

RSA Agent ID

Agentic identitásbiztonsági platform a szigorúan szabályozott iparágak számára.

Az AI-t a sebességre és a cselekvésre tervezték. Ez az ígérete – és egyben a legnagyobb kockázata is. Ha ugyanis a sebesség és a cselekvés a cél, a biztonság könnyen háttérbe szorul. Súrlódás nélkül az agentek pénzt utalhatnak. Felügyelet nélkül nemzetbiztonsági rendszereket hívhatnak meg. Kontroll nélkül hozzáférhetnek a betegek egészségügyi adataihoz.

Vannak szervezetek, amelyek megengedhetik maguknak, hogy a sebességért feláldozzák a biztonságot. A pénzügyi rendszert, a kormányzatokat és a kritikus infrastruktúrát fenntartó intézmények viszont nem.

Az RSA Agent ID a szigorúan szabályozott iparágak identitásbiztonsági platformja az agentic AI korára. A megoldás felderíti, védi és szabályozza az agenteket nyilvános és privát felhőkben, on-premises és air-gapped környezetekben egyaránt, a szabályzatokat pedig az Ön saját határain belül telepített AI/MCP Gateway érvényesíti. Ön határozza meg, mely műveletek nem hajthatók végre hitelesített, elszámoltatható emberi jóváhagyás nélkül. Az RSA Agent ID pedig minden agent-műveletről, sessionról és hívásról biztosítja a felügyeletet és a szabályozói megfeleléshez szükséges bizonyítékokat.

Az RSA által kiszolgált, magas biztonsági követelményű szervezetek számára az AI védelmének elmulasztása nem pusztán kellemetlenség, hanem katasztrófa. Az agentek jelentette kockázatok egyszerűen túl súlyosak.

Az agentic AI biztonsági kockázatai

Beköszöntött az agentic AI korszaka: a szervezetek azért vetnek be AI agenteket, hogy produktívak maradjanak, lépést tartsanak versenytársaikkal és kiszolgálják a növekvő igényeket. Sokan azonban nem tudnak válaszolni három alapvető kérdésre:

01

Milyen agentek működnek a környezetében?

02

Ki felel az egyes agentekért?

03

Meg tudja őket bárki állítani?

Ennek ára: új kockázatok, nagyobb pénzügyi veszteségek és súlyos üzleti fennakadások.

Azok a szervezetek, amelyek nem tudják számba venni agentjeiket, már most jelentős pénzügyi és működési kockázatokkal néznek szembe. A shadow AI-hoz – vagyis a munkavállalók által felügyelet nélkül használt, nem jóváhagyott AI-eszközökhöz – köthető incidensek aránya 2025 és 2026 között több mint a duplájára, 20%-ról 43%-ra nőtt.

A shadow AI felderítése csak egyre nehezebb lesz: a Gartner szerint a szervezetek 69%-a gyanítja vagy bizonyítékkal rendelkezik arról, hogy munkavállalói tiltott AI-eszközöket használnak. A National Cybersecurity Alliance felmérése szerint a munkavállalók 43%-a „bevallotta, hogy munkáltatója tudta nélkül osztott meg érzékeny munkahelyi információkat AI-eszközökkel”. A probléma tovább nő, ahogy a szervezetek egyre több agentet vezetnek be. A Gartner előrejelzése szerint 2028-ra egy átlagos Global 500 vállalat 150 000 agentet fog futtatni, szemben a 2025-ös kevesebb mint 15-tel.

A shadow AI jelentős költségekkel járhat. A shadow AI-hoz köthető incidensek átlagosan 5,39 millió dollárba kerülnek, ami 400 000 dollárral több egy átlagos adatvédelmi incidens költségénél (4,99 millió dollár). Az ilyen incidensek közel felében (49%) adatvesztés vagy adatsérülés történt, 42%-ukban pedig a működés is fennakadt. Az esetek 21%-ában a szervezeteknek szabályozói bírságot is fizetniük kellett.

Ezek a bírságok egyre komolyabb gondot jelenthetnek. Az amerikai szövetségi ügynökségek csak 2024-ben 59 AI-szabályozást adtak ki, több mint kétszer annyit, mint egy évvel korábban. Világszerte ma már több mint 1900 AI-szabályzati keretrendszer, jogszabály, szabvány és irányító testület működik.



Ha a jelenlegi trendek folytatódnak, sok szervezet nem fog tudni megfelelni ezeknek a globális követelményeknek. A kormányzati szervezeteknek mindössze 6%-a nyilatkozott úgy, hogy megbízik belső AI-rendszereiben. Az IDC előrejelzése szerint 2030-ra a G1000 szervezetek akár 20%-a is perekké, bírságokkal és informatikai vezetők (CIO-k) elbocsátásával nézhet szembe az AI agentek hiányos governance-éből fakadó, nagy nyilvánosságot kapó fennakadások miatt. A Gartner szerint a szervezeteknek csupán 13%-a gondolja úgy, hogy megfelelő AI agent governance-szel rendelkezik.

Az agentek a működést is jelentősen megzavarhatják. Egy népszerű AI-alapú kódolóeszköz a hírek szerint törölt egy éles adatbázist, majd hamis rekordokat generált, hogy elfedje, mit tett. Egy támadó adattörölő kódot juttatott egy nagy felhőszolgáltató AI-asszisztensébe, és arra utasította, hogy törölje a kritikus felhőerőforrásokat. Ugyanennél a szolgáltatónál egy másik incidens során egy mérnöki szintű jogosultságokkal felruházott belső agent kb. 13 óráig leállást okozott, amikor törölt, majd újraépített egy éles környezetet.

Az AI agentek nem a jövő. Már itt vannak.

Aki nem tudja felderíteni, védeni és szabályozni agentjeit, költséges adatvédelmi incidenseknek, megfelelőségi bírságoknak és működési fennakadásoknak teszi ki szervezetét.

Az RSA Agent ID áttekintése

Az RSA Agent ID előnyei

Az RSA Agent ID a kormányzati, pénzügyi és magas biztonsági követelményű szervezetek AI agentjeit védi. Három önálló modulként vagy egyetlen összekapcsolt rendszerként is elérhető, és a teljes identitás-életcikluson át nyújt védelmet:

DISCOVER

Az **RSA Agent ID Discover** felderíti és nyilvántartásba veszi az ismert és ismeretlen agenteket és MCP-szervereket, és teljes értékű identitást ad nekik kijelölt tulajdonossal, kockázati besorolással és életciklus-állapottal – az Ön identitásszolgáltatójával összekapcsolva.

SECURE

Az **RSA Agent ID Secure** bárhol szabályozza, mit tehetnek az agentek. Minden hívásnál érvényesíti a szabályzatokat az AI/MCP Gateway-en – az RSA felhőjében vagy az Ön környezetében. A magas kockázatú műveleteket kijelölt emberi operátor hagyja jóvá, a kivont agentek hozzáférését pedig a Secure visszavonja.

GOVERN

Az **RSA Agent ID Govern** ugyanúgy tanúsítja és felülvizsgálja az agenteket, ahogyan Ön az embereket irányítja: folyamatos tanúsítással, kockázatalapú hozzáférés-felülvizsgálatokkal és az agentek életciklusának automatizálásával.

Lásson rá minden agentre,
bárhol is fut.

Állítsa meg a kijelölt magas kockázatú műveleteket
valós időben: végrehajtásuk előtt hitelesített emberi jóváhagyás szükséges.

Egyesítse a felderítési jeleket egyetlen kereshető nyilvántartásban, kijelölt, elszámoltatható tulajdonossal.

Készítsen manipulációt kimutató auditnaplót minden agentről, hozzáférési döntésről és Gateway-műveletről, tulajdonoshoz rendelve.

Telepítse önállóan vagy összekapcsolt csomagként – a Discover a konnektor oldalán fut, a meglévő agent-infrastruktúrát nem kell módosítani.

Érvényesítse a least privilege elvet az agentek teljes életciklusában; a kockázatos műveletekhez hitelesített emberi jóváhagyás kell.

A kiemelt biztonságú szervezetek identitásstandardja

Az RSA azoknak a szervezeteknek készült, amelyeknek a legtöbb a veszítenivalójuk.

Ügyfeleink több mint 40 éve üzemeltetik a világot működtető rendszereket: energiahálózatokat, fizetési rendszereket, orvostechnikai és védelmi eszközöket.

Ezek a szervezetek nem hibázhatnak – és az agentjeik sem. Az RSA Agent ID pontosan erre a valóságra készült: ugyanazt a fegyelmet és ugyanazokat a szabványokat alkalmazza a mai kockázatokra, mint IAM- és IGA-megoldásaink.

Az RSA Agent ID azoknak a magas biztonsági követelményű szervezeteknek készült, amelyek nem engedhetik meg maguknak, hogy hibázzanak az AI terén:



Szuverén kontroll

A szabályzatok érvényesítése, a jóváhagyások és a bizonyítékok előállítása az Ön privát felhőjében, on-premises vagy air-gapped környezetében telepített RSA Agent ID AI/MCP Gateway-en történik. A jövőbeli kiadásokban teljesen szuverén control plane érkezik helyi adminisztrációval, szabályzatokkal, emberi jóváhagyással, kulcsokkal és bizonyítékokkal.



Magas szintű kontroll a magas kockázatú műveletekhez

Végrehajtás előtt ellenőriz minden olyan agent tool callt, amely az RSA Agent ID AI/MCP Gateway-en halad át. A megoldás biztosítja, hogy a magas kockázatú műveleteket – például átutalásokat vagy minősített információkhoz való hozzáférést – hitelesített, elsámoltatható emberi operátor hagyja jóvá.



Szabályozói bizonyítékok tíz iparági keretrendszerhez

Minden agentet emberi tulajdonoshoz rendel, és folyamatos bizonyítékláncot biztosít tíz jelentős megfelelőségi keretrendszerhez.



Széles körű integrációs támogatás

Az RSA Agent ID már ma integrálható az RSA ID Plus, a Microsoft Entra ID, az Okta, az AWS IAM, a CrowdStrike, a Microsoft Defender és más megoldásokkal, további agentplatform-integrációk pedig tervben vannak.

Az RSA Agent ID felhasználási esetei

Az RSA Agent ID három önálló modulként vagy egyetlen összekapcsolt rendszerként is elérhető, és a teljes identitás-életcikluson át védi az AI agenteket:

01 Vállalati szintű rálátás az AI-kockázatokra, mielőtt azok irányítási problémává válnának.

02 Folyamatos jogosultság-érvényesítés agentek és non-human identity-k (NHI) számára.

03 Hívás- és paraméterszintű szabályzatok a kockázatos agent-műveletekhez, teljes, visszakövethető auditnaplóval.

04 A shadow AI felszámolása és a szabályozói bizonyítékok hozzárendelése tíz iparági keretrendszerhez.

Pénzügyi felhasználási esetek

Támogatás a vezető AI-megfelelőségi keretrendszerekhez: konfigurálható kontrollcímkezés és bizonyíték-hozzárendelés a NIST AI RMF 1.0, az ISO/IEC 42001, a Treasury FS AI RMF, a NYDFS Part 500 és a DORA szerint.

Adatszuverenitási kontrollok, amelyekkel a multinacionális intézmények országonként különíthetik el az agenteket, az általuk elért adatokat és az általuk végzett műveleteket.

Human-in-the-loop jóváhagyás átutalásokhoz, kifizetésekhez és számlahozzáféréshez.

Kormányzati felhasználási esetek

Támogatás a vezető kormányzati AI-megfelelőségi keretrendszerekhez, köztük az OMB M-25-21 és M-25-22 memorandumokhoz, valamint az éves AI-felhasználásieset-leltár (Annual AI Use Case Inventory) követelményéhez (2027-re tervezve).

Minden agent felderítése nyilvános felhőben, privát felhőben és on-premises kormányzati hálózatokban; az air-gapped hálózatok támogatása tervben van.

Human-in-the-loop jóváhagyás minden olyan művelethez, amely minősített információt vagy személyes adatot (PII) érint.

Agentek felderítése és tulajdonoshoz rendelése: RSA Agent ID Discover

Amit nem lát, azt nem tudja megvédeni.
Egyetlen kontrollálatlan agent is elég ahhoz, hogy egy pénzügyi szolgáltató, kormányzati vagy magas biztonsági követelményű szervezet elveszítse az irányítást.

Az RSA Agent ID Discover folyamatosan felderíti a környezetében működő – jóváhagyott vagy shadow – agenteket és MCP-szervereket, nyilvántartásba veszi őket, és emberi tulajdonosokat rendel hozzájuk.

\$5,39
millió

A shadow AI-t érintő biztonsági incidensek átlagos költsége. Ez 400 000 dollárral több egy átlagos adatvédelmi incidensénél.

A Discover előnyei

Egyetlen agent sem marad rejtve.

Több felderítési jel alapján azonosítja a jóváhagyott és a shadow AI-t.

Emberi tulajdonos. Emberi felelősség.

Minden agentet felelős emberi tulajdonoshoz és kezelt életciklushoz rendel.

Lényeges elemzések.

A folyamatos analitika megmutatja, hogyan változnak agentjei, és kiemeli a kockázatokat.

Agent-műveletek kontrollja ott, ahol Ön működik: RSA Agent ID Secure

A magas kockázatú műveletekhez magas szintű biztonságot nyújtó emberi jóváhagyás szükséges.

Érvényesítse a szabályzatokat minden hívásnál az AI/MCP Gateway-en, amelyet az RSA üzemeltet, vagy amely a saját környezetében fut. Követeljen meg magas szintű, out-of-band jóváhagyást a magas kockázatú műveletekhez az RSA Agent ID Secure segítségével.

150 000

Ennyi agentet fog futtatni egy átlagos Global Fortune 500 vállalat 2028-ra a Gartner előrejelzése szerint

A Secure előnyei

Minden agent-művelet kontrollja.

Valós időben hitelesíti, engedélyezi és ellenőrzi az RSA Agent ID AI/MCP Gateway-en áthaladó műveleteket és hívásokat.

Hívásonkénti jogosultságkezelés.

Minden hívást a szabályzat alapján engedélyez, és a munka befejeztével azonnal érvényteleníti az agent sessionjét.

Részletes, biztonságos emberi kontroll.

A magas kockázatú műveleteket emberek hagyják jóvá, így igazolható, ki, mit, mikor és miért tett.

Korlátozott agent-jogosultságok, folyamatos tanúsítás: RSA Agent ID Govern

A pénzügyi szolgáltatóknak, a kormányzati szervezeteknek és a szabályozott iparágaknak a környezetükben működő minden agenttel el kell tudniuk számolni, hogy bizonyítékot szolgáltatthassanak az auditoroknak.

Minimalizálja a jogosultságokat, tanúsítsa a hozzáféréseket, és rendelje hozzá az agentekkel kapcsolatos bizonyítékokat tíz iparági keretrendszerhez az RSA Agent ID Govern segítségével.

1900

Ma már több mint 1900 AI-szabályzati keretrendszer, jogszabály, szabvány és irányító testület működik – és még több várható.

A Govern előnyei

Irányítás az agent teljes élettartama alatt.

Kézben tartja az agent életciklusát a létrehozásától az eltávolításáig.

Folyamatos tanúsítás éves felülvizsgálatok helyett.

Folyamatosan újratanúsítja az agentek hozzáférését, így a jogosultságok nem maradnak meg a szükségesnél tovább.

Kockázatalapú hozzáférés-felülvizsgálatok.

Feltárja és megszünteti a hozzáférési kockázatokat, mielőtt egy auditor – vagy egy támadó – rájuk bukkanna.



Ismerjen minden agentet. Kontrolláljon minden műveletet.

Agentic biztonsági platform a szigorúan szabályozott iparágak számára

KÉRJEN TÖBB INFORMÁCIÓT AZ RSA AGENT ID-RŐL



rsa.com/products/agent-id

Az RSA-ról

Az RSA a kormányzati szerek, a pénzügyi szektor és a magas biztonsági követelményű szervezetek identitásstandardja. Az RSA biztosítja azokat az identitásintelligencia-, hitelesítési, hozzáférés-kezelési, irányítási és életciklus-kezelési képességeket, amelyek a fenyegetések megelőzéséhez, a biztonságos hozzáféréshez, a folyamatos működéshez és a megfelelőségi elvárások túlteljesítéséhez szükségesek. Több mint 9000 biztonságtudatos szervezet bízta az RSA-ra több mint 60 millió identitás kezelését on-premises, hibrid és multicloud környezetekben. További információkért látogasson el weboldalunkra, ahol kapcsolatba léphet értékesítési csapatunkkal, partnert kereshet, vagy többet tudhat meg az RSA-ról.

©2026 RSA Security USA LLC vagy leányvállalatai. Minden jog fenntartva. Az RSA és az RSA logó az RSA Security USA LLC vagy leányvállalatai bejegyzett védjegyei vagy védjegyei az Egyesült Államokban és más országokban. Minden egyéb védjegy a megfelelő tulajdonosok tulajdona. Az RSA a jelen dokumentumban szereplő információkat pontosnak tekinti. Az információk előzetes értesítés nélkül változhatnak. Megoldásismertető 9/26