BeyondTrust

La gestione degli account privilegiati

Controllare e monitorare gli accessi privilegiati è oggi una sfida molto complessa. Dipendenti, collaboratori e terze parti hanno spesso autorizzazioni di accesso non necessari o eccessivi a sistemi e dati.

Gestire questi accessi è diventato estremamente importante se si vogliono mitigare i rischi provenienti dalle minacce interne e esterne, prevenire la violazione dei dati e, non ultimo, soddisfare i requisiti di conformità. I responsabili della sicurezza e dell'IT hanno un compito particolarmente complesso: conciliare la necessità di garantire la massima sicurezza ai sistemi e ai dati critici da qualunque possibile violazione, e fornire agli utenti, ai collaboratori e terze parti l'accesso per renderli produttivi.

LA SOLUZIONE PAM PIÙ COMPLETA DISPONIBILE OGGI SUL MERCATO

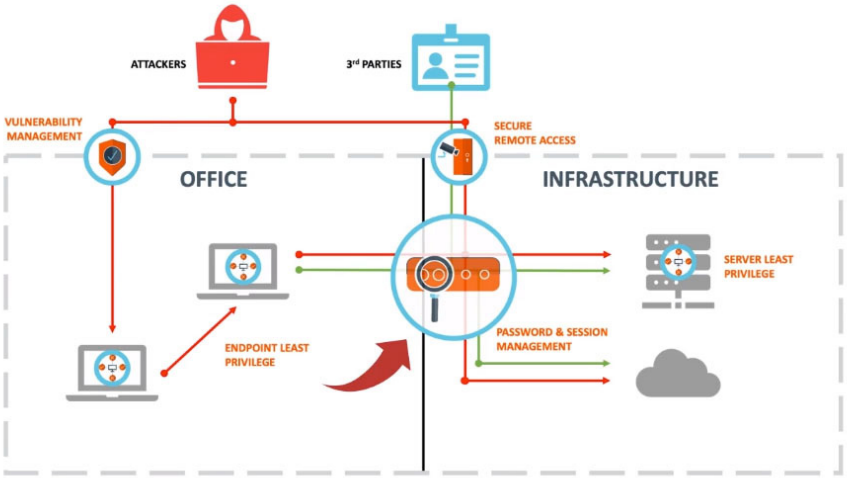
Il 2018 sarà considerato un anno rivoluzionario per la gestione degli accessi privilegiati, una delle aree più critiche in ambito Cyber Security.

Proprio nel 2018, Bomgar con una serie di importanti acquisizioni, come quelle di Avecto, Lieberman e BeyondTrust ha creato i presupposti per la nascita di una nuova entità in grado di fornire una soluzione PAM che non ha paragoni.

Aver riunito tutte queste tecnologie best-of-breed in un'unica piattaforma, ha permesso a Bomgar, che ha deciso di adottare il nome di BeyondTrust, di realizzare la soluzione PAM più completa disponibile fino ad oggi sul mercato, sia per ampiezza di offerta che per numero di clienti serviti.

Sicurezza Vs Produttività: la sfida

La maggior parte delle organizzazioni è costituito da un'ambiente IT diviso in due parti: le postazioni di lavoro e le infrastrutture. Purtroppo creare un perimetro solido, chiuso e sicuro intorno a ciascuna di queste parti è praticamente impossibile. Sono infatti molte le ragioni legittime per cui questo perimetro deve essere attraversato: gli amministratori di sistema necessitano di poter accedere da remoto, così come fornitori e terze parti. Non ultimo l'utilizzo di piattaforme Cloud che rende il concetto di perimetro ancora più vago. Gli attacchi Cyber non arrivano solo dagli accessi remoti privilegiati, ma anche da accessi interni Ma non sono solo gli accessi remoti a essere oggetto di attacco Cyber. Il 28% degli attacchi deriva infatti dall'utilizzo fraudolento di accessi legittimi con privilegi.

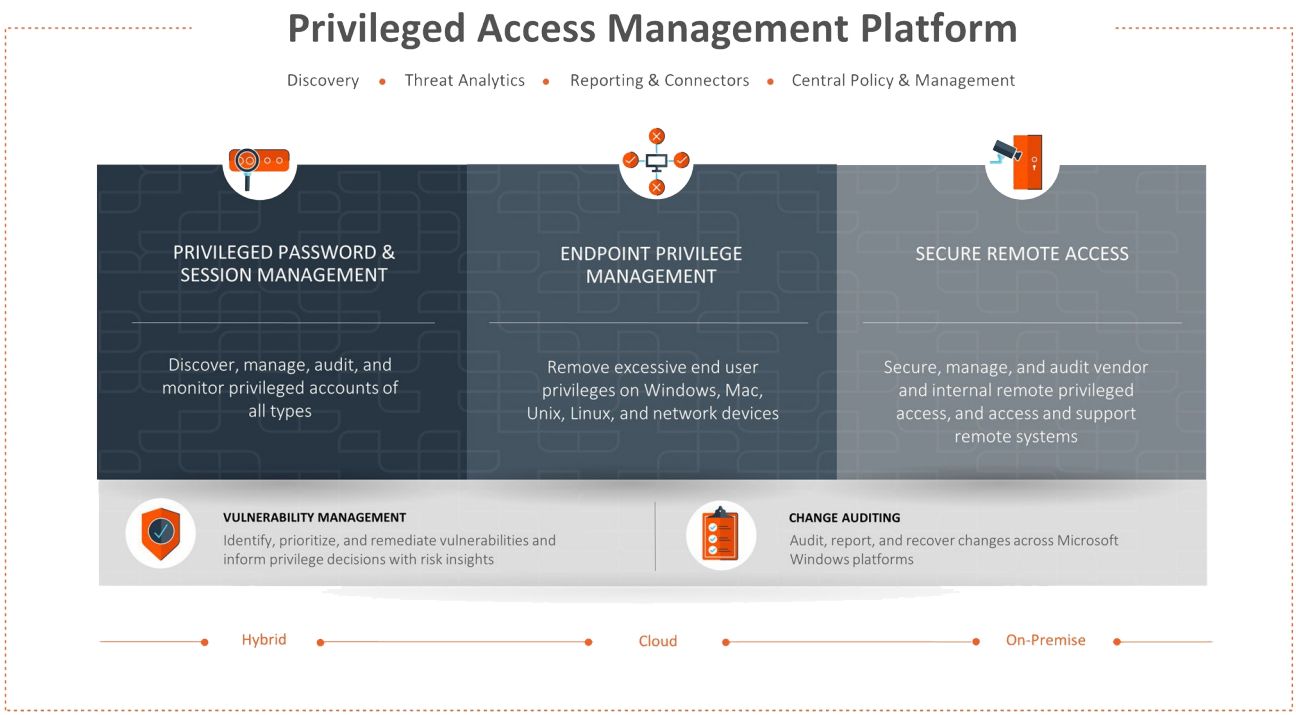


Sicurezza Vs Produttivita

La piattaforma BeyondTrust

La piattaforma di gestione degli accessi privilegiata BeyondTrust aiuta a gestire gli attacchi del Cyber Crime con una soluzione integrata che offre visibilità e controllo su tutti gli account e gli utenti con privilegi, riducendo i rischi e allo stesso tempo migliorando la produttività.

La soluzione BeyondTrust offre infatti la più ampia gamma di funzionalità nella gestione degli accessi privilegiati con un design flessibile che semplifica le integrazioni, migliora la produttività degli utenti, ottimizza gli investimenti dell'IT e riduce i rischi che derivano da una cattiva gestione delle credenziali privilegiate.



PRIVILEGED PASSWORD & SESSION MANAGEMENT

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, che possono derivare da un uso improprio dei privilegi condivisi.

La soluzione BeyondTrust Password Safe offre una 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 alle normative in termini di compliance. La soluzione fornisce un accesso sicuro agli account privilegiati garantendo un audit dettagliato, un sistema di alert e la registrazione di tutte le sessioni effettuate.

Password Safe gestisce account privilegiati di:

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

La soluzione Password Safe offre:

- Automated Discovery
- Privileged Session Management
- App-to-App Password Management
- Secure SSH Key Management
- Adaptive Access Control
- Privileged Threat Analytics

ENDPOINT PRIVILEGE MANAGEMENT

In un organizzazione capita frequentemente che gli utenti abbiano bisogno di alcuni diritti da amministratore per portare a termine il loro lavoro. Per proteggere gli Endpoint non è pensabile eliminare completamente tali diritti senza influire negativamente sulla produttività degli utenti.

La gestione di tutti gli Endpoint diventa un'attività complessa e particolarmente delicata 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 soluzione 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 rimuove 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.

Le piattaforme supportate dalla soluzione

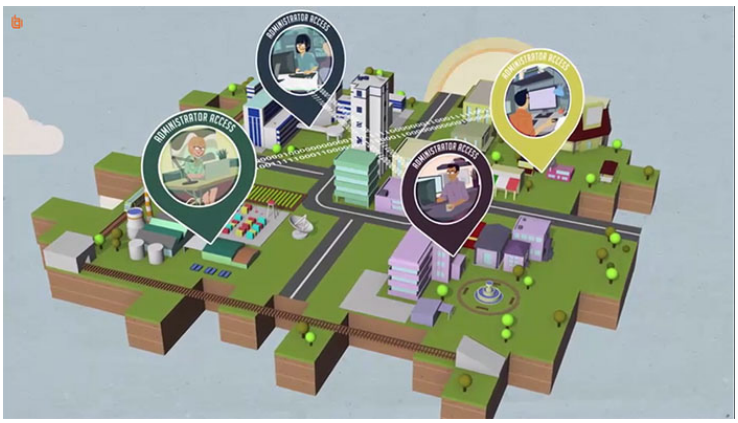
- Desktop
- Server Window
- Server Unix e Linux
- Dispositivi di rete

PRIVILEGED REMOTE ACCESS

Gli account privilegiati, rilasciati a personale interno ed esterno, sono la strada maestra utilizzata dal "cyber crime"per violare la sicurezza perimetrale e inserirsi all'interno della rete aziendale senza lasciare alcuna traccia di questo passaggio.

La situazione diventa ancora più critica quando questi accessi privilegiati vengono effettuati da remoto, con l'utilizzo di una VPN oppure sfruttando i protocolli RDP.

La soluzione Privileged Remote Access consente la gestione dei privilegi di acceso e il controllo delle sessioni remote in totale sicurezza e nel rispetto delle regole di compliance, senza ostacolare il lavoro degli utenti. Il controllo degli accessi privilegiati avviene applicando una politica di privilegio minimo che fornisce agli utenti il livello di privilegio necessario al proprio ruolo, con responsabilità individuale per gli account condivisi.



Privileged Remote Access consente di:

- Eliminare una minaccia per la Cyber Security, fornendo a chi si occupa di manutenere i sistemi critici un accesso privilegiato alle risorse, senza dover però fornire una VPN.
- Rispettare la Compliance, con una soluzione che soddisfa i requisiti di conformità interni ed esterni (incluso il GDPR).
- Gestire gli accessi privilegiati, consentendo agli utenti di svolgere il proprio lavoro più velocemente e facilmente.

VULNERABILITY MANAGEMENT

Le odierne infrastrutture IT sono spesso molto complesse, un mix di sistemi fisici e virtuali, ambienti basati su cloud, reti derivate da fusioni e acquisizioni.

Gli strumenti che si occupano di segnalare le vulnerabilità non sempre riescono, proprio a causa della complessità, a fornire un aiuto concreto alle organizzazioni. Sopratutto perché la necessità è spesso quella di comprendere rapidamente i rischi reali per poter assegnare correttamente le giuste priorità alle attività di risanamento.

Vulnerability Management è una soluzione di gestione delle vulnerabilità in grado di fornire una visione olistica sulla sicurezza e sui livelli di rischio anche in ambienti IT molto complessi.

La soluzione scansiona, identifica e valuta le vulnerabilità tra tutte le risorse (on-prem, cloud, mobile, virtual, container) all'interno dell'organizzazione.

Vulnerability Management è in grado di assegnare alle vulnerabilità identificate le giuste priorità, grazie ad un'analisi approfondita che tiene conto dell'impatto sul business e delle informazioni fornite da soluzioni di terze parti.

Ciò consente di effettuare solo gli interventi di risanamento effettivamente necessari per mettere in sicurezza le attività di business ed essere compliance con le normative vigenti.

La soluzione Vulnerability Management offre:

- End-to-End Management
- Zero-Gap Coverage
- Risk in Context
- Deep Reporting & Analytics
- Integrated Scanning

CHANGE AUDITING

Mitigare i rischi derivanti da modifiche indesiderate e comprendere le attività degli utenti per meglio soddisfare i requisiti di conformità è oggi essenziale per tutte le organizzazioni IT. Le infrastrutture Windows possono rappresentare in quest'ottica un elemento di criticità in mancanza di un controllo centralizzato e in tempo reale delle modifiche che vengono effettuate a risorse sensili come le Active Directory e i File System.

Change Auditing fornisce un controllo centralizzato e in tempo reale delle modifiche effettuate in Active Directory, file system, Exchange, SQL e NetApp. La soluzione è in grado di verificare "chi, cosa, dove e quando" effettua tali modifiche e inviare un Alert per ogni modifica effettuata.

La soluzione Change Auditing offre:

- Auditor for Active Directory
- Recovery for Active Directory
- Privilege Explorer per Active Directory e File System
- Auditor for File Sistem
- Auditor for Exchange
- Auditor for SQL Server

Change Auditing offre la possibilità di ripristinare oggetti o attributi di Active Directory, proteggendo in questo modo il business dai tempi di inattività.

Fornisce inoltre report sulle autorizzazioni e assicura che gli utenti abbiano accesso solo alle risorse necessarie per svolgere il proprio lavoro.

Con una gestione così semplificata le organizzazioni IT possono mitigare i rischi derivanti da modifiche indesiderate e comprendere le attività degli utenti per meglio soddisfare i requisiti di conformità.

Via Mario Bianchini 51
00142 Roma

NUMERO VERDE 800.741.423 SERVIZIO GRATUITO

gruppo Daman
Passione e Innovazione

www.gruppodaman.it
www.cyberguru.it
comunicazione@gruppodaman.it