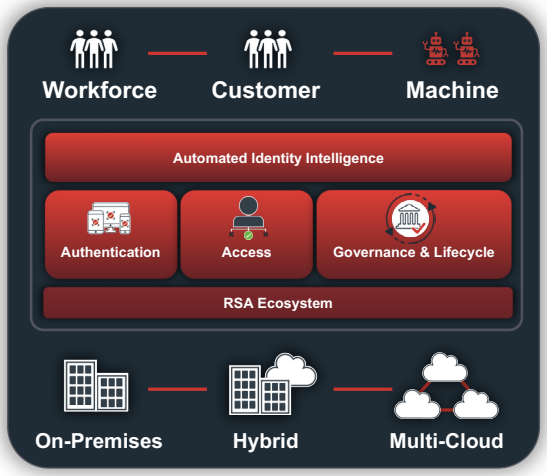
SOLUTION BRIEF

Secure, Compliant, and Resilient: The RSA Unified Identity Platform for State & Local Government

State and local agencies are responsible for delivering essential services, safeguarding sensitive data, and protecting critical infrastructure. Yet, they are under constant attack, with cybercriminals exploiting identity-based vulnerabilities to breach systems, steal data, and disrupt operations. According to the FBI's most recent IC3 report, government facilities were the third most-targeted critical infrastructure sector for ransomware attacks.[1] At the same time, agencies must navigate complex security mandates and aging IT systems, making identity security more challenging than ever.



The RSA Unified Identity Platform delivers a security-first approach to identity, combining authentication, access management, and governance to help public sector organizations strengthen security, enforce compliance, and improve operational efficiency, whether on-premises, in the cloud, or in hybrid environments.

From compliance to cyber resilience: how RSA supports government agencies

Prevent account takeovers and ransomware attacks

State and local governments are prime targets for cybercriminals who exploit stolen credentials and weak authentication to launch ransomware attacks and disrupt essential services. With 80% of breaches caused by stolen credentials, securing user identities is critical to preventing data theft, service outages, and financial losses. [2] The average cost for state and local governments to recover from a ransomware attack in 2024 was $2.83 million, more than double the cost in 2023.[3]

How RSA helps:

RSA® ID Plus delivers the identity and access management (IAM) security capabilities that state and local agencies need to prevent account takeovers, ransomware attacks, and other cyberattacks. The solution delivers:

- Phishing-resistant and passwordless authentication to stop credential-based attacks
- Adaptive access policies that block suspicious login attempts in real time
- Secure multi-factor authentication (MFA) that balances security and ease of access for public sector employees
- AI-driven risk analytics that detect and respond to anomalous access attempts before they become threats

Streamline identity lifecycle management

State and local governments rely on a mix of full-time employees, contractors, and public sector personnel across agencies, all of whom require secure and timely access to critical systems. Manual identity management can lead to delays, excessive permissions, and security risks, increasing the likelihood of insider threats and compliance violations.

How RSA helps:

RSA® Governance & Lifecycle provides the identity governance and administration (IGA) capabilities that state and local agencies need to facilitate and secure identity lifecycle management for all users and devices. The solution:

- Automates onboarding, offboarding, and access changes to ensure users have the right access at the right time
- Enforces role-based access controls (RBAC) to prevent privilege creep
- Eliminates manual approvals by streamlining identity requests with automated workflows
- Ensures immediate access removal when employees leave or change roles, reducing insider threats

Ensure compliance with government regulations

Government agencies must comply with strict security mandates such as CJIS, HIPAA, and IRS 1075, which require strong access controls, auditability, and identity governance. Non-compliance can result in the loss of federal funding, increased audit scrutiny, reputational damage, and potential legal consequences. Manual compliance processes are costly, prone to errors, and difficult to scale. Managing cybersecurity and other technology risks remains the top priority for 69% of US state government respondents.[4]

How RSA helps:

RSA ID Plus and RSA Governance & Lifecycle provides help state and local agencies maintain compliance with government mandates. The solutions:

- Automate access reviews and enforces least privilege policies to reduce compliance gaps
- Provide real-time audit trails that simplify reporting and audit readiness
- Enable encryption and secure authentication to meet data protection requirements
- Reduce the risk of compliance fines by proactively enforcing government security mandates

Secure hybrid and multi-cloud environments

Government IT environments are complex, often blending on-premises systems, private clouds, and SaaS applications. This fragmented infrastructure creates security blind spots and inconsistent access policies, making it easier for cybercriminals to exploit gaps in identity security. U.S. state and local government enterprise IT spending will reach nearly $125.4 billion by 2026, reinforcing the need for secure identity solutions that can scale with government IT investments.[5]

How RSA helps:

RSA ID Plus is the market's only IAM solution capable of securing all users across IT environments. The solution:

- Provides centralized identity and access management across on-prem, cloud, and hybrid environments
- Seamlessly integrates with legacy systems and modern cloud applications to ensure secure access everywhere
- Delivers flexible deployment options that meet the unique needs of state and local agencies
- Enhances visibility into access and authentication activity to detect threats before they escalate

A proven partner in government identity security

For over 40 years, RSA has helped state and local governments protect their most critical assets. As cyber threats grow more sophisticated and compliance requirements become more stringent, agencies must take proactive steps to secure identities, prevent attacks, and maintain operational resilience.

RSA delivers government-ready solutions designed to mitigate risk, simplify compliance, and provide resilient identity security so agencies can focus on their mission without compromise.

Visit RSA.com/solutions/public-sector/ for more information.

About RSA

The AI-powered RSA Unified Identity Platform protects the world's most secure organizations from today's and tomorrow's highest-risk cyberattacks. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable 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.

1. *2023 Federal Bureau of Investigation Internet Crime Report*
2. *2024 Verizon Data Breach Investigations Report*
3. *The State of Ransomware in State and Local Government, Sophos*
4. *2025 CIO Agenda: Top Priorities and Technology Plans for U.S. State Governments, Gartner*
5. *U.S. State and Local Government Overview: Kick-Starter for Technology Providers, Gartner*