BALASYS

One Identity Safeguard

Tárolja, kezelje, rögzítse és elemezze biztonságosan a privilegizált felhasználói hozzáféréseket

ELŐNYÖK

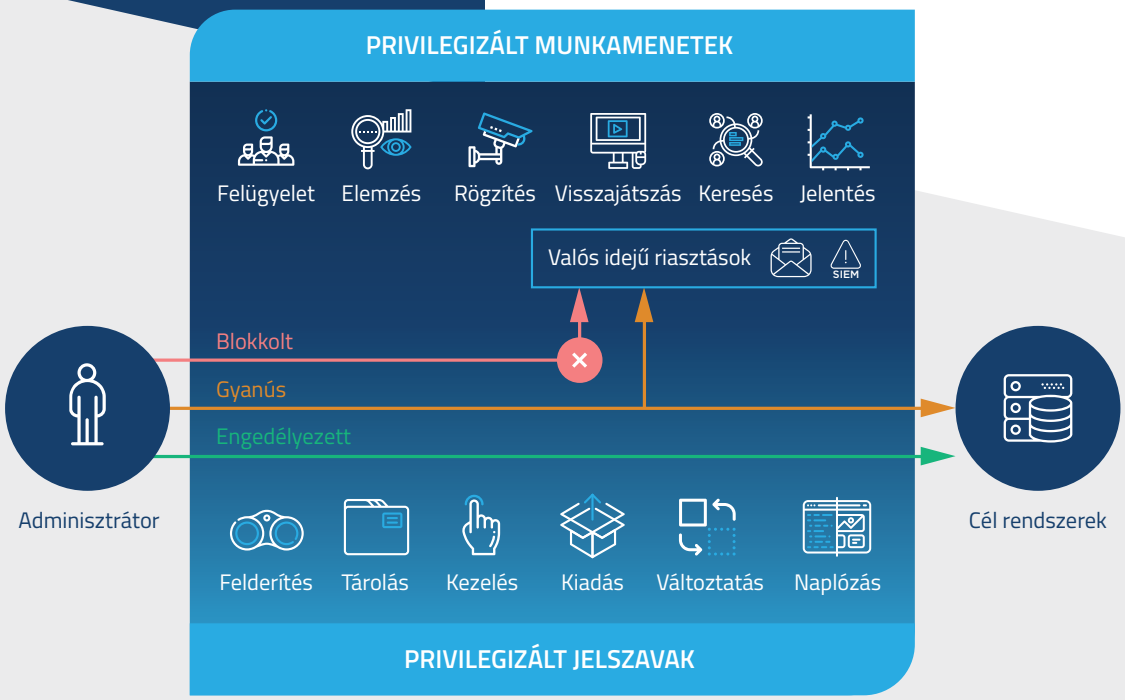
- Csökkenti a potenciális biztonsági incidensek kockázatát
- Teljesíti a törvényi megfelelés követelményeit
- Gyors megtérülést nyújt az egyszerű telepítésnek és üzemeltetésnek köszönhetően
- Hatékony audit jelentéseket készít
- Azonosítja a magas kockázatú felhasználókat, a kockázatos viselkedést és a szokatlan eseményeket
- Egyszerűsíti a privilegizált felhasználói fiókok kezelését

ÁTTEKINTÉS

A hackerek folyamatosan új módszerekkel próbálkoznak, hogy hozzáférjenek az Ön rendszereihez és adataihoz. Végső soron a privilegizált felhasználói fiókok megszerzése a céljuk. A közelmúlt elhíresült esetei közül szinte mindig privilegizált felhasználói fiókokat törtek fel, hogy hozzáférjenek a kritikus rendszerekhez és adatokhoz. Egy biztonsági incidens során Ön csökkentheti a károkat olyan megoldások telepítésével, amelyek biztonságos, hatékony, és a törvényi előírásoknak is megfelelő hozzáférést biztosítanak a privilegizált fiókokhoz.

Az IT menedzserek számára ezek a korlátlan hozzáféréssel rendelkező fiókok több okból is kihívást jelentenek. Egyrészt egy nagyvállalati környezetben ezen fiókok, és az azokat használók száma jellemzően nagyon magas. Másrészt a hagyományos privilegizált hozzáférés-kezelő (Privileged Access Management – PAM) megoldások általában komplexek, hosszadalmas a telepítésük, és az üzemeltetésük is nehézkes.

A Privileged Access Management óriási kihívást jelenthet, de ez nem feltétlenül kell, hogy így legyen. A One Identity Safeguard egy integrált megoldás, amely egy biztonságos, hardened password safe és egy munkamenet-kezelő és felügyelő megoldást ötvöz a fenyegetések észlelésével és elemzésével. Biztonságosan tárolja, kezeli, rögzíti, és elemzi a privilegizált hozzáféréseket.



Biztonságos privilegizált hozzáférés áldozatok nélkül

Könnyítse meg privilegizált fiókjai védelmét a One Identity Safeguard segítségével: tárolja, kezelje, rögzítse, és elemezze a privilegizált felhasználók hozzáférését, miközben az adminisztrátorok és az auditorok elvárásainak is megfelel.

Safeguard for Privileged Sessions

A One Identity Safeguard for Privileged Sessions megoldással kontrollálhatja, felügyelheti, és rögzítheti az adminisztrátorok, külsős szolgáltatók, illetve más magas kockázatú felhasználók munkameneteit. A rögzített munkamenetek tartalma indexelt, így az események keresése egyszerű, sőt a Safeguard for Privileged Sessions segíti az automatikus jelentéskészítést is, így a törvényi megfelelés követelményei is könnyen teljesíthetők. A Safeguard for Privileged Sessions proxyként működik és folyamatosan nyomon követi az alkalmazás szintű protokollok forgalmát. Ez hatékony védelmet biztosít a támadások ellen, mivel minden olyan forgalmat visszautasít, amely nem felel meg a protokoll szabályainak.

Safeguard for Privileged Passwords

A One Identity Safeguard for Privileged Passwords automatikus munkafolyamatokkal és szerep alapú hozzáférés- kezeléssel automatizálja, kontrollálja és biztonságossá teszi a privilegizált felhasználói jelszavak kezelését. 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.

Safeguard for Privileged Analytics

A One Identity Safeguard for Privileged Analytics az Ön szolgálatába állítja a felhasználói viselkedés elemzést. Segítségével megtudhatja, hogy mely privilegizált felhasználók jelentik a legnagyobb kockázatot, felderítheti, hogy melyek voltak az eddig ismeretlen belső és külső fenyegetések, és leállíthatja a gyanús tevékenységeket. A Safeguard for Privileged Analytics rangsorolja a potenciális kockázatokat, így Ön priorizálhatja a válaszadást – a legsürgetőbb fenyegetésekre azonnal válaszolhat – és végső soron megelőzheti a biztonsági incidenseket.

FUNKCIÓK

Szabály-alapú hozzáférés ellenőrzés

Ha biztonságos, és mobileszközöket is támogató böngészőt használ, akkor bárhonnan hozzáférést kérhet és jóváhagyást adhat a privilegizált felhasználói jelszavakhoz vagy munkamenetekhez. A kéréseket automatikusan vagy kettős/többszörös jóváhagyással is engedélyezhetjük, a szervezet előírásaitól függően. Ön szervezete előírásainak megfelelően konfigurálhatja a One Identity Safeguard-ot: a kérvényező személyét, hozzáférési szintjét, a kérés időpontját, illetve az elérni kívánt rendszert is figyelembe veheti. Ezen felül „reason" kódok is megadhatók, és/vagy ticketing rendszerekkel is integrálható a megoldás.

Teljes munkamenet audit, felvétel, és visszajátszás

Minden munkamenetet– beleértve az egyes billentyűk lenyomását, az egérmozgást és ablak megnyitást – rögzít, indexel, és hamisíthatatlan audit trail-ekben tárol, amelyeket úgy lehet megtekinteni, mint egy videót, és úgy lehet bennük keresni, mint egy adatbázisban. A biztonsági csapatok konkrét eseményeket kereshetnek a munkamenetekben és onnan játszhatják le a felvételt, ahol az első egyezést találták. Az audit trail-ek titkosítottak, időpecséttel ellátottak, és digitálisan is aláírtak.

Változtatás vezérlés

A Safeguard támogatja a megosztott jelszavak változtatásvezérlését , beleértve az idő és utolsó használat alapú változtatást, valamint a manuális, és kényszerített változtatást.

Valós idejű riasztás és megszakítás

A Safeguard for Privileged Sessions valós időben figyeli a forgalmat, és különböző intézkedéseket hajt végre, ha egy bizonyos sémát felismer a parancssorban, vagy a képernyőn. Az előre meghatározott sémák lehetnek például kockázatos parancsok, vagy szöveg egy szövegorientált protokoll esetében, vagy egy gyanús ablakcím grafikus kapcsolat esetén. Gyanús felhasználói tevékenység észlelésekor a Safeguard naplóbejegyzést készíthet az eseményről, riasztást küldhet, illetve akár azonnal meg is szakíthatja a munkamenetet.

Jóváhagyás bárhonnan

A One Identity Starling kétfaktoros authentikáció segítségével Ön bárhonnan jóváhagyhat, vagy elutasíthat bejelentkezési kéréseket – szinte bármilyen eszközről – akár VPN hozzáférés nélkül is.

Kedvencek

Már a bejelentkezési képernyőről hozzáférhet a leggyakrabban használt jelszavaihoz. Több jelszóigénylést egyetlen kedvenc csoportba összesíthet, így az összes szükséges fiókhoz hozzáférhet egyetlen kattintással.

Felderítés (Discovery)

Ön gyorsan feltérképezheti a privilegizált felhasználói fiókokat vagy rendszereket a hálózatán, a rugalmas host-, directory-, és hálózat-felderítés opciókkal.

Biometrikus viselkedéselemzés

Minden felhasználó egy egyedi, csak rá jellemző viselkedési mintával rendelkezik, amikor olyan ismétlődő cselekvést végez, mint például az egérmozgatás vagy a gépelés. A Safeguard for Privileged Analytics-be beépített algoritmusok megvizsgálják ezeket a viselkedési jellemzőket is. A billentyűzet dinamika és az egérmozgás elemzés segít a támadások azonosításában, sőt folyamatosan, biometrikus módszerekkel hitelesíti a felhasználót.

Kockázatos felhasználók azonosítása

A Safeguard for Privileged Analytics a felhasználói jogosultságokat összeveti a kockázati besorolással, és így azonosítja a magas kockázatú fiókokat. Proaktív riasztásokat küld, amikor egy felhasználót magas kockázati státuszú jogosultsággal ruháznak fel. Ez megszünteti a szükségtelen vagy „alvó" jogosultságok kockázatát, mielőtt a támadók kihasználhatnák ezt.

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.

Széleskörű protokolltámogatás

A Safeguard teljes körűen támogatja az SSH, Telnet, RDP, HTTP(s), ICA és VNC protokollokat. Ezen felül a biztonsági csapatok eldönthetik, hogy a protokollon belül mely hálózati szolgáltatásokat (pl. fájltranszfer, shell hozzáférés, stb.) akarnak hozzáférhetővé tenni az adminisztrátorok számára.

Szabadszöveges keresés

A Safeguard for Privileged Sessions Optical Character Recognition (OCR) motorjának köszönhetően az auditorok szabadszöveges keresést hajthatnak végre a rögzített parancsokon és a képernyőn található bármilyen szövegen. A file műveletek is listázhatók, sőt az átvitt fájlok is megtekinthetők. A munkameneti és metaadatokban való keresés megkönnyíti az incidens-kezelést és a hibaelhárítást is.

Egyszerű telepítés

Gyors, appliance alapú telepítésének és az egyszerű forgalom átirányítási szabályainak köszönhetően a One Identity Safeguard-dal akár napokon belül megkezdheti munkamenetei rögzítését, a felhasználók megzavarása nélkül.

Parancs és alkalmazásvezérlés

A Safeguard for Privileged Sessions a parancsok és ablakcímek engedélyezését és tiltását (white– and blacklisting) egyaránt támogatja.

"Instant on" mód

Transzparens módon telepítve, a Safeguard for Privileged Sessions nem igényel semmilyen változtatást a munkafolyamatokban. Képes proxy gateway-ként működni, mint egy router a hálózatban, a szerver és a felhasználó számára egyaránt láthatatlanul. Az adminisztrátorok továbbra is a megszokott kliens alkalmazásaikat használhatják, és hozzáférhetnek a célszerverekhez és más rendszerekhez a napi rutinjuk megváltoztatása nélkül.

One Identity Hibrid Előfizetés

Terjessze ki a Safeguard képességeit a One Identity Hibrid Előfizetésével, amely azonnali hozzáférést nyújt felhőszolgáltatásainkhoz. Ezek között megtalálható a Starling kétfaktoros authentikáció és a Starling Identity Analytics & Risk Intelligence, mellyel Ön proaktívan azonosíthatja a kockázatos felhasználókat. Egyetlen előfizetéssel minden One Identity megoldáshoz hozzáférhet.

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™