



Az RSA teljes körű, vállalati szintű passwordless megoldása

Passwordless védelem minden fenyegetés ellen, minden környezetben, minden felhasználónak és eszközre.

A többfaktoros hitelesítés (MFA) alapvető kiberbiztonsági képességeket nyújt a szervezeteknek. A hagyományos MFA azonban már nem elég: a támadók social engineeringgel, malware-ekkel, deepfake-ekkel és más új fenyegetésekkel kerülnek meg. Ráadásul az olyan kormányzati előírások, szabályozások és biztonsági modellek, mint a DORA, az Executive Order 14028, a NIS2 vagy az OMB M-22-09, phishing-ellenálló hitelesítést követelnek meg. Az új fenyegetések és megfelelési előírások többet kívánnak az MFA-nál: passwordless hitelesítést.

Bár sok szállító kínál egyes felhasználói csoportokat vagy felhasználási eseteket lefedő, részleges passwordless megoldásokat, az RSA a teljes szervezetre kiterjedő, skálázható passwordless képességeket nyújt – többek között QR-kódot, biometriát, FIDO2-tanúsított [hardveres](#) és szoftveres hitelesítést [iOS-re és Androidra](#), mobil push-t és még sok más – , környezettől és felhasználási esettől függetlenül.

Az iparág legbiztonságosabb hibrid identitásbiztonsági platformján, az [RSA® ID Plus](#) megoldáson keresztül elérhető RSA passwordless megoldások növelik a biztonságot, javítják a hatékonyságot, teljesítik a megfelelési követelményeket és csökkentik a költségeket. Az RSA mindezt egy átfogó biztonsági platformmal erősíti meg, amely védi a hitelesítési folyamatot, valós időben észleli a fenyegetéseket, és már csírájukban megállítja a támadásokat. [Kezdje el ID Plus próbaidőszakát még ma.](#)

Ismerje meg az RSA passwordless megoldását: azokat az operációs rendszereket és ökoszisztémákat, amelyekben technológiánk telepíthető, a szabványokat, amelyekre épül, a kiberfenyegetéseket, amelyek ellen véd, és az előnyöket, amelyeket nyújt.

Passwordless megoldások a modern kibertámadások ellen

Az RSA passwordless megoldását úgy tervezték, hogy ellenálljon a legújabb kibertámadásoknak. Az RSA olyan phishing-ellenálló, passwordless módszereket támogat, amelyek védelmet nyújtanak a malware, a brute force támadások, a csalások, a leállások és a megkerülési kísérletek ellen, megakadályozva, hogy a támadók szellemi tulajdont lopjanak vagy megzavarják a működést.

Az alábbiakban bemutatjuk, hogyan védenek az RSA megoldásai a legújabb kibertámadások ellen:

Védelem a phishing ellen

A phishing az egyik leggyakoribb és legköltségesebb kibertámadás. A phishing-támadások ráveszik a felhasználókat, hogy kiadják jelszavaikat, felhasználóneveiket és egyéb hitelesítő adataikat. A [2025-ös Verizon Data Breach Investigations Report](#) szerint 2024-ben 2,8 millió jelszó szivárgott ki vagy került veszélybe nyilvánosan, a ransomware-támadások 54%-a pedig közvetlenül jelszószivárgásra vezethető vissza. Az [IBM Cost of a Data Breach Report](#) szerint a phishing az adatvédelmi incidensek egyik leggyakoribb és legdrágább oka: átlagosan 4,88 millió dollárba kerül, megfékezése pedig átlagosan 261 napig tart.

Az RSA passwordless hitelesítése megszünteti azokat a jelszavakat, amelyeket a kiberbűnözők megpróbálnak megszerezni. Megoldásaink a hitelesítő adatok életciklusának kritikus szakaszaiban – például a regisztráció és a fiókhelyreállítás során – is szükségtelenné teszik a jelszavakat és a megosztott titkokat. Más helyzetekben, például felhőleállások esetén, az RSA folyamatosan elérhető képességeivel a felhasználók más passwordless módszerekkel csatlakozhatnak.

Próbálja ki!

Az RSA ID Plus támogatja a QR-kódot, a FIDO passkeyeket, a biometriát és számos más phishing-ellenálló, passwordless módszert.

[Kezdje el ID Plus próbaidőszakát most!](#)

Az RSA szoftveres és hardveres, passwordless, phishing-ellenálló hitelesítést is kínál. Az [RSA Authenticator App](#) eszközhöz kötött, phishing-ellenálló passkeyeket támogat iOS és Android eszközökön. A szervezetek emellett [RSA iShield Key 2 series](#) és [DS100](#) FIDO2 biztonsági kulcsokat is használhatnak, amelyek frissíthető firmware-rel, hardveralapú phishing-ellenálló hitelesítést nyújtanak.

Védelem a malware ellen

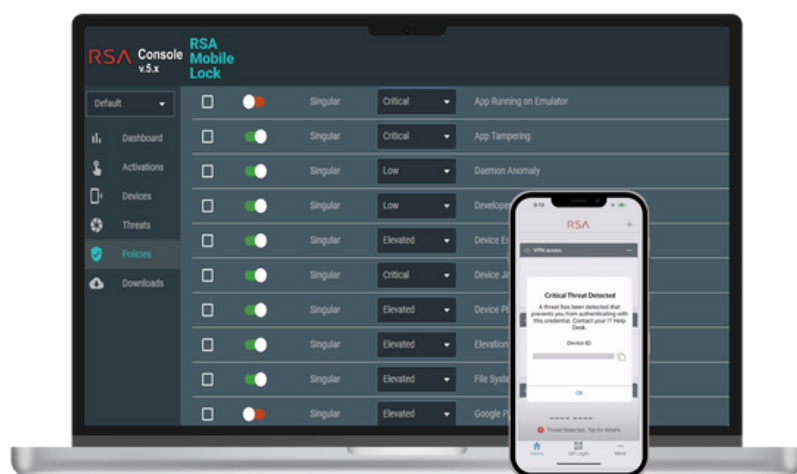
4000%

növekedés a malware-as-a-service terjedésében

Outseer 2024 Global Fraud and Scams Trend Report

A malware olyan rosszindulatú szoftver, amelyet rendszerek, felhasználók és adatok károsítására terveztek. A támadók egyre gyakrabban fordulnak a malware-as-a-service (MaaS) modellhez, amelyben előfizethetnek malware-programokra és infrastruktúrára, hogy ransomware- és egyéb támadásokat indítsanak. Az [Outseer](#) szerint a MaaS 4000%-kal nőtt, és a mobilbanki forgalom ma már a digitális banki tranzakciók 85%-át teszi ki, így a pénzügyi szolgáltatások a kiberbűnözők kiemelt célpontjává váltak.

Az RSA passwordless megoldásai többféleképpen segítenek a malware elleni védekezésben. Először is, a passwordless hitelesítés megszünteti számos olyan támadási vektort, amelyen keresztül a támadók átvehetnék egy felhasználó identitását és malware-t telepíthetnének. Másodszor, a szervezetek az [RSA® Mobile Lock](#) segítségével biztosíthatják a mobilos hitelesítést a felügyelt és a saját (BYOD) eszközökön. A megoldás képes malware-eket, trójai programokat (legitim programnak álcázott malware-eket) és egyéb sérülékenységeket keresni, hogy kompromittált eszköz ne jelentkezessen be a védett környezetbe.



Az RSA Mobile Lock konzol adminisztrátori nézete

Felhasználói nézet: észlelt fenyegetés a mobiltelefonon

Védelem a brute force támadások ellen

A password spraying, a credential stuffing vagy a rainbow table támadásokhoz hasonlóan a brute force támadások próbálgatással igyekeznek kitalálni a felhasználók jelszavait. A támadók automatizálhatják ezeket a támadásokat, vagy más adatvédelmi incidensekből ellopott hitelesítő adatokkal finomíthatják őket.

Az RSA passwordless megoldásai a jelszavak teljes kiküszöbölésével segítenek védekezni ezek ellen a támadások ellen. Az [RSA® Risk AI](#) emellett valós időben felismeri és megállítja a password spraying támadásokat olyan kontextuális kockázati jelek alapján, mint a felhasználó tartózkodási helye vagy a sikertelen bejelentkezési kísérletek gyakorisága. Ha egy „felhasználó” túl sokszor próbál bejelentkezni, a Risk AI automatikusan step-up hitelesítést kérhet, és riaszthatja a biztonsági csapatot, ha a „felhasználó” szokatlanul viselkedik. A megoldás csak akkor kér automatikusan step-up hitelesítést, ha a viselkedés meghaladja a szervezet kockázattűrési szintjét; egyébként a Risk AI megszünteti a felesleges súrlódást.

Védelem a csalások ellen

A kiberbűnözők számos csalásalapú támadással próbálhatják megtéveszteni a felhasználókat. Az MFA fatigue és a prompt bombing például olyan phishing-támadások, amelyek során a támadó több hamis MFA-kérést küld a felhasználónak. Ha a felhasználó teljesíti a kérést, vagy kiadja hitelesítő adatait a támadónak, vagy segít neki bejutni a védett környezetbe. Ilyen támadások áldozata lett már az [Uber](#), a [Cisco](#), az [X / Twitter](#), a [Robinhood](#), az [Okta](#), valamint [Office 365-felhasználók](#) is.

Az RSA passwordless megoldásai megvédik a szervezeteket a csalásoktól. Az RSA támogatja a code matchinget, amelynek során a felhasználónak egy regisztrált eszközére küldött kódot kell egyeztetnie, így igazolva, hogy valóban ő indította a hitelesítést – felhőalapú, hibrid, on-premises és RADIUS-környezetekben egyaránt. Az RSA Risk AI azt is észleli, ha egy felhasználó rendkívül sok hitelesítési kérést kap, és jelzi a biztonsági csapatnak, hogy vizsgálja ki a lehetséges prompt bombingot.

Védelem a leállások ellen

A szervezetek azt szeretnék, hogy felhasználóik egyszerre legyenek biztonságban és produktívak. Ezért egyes esetekben az MFA-szállítók vagy ügyfelek „fail open” hitelesítési folyamatot választanak, amely lehetővé teszi az MFA megkerülését, ha a felhasználó nem tud csatlakozni az internethez. Így a támadók gyakorlatilag kikapcsolhatják az MFA-t azzal, hogy bontják az internetkapcsolatot. Ez történt 2022-ben is, amikor egy orosz kötődésű támadó feltört egy [civil szervezetet](#). Ha a szervezetek a „fail close” megoldást választják, a támadók nem tudják kikapcsolni az MFA-t – egy valódi felhőleállás azonban megakadályozhatja a felhasználók bejelentkezését.

Valójában a valódi balesetek és technikai leállások hatása hasonló lehet a kibertámadásokéhoz. Amikor a felhő elérhetetlenné válik – ahogy 2025-ben, amikor Spanyolországban és Portugáliában [több tízmillió](#) ember maradt áram nélkül, vagy amikor technikai leállások 33 működési napnak megfelelő kiesést és potenciálisan több millió fontnyi [kártérítési kifizetést](#) okoztak a brit bankoknak –, a rugalmas és biztonságos hozzáférést fenntartó szervezetek boldogulnak, míg mások a csatlakozással küzdenek.

Az RSA passwordless megoldásai ellenállnak a leállásoknak. Ha egy felhasználó nem tud csatlakozni az internethez, az [RSA ID Plus Hybrid Failover](#) on-premises hitelesítésre vált, így a felhasználók OTP-vel is teljesíthetik az MFA-folyamatot. Az RSA még akkor is támogatja az offline passwordless hitelesítést, ha a felhasználó repülőgép-üzem módban van, és nem tud csatlakozni.

Védelem a megkerülés ellen

A social engineering támadások célja, hogy rávegyék a felhasználókat hitelesítő adataik kiadására, új fiókok létrehozására vagy olyan biztonsági intézkedések kikapcsolására, mint az MFA. Ilyen megkerülési módszerek például a technikai támogatásnak álcázott csalások, amelyek során a támadók kizárt felhasználónak adják ki magukat, és arra kérik az IT help desk munkatársait, hogy adjanak nekik hozzáférést vagy kapcsolják ki az MFA-t. Az ALPHV/BlackCat ezzel a technikával hajtott végre egy ransomware-támadássorozatot, amely [több száz millió dolláros](#) kárt okozott Las Vegas-i üdülőkomplexumoknak. Újabban a támadók [az egészségügyi és népegészségügyi szervezetek IT-munkatársait vették célba](#). A social engineering alapú megkerülés másik formája az [account takeover](#) (ATO), amikor egy támadó átveszi egy felhasználó fiókját, és azt felhasználva további felhasználókat vesz célba – néha a szervezet valamelyik vezetőjének kiadva magát.

A csalás következményei

„Egy MFA-értesítés jóváhagyása ugyanolyan katasztrofális lehet, mint rákattintani egy phishing e-mailben vagy kártékony oldalon lévő linkre. Ha egy hacker bejut a hálózatba, általában mindent megtesz, hogy továbbjusson, és más kritikus rendszerekhez is hozzáférjen.”

“Beware MFA Fatigue Attacks”

Dave Taku
VP, Product Management & UX
RSA

Az RSA passwordless megoldásai védelmet nyújtanak ezek ellen a támadások ellen. Az [RSA Help Desk Live Verify](#) kétirányú ellenőrzést biztosít, így sem a felhasználókat, sem a help desk munkatársait nem tudják megtéveszteni a magukat a másik félnek kiadó támadók: a help desk hívásakor a felhasználónak valós időben, phishing-ellenálló hitelesítéssel kell igazolnia személyazonosságát, mielőtt bármilyen művelet történne. A megoldás nem használ megosztott titkokat a személyazonosság igazolására.

\$100 millió

a 2023. októberi help desk elleni támadás becsült negatív hatása

MGM Resorts International Form 8K

Passwordless védelem minden fenyegetés ellen	
Phishing	✓
Malware	✓
Brute force támadások	✓
Csalások	✓
Leállások	✓
Megkerülés	✓

Biztonságos passwordless megoldások az identitás-életciklus minden szakaszára

A passwordless hitelesítés elterjedése arra készítette a támadókat, hogy továbbfejlesszék taktikáikat. A kiberbűnözők ma már a passwordless világhoz igazított módszereket alkalmaznak: technikai támogatásnak álcázott csalásokkal célozzák az identitás-életciklus kritikus szakaszait, manipulálják az IT help desket, vagy malware-as-a-service-t, deepfake-eket, csalásokat, brute force támadásokat és más taktikákat vetnek be, hogy teljesen megkerüljék a passwordless hitelesítést, és bejussanak a szervezetekbe.

Az RSA többretegű biztonsági képességekkel védi passwordless megoldásait a teljes identitás-életciklus során. Ezek a funkciók abban is segítenek, hogy a szervezetek lefedjék a leggyakoribb passwordless felhasználási eseteket, és hatékonyan, nagy léptékben kezeljék a passwordless hitelesítő adatokat.

Biztonságos regisztráció

A szervezetek gyorsan és biztonságosan regisztrálhatják az új felhasználókat az [RSA My Page](#) segítségével, amely önkiszolgáló SSO-val [biztonságos regisztrációs és helyreállítási munkafolyamatokat](#) kínál. Az új felhasználók hatósági igazolvánnyal végezhetik el az önkiszolgáló regisztrációt. A szervezet a natív ID Plus / ID-ellenőrzési integrációt további biztonsági réteggént használhatja a személyazonosság ellenőrzésére és a csalások kiszűrésére, például a felhasználók telefonszámának hitelirodai adatokkal való összevetésével. Az RSA My Page azt is biztosíthatja, hogy az új felhasználók alapértelmezés szerint passwordless hitelesítést használjanak minden SSO-kéréshez.

Ugyanígy, ha a felhasználóknak vissza kell állítaniuk hitelesítő adataikat, az ID Plus önkiszolgáló, biztonságos helyreállítási munkafolyamatot kínál az ID-ellenőrzési integráción keresztül.

Biztonságos helyreállítás

A technikai támogatásnak álcázott csalások – amelyek során a támadók a közösségi médiában elérhető információk alapján megszemélyesítik a felhasználókat, és ráveszik az IT help desk munkatársait az MFA kikapcsolására vagy új fiókok létrehozására – a passwordless korszak egyik legaggasztóbb taktikáját jelentik. A help desk elleni social engineering támadások csak 2025-ben 600 millió dollárnyi veszteséget okoztak; a Marks & Spencer, a Co-Op és a Christian Dior elleni csalások a korábbi, nagy visszhangot kiváltó, [MGM Resorts és Caesars Entertainment Group](#) elleni támadásokat idézik.

Az [RSA Help Desk Live Verify](#) segít a szervezeteknek megvédeni magukat ettől a taktikától. A funkció kétirányú help desk-ellenőrzést biztosít: a támogató személyzetet nem tudják megtéveszteni a felhasználónak kiadó kiberbűnözők, a felhasználókat pedig nem tudják átvérni az IT-munkatársnak álcázott támadók. Megosztott titkok vagy OTP helyett az RSA Help Desk Live Verify phishing-ellenálló online ellenőrzéssel igazolja a személyazonosságot. A képesség dinamikus, valós idejű szabályzat-érvényesítést is integrál: az [RSA® Risk AI](#) és az [RSA® Mobile Lock](#) segítségével kontextuális kockázati jelek – például a felhasználó tartózkodási helye és az eszköz biztonsági állapota – alapján proaktívan blokkolja a magas kockázatú hozzáférési kísérleteket.

Asztali bejelentkezés

Az RSA számos passwordless bejelentkezési lehetőséget kínál az asztali hitelesítéshez, többek között QR-kódot, mobilos FIDO2/passkey-hitelesítést és FIDO2 hardveres hitelesítőt bármely platformra.

SaaS-bejelentkezés

A felhasználók az RSA Authenticator App segítségével jelentkezhetnek be SaaS-szolgáltatásokba, amely támogatja a mobil eszközökhöz kötött passkeyeket, a pusht, a biometriát, a code matchinget és az OTP-t, valamint az olyan hardveres hitelesítőket, mint az RSA iShield Key 2 series és a DS100.

Hozzáférési kérelmek

Mivel az RSA passwordless alapú, biztonságos regisztrációt kínál, a szervezetek a teljes identitás-életciklus során támogathatják a passwordless hozzáférési kérelmeket és életciklus-kezelést. A felhasználók az RSA My Page felületén érhetik el alkalmazásaikat és nyújthatnak be önkiszolgáló hozzáférési kérelmeket. A megoldásba az RSA Authenticator Appal, RSA hardveres hitelesítéssel és más gyártók hardveres hitelesítőivel jelentkezhetnek be.

Offline hozzáférés

Egy orosz kötődésű támadó 2022-ben úgy tört fel egy [civil szervezet](#)re, hogy kihasználta az identitás-életciklus sérülékenységeit: regisztrált egy új eszközt, és kikapcsolta az MFA-t. Ezt részben úgy érte el, hogy leválasztott egy eszközt az internetről: emiatt az eszköz hitelesítési folyamata „fail open” módba lépett, vagyis nem kért MFA-t a bejelentkezéshez. A támadók tehát gyakorlatilag az internet kikapcsolásával iktatták ki az MFA-t.

Az [RSA ID Plus Hybrid Failover](#) ellenállóvá teszi a szervezeteket a leállásokkal szemben: leállások idején, vagy ha a felhasználók repülőgép-üzemmódban vannak, on-premises hitelesítésre vált, így a felhasználók akkor is jelszó nélkül jelentkezhetnek be, ha nem tudnak csatlakozni.

Passwordless megoldások minden használati esetre

Biztonságos regisztráció	✓
Biztonságos helyreállítás	✓
Asztali bejelentkezés	✓
SaaS-bejelentkezés	✓
Hozzáférési kérelmek	✓
Offline hozzáférés	✓

Passwordless hitelesítés minden környezetben és platformon

A szervezetek a biztonság növelése és a költségek – különösen az IT help desk terhelése – csökkentése érdekében vezetik be a passwordless hitelesítést. A részleges megoldások azonban lefedettségi hiányokat hagynak a felhasználói csoportokban, a környezetekben vagy mindkettőben, így nem hozzák el a várt biztonságot és megtakarítást. Az RSA egyetlen, teljes körű passwordless megoldást kínál, amely felhőalapú, hibrid és on-premises környezetben is minden felhasználót lefed: ugyanazok a képességek mindenhol biztonságosan működnek, és a passwordless hitelesítés az IT-infrastruktúrától függetlenül hatékony marad.



Felhőkörnyezetek

Az [RSA® ID Plus](#) a következő passwordless hitelesítési képességeket nyújtja a felhőben:

- Biometria
- Apple Face ID / Touch ID
- Windows Hello
- OTP
- QR-kód
- SMS / hanghívás
- Hardveres tokenek
- Code matching RADIUS-hoz



Hibrid környezetek

Az [RSA® ID Plus](#) az egyetlen valódi hibrid hozzáférés-kezelési platform: egységes IAM-platformot biztosít a környezetek között, és a következő passwordless képességeket nyújtja hibrid környezetekben:

- Biometria
- Apple Face ID / Touch ID
- Windows Hello
- OTP
- QR-kód
- SMS / hanghívás
- Hardveres tokenek
- Code matching RADIUS-hoz



On-premises környezetek

Az [RSA® ID Plus](#) a következő hozzáférési és passwordless hitelesítési képességeket nyújtja on-premises környezetekben:

- Biometria
- Apple Face ID / Touch ID
- Windows Hello
- OTP
- QR-kód
- SMS / hanghívás
- Hardveres tokenek
- Code matching RADIUS-hoz

Az [RSA ID Plus Hybrid Failover](#) segítségével a szervezetek internetkimaradások vagy egyéb fennakadások idején is biztosíthatják ezeket a passwordless módszereket. Az on-premises hitelesítésre való átállással továbbra is biztonságos, passwordless hitelesítést használhatnak ahelyett, hogy kevésbé biztonságos megoldásokra kényszerülnének, vagy kizárnák őket a saját környezetükből.

Az [RSA SecurID®](#) megoldások biztonságos hozzáférési, hitelesítési és identitáskezelési képességekkel védik az on-premises erőforrásokat. A SecurID a következő passwordless lehetőségeket kínálja on-premises környezetben:

- Asztali bejelentkezés
- Hardveres hitelesítők
- Mobilos hitelesítők
- Code matching RADIUS-hoz

Passwordless megoldások minden környezetbe	
Felhő	✓
Hibrid	✓
On-premises és adatközpontok	✓

Passwordless megoldások minden platformra

Az RSA Windows, Android, iOS és Linux környezetben is támogatja a passwordless hitelesítést.

Microsoft passwordless integráció

A Microsoft Entra környezetben működő szervezetek számára az RSA az [RSA External Authentication Methods \(EAM\) integráción](#) keresztül további passwordless hitelesítési képességeket kínál. Az RSA EAM lehetővé teszi, hogy a szervezetek az RSA phishing-ellenálló hitelesítési képességeivel – többek között FIDO2-tanúsított hitelesítési folyamatokkal, biometriával és QR-kódos hitelesítéssel – védjék a Microsoft-erőforrásokhoz való hozzáférést.

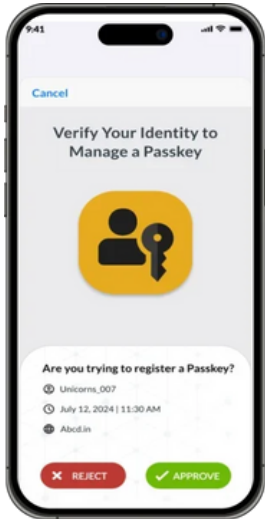
Passwordless megoldások minden platformra	
Windows	✓
MSFT-szerverek	✓
Bármely Windows endpoint (az AD-hez csatlakozó és az Entra-csatlakoztatott eszközök is)	✓
Android	✓
iOS	✓
Linux	✓

Passwordless megoldások minden felhasználói csoportnak és eszközre

A passwordless hitelesítés hatékony, nagy léptékű kezeléséhez és biztonságának megőrzéséhez a szervezeteknek minden felhasználói csoportot és eszközt figyelembe kell venniük. Ez azt jelenti, hogy hardveres és szoftveres passwordless hitelesítést is biztosítani kell, és gondoskodni kell arról, hogy az internethez csatlakozni nem tudó felhasználók is használhassák a passwordless hitelesítést.

Az RSA a passwordless eszköztípusok széles választékával minden felhasználót és eszközt lefed:

Szoftveres passwordless hitelesítés



Az [RSA Authenticator App](#) FIDO2-tanúsított, eszközhöz kötött passkeyt biztosít iOS és Android eszközökre.

A szinkronizált passkeyekkel ellentétben – amelyek több eszközön tárolják a hitelesítő adatokat (és azok [sérülékenységeit](#)) – az eszközhöz kötött passkey egyetlen eszközön tárolódik, és soha nem hagyja el azt, így a lehető legmagasabb szintű kontrollt és biztonságot nyújtja.

A megoldás segít a szervezeteknek megfelelni az Executive Order 14028, az OMB M-22-09 és az OMB M-24-14 előírásainak, a HIPAA követelményeinek és a DORA ajánlásainak, valamint számos más ország phishing-ellenálló hitelesítésre vonatkozó követelményeinek.

Passkey regisztrálása
RSA Authenticator Appban

Hardveres passwordless hitelesítés

Az RSA neve szinte egybeforrt a hardveres hitelesítéssel. Az RSA a biztonságos hardveres tokenek széles választékát kínálja kritikus és magas kockázatú helyzetekre – például tisztaterekbe, műtőkbe és olyan zárt területekre, ahol a PCI és más szabályozások miatt nem használhatók telefonok –, többek között:

RSA iShield Key 2 Series

A Swissbit által gyártott [RSA iShield Key 2 Series](#) a legmagasabb kiberbiztonsági szabványoknak megfelelően készült, és teljesíti a szövetségi kiberbiztonsági követelményeket. AAL3 szintű hardveres hitelesítőként az RSA iShield Key Series a következőket nyújtja:

- **Phishing-ellenálló biztonság:** Az RSA iShield Key 2 series FIDO2- és PIV-hitelesítéssel akadályozza meg a hitelesítő adatok ellopását és a jogosulatlan hozzáférést, így rendszerei biztonságban maradnak.
- **Smart card funkció:** Az RSA iShield Key 2 series biztonságos, manipulációbiztos tárolást nyújt a digitális tanúsítványok és hitelesítő adatok számára.
- **Szövetségi megfelelés:** FIPS 140-3 Level 3 tanúsítványú kriptográfiai modulra épül (4679-es tanúsítvány), és FIDO2-tanúsított, így megfelel a legszigorúbb amerikai szövetségi kiberbiztonsági követelményeknek, köztük az Executive Order 14028, az OMB M-22-09 és az M-24-14 előírásainak. Az [RSA ID Plus for Government](#) FedRAMP-engedéllyel rendelkező IAM-megoldás, amely teljesíti a NIST 800-53 keretrendszeren alapuló 325 biztonsági és adatvédelmi kontrollt.
- **Rugalmas használat:** Az RSA iShield Key 2 series egyetlen eszközön egyesíti a FIDO passkeyeket, a PIV smart cardot és az OATH HOTP OTP-t, USB-n és NFC-n keresztül egyaránt.



RSA iShield Key 2
USB-A és USB-C
hitelesítők

- **Frissíthető firmware:** A helyszínen frissíthető firmware felkészíti az eszközt az új fenyegetésekre, meghosszabbítja élettartamát, növeli értékét, és megkönnyíti az eszközkezelést.
- **Kesztyűbarát érzékelő:** Az RSA iShield Key 2 series az egyetlen olyan biztonsági kulcs, amely műanyag kesztyűben is aktiválható.

RSA DS100 hardveres hitelesítő

Az [RSA DS100](#) sokoldalú, több protokollt támogató passwordless hitelesítést nyújt egyetlen eszközzel:

- **FIDO2-hitelesítés:** A FIDO2-tanúsított DS100 biztonságos és kényelmes FIDO2 passwordless hitelesítést biztosít olyan környezetekben, ahol a hardveres hitelesítők előnyben részesítettek vagy kötelezőek. Egyszerűen csatlakoztatható USB-n keresztül, és a jövőben NFC-funkciót is kínál.
- **OTP-hitelesítés:** Olyan biztonságos környezetekben, ahol nincs lehetőség USB-csatlakozásra, vagy ahol a felhasználóknak VPN-hez kell csatlakozniuk, a DS100 online és offline OTP-bejelentkezést is biztosít. Az eszköz LCD-kijelzőn jeleníti meg az OTP-eket, a gombnyomásra generált OTP-t pedig automatikusan beírja.
- **Felhőalapú kezelés:** Bár a DS100 fizikai eszköz, kezelése a felhőben, az RSA Cloud Authentication Service segítségével történik. Ez hatékonyabb kezelést tesz lehetővé anélkül, hogy csorbulna egy teljes értékű hardveres hitelesítő biztonsága.
- **Frissíthető firmware:** A helyszínen frissíthető firmware révén a felhasználók naprakészen tarthatják az eszközt az új fenyegetésekkel szemben.



RSA DS100
hardveres hitelesítő

Offline passwordless hitelesítés

Az RSA ID Plus az [RSA ID Plus Hybrid Failover](#) segítségével támogatja az offline hitelesítést, így a szervezetek internetkimaradások vagy egyéb fennakadások idején is biztosíthatják a passwordless módszereket. Az on-premises hitelesítésre való átállással továbbra is biztonságos, passwordless hitelesítést használhatnak ahelyett, hogy kevésbé biztonságos megoldásokra kényszerülnének, vagy kizárnák őket a saját környezetükből.

Passwordless megoldások minden eszközre	
Szoftveres hitelesítők	✓
Hardveres hitelesítők	✓
Offline / tisztatéri hitelesítés	✓

Nézze meg, milyen egyszerű biztonságos passwordless hitelesítést bevezetni

Az RSA ID Plus a passwordless megoldások legszélesebb választékát kínálja, amelyeket a passwordless korszak támadásai ellen tervezett, átfogó biztonsági képességek erősítenek.

[Kezdje el ingyenes ID Plus próbaidőszakát még ma, és tapasztalja meg a teljes körű, vállalati szintű passwordless hitelesítés lehetőségeit.](#)



Az RSA-ról

Az RSA kritikus fontosságú kiberbiztonsági megoldásokkal védi a világ legérzékenyebb biztonsági igényű szervezeteit. Az RSA Unified Identity Platform valódi passwordless identitásbiztonságot, kockázatalapú hozzáférést, automatizált identitásintelligenciát és átfogó identitásirányítást biztosít felhőalapú, hibrid és on-premises környezetekben. Több mint 9000 magas biztonsági igényű szervezet bízta az RSA-ra több mint 60 millió identitás kezelését, a fenyegetések észlelését, a biztonságos hozzáférést és a megfelelőség támogatását. További információért látogasson el weboldalunkra, ahol [kapcsolatba léphet értékesítési csapatunkkal](#), [partnert kereshet](#), vagy [többet tudhat meg](#) az RSA-ról.