SOLUTION BRIEF

RSA SecurID® Suite

Accelerate business while managing identity risk

Security and control to manage identity risk

Convenient access to empower today's users

With your organization serving a growing and diverse user population inside and outside of the company, you need to control access to systems, applications and data that exist both on-premises and in the cloud. Cloud, mobile and the internet of things (IoT) are opening up more avenues for people in your organization to connect with each other and with key resources, which boosts collaboration and productivity. This digital transformation, however, also presents an increasing threat surface and more vectors for cyber attackers to find their way into your critical applications and sensitive information.

Identity has become one of the most consequential attack vectors to the modern enterprise. Last year, 81% of confirmed breaches to organizations' infrastructure, sensitive data or applications started with an identity takeover.[1] At the same time, organizations face increasing governance and compliance requirements—and may face hefty penalties for violations. In addition, users expect a mobile, convenient user experience to get their jobs done, and the lines of business are quick to adopt new SaaS applications to enable business agility.

Secure access transformed

RSA SecurID® Suite enables your organization to accelerate business while mitigating identity risk and ensuring compliance. To address today's toughest security challenges of delivering access to a dynamic and modern workforce across complex environments, the RSA SecurID Suite transforms secure access to be convenient, intelligent and pervasive across all access use cases.

Convenient

Today's users expect fast, convenient access to the data and applications they need to do their jobs. At the same time, IT needs an easy and effective way to protect anywhere-anytime-any device access to these assets that reside on-premises or in the cloud.

As a result, access controls must be secure, convenient and easy to deploy.

Key benefits at a glance

- Ensure your journey to the cloud is secure and convenient, without compromising either.
- Drive business agility through secure access.
- Accelerate secure user access to applications by providing a seamless and convenient user experience with modern authentication options when additional authentication is required.
- Reduce identity risks by eliminating inappropriate access.
- Empower business users to make smart, informed and timely access decisions.
- Enable visibility and control across all access use cases, ground to cloud, to provide a holistic identity solution.

Easy for your business users—Your users need to access applications and information with minimal friction. Additional authentication should be used only when required. When additional authentication is needed, users should have a broad variety of modern, convenient multi-factor authentication options that provide stronger authentication for a variety of access cases and diverse set of users including employees, contractors, help desk, partners and customers.

Another key element of convenience is empowering business users to make access and authentication decisions and react to risky situations with a simple-to-use interface.

Easy for your IT staff—It is important to make secure access deployment and management convenient for IT so they can respond rapidly to business needs and strengthen and extend access-compliant protection across traditional, web, mobile and SaaS applications:

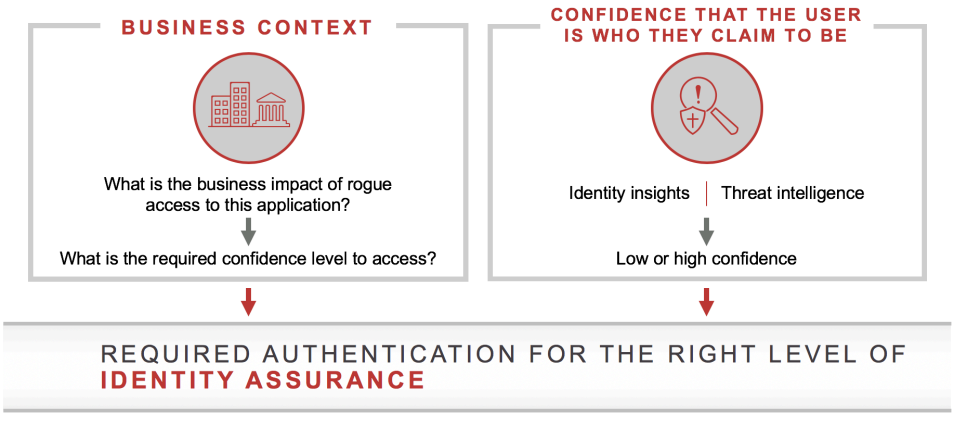
- Flexible deployment options, with the ability to respond to business needs quickly through easy onboarding of new applications
- Quick configuration options to optimize access decisions to respond to changing business needs and regulatory requirements

Intelligent

Intelligent authentication provides the benefit of reducing friction and adding security to protect applications and data that are critical to the business. It provides both security and convenience, and takes into account the needs of the modern workforce.

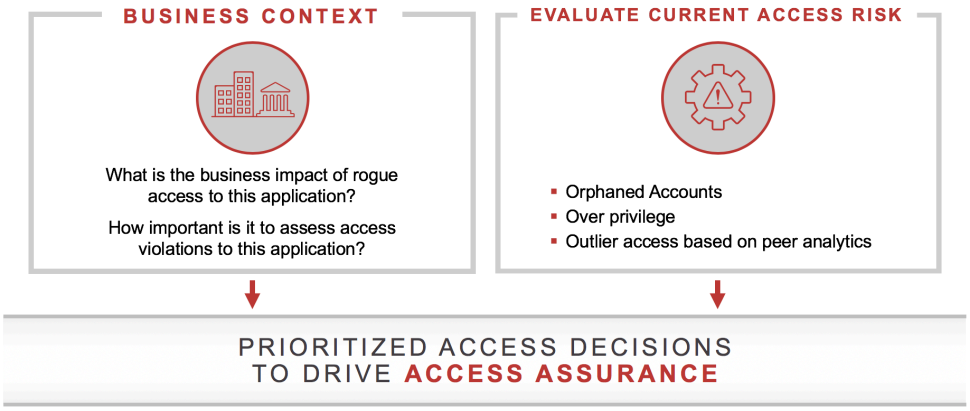
The intelligent approach to authentication considers the **business context**, or the impact of rogue access to an application on the business, to determine the policy or the required level of confidence needed to provide access to the application.

Identity assurance enables the organization to have confidence that users are who they claim to be. That assurance is evaluated at the time of access based on what the organization already knows about the user (e.g., a known device, user login information) as well as any risk indicators (e.g., login from a new location). Together, these determine a current level of confidence and drive the required levels of authentication to provide the appropriate level of identity assurance.



To manage risk effectively in an expanding attack surface, **Identity and Access Assurance** is critical. That's the confidence that users accessing applications and data are who they claim to be, have the right level of access and have access that's current with business requirements.

Intelligent access—When it comes to access control, the driver traditionally has been IT efficiency and streamlined provisioning of access to applications. But as organizations move to mobile and cloud technologies, it is critical to first gain a perspective on identity risk (for instance, the organization's current state of access, and how to stop inappropriate/unauthorized access). To minimize access risk of an application or data, an intelligent approach to access decisions considers the business context and impact of rogue access to an application on the business, in addition to evaluating current risk based on a set of defined criteria (e.g., number of orphaned accounts and overprivileged users).



The combined intelligent perspective and risk-based approach enables the organization to prioritize access decisions based on what matters most and to drive the right levels of identity assurance—the confidence that the right people have access—and access assurance—the confidence that the access is appropriate for the user's role/job and that the access is in compliance with corporate and regulatory policies.

Pervasive

Finally, a holistic identity solution needs to be pervasive and cover all access use cases. If a solution is good only for protecting a SaaS application or only an on-premises application and is not holistic across all use cases, an organization cannot achieve true identity and access assurance.

The reality is that with multiple sources of applications and data, user stores and identities will be scattered and decentralized. The goal is to connect to all of these "islands of identity" for unified visibility and control across all the access use cases.

By connecting to all applications, knowing who has access and having confidence that users are who they say they are at the time of access, organizations can apply a holistic approach to addressing the identity challenges of digital transformation.

With risk-based, multi-factor authentication, intelligent identity governance, and automated user lifecycle management, RSA delivers unprecedented identity and access assurance across all of your islands of identity—from ground to cloud.

Convenient, secure access for the modern workforce from ground to cloud

RSA SecurID Suite consists of two solutions that work together to address the security challenges of delivering access to a dynamic user population across complex environments.

RSA SecurID Access

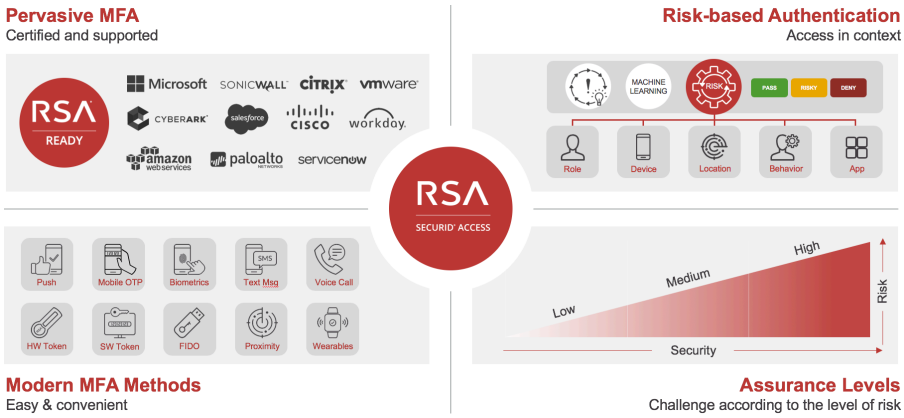
RSA SecurID Access enables organizations to empower employees, partners, contractors and customers to do more without compromising security or convenience. RSA SecurID Access ensures that users have timely access to the applications they need—from any device, anywhere—and ensures that users are who they say they are.

RSA SecurID Access provides these benefits with the following capabilities:

- **Pervasive visibility and control**—Your users need access to a wide variety of on-premises, cloud, SaaS and mobile applications. And you need the ability to make that access secure—and to do so relatively quickly—so people don't start doing their own thing, causing shadow IT.

  With RSA SecurID Access, you can quickly onboard new applications using wizard-based connectors that leverage leading integration standards such as SAML, password vaulting and RADIUS. Or you can reuse an existing integration via the RSA Ready program. RSA's dedicated team of partner engineers works with hundreds of leading technology vendors to document, certify and support the integration of RSA SecurID Access multi-factor authentication—giving you the peace of mind you need and at the speed the business needs it.

- **Modern multi-factor authentication**—RSA SecurID Access offers a wide range of authentication options to support the needs of the modern workforce. Options range from the well-known RSA hardware and software tokens, to mobile-enabled push notification, one time passcode (OTP) and biometric fingerprint and face as well as SMS and FIDO tokens. Users can choose which authentication methods are most convenient for them, ensuring that they will always have access while minimizing help desk calls and emergency access requests.



- **Risk-based authentication**—RSA SecurID Access provides risk-based authentication powered by machine-learning algorithms. The risk engine takes into account information about the user access, device, applications and behavior, and provides the confidence that users are who they claim to be based on comparing the current access request with the history of the user. This enables a frictionless user experience when the confidence is high, or prompts additional authentication and enhanced security layered on top of the MFA options.
- **Assurance levels**—The RSA solution balances security and convenience by setting up authentication policies intuitively based on low, medium and high levels of risk. Low-risk scenarios need low levels of assurance, while higher-risk instances may require different, more secure types of access controls.

RSA Identity Governance and Lifecycle

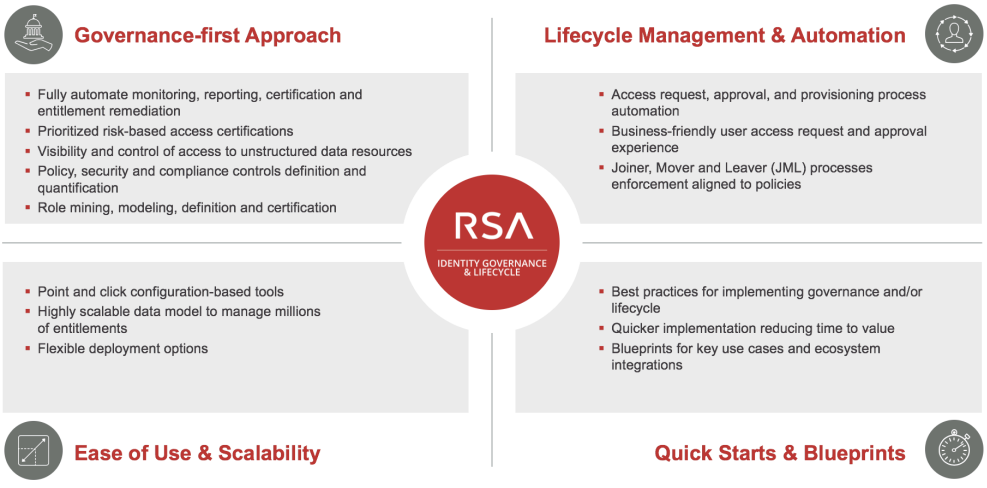
RSA Identity Governance and Lifecycle delivers continuous access assurance for organizations to help ensure that users across the organization have the proper level of access. By providing visibility across your islands of identity in today's blended cloud and on-premises environment, RSA Identity Governance and Lifecycle empowers business users to take action quickly and easily to address risky access situations with the highest business impact in order to reduce business risk and ensure compliance.

RSA Identity Governance and Lifecycle takes a governance-first approach to manage identity risk and ensure that the security posture of the organization is intact with regard to user access. This is accomplished by automating access review and certification processes for greater operational efficiency, cost and time savings, and by flagging issues between formal review campaigns. In addition, access certification responsibility and accountability are transferred to the people who understand access needs best—the business. Business-driven certification discourages access approval "rubber stamping." Business users are provided with prioritized access issues based on risk informed by intelligence so they are empowered to take action with insight on what matters most.

RSA Identity Governance and Lifecycle

- Prioritizes actions based on risk so that business-critical access violations are taken care of first
- Reduces time and manual effort with automated processes for access certifications and account lifecycle management
- Strengthens risk posture by having a clear picture of access violations and visibility into access
- Reduces chances of audit failure or breach by continually promoting resolution of risky access situations
- Reduces TCO with automated process and quick time to value

- RSA Identity Governance and Lifecycle enables you to implement security and compliance controls (e.g., segregation of duties, unauthorized access permissions) to ensure policy and control objectives are met continuously.
- To ensure users quickly gain access to the applications they need, RSA Identity Governance and Lifecycle provides the ability to grant access based on user roles and well-defined processes that enable the manager to provide access in a user-friendly way. It also manages entitlements (joiners, movers and leavers) across applications to ensure access stays current with users' roles and that there is no overprivilege. The entire process of access request, approval and provisioning is automated using business-friendly language for approvals in order to ensure that users obtain appropriate access quickly.
- Ease of use and scalability—In order to respond to ever-changing business needs and a dynamic threat landscape, RSA Identity Governance and Lifecycle provides security teams with the ability to configure and update policies, processes and controls quickly with point-and-click configuration tools that do not require customization and that provide quick time-to-value. In addition, high scalability allows your business to grow without needing to worry about the system, a critical factor given the number of applications and identities involved in business processes.
- Quick starts and blueprints—To ensure that your organization is managing identity risk effectively, we have recently introduced best practices and blueprints to provide a set of use cases and recommendations to allow you to speed your time-to-deployment and time-to-value.



For more information visit rsa.com/iam.

The information in this publication is provided "as is." RSA Security LLC or its affiliates make no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying and distribution of any software described in this publication requires an applicable software license.

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.

[1] Source: Verizon 2017 Data Breach Investigations Report