LÖSUNGSÜBERSICHT

Die komplette passwortlose Lösung für Unternehmen

Passwortlos für jede Bedrohung. Jede Umgebung. Jeder Benutzer. Jedes Gerät.

Die Multi-Faktor-Authentifizierung (MFA) bietet Unternehmen wichtige Cybersicherheitsfunktionen. Doch herkömmliche MFA reicht nicht aus: Bedrohungsakteure umgehen MFA mit Social Engineering, Malware, Deepfakes und anderen neuen Bedrohungen. Darüber hinaus erfordern staatliche Auflagen, Vorschriften und Sicherheitsmodelle wie DORA, Executive Order 14028, NIS2, OMB M-22-09 und andere eine Phishing-resistente Authentifizierung. Neue Bedrohungen und neue Compliance-Anforderungen erfordern mehr als nur MFA. Sie erfordern eine passwortlose Authentifizierung.

Während viele Anbieter punktuelle passwortlose Lösungen unterstützen, die einzelne Benutzergruppen oder Anwendungsfälle abdecken, bietet RSA organisationsübergreifende passwortlose Funktionen im großen Maßstab – einschließlich QR-Codes, Biometrie, FIDO2-zertifizierter hardware- und softwarebasierter Authentifizierung für iOS und Android, Mobile Push und mehr – unabhängig von Umgebung oder Anwendungsfall.

Die passwortlosen Lösungen von RSA werden über RSA® ID Plus angeboten, der branchenweit sichersten Hybrid-Identitätsplattform. Sie erhöhen die Sicherheit, steigern die Effizienz, erfüllen Compliance-Anforderungen und senken die Kosten. Darüber hinaus ergänzt RSA diese breite Palette passwortloser Optionen mit einer umfassenden Sicherheitsplattform, die den Authentifizierungsprozess sichert, Bedrohungen in Echtzeit erkennt und Angriffe im Keim erstickt. **Testen Sie ID Plus jetzt.**

Erfahren Sie mehr über die passwortlose RSA-Lösung, die Betriebssysteme und Ökosysteme, in denen unsere Technologie eingesetzt werden kann, die Standards, auf denen unsere Technologie basiert, die Cybersicherheitsbedrohungen, vor denen RSA Passwordless schützt, und die Vorteile, die RSA Passwordless bietet.

Passwortlose Lösungen für moderne Cyberangriffe

RSA Passwordless ist so konzipiert, dass sie neuen Cyberangriffen standhält. RSA unterstützt Phishing-resistente, passwortlose Methoden, die vor Malware, Brute-Force-Angriffen, Betrug, Ausfällen und Umgehungen schützen und so verhindern, dass böswillige Akteure geistiges Eigentum stehlen und den Betrieb stören.
Lesen Sie weiter, um zu erfahren, wie die passwortlosen Lösungen von RSA gegen neue Cyberangriffe vorgehen:

Phishing-resistent

Phishing ist eine der häufigsten und kostspieligsten Cyberangriffe. Bei Phishing-Angriffen werden Nutzer dazu verleitet, Passwörter, Benutzernamen und andere Zugangsdaten preiszugeben. Laut dem Verizon Data Breach Investigations Report 2025 wurden im Jahr 2024 2,8 Millionen Passwörter öffentlich geleakt oder kompromittiert, und 54 % der Ransomware-Angriffe standen in direktem Zusammenhang mit Passwortlecks. Der IBM Cost of a Data Breach Report stellte fest, dass Phishing eine der häufigsten und teuersten Ursachen für Datenschutzverletzungen ist. Die Kosten betragen durchschnittlich 4,88 Millionen US-Dollar, und die Eindämmung dauert durchschnittlich 261 Tage.

Die passwortlose Authentifizierung von RSA macht Passwörter überflüssig, die Cyberkriminelle zu stehlen versuchen. Unsere Lösungen machen Passwörter und gemeinsame Geheimnisse in kritischen Phasen des Anmeldedatenlebenszyklus, einschließlich Onboarding und Kontowiederherstellung, überflüssig. In anderen Situationen, beispielsweise bei Cloud-Ausfällen, bietet RSA Always-On-Funktionen, die es Benutzern ermöglichen, sich über andere passwortlose Methoden zu verbinden.

Testen Sie ID Plus

RSA ID Plus unterstützt QR-Codes, FIDO-Passkeys, Biometrie und eine Vielzahl von Phishing-resistenten, passwortlosen Lösungen.

Starten Sie jetzt Ihre ID Plus-Testversion!

RSA bietet sowohl software- als auch hardwarebasierte passwortlose, Phishing-resistente Authentifizierung. Die RSA Authenticator App unterstützt Phishing-resistente, gerätegebundene Passwörter auf iOS- und Android-Geräten. Unternehmen können auch die RSA iShield Key 2-Serie und DS100 FIDO2-Sicherheitsschlüssel einsetzen, die über eine firmware-aktualisierbare, hardwarebasierte, phishing-resistente Authentifizierung verfügen.

Malware-resistent

4.000 %

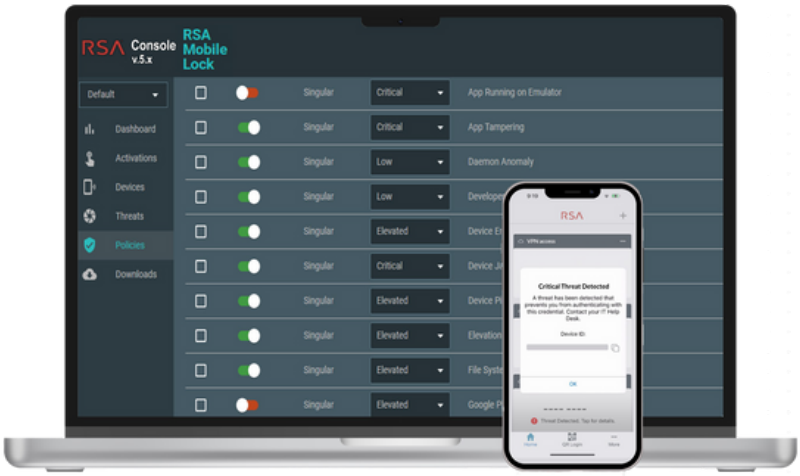
Zunahme des Wachstums von Malware-as-a-Service

Outseer 2024 Globaler Trendbericht zu Betrug und Schwindel

Malware ist Schadsoftware, die darauf ausgelegt ist, Systeme, Benutzer und Daten zu schädigen. Immer häufiger nutzen Bedrohungsakteure Malware-as-a-Service (MaaS). Cyberkriminelle können damit Schadsoftware und -infrastruktur abonnieren, um Ransomware und andere Angriffe zu starten. Laut Outseer ist MaaS um 4.000 % gewachsen. Das Unternehmen stellte außerdem fest, dass der Mobile-Banking-Verkehr mittlerweile 85 % der digitalen Banktransaktionen ausmacht, was Finanzdienstleistungen zu einem bevorzugten Ziel für Cyberkriminelle macht.

RSA Passwordless unterstützt Unternehmen auf vielfältige Weise bei der Abwehr von Malware. Erstens blockiert die Passwortlosigkeit viele Angriffsvektoren, die Cyberangreifer nutzen würden, um die Identität eines Benutzers zu missbrauchen und Malware zu installieren.

Zweitens können Unternehmen RSA® Mobile Lock einsetzen, um die mobile Authentifizierung auf verwalteten und BYOD-Geräten zu sichern. Die Lösung scannt nach Schadsoftware, Trojanern (eine Art von Schadsoftware, die als legitimes Programm getarnt ist) und anderen Schwachstellen, um zu verhindern, dass sich potenziell kompromittierte Geräte in einer sicheren Umgebung authentifizieren.



Administratoransicht der RSA Mobile Lock-Konsole

Benutzeransicht der auf dem Mobiltelefon erkannten Bedrohung

Brute-Force-resistent

Ähnlich wie bei Password Spraying, Credential Stuffing oder Rainbow Table-Angriffen werden bei Brute-Force-Angriffen Benutzerpasswörter durch Ausprobieren erraten. Angreifer können diese Angriffe automatisieren oder bei anderen Datenlecks gestohlene Anmeldeinformationen anpassen, um Brute-Force-Angriffe zu verfeinern.

RSA-Lösungen für passwortloses Login helfen Unternehmen, sich gegen diese Angriffe zu schützen, indem Passwörter vollständig eliminiert werden. RSA® Risk AI kann Unternehmen zudem dabei helfen, Password-Spraying-Angriffe in Echtzeit zu erkennen und zu stoppen, indem kontextbezogene Risikosignale wie der Benutzerstandort und die Häufigkeit fehlgeschlagener Anmeldeversuche ausgewertet werden. Sollte ein Benutzer zu oft versuchen sich anzumelden, kann Risk AI die verstärkte Authentifizierung automatisieren und das Sicherheitsteam bei ungewöhnlichem Verhalten benachrichtigen. Die Lösung automatisiert die verstärkte Authentifizierung nur, wenn das Benutzerverhalten die Risikotoleranz eines Unternehmens überschreitet; andernfalls beseitigt Risk AI unnötige Reibungspunkte.

Betrugssicher

Cyberkriminelle können verschiedene betrügerische Angriffe nutzen, um Nutzer zu täuschen. Beispielsweise handelt es sich bei MFA-Fatigue und Prompt-Bombing um Phishing-Angriffe, bei denen ein Angreifer Nutzern mehrere gefälschte MFA-Anfragen sendet. Versucht der Nutzer, die Anfrage abzuschließen, gibt er dem Angreifer entweder seine Anmeldeinformationen oder hilft ihm bei der Authentifizierung in einer sicheren Umgebung. Nutzer von Uber, Cisco, X/Twitter, Robinhood, Okta und Office 365-User wurden bereits Opfer solcher Angriffe.

Passwortlose Lösungen von RSA schützen Unternehmen vor Betrug. RSA unterstützt Code-Matching: Dabei werden Benutzer aufgefordert, einen an ein registriertes Gerät gesendeten Code abzugleichen, um sicherzustellen, dass sie den Authentifizierungsprozess in Cloud-, Hybrid-, lokalen und RADIUS-Umgebungen gestartet haben. RSA Risk AI erkennt außerdem, wenn ein Benutzer eine außergewöhnlich hohe Anzahl von Authentifizierungs-aufforderungen erhält, und weist das Sicherheitsteam darauf hin, Prompt Bombing zu untersuchen.

Die Folgen von Betrug

„Ähnlich wie das Klicken auf einen Link in einer Phishing-E-Mail oder auf einer Malware-Site kann die Genehmigung einer MFA-Benachrichtigung katastrophale Folgen haben. Sobald ein Hacker in das Netzwerk eindringt, versucht er in der Regel, sich dort zu bewegen und auf andere kritische Systeme zuzugreifen.“

„Vorsicht vor MFA-Ermüdungsangriffen“

Dave Taku
VP, Produktmanagement & UX RSA

Ausfallsicher

Unternehmen legen Wert darauf, dass ihre Benutzer sowohl sicher als auch produktiv sind. Deshalb setzen MFA-Anbieter oder ihre Kunden in manchen Fällen auf „Fail-Open“-Authentifizierungsverfahren, die es einem Benutzer ermöglichen, MFA zu umgehen, wenn er keine Internetverbindung herstellen kann. So können Bedrohungsakteure MFA effektiv deaktivieren, indem sie die Internetverbindung trennen. Dies war 2022 der Fall, als ein mit Russland in Verbindung stehender Cyberangreifer in eine NGO eindrang. Entscheiden sich Unternehmen für „Fail-Close“, können Bedrohungsakteure die MFA zwar nicht deaktivieren – allerdings könnte ein echter Cloud-Ausfall Benutzer daran hindern, sich anzumelden.

Tatsächlich haben echte Unfälle und technische Ausfälle ähnliche Auswirkungen wie Cyberangriffe. Wenn die Cloud nicht mehr erreichbar ist – wie es 2025 der Fall war, als in Spanien und Portugal zig Millionen Menschen ohne Strom waren oder als britische Banken aufgrund technischer Ausfälle 33 Betriebstage und Millionen an potenziellen Entschädigungszahlungen verloren –, werden Unternehmen, die einen stabilen und sicheren Zugang aufrechterhalten, erfolgreich sein, während andere Schwierigkeiten haben, eine Verbindung herzustellen.

Die passwortlosen Lösungen von RSA sind ausfallsicher. Wenn ein Benutzer keine Verbindung zum Internet herstellen kann, greift RSA ID Plus Hybrid Failover auf die lokale Authentifizierung zurück und ermöglicht Benutzern die Durchführung von MFA-Prozessen mit einem Einmalpasswort (OTP). Selbst wenn Benutzer im Flugmodus sind und keine Verbindung herstellen können, unterstützt RSA passwortlose Offline-Prozesse.

Bypass-resistent

Bei Social-Engineering-Angriffen wird versucht, Benutzer dazu zu verleiten, Anmeldeinformationen preiszugeben, neue Konten zu erstellen oder Sicherheitsmaßnahmen wie MFA zu deaktivieren. Zu diesen Umgehungsmethoden gehören Betrugsmaschen beim technischen Support, bei denen sich Angreifer als gesperrte Benutzer ausgeben und Mitarbeiter des IT-Helpdesks bitten, ihnen Zugriff zu gewähren oder MFA zu deaktivieren. ALPHV/BlackCat nutzte diese Technik bei einer Reihe von Ransomware-Angriffen, die Resorts in Las Vegas Hunderte Millionen Dollar kosteten. In jüngerer Zeit hatten es Angreifer auch auf IT-Mitarbeiter in Gesundheits- und öffentlichen Gesundheitsorganisationen abgesehen. Zu den weiteren Formen der Social-Engineering-Umgehung gehört die Kontoübernahme (Account Takeover, ATO), bei der ein Angreifer das Konto eines Benutzers übernimmt und es nutzt, um weitere Benutzer anzugreifen. Dabei gibt er sich manchmal als Führungskraft der Organisation aus.

Die passwortlosen Lösungen von RSA schützen vor diesen Angriffen. RSA Help Desk Live Verify bietet bidirektionale Verifizierungsfunktionen, die sicherstellen, dass weder Benutzer noch Helpdesk-Mitarbeiter von Angreifern getäuscht werden, die sich als das eine oder andere ausgeben: Stattdessen muss sich ein Benutzer beim Helpdesk-Anruf mit einer phishing-resistenten Authentifizierung identifizieren, um seine Identität in Echtzeit zu überprüfen, bevor Maßnahmen ergriffen werden. Die Lösung verwendet keine gemeinsamen Geheimnisse zur Identitätssicherung.

100 Millionen

geschätzte negative Auswirkungen des IT-Helpdesk-Angriffs im Oktober 2023

MGM Resorts International Form 8K

Passwortlose Lösungen für jede Bedrohung	
Phishing-resistent	✓
Malware-resistent	✓
Brute-Force-resistent	✓
Betrugssicher	✓
Ausfallsicher	✓
Bypass-resistent	✓

Sichere passwortlose Lösungen für jeden Anwendungsfall im Identitätslebenszyklus

Die Einführung passwortloser Systeme hat Bedrohungsakteure dazu veranlasst, ihre Taktiken weiterzuentwickeln. Cyberkriminelle nutzen mittlerweile Taktiken, die auch nach der Einführung passwortloser Systeme eingesetzt werden. Dazu gehören beispielsweise Betrugsversuche im technischen Support, die auf kritische Phasen im Identitätslebenszyklus abzielen, Social Engineering beim IT-Helpdesk oder der Einsatz von Malware-as-a-Service, Deepfakes, Betrug, Brute-Force-Angriffen und anderen Taktiken, um passwortlose Systeme vollständig zu umgehen und in Unternehmen einzudringen.

RSA schützt seine passwortlosen Lösungen über den gesamten Identitätslebenszyklus hinweg mit einer Reihe mehrschichtiger Sicherheitsfunktionen. Diese Funktionen helfen Unternehmen zudem dabei, die häufigsten passwortlosen Anwendungsfälle zu berücksichtigen und passwortlose Anmeldeinformationen effizient und skalierbar zu verwalten.

Sichere Registrierung

Mit RSA My Page können Unternehmen neue Benutzer schnell und sicher einbinden. RSA My Page bietet sichere Registrierung und Wiederherstellungs-Workflows per Self-Service-Single-Sign-On (SSO). Neue Benutzer können den Self-Service-Registrierungs-Workflow mit einem amtlichen Ausweisdokument abschließen. Die Organisation kann die native ID Plus-/ID-Verifizierungsintegration als zusätzliche Sicherheitsebene nutzen, um die Identität des Benutzers zu überprüfen und Betrugsversuche durch den Abgleich der Telefondaten der Benutzer mit den Daten der Kreditauskunftei zu erkennen. RSA My Page stellt außerdem sicher, dass neue Benutzer für alle SSO-Anfragen standardmäßig die passwortlose Authentifizierung verwenden.

Wenn Benutzer Anmeldeinformationen wiederherstellen müssen, bietet ID Plus über die ID-Verifizierungsintegration einen sicheren Self-Service-Wiederherstellungsworkflow.

Sichere Wiederherstellung

Betrugsmaschen im technischen Support, bei denen Angreifer Informationen aus sozialen Medien nutzen, um sich als Benutzer auszugeben und IT-Helpdesk-Mitarbeiter dazu zu bringen, die MFA zu deaktivieren oder neue Konten zu erstellen, stellen eine der beunruhigendsten Taktiken seit der Einführung von Passwörtern dar. Social-Engineering-Angriffe auf Helpdesks von Unternehmen haben allein im Jahr 2025 zu Verlusten in Höhe von 600 Millionen US-Dollar geführt. Betrugsmaschen im technischen Support bei Marks & Spencer, Co-Op und Christian Dior spiegeln die früheren, für Schlagzeilen sorgenden Angriffe auf den technischen Support bei MGM Resorts und der Caesars Entertainment Group wider.

RSA Help Desk Live Verify hilft Unternehmen, sich vor dieser Taktik zu schützen. Die Funktion bietet eine bidirektionale Helpdesk-Verifizierung, um sicherzustellen, dass Supportmitarbeiter nicht von Cyberkriminellen, die sich als Benutzer ausgeben, getäuscht werden und dass Benutzer nicht von Bedrohungsakteuren betrogen werden, die sich als IT-Mitarbeiter ausgeben. Anstatt Benutzer auf gemeinsame Geheimnisse oder OTPs zu verlassen, nutzt RSA Help Desk Live Verify eine Phishing-resistente Online-Verifizierung zur Validierung ihrer Identität. Die Funktion integriert außerdem eine dynamische Richtliniendurchsetzung in Echtzeit und nutzt kontextbezogene Risikosignale wie Benutzerstandort und Gerätesicherheitsstatus, um risikoreiche Zugriffsversuche mit RSA® Risk AI und RSA® Mobile Lock proaktiv zu blockieren.

Desktop- Anmeldung

RSA bietet eine Reihe von passwortlosen Anmeldefunktionen für die Desktop-Authentifizierung, darunter QR-Codes, mobile FIDO2/Passkeys und FIDO2-Hardware-Authentifikatoren für jede Plattform.

SaaS-Anmeldung

Benutzer können sich bei SaaS-Diensten mit der RSA Authenticator App authentifizieren, die an Mobilgeräte gebundene Passkeys, Push, Biometrie, Code-Matching, OTP und Hardware-Authentifikatoren wie die RSA iShield Key 2-Serie und den DS100 unterstützt.

Zugriffsanfragen

Da RSA eine sichere, passwortlose Registrierung ermöglicht, können Unternehmen passwortlose Zugriffsanfragen und Lebenszyklusmanagement über den gesamten Identitätslebenszyklus hinweg unterstützen. Benutzer können über RSA My Page auf ihre Apps zugreifen und Self-Service-Zugriffsanfragen abschließen.
Die Authentifizierung erfolgt über die RSA Authenticator App, die RSA-Hardwareauthentifizierung und andere Hardware-Authentifikatoren von Drittanbietern.

Offline-Zugriff

Im Jahr 2022 drang ein mit Russland in Verbindung stehender Cyberangreifer in eine NGO ein, indem er Schwachstellen im Identitätslebenszyklus der Organisation ausnutzte, ein neues Gerät registrierte und die MFA deaktivierte. Dies gelang ihm unter anderem, indem er ein Gerät vom Internet trennte: Dadurch schlug der Authentifizierungsprozess des Geräts fehl, was bedeutete, dass keine MFA zur Anmeldung erforderlich war. Die Angreifer deaktivierten MFA effektiv, indem sie das Internet abschalteten.

RSA ID Plus Hybrid Failover macht Unternehmen ausfallsicher und stärkt ihre Widerstandsfähigkeit: Bei Ausfällen oder wenn sich Benutzer im Flugmodus befinden, wird auf die lokale Authentifizierung umgeschaltet. Das bedeutet, dass sich Benutzer weiterhin ohne Kennwort anmelden können, auch wenn sie keine Verbindung herstellen können.

Passwortlose Lösungen für jeden Anwendungsfall	
Sichere Registrierung	✓
Sichere Wiederherstellung	✓
Desktop-Anmeldung	✓
SaaS-Anmeldung	✓
Zugriffsanfragen	✓
Offline-Zugriff	✓

Passwortlos für jede Umgebung und Plattform

Unternehmen setzen auf passwortloses Arbeiten, um die Sicherheit zu erhöhen und Kosten durch die Minimierung des IT-Helpdesk-Supports zu sparen. Mit passwortlosen Punktlösungen erreichen Unternehmen jedoch keine höhere Sicherheit und keine Kosteneinsparungen, da sie Lücken in der Abdeckung von Benutzergruppen, Umgebungen oder beidem hinterlassen.

RSA bietet eine umfassende passwortlose Lösung, die alle Benutzer in Cloud-, Hybrid- und lokalen Umgebungen abdeckt. So wird sichergestellt, dass überall dieselben passwortlosen Funktionen sicher bereitgestellt werden und die Effizienz des passwortlosen Arbeitens unabhängig von der IT-Infrastruktur erhalten bleibt.

Cloud-Umgebungen

RSA® ID Plus bietet die folgenden Funktionen zur passwortlosen Authentifizierung in der Cloud:

- Biometrie
- Apple Face ID / Touch ID
- Windows Hello
- OTP
- QR-Code
- SMS / Sprache
- Hardware-Token
- Code-Matching für RADIUS

Hybrid-Umgebungen

RSA® ID Plus ist die einzige echte hybride Zugriffsverwaltungsplattform. Die Lösung bietet eine einheitliche IAM-Plattform für alle Umgebungen und bietet die folgenden passwortlosen Funktionen für Hybridumgebungen:

- Biometrie
- Apple Face ID / Touch ID
- Windows Hello
- OTP
- QR-Code
- SMS / Sprache
- Hardware-Token
- Code-Matching für RADIUS

On-Premise

RSA® ID Plus bietet Zugriff und die folgenden passwortlosen Authentifizierungsfunktionen in lokalen Umgebungen:

- Biometrie
- Apple Face ID / Touch ID
- Windows Hello
- OTP
- QR-Code
- SMS / Sprache
- Hardware-Token
- Code-Matching für RADIUS
-

Mit RSA ID Plus Hybrid Failover können Unternehmen ihren Benutzern diese passwortlosen Methoden auch bei Internetausfällen oder anderen Störungen bereitstellen. Durch die Umstellung auf die lokale Authentifizierung können Unternehmen weiterhin die sichere passwortlose Authentifizierung nutzen, anstatt auf weniger sichere Methoden zurückzugreifen oder aus ihren Umgebungen ausgeschlossen zu werden.

RSA SecurID®-Lösungen schützen lokale Ressourcen mit Funktionen für sicheren Zugriff, Authentifizierung und Identitätsmanagement. SecurID bietet folgende kennwortlose Optionen vor Ort:

- Desktop-Anmeldung
- Hardware-Authentifikatoren
- Mobile Authentifikatoren
- Code-Matching für RADIUS

Passwortlose Lösungen für jede Umgebung	
Cloud	✓
Hybrid	✓
Vor Ort und in Rechenzentren	✓

Passwortlose Lösungen für jede Plattform

RSA unterstützt passwortloses Arbeiten in Windows-, Android-, iOS- und Linux-Umgebungen.

Passwortlose Integration von Microsoft

Für Unternehmen, die in Microsoft Entra-Umgebungen arbeiten, bietet RSA über die Integration von RSA External Authentication Methods (EAM) zusätzliche Funktionen zur passwortlosen Authentifizierung.

RSA EAM ermöglicht es Unternehmen, den Zugriff auf Microsoft-Ressourcen durch die Bereitstellung von Phishing-resistenten Authentifizierungsfunktionen von RSA zu schützen, darunter FIDO2-zertifizierte Authentifizierungsabläufe, Biometrie
und QR-Code-Authentifizierung.

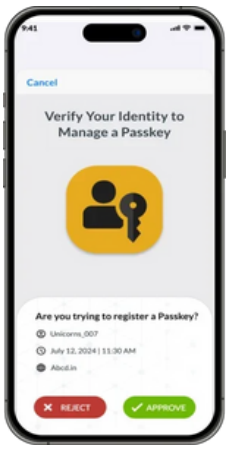
Passwortlose Lösungen für jede Plattform	
Windows	✓
MSFT-Server Jeder Windows-Endpoint (einschließlich AD-verbunden und Entra-verbunden)	✓ ✓
Android	✓
iOS	✓
Linux	✓

Passwortlose Lösungen für jede Benutzergruppe und jedes Gerät

Um passwortlose Authentifizierung effizient und skalierbar zu verwalten und sicher zu halten, müssen Unternehmen jede Benutzergruppe und jedes Gerät berücksichtigen. Das bedeutet, passwortlose Hardware- und Software-Authentifizierung bereitzustellen und sicherzustellen, dass Benutzer, die keine Internetverbindung herstellen können, die passwortlose Authentifizierung weiterhin nutzen können.

RSA berücksichtigt jeden Benutzer und jedes Gerät, indem es eine Reihe von passwortlosen Formfaktoren unterstützt:

Softwarebasiert, passwortlos



Registrieren eines Passkeys über die RSA Authenticator App

Die RSA Authenticator App bietet einen FIDO2-zertifizierten gerätegebundenen Passkey zur Verwendung auf iOS- und Android-Geräten.

Im Gegensatz zu synchronisierten Passkeys, die Anmeldeinformationen (und Schwachstellen) auf mehreren Geräten speichern, wird ein gerätegebundener Passkey auf einem einzigen Gerät gespeichert und verlässt dieses Gerät nie. Dadurch wird ein Höchstmaß an Kontrolle und Sicherheit gewährleistet.

Die Lösung kann Unternehmen dabei helfen, die Executive Order 14028, OMB M-22-09 und OMB M-24-14 zu erfüllen, die HIPAA-Anforderungen einzuhalten, die DORA-Empfehlungen zu erfüllen und die Anforderungen vieler anderer Länder hinsichtlich einer Phishing-resistenten Authentifizierung zu erfüllen.

Hardwarebasiert, passwortlos

RSA ist praktisch gleichbedeutend mit hardwarebasierter Authentifizierung. RSA unterstützt eine Reihe sicherer Hardware-Token für kritische und risikoreiche Szenarien wie Reinräume, Operationssäle und Sperrbereiche, in denen Telefone aufgrund von Vorschriften wie PCI und anderen nicht erlaubt sind, darunter:

RSA iShield Key 2-Serie

Die RSA iShield Key 2 Serie von Swissbit erfüllt höchste Cybersicherheitsstandards und die bundesstaatlichen Cybersicherheitsanforderungen. Als AAL3-Hardware-Authentifikator bietet die RSA iShield Key Serie:

- **Phishing-resistente Sicherheit:** Die RSA iShield Key 2-Serie nutzt FIDO2- und PIV-Authentifizierung, um den Diebstahl von Anmeldeinformationen und unbefugten Zugriff zu verhindern und so die Sicherheit Ihrer Systeme zu gewährleisten.
- **Smartcard-Funktionalität:** Die RSA iShield Key 2-Serie bietet sicheren, manipulationssicheren Speicher für digitale Zertifikate und Anmeldeinformationen.
- **Bundeskonformität:** Die RSA iShield Key 2-Serie basiert auf einem FIPS 140-3 Level 3-zertifizierten kryptografischen Modul (Zertifikat 4679) und ist FIDO2-zertifiziert. Damit erfüllt sie die strengsten bundesstaatlichen Cybersicherheitsanforderungen, darunter Executive Order 14028, OMB M-22-09 und M-24-14. RSA ID Plus for Government ist eine FedRAMP-autorisierte IAM-Lösung, die die 325 Sicherheits- und Datenschutzkontrollen basierend auf dem NIST 800-53-Framework erfüllt.
- **Flexible Nutzung:** Die RSA iShield Key 2-Serie integriert FIDO-Passkeys, PIV-Smartcard und OATH HOTP OTP über USB und NFC auf einem Gerät.

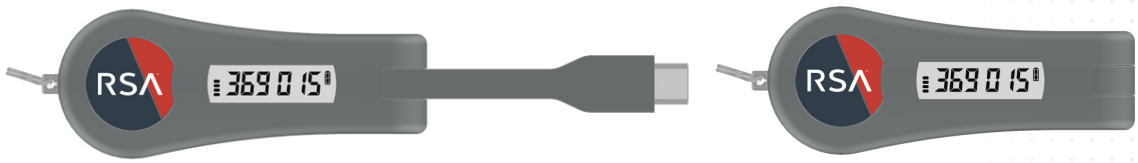
RSA iShield Key 2 USB-A- und USB-C-Authentifikatoren

- **Aktualisierbare Firmware:** Die vor Ort aktualisierbare Firmware trägt dazu bei, das Gerät zukunftssicher gegen neue Bedrohungen zu machen, den Wert und die Nutzung des Geräts zu steigern und die Geräteverwaltung zu erleichtern.
- **Handschuhfreundlicher Sensor**: Die RSA iShield Key 2-Serie sind die einzigen Sicherheitsschlüssel, die mit Plastikhandschuhen aktiviert werden können.

RSA DS100 Hardware-Authentifikator

Der RSA DS100 bietet multifunktionale, protokollübergreifende passwortlose Authentifizierung auf einem Gerät:

- **FIDO2-Authentifizierung:** Der FIDO2-zertifizierte DS100 ermöglicht sichere, komfortable FIDO2-Authentifizierung ohne Passwort in Umgebungen, in denen Hardware-Authentifikatoren bevorzugt oder sogar erforderlich sind. Der Anschluss erfolgt einfach über USB und bietet auch NFC-Funktionalität für die Zukunft.
- **OTP-Authentifizierung**: In sicheren Umgebungen, in denen USB-Konnektivität nicht möglich ist oder Benutzer eine VPN-Verbindung benötigen, bietet der DS100 die OTP-Anmeldefunktion für verbundene und getrennte Geräte. Das Gerät zeigt OTPs auf dem LCD-Display an und gibt sie per OTP-Taste automatisch in Ressourcen ein.
- **Verwaltung in der Cloud**: Obwohl der DS100 physisch bereitgestellt wird, erfolgt die Verwaltung in der Cloud mithilfe des RSA Cloud Authentication Service. Dies ermöglicht eine effizientere Verwaltung, ohne die Sicherheit eines voll funktionsfähigen Hardware-Authentifikators zu beeinträchtigen.
- **Aktualisierbare Firmware**: Benutzer können die vor Ort aktualisierbare Firmware aktualisieren, um das Gerät vor neuen Bedrohungen zu schützen.



RSA DS100 Hardware-Authentifikator

Offline ohne Passwort

RSA ID Plus unterstützt die Offline-Authentifizierung mit RSA ID Plus Hybrid Failover. Dadurch können Unternehmen ihren Benutzern auch bei Internetausfällen oder anderen Störungen passwortlose Methoden bereitstellen. Durch die Umstellung auf die lokale Authentifizierung können Unternehmen weiterhin sichere, passwortlose Methoden zur Authentifizierung nutzen, anstatt auf weniger sichere Methoden zurückzugreifen oder aus ihren Umgebungen ausgeschlossen zu werden.

Passwortlose Lösungen für jedes Gerät	
Software-Authentifikatoren	✓
Hardware-Authentifikatoren	✓
Offline-/Reinraum-Authentifizierung	✓

Überzeugen Sie sich, wie einfach es ist, noch heute sichere passwortlose Lösungen einzusetzen.

RSA ID Plus unterstützt die breiteste Palette an passwortlosen Lösungen, die alle durch umfassende Sicherheitsfunktionen zum Schutz vor Angriffen nach der Passwortabschaffung verstärkt sind.

Starten Sie noch heute Ihre kostenlose ID Plus-Testversion und erleben Sie umfassende, passwortlose Authentifizierungsfunktionen auf Unternehmensniveau.

Über RSA

RSA bietet unternehmenskritische Cybersicherheitslösungen zum Schutz sicherheitskritischer Organisationen weltweit. Die RSA Unified Identity Platform bietet echte passwortlose Identitätssicherheit, risikobasierten Zugriff, automatisierte Identitätsintelligenz und umfassende Identitätsverwaltung in Cloud-, Hybrid- und lokalen Umgebungen. Mehr als 9.000 Hochsicherheitsorganisationen vertrauen RSA bei der Verwaltung von über 60 Millionen Identitäten, der Erkennung von Bedrohungen, dem sicheren Zugriff und der Einhaltung von Compliance-Vorgaben. Weitere Informationen finden Sie auf unserer Website. Kontaktieren Sie unseren Vertrieb, finden Sie einen Partner oder erfahren Sie mehr über RSA.