RSA

CASE STUDY

Modernizing Identity at Scale: How a State Government Agency Reduced Help Desk Burden, Advanced Zero Trust, and Strengthened its Microsoft Environment with RSA

A long-standing RSA customer builds a FedRAMP-authorized, CJIS-aligned identity platform that complements Microsoft Entra Identity and secures over 145,000 users across a hybrid environment without disrupting a single existing workflow.

INDUSTRY

State Government IT Services

USERS

145,000+

RSA SOLUTIONS

- RSA ID Plus
- RSA ID Plus Prime
- RSA Help Desk Live Verify
- RSA Professional Services

Overview

A large state government information technology services agency manages identity and access for more than 145,000 users across dozens of state entities, including law enforcement agencies whose systems must meet stringent Criminal Justice Information Services (CJIS) security requirements.

As a long-standing RSA customer, the agency had trusted RSA SecurID and Authentication Manager to protect its on-premises environment for years. What it needed next was a path forward: a way to extend that trusted foundation into a cloud-first Microsoft environment, eliminate the help desk burden that had grown with its user base, and build the phishing-resistant, passwordless authentication posture its Zero Trust strategy required.

The agency found that path with RSA. Rather than replacing what it had, the agency modernized its capabilities, extending its existing RSA platform into the cloud with RSA ID Plus, adding self-service and lifecycle automation with RSA ID Plus Prime, and deploying RSA Help Desk Live Verify to close one of the most exploited vulnerabilities in any large organization: the help desk itself. The result is a FedRAMP-authorized, FIPS 140-3 ready, CJIS-aligned identity platform that works in concert with Microsoft Entra Identity, protecting cloud, hybrid, and on-premises resources from a single, unified console.

The opportunity

State government IT organizations operate at a scale that makes identity modernization both urgent and complex. This agency alone manages over 145,000 user identities spanning dozens of entities, each with different risk profiles, compliance obligations, and authentication needs. The Microsoft estate at the center of its infrastructure had grown significantly, with Microsoft 365 and Microsoft Entra Identity now handling access to cloud-based workloads across the enterprise. At the same time, on-premises systems, RADIUS-connected network access, legacy applications, and high-security environments that could not move to the cloud remained essential to daily operations.

Microsoft provides strong identity capabilities within its own ecosystem, but the areas where Entra is limited were also where this agency's risk was concentrated: hybrid and on-premises workloads, legacy applications requiring hardware token authentication, air-gapped or RADIUS-dependent environments, and high-assurance use cases with FIPS and CJIS compliance requirements. Closing those vulnerability gaps required a platform purpose-built to extend where Microsoft stops. RSA ID Plus, as a FedRAMP-authorized complement to Microsoft Entra, was that platform.

The challenge

The agency's existing identity infrastructure ran on an older iteration of an on-premises RSA authentication solution. That older solution supported approximately 109,000 software tokens and 36,000 hardware tokens. And while it had been reliable, it was no longer sufficient to meet the agency's growing needs. Several business-critical problems had emerged:

Help desk burden

Credential resets and onboarding requests were generating roughly 2,500 help desk calls per month. The self-service experience tied to the legacy solution offered limited customization and no path to reducing that volume. Worse, the help desk itself was a security liability: social engineering attacks that impersonate legitimate users to gain access through support channels were an unaddressed risk.

Zero Trust and phishing-resistant MFA

The agency's Zero Trust initiative required phishing-resistant authentication across all environments, not just cloud-native systems. Traditional OTP and password-based flows could not satisfy that requirement, and the agency needed to expand to push, biometrics, QR codes, FIDO2, and FIDO-certified hardware authenticators while keeping its existing token investment intact.

Compliance and certification

Law enforcement entities within the agency required CJIS-compliant authentication with centralized audit trails and real-time reporting. Federal alignment requirements pointed toward FedRAMP-authorized solutions. High-security use cases demanded FIPS 140-3 certified hardware authenticators.

Reporting and governance

Manual, spreadsheet-based reporting could not scale to meet audit and compliance demands across **145,000 users.** The agency needed real-time, automated visibility into authentication events, token lifecycle status, and user activity.

The modernization had to address all of these at once, and do so without forcing a rip-and-replace that would have disrupted a workforce of 145,000 users already familiar with RSA authentication.

Why RSA

RSA ID Plus is FedRAMP authorized and purpose-built for highly-complex hybrid environments. It integrates with Microsoft Entra Identity via SAML and OpenID Connect, extending consistent authentication policy across Microsoft 365, cloud-hosted applications, and on-premises systems, without replacing the Microsoft identity layer or requiring the agency to manage two separate consoles. Where Entra covers the Microsoft cloud, RSA covers everything else: RADIUS, legacy applications, air-gapped environments, and workloads that require higher assurance than cloud-native tools provide.

> *"The agency did not have to choose between protecting its Microsoft environment and preserving its investment in RSA. RSA ID Plus made both possible simultaneously."*

RSA also offered something no point solution could: a complete answer to the help desk problem. RSA Help Desk Live Verify (patent pending) provides bi-directional, passwordless identity assurance for help desk interactions, enabling help desk staff and users to verify each other's identities without PINs, shared secrets, or knowledge-based questions that can be researched or socially engineered. For an agency managing 145,000 users across dozens of entities, Help Desk Live Verify addressed a systemic vulnerability that no amount of MFA expansion alone would close.

For the agency's highest-assurance use cases, CJIS-covered environments, law enforcement systems, and roles requiring FIPS-certified hardware, RSA offered the RSA iShield Key 2 series: FIDO2-certified hardware authenticators with FIPS 140-3 Level 3 certification, supporting phishing-resistant, passwordless authentication that satisfies Executive Order 14028, OMB M-22-09, and M-24-14. No other vendor in the evaluation could provide that level of hardware assurance alongside the hybrid breadth RSA delivered.

The solution

The engagement was facilitated through **ThunderCat Technology** as the solution reseller and **Carahsoft Technology Corp** as distributor, both bringing deep public sector procurement experience to the program. RSA Professional Services provided a dedicated half-time resident consultant for twelve months, embedded in the agency's environment, responsible for design, implementation, and knowledge transfer throughout.

The deployment moved in two phases. In the first, RSA ID Plus was deployed in a hybrid cloud model, connecting the agency's legacy RSA authentication solution to the RSA cloud platform through embedded Identity Routers. Existing hardware and software tokens were carried forward without re-enrollment. Microsoft Active Directory and LDAP were integrated as identity sources. Authentication policies were extended to Microsoft Entra and Microsoft 365 via SAML and OIDC. The full range of modern authenticators, push, biometrics, QR codes, FIDO2, FIDO-certified hardware, was enabled alongside the legacy token estate. The agency deployed its first single sign-on (SSO) portal.

In the second phase, RSA ID Plus Prime was layered onto the platform. Prime's Self-Service Portal replaced the legacy Authentication Manager console, configured to mirror existing workflows so the transition required minimal retraining. The Help Desk Administration Portal gave support staff a dedicated interface, while RSA Help Desk Live Verify secured those interactions against social engineering. The Prime AMIS integration framework replaced manual reporting with automated, real-time API, workflow, and audit capabilities. Identity proofing via the Prime Identity Verification Portal as the frontend for Socure ID Proofing (the agency's existing ID Proofing solution) secured and streamlined new user onboarding and credential recovery workflows without requiring high-touch IT intervention with end users.

Results and business impact

The modernization delivered outcomes across three dimensions: security posture, operational efficiency, and compliance readiness.

2,500
help desk calls removed per month

145K
users transitioned with zero re-enrollment

FIPS 140-3
Level 3 certified hardware for high-assurance use cases

Security and compliance

- **Phishing-resistant MFA across the enterprise:** The agency moved from traditional OTP to a full suite of phishing-resistant authenticators, push, biometrics, QR codes, FIDO2, and FIPS 140-3 certified hardware, managed from a single console across cloud, hybrid, and on-premises environments. This satisfied Zero Trust mandates and addressed CJIS requirements for high-assurance authentication in law enforcement systems.
- **FedRAMP and FIPS alignment:** RSA ID Plus's FedRAMP authorization provided the federal compliance baseline the agency required. For highest-assurance use cases, the RSA iShield Key 2's FIPS 140-3 Level 3 certification satisfied requirements under EO 14028 and OMB M-22-09, with no equivalent available from Microsoft's native toolset.
- **Help desk social engineering risk eliminated:** RSA Help Desk Live Verify closed the help desk attack vector by replacing knowledge-based verification with bi-directional, passwordless identity assurance, ensuring neither users nor support staff can be socially engineered into a credential compromise.

Operational improvements

- **Help desk volume reduced:** The Prime Self-Service Portal enabled users to manage their own credentials, enroll authenticators, and complete onboarding without IT intervention. The agency expects to remove 2,500 help desk calls per month for identity-related requests.
- **Real-time reporting and audit readiness:** Automated reporting via the Prime AMIS framework replaced manual processes, giving compliance teams real-time visibility into authentication events, token lifecycle status, and user activity, critical for CJIS audit obligations across the agency's law enforcement entities.
- **Modernization without disruption:** The agency's 109,000 software tokens and 36,000 hardware tokens were preserved and carried forward. No re-enrollment was required across 145,000 users. The new self-service portal was configured to mirror existing workflows. End users experienced the transition as an improvement, not a disruption.
- **High availability at scale:** The hybrid high-availability architecture ensured resilience across all authentication paths, cloud, on-premises, and RADIUS, without adding infrastructure.

Microsoft environment strengthened

- **RSA as the security layer Entra needed:** RSA ID Plus extended authentication policy across Microsoft 365, Azure workloads, and on-premises systems through a single integration, adding the hybrid coverage, hardware assurance, and compliance depth that Microsoft Entra alone could not provide. The RSA/Microsoft Entra External Authentication Method (EAM) integration kept the existing Microsoft investment intact while raising the security bar across the combined environment.
- **Unified experience across both platforms:** The RSA My Page SSO portal gave users a consistent authentication interface whether their workload sat in Microsoft 365 or an on-premises system. Policies traveled with the user regardless of environment.

Looking ahead

The platform the agency now operates is designed to grow. The hybrid architecture can absorb new agencies, users, and use cases without re-architecture. FIDO2, identity proofing, and FIPS-certified hardware capabilities are in place to support passwordless mandates as they extend across state entities. The knowledge transfer embedded throughout the RSA Professional Services residency ensures the agency's own staff can operate and extend the platform independently.
For a state government organization that had trusted RSA for years and needed to modernize without starting over, the path forward ran directly through the partnership it already had, and through a Microsoft environment that is now meaningfully more secure because of it.

Solution partners

This engagement was delivered in partnership with ThunderCat Technology, a leading public sector technology reseller, and Carahsoft Technology Corp, one of the largest government IT distributors in the United States. ThunderCat and Carahsoft's experience navigating state and federal procurement channels helped bring this modernization program to contract efficiently, and their continued involvement in the RSA ecosystem supports ongoing public sector identity initiatives across the country.

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 solve the hardest security problems, under the most demanding conditions, where failure is not an option. For additional information, visit our website to **contact sales**, **find a partner,** or learn more about **RSA**.

carahsoft.

About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider, supporting Public Sector organizations across Federal, State and Local Government agencies and Education and Healthcare markets. As the Master Government Aggregator® for our vendor partners, we deliver **solutions** for Cybersecurity, MultiCloud, DevSecOps, Artificial Intelligence, Customer Experience and Engagement, Open Source and more. Working with resellers, systems integrators and consultants, our sales and marketing teams provide industry leading IT products, services and training through hundreds of contract vehicles. Visit us at **www.carahsoft.com**.

THUNDERCAT TECHNOLOGY

About ThunderCat Technology

Currently ranked #48 on the Solution Provider 500, the award winning ThunderCat Technology is a Service-Disabled Veteran-Owned Small Business (SDVOSB) that delivers technology products and services to government organizations, educational institutions, and commercial companies. Led by a combat-wounded CEO, ThunderCat is a systems integrator that brings an innovative approach to solving customer problems in and around the datacenter by providing strategies for Data Storage, Networking, Cyber Security, and Cloud Transformations. A proven leader, ThunderCat Technology provides and optimizes technologies from best of breed manufacturers. Clients include DOD, DHS, VA, Treasury, FBI, State of Virginia, State of NY, Sony, VISA, and CareFirst. **www.ThunderCattech.com**