SOLUTION BRIEF

The RSA Complete Enterprise-Grade Passwordless Solution

Passwordless for every threat. Every environment. Every user. Every device.

Multi-factor authentication (MFA) provides essential cybersecurity capabilities to organizations. But traditional MFA isn't enough: threat actors are bypassing MFA with social engineering, malware, deepfakes, and other emerging threats. Moreover, government mandates, regulations, and security models like DORA, executive order 14028, NIS2, OMB M-22-09, and more require phishing-resistant authentication. Emerging threats and new compliance mandates require more than just MFA. They require passwordless authentication.

While many vendors can support point passwordless solutions that cover individual user groups or use cases, RSA delivers organization-spanning passwordless capabilities at scale—including QR codes, biometrics, FIDO2-certified hardware- and software-based authentication for iOS and Android, mobile push, and more—regardless of environment or use case.

Offered through RSA® ID Plus, the industry's most secure hybrid identity security platform, RSA passwordless solutions enhance security, drive efficiency, fulfill compliance requirements, and reduce costs. Moreover, RSA fortifies this broad range of passwordless options with a deep security platform that secures the authentication process, detects threats in real time, and stop attacks before they start. Start your ID Plus trial today.

Learn more about the RSA passwordless solution, the operating systems and ecosystems that our technology can be deployed in, the standards that our technology is built on, the cybersecurity threats RSA passwordless defends against, and the benefits RSA passwordless provides.

Passwordless solutions designed for modern cyberattacks

The RSA passwordless solution is built to withstand emerging cyberattacks. RSA supports phishing-resistant passwordless methods that protect against malware, brute force attacks, fraud, outages, and bypasses, stopping bad actors from stealing intellectual property and disrupting operations.

Read on to learn how RSA passwordless solutions address emerging cyberattacks:

Phishing-resistant

Phishing is one of the most prevalent and costly cyberattacks. Phishing attacks trick users into revealing passwords, usernames, and other credentials. According to the 2025 Verizon Data Breach Investigations Report, 2.8 million passwords were leaked or compromised publicly in 2024, and 54% of ransomware was tied directly to password leaks. The IBM Cost of a Data Breach Report found that phishing was one of the most frequent and most expensive causes of data breaches, costing an average of $4.88 million and taking an average of 261 days to contain.

RSA passwordless authentication removes the passwords that cybercriminals try to phish. Our solutions eliminate the need for passwords and shared secrets in critical credential-lifecycle phases, including onboarding and account recovery. In other situations like cloud outages, RSA provides always-on capabilities that allow users to connect using other passwordless methods.

Try ID Plus

RSA ID Plus supports QR codes, FIDO passkeys, biometrics, and a variety of phishing-resistant, passwordless solutions.

Start your ID Plus trial now!

RSA provides both software- and hardware-based passwordless phishing-resistant authentication. RSA Authenticator App supports phishing-resistant device-bound passkeys on iOS and Android devices. Organizations can also deploy RSA iShield Key 2 series and DS100 FIDO2 security keys featuring firmware-upgradable, hardware-based phishing-resistant authentication.

Malware-resistant

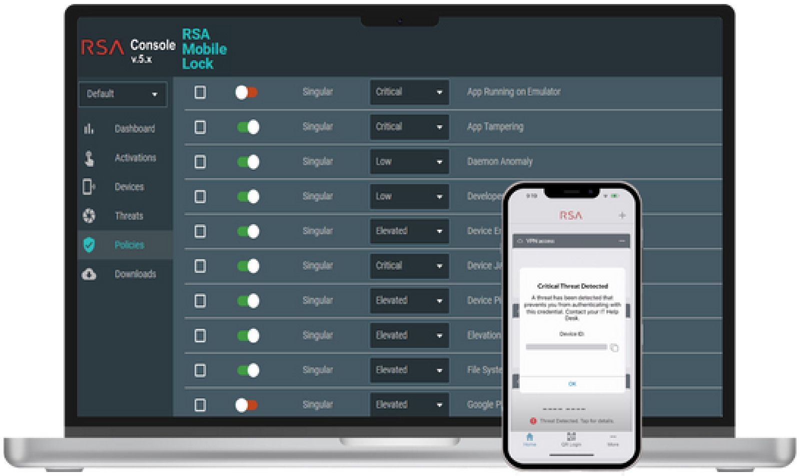
4,000%

increase in the growth of malware-as-a-service

Outseer 2024 Global Fraud and Scams Trend Report

Malware is malicious software designed to harm systems, users, and data. Increasingly, threat actors are turning to malware-as-a-service (MaaS), which allows cybercriminals to subscribe to malware software programs and infrastructure to launch ransomware and other attacks. MaaS has grown by 4,000%, per Outseer, which also found that mobile banking traffic now accounts for 85% of digital banking transactions, making financial services a prime target for cybercriminals.

RSA passwordless solutions help organizations defend against malware in a variety of ways. First, passwordless stops many of the threat vectors that cyberattackers would use to co-opt a user's identity and install malware. Second, organizations can deploy RSA® Mobile Lock to secure mobile authentication on managed and BYOD devices. The solution can scan for malware, trojan horses (a type of malware disguised as a legitimate program), and other vulnerabilities to prevent any potentially compromised devices from authenticating into a secure environment.



□	○	Singular	Critical	App Running on Emulator
□	●	Singular	Critical	App Tampering
□	●	Singular	Low	Daemon Anomaly
□	●	Singular	Low	Develope
□	●	Singular	Elevated	Device E
□	●	Singular	Critical	Device J
□	●	Singular	Elevated	Device P
□	●	Singular	Elevated	Elevation
□	●	Singular	Elevated	File Syste
□	○	Singular	Elevated	Google P

Critical Threat Detected

A threat has been detected that prevents you from authenticating with this credential. Contact your IT Help Desk.

Device ID:

Threat Detected. Tap for details.

Admin view of RSA Mobile Lock console

User view of threat detected on mobile phone

Brute force-resistant

Similar to password spraying, credential stuffing, or rainbow table attacks, brute force attacks use trial-and-error to guess users' passwords. Adversaries can automate these attacks, or adapt credentials stolen from other data breaches to refine brute force attacks.

RSA passwordless solutions help organizations defend against these attacks by eliminating passwords altogether. RSA® Risk AI can also help organizations recognize and stop password-spraying attacks in real-time by assessing contextual risk signals such as user location and the frequency of failed login attempts. Should a "user" try to log in too many times, Risk AI can automate step-up authentication and alert the security team when "users" are behaving out of the ordinary. The solution only automates step-up authentication when user behavior exceeds an organization's risk tolerance; otherwise, Risk AI removes unnecessary friction.

Fraud-resistant

Cybercriminals can use a number of fraud-based attacks to trick users. For instance, MFA fatigue and prompt bombing are phishing attacks in which an adversary sends users multiple fake MFA requests. When the user tries to complete the request, they either provide the attacker with their credentials or help them authenticate into a secure environment. Uber, Cisco, X / Twitter, Robinhood, Okta, and Office 365 users have been scammed by these types of attacks.

RSA passwordless solutions defend organizations against fraud. RSA can support code matching, in which users are asked to match a code sent to a registered device to ensure that they began the authentication process, in cloud, hybrid, on-premises, and RADIUS environments. RSA Risk AI can also detect if a user is receiving an extraordinary number of authentication prompts and flag the security team to investigate prompt bombing.

Outage-resistant

Organizations want their users to be both secure and productive. That's why, in some cases, MFA vendors or their customers will opt for "fail open" authentication processes, which allow a user to bypass MFA if they can't connect to the internet. This allows threat actors to effectively switch off MFA by disconnecting from the internet. Such was the case in 2022, when a Russian-linked cyberattacker breached an NGO. Should organizations choose to "fail close," then threat actors won't be able to deactivate MFA—but a genuine cloud outage could prevent users from logging in.

The consequences of fraud

"Much like clicking a link in a phishing email or malware site, approving an MFA notification can lead to catastrophic consequences. Once a hacker gets inside the network, they typically do their best to find ways to move around and access other critical systems."

"Beware MFA Fatigue Attacks"
Dave Taku
VP, Product Management & UX
RSA

In fact, genuine accidents and tech outages have similar effects to cyberattacks. When the cloud becomes unreachable—as was the case when tens of millions of people across Spain and Portugal lost power in 2025, or when tech outages cost UK banks the equivalent of 33 operating days and millions in potential compensation payments—organizations that maintain resilient and secure access will thrive while others struggle to connect.

RSA passwordless solutions are outage-resistant. If a user cannot connect to the internet, then RSA ID Plus Hybrid Failover falls back to on-premises authentication, allowing users to complete MFA processes using a one-time passcode (OTP). Even when users are in airplane mode and can't connect, RSA supports offline passwordless processes.

Bypass-resistant

Social engineering attacks attempt to trick users into providing credentials, creating new accounts, or deactivating security measures like MFA. These types of bypasses include technical support scams, in which adversaries pose as locked-out users and ask IT help desk personnel to provide them with access or deactivate MFA. ALPHV/BlackCat used this technique in a series of ransomware attacks that cost Las Vegas resorts hundreds of millions of dollars. More recently, threat actors were targeting IT staff at healthcare and public health organizations. Other types of social engineering bypasses include account takeover (ATO) in which a bad actor co-opts one user's account and uses it to target additional users, sometimes posing as someone in that organization's leadership.

RSA passwordless solutions defend against these attacks. RSA Help Desk Live Verify provides bi-directional verification capabilities that ensure that neither users nor help desk staff are tricked by threat actors posing as one or the other: instead, on calling the help desk, a user will have to authenticate using phishing-resistant authentication to validate user identities in real-time before taking any actions. The solution does not use shared secrets to assure identities.

$100 million

estimated negative impact from the October 2023 IT help desk attack

MGM Resorts International Form 8K

Passwordless solutions for every threat	
Phishing-resistant	✓
Malware-resistant	✓
Brute force-resistant	✓
Fraud-resistant	✓
Outage-resistant	✓
Bypass-resistant	✓

Secure passwordless solutions for every identity lifecycle use case

The adoption of passwordless has spurred threat actors to evolve their tactics. Cybercriminals are now using post-passwordless tactics like technical support scams that target critical stages in the identity lifecycle, socially engineer the IT help desk, or deploy malware-as-a-service, deepfakes, fraud, brute force attacks, and other tactics to bypass passwordless altogether and breach organizations.

RSA protects its passwordless solutions across the identity lifecycle with a range of layered security capabilities. These features also help organizations account for the most frequent passwordless use cases and manage passwordless credentials efficiently and at scale.

Secure enrollment

Organizations can onboard new users quickly and securely with RSA My Page, which provides secure enrollment and secure recovery workflows via self-service single sign-on (SSO). New users can complete a self-service enrollment workflow using government-issued identification. Their organization can use the native ID Plus / ID verification integration as an added layer of security to verify the user's identity and screen for fraud by checking users' phones against credit bureau data. RSA My Page can also ensure that new users default to passwordless authentication for all SSO requests.

Likewise, if users need to recover credentials, ID Plus provides a self-service secure recovery workflow via the ID verification integration.

Secure recovery

Technical support scams, in which threat actors use information available on social media to impersonate users and trick IT help desk personnel into deactivating MFA or creating new accounts, represent one of the most troubling post-passwordless tactics. Social engineering attacks on organizations' help desks have led to $600 million in losses in 2025 alone, with technical support scams on Marks & Spencer, Co-Op, and Christian Dior mirroring earlier headline-generating technical support attacks on MGM Resorts and Caesars Entertainment Group.

RSA Help Desk Live Verify helps organizations defend themselves from this tactic. The feature provides bi-directional help desk verification to ensure support personnel aren't tricked by cybercriminals claiming to be users and that users aren't scammed by threat actors impersonating IT staff. Rather than asking users to rely on shared secrets or OTP, RSA Help Desk Live Verify uses phishing-resistant online verification to validate their identities. The capability also integrates dynamic real-time policy enforcement, using contextual risk signals such as user location and device assurance posture to proactively block high-risk access attempts with RSA® Risk AI and RSA® Mobile Lock.

Desktop logon

RSA provides a range of passwordless logon capabilities for desktop authentication, including QR codes, mobile FIDO2/passkeys and FIDO2 hardware authenticator for any platform.

SaaS sign-on

Users can authenticate into SaaS services using the RSA Authenticator App, which supports mobile device-bound passkeys, push, biometrics, code matching, OTP, and with hardware authenticators like the RSA iShield Key 2 series and the DS100.

Access requests

Because RSA offers passwordless-based secure enrollment, organizations can support passwordless access requests and lifecycle management throughout the identity lifecycle. Users can access their apps and complete self-service access requests via RSA My Page. They can authenticate into the solution with the RSA Authenticator App, RSA hardware authentication, and other third-party hardware authenticators.

Offline access

In 2022, a Russian-linked cyberattacker breached an NGO by attacking vulnerabilities in the organization's identity lifecycle, enrolling a new device, and disabling MFA. They were able to do this in part by disconnecting a device from the internet: doing so caused the device's authentication process to "fail open," which means that it did not need MFA to log in. The attackers effectively disabled MFA by turning off the internet.

RSA ID Plus Hybrid Failover makes organizations outage-resistant and builds their resilience: during outages or if users are in airplane mode, the capability fails over to on-premises authentication, meaning that users can continue using passwordless to login, even if they can't connect.

Passwordless solutions for every use case

Secure enrollment	✓
Secure recovery	✓
Desktop logon	✓
SaaS sign-on	✓
Access requests	✓
Offline access	✓

Passwordless for every environment and platform

Organizations implement passwordless to enhance security and recoup costs by minimizing IT help desk support. But organizations will fail to realize enhanced security and cost savings with point passwordless solutions, which will leave coverage gaps in user groups, environments, or both. RSA provides one complete passwordless solution that can account for all users across cloud, hybrid, and on-premises environments, ensuring that the same passwordless capabilities are deployed securely everywhere, and that passwordless remains efficient no matter the IT infrastructure.

Cloud environments

RSA® ID Plus can provide the following passwordless authentication features capabilities in the cloud:

- Biometrics
- Apple Face ID / Touch ID
- Windows Hello
- OTP
- QR Code
- SMS / Voice
- Hardware tokens
- Code matching for RADIUS

Hybrid environments

RSA® ID Plus is the only true hybrid access management platform. The solution can provide one IAM platform across environments and deliver the following passwordless capabilities to hybrid environments:

- Biometrics
- Apple Face ID / Touch ID
- Windows Hello
- OTP
- QR Code
- SMS / Voice
- Hardware Tokens
- Code matching for RADIUS

On-premises

RSA® ID Plus can provide access and the following passwordless authentication capabilities in on-premises environments:

- Biometrics
- Apple Face ID / Touch ID
- Windows Hello
- OTP
- QR Code
- SMS / Voice
- Hardware Tokens
- Code matching for RADIUS

With RSA ID Plus Hybrid Failover, organizations can deliver these passwordless methods to users even during internet outages or other disruptions. By failing over to on-premises authentication, organizations can continue using secure passwordless to authenticate instead of defaulting to less secure means or being locked out of their environments.

RSA SecurID® solutions protect on-premises resources with secure access, authentication, and identity management capabilities. SecurID can deliver the following passwordless options on-premises:

- Desktop logon
- Hardware authenticators
- Mobile authenticators
- Code matching for RADIUS

Passwordless solutions for every environment	
Cloud	✓
Hybrid	✓
On-premises and data centers	✓

Passwordless solutions for every platform

RSA supports passwordless in Windows, Android, iOS, and Linux environments.

Microsoft passwordless integration

For organizations operating in Microsoft Entra environments, RSA can bring additional passwordless authentication capabilities via the [RSA External Authentication Methods (EAM) integration](). RSA EAM allows organizations to protect access to Microsoft resources by deploying phishing-resistant authentication capabilities from RSA, including FIDO2-certified authentication flows, biometrics, and QR Code authentication.

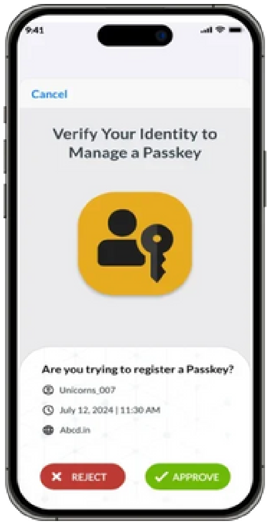
Passwordless solutions for every platform	
Windows	✓
MSFT servers	✓
Any Windows endpoint (including AD-connected and Entra-joined)	✓
Android	✓
iOS	✓
Linux	✓

Passwordless solutions for every user group and device

To manage passwordless efficiently at scale and to keep passwordless authentication secure, organizations must account for every user group and device. That means providing passwordless hardware authentication and software authentication, and ensuring that users who are unable to connect to the internet can still use passwordless authentication.

RSA accounts for every user and device by supporting a range of passwordless form factors:

Software-based passwordless



Verify Your Identity to Manage a Passkey

Are you trying to register a Passkey?

Unicorns_007

July 12, 2024 | 11:30 AM

Abcd.in

Registering a passkey via RSA Authenticator App

The RSA Authenticator App provides a FIDO2-certified device-bound passkey for use on iOS and Android devices.

Unlike synced passkeys, which store credentials (and vulnerabilities) across multiple devices, a device-bound passkey is stored on a single device and never leaves that device, ensuring the highest level of control and security.

The solution can help organizations meet Executive Order 14028, OMB M-22-09, and OMB M-24-14, comply with HIPAA requirements, meet DORA recommendations, and address many other countries' requirements for phishing-resistant authentication.

Hardware-based passwordless

RSA is almost synonymous with hardware-based authentication. RSA supports a range of secure hardware tokens for critical and high-risk scenarios like clean rooms, operating rooms, and restricted areas where phones are not allowed due to regulations like PCI and more, including:

RSA iShield Key 2 Series

The RSA iShield Key 2 Series, powered by Swissbit, is built to meet the highest cybersecurity standards and complies with federal cybersecurity requirements. An AAL3 hardware authenticator, the RSA iShield Key Series provides:

- **Phishing-resistant security**: The RSA iShield Key 2 series leverages FIDO2 and PIV authentication to prevent credential theft and unauthorized access, ensuring your systems remain secure.
- **Smart card functionality**: The RSA iShield Key 2 series provides secure, tamper-resistant storage for digital certificates and credentials.
- **Federal compliance**: The RSA iShield Key 2 series is based on a FIPS 140-3 level 3 certified cryptographic module (certificate 4679) and is FIDO2-certified, fulfilling the most stringent federal cybersecurity requirements, including Executive Order 14028, OMB M-22-09, and M-24-14. RSA ID Plus for Government is a FedRAMP-authorized IAM solution that satisfies the 325 security and privacy controls based on the NIST 800-53 framework.
- **Flexible usage**: The RSA iShield Key 2 series integrates FIDO passkeys, PIV smart card, and OATH HOTP OTP via both USB and NFC on one device.

RSA iShield Key 2 USB-A and USB-C authenticators

- **Upgradable firmware:** The field-upgradable firmware helps to future-proof the device against new threats, extends the device's value and usage, and facilitates device management.
- **Glove-friendly sensor:** The RSA iShield Key 2 series are the only security keys that can be activated with plastic gloves.

RSA DS100 Hardware Authenticator

The RSA DS100 provides multi-functional, multi-protocol passwordless authentication on one device:

- **FIDO2 authentication**: The FIDO2-certified DS100 brings secure, convenient FIDO2 passwordless authentication to environments where hardware authenticators are preferred or even required. It connects easily via USB plug and also includes NFC future functionality.
- **OTP authentication**: In secure environments where USB connectivity is not an option, or where users need to connect to a VPN, the DS100 provides connected and disconnected OTP login functionality. The device displays OTPs via LCD and push-button OTP that inputs them into resources automatically.
- **Managed in the cloud**: Even though the DS100 is physically deployed, it's managed in the cloud using the RSA Cloud Authentication Service. This makes it possible to increase management efficiency without compromising the security of a full-featured hardware authenticator.
- **Upgradable firmware**: Users may update the field-updatable firmware to keep the device secure from new threats.

RSA DS100
Hardware Authenticator

Offline passwordless

RSA ID Plus supports offline authentication with RSA ID Plus Hybrid Failover, which allows organizations to deliver passwordless methods to users even during internet outages or other disruptions. By failing over to on-premises authentication, organizations can continue using secure passwordless to authenticate instead of defaulting to less secure means or being locked out of their environments.

Passwordless soluitions for every device	
Software authenticators	✓
Hardware authenticators	✓
Offline / Clean Room authentication	✓

See how easy it is to deploy secure passwordless today

RSA ID Plus supports the broadest range of passwordless solutions, all fortified by deep security capabilities designed to protect against post-passwordless attacks.

Start your free ID Plus trial today to experience complete, enterprise-grade passwordless authentication capabilities.

About RSA

RSA provides mission-critical cybersecurity solutions that protect the world's most security-sensitive organizations. The RSA Unified Identity Platform provides true passwordless identity security, risk-based access, automated identity intelligence, and comprehensive identity governance across cloud, hybrid, and on-premises environments. More than 9,000 high-security organizations trust RSA to manage more than 60 million identities, detect threats, secure access, and enable compliance. For additional information, visit our website to contact sales, find a partner, or learn more about RSA.