RSA

WHITE PAPER

Authentication Your Way

Securing access in a changing world

Imagine that you're a CISO in charge of identity and access management for a major global technology and manufacturing company. You provide authentication for more than 300,000 employees and contractors across 3,000 applications. To secure access, you've taken on over 35 separate authentication and SSO technologies, which prove impossible to properly manage. The result? Undue complexity and dissatisfied users.

Now you see your job becoming even harder as your company—like the rest of the world—moves quickly to a "perimeter-less" network, in which apps and data reside anywhere, and old approaches don't work. Suddenly cloud authentication becomes a critical need, and the thought of a VPN restricting access to your organization's critical assets feels antiquated.

You can't stop the IT cloud revolution. Not that you'd want to: Cloud deployment offers much needed scalable capacity, business agility and, in many cases, dramatically lower operating costs. But you are on the hook to secure your organization's access. You need a new approach that works with today's modern infrastructure while keeping existing applications secure.

Mind the gap: Today's security challenges

The rush of cloud adoption and the explosion in mobile device usage have left organizations with information scattered across resources and applications, both inside and outside the traditional perimeter. Each of these applications and information sources requires unique access, creating "islands of identity" that become increasingly complex to manage—while making it more difficult for users to quickly and conveniently access what they need to do their jobs. As users travel from application to application (or island to island), they must remember multiple credentials, including usernames and passwords, while grappling with varying access policies and processes.

In many cases, a company could use multiple approaches to securing its islands of identity—perhaps a VPN, PAM, internal web portal and multiple SaaS vendors. Each resource is working to protect access to its assigned area, but the company as a whole lacks centralized visibility, a convenient user experience, and a consistent approach to authentication policies and procedures.

For IT security and operations teams, these daily realities complicate the authentication and identity process:

- **The VPN gauntlet**. As more and more data moves to the cloud, IT defaults to what it knows, requiring everyone to access cloud apps through the VPN. This introduces a complex user experience, duplicates authentication processes and forfeits the benefits of always-on mobile cloud access.
- **The Fort Knox Paradox.** IT's historic approach has been to implement the strongest form of authentication available, all the time. In a perimeter-less world, you need the flexibility to apply intelligent, appropriate control, without frustrating users or disrupting business continuity.
- **Mob rule**. Users demand access to an ever-widening array of applications, via a similarly expanding range of mobile devices. Increasingly distributed workforces drive toward two seemingly competing objectives: convenient access for users and secured access for IT.

A comprehensive approach to authentication

To address the constantly changing threat landscape, RSA recommends an intelligent, proactive and continuous approach to authentication called identity assurance. RSA SecurID® Access provides a context- and risk-based approach that first assesses the risk associated with each request, to determine how much assurance is actually required. Identity assurance makes better access decisions in real time and removes user friction. Through identity risk analytics, it evaluates user role, device type, session time and duration, application and data sensitivity, IP network, geolocation and other attributes to determine normal and abnormal patterns. It then automatically tunes itself to the patterns of behavior unique to each organization, group and individual, and assesses the level of risk associated with each access request. If a request is deemed risky, step-up authentication is triggered.

When step-up authentication is required, RSA SecurID Access provides a broad range of best-of-breed authentication methods, scalable to hundreds of thousands of diverse users and use cases. At the same time, its support for modern identity frameworks and standards enables further consolidation of many other access and identity systems. It protects all of your resources with the broadest set of authentication methods, including push notification, biometrics (eyeprint ID and fingerprint), one-time password (OTP), SMS, Fast Identity Online (FIDO)-certified, and traditional hardware and software tokens. With a strategy that extends secure access to traditional, web, mobile and SaaS applications, you get consistent policy enforcement across on-premises systems, mobile and the cloud.

When you review options, you may find that the solution to your needs is already in place and deployed. With RSA, you can get it all—from hardware tokens to advanced biometrics to risk-based identity assurance—from a single trusted provider.

81% of confirmed data breaches involve weak, default or stolen passwords,[1] making identity today's most common attack vector.

Does your security solution:

- Provide a range of options for all your users (employees, clients, partners, admin and casual users—those with smartphone and those without)?
- Offer the flexibility to add new methods?
- Offer risk- and context-based identity assurance?
- Support flexibility, user choice and emergency access?

Extending and simplifying authentication

Remember the challenge facing the CISO in our opening scenario? With RSA SecurID Access, the CISO was able to achieve both modernization and simplification. Now the same multi-factor authentication (MFA) solution tool secures access to cloud and VPN assets. And the company can take advantage of the intelligent risk-based capabilities of RSA SecurID Access.

RSA SecurID Access, the world's most widely deployed multi-factor authentication solution, helps to secure access in a world without boundaries. RSA SecurID Access provides convenient, secure access to on-premises, web, mobile and cloud applications, and helps bridge the gaps between islands of identity by giving you visibility into—and control over—access across your organization. Whether you want MFA as a service or implemented on premises as a hybrid, RSA has the right solution. RSA offers the widest range of authentication options to suit any user's preference or environment, allowing you to migrate to the cloud on your own schedule.

Trust a market leader

Organizations need to provide convenient and secure access so users can quickly get to the information they need, whether the application is on premises or in the cloud. RSA SecurID Access uses risk-based analytics and context-aware user insights to provide seamless authentication, using a variety of authentication methods that don't impede work. You can give your organization the confidence that people are who they say they are, while providing an easy experience for your users.

RSA SecurID Access:

- **Offers Industry-leading authentication technology** that can be deployed quickly as a service, speeding deployment while alleviating IT of the operating requirements associated with deploying and maintaining software and related infrastructure.
- **Incorporates a broad range of authentication choices**—from push notification to biometrics, FIDO to hardware and software tokens—depending on the level of risk identified and assurance required.
- **Delivers innovative identity assurance** by evaluating identity risk using risk-based analytics and real-time context attributes. This makes authentication not only stronger but seamless to the user, without sacrificing convenience or security.

RSA SecurID Access provides the most trusted, resilient and flexible forms of secure access on the market today. Our solutions are trusted by 25,000 customers and protect more than 60 million end users worldwide. RSA invented the secure access market more than 30 years ago and continues to invest in and evolve the RSA SecurID Access solution to help organizations provide convenient and secure access across on-premises, cloud and mobile environments.

RSA can serve as your strategic authentication advisor and work with you to incorporate best-of-breed, third-party and RSA solutions to support a futureproof security solution—one that enables secure and convenient access for any user, from anywhere to anything.

Learn more

Wherever your organization falls on the on-premises/hybrid/cloud continuum, you need consistent authentication and identity assurance. This secure access must be seamless and convenient for users—no matter where they are, what data they want to access, or how they want to access it.

RSA SecurID Access uses risk analytics and context-based user awareness to provide authentication your way: a blend of flexibility, convenience and security designed to fit your organization's unique usage and risk profile. As an innovative multi-factor authentication solution, it ensures that your organization gives the right individuals appropriate access, conveniently and securely.

Find what's right for you

There's a version of RSA SecurID Access to suit every organization's unique needs for industry-leading multi-factor authentication and identity assurance. Answer four simple questions and our online product selector tool will recommend the edition that best suits your organization's requirements. It couldn't be any easier.

Ready for authentication your way?
Learn more at www.rsa.com/authentication.