COMGUARD

WALLIX
CYBERSECURITY SIMPLIFIED

WALLIX Bastion

Kompromitace a následné zneužití privilegovaných účtů je nepochybně jedním z nejvýznamnějších rizik, kterým naše IT infrastruktury čelí. Tento zásadní milník většiny kybernetických útoků umožní nepozorované obcházení detekčních mechanismů, exfiltraci citlivých dat či znepřístupnění kritických prvků a celkovou paralýzu firemní platformy. Proč bychom měli tyto účty z bezpečnostního pohledu vnímat jako nutné zlo, když existuje efektivní řešení pro jejich zabezpečení a jasné vytyčení pravidel s jejich nakládáním?

WALLIX PAM4ALL

Díky WALLIXu již nadále neplatí, že se u Privileged Access Managementu (PAM) musíte rozhodnout mezi špičkovou technologií nebo snadným nasazením, užíváním a správou – tento Gartner Leader spojil oba atributy ve svém produktu ***Bastion***. Jedná se o proxy-based PAM nástroj s unikátními dočasnými agenty, který je dostupný i ve formě All-In-One appliance. Tato koncepce umožňuje v řádu jednotek dní dosáhnout stavu kompletně řízených přístupů, včetně velice podrobných záznamů průchozích relací. Modulární platformu ***PAM4ALL*** dále doplňují volitelné nástroje ***Authenticator*** pro vícefaktorové ověření, ***Access Manager*** pro usnadnění přístupů externistů, ***BestSafe*** pro granulární správu oprávnění na koncových bodech a ***Trustelem*** pro zajištění silné autentizace běžných uživatelů k jejich webovým a podnikovým aplikacím.

Bastion

Základním modulem Bastionu je komponenta ***Session Manager***, která poskytne administrátorům jednotný bod pro přístup ke kritickým zařízením, aplikacím a prvkům. Po přihlášení administrátora na základě definovaných autorizačních politik působí jako rozcestník umožňující jedním kliknutím přejít na cílový bod – autorizační politiky umožní kromě „kdo a kam" dále definovat i přesné časové rámce či potřebu schválení přístupu určeným pracovníkem. Pro přihlášení na cílovém systému je heslo vyjmuto z šifrovaného trezoru *Password Vault* – uživatel jej tedy **nepotřebuje nadále znát, čímž minimalizujeme riziko jeho úniku**. Díky unikátnímu dočasnému agentovi *Session Probe* je v moment navázání relace na klíčovém bodu spuštěn kód, který umožní velice podrobný sběr metadat – získáme tak náhled do běžících procesů, otevřených oken, úhozech klávesnice, aktivitě clipboardu a dále i širší rámec kontroly nad průběhem relace – možnost testování průchozích souborů antimalware enginem či DLP nástrojem, zamezení odchozích spojení, blacklisting nežádoucích aktivit a další. **Data sesbíraná relační sondou jsou pro případy auditu a investigace snadno vyhledatelná** a doplněná o kompletní videozáznam aktivity.

Komponenta ***Password Manager*** umožní řízení životního cyklu hesel uložených v *Password Vault* – automaticky je obměňuje zde i na cílových systémech v souladu s definovanou politikou komplexity a periodicity, klidně i po každém využití. Tímto zcela eliminuje možnost jejich zneužití. Funcionalita *Application to Application Password Management* dále zajistí zabezpečené předávání přihlašovacích údajů aplikacím a skriptům jako zabezpečenou alternativu k hardcoded heslům.

- Dostupné jako All-In-One appliance – HW / Virtual / Cloud
- Snadná definice a prosazení autorizačních politik
- Možnost podmínění přístupu časovým rámcem či schválením pověřených osob
- Možnost zajištění připojení k libovolnému cílovému prvku – server, aplikace, management konzole, databáze a další
- Možnost spojení s OT prvky Schneider, Siemens, ABB a další nativním protokolem
- Videozáznam s podrobnými metadaty pro účely investigace
- Hloubkový náhled díky *Session Probe* agentovi
- Možnost real-time monitoringu či spolupráce (4 eyes 4 hands mode)
- Zero-trust nástroj pro vyhovění ZoKB, ISO 27001, GDPR, NIST, HIPAA

COMGUARD

WALLIX CYBERSECURITY SIMPLIFIED

WALLIX Bastion

Access Manager

Nadstavbový modul *Access Manager* umožní **centralizaci přístupu k více odděleným instancím** PAM Bastion (Bastion Praha / Bastion Brno či Bastion operativa / Bastion výroba) formou webového portálu s embedded RDP a SSH klienty pro snadné využívání. Dále poskytne **zabezpečenou metodu přístupu externistů** bez potřeby VPN a s kompletní izolací od spravovaného prostředí. V neposlední řadě slouží jako konzole pro *Global Search*, tedy vyhledávání konkrétních aktivit ze separátních PAM jednotek.

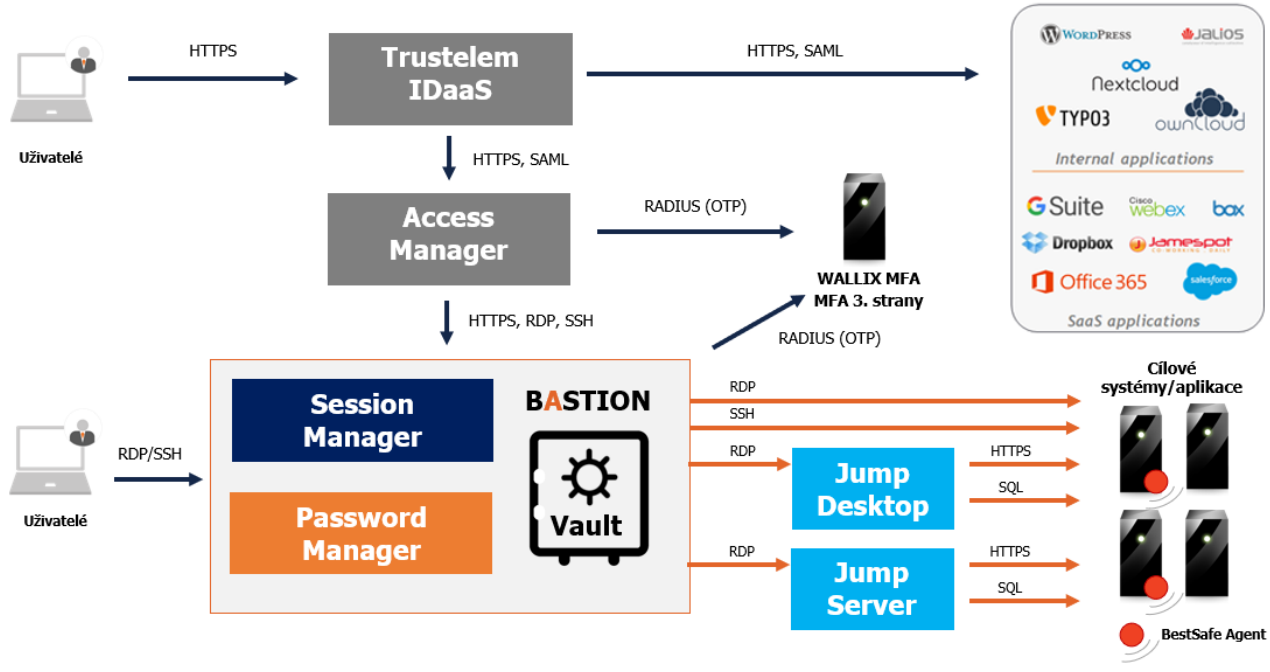
BestSafe

Privilege Elevation and Delegation Management je nástroj využitelný samostatně, i jako součást PAM kaskády. Jedná se o agentské řešení, které na úrovni koncových bodů granulárně **uděluje privilegia pro prosazení principu nejnižších oprávnění**, čímž dále **snižuje rizika** vyplývající z pochybení či pokusu o zneužití předmětných účtů. Účet typu admin je tak v praxi nahrazen běžným účtem, který dokáže s administrátorskou úrovní spouštět pouze definované úlohy a procesy. Toto řešení je mnohdy využíváno i na běžných pracovních stanicích, jejichž uživatelé vyžadují k vykonání práce programové vybavení standardně vyžadující administrátorská oprávnění. Druhotně pak může fungovat jako podpůrný mechanismus ke řešení zabezpečení pracovní stanice – Efektivně blokuje CryproAPI využívané ransomwarem a uzavírá dveře technikám zneužití zranitelností závislým na administrátorském oprávnění – V roce 2019 to bylo 81 % ze 189 kritických zranitelností Microsoft.

Trustelem

Jednotný vstupní bod opatřený silnou autentizací nemusí být vyhrazen pro administrátory – Trustelem je *IDaaS* (*Identity as a Service*) **platforma umožňující SSO přístup uživatelů ke všem webovým či podnikovým aplikacím** využívajícím SAML 2.0, OAuth2 či OpenID Connect. U těchto aplikací lze tak centrálně prosadit silná hesla vícefaktorovou autentizací. Toto řešení je tak výrazně pohodlnější jak z pohledu uživatelů, tak i z pohledu helpdesku, kterému téměř odpadnou požadavky na obnovení hesla. Kombinace cloudové architektury a integrace s adresářovými službami AD, AAD, LDAP či G-Suite pak zajistí možnost nasazení a zprovoznění v řádu hodin.

Referenční architektura



COMGUARD
communication security

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