Multifaktorová autentizace

Endpoint Privilege Management

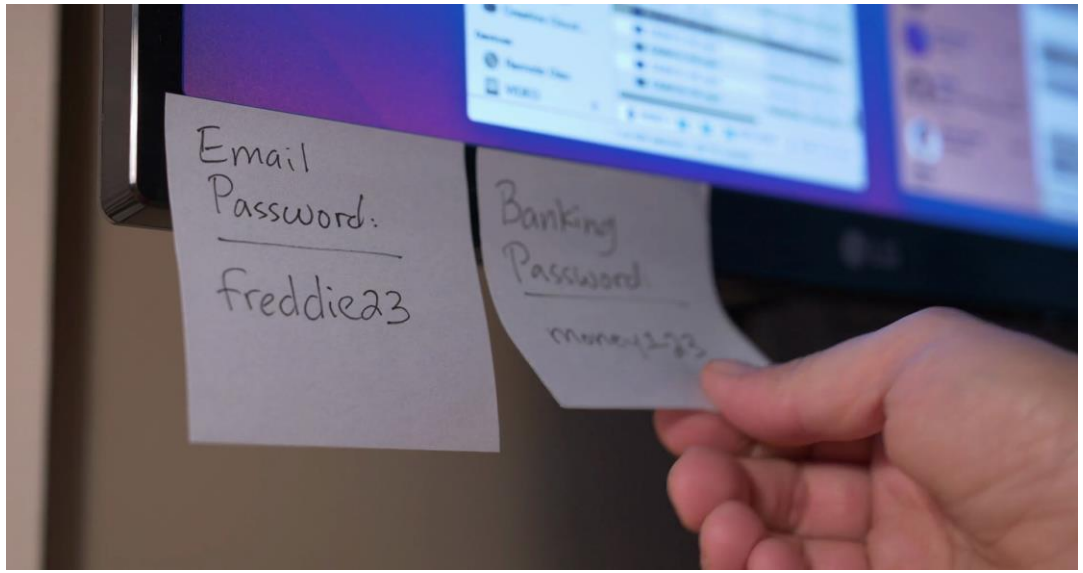
JAN STRNAD
Security architekt

AUTENTIZACE UŽIVATELŮ DO SYSTÉMŮ

Autentizace je proces ověření uživatele při připojení k systému nebo službě. K ověření se používá jméno a heslo…….

Hesla ale již nestačí….

- Slabá hesla
- Slovníková hesla
- Stejná hesla do více systémů
- Sdílená hesla
- ……
- Silné heslo = heslo na monitoru



Uživatelské heslo je v současné době nedostačující pro přihlášení k IT systémům

AUTOCONT

CO JE MULTIFAKTOROVÁ AUTENTIZACE (MFA)?

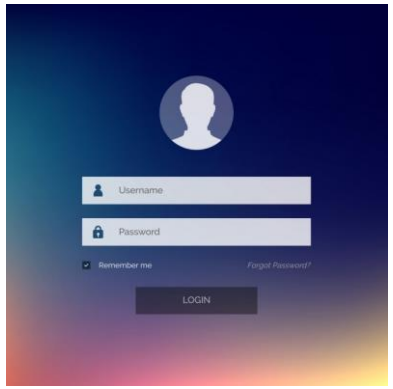
Multifaktorové (dvoufázové) ověření je proces, který zahrnuje minimálně dva nezávislé způsoby, jak ověřit totožnost uživatele při přihlašování k počítačům v síti, nebo k přihlašování k různým službám na internetu.

Hlavní podmínkou dvou a vícefázového ověřování je, aby byla jednotlivá ověření nezávislá. To znamená, aby každá fáze ověření probíhala jinou komunikační cestou. Například ověřování pomocí uživatelského jména a hesla není dvoufázové, ale jen dvoukrokové ověřování. V tomto případě se obě informace přenášející stejnou cestou a to internetem. Jinou komunikační cestou se rozumí například přihlášení pomocí hesla, které přijde uživateli na mobil jako SMS, nebo například bezpečnostním tokenem. Toto jsou fyzická zařízení, která majitel má u sebe.

AUTOCONT

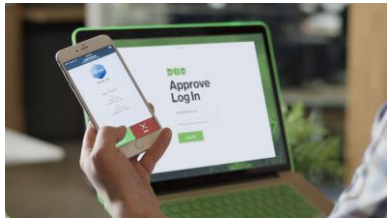
MFA - FAKTORY PRO PŘIHLÁŠENÍ

- **něco vím** – klasické přihlašovací údaje
  - jméno (login) a heslo
  - kódy pro platební karty
  - PIN kód pro SIM karty



- **něco jsem** - různé biometrické senzory
  - Snímače otisku prstů
  - Skenery oční sítnice
  - Senzory pro detekci a měření hlasu, chůze….

- **něco mám** – zařízení, které uživatel vlastní
  - Tokeny (OTP)
  - Čipové karty (certifikáty)
  - Mobilní telefony (Autenticator, Push Notifikace)

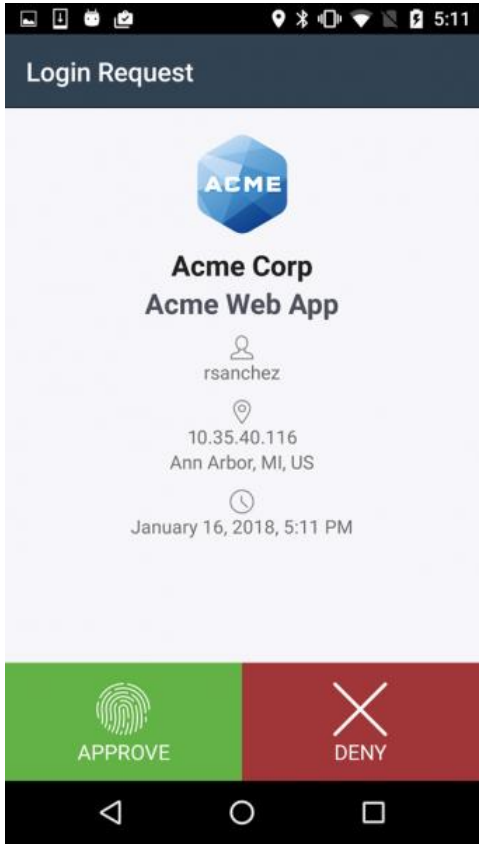


AUTOCONT

ZPŮSOBY OVĚŘENÍ POUŽÍVANÉ MFA

- Tradiční metody:
  - HW tokeny generující OTP
  - Karty
  - Zpětná SMS
  - Zpětné volání

- Moderní metody:
  - Aplikace na mobilním telefonu Android a IOS
    - Jednorázové heslo
    - Push notifikace
      - i s možností biometricky
    - FIDO



AUTOCONT

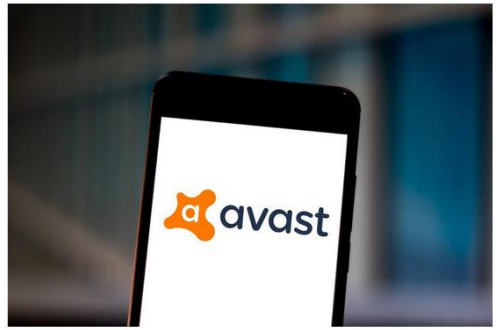
MFA SE STÁVÁ NUTNOSTÍ ….. JEDEN PŘÍKLAD Z ČESKÉHO PROSTŘEDÍ….

Stačilo zcizení jednoho přihlašovacího účtu externího dodavatele a společnost Avast byla napadena útočníkem

14,998 views | Oct 21, 2019, 05:57am

Antivirus Giant Avast Hacked By Spies Who Stole Its Passwords

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.



Avast has suffered a breach of its internal IT network thanks to what it calls a sophisticated hack. PHOTO ILLUSTRATION BY RAFAEL HENRIQUE/SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

Avast has become the victim of a cyberespionage campaign that saw hackers gain deep access to its network. But the Czech company, which has more than 400 million customers for its various antivirus and cybersecurity products, claims the damage is limited.

In an announcement Monday morning, Avast said its **internal network had been breached using a username and password for a temporary VPN account.** The account had mistakenly been kept open and did not require a second factor of authentication, providing an easy way onto Avast computers.

The attack was detected on September 23 when a Microsoft security tool put out an alert due to "malicious replication of directory services from an internal IP." Directory services are software programs that provide admins with a single point in a business IT network where they can manage things like identities and security of employees. **The hackers managed to acquire domain administrator privileges, which would have given them significant control over the Avast network.**

"It gives you licence to plunder all the other accounts," explained professor Alan Woodward, a cybersecurity expert from the University of Surrey. "Change passwords, access just about anything basically."

The hackers had been trying to break into the Avast network through its VPN as early as May 14. Various usernames and passwords were used to access that VPN, leading the company to suspect they had been stolen, though it is unclear how.

Pro vzdálené přihlášení z Home Office, vzdálený přístup pro správu nebo přihlášení do cloudových služeb je často **MFA JEDINÁ** ochrana při přístupu!

AUTOCONT

Řešení Microsoft

Windows Hello
MFA
Conditional Access

MICROSOFT HELLO

Microsoft Hello multifaktorové ověření

- Přihlášení pomocí PIN, biometriky, HW klíče nebo hesla – volba preference přihlášení
  - zůstává na pracovní stanici v TPM čipu nebo v OS
  - Přihlašovací faktory jsou svázány se zařízením, není možné přihlásit se na jiném zařízení
- Hello ověřuje uživatele na jeho koncovém zařízení bez dalšího faktoru – není možné považovat za plnohodnotné dvoufaktorové ověření (kromě externího HW klíče s podporou FIDO2)
- **Bezpečnost přihlášení závisí na podpoře kamery a senzoru otisku prstu**

- **Nepodporuje přihlášení přes RDP**

Správa a nastavení

- Windows Hello - Lokální nastavení – zařízení bez domény
- Windows Hello for Business
  - Správa přes GPO – lokální AD
  - Správa přes Intune – M365

AUTOCONT

Microsoft MFA

MICROSOFT MFA

Microsoft Multi-Factor Authentication

- Zajišťuje dvoufázové ověření uživatelů do **MS cloudových služeb**, nebo služeb napojených na Azure portál pomocí SAML protokolu
- Integrace s **Conditional Access** – podmíněný přístup pro přihlášení

- Druhý faktor
  - Moderní metody:
    - Microsoft authenticator – aplikace na mobilním telefonu Android a IOS
      - Jednorázové heslo
      - Push notifikace
  - Starší metody:
    - Zpětná SMS
    - Zpětné volání

AUTOCONT

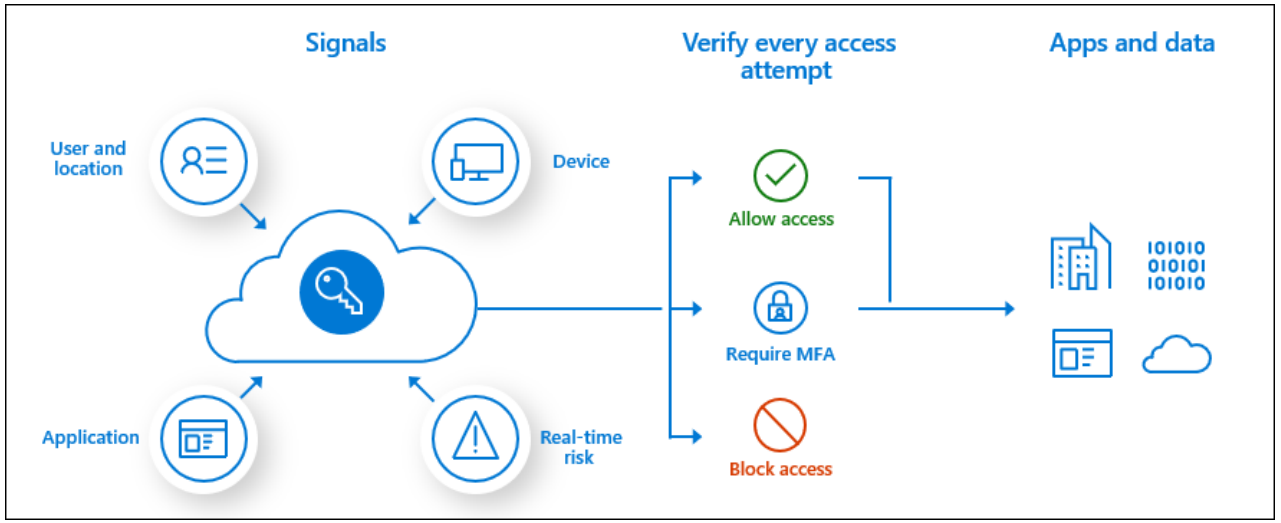
MICROSOFT CONDITIONAL ACCESS

Microsoft Conditional Access

- nastavuje podmínky, na základě kterých umožňuje nebo blokuje přístup uživatele k M365 aplikacím a datům

Politiku je možné uplatnit na:

- Uživatele
- M365 aplikace
- Zařízení nebo lokalita
- Rizikovost uživatele



- Nastavení akce:
  - Povolit přístup
  - Blokovat přístup
  - Vynutit multifaktorovou autentizaci

AUTOCONT

Cisco DUO

(DUO Security)

CISCO DUO

Multifaktorové ověřování uživatelů do systémů

- Kompletní správa v cloudové konzoli
- Podpora velkého množství aplikací pro multifaktorové ověření (cca 170)
- Politiky pro jednotlivé aplikace
- Klient na **Windows OS pro online i offline** ověření
- Kontrola zdraví zařízení – Windows, Mac OS, Android, IOS
- DUO autentikátor a Android a IOS zařízení
- Dashboard a reporting

AUTOCONT

RSA SecureID

RSA SECURID ACCESS – OVĚŘENÁ TECHNOLOGIE MFA

Standard
pro silnou autentizaci

- RSA důvěřuje více jak 25,000 organizací
- Více než 50 million *aktivních uživatelů*
- 500+ certifikovaných technologických partnerů

RSA SecurID
platforma pro zajištění autentizace a idetity

- Zajišťuje dynamické ověřování uživatelů do systémů, aplikací i služeb
- Mobilní MFA: Push, OTP, biometrika…
- Pro jakoukoliv aplikaci: on-prem nebo cloud
- Možnost on-prem i SaaS správy, subscription nebo perpetual licencování

AUTOCONT

Porovnání MFA technologií

Microsoft MFA
Cisco DUO
RSA SecureID

ROZDÍLY V TECHNOLOGIÍCH MICROSOFT, CISCO DUO A RSA

Vlastnost	Microsoft MFA	Cisco DUO	RSA SecureID
Způsoby ověření	Authenticator, SMS, Push, HW token - FIDO, call	Authenticator, Push, SMS, HW token, karty, FIDO, call	Authenticator, HW token, Push, SMS, karty, FIDO, call
Podpora systémů a aplikací	nativně M365, SAML	stovky aplikací, Radius, SAML, aplikace	stovky aplikací, Radius, SAML, aplikace
Autentizace do OS Win 10	NE, pouze Hello	ano, klient	ano, klient
Podmíněný přístup	ANO, pouze pro M365	ANO	ANO
Nasazení	jednoduché, cloudová služba	jednoduché, cloudová služba	Cloud - jednoduché, on-prem nutnost serveru
SW token	ANO, authenticator	ANO, authenticator	ANO, authenticator
HW token	NE	NE	ANO
Správa on-premise	pouze Hello	NE	ANO
Správa cloudová služba	ANO	ANO	ANO
Licence	Předplatné	Předplatné	Předplatné nebo perpetuální licence
Orientační cena	součástí M365 nebo EMS licencí	od 3 Euro/měsíc na uživatele	od 4 Euro/měsíc na uživatele

AUTOCONT

Endpoint Privilege Management

ANATOMIE DNEŠNÍCH ÚTOKŮ – VYUŽITÍ ÚČTŮ UŽIVATELŮ A SPRÁVCŮ

Počáteční fáze, velmi často phishing, databáze uniklých hesel (AVAST)….

Stanice

Získání lokálního admin hesla

Stanice

Získání admin hesla pro přístup na server

Získání přístupu na VŠECHNA kritická zařízení

Kritické stanice

Kritické servery

Bezpečnostní nástroje

Cloudová infrastruktura

Server

Použití admin hesla. Pokud nic nenajde, pokračuje dál.

Server

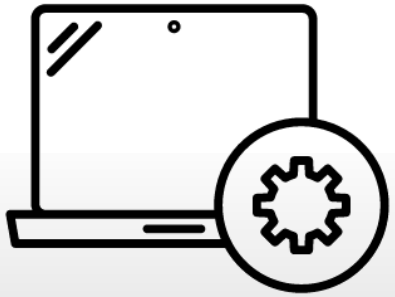
Získání hashe admin hesla se širšími pravomocemi

Doménový kontroler

Vytvoření admin účtu pro ovládnutí domény

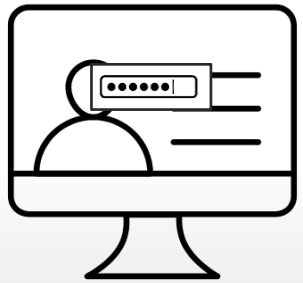
AUTOCONT

RIZIKO LOKÁLNÍCH ÚČTŮ - CO MOHOU UŽIVATELÉ S LOCAL ADMIN OPRÁVNĚNÍM…



Změna konfigurace

Instalace malware



Přístup a změny účtů

> 87% organizací dosud neodebralo oprávnění “local admin“ svým uživatelům

Zdroj: CyberArk Threat Landscape Survey, February 2018

AUTOCONT

CHYBĚJÍCÍ ZÁKLADNÍ STAVEBNÍ BLOK V BEZPEČNOSTI STANIC A SERVERŮ

Antivirus/Firewall/IPS/EDR
Detekuje a blokuje útoky na základě signatur a chování nebo reputace (viry, červy, ransomware, phishing)

Privilege Management
Zajišťuje nejnižší potřebné oprávnění uživatele pro práci na počítači nebo serveru (odstraňuje lokálního administrátora)

Configuration Management
Detekuje zranitelnosti systémů (skener zranitelností) a zabraňuje jejich zneužití (aktualizace kódu OS a aplikací)

AUTOCONT

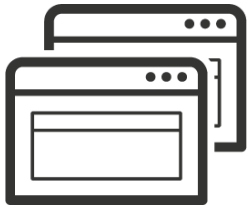
CYBERARK ENDPOINT PRIVILEGE MANAGER (EPM)

Uzamčení privilegií na Windows a Mac stanicích a serverech – zabrání útoku ihned v prvopočátku

Privilege management

- Odstranění práv lokálního administrátora pro uživatele
- Automatické politiky pro povyšování práv a whitelisting
- Oddělení oprávnění na Windows Serverech

+



Application control

- Blokuje nevyžádané aplikace
- Automaticky povýší oprávnění pro vybrané aplikace
- Zabrání neznámým aplikacím způsobit škodu

+

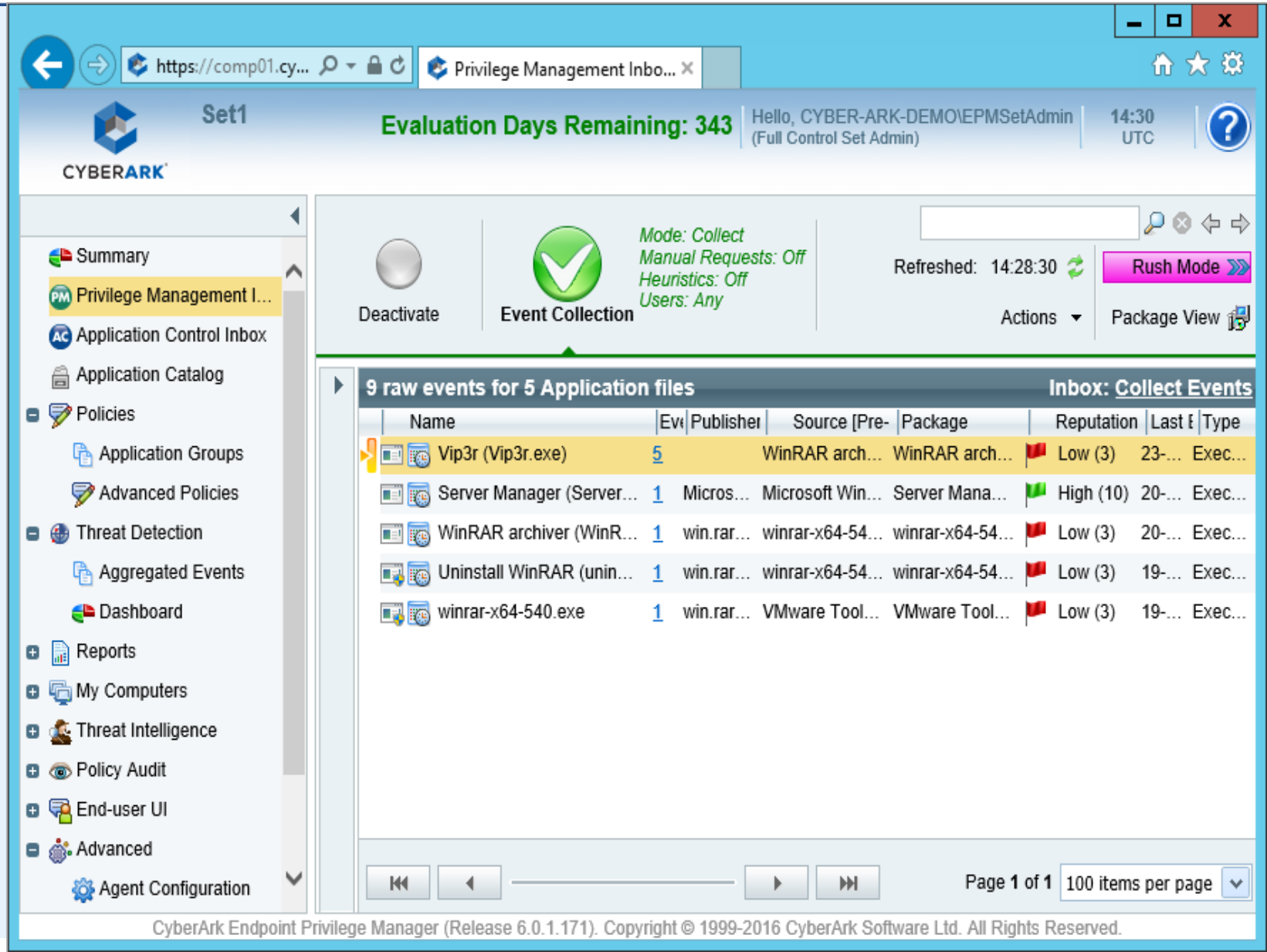
Credential theft protection

- Detekce a blokace odcizení přihlašovacích údajů na Windows stanicích
- Ochrana úložišť hesel OS, prohlížečů, admin. nástrojů
- Ochrana před Ransomware

AUTOCONT

UKÁZKA KONZOLE - PRIVILEGE MANAGEMENT INBOX

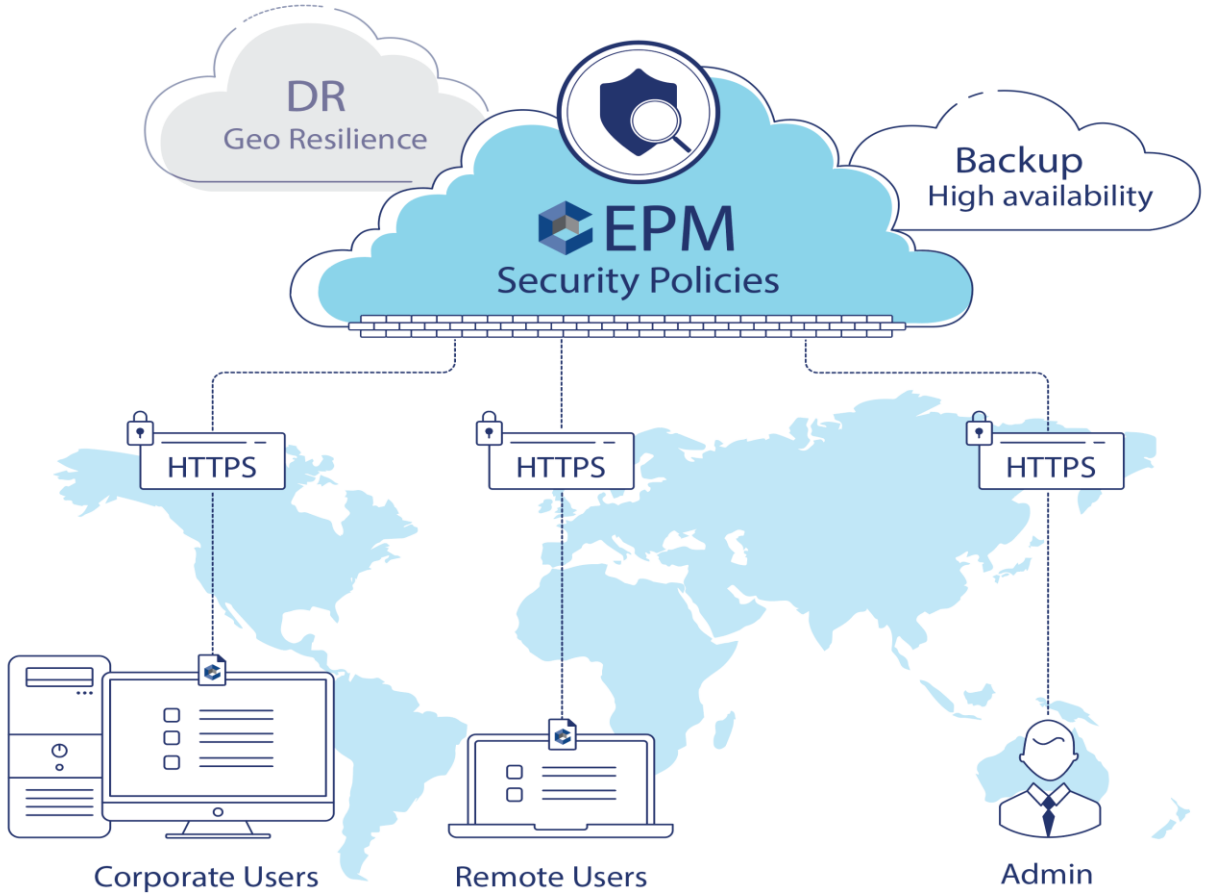
- EPM agent sbírá informace o aplikacích , které ke svému běhu vyžadují vyšší oprávnění a zobrazuje je v management konzoli v Privilege Management Inbox
- Zobrazuje nejen aplikace, ale i akce OS, která vyžadují vyšší oprávnění
- Na základě nasbíraných informací je možné vytvořit politiku, která zajistí vyšší oprávnění pro zvolené aplikace a uživatele/počítače



SPRÁVA CYBERARK EPM V CLOUDU

Podporuje:

- Windows Workstations
- Windows Servers
- MacOS systemy



AUTOCONT

LICENCOVÁNÍ A VYZKOUŠENÍ EPM

- Licence na pracovní stanice a servery
- Licence je dodávána jako subscripce na měsíc. Možné zakoupit na 3 roku dopředu
  - Cena licence pro pracovní stanici – 2,25 Euro/měsíc (27 Euro/rok), cca 700 Kč za rok
  - Cena licence pro server – 8,5 Euro/měsíc (102 Euro/rok), cca 2.700 Kč za rok

  Do konce roku akce, cena licence serveru za cenu pracovní stanice

Nabídka na otestování:

PoC – velmi snadné nasazení a otestování funkcí CyberArk EPM

- Vytvoření Setu pro zákazníka v cloudové konzoli
- Instalace klienta na 1-3 koncové zařízení
- Sken a learning mód po instalaci
- Nastavení politik skupin aplikací

Po základním zaškolení zvládne každý IT správce

AUTOCONT

JAN STRNAD

- +420 602 280 387
- jan.strnad@autocont.cz

AUTOCONT