BALASYS

One Identity Password Manager

Önállóbb felhasználók, alacsonyabb költségek, magasabb biztonság

ELŐNYÖK

- Csökkenti a helpdesk és az IT beavatkozások számát a rutin jelszóproblémák során
- Jelentősen csökkenti a felhasználói állásidőt
- Azonnal megtérülő befektetés
- Egyszerűen telepíthető és használható, így növeli az IT-csapat, és a felhasználók elégedettségét
- Növeli a hálózatbiztonságot
- Lehetővé teszi a különböző rendszerek közötti jelszavak szinkronizálását
- Integrálható a One Identity kétfaktoros hitelesítési (TFA) megoldásaival, a magasabb biztonság érdekében
- Integrálható a One Identity single sign-on megoldásával, mellyel egy teljes körű vállalati jelszókezelő megoldás építhető

ÁTTEKINTÉS

Az IT helpdesk-hez befutott kérések nagy része jelszócserével kapcsolatos. Mivel azonban a szervezetek egyre szigorúbb biztonsági szabályokat követelnek meg, a jelszókezelés problémája egyre több gondot okoz. Az erős jelszavak és gyakori jelszócserék megkövetelése hozzájárul ahhoz, hogy a felhasználók sokszor elfelejtik őket, és a helpdesk-hez fordulnak segítségért. A problémát súlyosbítja, hogy a szervezetek a különböző rendszerekhez és alkalmazásokhoz többféle jelszót rendelnek. Ennek következtében a szervezetek azzal a dilemmával szembesülnek, hogy növeljék a biztonságot, vagy inkább a helpdesk költségeket csökkentsék.

A Password Manager egy egyszerű, biztonságos és önkiszolgáló megoldás, amely lehetővé teszi a végfelhasználók számára, hogy visszaállítsák elfelejtett jelszavaikat, és feloldják felhasználói fiókjaikat. Segít a rendszergazdáknak az erős jelszavak megkövetelésében, úgy, hogy közben a helpdesk leterheltsége is csökken. Az Ön szervezetének már nem kell többé feláldoznia a biztonságot a költségek csökkentése érdekében.

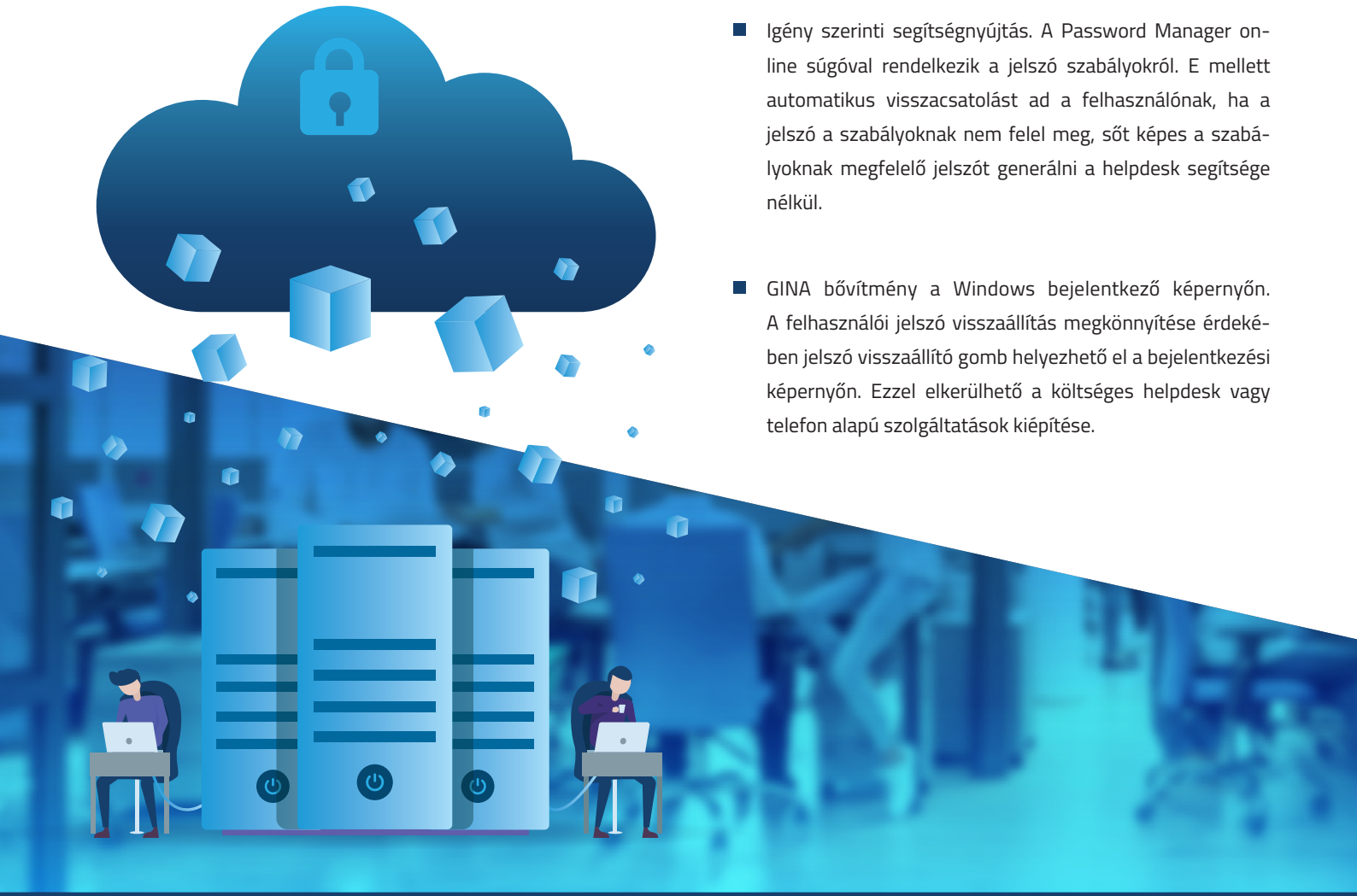
JELLEMZŐK

Egyszerűen növelhető biztonság

A Password Manager lehetővé teszi a vállalatok számára, hogy a Microsoft Active Directory natív képességein túlmutató adathozzáférési szabályokat alkalmazzanak. A Password Manager kiküszöböli a helpdesk hibákat. Nem kell a jelszavakat sehova feljegyezni, így a felhasználói fiókok feltörését és a jelszó megfejtését is megnehezíti. A beépített adattitkosítás lehetővé teszi a távoli hozzáférést, miközben garantálja az adatbiztonságot.

Gyors beruházás megtérülés a felhasználók közreműködése által

A Password Manager lehetővé teszi, hogy a legegyszerűbb jelszókezelési feladataikat a végfelhasználók saját maguk végezzék. Így IT költséget takaríthat meg, és biztosíthatja befektetésének gyors megtérülését.



Okos befektetés

A Password Manager hosszú távú megoldást kínál egy növekvő problémára, ezért okos befektetést jelent minden vállalkozásnak, amely egyszerre szeretne magasabb biztonságot és hatékonyabb IT működést.

- Költséghatékony, mert a meglévő Active Directory infrastruktúrán alapul. Gyorsan beüzemelhető, és azonnali megtérülést tesz lehetővé. Ezen felül a Windows Server 2008-nál részletesebb, csoport alapú jelszó szabályokat biztosít.

- Csökkenő helpdesk munkaterhelés és költségek, fokozott felhasználói produktivitás. A Password Manager segítségével a felhasználók visszaállíthatják a jelszavukat és felhasználói fiókjukat anélkül, hogy a helpdesk vagy a rendszergazda segítségét kellene igénybe venniük.

- Igény szerinti segítségnyújtás. A Password Manager online súgóval rendelkezik a jelszó szabályokról. E mellett automatikus visszacsatolást ad a felhasználónak, ha a jelszó a szabályoknak nem felel meg, sőt képes a szabályoknak megfelelő jelszót generálni a helpdesk segítsége nélkül.

- GINA bővítmény a Windows bejelentkező képernyőn. A felhasználói jelszó visszaállítás megkönnyítése érdekében jelszó visszaállító gomb helyezhető el a bejelentkezési képernyőn. Ezzel elkerülhető a költséges helpdesk vagy telefon alapú szolgáltatások kiépítése.

A szervezeti szabályok érvényesítése

A Password Manager alkalmazkodik a legátfogóbb szervezeti házirendekhez és adatbiztonsági szabványokhoz.

- Szigorú házirend érvényesítés - a Password Manager kikényszeríti a rendszergazdák által beállított jelszó szabályokat, naplózza a sikertelen belépési kísérleteket, és, ha szükséges, zárolja a felhasználói fiókot.

- Megkerülhetetlen használat – a Password Manager több mechanizmussal is biztosítja, hogy a felhasználók valóban használják a szoftvert, így garantálva annak hatékonyságát.

- Megbízható hitelesítés – A személyes kérdés-válasz (Q&A) profilok olyan kérdéseket tartalmaznak, amelyekre a felhasználók könnyen emlékeznek, de másoknak nehéz kitalálni. E mellett a Password Manager a One Identity kétfaktoros hitelesítő eszközével kombinálva is telepíthető, így az egyszer használatos jelszavak (One Time Passwords, OTP) még biztonságosabb azonosítást tesznek lehetővé, kiegészítve - vagy akár helyettesítve - a kérdés-válasz profilokat.

- Biztonság és egyszerűség – a Password Manager zökkenőmentesen integrálható Windows környezetbe, így több domainből is kiszolgálhat felhasználókat. A Password Manager erős titkosítást és biztonságos adattovábbítást biztosít olyan vezető technológiáknak köszönhetően, mint a 3DES, MD5, SSL, és Microsoft CryptoAPI.

Rendszertevékenységek felügyelete

A Password Manager robosztus naplózási és jelentéskészítési képességekkel támogatja a rendszergazdákat, így az anomáliák könnyen korrigálhatók.

Jogosultság-kezelő rendszerek támogatása

A Password Manager többféle böngészőt is támogat, és biztosítja a jelszókezelést minden olyan rendszerhez, amely kapcsolódik a Microsoft Identity Integration Server-hez (MIIS). A One Identity Authentication Services segítségével kiterjeszthető nem Microsoft operációs rendszerekre is, mint például a Linux vagy a Unix. Támogatja a kétfaktoros hitelesítést (Starling Two-Factor Authentication), sőt a teljes szervezetre kiterjedő Single sign-on megoldást is bevezethető a One Identity Enterprise Single Sign-on és a Cloud Acces Manager integrálásával.

One Identity Hybrid előfizetés

Terjessze ki az Active Roles funkcionalitását a One Identity Hybrid előfizetéssel, amely azonnali hozzáférést nyújt számos további felhő-alapú funkciókhoz és szolgáltatáshoz. Ezek közé tartozik a Starling Two-Factor Authentication, amely biztonságos adminisztrátori hozzáférést tesz lehetővé, és a Starling Identity Analytics & Risk Intelligence, amely előre jelzi a kockázatokat, valamint elemzi az Active Roles-hoz való hozzáféréseket is. Ez a szolgáltatás további célrendszerekre és alkalmazási területekre is kiterjeszthető, így egyetlen One Identity előfizetéssel minden megoldásunkhoz hozzáférhet.

ONE IDENTITY™

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.