filter:max

Delinea portfólió ismertetése

1118 Budapest, Muskotály utca 11. info@filtermax.hu www.filtermax.hu
tel.: +36 20 520 0967

Tartalomjegyzék

Cégismertetés 3
Programok 3
Delinea Secret Server 3
A Secret Server előnyei 3
Összefoglaló 4
Delinea Privilage Manager 5
A Delinea Privilage Manager előnyei: 5
Összefoglaló 6
Delinea Server PAM 6
A Delinea Server PAM előnyei 6
Összefoglaló 7

Cégismertetés

2021 áprilisában, a Centrify és Thycotic vállalkozás egyesítette erejét és megalapították közös cégüket, amit akkor ThycoticCentrify néven indítottak útjára. 2022 januárjában az egyesülés végleges lett és egy nagyszabású márkaváltással, Delinea néven folytatták közösen útjukat, hogy felvegyék a kiber fenyegetések elleni harcot. Ettől a dátumtól kezdve a Delinea programjai egyesítette a két gyártó előnyeit és egy megújult, de funkcióban hasonló megoldás portfólióval állt elő.

Programok

A Delinea programjai között, találunk megoldást privilegizált hozzáférés kezelésre, jelszó biztonságos kezelésre, valamint távoli munkavégzés ellenőrzött végrehajtására.

Az elérhető programok listája:

Delinea Secret Server

Delinea Privileged Behavior Analytics

Delinea DevOps Secrets Vault

Delinea Account Lifecycle Manager

Delinea Server PAM

Delinea Privilege Manager

Delinea Connection Manager

Remote Access Service

Delinea Platform

Delinea Secret Server

Ahogyan a kiber fenyegetések egyre nőnek mennyiségben és komplikáltságaikban fejlődnek, úgy növekszik az igény egy kifinomult, effektív és rugalmas, emelt szintű hozzáférés (PAM) alkalmazásra, ami bármilyen terjedelmű cégnek manapság üzlet kritikus. A Secret Server alkalmazásával egy határozott megoldást nyújtunk akár nagyvállalati szinten is, akár on-premises környezetben, akár a felhőben a Delinea Platform segítségével. Bátran ajánljuk mind az információ biztonsági, mind az IT csapatoknak, hogy alkalmazzák ezt a környezetükbe, így könnyen és biztonságosan tudják kezelni az emelt szintű hozzáféréseket.

A Secret Server előnyei:

Privilegizált felhasználói adatok védelme

A program széfjeinek használata, megőrzi a jelszavakat, titkos adatokat, kulcsokat és minősítéseket a cégen belül.

Proaktív védelemet nyújt automatikus jelszó generálással, cserével és lejárati idők meghatározásával

Inteligens munkafolyamatok melyek tartalmazzák a „kikérés” funkciót, privilegizált hozzáférések igénylését, azok elfogadásának és tiltásának lehetőségét több lépcsős folyamatban

Támadási felület csökkentése

A discovery funkció segítségével feltárhatjuk a nem kezelt privilegizált felhasználókat az egész cég környezetében

Az automatikus jelszó cserék biztosítják a jelszavak aktualizálását, anélkül, hogy bármilyen jogosultságot megtörne

DevOps munkafolyamat kiterjesztése PAM védelemre a fejlesztői és üzemeltetői oldalra

Privilegizált hozzáférések kezelése

Saját részletes szabályrendszer kialakítás, amit bármelyik privilegizált felhasználóra alkalmazhatunk

Egyéni scriptek támogatása lehetőséget ad a felhasználónak, hogy a különböző integrációkat, függelékeket

Gyanús folyamatok észlelése

Valós idejű munkamenet menedzselés, ami tartalmaz felvétel készítést, megfigyelést és billentyű loggert

SIEM rendszerekkel való integrációja és sérülékenység vizsgálatok betekintést engednek, egy esetleges incidens megoldására

Viselkedés vizsgáló rendszerekkel való integrációja segíti a rendellenes felhasználói viselkedés azonosítását

Audit és jelentés

Változtathatatlan audit log segítségével bebizonyítható a megfelelőség bármilyen leglegjobb eljárásnak vagy szabályozási keretnek

Tagolt, kereshető log-ok megegyeznek a törvényszéki felülvizsgálat elvárásainak

Összefoglaló

A PAM vezérlők védelmet biztosítanak a kritikus rendszerekhez való hozzáférésre, az IT végrehajtói és biztonsági csoportok átfogó, házirend alapú vezérlésekkel kezelhetik a Secret Server-t. A rendszer lehetővé teszi, hogy a hatékony PAM megoldásokat, leegyszerűsítse és intuitív kezelőfelületével megkönnyítse.

Delinea Privilage Manager

A felhasználói munkaállomások nagyon gyakori betörési pontok a különböző kibertámadásoknak. A kiberbűnözők ezeken az állomásokon keresztül különböző malware, ransomware és más káros támadásokkal próbálnak bejutni és megakadályozni a megfelelő működését az informatikai környezetnek. A munkaállomáson keresztül pedig, a különböző támadásokkal az itt szerzett hozzáférést magasabb szintre emelve, akár rendszer adminisztrátori jogosultságot szerezve kritikus rendszerek működését szakíthatja meg

Delinea Privilage Manager-e lehetőséget nyújt a legkisebb jogosultság elve alapján való kialakítását környezetünkbe, ezzel a munkaállomások adminisztrátori jogosultságait megszüntetve. A jogosultság növelés éa a beépített alkalmazás irányítás biztosítja a szünetmentes és biztonságos munkavégzést a munkaállomásokon.

A Delinea Privilage Manager előnyei:

A legkisebb jogosultság bevezetése és alkalmazása

- Túl nagy kiváltságok megszüntetése és a helyi csoportok tagjainak állandó kezelése
- Folyamatos felfedezése az alkalmazásoknak és folyamatoknak, amelyek privilegizált felhasználókkal működnek

Részletes alkalmazás irányítási szabályok létrehozása

- Az alkalmazottaknak lehetőséget adni a programok használatára mely a munkához szükségesek, anélkül, hogy helyi adminisztrátorok lennének
- Központi kezelés szabályrendszerekkel, threat intelligence és engedélyező vagy tiltó listával

Csökkenti az IT támogatás költségeit

- A helpdesk újabb jegyeinek nyitását elkerülhetjük a jogosultság kérések tárgyában
- A különböző hardveres problémák elkerülése az egységesített munkaállomások jogosultságainak kezelése miatt
- A produktivitás tartása és növelése különböző integrációkkal, mint például ServiceNow és mobil alkalmazás segítségével

Munkaállomások védelme

- Automatikus felfedezése és megszüntetése az admin jogosultságoknak a domain-ben és akár azon kívüli munkaállomásokon, Windows, Unix/Linux vagy Mac eszközökön is.

Akár cloud, akár on-premises implementáció és egyszerű skálázhatóság

- Több ezer munkaállomás kezelése egyidejűleg
- Szabad skálázhatóság, köszönhetően a flexibilis szerkezetnek

Összefoglaló

Házirendi szabályok beállítása és kezelése, biztonsági és üzleti igényeinek megfelelően. A Delinea Privilage Manager, a legátfogóbb privilege elevation és alkalmazás vezérlő megoldás a munkaállomásokra, amely képes a vállalkozások és gyorsan növekvő szervezetek igényeihez alkalmazkodni, akár felhős mértékben. A munkaállomásokról a felesleges jogosultságok eltávolításával megakadályozzuk a rosszindulató programok támadásait, a házirend alapú alkalmazásvezérlők pedig a folyamatos munkavégzési biztosítják. A jelentések és log-ok összessége, pedig megfelelést biztosít a vezetésnek és a vizsgálatoknak.

Delinea Server PAM

A digitális átalakulás, továbbra is képes megzavarni a vállalati környezetek működését, köszönhetően a komplexitás fokozódásának és az identitások tördelésének. A modern PAM megoldások a legkisebb privilégium elvén a felhasználók által ért támadások ellen véd, míg a zero trust pedig a legfrissebb és fejlődő támadások elleni identitáson alapuló fenyegetések ellen véd. A Delinea Server PAM egy nagyszabású átalakítást biztosít, modernizálva a szervezetek hozzáférés kezelését a szerverekhez, mind on-premises, mind cloud környezetben. A program lehetővé teszi az emberek és gépek számára a zökkenőmentes hitelesítést, kikényszerítve a least privilege elvét és a just in time privilege együttes kombinációját, ezzel növelve a láthatóságot és csökkenti az adminisztratív kockázatokat.

A Delinea Server PAM előnyei

Központosított identitás és szabályzat vezérlés

Válaszd ki számodra a legmegfelelőbb megoldást! A privilegizált hozzáférések, az MFA szabályok kezelése, az Active Directory Patented Zone technológia segítségével. Ezzel a technológiával megszilárdítja az alapvetően komplex kezelését a nem active directoryba tartozó nem windows-os eszközök központosított irányítását.

Identitás megerősítése fejlett active directory bridge technológiával

Delinea Server PAM kiterjeszti az Active Directory szabályait és autentikációs előnyeit LINUX és UNIX platformokra, így megkönnyítve az adminisztrátori munkákat egy központosított kezelő felület segítségével.

Multi-directory brokering

Autentikációs közvetítés Active directory, OpenLDAP felé, valamint felhő alapú szolgáltatások felé is, mint például Azure AD, Okta vagy Ping, anélkül, hogy közvetlen kapcsolatot kellene felépítenie a Linux vagy Windows szervereknek

Cloud-Native

Használd ki a felhő előnyeit egy modern PAM megoldással, ami kifejezetten a hibrid környezetekre lett fejlesztve.

Multi-factor autentikáció

Blokkolja a különböző malware és ransomware támadásokat, valamint ezzel a lateral movement támadásokat is meggátolja, mivel a rendszerbejelentkezésekkor és jogosultság kérésekkor is szükséges az MFA megadására

Host alapú auditálás, jelentés és munkamenet rögzítés

Könnyen észlelhető káros tevékenységek, melyek a biztonsági rendszerek megkerülésével a felhasználókhoz rendeli a tevékenységeket. Minden magas jogosultsággal rendelkező tevékenységek ellenőrzése, tevékenységek naplózása, részletes jelentésekkel, melyek megfelelnek az auditálási kötelezettségeknek, valamint segítséget nyújtanak a javítási intézkedéseknek.

Összefoglaló

Az emelt szintű hozzáférés kezelését lehetővé teszi mind on-premises, mind felhős környezetben. A Server PAM lehetőséget ad a cégeknek, hogy kezükbe vegyék az irányítást a privilegizált hozzáférések felett, központi irányítással és szabályrendszerekkel. A multi-directory brokering leegyszerűsíti és megszilárdítja az adminisztrátori hitelesítéseket, ezzel megteremtve a megbízható kapcsolatot eltérő identitás szolgáló programok és a Windows vagy Linux szervereink között, legyen szó bármilyen hibrid környezetről. Ezen kívül a privilege elevation valamint az MFA újabb biztonsági faktorok, amivel növeljük a kritikus szerverekhez való biztonságos hozzáféréseket. Valós idejű munkamenet megfigyeléssel, valamint a rögzítés funkcióval pedig biztosítjuk a teljes láthatóságot és az események részletes leírását.