

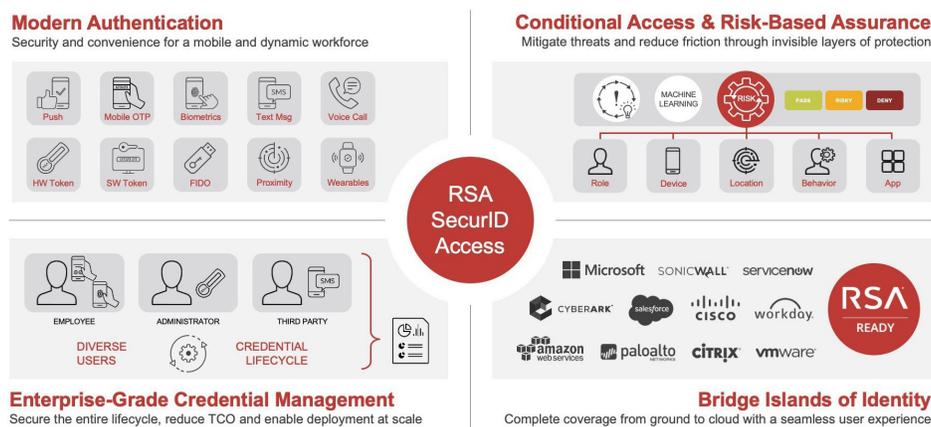
RSA SecurID® Access

A hybrid approach to authentication and identity management

RSA SecurID® Access is the world’s most widely deployed intelligent multi-factor authentication (MFA) solution and the identity management platform businesses trust to empower employees, partners and contractors to do more—without compromising security or convenience.

As organizations turn on a growing number of cloud and mobile applications, their attack surfaces increase, as does the probability that a single compromised identity can lead to a catastrophic data breach. With most attacks relying on compromised identities somewhere in the chain, identity has become the most consequential threat vector.

Now more than ever, organizations need a high level of assurance that users are who they say they are. But to be effective, and to ensure their businesses stay agile, they also need a secure access solution that won’t slow users down, but instead provide them with a common and convenient experience to any application, from any device.



The gold standard in modern authentication

RSA SecurID Access provides the most reliable MFA solution for cloud and mobile applications, including Microsoft 365, Salesforce and Workday, 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 organizational needs. And, RSA SecurID Access is the only 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, RSA SecurID Access 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. RSA SecurID Access 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.

Enterprise-grade 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 RSA SecurID Access, weak points such as onboarding, emergency access and credential recovery can be eliminated.

To support multiple identity assurance levels and regulatory requirements, RSA SecurID Access 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 RSA Ready certified integrations, RSA SecurID Access 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 business complexities, organizations need an easy, secure and cost-effective way to pull it all together—a hybrid approach to managing authentication and identity risks. RSA SecurID Access instills confidence with its highly available, secure, scalable and convenient hybrid platform with on-premises, virtualized, cloud and hybrid-cloud options for the most security-sensitive organizations. And, RSA uniquely provides the highest level of software-as-a-service (SaaS) availability with its on-premises failover feature.

Unified, core components

- **Authentication Methods.** In addition to award winning hardware tokens, RSA SecurID Access offers a broad set of authentication options including 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.
- **RSA Cloud Authentication Service (CAS).** CAS is a SaaS platform that provides single sign-on (SSO) and MFA for SaaS, web and mobile applications. CAS also accepts authentication requests from third-party SSO solutions or cloud applications configured to use RSA SecurID Access as the identity provider for authentication.
- **RSA Authentication Manager (AM).** AM verifies authentication requests, and centrally administers policies, users, agents and resources across physical sites. It helps secure access to on-premises, cloud and web-based applications.
- **RSA Agents and APIs.** RSA provides 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.

Trust RSA to help you do more—reduce identity risks, improve user productivity and improve TCO—with the ubiquitous, frictionless and dynamically secure capabilities of RSA SecurID Access.

About RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.

