Privileged Password Management & Privileged Session Management

PASSWORD SAFE

Gestione e monitoraggio degli account privilegiati

Il 2018 è stato un anno rivoluzionario per la gestione degli accessi privilegiati, una delle aree più critiche in ambito Cyber Security.

Bomgar, partner tecnologico del Gruppo Daman, con una serie di acquisizioni importanti, come quelle di Avecto, Lieberman e BeyondTrust ha data vita a una nuova entità in grado di fornire una soluzione PAM che non ha paragoni, sia per ampiezza di offerta che per numero di clienti serviti. Riunire tutte queste tecnologie best-of-breed, consentirà infatti alla nuova azienda di fornire la soluzione PAM più completa disponibile fino ad oggi sul mercato.

Bomgar ha deciso di adottare il nome di BeyondTrust, associandolo a un nuovo logo che richiamerà nelle forme grafiche il brand originale Bomgar.

Molte organizzazioni utilizzano account privilegiati condivisi allo scopo di mantenere un set limitato di credenziali per gruppi di utenti, amministratori o applicazioni.

Tuttavia, questa pratica, se gestita in modo errato, presenta significativi rischi per la sicurezza derivanti da un uso improprio dei privilegi condivisi, e questo indipendentemente dal fatto che l'abuso sia intenzionale o solamente accidentale.

La cosa più grave è che, in presenza di abusi, l'account condiviso crea un'oggettiva difficoltà ad attribuire la responsabilità dell'accaduto e quindi a garantire un corretto livello di accountability.

Sono tante le motivazioni che giustificano questo tipo di pratica ed evidenziano un'oggettiva difficoltà a implementare un corretto metodo di gestione, monitoraggio e audit delle credenziali di accesso alle risorse privilegiate.

In uno scenario così complesso, in quale modo le organizzazioni possono assicurare un corretto livello di accountability sugli account privilegiati condivisi, rispettando da una parte i rigidi requisiti di conformità e sicurezza, evitando dall'altra di impattare negativamente sulla produttività degli amministratori?

BEYONDTRUST PASSWORD SAFE

Aumenta il livello Accountability e di controllo sulle Password privilegiate

Password Safe è una soluzione di gestione automatica delle password e delle sessioni privilegiate che garantisce sicurezza, controllo e produttività, per qualsiasi tipologia di account privilegiato.

Attraverso la gestione e il controllo degli account privilegiati, Password Safe riduce sensibilmente i rischi per la **sicurezza** e supporta l'adeguamento delle organizzazioni alle normative attuali in termini di **compliance**.

La soluzione fornisce un accesso sicuro agli account privilegiati garantendo un audit dettagliato, un sistema di alert oltre che la registrazione di tutte le sessioni effettuate.

Password Safe è in grado di prendere in carico e gestire account privilegiati di:

- amministrazione, sia locali sia di dominio
- servizi
- sistemi operativi
- sistemi di rete
- database
- applicazioni
- SSH Key
- spazi Cloud e Social

FATTORI DI UNICITA'

Gestione completa delle Password
Automatizza e rende sicuri i processi di discovery, gestione e rotazione delle Password.

Gestione avanzata delle sessioni privilegiate
Registra, blocca e documenta i comportamenti sospetti, utilizzando un controllo duale che minimizza le interruzioni nelle sessioni e gli impatti sulla produttività.

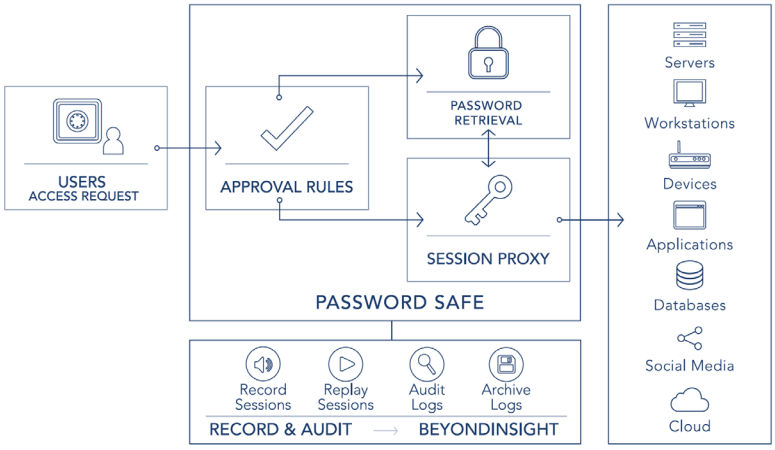
Gestione sicura delle SSH KEY
Ruota automaticamente le chiavi sulla base di una schedulazione e impone il controllo granulare degli accessi e del flusso di lavoro. Utilizza le chiavi private archiviate per garantire accessi sicuri a sistemi Unix e Linux, senza esporre le chiavi agli utenti.

Gestione di Password Application-to-Application (AAPM)
Elimina la necessità di incorporare le credenziali all'interno del codice applicativo, attraverso un'interfaccia API che prevede Password Cache illimitate, garantendo scalabilità e ridondanza.

Policy dinamiche, discovery-driven
Scansiona, identifica e profila tutti gli asset, attraverso un motore di discovery distribuito. Le funzionalità di onboarding automatizzate, includono la definizione dinamiche delle policy e delle classificazioni, che si adattano ai cambiamenti ambientali.

Controllo accessi adattivo
Concede l'accesso in base al contesto di ogni richiesta, considerando parametri come giorno, data, ora e posizione.

Analisi avanzata delle minacce
Correla i dati, collega le prove e determina i rischi correlati con gli utenti e con le risorse. Genera notifiche basate sullo scopo e sulla velocità dei cambiamenti sia nelle caratteristiche delle risorse sia nei comportamenti degli utenti.



PRIVILEGED ACCESS MANAGEMENT

Password Safe è parte della piattaforma BeyondTrust di Privileged Access Management, la quale fornisce visibilità e controllo su tutte le tipologie di account, utenti e risorse privilegiate. La piattaforma è il risultato del processo di integrazione delle soluzioni sviluppate dalle società già leader di settore: BEYONDTRUST, BOMGAR, AVECTO, LIEBERMAN SOFTWARE.

Password Safe:
Garantisce accountability e pieno controllo su credenziali e sessioni privilegiate.

Endpoint Least Privilege:
Rimuove i privilegi eccessivi a livello utente e controlla le applicazioni sugli endpoint.

Secure Remote Access:
Garantisce gestione, controllo e sicurezza sugli accessi privilegiati remoti, per utenti interni e per le terze parti, e sui servizi di assistenza remota.

Vulnerabiliy Management:
Identifica e risolve vulnerabilità sugli accessi privilegiati.

Change Auditing:
Garantisce un pieno controllo sui cambiamenti che intervengono nelle piattaforme Microsoft Windows.

gruppo Daman
Passione e Innovazione

Le soluzioni BeyondTrust sono distribuite in Italia dal Gruppo Daman.

Per saperne di più:
www.gruppodaman.it

Per contattarci:
comunicazione@gruppodaman.it
+39.800.741.423

PRINCIPALI CARATTERISTICHE

Discovery and Profiling

- Individua tutte le risorse (conosciute o sconosciute) gli utenti condivisi e gli account di servizio
- Individua automaticamente tutte le chiavi SSH e i sistemi host
- Identifca e gestisce le risorse che hanno tratti in comune via Smart Rules

Password Protection and SSH Key Management

- Processa selettivamente i cambi password, i test sulle password, le code di notifica a livello account per gruppi di lavoro designatiy
- Supporta gli algoritmi di crittografia standrd. come AES 256 e DES Triplo
- Ruota le chiavi SSH in modo automatico e forza il controllo degli accessi
- Consente di acquisire il controllo oltre gli script, eliminando le credenziali a livello di applicazione, file, codice e chiavi incorporate

Privileged Session Management

- Usa funzioni di ricerca per chiavi per dare agli amministratori la capacità di osservare, registrare, bloccare, terminare o cancellare sessioni attive
- Registra le sessioni privilegiate in tempo reale via servizi proxy per SSH, RDP e TOAD
- E' conforme agli aspetti regolatori definiti in SOX, HIPAA, GLBA, PCI DSS, FDCC, FISMA [...]
- Utilizza la funzione "log off on disconnect" per assicurare che i dati sensibili non vengano esposti sulle sessioni RDP successive
- Permette a tutte le applicazioni Windows di inserire le credenziali di login in modo automatico

Workflow and Usability

- Usa DirectConnect per lanciare sessioni SSH o RDP passando una stringa al proxy
- Valorizza il controllo degli accessi Role-Based, con integrazione verso AD e LDAP per assegnare ruoli e diritti agli utenti
- Un'unica interfaccia con servizi di localizzazione
- Gestisce il workflow di checkout con connettività verso RDP e SSH, via tools di desktop nativo PuTTY and MSTSC
- Ospita richieste fire-call fuori orario o in altre situazioni di emergenza
- Usa Jumphost Unix/Linux per eseguire comandi o script dopo la connessione
- Usa "OneClick" to velocizzare il checkout di password, sessioni e applicazioni

Deployment

- Un'unica soluzione per la gestione di sessioni e password
- Si integra con McAfee ePolicy Orchestrator per realizzare una gestione completa del ciclo di vita degli account privilegiati
- Può essere rilasciata attraverso appliance fisici, virtuali o software
- Impiega connettori out-of-the-box, più un "custom connector builder" per tutti i sistemi che supportano Telenet o SSH

Security and Uptime

- Rilasciato su appliance rinforzate con componenti validati FIPS 1402, crittografia AES256, e comunicazioni HTTPS/SSLv3
- Analizza i comportamenti a livello di password privilegiate, utenti e account con capacità di individuare minacce
- Supporta un numero illimitato di appliance Password Safe con connessione verso un SQL AlwaysOn Availability Group esterno, garantendo un'architettura ad alta disponibilità ed elevata scalabilità.