BALASYS

One Identity Safeguard for Privileged Sessions

Csökkentse kockázatait a privilegizált hozzáférések szabályozásával, felügyeletével és rögzítésével

ELŐNYÖK

A felhasználói tevékenység folyamatos felügyeletével és megjelenítésével teljes rálátást biztosít IT környezetére.

Csökkenti a biztonsági incidensek kockázatát az IT eszközökhöz való hozzáférés korlátozásával.

Könnyedén teljesíthető a kiemelt hozzáférések felügyeletére vonatkozó törvényi megfelelés.

Gyorsabb megtérülés az egyszerű telepítésnek és üzemeltetésnek köszönhetően.

A rendszergazdák megszokott eszközeikkel dolgozhatnak, így elégedettek maradnak.

Maximális termelékenység a rövid tanulási görbének és az elegáns felhasználói felületnek köszönhetően.

Csökkenti az audit jelentésekhez szükséges munkát az információkhoz való gyors hozzáféréssel.

Bármilyen rendszerhez való hozzáférés nyomon követhető a platformfüggetlen, agentless működés révén.

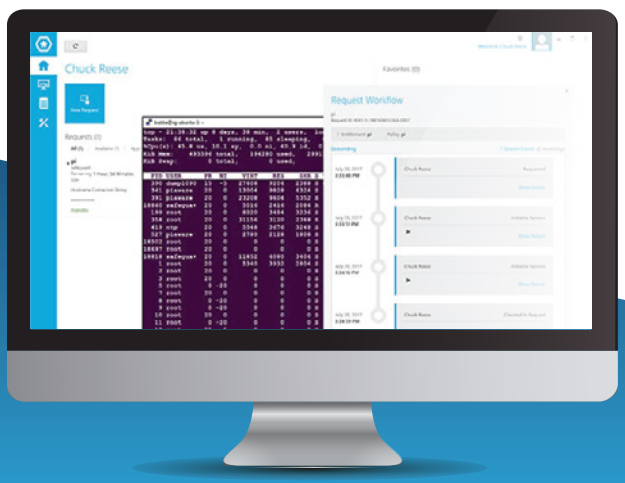
Gyorsabb incidenskezelés a munkamenetben való teljes, szabadszöveges kereséssel.

ÁTTEKINTÉS

Jelentős kockázatot jelenthet, ha a privilegizált hozzáféréseket ellenőrizetlenül adjuk ki rendszergazdáinknak, IT szolgáltatóinknak vagy alvállalkozóinknak. Ezzel ugyanis kinyitjuk az ajtót a rosszindulatú adminisztrátoroknak, vagy azoknak a támadóknak, akiknek célpontja a privilegizált felhasználói fiókok megszerzése. A nemrégiben történt, nagy publicitást kapott esetek rámutattak ennek a kockázatnak a sajnálatos – és drága – következményeire. A valódi biztonság és a törvényi megfelelés érdekében a rendszergazdai jelszavak kezelésénél többre van szükség. Önnek folyamatosan felügyelnie és rögzítenie kell, hogy a felhasználók mire használják a kiemelt jogosultságaikat.

A One Identity Safeguard for Privileged Sessions-szel Ön 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 könnyen teljesíthetők a törvényi megfelelés követelményei.

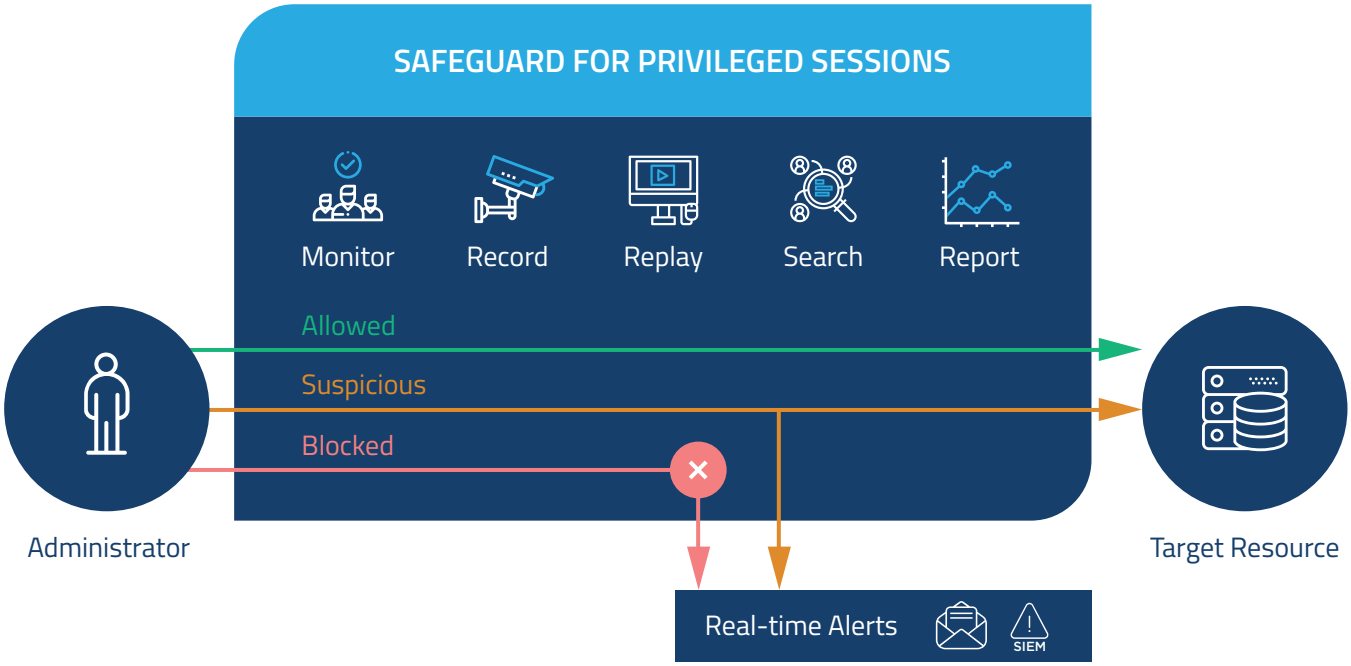
A Safeguard for Privileged Sessions proxyként működik és folyamatosan nyomon követi az alkalmazás szintű protokollok forgalmát. Ez hatékony védelmet biztosít a támadások ellen, mivel minden olyan forgalmat visszautasít, amely nem felel meg a protokoll szabályainak. Transzparens módban a hálózaton csak minimális változtatásokat igényel, és a felhasználóknak sem kell megváltoztatni a korábbi munkafolyamataikat, vagy alkalmazásaikat, miáltal az implementáció nagyon leegyszerűsödik. De a munkafolyamatok szabályait szigorúbbra is állíthatjuk, például az előzetes felhasználói hitelesítéssel, vagy bizonyos erőforrásokhoz való hozzáférés korlátozásával, sőt, riasztást is kérhetünk, ha a kapcsolat túllépte az előre beállított időt. A Safeguard képes a munkameneteket valós időben felügyelni és különböző intézkedéseket végrehajtani: például kockázatos parancs vagy alkalmazás használat esetén, képes megszakítani a kapcsolatot, vagy riasztást küldeni.



FUNKCIÓK

Rögzítsen és monitorozzon minden privilegizált hozzáférést

A szabadszöveges kereséssel, valós idejű riasztással és kapcsolat blokkolással, a Safeguard csökkenti a kockázatait, miközben segíti a követelményeknek való megfelelést.



Teljes munkamenet audit, felvétel, és visszajátszás

A Safeguard for Privileged Sessions minden munkamenetet– beleértve az egyes billentyűk lenyomását, az egér mozgatását, ablak megnyitását – rögzít, indexel, és hamisíthatatlan audit trail-ekben tárol, amelyeket úgy lehet megtekinteni, mint egy videót, és ugyanúgy lehet bennük keresni, mint egy adatbázisban. Az IT Security csapatok konkrét eseményekre rákeresve onnan játszhatják le a felvételt a munkamenetekben, ahol az első egyezést találták. Az audit trail-ek titkosítottak, időpecséttel ellátottak, és digitálisan is aláírtak.

Valós idejű riasztás és blokkolás

A Safeguard for Privileged Sessions valós időben figyeli a forgal▪mat, 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.

Két működési mód

Válassza az igényeinek megfelelőt

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.

"Instant on" mód

Telepítse transzparens módon, így semmilyen változtatás nem szükséges a munkafolyamatokban. Képes proxy gateway-ként működni, úgy, 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.

Proxy hozzáférés

Mivel a felhasználóknak nincs közvetlen hozzáférése az erőforrásokhoz, a szervezet védett marad az érzékeny adatokhoz és rendszerekhez való nem engedélyezett, illetve korlátlan hozzáféréstől. A Safeguard for Privileged Sessions képes proxyként működni, és rögzíteni számos célrendszerhez való hozzáférést, többek közt: Linux/UNIX, Windows szerverekhez, hálózati eszközökhöz, tűzfalakhoz, routerekhez, és számos más eszközhöz.

Parancs és alkalmazásvezérlés

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

Dolgozzon úgy, ahogyan Ön szeretne

A privilegizált munkafolyamatokhoz való hozzáféréskor az adminisztrátorok választhatják meg saját eszközeiket, klienseiket, és beállításaikat, még az eszköz rendszerbe illesztése után is. Így ezzel a zökkenőmentes megoldással biztosított az adminisztrátorok hozzáférése, miközben a biztonsági és megfelelősségi előírásoknak is megfelel vállalata.

Szabadszöveges keresés

A Safeguard for Privileged Sessions Optical Character Recognition (OCR) motorjának köszönhetően az auditorok szabadszöveges keresést hajthatnak végre a begépelt parancsokon és a képernyőn található bármilyen szövegen. A file műveletek is listázhatók, sőt még az átvitt fájlok is megtekinthetők. Ezenfelül a munkamenet tartalmában és metaadatában való keresés megkönnyíti az incidenskezelést és a hibaelhárítást is.

Automatikus beléptetés

A jelszó beillesztés (password-injection) funkció segítségével a szerverekre való belépés automatizálható, amely megnöveli a biztonságot, mivel soha nem fedi fel a jelszót a felhasználónak.

Széleskörű protokolltámogatás

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

Azonnali kapcsolatmegszakítás

Virtuális tűzfalként működve, a One Identity Safeguard növeli szerverei védelmét, mivel szinte azonnal megszakítja a gyanús, vagy rosszindulatú kapcsolatokat. Ezenkívül, a félre konfigurálás és más emberi hibák kiküszöbölésére a megoldás támogatja a four-eyes authorizációt, mellyel a megfigyelő adminisztrátor bármikor megszakíthatja a munkamenetet.

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.

ONE IDENTITY™

A One Identity-ről

A One Identity a Quest Software egyik üzletága, amely segíti a vállalatok jogosultság és hozzáférés kezelését (Identity and Access Management, IAM). Jogosultság szabályozást (Identity Governance), hozzáférés kezelést, privilegizált felhasználó kezelést és jogosultságot, mint szolgáltatást (Identity as a Service) tartalmazó egyedi termékportfóliója támogatja a szervezeteket üzleti lehetőségeik kihasználásában, mindezt biztonsági béklyók nélkül, mégis védelmet nyújtva a fenyegetések ellen.