

WALLIX Bastion

Platforma za upravljanje privilegiranih dostopov

Zavezani zaščiti strateških podatkov in virov

Funkcije in prednosti:

- Polna integracija z obstoječimi okolji s pomočjo univerzalnih povezav in vtičnikov, ki izkoristi prejšnje investicije v varnostne rešitve.
- Platforma zagotavlja enotno točko dostopa, ki jo je mogoče prilagoditi tako, da zadošča edinstvenim potrebam vaše organizacije z uporabo razširljive in združljive arhitekture.
- Preprosta in učinkovita vpeljava za doseganje hitro dosegljivih mejnikov, kar prinaša boljši nadzor nad uvedbo in stroški, ob tem pa tudi optimizira skupne stroške lastništva (TCO).
- Uveljavite skladnost z uredbami s sledljivimi revizijskimi podatki in izločitvijo operativnih nalog iz administrativnega okolja.
- Poiščite, kateri računi predstavljajo tveganje in jih povežite s privilegiranimi računi z orodjem WALLIX Discovery.

WALLIX Bastion: Zavarujte privilegirani uporabniški dostop

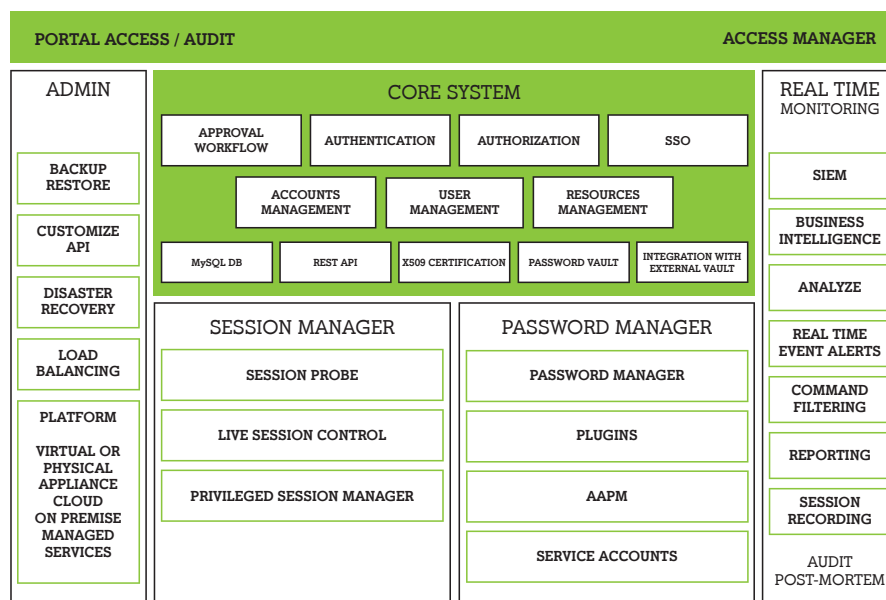
WALLIX Bastion je centralizirana rešitev, ki zavaruje privilegirani dostop in nadzoruje privilegirane seje. Zagotavlja revizijske sledi, ki jih ni mogoče spreminjati in poročila analize vedenja o aktivnostih privilegiranih uporabnikov. Ti viri so uporabni pri sprejemanju varnostnih odločitev in lahko pomagajo preprečiti širjenje zlonamerne programske opreme na druge sisteme.

Jedro WALLIX Bastion

Jedro rešitve WALLIX Bastion vam omogoča zavarovati vaše privilegirane račune in nudi podporo ekipam pri zagotavljanju skladnosti z uredbami. Rešitev vključuje naslednje funkcionalnosti:

- **Administracija**
 - uravnavanje bremen/HA
 - ponovna vzpostavitev
 - varnostne kopije in obnovitev
 - API-ji za upravljanje
- **Revizija/nadzor v realnem času:**
 - nadzor v realnem času za vse aktivnosti privilegiranih uporabnikov z opozorili, poročili in oddaljenimi sejami
 - samodejna prekinitev seje glede na dejavnosti: seznam prepovedanih aktivnosti, poročila dogodkov, procesne sekvence, uporabo tipkovnice (»4 oči«, OCR)
 - odgovornost uporabnikov in sledenje za pripravo statističnih poročil o nadzorovanih aktivnostih z uporabo:
 - video posnetkov in besedila za vse video posnetke
 - celotne revizijske dnevnikne in napredno iskanje ločenih incidentov
- **Hramba gesel**
 - varovanje gesel in ključev SSH v certificiranem WALLIX trezorju
 - odprta arhitektura omogoča integracijo s trezorji drugih proizvajalcev
- **Poročanje**
 - osnovna poročila so dostopna prek uporabniškega vmesnika in jih je mogoče prenesti v datoteki .csvs
 - dvosmerna integracija z orodji SIEM za napredna poročila in obdelavo zaznave škodljivega vedenja v realnem času

WALLIX Bastion vključuje funkcije za upravljanje s sejami, gesli in dostopom preko portala na enotni in razširljivi platformi za optimalno varnost.



Tehnične specifikacije:

Šifrirni algoritem
AES 256.

Način preverjanja pristnosti
Identifier, LDAP, Active Directory, Radius, TACAS+, Kerberos, X509, OTP, Web SSO,
Tehnologije preverjanja pristnosti izvaja WALLIX ALLIANCE PARTNERS-WAP.

Protokoli
HTTP/HTTPS, RDP/TSE, SSH, VNC, Telnet, SFTP.

Nadzorovanje
SNMP in nadzor prek e-pošte z orodji za spremljanje delovanja in delovnih tokov za obvestila administratorjem.

Arhitektura
3 ravni za razširljivost (WALLIX Bastion farma, gruča Bastion, gruča t.i. »bounce« strežnikov).

Integracija/vpeljava
Bastion deluje kot proxy ali v transparentnem načinu.

- Na voljo je za namestitve na lokaciji ali na zahtevo.
- Dosegljiv je prek spletnih storitev AWS & Azure
- Na voljo kot fizična naprava za virtualne stroje ali pa kot programska oprema.

Preprosta vpeljava in sinhronizacija s centralnimi rešitvami za upravljanje identitet za dostop z vmesnikom REST API.

Vtičniki za integracijo z okolji vseh poslovnih partnerjev, ki jih podpira združenje WALLIX ALLIANCE PARTNERS-WAP.

Visoka razpoložljivost in uravnavanje obremenitve
Gruče Bastion.
F5 BIG IP, A10 Thunder.

WALLIX Session Manager

Ta modul omogoča administratorjem upravljanje s sejami privilegiranih uporabnikov v realnem času za izboljšano preprečevanje tveganja:

- upravljanje in nadzorovanje privilegiranih računov na:
 - operacijskih sistemih Unix in Windows, omrežnih napravah, podatkovnih bazah, računalniških mainframe, virtualnih infrastrukturah ali SU/SUDO vnosu,
 - konzolah, poslovnih spletnih aplikacijah in drugih odjemalcih (npr. upravljanje požarnega zidu, Salesforce ali Sage),
 - neposredni dostop do virov z uporabo privzetega odjemalca (PuTTY, WinSCP, MSTC, OpenSSH idr.) s pravili povezave, ki so vgrajena neposredno v Bastion ,
 - delovnem toku, ki je zasnovan z nastavitvami dostopa glede na ustrezni kontekst.
- zbiranje metapodatkov (spremljanje sej), ki so v nadzornih ploščah predstavljeni kot informacije z ustreznim kontekstom,
- oddaljeno upravljanje aplikacij

WALLIX Password Manager

Ta modul omogoča administratorjem upravljanje z gesli in uveljavitev pravilnikov za gesla. Z zagotovitvijo, da imajo uporabniki zgolj dostop do virov, ki jih potrebujejo za izvedbo svojih delovnih nalog, se dvigne stopnja varnosti. To pripomore k zagotovitvi, da ne bo prišlo do razkritja ali zlorabe gesel in ključev SSH:

- uveljavitev redne zamenjave in rotacije gesel

- vključuje namensko knjižnico vtičnikov za upravljanje z gesli za ciljne naprave
- podpora s certifikatom SSH
- upravljanje gesel in računov storitev (Application-to-Application)

WALLIX Acces Manager

WALLIX Access Manager nudi spletni portal za uporabnike in administratorje. Administratorji lahko sledijo delovanju učinkoviteje in v realnem času:

- globalno iskanje po celotni infrastrukturi Bastion
- enotna prijava (SSO) je integrirana prek vseh vpeljanih rešitev Bastion z uporabo arhitekture SSH in RDP
- zaščita virov in sistemov prek nabora pravil, ki lahko uporabniku samodejno dodelijo ali odvzamejo dostop
- prenos na sisteme tretjih strank za preverjanje pristnosti in identifikacijo (SAML 2.0)
- arhitektura s podporo za več instanc, ki je združljiva z okolji ponudnikov storitev in s popolno izolacijo ločenih instanc
- prilagodljiv spletni vmesnik
- ni potrebe po povezavi VPN za oddaljeni dostop