RSA

DATA SHEET

SecurID for Public Sector

A hybrid approach to identity management and authentication

FedRAMP

Cloud authentication

FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies.

SecurID is a widely deployed intelligent multi-factor authentication (MFA) solution and the identity management platform the public sector trusts to empower employees, partners and contractors to do more—without compromising security or convenience.

Certified to comply

SecurID is certified to comply with FIPS 140-2 and other standards that are critical to public-sector technology selection. SecurID also conforms to VPAT accessibility requirements and other relevant specifications and standards.

RSA SecurID® authentication in the cloud

Long trusted by government for on-premises authentication, RSA is committed to supporting federal agencies, public sector organizations and approved federal contractors as they move to the cloud. Part of that commitment is the SecurID Federal solution, a cloud-based service with FedRAMP Authorized Moderate Impact Level 2 designation. Sponsored by the US Census Bureau and prioritized by FedRAMP JAB for P-ATO status, SecurID is available for US government agencies and Federal System Integrators to take their journey to the cloud.

FedRAMP Moderate has a baseline of 325 controls and is the standard for cloud computing security for controlled unclassified information (CUI) across federal government agencies. SecurID Federal cloud service delivers added security from the security controls (e.g. FIPS 140-2 validated crypto, system hardening, etc.) and is supported with US Citizen/US Soil personnel.

The gold standard in modern authentication

SecurID provides a reliable MFA solution for cloud and mobile applications such as Microsoft O365, as well as on-premises applications like virtual private networks (VPNs). With a broad range of authentication options, including hardware, embedded, software and mobile form factors, the solution enables a wide variety of use cases addressing agency-wide needs. SecurID is also the only true hybrid identity solution with no fail-open for MacOS and Microsoft Windows machines, for a seamless and secure experience online and offline.

Dynamically secure, risk-based identity assurance

For added security and improved usability, SecurID uses machine-learning behavioral analytics, business context and threat intelligence to draw a comprehensive picture of the user and create real-time risk scoring associated with their access. SecurID provides easy-to-implement role and attribute-based access authentication policies and conditional policies (e.g., network, country of origin, geo-fencing, known device, etc.), and allows for the customization of more complex, hybrid policies by combining multiple attributes. The risk dashboard and tools provide insights into risk-engine tuning to assist with planning and troubleshooting.

OWN YOUR IDENTITY.

Unified, core components

- **Cloud Authentication Service (CAS)**—A SaaS platform providing single sign-on (SSO) and MFA for SaaS, web and mobile applications.
- **Authentication Manager (AM)**—AM secures access to on-premises, cloud and web-based applications, verifies authentication requests, and centrally administers policies, users, agents and resources across physical sites.
- **Authentication Methods**—A broad set of authentication options including award-winning hardware tokens, push to approve, OTP, biometrics, FIDO, SMS and more. Supported by risk-based authentication, the solution uses machine-learning behavioral analytics for best-in-class identity assurance.
- **Agents and APIs**—Connectors and standard agents for SAML and RADIUS-based applications, as well as for IIS/ Apache, Windows, Unix/ Linux and ADFS. In addition, a REST-based API is available to enable MFA for custom applications.

World-class credential management made easy

More than ever, securing the entire credential lifecycle and supporting the unique needs of diverse groups—remote workers, on-site employees, third parties and administrators—is critical. With SecurID, weak points in areas such as onboarding, emergency access and credential recovery can be eliminated. To support multiple identity assurance levels and regulatory requirements, SecurID enables both administrator-led and self-service credential management and provides full customization and application programming interface (API) capabilities for integration into existing back-office systems, processes and workflows.

Frictionless, ground-to-cloud

Strengthened by over 500 certified integrations, SecurID has the most robust support for mission-critical on-premises/legacy platforms, applications and infrastructure, with thousands more supported through open standards. This eliminates the need for multiple identity management solutions, and ensures a seamless user experience, from the desktop to the data center to the cloud.

Highest availability and security with hybrid approach

With today's complexities, agencies need an easy, secure and cost-effective way to pull it all together—a hybrid approach to managing authentication and identity risks. SecurID instills confidence with its highly available, secure, scalable and convenient hybrid platform with cloud, on-premises, virtualized and hybrid-cloud options for the most security-sensitive use cases. SecurID uniquely provides the highest level of software-as-a-service (SaaS) availability with its on-premises failover feature.

About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to RSA.com.

RSA