



SOLUTION BRIEF

Identity Security for Agencies that Can't Afford Disruption

RSA ID Plus for government agencies

Governments are responsible for delivering critical services that citizens depend on every day. At the same time, they must defend against increasingly sophisticated cyberattacks while supporting employees, contractors, partners, and constituents across cloud, hybrid, and legacy environments.

Identity has become one of government's most critical vulnerabilities, with 65% of government organizations reporting an identity-related breach in the last three years. As agencies modernize infrastructure and advance Zero Trust initiatives, **RSA® ID Plus** helps reduce identity risk with phishing-resistant authentication, adaptive security, and identity verification across cloud, hybrid, legacy, and air-gapped environments.

From identity risk to operational resilience: How RSA ID Plus supports government agencies

Modernize authentication across government environments

Most agencies operate across a mix of cloud services, legacy systems, remote workers, contractors, and shared devices. Security solutions must work across all environments without disrupting operations or requiring agencies to replace existing infrastructure.

How RSA helps:

- Provides deployment flexibility across cloud, legacy, and air-gapped environments, including integration with existing identity investments such as **Microsoft Entra ID**
- Supports passkeys, FIDO, hardware, and mobile authenticators
- Provides deployment flexibility without requiring infrastructure replacement

Stop phishing and credential-based attacks

Passwords remain one of the most common attack vectors used by cybercriminals. Yet 57% of organizations still rely on passwords as their primary authentication method. As phishing campaigns continue to evolve, agencies need stronger methods of authenticating users without adding friction or complexity.

How RSA helps:

- RSA ID Plus delivers phishing-resistant and passwordless authentication
- **RSA® Risk AI** applies adaptive authentication based on user, device, and risk context
- Supports passkeys, FIDO authenticators, and hardware authenticators
- Extends strong authentication across cloud, hybrid, and on-premises environments

Keep authentication running during outages and disruptions

When identity systems go down, agency operations stop. A single point of failure in authentication infrastructure puts critical services at risk exactly when continuity matters most.

Built for government agencies

RSA has supported federal, state, and local government organizations for more than 40 years, helping secure critical systems, sensitive data, and mission-critical operations.

- Trusted by 90%+ of U.S. federal agencies and departments
- Deployed by 67 governments worldwide
- Supports NIST, FIPS, FedRAMP, and Zero Trust initiatives

Built for high-assurance organizations

Modern identity security must work everywhere: 79% of organizations depend on air-gapped environments, and 54% require private cloud infrastructure. RSA ID Plus delivers phishing-resistant authentication and identity assurance across the high-assurance environments where security cannot bend.

Deployment models



On-premises



Air-gapped / classified environments



Private cloud



Hybrid (cloud and on-premises)

Certifications

- FIPS 140-2
- FIPS 140-3
- FedRAMP
- FIDO2
- PIV/CAC
- ISO9001:2015
- CMMC 2.0

Key mandates addressed

- EO 14028 + CISA Zero Trust Architecture
- FISMA / NIST SP 800-53
- NIST SP 800-63B (AAL2 / AAL3)
- FedRAMP
- CJIS Security Policy
- CMMC 2.0

How RSA helps:

- Adaptive authentication with offline and fallback capabilities keeps access running during outages and disruptions
- Continuous authentication ensures agencies maintain access during outage scenarios
- Hybrid deployment reduces reliance on any single point of failure

Defend against help desk social engineering

Cybercriminals increasingly target help desks and service desks to bypass authentication controls through impersonation and social engineering. These attacks can undermine even strong authentication programs if agencies lack reliable methods for verifying user identities.

How RSA helps:

- **RSA ID Proofing** verifies identities during enrollment and credential recovery
- **RSA Help Desk Live Verify** supports high-risk identity verification workflows
- RSA Risk AI detects suspicious activity and allows admins to implement adaptive security controls
- **RSA® Mobile Lock** strengthens trust in mobile and BYOD devices

Extend passwordless to every environment—including legacy

Passwordless initiatives stall when they can't reach legacy systems, VPN, RADIUS, or field devices. Agencies need strong authentication that works everywhere, not just modern SaaS apps.

How RSA helps:

- Passwordless and phishing-resistant authentication extends across cloud, hybrid, on-premises, and legacy environments
- Supports passkeys, FIDO authenticators, hardware tokens, and mobile authenticators for diverse device populations
- Flexible deployment without requiring infrastructure replacement

Continuous authentication policy enforcement

Audit processes that rely on manual evidence gathering are slow, inconsistent, and difficult to scale across hybrid environments.

How RSA helps:

- Policy enforcement during authentication ensures consistency across every access event
- Continuous, audit-ready evidence reduces manual effort for compliance and reporting
- Consistent authentication posture across cloud, hybrid, and on-premises environments supports audit and regulatory requirements

To learn more about how RSA secures identity for government agencies worldwide, visit <https://www.rsa.com/solutions/government>.

About RSA

RSA is the identity standard for government agencies, finance, and high-assurance organizations. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, maintain operations, and surpass compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For additional information, visit our website to [contact sales](#), [find a partner](#), or [learn more](#) about RSA.

©2026 RSA Security USA LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security USA LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 7/26