

RSA®



SOLUTION BRIEF

RSA SECURID® ACCESS

MODERN AUTHENTICATION FOR
TODAY'S IDENTITY CHALLENGES



TRANSFORMING SECURE ACCESS

RSA SecurID® Access, the world's most widely deployed multi-factor authentication solution, delivers a comprehensive set of modern capabilities so you can protect what matters most. You need authentication that's:

Convenient for end users and easy for IT to deploy and maintain

Intelligent and uses real-time context to challenge to the level of risk

Pervasive and can be deployed everywhere

That's RSA SecurID Access.

IDENTITY IS YOUR WEAKEST LINK

As organizations turn on a growing number of on-premises, 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 that organizations are facing today.

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.

SETTING THE STANDARD FOR MODERN AUTHENTICATION

WE WORK HARD SO YOU DON'T HAVE TO

Most midsize to large organizations have hundreds of applications deployed and in use. It's not just the number that poses a challenge, but the fact that they have a mix of on-premises, cloud and mobile apps—all of which need protected access.



RSA SecurID Access provides the most reliable multi-factor authentication (MFA) solution for on-premises applications like virtual private networks (VPNs) and for cloud and mobile applications, including Office 365, Salesforce and Workday.

For over twenty years, RSA's dedicated partner engineering team has been working hand-in-hand with leading technology vendors to test, certify and support all of our application integrations, to ensure that your security works flawlessly out of the box, and keeps working smoothly even after application providers patch and update their code.

Whether you're new to MFA or have been using it for years, RSA SecurID Access provides a single, strong authentication platform that covers you from ground (desktops) to the cloud.

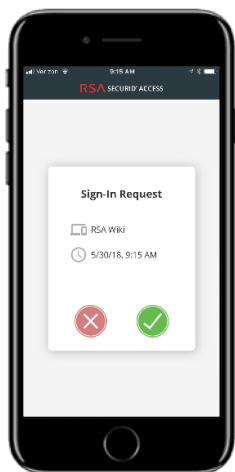
SECURE AND CONVENIENT AUTHENTICATION METHODS

While employees will always be a main concern, organizations have a growing need to provide third parties access.

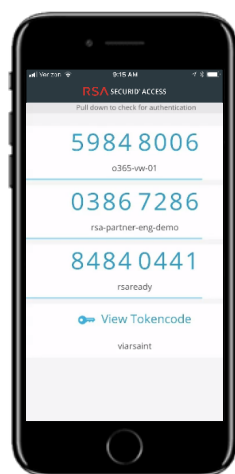
Contractors, partners and customers all need access, for a variety of reasons and use scenarios—and all with different preferences and requirements.



Users need easy and convenient access, while you need the confidence of knowing they are who they say they are. With RSA SecurID Access, you don't have to trade convenience for security. In addition to our award-winning tokens,



PUSH-TO-APPROVE



MOBILE OTP

RSA offers a broad set of authentication options that work directly on users' mobile phones—including push to approve, biometrics, SMS and more—ensuring you have the “right size” authentication for each user and every use case.

Whether you need the “air gap” security hardware tokens uniquely provide or the low touch capabilities of SMS, RSA SecurID Access delivers a solution that's easy for users to use, and for you to deploy, while giving you peace of mind that your most sensitive assets are protected.

GOING BEYOND MULTI-FACTOR

For added security and improved usability, RSA has taken authentication beyond simply two or three factors. RSA SecurID Access uses machine learning behavioral analytics, business context and threat intelligence to draw a comprehensive picture of the user and the risks associated with their access.



Analyzing contextual attributes related to when and where an access request comes from, the security posture of a device, the user's role and sensitivity of the application, and whether they've been associated with known fraud or exposed to known threats, provides a 360-degree view of the risk associated with user access.

RSA SecurID Access automatically, and without requiring any intervention, calculates an identity confidence score (Low or High) for each user, based on a variety of data points. By doing this in real time, organizations can automatically challenge users based on the level of risk—ensuring that high risk is met with high security, while low-risk cases are afforded the convenience of not being asked for any additional authentication.

SIMPLIFYING AUTHENTICATION REQUIREMENTS

With a large number of applications to support, and an increasing variety of ways to verify users and measure access risk, organizations need an easy way to pull it all together—a simple way to define their authentication requirements.



Since different use cases require different levels of authentication, RSA SecurID Access provides organizations an easy way to configure authentication options based on the user, application, context and risk information it collects.

RSA SecurID Access Assurance Levels enable organizations to simply group their use-case requirements into three levels—Low, Medium and High assurance. Each level corresponds to the relative strength of security organizations require for a particular application or use scenario. Low-risk scenarios need low levels of assurance (verification), while those of the higher-risk variety may require different, more secure types of access controls.



RSA SECURID ACCESS CORE COMPONENTS



Authentication Methods: In addition to our award-winning tokens, RSA SecurID Access offers a broad set of phone-based authentication options including push to approve, OTP, biometrics, SMS and more. Further, RSA SecurID Access also offers risk-based or adaptive authentication, which uses machine learning behavioral analytics to determine a real-time confidence score for each user.

RSA Cloud Authentication Service is a Software-as-a-Service (SaaS) access and authentication platform that provides single sign-on (SSO) and multi-factor authentication for SaaS, cloud, web and mobile applications. The Cloud Authentication Service can also accept authentication requests from third-party SSO solutions or cloud applications that have been configured to use RSA SecurID Access as the identity provider (IdP) for authentication.

RSA Authentication Manager verifies authentication requests, and centrally administers authentication policies, RSA tokens, users, agents and resources across physical sites, to help secure access to on-premises, cloud and web-accessible applications such as VPNs and web portals.

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, RSA provides a REST-based API so organizations can add multi-factor authentication to their custom applications.

CONNECTING YOUR SECURITY DOTS

While having certified integrations, a broad set of authenticators and intelligent risk-based authentication are all critical capabilities for ensuring you know who a user is, staying ahead of continually advancing attacks requires comprehensive visibility across your organization.



RSA is connecting the dots between its solutions, to eliminate identity-related blind spots, enabling you to respond more quickly to identity-based threats and in an orchestrated and automated way.

RSA® Identity Governance and Lifecycle can provide user access authorization data to ensure users only get access to what's appropriate.

RSA NetWitness® Platform can provide User and Entity Behavioral Analytics (UEBA) to warn you about suspicious user activity on the network.

RSA® Fraud Risk and Intelligence Suite can alert you to whether or not a user or any of their devices has been associated with known fraud in the wild.

And last but not least, RSA Archer® Suite can provide insight into how a user's access could impact your business and its associated compliance posture.



RSA SecurID Access, the industry's most advanced authentication platform, enables your users to do more by giving them the freedom to work wherever and whenever they need, while giving you the ability to transform your business and its associated IT infrastructure and while preventing identity risks from becoming a drag on your bottom line. Learn more at rsa.com/authentication.