WALLIX
CYBERSECURITY SIMPLIFIED

PRIVILEGED ACCESS MANAGEMENT

WALLIX Bastion – Správa přístupů ke kritické infrastruktuře

Nehledě na zaměření Vaší společnosti, zabezpečení IT infrastruktury a informací v ní kolujících je kritické pro zachování jejího plynulého chodu. Nestřežený přístup k těmto informacím a zdrojům je stále ve velkém množství společností umožněn příliš mnoha uživatelům včetně externistů. Tím mohou být vystaveny nechtěným změnám, uživatelským chybám či dokonce zcizení a zneužití.

Klíčové vlastnosti:

- ✓ **Flexibilita nasazení**
- ✓ **Rychlá a snadná implementace** díky integraci s Microsoft Active Directory / LDAP / MFA
- ✓ **Definice uživatelů, systémů a aplikací**, ke kterým je třeba zabezpečit a monitorovat přístup
- ✓ Nastavení pravidel pro **rotaci hesel** k privilegovaným účtům
- ✓ **Udělení oprávnění** k přístupu uživatelů do jednotlivých oblastí infrastruktury
- ✓ **Zasílání notifikací** o zahájení definované relace
- ✓ Možnost **real-time monitorování relací** externích pracovníků a jejich okamžité ukončení v případě potřeby
- ✓ **Nahrávání relací** a ukládání event logů pro **potřeby auditu**
- ✓ Snadná **synchronizace** se stávajícím Identity Access Managementem v rámci REST API
- ✓ **Pluginy** pro integraci s technologickými partnery

Účinným řešením této problematiky je **WALLIX Bastion**. Jedná se o technologii určenou pro správu přístupů ke kritické infrastruktuře, která zároveň zajišťuje správu a rotaci hesel privilegovaných účtů. Hlavní komponentou je proxy brána určená pro správu a monitoring privilegovaných přístupů. Poskytuje záznamy uživatelských relací včetně logů, nepozměnitelné podklady pro audit a analytické reporty uživatelského chování. WALLIX Bastion nevyužívá pro sběr informací agenty, což zjednodušuje jeho provoz i nasazení. Celé řešení se skládá ze 3 modulů – **Session Manager, Password Manager a Access Manager**, každý z nich je určen pro zabezpečení jiného vektoru problematiky PIM/PAM. Díky modulární koncepci a velice snadné implementaci se Bastion navíc přizpůsobí Vašim potřebám a současné infrastruktuře bez nutnosti ji upravit.

WALLIX Bastion monitoruje činnosti administrátorů (interních i externích), **chrání přihlašovací údaje k privilegovaným účtům** (root, local admin atd.), monitoruje práci třetích stran v reálném čase, udržuje přehled o přístupech a zákrocích a dokáže exportovat události do SYSLOG / SIEM technologií.

Technologické opatření zabezpečení privilegovaných přístupů může být jedním z důležitých pilířů pro dosažení souladu s GDPR a dalšími normami, regulacemi nebo bezpečnostními standardy (jako jsou např.: ISO 27001, HIPAA, SOX, PCI-DSS a další).

LeadershipCompass KuppingerCole
PRODUCT LEADER

WALLIX Bastion v kostce:

- **Rychlý a snadný** proces implementace do existující infrastruktury
- **Bez-agentské řešení**, které nevyžaduje instalaci softwaru na monitorované systémy
- **Protokoly autentizace:** LDAP, Microsoft Active Directory, Radius, TACACS+, Kerberos, X.509, OTP, Web SSO
- **Formování high-availability clusterů :** Active/Passive nebo Active/Active
- **Podpora pro** Microsoft RemoteApp
- **Umožnění periodických rotací hesel** k privilegovaným účtům (Windows, Unix, Cisco, Oracle, MySQL, Fortinet, PaloAlto i itp.)
- **Podporované platformy:** HW Appliance, VMware, Microsoft Hyper-V, Microsoft Azure, Amazon Web Services

COMGUARD
security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

WALLIX
CYBERSECURITY SIMPLIFIED

PRIVILEGED ACCESS MANAGEMENT

Ekosystém správy privilegovaných přístupů

Díky kompletním analytickým reportům z WALLIX Bastion máte možnost definovat efektivní bezpečnostní politiky určené pro kontrolu přístupů s rozšířeným oprávněním, můžete nastavit pravidla pro jednotlivé uživatele a aplikovat mechanismy k jejich vynucení. Pomocí WALLIX budete mít přehled o přístupech a zákrocích. Zároveň Vám technologie WALLIX Bastion pomůže snížit náklady na práci externích pracovníků.

Session Manager

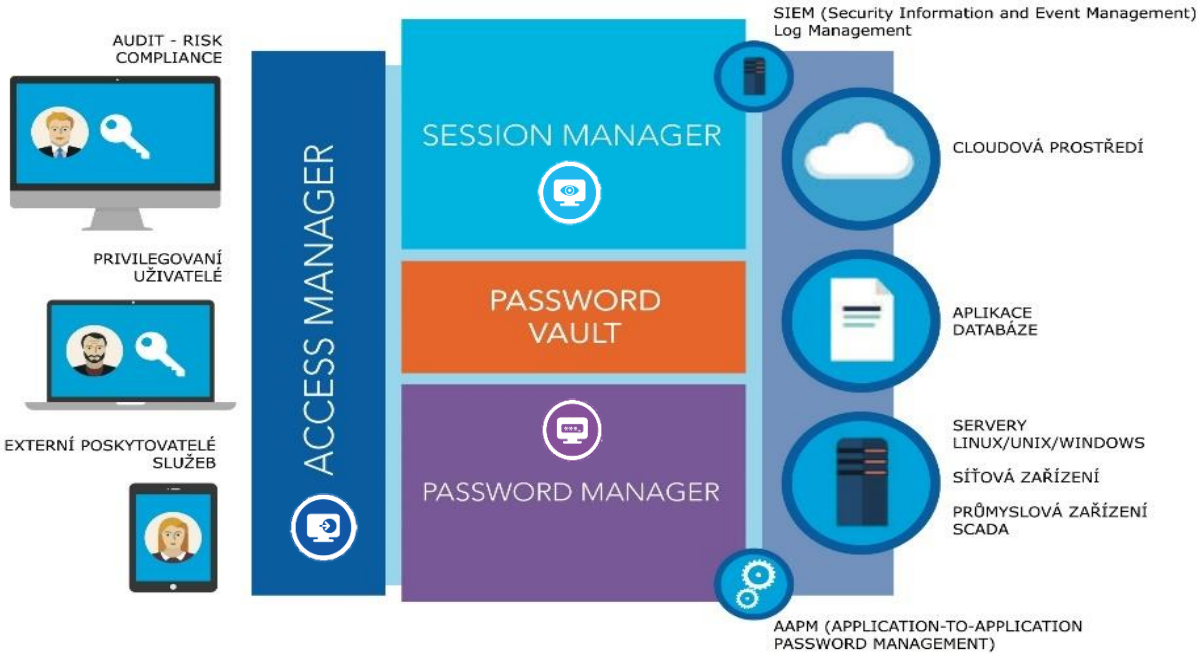
Základní modul s konfigurační konzolí, která obstarává administraci, kontrolu a monitoring privilegovaných uživatelů. Poskytuje reporty a podklady pro audit. Přihlašovací údaje uchovává v zabezpečeném trezoru, koncový uživatel je pro připojení znát nepotřebuje.

Password Manager

Správce hesel určený k řešení jejich životního cyklu a automatizaci periodických obměn. Díky provázanosti celé platformy hesla poskytuje ostatním komponentám. Hesla a SSH klíče uchovává v AES 256 šifrovaném trezoru.

Access Manager

HTTPS portál fungující jako single sign-on „vstupní brána" k více různým instancím WALLIX Bastion. Podporuje multi-tenantní architekturu a je vhodný pro organizace s rozsáhlou či necentralizovanou infrastrukturou.



Protokoly
HTTP/HTTPS, DRP/TSE, SSH, VNC, Telnet, SFTP
Šifrovací alg.: AES 256

Možnosti nasazení
On Premise
Dostupné na AWS a Azure
HW / Virtual Appliance

Metody autentikace
Identifier, LDAP, Active Directory, Radius, TACAS+, Kerberos, X509, OTP, Web SSO

Architektura
3 vrstvy pro škálovatelnost (WALLIX Bastion Farm, Bastion Cluster, bounce server cluster)

COMGUARD security & networking
COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz