RSA

RSA ID Plus –
Egységes Identitásplatform

OWN YOUR IDENTITY.

Tartalomjegyzék

Vezetői összefoglaló

A változás átalakítja az üzletmenetet, az ügyfelekkel és a külső felhasználókkal való interakciót, valamint azt, ahogyan az alkalmazottak hozzáférnek az adatokhoz és az alkalmazásokhoz. A változás az átalakuló piaci dinamikából, az új üzleti célokból és a feltörekvő technológiákból is adódik.

Az évek során a szervezetek rájöttek, hogy az identity and access management (IAM) megoldások összetett IT-igények szélesebb körét tudják kiszolgálni azáltal, hogy lehetővé teszik a felhasználói szerepkörök, a csoportok és a hozzáférési jogosultságok központi kezelését. Ez idő alatt a szervezetek a helyszíni munkaterheket és szolgáltatásokat a felhőbe helyezték át, ami egy erősen elosztott identitásmodellt eredményezett, ahol minden felhőszolgáltatás és alkalmazás saját rendelkezésre bocsátási rendszert használ a felhasználók és jogosultságok számára. Ez jelentősen megnövelte az emberi hibák egyéni felhasználói élményekre gyakorolt hatását, ez pedig jelentős következetlenségeket okozhat abban, hogy két azonos szerepkörbe sorolt felhasználó hogyan fér hozzá a szolgáltatásokhoz. A hitelesítési, hozzáférési és kezelési módok ezen következetlenségei szükségtelen kockázatot, megnövekedett költségeket eredményeznek, valamint negatív hatást gyakorolnak a termelékenységre.

Az új technikai követelményekhez való gyors alkalmazkodás során – ideértve a hibrid munka támogatását, a digitális élmények létrehozását és az IT-veremek korszerűsítését – sok szervezetnek olyan pontszerű identitásmegoldásokba kellett befektetnie, amelyek egy sokkal összetettebb és integráltabb identitássíknak csak egyetlen komponensét kezelik. Az idő múlásával ezek a pontszerű megoldások hozzájárultak az ún. Identity Debt („identitásadósság”), azaz a komplexitásból, a költséges szerződésekből és a felhasználók hitelesítő adatait támadó fenyegető tényezők nagyobb kockázatából álló keverék kialakulásához.

Fizesd ki az identitásadósságot!

A leghatékonyabb és leggyorsabb módja az identitásadósság kezelésének, a komplexitás megszüntetésének, a felhasználói élmény egyszerűsítésének, a költségek csökkentésének, valamint az IT-kockázatok és fenyegetések mérséklésének az egy egységes identitásplatform. Az RSA Egységes Identitásplatform egyedülálló megközelítést kínál a szervezetek hitelesítési, hozzáférési, életciklus- és irányítási igényeinek egységesítésére. Magában foglalja az automatikus identitás-intelligenciát, amely mélyebb betekintést és kontextust biztosít a felhasználók és eszközök kockázataival kapcsolatban, ami segíthet a kritikus azonosítási folyamatok automatizálásában.

Ezek a tulajdonságok segítenek a szervezeteknek megbirkózni azokkal a kihívásokkal, amelyekkel sok szervezet szembesül, amikor kulcsfontosságú képességeket telepít a legfontosabb felhasználási módokhoz:

- ✓ Biztonságos hitelesítés és hozzáférés biztosítása az alkalmazásokhoz és az adatokhoz
- ✓ Az identitással kapcsolatos kockázatok és fenyegetések felderítése és az azokra való reagálás
- ✓ Végpontok közötti auditálhatóság és életciklus-menedzsment lehetővé tétele

Az identitás most a legfelsőbb vezetők döntése

Titulustól függetlenül minden vezetőnek érdeke, hogy megértse, hogyan tudja egy identitáspartner a szervezet speciális igényeit kielégíteni.

- ✓ Hogyan tud az információbiztonsági vezető megbizonyosodni arról, hogy a szervezeti hozzáférési szabályzatok minden üzleti alkalmazásban következetesek?
- ✓ Miből érezheti az informatikai vezető, hogy az identitásszolgáltató támogatja az új és bővülő üzleti célok és célkitűzések megvalósítását?
- ✓ Rendelkezik-e az adatvédelmi igazgató az érzékeny adatok védelmének biztosításához szükséges eszközökkel?
- ✓ Hogyan vélekedik az operatív igazgató arról, hogy képesek-e mérsékelni a bírságokkal, túlköltekezéssel vagy elszalasztott lehetőségekkel kapcsolatos kockázatokat, amelyeket a hatékony identitás képes kezelni?

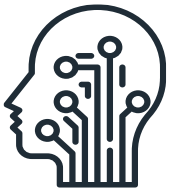
Az RSA segít a vállalatoknak megválaszolni ezeket a kérdéseket. A legjobb identitásmegoldások segítenek a vállalatoknak elérni céljaikat, csökkenteni a működési költségeket, egyszerűsíteni a komplexitáson, valamint jobban rálátni a biztonsági verem hatékonyságára a felhőben való útjuk során.

A biztonság az RSA DNS-e

Biztonságban első

Az RSA régóta hírnevet szerzett a fokozott biztonságú környezetek számára történő legfontosabb biztonsági megoldások gyártásában. Valójában ez az egyetlen dolog, amit csinálunk. Nem ez a missziónk központi eleme... ez az EGYETLEN missziónk.

Intelligens



Úgy gondoljuk, hogy azok a szervezetek, amelyek nem használják a legújabb mesterséges intelligenciát, automatizálási és munkafolyamatokat, veszélynek teszik ki magukat azokkal a támadókkal szemben, akik ezeket az eszközöket bevetik a célpontjaik ellen. Az RSA Egységes Identitásplatform alapját fejlett, intelligens automatizálási technológiák képezik, amelyek segítségével a megoldás csökkenti a kockázatokat és növeli a tudatosságot.

Nyílt

A szervezetek beszállítói stratégiái nem monolitikusak. Heterogének és változatosak. Az RSA platform támogatja ezt a megközelítést: hasznosítjuk a nyílt szabványokat, az alkalmazásprogramozási felületeket és a megoldásspecifikus csatlakozókat, amelyek lehetővé teszik az RSA számára, hogy több ezer alkalmazással integrálódjon hibrid és többfelhős módban.

A hibrid dilemma

Az RSA tisztában van azzal, hogy nincs két vállalat, amely ugyanazon utakat járná. Minden szervezetnek egyedi prioritásai, üzleti céljai és stratégiái vannak a felhő bevezetésére. Egyesek teljes mértékben a felhőbe fektetnek be, míg mások a saját adatközpontjaikban lévő szolgáltatásaik teljes körű ellenőrzését tartják elsődlegesnek. A legtöbben azonban még mindig mindkét világban tevékenykednek, és talán még évekig befektetnek mindkettőbe.

A helyszíni és a többfelhős erőforrásokon is átnyúló hibrid környezetek támogatásához rugalmas és igényekre szabható megoldásra van szükség.

Az RSA az egyetlen identitásszolgáltató, amely olyan, valódi hibrid identitásmegoldást kínál, amely többféle környezetet is tud támogatni, így biztosítva, hogy segíthessünk a szervezeteknek abban, hogy hol tartanak jelenleg, és a felhőben való útjuk során hová szeretnének elérni a jövőben.

Az egységes identitáshoz egységes partnerekre van szükség

Az RSA Ready technológiai partner ökoszisztéma több száz közvetlen megoldást tartalmaz, amelyek több ezer felhasználási módot tesznek lehetővé. Az RSA technológiai partnerei támogatottak vagy tanúsítottak az RSA-val való együttműködéssel kapcsolatban, annak érdekében, hogy segítsék az ügyfeleket az identitáskockázatok kezelésében.

Az RSA Ready programmal kapcsolatos további információkért látogasd meg Technológiai Partner oldalunkat: https://www.rsa.com/technology-partner-integrations!

RSA Egységes identitásplatform

Hozzáférés és hitelesítés

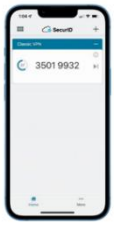
A SecurID hozzáférési és hitelesítési képességek lehetővé teszik a vállalatok számára, hogy az alkalmazottak, partnerek és alvállalkozók többet tehessenek a biztonság és a kényelem veszélyeztetése nélkül. A SecurID felöleli a mai felhő- és helyszíni környezetek, a saját eszközeink és a mobileszközök biztonsági kihívásait, gondoskodik róla, hogy a felhasználók időben hozzáférjenek a szükséges alkalmazásokhoz – bármilyen eszközről, bárhol –, és modern, kényelmes felhasználói élményt nyújtva biztosítja, hogy a felhasználók valóban azok legyenek, akiknek mondják magukat. A SecurID, a világ legszélesebb körben elterjedt többfaktoros hitelesítési és identitásbiztosítási megoldása ökoszisztéma-megközelítéssel teszi lehetővé a hitelesítést az egész alkalmazási területen, „a földtől a felhőig". Figyelembe véve az alkalmazás üzleti környezetét és a felhasználó hozzáférésének aktuális kockázatát, a SecurID identitásbiztosítást nyújt, amely számos modern hitelesítési lehetőséget kínál, úgymint koppintással történő jóváhagyás, biometrikus azonosítás – például ujjlenyomat- és arcellenőrzés –, egyszer használható jelszó és más megoldások, hogy a hitelesítést az általad kívánt módon biztosítsa.

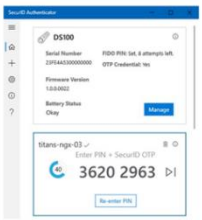
Modern hitelesítésünk:

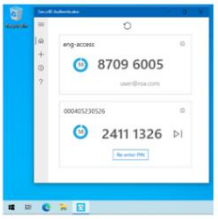
1. Hardveres hitelesítő: privilegizált adminisztrátor, biztonságos környezetek, önálló használat, szakszervezeti munka
2. Asztali hitelesítők: végrehajtók (macOS), helyszíni felhasználók, mobilkorlátozások
3. Hitelesítő kiválasztása: az irányelvek és a biztosítási szint korlátozza

Aranyszabvány

Hibrid hitelesítő







- ✓ Lehetőségek széles skáláját kínálja, beleértve a hardveres, beágyazott, szoftveres és mobil formájú faktorokat.
- ✓ Támogatja a feltörekvő szabványokat, például a FIDO2-t, valamint a technológiai innovációk, például a viselhető eszközök korai támogatását.
- ✓ Számos jelszó nélküli hitelesítési lehetőséget kínál a FIDO-val.
- ✓ Lehetővé teszi a faktorok gyors hozzáadását, eltávolítását és cseréjét.
- ✓ Rugalmas hitelesítési irányelveket biztosít, amelyek lehetővé teszik a rendszergazdai felügyeletet és támogatják a végfelhasználók választási lehetőségeit.
- ✓ Szervezeti preferencia (milyen módszerek megengedettek?)
- ✓ Végfelhasználói preferencia (pl. mobiltelefont vagy hardvertokent szeretne használni?)
- ✓ Felhasználói szerepkörök (pl. SMS engedélyezése harmadik felek dolgozói számára; hardvertoken szükséges a rendszergazdáknak; kivételek engedélyezése fogyatékkal élő felhasználók számára))
- ✓ Biztosítási szint (pl. kevésbé érzékeny alkalmazások esetében engedélyezi a mobil push-értesítést, érzékenyebb alkalmazások esetében a módszerek kombinációját követeli meg)
- ✓ Kényelmes és intuitív felhasználói élményt tesz lehetővé.
- ✓ Lehetővé teszi a felhasználók számára, hogy megadják az általuk preferált beállítást.
- ✓ A felszólítás előtt automatikusan felméri a végfelhasználó eszközének képességeit.

Governance & Lifecyle

A SecurID Governance & Lifecycle a folyamatos hozzáférési garanciát nyújt a szervezetek számára annak érdekében, hogy felhasználóik megfelelő szintű hozzáférést kapjanak az alkalmazásokhoz. Azáltal, hogy a SecurID átláthatóságot biztosít a mai vegyes felhő- és on-prem környezetben az identitás szigetein, és kombinálja a kockázatelemzési funkciókat, lehetővé teszi a magas kockázatú hozzáférési helyzetek rangsorolását, valamint képessé teszi a vállalati felhasználókat arra, hogy gyorsan és egyszerűen kezeljék a legnagyobb üzleti hatással járó helyzeteket az üzleti kockázat csökkentése és a megfelelőség biztosítása érdekében. A SecurID Irányítás és életciklus egy automatizált identitásirányítási és megfelelőségi platform, amely egyszerűsített hozzáférés-irányítást és felhasználói életciklus-kezelést biztosít, hogy a felhasználók gyorsabban tudjanak elkezdeni dolgozni, és teljesítsék a megfelelőségi követelményeidet. Más identitásirányítási megoldásokkal ellentétben az Governance & Lifecycle platform a hozzáférés legalacsonyabb szintjén is átláthatóságot biztosít a megfelelőség megsértésének, illetve az illetéktelen hozzáférésnek a felderítéséhez, valamint a szervezeten belüli identitáskockázat számszerűsítéséhez. A kifinomult kockázatelemzés ezután rangsorolja a hozzáférés helyreállítását és az üzleti tevékenységeket az identitáskockázat csökkentése érdekében.

A SecurID megválaszolja a kérdést: „**Kinek van *hozzáférése* mihez**” – ez a hozzáférési garancia, amely teljes körű megértést és átláthatóságot biztosít azzal kapcsolatosan, hogy ki kicsoda a szervezetekben, és milyen hozzáféréssel rendelkezik az illető. Szükséges számukra ez a hozzáférés? Sérti-e ez a hozzáférés a vállalati irányelveket? Valamint ugyanilyen fontos az is, hogy a szervezetek hogyan szabják igényekre és hogyan biztosítják, hogy a vállalati felhasználók megértsék a kontextust – vagyis a kockázatot –, és megfelelően tájékozottan, időben és magabiztosan hozzanak üzleti döntéseket – ugyanakkor biztosítják azt is, hogy a felhasználók a megfelelő hozzáférési szintekkel rendelkezzenek a megfelelő alkalmazásokhoz, a megfelelő időben a munkájuk elvégzéséhez.

A SecurID segít támogatni a „legalacsonyabb szintű jogosultság” koncepcióját egy zéró bizalmi keretrendszerben a hozzáférés és a jogosultságok mély átláthatóságával, valamint az ellenőrzési követelményeket támogató irányelvek kialakításának lehetőségével. A SecurID lehetővé teszi a különböző méretű szervezetek számára az identitáskockázatok csökkentését és a megfelelőség fenntartását anélkül, hogy a felhasználók termelékenységét akadályozná.

Az ügyfelek ma a SecurID Governance & Lifecycle szolgáltatást a következőkre használják:

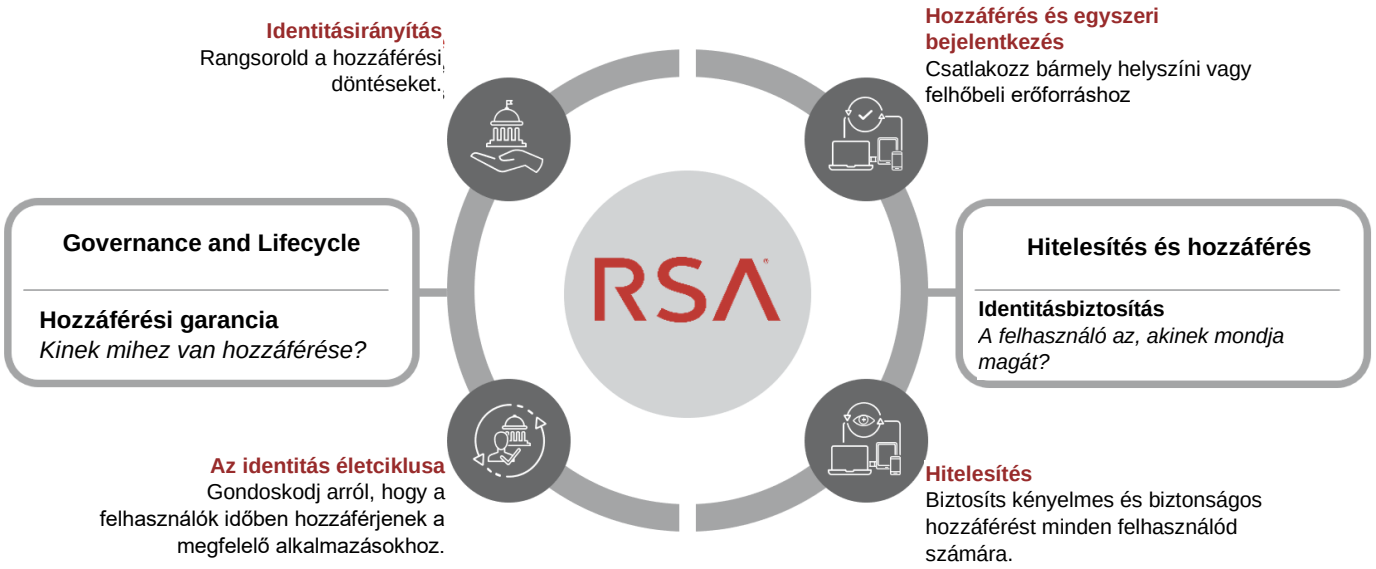
- **TELJES** áttekinthetőséget kapnak az összes alkalmazásában – a helyszíni és a felhőalapú alkalmazásokban – arról, hogy kinek mihez van hozzáférése. A legmélyebb jogosultsági részletekig láthatják, hogy ki mire jogosult.
- **GAZDAG** kiegészítő kontextust és betekintést kapnak annak érdekében, hogy ne csak a biztonsági vizsgálatok legyenek támogatottak, hanem az irányítási folyamatok is pontosak legyenek.

E kockázati rés áthidalására van az **Identity and Access Analytics**, amely biztosítja a szükséges rangsorolást, az útmutatást, valamint azt az üzleti környezetet, amely szükséges a vállalat számára a bővülő kockázatok csökkentéséhez és az optimális hozzáférési garanciához.

Kockázatalapú identitás- és hozzáféréselemzést vezettünk be és használunk, így a szervezetek most könnyen azonosíthatják azokat a kockázatokat, amelyeknek korábban nem voltak tudatában. Folytatjuk a fejlődést ezen a területen, hogy segítsünk a szervezeteknek teljesen új megvilágításban rangsorolni a kockázatokat.

Ügyfélkihívások és követelmények

- ✓ Maximalizáld az erőforrásokat, és okosan költsd el a büdzsét.
- ✓ Először alkalmazz felhőalapú megközelítést.
- ✓ Biztosíts kiszámítható költségszerkezetet.
- ✓ Tartsd fenn a legmagasabb szintű biztonságot és ellenőrzést az adatok és alkalmazások felett.
- ✓ Valósítsd meg a legnagyobb értékű projekteket, amelyek közvetlenül a vállalkozás hasznára válnak.
- ✓ Biztosítsd az üzletmenet folytonosságát, az üzemidőt és a teljesítményt.
- ✓ Minimalizáld a közvetett költségeket: állásidő, csökkent agilitás stb.



A megoldás bizosítja:

- ✓ Indítási szolgáltatások, valamint a SecurID SecurID G&L (felügyelet, frissítések, javítások, operatív irányítási tevékenységek)
- ✓ Hozzáférési áttekintések és gyűjtemények felügyelete
- ✓ Jelentéskészítés és irányítópultok hozzáadása
- ✓ Vírusvizsgálat, teljesítményteszt, penetrációs tesztelés
- ✓ Elakadt munkafolyamatok és folyamatok feloldása
- ✓ Customer Success manager, 24 órás támogatás, előfizetés oktatásra

Biztonságos és kényelmes hitelesítési módszerek

Bár a fő aggodalmat mindig is az alkalmazottak fogják jelenteni, a szervezeteknek egyre nagyobb szükségük van arra, hogy hozzáférést biztosítsanak harmadik felek számára. Az alvállalkozóknak, a partnereknek és az ügyfeleknek egyaránt hozzáférésre van szükségük, különféle okok és a felhasználási forgatókönyvek miatt – és mindannyian különböző preferenciákkal és követelményekkel rendelkeznek.

A felhasználóknak könnyű és kényelmes hozzáférésre van szükségük, neked pedig arra, hogy biztos lehess abban, hogy a felhasználók valóban azok, akiknek mondják magukat. A SecurID segítségével nem kell a kényelmet biztonságra cserélned. A díjnyertes tokenjeinken kívül a SecurID a hitelesítési lehetőségek széles skáláját kínálja, amelyek közvetlenül a felhasználók mobiltelefonján működnek – beleértve a koppintással történő jóváhagyást, a biometrikus azonosítást, az SMS-t és egyebeket –, a „megfelelő méretű” hitelesítést biztosítva minden felhasználó és minden felhasználási mód számára.

Akár a hardvertokenek által egyedülállóan nyújtott „légrés” biztonságára van szükséged, akár az SMS alacsony érintési képességére, a SecurID olyan megoldást kínál, amelyet a felhasználók könnyen tudnak használni, te pedig könnyen telepíthetsz, miközben nyugodt lehetsz, hogy a legérzékenyebb eszközeid védve vannak.

A közelmúltban az RSA kiadott egy új tokent, melynek neve DS100. A DS100 egy jelszó nélküli, többfunkciós biztonsági megoldás, amely a FIDO protokollok kriptográfiai előnyeit hordozza az egyszer használható jelszó (OTP) biztonsági előnyeivel. Más hitelesítőkkel ellentétben a DS100 csatlakoztatva vagy kihúzva is működik, így tökéletes, rugalmas hitelesítési megoldás.

A nem felügyelt BYOD („Használd a saját eszközöd”) védelme (RSA Mobile Lock)

A nagyobb biztonság és a jobb használhatóság érdekében a SecurID a hitelesítést két–három faktoron túlmutatóvá tette. A SecurID gépi tanulásra épülő viselkedéselemzést használ, és üzleti környezetet, valamint fenyegetésekkel kapcsolatos információkat alkalmaz, hogy átfogó képet alkosson a felhasználóról és a hozzáférésükkel kapcsolatos kockázatokról.

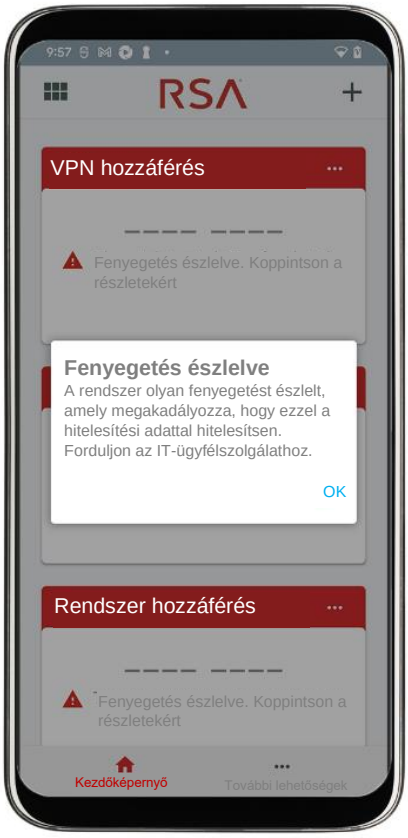
Az arra vonatkozó kontextussal kapcsolatos attribútumok elemzése, hogy mikor és honnan érkezik egy hozzáférési kérelem, az eszköz biztonsági helyzete, a felhasználó szerepe és az alkalmazás érzékenysége, valamint az, hogy a felhasználók ismert csalással kapcsolatba hozhatóak-e, vagy ki vannak-e téve fenyegetéseknek, 360 fokos képet ad a felhasználói hozzáféréssel kapcsolatos kockázatokról.

A SecurID automatikusan és mindenféle beavatkozás nélkül kiszámítja az identitásmegbízhatóság pontszámát (alacsony vagy magas) minden egyes felhasználó számára, különféle adatpontok alapján. Ennek valós időben történő végzésével a szervezetek automatikusan próbára tehetik a felhasználókat a kockázat szintje alapján, biztosítva, hogy a magas kockázatot magas biztonsággal kezeljék, míg az alacsony kockázatú esetekben a felhasználók kényelmét szolgálja, hogy nem kérnek tőlük további hitelesítést.

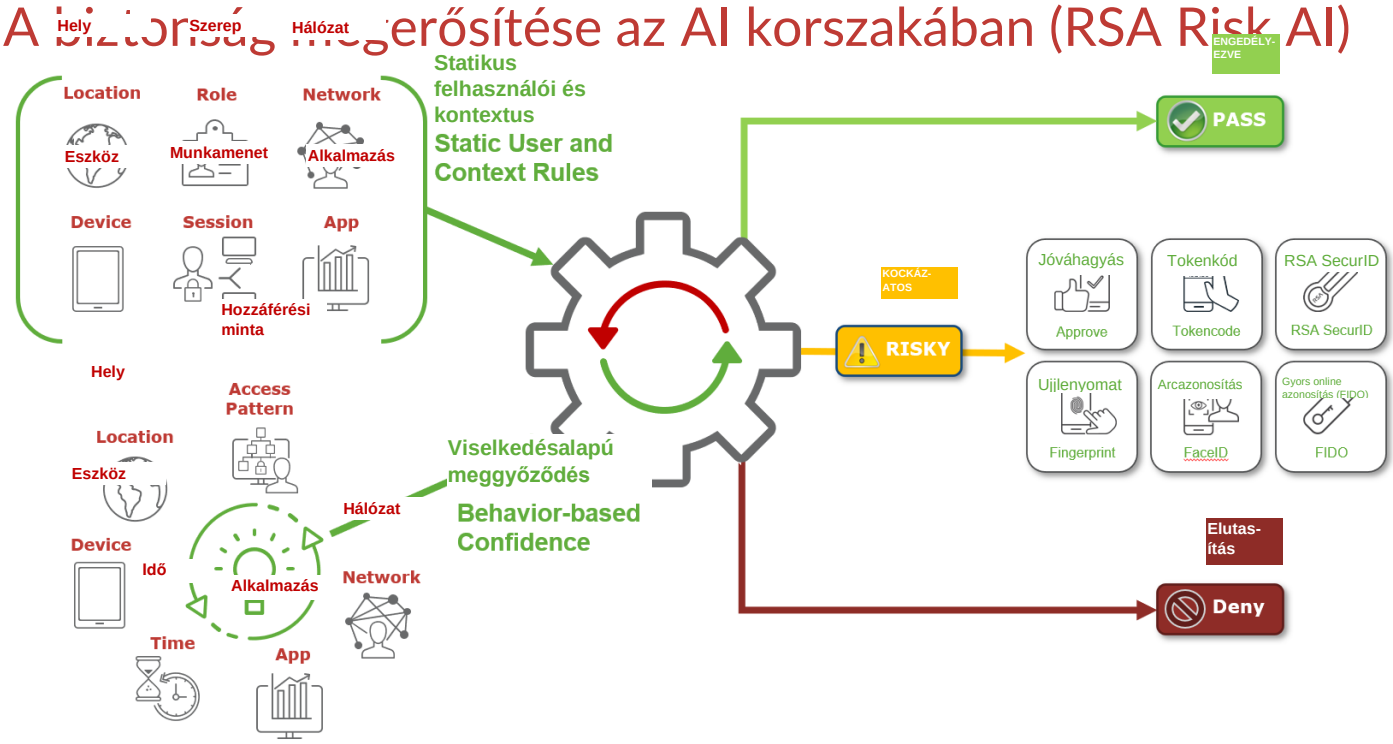
Emellett a SecurID Access további funkciókkal bővült, hogy megkönnyítse és fokozza ügyfeleink identitásának és hitelesítési eszközeinek biztonságát. Például az egyik újonnan hozzáadott szolgáltatásunk, az **RSA Mobile Lock** észleli a mobileszközt érő kritikus fenyegetéseket, és a probléma megoldásáig korlátozza a felhasználó hitelesítési képességét. Fenyegetés esetén az RSA mobilzár figyelmezteti a felhasználót és az IT-t, megakadályozva a hozzáférést a szervezet rendszereihez és adataihoz.

Egy másik újonnan hozzáadott szolgáltatás az **Egységes könyvtár**, amely egy új felhasználói azonosító tároló az RSA felhőalapú hitelesítési szolgáltatás számára, amely lehetővé teszi a jövőben a teljes, kizárólag felhőalapú telepítést. Az RSA Egységes könyvtár képes létrehozni és tárolni helyi felhasználókat és jelszavaikat a nyílt szabványú domainek közötti identitáskezelő rendszer (SCIM) alkalmazásprogramozási felület segítségével. A rendszergazdák a helyi felhasználókat a Felhőfelügyeleti Konzolból kezelhetik. A felhasználók a My Page önkiszolgáló portálon keresztül kezelhetik saját ügyeiket. A helyi felhasználói jelszavakat teljes mértékben a felhőalapú hitelesítési szolgáltatás hagyja jóvá.


RSA
VPN hozzáférés
Fenyegetés észlelve. Koppintson a részletekért
Felhő alkalmazás hozzáférés
Fenyegetés észlelve. Koppintson a részletekért
Rendszer hozzáférés
Fenyegetés észlelve. Koppintson a részletekért
Kezdőképernyő
További lehetőségek


RSA
VPN hozzáférés
Fenyegetés észlelve. Koppintson a részletekért
Fenyegetés észlelve
A rendszer olyan fenyegetést észlelt, amely megakadályozza, hogy ezzel a hitelesítési adattal hitelesítsen. Forduljon az IT-ügyfélszolgálathoz.
OK
Rendszer hozzáférés
Fenyegetés észlelve. Koppintson a részletekért
Kezdőképernyő
További lehetőségek

A biztonság megerősítése az AI korszakában (RSA Risk AI)



Az **RSA® Risk AI** gépi tanulást és egyedi anomália-észlelést használ a szervezet egészére kiterjedő, összefüggésalapú kockázatelemzéshez.

Ne cseréld el a hozzáférhetőséget biztonságra, vagy fordítva – Hogyan lehet úgy védeni az érzékeny erőforrásokat, hogy közben továbbra is észszerűen egyszerű hozzáférést biztosítasz azoknak a felhasználóknak, akiknek szükségük van rájuk? Az RSA® Risk AI intelligensen beállítja a könnyű hozzáférést az egyének kockázati profiljai és korábbi hozzáférési adatai alapján.

Kontextus alapú értékelés – Az RSA® Risk AI technikákat és technológiákat használ – beleértve az adatgyűjtést, az eszközillesztést, az anomáliák észlelését és a viselkedéselemzést – a hozzáférési kísérlet kontextusának meghatározásához. Megvizsgálja, hogy ki kér hozzáférést, hol van az illető, és milyen eszközt használ. A kontextus alapján felméri a hozzáférési kockázatot.

RSA® Risk AI – A hozzáférési kérelmek kockázatának felmérése mellett a Risk AI egy gépi tanulási kockázati motor, amely viselkedéselemzést végez az anomáliák valós idejű kockázatpontozással történő észlelésére. A Risk AI tanul az értékeléseiből, és ezt a tudást alkalmazza a jövőbeni kérésekre.

Hitelesítési lehetőségek – Ha a hozzáférési kockázat szintje a hitelesítés egy másik faktorát indokolja, az RSA többfaktoros hitelesítés (MFA) számos lehetőséget kínál az erős hitelesítéshez. Ez megakadályozza, hogy egy illegitim hozzáférési kísérlet ne hárítson szükségtelenül nagy terhet a jogos felhasználókra.

A hitelesítési követelmények egyszerűsítése

Mivel számos alkalmazást kell támogatni, és egyre többféle módon lehet ellenőrizni a felhasználókat és mérni a hozzáférési kockázatot, a szervezeteknek szükségük van egy egyszerű módszerre, amellyel mindezt összefoghatják – egy egyszerű módszerre a hitelesítési követelmények meghatározásához.

Mivel a különböző használati módok különböző szintű hitelesítést igényelnek, a SecurID egyszerű módot biztosít a szervezetek számára a hitelesítési beállítások konfigurálására az általa gyűjtött felhasználói, alkalmazási, környezeti és kockázati információk alapján.

A SecurID biztosítási szintjei lehetővé teszik a szervezetek számára, hogy egyszerűen három szintre – alacsony, közepes és magas megbízhatósági szintre – osszák be a felhasználási módokra vonatkozó követelményeiket. Mindegyik szint megfelel annak a relatív erősségnek, amelyet a biztonsági szervezetek egy adott alkalmazáshoz vagy felhasználási forgatókönyvhöz igényelnek. Az alacsony kockázatú forgatókönyvek alacsony szintű biztosítást (ellenőrzést) igényelnek, míg a magasabb kockázatú forgatókönyvek eltérő, biztonságosabb típusú hozzáférés-szabályozást igényelhetnek.

SecurID alapelemek

Hitelesítési módszerek – A SecurID díjnyertes hardver-és szoftvertokenek mellett a SecurID a telefon alapú hitelesítési lehetőségek széles skáláját kínálja, beleértve a koppintással történő jóváhagyást, az egyszer használható jelszót, a biometrikus azonosítást, az SMS-t, és másokat. Ezenkívül a SecurID kockázatalapú vagy adaptív hitelesítést is kínál, amely gépi tanulási viselkedéselemzést használ az egyes felhasználók valós idejű megbízhatósági pontszámának meghatározásához.

SecurID Cloud Authentication Service – egy szolgáltatott szoftver (SaaS) hozzáférési és hitelesítési platform, amely egyszeri bejelentkezést (SSO) és többfaktoros hitelesítést biztosít SaaS-, felhő- web- és mobilalkalmazásokhoz. A felhőalapú hitelesítési szolgáltatás elfogadhat olyan, harmadik fél SSO-megoldásaitól vagy felhőalkalmazásaitól származó hitelesítési kérelmeket is, amelyek úgy lettek konfigurálva, hogy a SecurID-t identitásszolgáltatóként (IdP) használják a hitelesítéshez.

SecurID Authentication Manager – ellenőrzi a hitelesítési kérelmeket, és központilag felügyeli a hitelesítési irányelveket, a SecurID tokeneket, a felhasználókat, az ügynököket és az erőforrásokat a fizikai webhelyeken, hogy segítse a biztonságos hozzáférést a helyszíni, felhőalapú és weben elérhető alkalmazásokhoz, például VPN-ekhez és webportálokhoz.

SecurID Agents and APIs – A SecurID csatlakozókat és szabványos ügynököket biztosít SAML- és RADIUS-alapú alkalmazásokhoz, valamint IIS/Apache-hez, Windowshoz, Unix/Linuxhoz és ADFS-hez. Ezenkívül az RSA REST-alapú API-t biztosít, így a szervezetek többfaktoros hitelesítést adhatnak egyéni alkalmazásaikhoz.

A biztonsági pontok csatlakoztatása

Míg a tanúsított integrációk, a hitelesítők széles skálája és az intelligens, kockázatalapú hitelesítés mind kritikus képességek annak biztosításához, hogy tudd, ki a felhasználó, a folyamatosan fejlődő támadások megelőzéséhez átfogó átláthatóságra van szükség az egész szervezetben.
A SecurID összekapcsolja a pontokat a megoldásai között, hogy kiküszöbölje az identitáshoz kapcsolódó holttereket, lehetővé téve az identitáson alapuló fenyegetésekre való gyorsabb reagálást, összehangolt és automatizált módon.

SecurID Governance & Lifecycle – felhasználói hozzáférési engedélyezési adatokkal tudja biztosítani, hogy a felhasználók csak a megfelelő dolgokhoz férjenek hozzá.

A SecurID, az iparág legfejlettebb hitelesítési platformja lehetővé teszi a felhasználók számára, hogy többet tegyenek, azáltal, hogy szabadságot ad számukra, hogy ott és akkor dolgozzanak, ahol és amikor csak akarnak, miközben lehetővé teszi a vállalatod és a hozzá kapcsolódó IT-infrastruktúra átalakítását, miközben megakadályozza, hogy az identitáskockázatok rontsák az üzleti eredményed. További részletek: www.rsa.com

SecurID bizonyított piaci tapasztalat

- ✓ Több mint 25 000 ügyfél világszerte
- ✓ Több mint 50%-os piaci részesedés
- ✓ Több mint 50 millió aktív token van forgalomban
- ✓ Évente 10 millió egységet szállítunk ki
- ✓ Együttműködőképes több mint 500 tanúsított megoldással (SaaS és helyszíni)
- ✓ Naponta több tíz millió hitelesítést hajtanak végre
- ✓ A többfaktoros hitelesítés vitathatatlan vezetője
    - ✓ Az SC Magazine 2019-es „Legjobb többfaktoros hitelesítési megoldás” díjazottja
    - ✓ Az SC Magazine által „az elmúlt 30 év egyik legkritikusabb megoldása” díj győztese (2019)
    - ✓ Több mint 30 éve úttörő és innovatív piacvezető a vállalati többfaktoros hitelesítés területén

SecurID hitelesítési beállítások

- ✓ Push/Approve
- ✓ Mobil token kód (OTP)
- ✓ Eszköz biometrikus adatai
- ✓ Apple watch / Android Wear
- ✓ FIDO token
- ✓ SecurID szoftvertokenek
- ✓ SecurID hardvertokenek
- ✓ SecurID DS100 token
- ✓ SMS/Email OTP igény szerint
- ✓ QR kód
- ✓ További lehetőségek...

SecurID ügyfelek

A SecurID világszerte kiterjedt ügyfélkörrel rendelkezik, több mint 25 000 ügyféllel számos iparágban, többek között:

- ✓ 20. a TOP 20 gyártó közül
- ✓ 19. a TOP 20 pénzügyi szolgáltató közül
- ✓ 19. a TOP 20 egészségügyi szervezet közül
- ✓ 19. a TOP 20 közlekedési szervezet közül
- ✓ 19. a TOP 20 fogyasztó közül
- ✓ 18. a TOP 20 telekommunikációs szolgáltató közül
- ✓ 16. a TOP 20 energiaszolgáltató közül
- ✓ 13. az USA kormányának 15 végrehajtó minisztériuma közül

SecurID termékelemek és biztonság

A SecurID biztonságos és kényelmes hozzáférést biztosít a mai SaaS-hoz és a helyszíni webalkalmazásokhoz, a harmadik féltől származó SSO-megoldásokhoz, valamint a RADIUS-t támogató helyszíni erőforrásokhoz, így visszaszerezheted az irányítást a megszakadt terület felett, és felgyorsíthatod a felhasználói termelékenységet. Ez a szakasz a SecurID elemeit és a biztonsági áttekintést ismerteti.

Infrastrukturális réteg

Infrastruktúraszolgáltató

A SecurID a Microsofton® Azure® rendszeren található felhőalapú számítástechnikai platform, amelyet a Microsoft adatközpontjainak globális hálózatán keresztül üzemeltetnek. A SecurID többvállalatos adatbázist használ egy olyan környezetben, amely megosztott infrastruktúrán alapul, ugyanakkor az ügyféladatokat elkülöníti az adatvédelem biztosítása érdekében. A hardverinfrastruktúra-elemek – beleértve, de nem kizárólagosan a tűzfalakat, a terheléselosztókat, a webszervereket, az adatbázisszervereket és a tárolóeszközöket – több ügyfél között vannak megosztva. A szolgáltatási szintek és működési eljárások a platform közös jellegéből adódóan minden ügyfél számára egységesek. További információk: Microsoft Azure Trust Center.

Szolgáltatási infrastruktúra

A SecurID infrastruktúra egymásra épülő szolgáltatásokból áll. A felső réteg szolgáltatásai szélesebb körben elérhetők, de a legkevesebb érzékeny információt tartalmazzák. Az alsóbb rétegek szolgáltatásai rendelkeznek a legtöbb jogosultsággal; az ezekhez a rétegekhez való hozzáférés ezért szigorúbban ellenőrzött. Az RSA SaaS Operation szolgáltatásai ennek az infrastruktúrának a középpontjában állnak, és felelősek a teljes rendszer állapotának felügyeletéért, valamint a karbantartási eljárások végrehajtásáért, például a termékfrissítésekért. Az RSA SaaS Operations rendszernek privilegizált hozzáférésre van szüksége a teljes szolgáltatási környezethez, és a szolgáltatásokat egy auditált, lezárt és szigorúan ellenőrzött rendszerből végzik.

Ügyfél infrastruktúra

A SecurID lehetővé teszi az ügyfelek számára, hogy SaaS-hez, mobil- vagy webalkalmazásokhoz kapcsolódjanak. Az alkalmazások hitelesítését az identitásrouter kezeli, amely egy virtuális eszköz, amelyet az ügyfelek a környezetükben vagy a felhőben telepítenek. Az identitásrouter biztosítja az irányelvek érvényesülését és egy központi döntési pontot, amely minden felhasználó számára érvényesíti a hitelesítést és a jogosultságot. Az identitásrouter az összes felhasználói művelet ellenőrzési gyűjtőpontjaként is szolgál.

Biztonsági ellenőrzések

Adatbiztonság és titkosítás

A SecurID szolgáltatás kriptográfiailag erős titkosítást és kulcskezelést használ az érzékeny adatok nyugalmi és átviteli biztonsága érdekében. A titkosítás szabványos, szakértői értékeléssel rendelkező kriptográfiai algoritmusokkal van biztosítva, és AES 128 bites kulcsot használ az átviteli adatokhoz és AES 256 bites kulcsot a nyugalmi adatokhoz. A SecurID Access felhőalapú hitelesítési szolgáltatásból/szolgáltatásba érkező összes kapcsolat az adatok érzékenységétől függetlenül TLS 1.2 protokollal, ECDHE műveletkulcs megegyezéssel, 2048 bites RSA aláírással és AES 128 bites kulcsokkal van biztosítva. A SecurID felhőalapú hitelesítési szolgáltatás és a helyszíni identitásrouter között váltott üzenetek tanúsítványalapú digitális aláírást és titkosítást használnak. A hibrid felhőmodell a többrétegű titkosítás mellett lehetővé teszi a SecurID ügyfelek számára, hogy legérzékenyebb adataikat a helyszínen tartsák, és minimalizálják a felhőbe küldött érzékeny adatok mennyiségét.

SecurID Felhőalapú hitelesítési szolgáltatás

A SecurID az Egyesült Államokban és Európában üzemeltet adatközpontokat. A felhőalapú hitelesítési szolgáltatás infrastruktúra biztosítja a rendszergazdai felületet a SecurID identitásrouter, a hitelesítési irányelvek, az identitásforrások és az alkalmazáskonfiguráció kezeléséhez. A SecurID felhőalapú hitelesítési szolgáltatás infrastruktúrát biztosít a push értesítések mobileszközökre küldéséhez az erős hitelesítés érdekében.

A SecurID felhőalapú hitelesítési szolgáltatás számos natív biztonsági funkcióval rendelkezik, többek között:

- ✓ Tűzfalak, VPN-ek, hálózati elkülönítés.
- ✓ Terheléselosztás és magas rendelkezésre állás.
- ✓ Az elosztott szolgáltatásmegtagadással járó támadások (DDoS-támadások) elhárítása.
- ✓ Host alapú IDS és szolgáltatásfelügyelet.
- ✓ Titkosított kommunikáció a szolgáltatás elemei között.

A SecurID felhőalapú hitelesítési szolgáltatás több rétegre van felosztva a különböző hálózati szegmensekben. A szintek közötti kommunikáció korlátozott, annak biztosítása érdekében, hogy az első szintet veszélyeztető támadó ne férhessen hozzá a következő szintekhez.

SecurID hitelesítési alkalmazás

A SecurID hitelesítési alkalmazás a SecurID szolgáltatás további hitelesítőjeként működik. A SecurID végfelhasználók a készüléket eszközhitelesítéssel, push-értesítés jóváhagyásával vagy tokenkód hitelesítéssel „valami, amivel rendelkezel” hitelesítési faktorként használhatják. Ha megköveteli a felhasználóktól, hogy a tokenkód megtekintése előtt elvégezzék a hitelesítést, az alkalmazás is lehet „valami, amit tudsz”. Az alkalmazás a „valami vagy” hitelesítési faktorok, például az ujjlenyomat vagy a retina beolvasásával történő biometrikus azonosítás beviteli mechanizmusaiként is funkcionál. A hitelesítési alkalmazás számos natív biztonsági funkcióval rendelkezik, amelyek a következőket tartalmazzák:

- ✓ Az alkalmazáscsomag aláírásának ellenőrzése telepítéskor.
- ✓ A helyileg tárolt érzékeny adatok titkosítása.
- ✓ A SecurID felhőalapú hitelesítési szolgáltatásból/szolgáltatásba érkező összes forgalom titkosítása.
- ✓ Az eszköz biztonságos regisztrálása tanúsítványrögzítéssel.

- ✓ Android-eszközökön bájtkód-obfuszkáció és hardveres kulcstárolás.
- ✓ Az RSA teszteli az összes alkalmazást biztonsági és sebezhetőségi szempontokból.

Identity Router

Az identity router egy védett virtuális eszköz, amelyet az ügyfél a helyszínen vagy felhőkörnyezetben üzemeltet és kezel. A telepítéstől függően az identity router vagy a felhőalapú hitelesítési szolgáltatás irányelv-döntési pontként (PDP) és irányelv-végrehajtási pontként (PEP) működik. Az identity router a helyszíni infrastruktúrával (pl. Microsoft Active Directory, LDAP v3 könyvtárszerver, hitelesítéskezelő) és a SecurID felhőalapú hitelesítési szolgáltatással kommunikál. Az identity router fordított proxyként is működik a HTTP-összevonás/jelszótároló vagy a HTTP-fejlécek harmadik féltől származó alkalmazásaival való integrációjához. Az identity router lehetővé teszi a SecurID szolgáltatás számára, hogy hibrid üzembe helyezési modellt biztosítson, amely által a legérzékenyebb adataid a helyszínen és a te irányításod alatt maradhatnak.

Az identity router számos biztonsági funkcióval rendelkezik, amelyek a következőket tartalmazzák:

- ✓ Védett, lezárt, harmadik fél által tesztelt készülék.
- ✓ Az IDR és a SecurID szolgáltatás közötti titkosított kommunikáció TLS v1.2 protokollt használ.
- ✓ A nyilvános kulcs kitűzése a konfiguráció során a szolgáltatáshoz való csatlakozáshoz használatos.
- ✓ Az IDR csak egy korlátozott élettartamú, egyszeri jelszóval regisztrálható a szolgáltatásba, amelyet az üzemeltetett szolgáltatás rendszergazdai konzolján generáltak.
- ✓ A felhasználói kulcsláncok felhasználóspecifikus kulcsokkal vannak titkosítva.
- ✓ A felhasználóspecifikus kulcsok egyedi vállalati kulccsal vannak titkosítva.
- ✓ Minden érzékeny adat titkosítva van a virtuális eszközön.

A telepítés után az identity router konfigurációját a SecurID felhőalapú hitelesítési szolgáltatás kezeli.

Felhasználói adatok

A SecurID felhasználói adatokat gyűjt, hogy a hitelesítés során kiszámítsa az identitás megbízhatósági pontszámát. A megbízhatósági pontszám segítségével meghatározhatod, hogy milyen szintű hitelesítésre van szükség. Például, ha a megbízhatóság alacsony, magasabb szintű hitelesítést igényelhetsz.

A SecurID adatokat gyűjt a következők meghatározásához:

- ✓ Helymeghatározás
- ✓ Hálózat
- ✓ Eszköz ujjlenyomat
- ✓ Idő
- ✓ Hozzáférési minták

RSA SaaS műveletek

Személyzeti belépés ellenőrzése

A SecurID egy külön SaaS-műveleti csapattal rendelkezik, amely a SecurID szolgáltatás és infrastruktúra napi karbantartását és üzemeltetését végzi. Az RSA földrajzilag elosztott műveleti központokat tart fenn az Egyesült Államokban, Izraelben és Indiában. A szolgáltatási környezet a SecurID műveleti konzolon keresztül kezelhető.

- ✓ A műveleti konzolhoz csak az üzemeltetési csapat azon tagjai férhetnek hozzá, akik a szolgáltatás fenntartásáért felelősek.
- ✓ Az alkalmazottaknak el kell végezniük az üzemeltetési, a biztonságtudatossági és a biztonságos fejlesztési képzést, mielőtt hozzáférést kapnak a műveleti konzolhoz.
- ✓ A műveleti konzol szerepkör alapú hozzáférés-vezérlő rendszert használ, hogy a kezelő hozzáférését az adott kezelő feladatainak ellátásához szükséges funkciókra korlátozza.
- ✓ A műveleti konzolon végrehajtott összes művelet naplózásra kerül ellenőrzés céljából.
- ✓ A hozzáférés az alkalmazott felmondása után azonnal visszavonásra kerül.

Fizikai belépés ellenőrzése

Fizikai beléptetőrendszerek működnek, amelyek korlátozzák a hozzáférést a műveleti központokhoz és azokon belül.

- ✓ A belépőkártyás beléptetőrendszer a létesítmények határain és a létesítményeken belül is működik.
- ✓ Az adatközpont eléréséhez kétfaktoros hitelesítés szükséges.
- ✓ A látogatói naplók rögzítik a látogatók vállalati létesítménybe való belépését.
- ✓ A látogatóknak látogatói jelvényt kell viselniük a helyszínen, és ezek a kitűzők megkülönböztethetők az alkalmazottak jelvényeitől.
- ✓ A látogatókhoz mindenkor kíséret szükséges.

Felügyelet

A folyamatos üzemidő biztosítása érdekében a szerverinfrastruktúra minden eleme felügyelet alatt áll. A felügyelet a következőkről történik:

- ✓ A Microsoft Azure felhőből, hogy betekintést nyújtson a külső hálózatokról nem elérhető belső szolgáltatások állapotába.
- ✓ Külső felügyeleti szolgáltatás, amely független üzemidő-értékelést végez.

A szolgáltatás által észlelt rosszindulatú események kivizsgálására és az azokra való reagálásra meghatározott eljárásokat alkalmaznak az időben történő megoldás érdekében.

Frissítés és javítás

A felhőinfrastruktúra összes eleme a Microsoft Azure rendszerben található a legújabb biztonsági és operációsrendszer-javításokkal. Alkalmazás előtt minden szoftverfrissítés a SecurID fejlesztői környezetében kerül tesztelésre és jóváhagyásra. A szoftverfrissítés kiadása után a rendszereket gondos felügyelet alatt állnak, hogy biztosítsák az érintett szolgáltatások folyamatos és zavartalan működését.

RSA ID Plus

A SecurID ügyfelei számos lehetőség közül választhatják ki hitelesítőiket – a hardvertokenektől a mobilos többfaktoros hitelesítési lehetőségekig, beleértve az egyszer használható jelszót, a koppintással történő jóváhagyást, a biometrikus azonosítást, az SMS-t és a FIDO-t.

A SecurID kényelmesen megvásárolható attól függően, hogy egy szervezetnek mit kell védenie, hogyan akarja azt védeni, és hogyan kívánja telepíteni a megoldást. A SecurID ajánlatok már elérhetőek. További információ a securid.com/cloud pricing felületen található.

SecurID licencelési lehetőségek:

- ✓ **ID Plus C1 –** Felhőalapú hozzáférési és hitelesítési megoldás az elinduláshoz. Biztosítsa felhőalapú alkalmazásait, rendszereit és felhasználóit a felhőben a következő generációs, mobilra optimalizált hitelesítési lehetőségeket, beleértve a push-üzeneteket, a biometrikus azonosítást, a tokeneket stb. Biztosítsa a hozzáférést a felhőalkalmazásokhoz egyszeri bejelentkezéssel (SSO).

- ✓ **ID Plus E1 –** Vállalata bővülése során ez a terv támogat téged, hogy testreszabott vezérlőkkel kezelhesse a növekvő felhasználói hozzáférést és használatot. A SecurID Cloud Plus csomagban foglaltakon túlmenően ez a csomag feltételes szabályalapú, helyszíni és ügyfélalapú szerverek és alkalmazások védelmét, a SecurID implementáció sikerének biztosítása érdekében egy digitális ügyfélsiker-menedzsert és még sok mást is tartalmaz.

- ✓ **ID Plus E2 –** Egy hibrid on-prem, felhőalapú identitásmegoldás esetén a Cloud Premier csomag dinamikus, adaptív irányelvekkel védi a gyorsan fejlődő hozzáférést on-prem és a felhőben. Ez a szintű identitásbiztosítás magában foglalja a SecurID Cloud Plus összes előnyét, valamint a dinamikus, kockázatalapú hitelesítést és a hozzáférés-szabályozást, a testreszabható SSO portált, az RSA Mobile SDK-t, a SecurID Authentication Manager rendszerben történő helyszíni hitelesítéskezelést, a névre szóló ügyfélsiker-menedzsert, aki rendszeresen együttműködik a sikerességi mutatók tekintetében, és még sok minden mást.

- ✓ **ID Plus E3 –** Egy hibrid on-prem, felhőalapú identitásmegoldás, tartalmazva a piacon elérhető legjobb differenciálóinkat. Megkpja az összes helyszíni SecurID és Cloud Plus előnyt, beleértve a Risk AI motort, a fenyegetéstudatos hitelesítést, a mobile-lock-ot és egyéb funkciókat. Ez a csomag biztonságossá teszi környezetedet, optimális szintű identitásbiztosítást nyújt, bizalmat ébreszt a nem felügyelt mobileszközökben, és még sok más.

RSA Risk & Cybersecurity gyakorlat

Az RSA kockázati és kiberbiztonsági gyakorlata segít az ügyfeleknek olyan megoldások bevezetésében, amelyek csökkentik a kockázatokat, biztosítják a megfelelőséget és felgyorsítják a kitűzött üzleti célok megvalósítását. A gyakorlat magában foglalja a tervezést, a megvalósítást és a működési hatékonyságot a kockázatkezelésen, az identitásbiztosításon és a biztonsági műveleteken belül. A kiberfenyegetések azonosításával, csökkentésével és felszámolásával, a kockázatkezelési programok fejlesztésével és a megfelelőségi követelmények teljesítésével csökkentjük az üzleti kockázatokat.

RSA Risk & Cybersecurity gyakorlat

RSA kockázati és kiberbiztonsági tanácsadó szolgáltatások élen járnak az üzleti követelményekhez igazodó kiberbiztonsági stratégiák szervezetek számára történő kidolgozásának segítésében.

RSA professzionális szolgáltatások segítenek a szervezeteknek optimalizálni az RSA technológiákba való befektetéseiket, beleértve az RSA SecurID csomagot, az RSA NetWitness Platformot, az RSA Archer csomagot és az RSA Csalás-és kockázatiIntelligencia csomagot.

https://www.rsa.com/en-us/services/rsa-risk-and-cybersecurity-practice

RSA Risk and Cybersecurity tanácsadó szolgáltatások

A szervezetek továbbra is küzdenek a szigorú megfelelőségi követelményekkel, a kifinomult fenyegetésekkel és a célzott támadásokkal. Az összetett szabályozások és az elszánt ellenfelek még a legszilárdabb képességeket és védelmet is alááshatják. Az RSA kockázati és kiberbiztonsági tanácsadó szolgáltatásai segítenek a szervezeteknek az üzlethez igazított biztonsági stratégiák kidolgozásában, és olyan biztonsági irányt jelölnek ki, amely a fenyegetésekkel együtt fejlődik, és védi a szervezet misszióját.

RSA professzionális szolgáltatások

Az ügyfelek elvárásai akkor teljesülnek a legjobban, ha a termékek telepítését megfelelően megtervezik, végrehajtják és megfelelően karbantartják. Azok a szervezetek, amelyek a házon belüli erőforrásokat további szakértelemmel kívánják kiegészíteni, hasznosíthatják a gyakorlatot, hogy az RSA termékbefektetésekkel felgyorsítsák az értékteremtési időt:

- ✓ ***Fenyegetésészlelés és reakció:*** RSA NetWitness csomag
- ✓ ***Egységes vállalati kockázatkezelés:*** RSA Archer csomag
- ✓ ***Identitás és hozzáférésmenedzsment:*** RSA SecurID and RSA Identity Governance & Lifecycle
- ✓ ***A csalás megelőzése:*** RSA Fraud & Risk Intelligence csomag

Az RSA globálisan elosztott személyzettel és erőforrásokkal, valamint több ezer megbízás során szerzett tapasztalattal segíti a szervezeteket a megoldások jellemzőinek és funkcióinak megtervezésében és optimalizálásában. Ez felgyorsítja az értékteremtési időt és maximalizálja a technológiai beruházások megtérülését.

RSA globális szolgáltatási partnerek

Az RSA Risk and Cybersecurity gyakorlat a SecurWorld partnereinkkel, az RSA-termékeket értékesítő akkreditált cégek globális hálózatával dolgozik együtt, hogy tervezési, megvalósítási és támogatási szolgáltatásokat nyújtsanak, valamint stratégiai szolgáltatásokat kínáljanak, amelyek összhangban vannak módszereinkkel és gyakorlatainkkal. Mindannyian elkötelezettek vagyunk amellett, hogy megfelelő szakértelmet, tudást és erőforrásokat biztosítsunk ügyfeleink üzleti igényeinek kielégítéséhez, és a kockázati

és kiberbiztonsági programok jobb irányításának útjára tereljük őket, hogy magabiztosabban tudjanak megfelelni az előttük álló kihívásoknak.

Az RSA megoldás tervezése és megvalósítása

A hitelesítés és az identitás igazolása minden vállalati biztonsági kezdeményezés szükséges eleme az információkhoz való hozzáférés védelme érdekében, különösen napjainkban, a digitális munkaerő-átalakítás világában. Az RSA világszerte elismert megoldásainak 30 éves múltját hasznosítva emberek milliói használják az RSA SecurID hitelesítőket VPN-ek, vezeték nélküli hozzáférési pontok, távoli hozzáférésű tűzfalak, webes és SaaS alkalmazások, valamint hálózati operációs rendszerek biztonságos eléréséhez.

Ugyanígy az RSA ügyfelei is bíznak a SecurID Access zászlóshajó megoldásunkban és tudják, hogy számíthatnak az RSA szervizszakembereire. Az RSA csapata képzett szakemberekből áll, akik minden egyes projekthez a biztonsági trendek széleskörű ismeretét, a szervezetek szolgálatában eltöltött évek tapasztalatát és az RSA hitelesítési technológiájának mélyreható ismeretét hozzák.

Az RSA professzionális szolgáltatások biztosítják azt a szakértelmet, amelyre szükséged van az üzleti céljaidnak megfelelő biztonsági szint eléréséhez.

- ✓ Áttekintést nyújt az erős hitelesítéssel és az új funkciók hasznosításával kapcsolatos üzleti követelményekről.
- ✓ Megoldást határoz meg logikai és fizikai architektúrákkal.
- ✓ Részletes migrációs/frissítési tervet határoz meg a zökkenőmentes átállás biztosítása érdekében.
- ✓ RSA Authentication Manager és Agent alkalmazásintegrációkat valósít meg a fokozott biztonság érdekében.
- ✓ RSA SecurID SSO ügynök- és felhőszolgáltatásokat valósít meg a többfaktoros mobil identitásbiztosításhoz.
- ✓ Átfogó tesztelési és gyártási megvalósítási támogatást nyújt.
- ✓ Testreszabott megoldásokat határoz meg az üzleti igényeid alapján.
- ✓ Biztosítja az RSA és a szervezeted közötti együttműködéshez kapcsolódó alapvető projektmenedzsment tevékenységeket.

Az RSA professzionális szolgáltatások előnyei

A biztonsági technológiába történő befektetés megtérülésének maximalizálása érdekében világos képet kell kapnod a megvásárolt termékek konfigurálásának, bevezetésének, rendszergazdai irányításának és támogatásának legjobb módszereiről. Az RSA professzionális szolgáltatások biztosítja azt a szakértelmet, amely a biztonság mérhető, a te üzleti céljaidhoz igazodó fejlesztéséhez szükséges.

Az igényekre szabható, erős hitelesítési infrastruktúra sikeres telepítéséhez alapos követelményelemzésre és megfelelő tervezésre van szükség. Az RSA olyan szakaszos megközelítést javasol, amely biztosítja a legfontosabb mérföldkövek sikeres teljesítését még a legkisebb bevezetések előtt. Ezek a fázisok magukban foglalják a követelményelemzést, a megoldás/architektúra megtervezését, a tesztelés végrehajtását, a gyártás megvalósítását, a tudásátadást és a lezárást.

Az RSA professzionális szolgáltatásokat választó szervezetek a következő üzleti előnyöket realizálják:

- ✓ Minimalizálják a projekt azon kockázatait, amelyek az RSA többtényezős hitelesítés környezetükbe történő bevezetésével kapcsolatosak.
- ✓ Minimalizálják az RSA SecurID-környezetük legújabb kiadásra történő frissítésével járó leállási időt.
- ✓ Biztosak lehetnek afelől, hogy az ügyfelek az RSA SecurID összes funkcióját üzleti céljaik támogatása érdekében hasznosítják.
- ✓ Hasznosítják az elkötelezett RSA SecurID-tanácsadók tudását és tapasztalatát.
- ✓ Biztosak lehetnek afelől, hogy az RSA SecurID környezetük összhangban van az RSA és az iparági bevett gyakorlataival.

RSA SecurID szolgáltatásportfólió

Az RSA világszínvonalú szakértelemmel rendelkezik a megoldási stratégia, a tervezés, a megvalósítás és a menedzsmentgyakorlatok irányításához, amelyek elengedhetetlenek annak biztosítása érdekében, hogy az ügyfelek a lehető legnagyobb értéket vehessék ki az RSA SecurID technológiába történő befektetésükből. Sok ügyfél is, aki képes a saját maga elvégezni a telepítést, az RSA professzionális szolgáltatásait választja, hogy konzultáljon a SecurID Access telepítésének stratégiájával, tervezésével és architektúra-tervezésével kapcsolatban annak érdekében, hogy az áttéréskor a technológia teljes értékét hasznosíthassa.

Az RSA professzionális szolgáltatások kiforrott kínálati portfólióval rendelkeznek az ügyfelek és az RSA SecurID telepítési forgatókönyveinek széles skálájához. Ez a portfólió magában foglal egy sor fix áras „Quick Start" szolgáltatási ajánlatot, amelyek célja, hogy a kevésbé összetett telepítésekkel rendelkező ügyfelek számára felgyorsítsák az értékteremtési időt, valamint testreszabható szolgáltatási ajánlatokat kínáljanak, amelyek megfelelnek a nagyvállalatok igényeinek, és lehetővé teszik az olyan személyre szabott megoldások telepítését, amelyek mélyen integrálják az Authentication Manager, a SecurID Agents, a SecurID SSO Agent és a felhőszolgáltatások funkcióit az ügyfél infrastruktúrájába.

Szolgáltatási adatlap – RSA SecurID „Quick Start" szolgáltatások

RSA professzionális szolgáltatások az RSA SecurID bővítési és átállási forgatókönyveihez

Az RSA professzionális szolgáltatások kulcsszerepet játszik abban, hogy az RSA meglévő ügyfelei optimalizálják az új RSA SecurID termékjellemzők és funkciók használatát, hogy új felhasználási módok felé terjeszkedhessenek, és szükség szerint más hitelesítési módszerekre térhessenek át. Az RSA SecurID – az Authentication Manager rendszeren és az RSA felhőalapú hitelesítési szolgáltatáson keresztül – számos MFA-módszert kínál a szervezet biztonsági igényeinek és a kívánt végfelhasználói élménynek legjobban megfelelő módon. Az RSA professzionális tanácsadói csapata végigkíséri az ügyfeleket az MFA-útjukon, az egyes ügyfelek számára megfelelő átállási ütemben.

Az RSA professzionális szolgáltatások kritikus segítséget nyújtanak az architektúra tervezésében és az infrastruktúra, a felhasználók és/vagy hitelesítők migrációjában. Az RSA professzionális szolgáltatások migrációs szolgáltatások áttekintése a következő címen található:
Szolgáltatási adatlap – SID Access Migration Services

RSA SecurID Prime

Az RSA SecurID Prime az RSA előre csomagolt, ugyanakkor rendkívül rugalmas és bővíthető szoftverkomponensekből álló csomagja, amely lehetővé teszi az RSA SecurID életciklus-kezelésének racionalizálását. RSA SecurID Prime szoftver a kifinomult RSA Authentication Manager-ügyfelek egyedi igényeit célozza meg, kibővítve az iparág vezető erős hitelesítési platformját. Az előre csomagolt szoftver egyik előnye, hogy az RSA SecurID Prime elemei idővel frissülnek, és ezek rendszeresen elérhetővé válnak. Ezek az elemek következők:

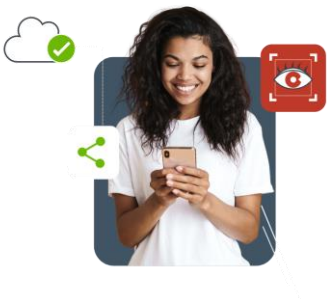
- ✓ **RSA Authentication Manager Integration Services (AMIS)** – REST-alapú webes szolgáltatásközvetítő csomag, amely üzleti szintű API-kon keresztül megkönnyíti és egyszerűsíti az AM-hez való integrációt. Támogatja az AM 6.1, 7.1 és 8-as verzióival való integrációt.
- ✓ **RSA SecurID Prime Self-Service Portal (SSP)** – Végfelhasználói webes portál, amely támogatja a token-önkiszolgáló funkciókat a token(ek) igényléséhez, aktiválásához, cseréjéhez és kezeléséhez. Akkor alkalmazható, ha az ügyfél munkafolyamat- és/vagy testreszabási követelményei nem teljesíthetők az RSA AM 8 önkiszolgáló konzolon keresztül.
- ✓ **RSA SecurID Prime Help Desk Admin Portal (HDAP)** – Egyszerű, észszerűsített webes adminisztrációs felület a mindennapi RSA SecurID ügyfélszolgálati feladatokhoz. Különösen alkalmas a több száz ügyfélszolgálatos munkatárssal rendelkező szervezetek számára. Telepíthető önállóan vagy az AM Prime SSP-vel együtt az integrált tokenszolgáltatási munkafolyamatok támogatása érdekében.

Az RSA SecurID Prime elemek támogatási mechanizmusát a PS csomagolt egyéni alkalmazástámogatás (CAS) biztosítja. Ha az ügyfelek éves CAS-t vásároltak az RSA SecurID Prime elem(ek)re, akkor a problémákat/hibákat a szokásos RSA ügyfélszolgálati kapcsolattartási pontokon keresztül jelenthetik. Az RSA ügyfélszolgálaton belül, ha egy hiba megerősítést nyer, a probléma egy dedikált PS-csapathoz kerül, amely karbantartja és támogatja az RSA SecurID Prime szoftvert.

Szolgáltatási adatlap – AM Prime

RSA oktatás

RSA Tanulói bérlet előfizetési csomag



Indulj el az üzletközpontú biztonság felé vezető tanulási úton az új RSA oktatási előfizetési csomagjainkkal! Ezek az ajánlatok fejlett és rugalmas módot biztosítanak a tanulók számára a képzéshez, valamint a tanúsítási forrásokhoz való hozzáféréshez, amelyek szükségesek ahhoz, hogy a tanulók képesek legyenek a különböző RSA-termékek megfelelő használatára és kezelésére.

Mivel mindig igyekszünk új tartalmakat biztosítani, hogy lépést tartsunk termékeink új és fejlődő funkcióival, valamint a tanulóink igényeivel, előfizetéseink tartalmazni fogják a katalógusunkban „Hamarosan” jelzéssel ellátott tanfolyamokat, valamint minden olyan új képzési elemet, amely az aktív előfizetési időszak alatt jelenik meg.

Releváns szerep

Rendszergazda + Ügyfélszolgálat + Kivitelező

Előnyök:

- Egyetlen egyszerű tranzakció.
- Tanúsítványvócsereket tartalmaz.
- Nagyobb értéket ad, mint az egyénileg vásárolt tanfolyamok.
- A képzési költségvetések tervezése, a szervezetek általában tanulói bérleteket vásárolnak.
- Kiváló módja annak, hogy megszerezd a minősítési vizsgákra való felkészüléshez szükséges tudást.
- Ugyanazokat a gyakorlati laborokat tartalmazza (a laborkörnyezetek kurzusonként meghatározott időtartamra állnak rendelkezésre).

Az előfizetés tartalma

1 tanúsítványvócser

1 választható vizsgára

Self-paced Training

1 választható termékre
G&L vagy SecurID vagy ID Plus

Gyakorlati laborok

A laborkörnyezetek kurzusonként meghatározott időtartamra állnak rendelkezésre.

A képzésre hitelkártyával vagy megrendeléssel lehet előfizetni.

12 hónapig érvényes 1 megnevezett felhasználóra.

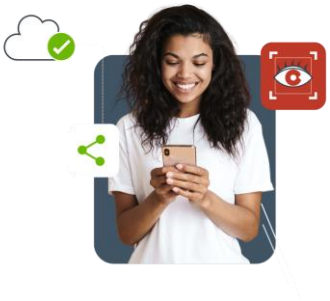
A tanulói bérletek névvel ellátott felhasználók alapján kerülnek kiadásra, nem oszthatóak meg több ember között, és aktiválás után nem ruházhatóak át másik felhasználóra.

Éves ár, megnevezett felhasználónként* *3000 USD*

Ha további segítségre van szükséged, lépj velünk kapcsolatba a következő e-mail címen education@rsa.com

RSA Tanulói bérlet előfizetési csomag

Indulj el az üzletközpontú biztonság felé vezető tanulási úton az új RSA oktatási előfizetési csomagjainkkal! Ezek az ajánlatok fejlett és rugalmas módot biztosítanak a tanulók számára a képzéshez, valamint a tanúsítási forrásokhoz való hozzáféréshez, amelyek szükségesek ahhoz, hogy a tanulók képesek legyenek a különböző RSA-termékek megfelelő használatára és kezelésére.



Mivel mindig igyekszünk új tartalmakat biztosítani, hogy lépést tartsunk termékeink új és fejlődő funkcióival, valamint a tanulóink igényeivel, előfizetéseink tartalmazni fogják a katalógusunkban „Hamarosan” jelzéssel ellátott tanfolyamokat, valamint minden olyan új képzési elemet, amely az aktív előfizetési időszak alatt jelenik meg.

Releváns szerep

Rendszergazda + Ügyfélszolgálat + Kivitelező

Előnyök:

- Egyetlen egyszerű tranzakció.
- Tanúsítványvócsereket tartalmaz.
- Nagyobb értéket ad, mint az egyénileg vásárolt tanfolyamok.
- A képzési költségvetések tervezése, a szervezetek általában tanulói bérleteket vásárolnak.
- Kiváló módja annak, hogy megszerezd a minősítési vizsgákra való felkészüléshez szükséges tudást.
- Ugyanazokat a gyakorlati laborokat tartalmazza (a laborkörnyezetek kurzusonként meghatározott időtartamra állnak rendelkezésre).

Az előfizetés tartalma:

3 tanúsítványvócser 1 választható vizsgára	***Hozzáférés az összes RSA oktatási termékhez*** Saját tempójú tréning	***Gyakorlati laborok*** A laborkörnyezetek kurzusonként meghatározott időtartamra állnak rendelkezésre	***Korlátlan hozzáférés nyilvános virtuális oktató által vezetett tréningekhez***

A képzésre hitelkártyával vagy megrendeléssel lehet előfizetni.

12 hónapig érvényes 1 megnevezett felhasználóra.

A tanulói bérletek névvel ellátott felhasználók alapján kerülnek kiadásra, nem oszthatóak meg több ember között, és aktiválás után nem ruházhatóak át másik felhasználóra.

Éves ár, megnevezett felhasználónként* *9000 USD*

Ha további segítségre van szükséged, lépj velünk kapcsolatba a következő e-mail címen education@rsa.com

RSA ügyféltámogatás

Az RSA több mint 230 főt foglalkoztató globális támogatási szervezete átfogó támogatási tervvel tudja bővíteni biztonsági megoldásodat, amely fontos biztonsági figyelmeztetéseket, értékes frissítéseket és szakértői tanácsadáshoz való hozzáférés biztosítását jelenti. Az RSA biztosítja a szükséges erőforrásokat a termékkel kapcsolatos problémák és kérdések gyors és proaktív megoldásához az üzletmenet folyamatosságának biztosítása érdekében.

Az RSA többszintű támogatási módszert alkalmaz, amely gyors problémamegoldást tesz lehetővé, és háromféle kapcsolatba lépési lehetőséget biztosít az RSA ügyféltámogatásához: **telefon, web és e-mail** Az RSA világszínvonalú ügyféltámogatása arra törekszik, hogy teljesítse vagy meghaladja az aktív támogatási szerződések feltételeit. Világszínvonalú telefonos támogatási szolgáltatásokat nyújtunk az RSA ügyfeleinek.

Súlyosság

Az eset súlyosságát akkor határozzuk meg, amikor az alapvető információkat bejegyezzük a híváskezelő rendszerbe. Minden esetet rangsorolunk az ügyfélre gyakorolt hatásuk szerint: Súlyosság 1 (S1) – Súlyosság 4 (S4), ahol az S1 a legfontosabb és legsürgősebb.

Kövesd a Napot stratégia

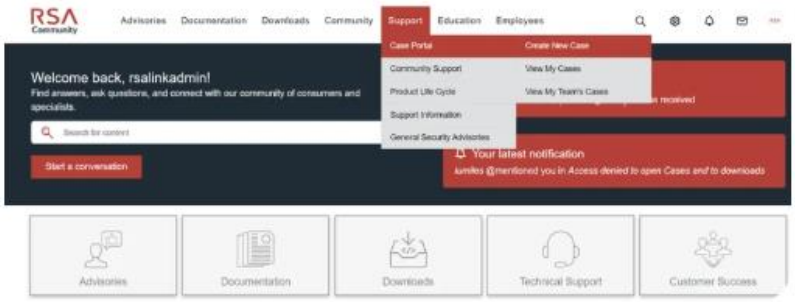
Az RSA a „kövesd a Napot” eljárást alkalmazza az ügyek ügyféltámogatási központok közötti átadására, így biztosítva, hogy az ügyön éjjel-nappal dolgozzunk.

Az ügyféltámogatási szolgáltatások szintje az ID Plus tervhez kapcsolódik. Operacionalizlja befektetését, és gyorsítsa fel a SecurID és az ID Plus értékteremtési idejét. Az erőforrások közé tartozik a világszínvonalú csapat 24 órás technikai támogatása, a személyre szabott támogatás és a peer-to-peer tudásmegosztás.

További információkért lásd: https://www.rsa.com/support/

Hogyan hozhatók létre ügyek

1. Menj az RSA közösséghez (RSA Community)
2. Jelentkezz be RSA közösségi (RSA Community) fiókoddal Vagy, Regisztrálj most (Register Now)
3. Vidd a kurzort a Támogatáshoz (Support)
4. Vidd a kurzort az Ügyportálra (Case Portal)



Technikai támogatás telefonszámai

Amerikai kontinens	Telefonszámok
Amerikai Egyesült Államok	+1-800-995-5095 +1-781-515-7700 +1-800-732-8743
Európa, Közel-Kelet és Afrika	
Egyesült Királyság	+448000668073
Franciaország	+33187212289
Németország	+498920194097

Ázsia csendes-óceáni térsége	
Ausztrália	+61238138723 +611800549838
Kína	+861053875939
India	0008000502408
Japán	+81 3-4520-3203
Szingapúr	+6531292638

„+" = IDD előtag kódja. Egyes országokban több IDD is van. Mindegyiket más-más távolsági fuvarozó használja.

Személyre szabott támogatás

Az RSA az alap, bővített és egyéni alkalmazástámogatási opciókkal személyre szabott, proaktív támogatást nyújt – beleértve egy éjjel-nappal elérhető globális támogatói csapatot –, amely lehetővé teszi, hogy a technikai problémákat még azelőtt kezeld, re mielőtt azok kihatással lennének az üzletedre. Azért vagyunk itt, hogy segítsünk maximalizálni a rendelkezésre állást és az üzemidőt, hogy a lehető

RSA közösség

A termékszakértőkből és ügyfelekből álló élénk online közösség készen áll arra, hogy gyors és pontos válaszokat adjon minden RSA-val kapcsolatos kérdésedre. A közösségi és támogatási portál, amely kiterjedt tudásbázist kínáló könyvtárral rendelkezik, egyablakos forrásként szolgál a termékinformációkhoz, beleértve a licenceket, a dokumentációt, a letöltéseket és a képzést.

Kijelölt támogató mérnök

Az összetett biztonsági kihívásokkal küzdő, magasabb szintű műszaki szolgáltatást és programtámogatást igénylő szervezetek számára az RSA lehetőséget kínál arra, hogy a karbantartási szerződést egy kijelölt támogató mérnök (DSE) szolgáltatásaival egészítsék ki. A DSE magas szintű technikai erőforrásként szakértői ügyféltámogatási esetkezelést és gyors problémamegoldást biztosít az üzleti célkitűzések eléréséhez szükséges termékstabilitás biztosítása érdekében.

RSA Link

Az RSA Link az RSA ügyféltámogatási portálja, ahol a felhasználók hozzáférhetnek a dokumentációhoz, letöltésekhez, tanácsokhoz, tudásbázis-cikkekhez és sok máshoz, miközben valós idejű vitákban is részt vehetnek más ügyfelekkel, partnerekkel és az RSA munkatársaival.

Az RSA Link célja, hogy egyablakos ügyintézést tegyen lehetővé, ahol mindent megkaphatsz, ami ahhoz szükséges, hogy a legtöbbet hozd ki az RSA termékcsomagokból. Az alábbiakban felvázolunk néhány funkciót, amelyek az RSA Linken keresztül érhetők el: https://community.rsa.com/

Közösség

Minden termékterület saját közösséggel is rendelkezik, ahol a felhasználók a termékkel kapcsolatos vitákat és kérdéseket vethetnek fel.

Dokumentáció és letöltések

Az RSA Linken a felhasználók megtalálhatják az RSA-termékeikhez kapcsolódó összes dokumentációt és letöltést. Minden termékdokumentáció nyilvánosan hozzáférhető, és még a Google, Yahoo és Bing keresőmotorok segítségével is megtalálható.

Tanácsok

Az összes termékbejelentés, valamint a műszaki és biztonsági tanácsok (korábbi nevén SCOL jegyzetek és tanácsok) megtalálhatók és megoszthatók az RSA Linken. A felhasználók könnyen megtalálhatják az őket érdeklő tanácsokat, és feliratkozhatnak, hogy e-mailes értesítéseket kapjanak az új tanácsok közzétételéről.

Tudásbázis

Az ismert problémákkal foglalkozó cikkek ezreit és termékismertetőket tartalmazó RSA Tudásbázist most már teljesen integráltuk az RSA Linkkel. A termékdokumentációhoz hasonlóan az összes tudásbázis-cikk nyilvánosan elérhető, regisztráció nélkül.

Esetkezelés

Az RSA Link használatával az ügyfelek zökkenőmentesen léphetnek át a közösség és a termékdokumentáció böngészésétől a nyitott támogatási ügyeik eléréséig. A My RSA felületen az ügyfelek megtekinthetik a meglévő támogatási ügyeket, új ügyeket nyithatnak, megtekinthetik és kezelhetik a meglévő termékeket és karbantartási szerződéseket (az úgynevezett jogosultságokat), valamint kezelhetik a csapatukat annak meghatározása érdekében, hogy ki férhet hozzá ugyanahhoz az információhoz.

Ügyfélelégedettség

Az RSA rendelkezik egy hivatalos Ügyfelek hangja (VoC) programmal, amelynek célja, hogy összegyűjtse az ügyfelek visszajelzéseit, és segítsen mérni termékeink és szolgáltatásaink minőségét. Az RSA VoC programja három elsődleges mechanizmus segítségével gyűjti az ügyfelek visszajelzéseit, hogy megértse elégedettségi szintjüket:

1:1 Interjúk: Részletes és fókuszált interjúk, amelyek célja, hogy mélyre merüljenek az ügyfelek termékeinkkel és szolgáltatásainkkal kapcsolatos tapasztalataiban.

Üzleti: Mechanizmus az ügyfél tapasztalatainak mérésére egy adott eseménnyel, például egy támogatási jeggyel, egy szolgáltatási megbízás teljesítésével vagy egy tréninggel kapcsolatban.

Kapcsolat: Éves felmérés, amelynek célja az RSA-val, valamint termékeivel és szolgáltatásaival kapcsolatos általános tapasztalatok felmérése.

- ✓ Az RSA VoC a következő mérőszámokat használja a teljesítmény mérésére:
- ✓ Net Promoter Score (NPS)
- ✓ Értékteremtési idő
- ✓ Ügyfélelégedettség (professzionális szolgáltatások, ügyféltámogatás, oktatási szolgáltatások)
- ✓ Ügyféltámogatási idő
- ✓ Termékekkel és szolgáltatásokkal kapcsolatos elégedettség
- ✓ Üzletkötés könnyűsége

RSA Identitás- és hozzáférésmenedzsment (IAM) közösség

Az RSA Link egy élénk, nyilvános online közösség, ahol az ügyfelek találkozhatnak, hogy többet tudjanak meg az RSA IAM termékekről, kérdéseket tegyenek fel, és megosszák a bevett gyakorlatokat a gondolatvezérekkel, szakértőkkel és társaikkal. Íme egy pillanatkép az RSA Linken történő eseményekről:

Blogok: Szerezz hozzáférést több mint 25 gondolatvezér bloggerhez és tartalomszakértőhöz!

Podcastok: Tanulj az IAM Podcast Radio-ban készült szakértői interjúkból a legfrissebb biztonsági témákról!

Vitafórumok: Tartsd a kapcsolatot az RSA biztonsági termékeket használó ügyfelekkel, hogy megvitassátok és kicseréljétek az RSA termékek használatával és konfigurálásával kapcsolatos bevett gyakorlataitokat!

Webináriumok: Regisztrálj a rendszeresen megrendezett termék-webináriumokra, amelyek során az ügyfelek és a mérnökök valós példákat és demókat mutatnak be a legújabb felhasználási módokkal kapcsolatban!

Események: Kérj értesítéseket, és regisztrálj ügyfélkonferenciákra és tanácsadó találkozókra, Birds of a Feather (BoFs) telefonkonferenciákra és egyéb IAM-eseményekre!

Videók: Nézd meg a korábbi RSA termékfórumokat és RSA felhasználói csoportok prezentációit, vitaindító előadásait és termékbemutatóit!

Ötletbörze: Nyújts be és beszélj meg termékfejlesztési kéréseket! Az ügyfelek tanácsadó testületeinek, felhasználói csoportjainak és az RSA identitásközösségen keresztül benyújtott javaslatokat a belső termékfejlesztési ütemterv részeként figyelembe vesszük. A fejlesztéseket a legnagyobb számú ügyfél számára jelentkező potenciális előnyök alapján rangsorolják, és ennek megfelelően építik be az ütemtervbe.

RSA partnerségek

Az üzletközpontú biztonság alapvetően megköveteli, hogy az RSA termékei és szolgáltatásai zökkenőmentesen működjenek együtt mindazokkal a technológiákkal, amelyekre ügyfeleink támaszkodnak. Az RSA tisztában van azzal, hogy az ügyfelek egymást kiegészítő biztonsági megoldásokból álló ökoszisztémára vágynak, amelyek együttműködnek egymással. Támogatott technológiai ökoszisztémánkat technológiai partnerségek révén fejlesztjük, beleértve saját RSA Ready programunkat is.

Ma a partnerek listája több mint **400+ vállalatot** és **1000+ megoldást** tartalmaz a kockázati és informatikai biztonság és technológia minden területéről.

Cég alapadatai

RSA Security LLC	
RSA irodák	https://www.rsa.com/en-us/contact-us
Weboldal	www.rsa.com
DBA	RSA Security LLC
RSA Vezetőség	https://www.rsa.com/en-us/company/leadership
Alapítás éve	1982.
A bejegyzés helye szerinti állam	Delaware
Szövetségi adószám (USA)	27-1496036
DUNS-szám	121-615-538
NATO Kereskedelmi és Kormányzati Cég Kód	5Z940
Elsődleges SIC-kód	3577
NAICS-kód	511210
RSA garanciális információk:	https://community.rsa.com/docs/DOC-40403
Vásárlói tájékoztató az RSA műszaki támogatásával kapcsolatban	https://community.rsa.com/docs/DOC-86656
RSA Link / közösség	https://community.rsa.com/
RSA támogatási információk	https://www.rsa.com/en-us/services/rsa-product-and-customer-support
RSA szabványos formátumú nyomtatványok:	https://www.rsa.com/en-us/standard-form-agreements