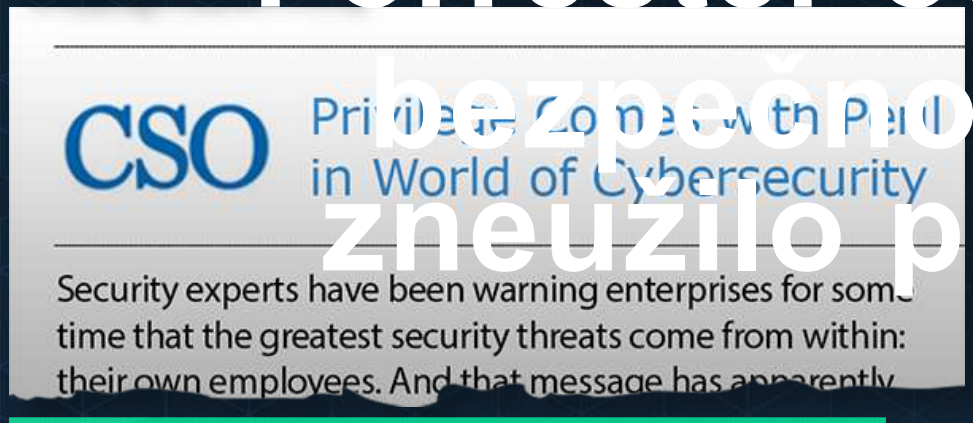

InformationWeek
DARKReading

'Trusted' Employees


The New York Times

Attack Gave Chinese Hackers Pri ileged Access to U.S. Systems

By DAVID


CSO

Security experts have been warning enterprises for som time that the greatest security threats come from within: their own employees. And that message has apparently


USA TODAY

Privileged Accounts: The Master Keys Hackers Know Best

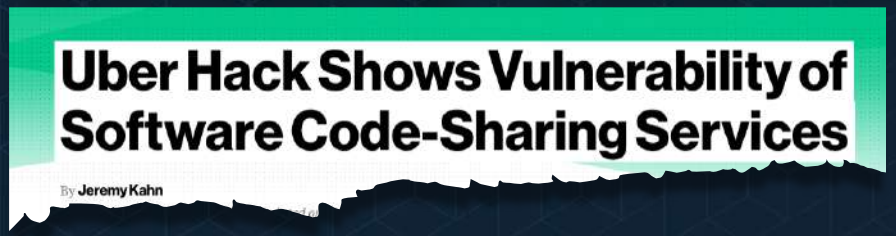
One big reason cyberintruders can easily roam far and wide, once they crack inside a company network, is that many organizations pay scant heed to privileged accounts


FINANCIAL TIMES
myFT

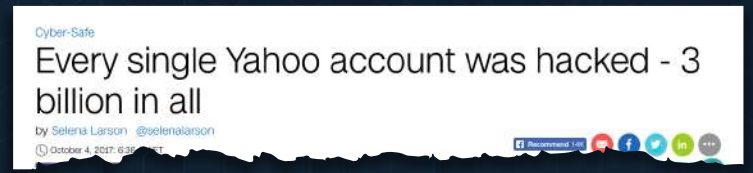
England's NHS hit by large scale cyber attack

AGO by

England's National Health Service has been hit by a large scale cyber attack, with hospitals across the country reporting IT systems are down.


Uber Hack Shows Vulnerability of Software Code-Sharing Services

By Jeremy Kahn


Cyber-Safe

Every single Yahoo account was hacked - 3 billion in all

by Selena Larson @selenalarson


"WannaCry" ransomware attack losses could reach $4 billion

Forrester odhaduje, že 80% bezpečnostných incidentov zneužilo privilegované účty.

The Forrester Wave: Privileged Identity Management, Q3 2016

Office of Personal Management – Stručný prehľad útoku

Organization Overview	
Industry	Federal Government
Employees	4.1 million (federal employees)[1]
Headquarters	Washington, DC

Co se vlastne stalo?

- **Apríl 2015:** OPM zisťuje, že im bol odcudzených 4.2 milionov citlivých údajov štátnych zaměstnancov
- **Jún 2015:** Bolo odhalené, že rozsah celého prípadu je pravdepodobne o mnoho väčší
- **Počet zasiahnutých osôb:** 21.5 miliónov štátnych zamestnancov a dodávateľov
- **Čo bolo ukradnuté:** osobné, zdravotné a rodinné údaje, informácie o previerkach, atp…
- **Odkiaľ hrozba pochádza:** Čína
- **Motivácia: Špionáž**


The Washington Post

New OPM data breach numbers leave federal employees anguished, outraged

By Joe Davidson July 9 Follow @JoeDavidsonWP

If misery loves company, the Office of Personnel Management had a
of good days. Then, its cyber sinkhole got much, much deeper.

News about computer problems grounding United Airlines, shutti
New York Stock Exchange and taking the Wall Street Journal's h
offline momentarily overshadowed OPM's problems and de
vulnerable the digital world is, even in the private sector.


The New York Times

Attack Gave Chinese Hackers Privileged Access to U.S. Systems

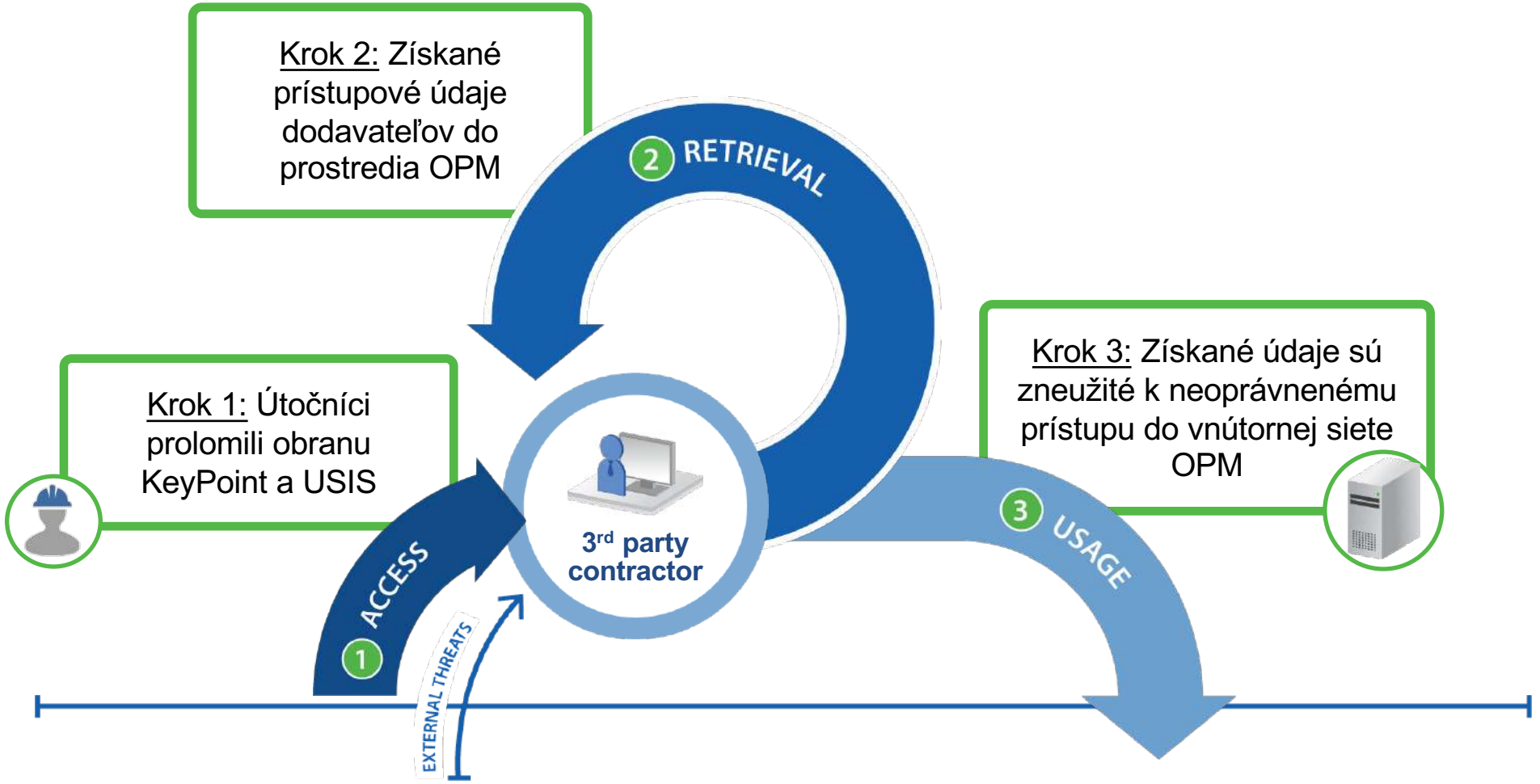
By DAVID E. SANGER, NICOLE PERLROTH and MICHAEL D. SHEAR JUNE 20, 2015

Katherine Archuleta, director of the Office of Personnel Management, in Congress on Tuesday.
Cliff Owen/Associated Press

WASHINGTON — For more than five years, American intelligence
agencies followed several groups of Chinese hackers who were
systematically draining infor

CYBERARK®

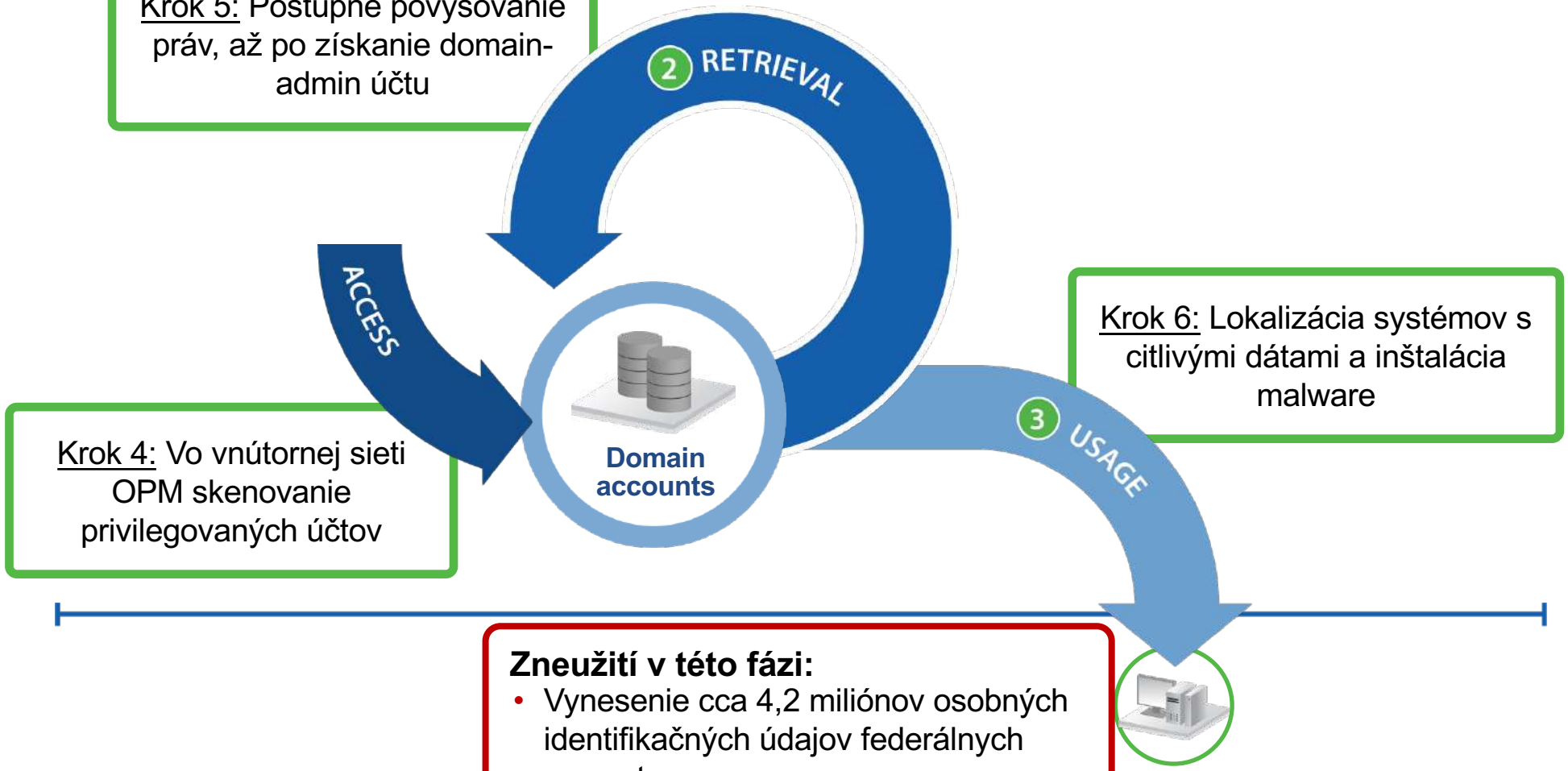
Ako útok začal?



CYBERARK

Čo nasledovalo?

Krok 5: Postupné povyšovanie práv, až po získanie domain-admin účtu



Krok 4: Vo vnútornej sieti OPM skenovanie privilegovaných účtov

Krok 6: Lokalizácia systémov s citlivými dátami a inštalácia malware

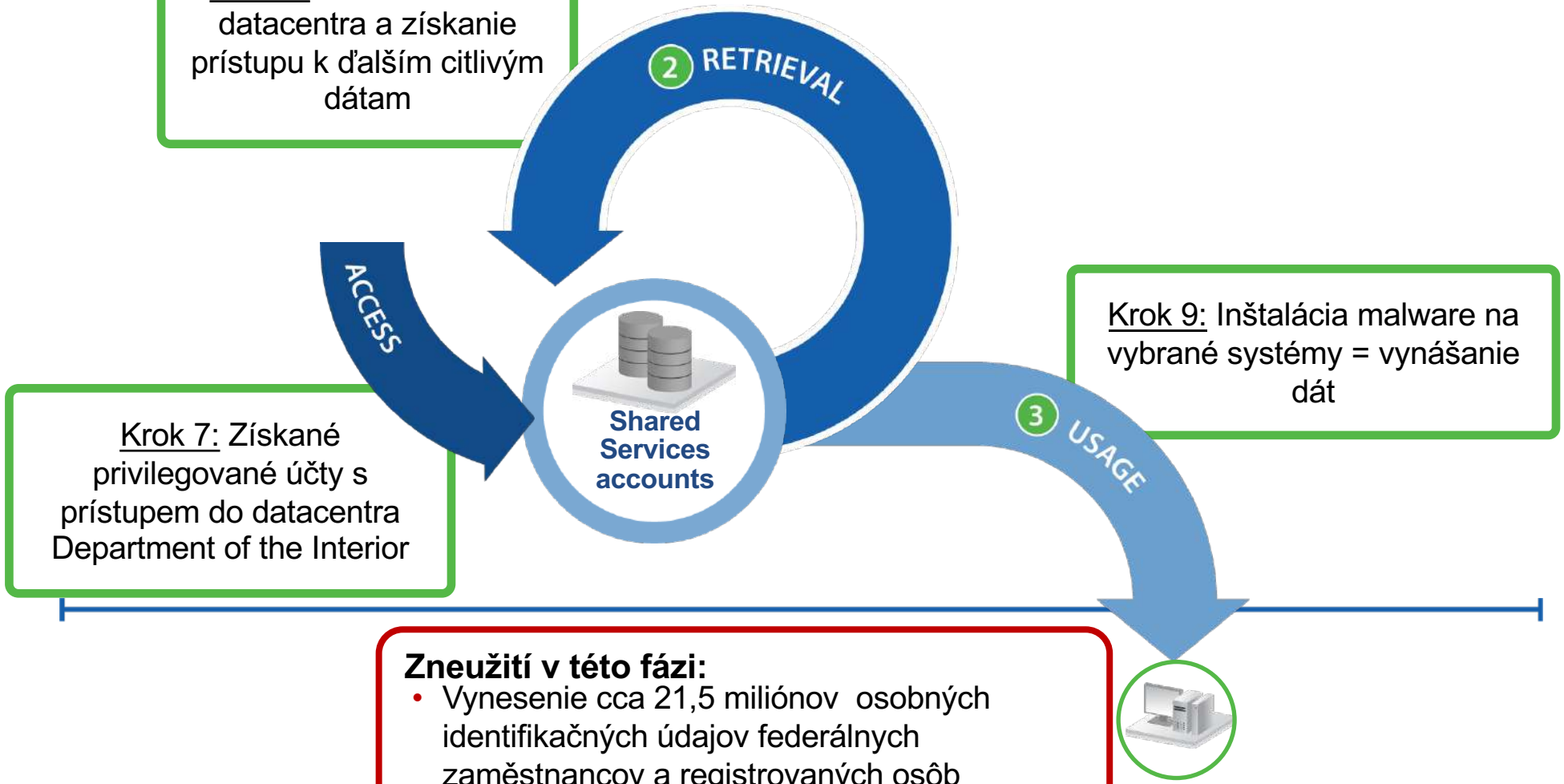
Zneužití v této fázi:

- Vynesenie cca 4,2 miliónov osobných identifikačných údajov federálnych zamestnancov
- Lokalizácia privilegovaných účtov Dept. of the Interior

CYBERARK

Aký bol konečný výsledok aktivít útočníkov?

Krok 8: Preskenovanie datacentra a získanie prístupu k ďalším citlivým dátam



Krok 9: Inštalácia malware na vybrané systémy = vynášanie dát

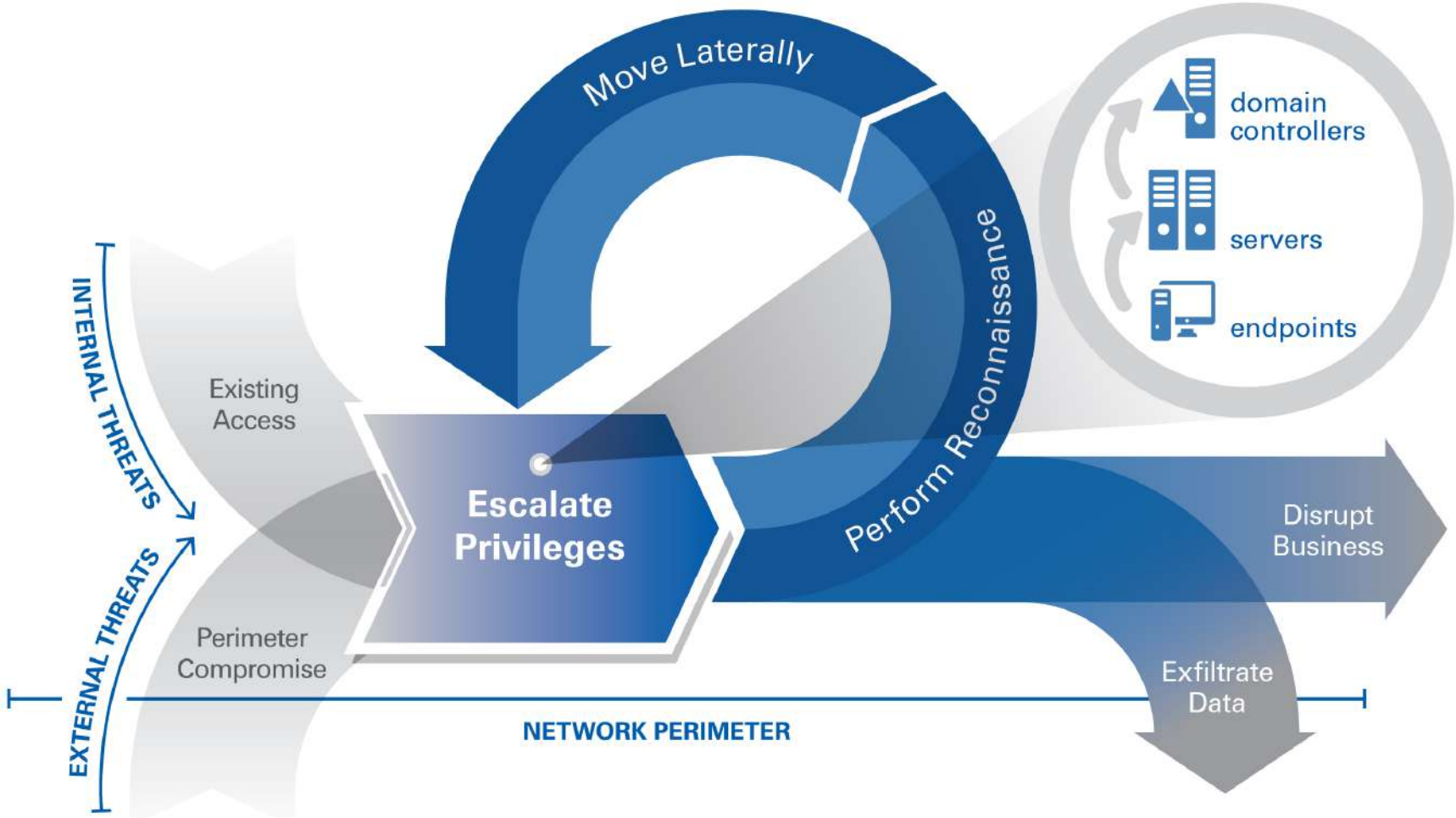
Krok 7: Získané privilegované účty s prístupem do datacentra Department of the Interior

Zneužití v této fázi:

- Vynesenie cca 21,5 miliónov osobných identifikačných údajov federálnych zaměstnancov a registrovaných osôb
- Ukradnuté osobné, rodinné, zdravotné informácie a ďalšie údaje

CYBERARK

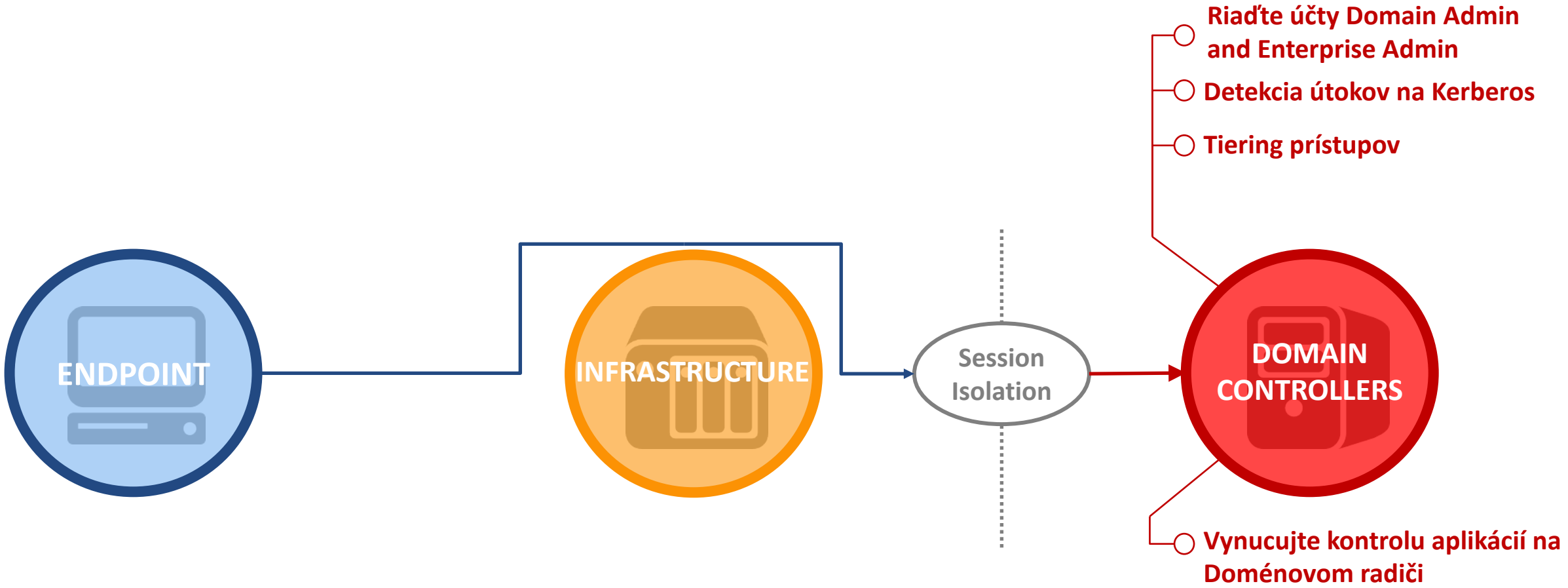
Cieľom útočníka je získať najvyššie oprávnenia



CYBERARK

1

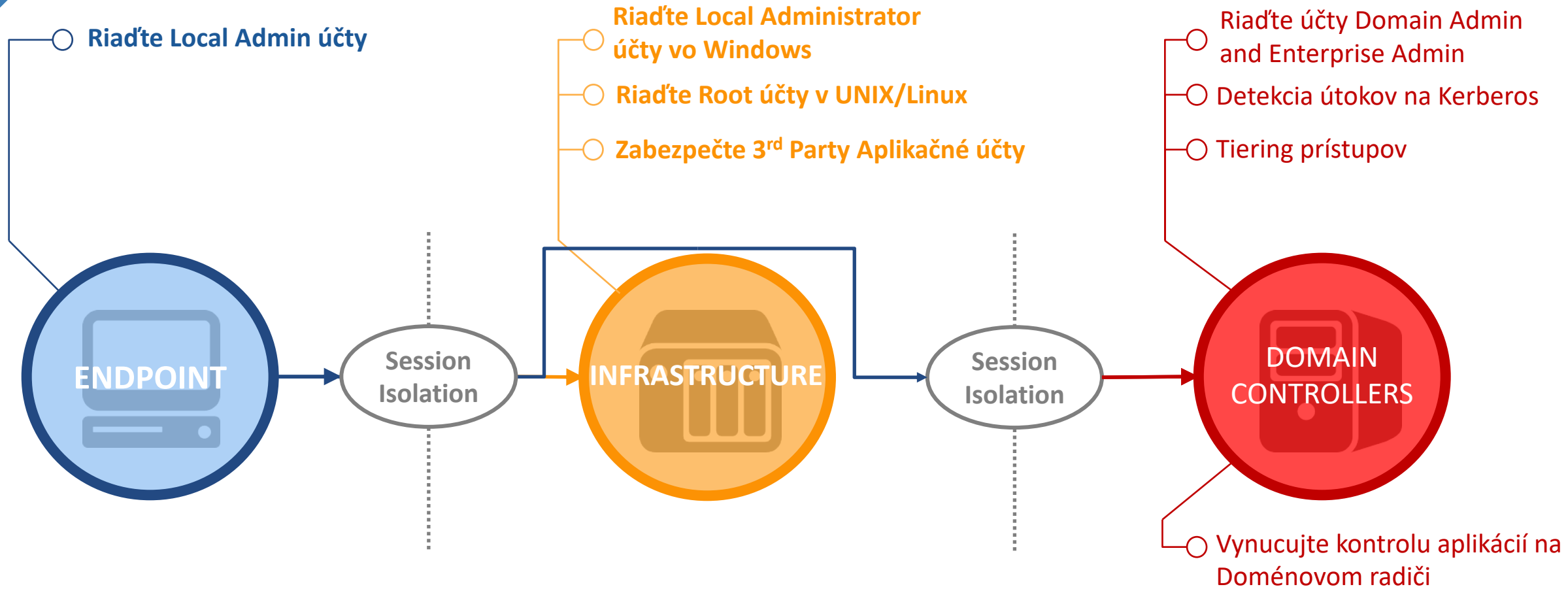
Krok JEDEN: Nevratné a úplné prevzatie siete
Riaďte a zabezpečte Doménové Admin účty



CYBERARK

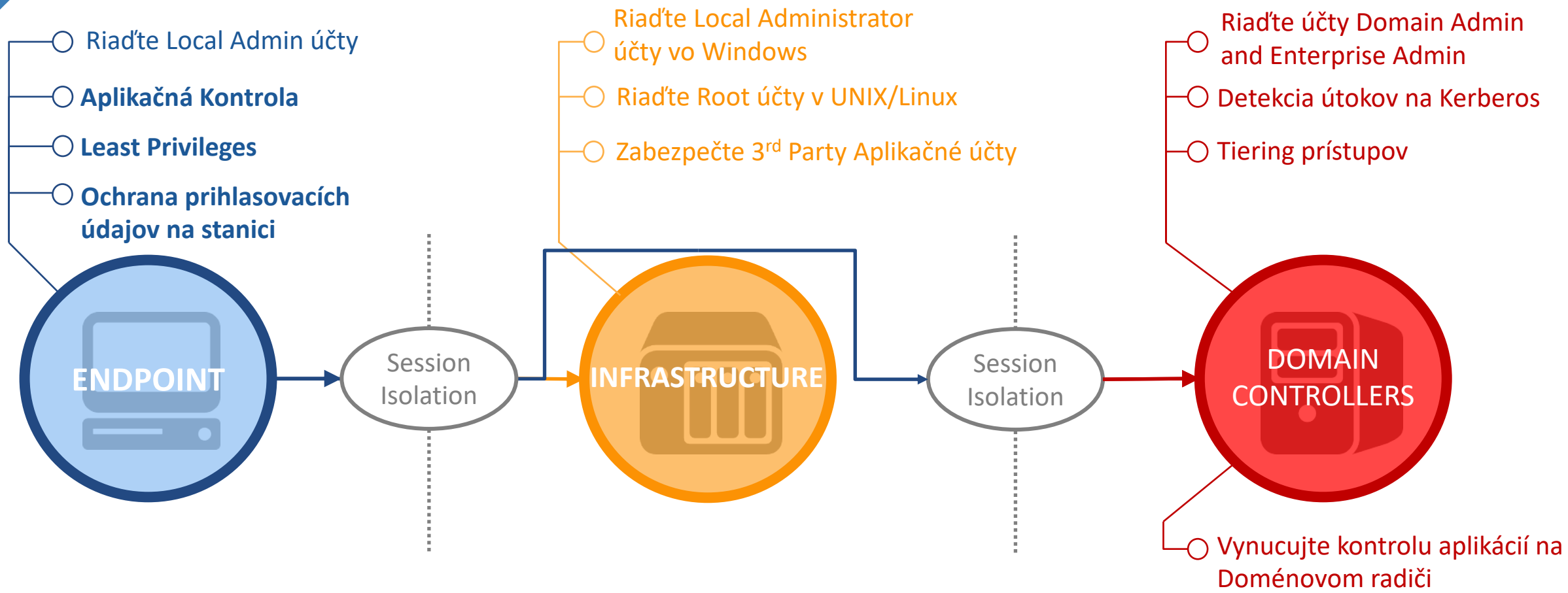
2

Krok DVA: Zamedzte eskalácií privilégií
Riaďte a zabezpečte lokálne a infraštruktúrne účty



CYBERARK

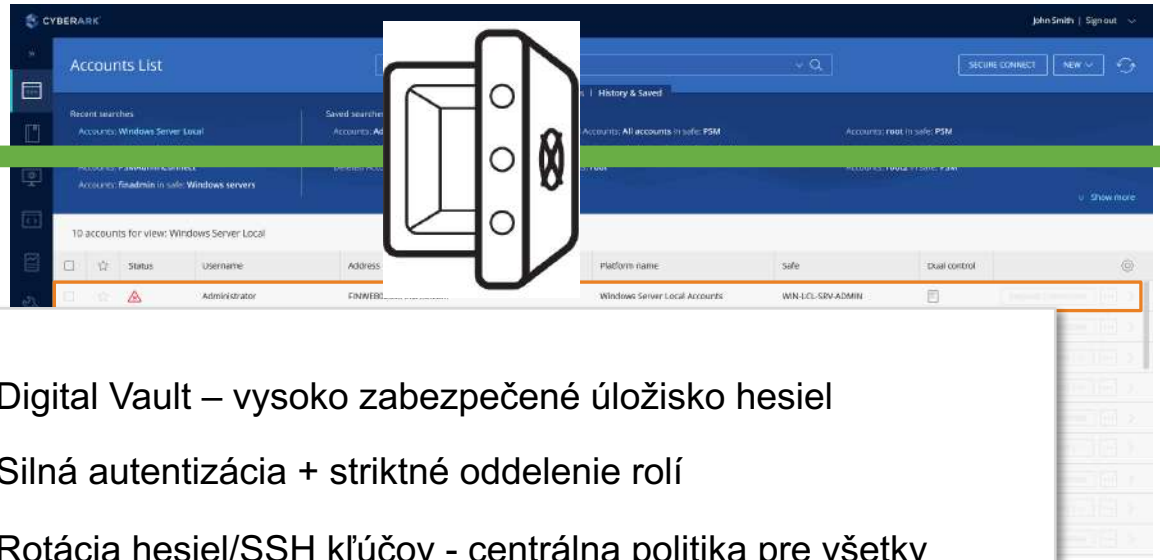
Krok TRI: Obmedzte laterálne pohyby
Hardening koncových staníc



CYBERARK

CyberArk riešenie
Privileged Account Security

Zabezpečenie a správa prihlasovacích údajov



CYBERARK WEB PORTAL

- Digital Vault – vysoko zabezpečené úložisko hesiel
- Silná autentizácia + striktné oddelenie rolí
- Rotácia hesiel/SSH kľúčov - centrálna politika pre všetky privilegované účty
- Široká škála podporovaných systémov – out-of box
- Auditný záznam o každom použití privilegovaného účtu

SECURE STORAGE

ENTERPRISE RESOURCES

SERVERS

MAINFRAMES

DATABASES

APPLICATIONS

NETWORK DEVICES

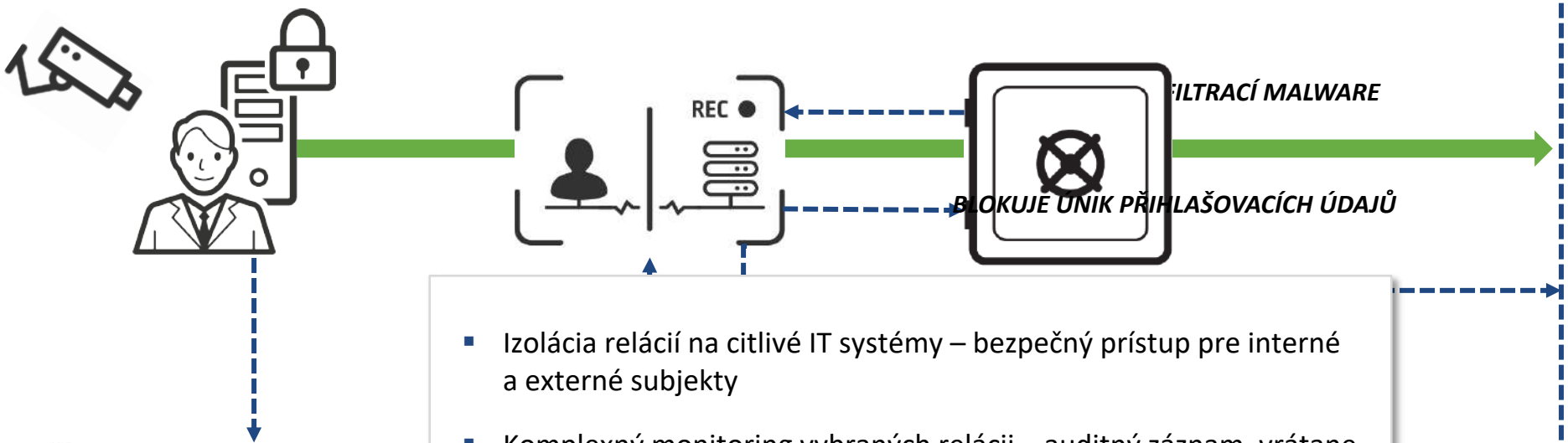
SECURITY APPLICANCES

WEBSITES/ WEBAPPS

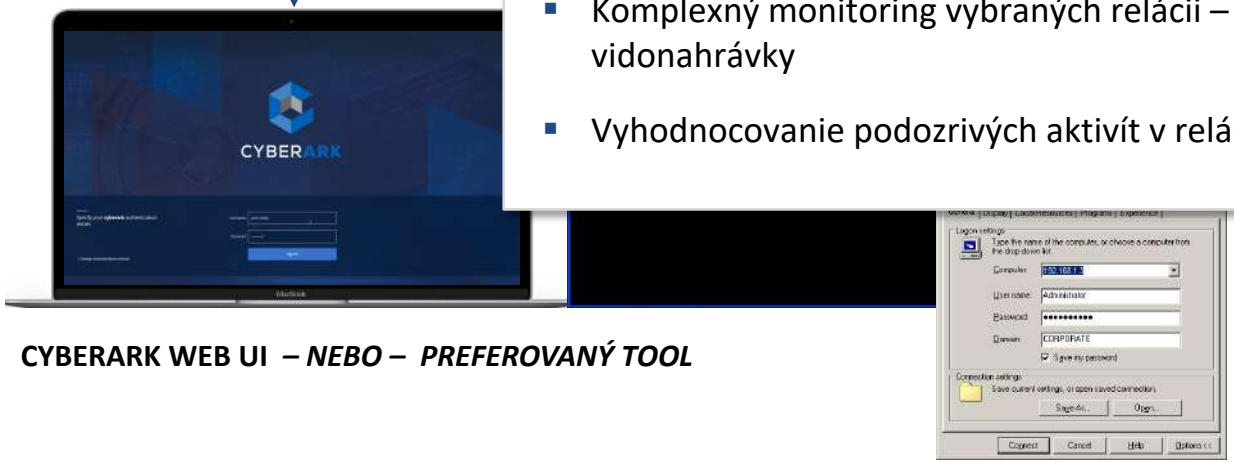
CLOUD INFRASTUCTURE

CYBERARK

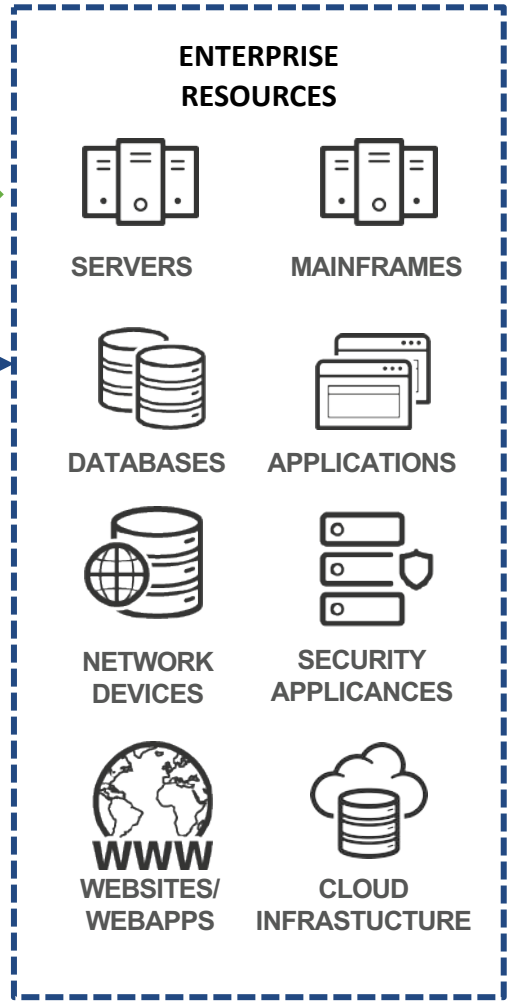
Session isolation, monitoring and recording



- Izolácia relácií na citlivé IT systémy – bezpečný prístup pre interné a externé subjekty
- Komplexný monitoring vybraných relácii – auditný záznam, vrátane vidonahrávky
- Vyhodnocovanie podozrivých aktivít v reláciach



CYBERARK WEB UI – ***NEBO*** – ***PREFEROVANÝ TOOL***



CYBERARK®

PRIVILEGED THREAT ANALYTICS with Domain Controller Protection Option

PRIVILEGED ACCOUNT ACTIVITY

Authentication Activity

Microsoft Active Directory

Privileged User Activity

Critical System Access

ORACLE

Network Tap

Gigamon

CyberArk Vault & PTA DC agent

SIEM Solution

ArcSight CERTIFIED CEF COMPLIANT

IBM

splunk>

Privileged Threat Analytics

Behavioral Analysis & Deep Packet Inspection

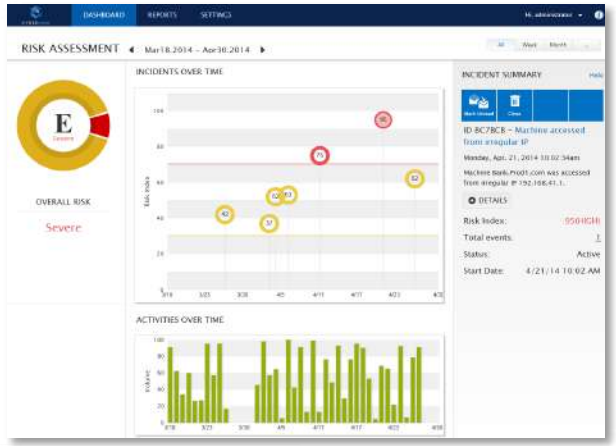
Normal

Abnormal

ALERT: SIEM & CyberArk

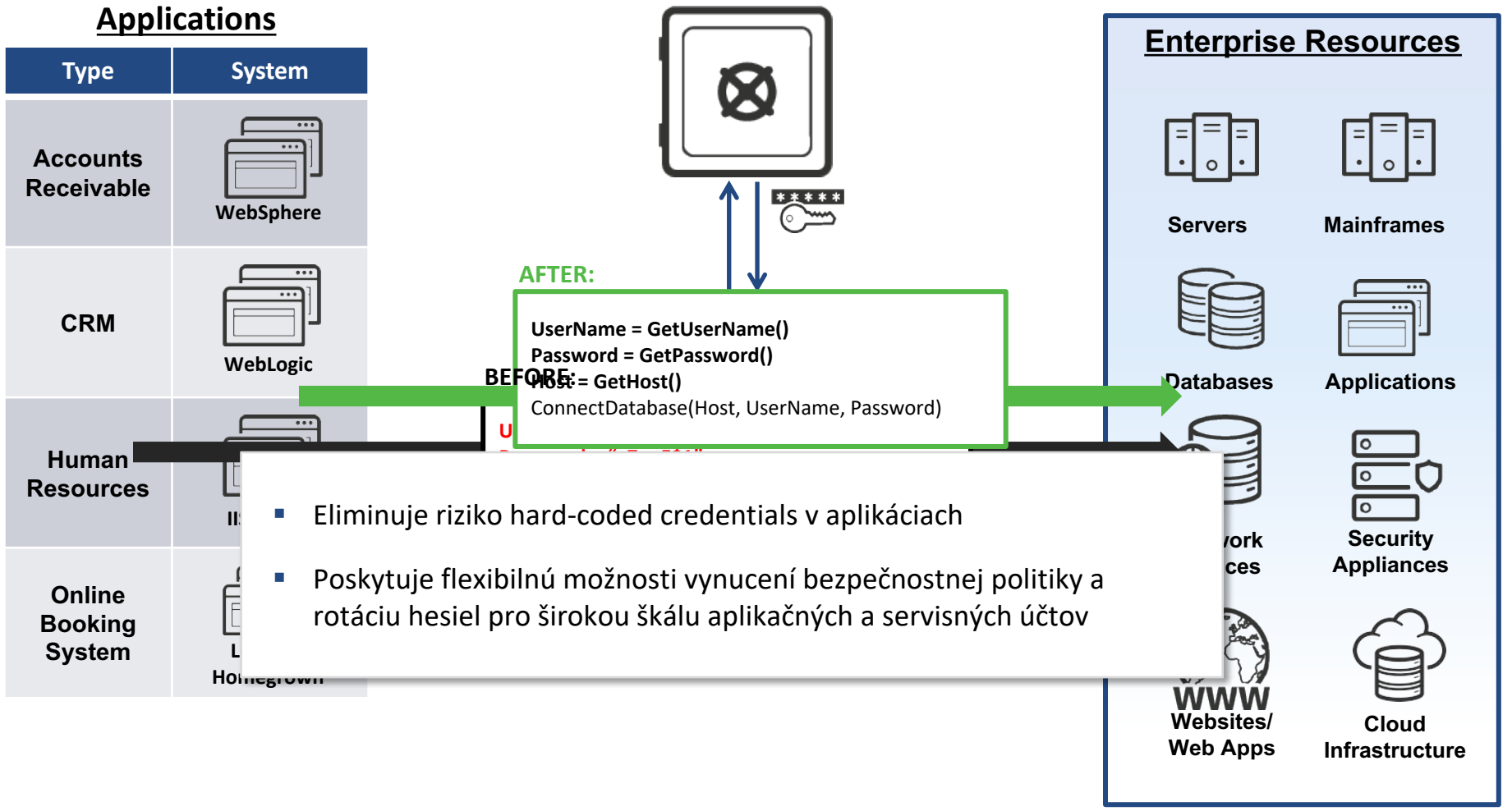
****

Golden ticket detected



- Minimalizuje čas na detekciu zneužitia privilegovaných účtov
- Odhalí a upozorní na zneužitie privilegovaných účtov v reálnom čase – detekcia útokov na zranitelnosti Kerberos, kompromitáci prístupov, neštandardné správanie užívateľa

APPLICATION IDENTITY MANAGER

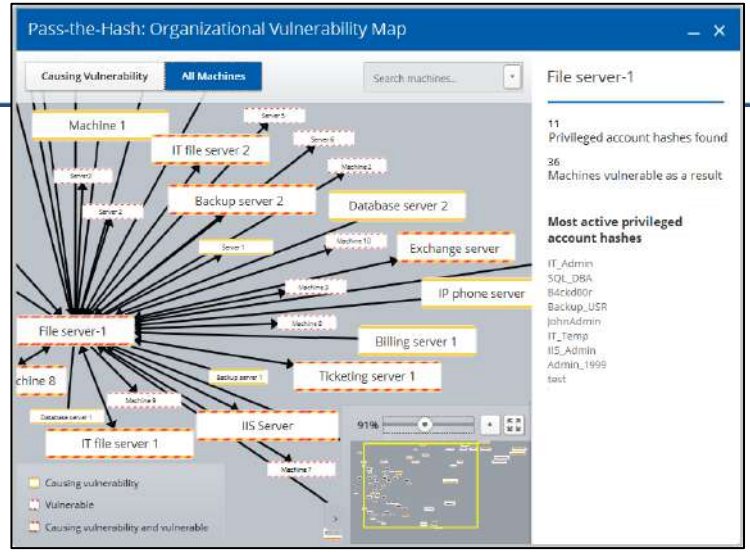


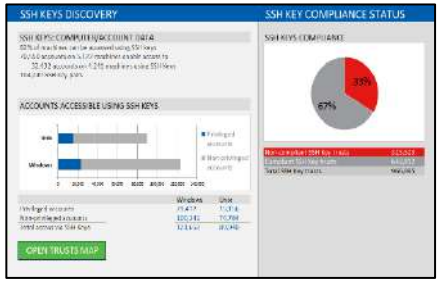
- Eliminuje riziko hard-coded credentials v aplikáciach
- Poskytuje flexibilnú možnosti vynucení bezpečnostnej politiky a rotáciu hesiel pro širokou škálu aplikačných a servisných účtov

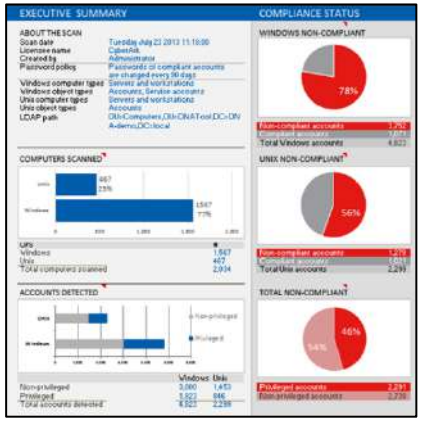
CYBERARK

CyberArk Discovery & Audit (DNA)

- Vyhľadá všetky účty (privilegované i štandardné)
- Identifikuje privilegované účty a typ přihlašování:
  - SSH klíče
  - Vložené/hard-coded účty na IIS/WebSphere/WebLogic
  - Nezabezpečené užívaní práv na UNIX systémech
  - Hashe hesel na stanicích a serverech
  - AWS IAM uživatele, Access Keys a EC2 Key pairs
  - Riziko Golden Ticket attack
- Přehledné reporty s výsledky skenu - Executive Summary Dashboard
- Vytvoření tzv. Trust map s vyhledanými SSH klíči a hash hesel
- Sken běží v pozadí s minimálním dopadem na výkon
- Aplikace se neinstaluje (spustitelný exe soubor)
- Nízké nároky na výkon



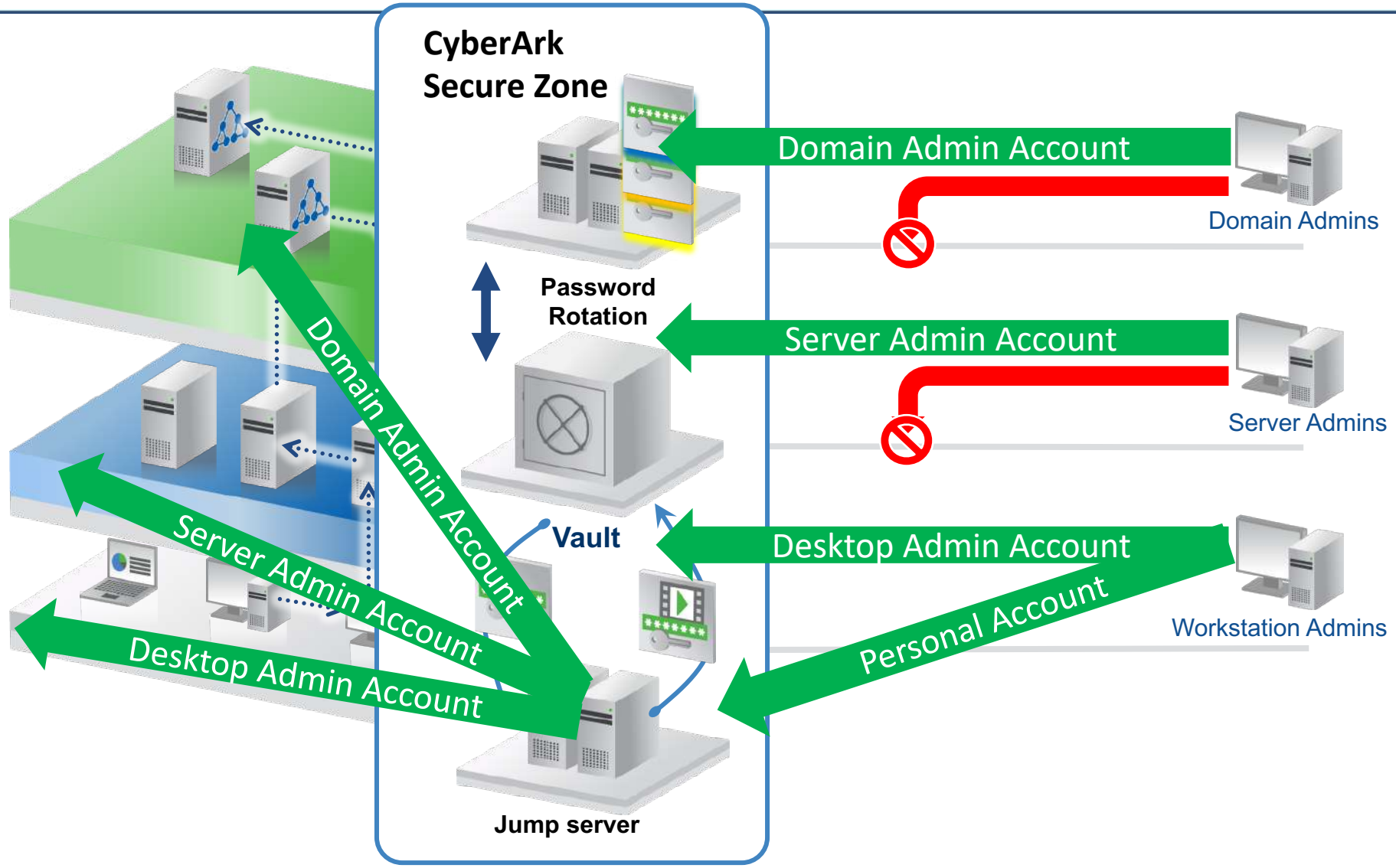




CYBERARK

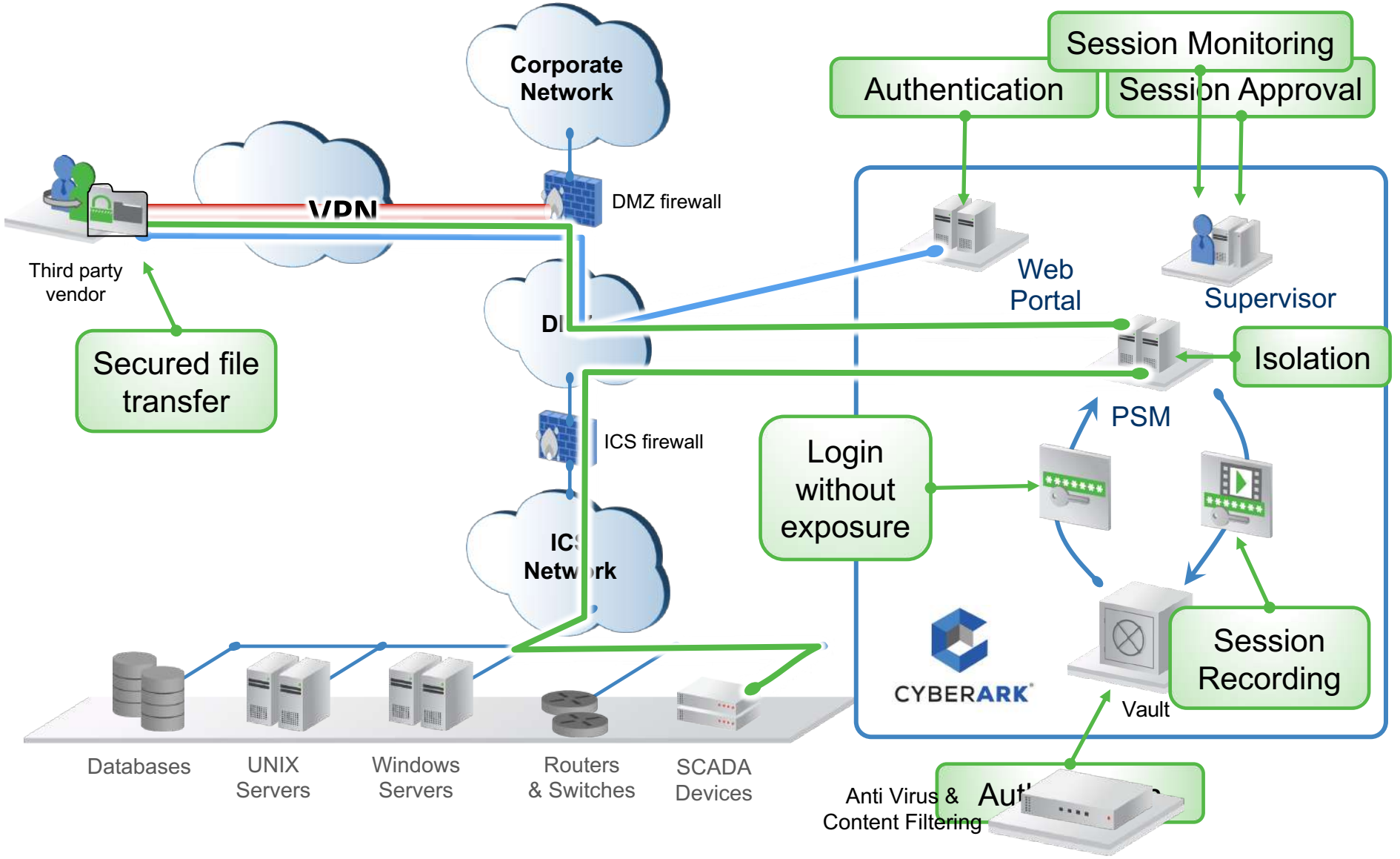
CyberArk riešenie
Use cases

Ochrana Windows Prostredia – Tiering model



CYBERARK

Kontrola vzdialených prístupov dodávateľov



CYBERARK

CYBERARK LEADER IN GARTNER 2018 MAGIC QUADRANT FOR PAM

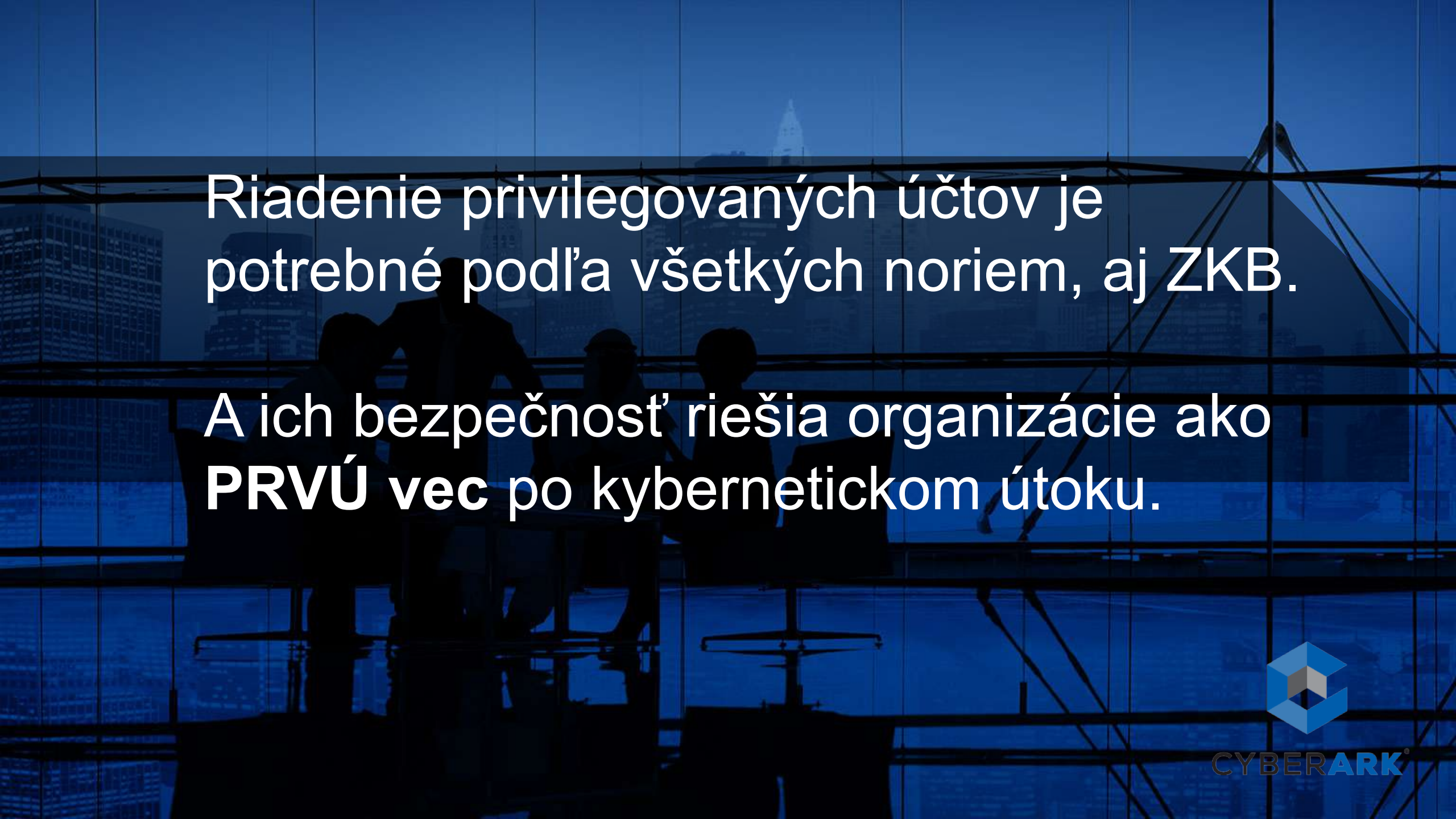
- CyberArk positioned highest for ability to execute and furthest for completeness of vision

Gartner, Magic Quadrant for Privileged Access Management, Felix Gaehtgens, Dale Gardner, Justin Taylor, Abhyuday Data, Michael Kelley, 3 December 2018

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from https://lp.cyberark.com/gartner-mq-pam-leader

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

CYBERARK


Riadenie privilegovaných účtov je potrebné podľa všetkých noriem, aj ZKB.
A ich bezpečnosť riešia organizácie ako **PRVÚ vec** po kybernetickom útoku.
CYBERARK