BALASYS

One Identity Safeguard for Privileged Passwords

Csökkentse a megosztott privilegizált hozzáférésekből eredő kockázatot

A közelmúltban történt biztonsági incidensek újra rávilágítottak arra, hogy az IT rendszerek legsérülékenyebb – egyben a legnagyobb károkozási potenciállal rendelkező – elemei a privilegizált fiókok jelszavai. Ezek a jelszavak "kulcsok a királysághoz". Ha a hackerek megszerezték őket, korlátlan hozzáférést kapnak az Ön rendszereihez és adataihoz. És, ahogyan a hírekből Ön is láthatja, ez óriási kárt tud okozni az érintett szervezet hírnevében és szellemi tulajdonában.

A privilegizált jelszavak védelme sok kellemetlenséget okoz, és csökkenti a produktivitást, mind a napi, mind a hosszú távú működés során. Ez a dilemma kényelmetlen helyzetbe hozza az IT managereket és a biztonsági szakembereket: a biztonságot vagy a könnyű használhatóságot válasszák? A One Identity Safeguard for Privileged Passwords segítségével Ön mindkettőt megkaphatja.

A One Identity Safeguard for Privileged Passwords automatikus munkafolyamatokkal és szerep alapú hozzáférés-kezeléssel automatizálja, kontrollálja és biztonságossá teszi a privilegizált felhasználói jelszavak kezelését. A Safeguard for Privileged Passwords hardened appliance-re telepítve kerül szállításra, ami garantálja a magához az eszközhöz való biztonságos hozzáférést, és felgyorsítja a rendszereivel és IT stratégiájával való integrációt. Felhasználóbarát felülete gyorsan megtanulható. A jelszavak bárhonnan és szinte bármilyen eszközről kezelhetők. Az eredmény pedig egy olyan megoldás, amely biztonságossá teszi a vállalatát, és a privilegizált felhasználóinak a szabadság és funkcionalitás új szintjét biztosítja.

ELŐNYÖK

- Csökkenti a biztonsági incidensek által okozott kárt a privilegizált felhasználói fiókokhoz való hozzáférés kontroljával.
- Könnyedén teljesíti a privilegizált felhasználói fiókokra vonatkozó megfelelősségi előírásokat.
- Gyorsabb megtérülés az egyszerűsített telepítésnek és menedzsmentnek köszönhetően.
- Maximális termelékenység, rövid tanulási görbével és korszerű felhasználói felülettel.
- Egyszerűbb és gyorsabb audit jelentéskészítés.

FUNKCIÓK

Release control

Kezeli a jogosultsággal rendelkező felhasználóktól érkező jelszókérelmeket. A felhasználók egy biztonságos böngésző-kapcsolaton keresztül kapnak hozzáférést, ami a mobilesz-közöket is támogatja.

Workflow Engine

A Workflow Engine támogatja az időkorlát beállítást, a jóváhagyást és áttekintést több szinten, a vészhelyzeti hozzáférés kezelését, valamint lehetőség van a policy-k érvényességét beállítani, hogy az meddig legyen érvényes. Ezen kívül lehetőség van „reason" kódok megadására, és a ticketing rendszerekkel való integrálásra. Jelszókérelmet automatikusan jóvá lehet hagyni, vagy bármilyen szintű jóváhagyási folyamat beállítható.

Kedvencek

Már a bejelentkezési képernyőről hozzáférhet a leggyakrabban használt jelszavaihoz.

Jóváhagyás bárhonnan

A One Identity Starling-ot kihasználva, Ön bárhonnan jóváhagyhat vagy elutasíthat bármilyen jelszókérelmet VPN hozzáférés nélkül is.

Mindig online

Disztributált cluster tervezésnek köszönhetően valódi magas rendelkezésre állást (high availability) kap.

Ezen felül, a terheléselosztásnak köszönhetően a jelszókérelmek és munkamenetek magasabb teljesítménnyel és alacsonyabb válaszidőkkel párosulnak, miközben bármilyen eszközről igényelheti azokat.

RESTful API

A Safeguard egy modernizált, a REST-en alapuló API interfészt használ a más rendszerekkel és alkalmazásokkal való csatlakozáshoz. Ezen a felületen minden funkció elérhető, és lehetővé válik a könnyű és gyors integráció függetlenül az alkalmazások programozási nyelvétől.

Tevékenységközpont (Activity Center)

A lekérdezés készítő segítségével könnyen és gyorsan áttekinthet minden tevékenységet. Attól függően, hogy ki igényelte a jelentést – például az IT üzemeltetés vagy az ügyvezetők – hozzáadhat vagy elvehet adatokat, hogy pontosan azt az információt jelenítse meg, amire szükség van. Ezen felül a lekérdezések időzíthetők, az adatok pedig menthetők és exportálhatók különféle formátumban.

Felderítés (Discovery)

Gyorsan feltérképezi a privilegizált felhasználói fiókokat vagy rendszereket az Ön hálózatán, host, directory, vagy hálózat felderítési opciókkal.

Kétfaktoros authentikáció

A jelszavakhoz való hozzáférést nem elég egyszerűen egy másik jelszóval védeni. Növelje a biztonságot a kétfaktoros authentikáció megkövetelésével. A Safeguard támogatja a RADIUS alapú kétfaktoros megoldásokat és 25 darab licencet tartalmaz a Starling Two-Factor Authentication felhőszolgáltatásához.

Smartcard támogatás

Használja saját erős hitelesítési módszereit, hogy biztonságban tartsa a jelszószéfhez való hozzáférést.

A One Identity privilegizált felhasználó-kezelési koncepciója

A One Identity portfóliója az iparág legátfogóbb privilegizált felhasználó-kezelési megoldása. Ön bátran építhet a Safeguard for Privileged Sessions átfogó funkcionalitására, ezen belül a privilegizált felhasználói jelszó-kezelésre és a privilegizált felhasználói elemző megoldásokra. Termékpalettánkon megtalálhatók a UNIX root-, és Active Directory adminisztrátor account delegálási megoldások, egyéb kiegészítő modulok, amelyekkel például az open source sudo nagyvállalati környezetbe illeszthető, vagy billentyűzet leütés figyelő alkalmazás UNIX root tevékenységekhez – mindez szorosan integrálva az iparág vezető Active Directory bridge megoldásunkkal.

A One Identity-ről

A One Identity segít a cégeknek a jogosultság és hozzáférés-kezelést (Identity and Access Management, IAM) jól csinálni. Jogosultság szabályozást (identity governance), hozzáférés-kezelést, kiemelt-felhasználó kezelést és jogosultságot, mint szolgáltatást (identity as a service) tartalmazó egyedi termékportfóliója támogatja a szervezeteket üzleti lehetőségeik teljes kihasználásában, mindezt biztonsági béklyók nélkül, mégis védelmet nyújtva a fenyegetések ellen.

ONE IDENTITY™