SOLUTION BRIEF

RSA SECURID® ACCESS MODERN MOBILE AUTHENTICATION FOR VPN ACCESS

KEY BENEFITS

- *Reduce the risk of security breaches caused by unauthorized access*
- *Mitigate the risk of compliance violations*
- *Convenient, cost-effective and mobile-optimized authentication methods for VPN*
- *Leverage a proven, scalable enterprise-grade MFA solution trusted by more than 25,000 customers worldwide*

Today's world moves fast, and your business needs to move even faster to keep pace with unexpected market shifts and customer demands. To that end, your employees must have information at their fingertips, and around the clock, regardless of whether they are working from home, at a coffee shop or in a hotel room.

The trends are clear: Workers are no longer bound to the office. In fact, 50 percent of U.S. workers had the ability to work from home in 2017. Companies are embracing flexible work arrangements more and more: 40 percent more companies are offering flexible work options now compared with five years ago.[1]

In addition to changing *where* they work, employees are also demanding changes to *how* they work. Specifically, they want enterprise technology to be as intuitive as the consumer technology they use in their personal lives. They also expect simple, convenient ways to get access to the apps and data they need to do their job regardless of where they are or what device they are using.

These changing workforce dynamics have clear implications for remote access security: Access must be secure, but the controls organizations implement to secure remote access can't impede users' productivity.

REMOTE ACCESS SECURITY AND THE FUTURE OF VPNS

Organizations have long used virtual private networks (VPNs) to secure remote access to the network. To this day, many VPNs rely on passwords to authenticate users. Given that VPNs often provide unfettered access to corporate networks and passwords offer notoriously weak security, smart organizations are looking for stronger authentication to reduce the risk of a breach, and many are turning to multi-factor authentication (MFA).

Specifically, they're looking for an MFA solution that:

- Is easy to deploy and manage.
- Provides a high level of identity assurance (in other words, has strong mechanisms for confirming users are who they say they are).
- Gives users choice over how they authenticate (e.g., push to approve, biometric or one-time password).
- Doesn't stand in the way of users' productivity.

SOLUTION OVERVIEW:

RSA SecurID® Access enables businesses to empower employees, partners and contractors to do more without compromising security or convenience. RSA SecurID Access is built to address the security challenges posed by the mobile workforce, bring-your-own-device policies and today's blended cloud and on-premises environments. It ensures that users have timely access to the applications they need—from any device, anywhere—with a modern, convenient user experience. RSA SecurID Access confirms the legitimacy of access attempts with machine learning and risk analytics.

What's more, RSA SecurID Access provides organizations with flexible options for extending MFA to the VPN, in order to support today's wider population of remote users. The wide range of authentication methods RSA SecurID Access offers—from mobile push to approve, biometrics and one-time passcodes to hardware and software tokens—allows organizations to enable convenient access to the VPN without compromising security.

RSA SecurID Access provides the largest variety of authentication options, including mobile-enabled push to approve, SMS, biometrics and FIDO (Fast IDentity Online) tokens as well as industry-proven hardware and software tokens.

RSA SecurID Access, the world's most widely deployed multi-factor authentication and identity assurance solution. In real time, RSA SecurID Access makes intelligent access decisions based on a number of factors, including the asset a user is trying to log into, the profile of the user (her role and typical login patterns), the user's device profile and threat intelligence. Based on these and other factors, RSA SecurID Access leverages machine learning algorithms to create a "confidence score." The higher the score, the more likely the user is legit and the lower the risk her access request poses. If the confidence score falls below a certain threshold set by the organization, the system may trigger step-up authentication to prevent unauthorized access. In this manner, RSA has changed the authentication game from simple "in or out" access decisions to intelligent, risk-aware authentication that's pervasive, continuous and connected.

The bottom line: For your many and varied VPN users, RSA SecurID Access is the only multi-factor authentication solution they'll need. It offers a range of authenticators so you can give your users choice and select the options that work best for your business (we know authentication isn't a one-size-fits-all proposition). And it provides the identity assurance you need to mitigate today's access risks while providing a seamless authentication experience for users. With RSA SecurID Access, you don't have to compromise between user convenience and security.

SUMMARY:

VPNs are effective remote access gateways. However, given changing workforce dynamics, organizations are reevaluating the way they secure access to the VPN to ensure users *really are* who they say they are. RSA SecurID Access ensures that users have secure and convenient access to the VPN—from any device, anywhere—while providing high confidence that access attempts are legit. RSA delivers the single solution that can modernize your access to VPN, on-premises and cloud applications.

Interested in seeing how easy it is to use mobile authenticators from RSA SecurID Access? Sign up for the Test Drive at rsa.com/testdrive.

ABOUT RSA

RSA® Business-Driven Security™ solutions uniquely link business context with security incidents to help organizations manage digital risk and protect what matters most. With award-winning cybersecurity solutions from RSA, a Dell Technologies business, organizations can detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA solutions protect millions of users around the world and help more than 90 percent of Fortune 500 companies take command of their security posture and thrive in an uncertain, high-risk world. For more information, visit rsa.com.

[1] The 2017 State of Telecommuting in the U.S. Employee Workforce Report