

ENDPOINT PRIVILEGE MANAGEMENT



Proteggere gli account privilegiati e ottenere la conformità

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 dato 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.

Gestire gli accessi privilegiati è estremamente importante se si vogliono mitigare i rischi provenienti dalle minacce interne e esterne alle organizzazioni. Altrettanto importante è gestire tutti gli Endpoint per eliminare i privilegi non necessari e i diritti eccessivi. Privilegi che diventano spesso un punto di debolezza nell'organizzazione, facile bersaglio del Cyber Crime.

La gestione di questi accessi privilegiati non può quindi essere approcciata in un'ottica o "tutto o niente". E' invece necessario che vengano gestiti adottando una posizione di privilegio minimo e limitando i permessi da amministratore alle sole azioni che devono essere eseguite.

La soluzione BeyondTrust Privilege Management for Unix & Linux è in grado di proteggere gli account con privilegi, ottenere la conformità, prevenire e contenere le violazioni che possono colpire i sistemi Unix e Linux. La soluzione elimina la condivisione delle credenziali, controlla le attività e consente che l'esecuzione di comandi privilegiati avvenga senza la necessità per gli utenti di accedere come root. Tutte le attività degli utenti vengono controllate, per proteggere i sistemi da modifiche non autorizzate a file, script e directory.

FATTORI DI UNICITA'

Auditing & Governance

Analizza il comportamento degli utenti raccogliendo, memorizzando in modo sicuro e indicizzando keystroke log, le registrazioni di sessione e altri eventi privilegiati.

Fine-grained Least Privilege

Eleva i privilegi per gli utenti standard su Unix e Linux attraverso controlli capillari basati su policy.

Dynamic Access Policy

Utilizza elementi come il tempo, il giorno, la posizione e lo stato di vulnerabilità di applicazioni/risorse per prendere decisioni di elevazione dei privilegi.

Remote System & Application Control

Consente agli utenti di eseguire comandi specifici e effettuare delle sessioni da remoto basandosi su regole, senza necessità di accedere come amministratore o root.

File & Policy Integrity Monitoring

Controlla e segnala le modifiche effettuate a policy, sistemi, applicazioni e file dati considerati critici.

Privileged Threat Analytics

E' in grado di correlare il comportamento degli utenti rispetto alle informazioni sulle vulnerabilità degli asset e a quelle sulla sicurezza provenienti da soluzioni di sicurezza best of breed per fornire un quadro generale del rischio per l'utente finale.

BEYONDTRUST ENDPOINT PRIVILEGE MANAGEMENT

MASSIMA PRODUTTIVITÀ CON IL MINIMO PRIVILEGIO

Endpoint Privilege Management elimina i privilegi non necessari e i diritti eccessivi da tutti i dispositivi, senza ostacolare la produttività degli utenti finali. La soluzione è in grado di rimuovere i privilegi eccessivi degli utenti da qualsiasi piattaforma (Windows, Mac, Unix, Linux, dispositivi di rete, Cloud, IoT, DevOps endpoint). Grazie ad un controllo granulare sulle applicazioni e sui comandi, è in grado di implementare il concetto di minimo privilegio.

Endpoint Privilege Management è inoltre di rapida implementazione grazie al modello out-of-the-box.

Limita gli accessi Root

Fornisce regole capillari di elevazione dei privilegi necessarie ad eseguire solo specifici task o comandi.

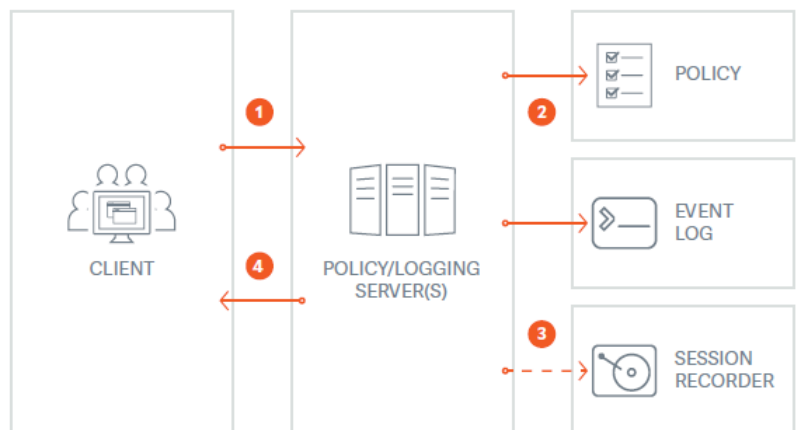
Controlla tutte le attività degli utenti

Protegge file, script e directory da modifiche non autorizzate.

Monitora log e sessioni

Rileva in tempo reale le attività sospette di account, user e asset.

HOW IT WORKS



1 User requests are sent to the policy servers

2 Requests are checked against central policy

3 Request is written to central event log, with optional session recording

4 Policy decision is sent back to the user

PRIVILEGED ACCESS MANAGEMENT

Endpoint Privilege Management 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.

VULNERABILITY MANAGEMENT:

Identifica e risolve vulnerabilità sugli accessi privilegiati.

CHANGE AUDITING:

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



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

VANTAGGI

Garantisce la conformità

- Fornisce un controllo ineccepibile di tutte le attività degli utenti.
- Abilita la conformità attraverso la compartimentalizzazione delle attività IT che richiedono account con privilegi.
- Assicura che i file e le politiche critiche non siano stati manomessi.

Garantisce la sicurezza di sistemi e file critici

- Limita le superfici di attacco fornendo un accesso sufficiente per completare un'attività.
- Evita l'uso dell'account root.
- Abilita solo le applicazioni/comandi la cui esecuzione è stata approvata.
- Elimina workaround o gap che potrebbero portare a exploit.
- Consente di prendere decisioni sui privilegi in base al contesto e al rischio.
- Protegge i file critici da malware e uso improprio.

Migliora l'efficienza

- Razionalizza i processi complessi con Sudo.
- Semplifica la gestione e velocizza le implementazioni grazie a una console di gestione centralizzata.



Piattaforme supportate

BeyondTrust Privilege Management for Unix & Linux supporta più di 100 piattaforme diverse, incluso Debian GNU, HP-UX, HP Tru 64, Red Hat Enterprise Linux, Sun Solaris, SuSE Linux Enterprise, VMware ESX, IBM AIX, e molti altri.