SOLUTION BRIEF

RSA SecurID® Access for Cloud Applications

Companies across industries continue to adopt popular cloud-based applications—such as Microsoft 365, Salesforce.com, Workday, ServiceNow and more—to reduce IT costs, improve business agility and enable their digital transformations.

Hackers have their eyes on these cloud-based applications, too. They see them as attractive targets to attack, given how much sensitive data these applications hold, how frequently they're "secured" with just a username and password, and how little control IT and security teams generally have over them.

So what's a CISO to do?

Since some of these cloud applications offer their own multi-factor authentication (MFA) capabilities, one option is to turn on those capabilities. But this option isn't nearly as simple as it seems. For one thing, different MFA capabilities from different providers would quickly confuse users and impede their productivity, heightening their frustration and potentially leading to more calls to the help desk.

It would also be burdensome for IT to have to administer and support multiple MFA capabilities from different vendors. As it is, in many organizations today, help desks and IT admins are strapped. Adding extra authentication for individual cloud applications would add even more complexity.

And what if the cloud application doesn't offer an MFA capability?

Every user and every application, ground to cloud

One way to make it easier to provide convenient, secure access to users leveraging resources in the cloud (and on-premises) is to enable MFA across the enterprise. It may sound daunting, but with RSA SecurID® Access, **modern MFA can be made simple.**

Ground To Cloud

RSA SecurID Access is designed to work with your cloud and your on-premises resources, including your VPN and even legacy systems and custom applications. Certified out-of-the-box integration with more than 500 cloud-based and on-premises applications means that you can quickly configure RSA SecurID Access

Security challenges with cloud applications:

- Password vulnerabilities
- Lack of visibility and control; islands of identity
- Impacts large number of users
- Need to provide convenient, frictionless access
- Managing and administering multiple authentication tools

to work with your most critical resources, speeding time to value and allowing you to quickly mitigate your most pressing access risks. And you can deploy it on-premises, in the cloud or in a hybrid environment.

Convenient Cloud Services Backed By On-Premises Assurance

Reliability is critical for accessing software-as-a-service (SaaS) and web-based applications, and always-on security is critical to alleviating organizational risk. With a hybrid identity management approach, organizations can enjoy the benefits of the cloud combined with the availability and assurance of an on-premises system. This results in 24x7 authentication availability, and the added bonus that workers won't notice if (or when) the cloud becomes unavailable.

Intelligent Access. Frictionless Experience.

To provide strong security without sacrificing the user experience, RSA SecurID Access makes access decisions based on sophisticated machine-learning algorithms that take into consideration both risk and behavioral analytics. This lets RSA SecurID Access provide users with a completely seamless authentication experience (triggering step-up authentication only when needed, based on risk level and policies) while providing high levels of identity assurance, ensuring users are who they say they are and are not hackers in disguise.

Choice of Authentication

To further satisfy demanding users, RSA SecurID Access offers the widest range of authentication options, including mobile push authentication, biometrics, SMS, traditional hardware and software tokens, Fast IDentity Online (FIDO) and more. What's more, you can easily implement different authenticators for different user populations, allowing you to strike the right balance for your organization among convenience, security and cost. And, with the RSA SecurID Access platform, authenticators are backward-compatible to quickly authenticate with both cloud and on-premises applications.

One Platform For All Your Identity Needs

By providing coverage for the widest range of resources across your enterprise with the widest range of authenticators and by making intelligent, risk- and behavior-based access decisions in real time, RSA SecurID Access can function as the one authentication platform for all of your authentication needs. With a modern MFA solution that provides complete coverage for all your users and all your resources, and is easy for IT to implement and manage, you'll be better positioned to capitalize on digital transformation opportunities.

About RSA SecurID Access

RSA SecurID Access, part of the RSA SecurID Suite, enables businesses to empower employees, partners and contractors to do more without compromising security or convenience. Embracing the security challenges of today's blended cloud and on-premises environments, bring your own device, and mobile, RSA SecurID Access ensures that users have timely access to the applications they need—from any device, anywhere and ensures that users are who they say they are, with a modern, convenient user experience.

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.