

RSA®



SOLUTION BRIEF

RSA SECURID® SUITE

ACCELERATE BUSINESS WHILE
MITIGATING IDENTITY RISK



KEY BENEFITS

- *Reduce identity and user access risk while protecting critical data and applications from unauthorized use and access.*
- *Deliver the right level of access conveniently and securely to your users - at the right time from anywhere, on any device.*
- *Improve your overall security posture with invisible, yet effective, continuous authentication.*
- *Meet industry regulations and organizational policies with sustainable compliance.*
- *Maximize user productivity with convenient application access and streamline user access fulfillment lifecycle.*

A new set of challenges requires a new approach to identity and access management. Organizations are no longer ensuring the identities of just workers inside a protected network. They're managing millions of user identities inside and outside their walls, providing access to systems, applications and data that exist on-premises and in the cloud, as well as addressing increasing governance and compliance requirements. It's time to reimagine your identity strategy—are you ready?

Introducing the RSA SecurID® Suite, the only identity and access assurance solution that meets the dynamic access needs of today's modern workforce.

The RSA SecurID Suite offers a comprehensive set of capabilities including access management, authentication, risk analytics, identity governance and lifecycle management.

The RSA SecurID Suite helps solve two fundamental challenges for your organization. Are my users who they say they are, and do they have the right level of access?

IDENTITY ASSURANCE

The first challenge is identity assurance. Organizations need to provide convenient yet secure access so that users can get to the information they need regardless if the application is on-premises or in the cloud. RSA uses context-aware, dynamic risk-based analytics to provide seamless, robust access that doesn't impede work yet gives your organization the confidence that people are who they say they are.

ACCESS ASSURANCE

The second challenge is access assurance—making sure users have the appropriate level of access to do their jobs. This involves reviewing, requesting, granting (and revoking) user access using automated processes that are in the hands of business owners and that are based upon identity intelligence that prioritizes activities according to risk. It also means ensuring compliance and governance through visibility and control in a way that results in your organization being in continuous compliance.

A UNIQUE IDENTITY SOLUTION TO FIT ANY ORGANIZATION

The RSA SecurID Suite is an innovative identity and access assurance solution that ensures your organization provides the right individuals appropriate access while ensuring compliance measures are met to reduce identity risk and meet the needs of your modern enterprise.

At RSA, we're continuously making advances in our identity and access solutions so that identities can be managed and protected more intelligently, more conveniently and more effectively. Only the RSA SecurID Suite helps protect your organization from identity threats that put your business at risk. By leveraging powerful real time user analytics, organizations can now be confident that they have the security measures that protect what matters most while providing convenient AND secure access.

By implementing a context-based, risk analytics framework across access management, authentication, identity governance and user lifecycle, RSA enables business-driven identity and access management for today's modern organization.

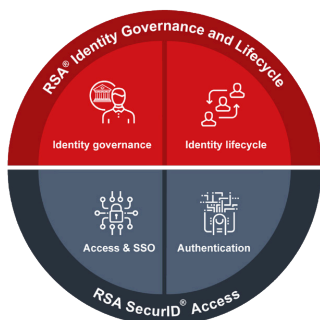
RSA pioneered the identity market and remains at the cutting edge. The RSA SecurID Suite ensures access, identity assurance, governance and lifecycle management work seamlessly together. As a result, business stakeholders and security teams can act with maximum insight to achieve seamless security while improving productivity and user experience.

The RSA SecurID Suite:

- Enables business-driven identity and access management (IAM) with integrated identity access, governance and lifecycle solutions.
- Makes IAM easy by giving users seamless, friction-less access to applications and conveniently connects them to the applications most necessary to get their jobs done from anywhere, any device. And, RSA offers flexible, scalable, and secure IAM solutions that are easy to deploy and manage—whether on-premises, in the cloud or as a hybrid model.
- Extends access protection to traditional, web, mobile and SaaS applications, enhancing the value of your current security technology investments.
- Helps ensure you address regulatory and industry data protection requirements and effectively meet compliance demands by automating identity lifecycle processes and ongoing governance efforts.

TWO SOLUTIONS SOLVING A COMMON CHALLENGE

The RSA SecurID Suite consists of two solutions that work together to solve the joint challenges of identity and access assurance.



RSA SECURID® ACCESS

CONVENIENT AND SECURE ACCESS FOR THE MODERN WORKFORCE

RSA SecurID Access is an innovative identity assurance solution that ensures your organization provides the right individuals appropriate access, conveniently and securely, from anywhere to anything, from any device. It enables organizations to consistently and centrally enforce dynamic risk-driven access policies based on context achieving convenience and strong security without compromise.

The solution incorporates the award-winning RSA SecurID® multi-factor authentication product that has protected organizations' internal applications for decades. And then it significantly expands the capabilities. A cloud presence seamlessly integrates with the solution to deliver single sign-on (SSO) for user convenience and standards-based access to cloud and mobile applications. Now with a reach into your on-premises, web, mobile and cloud applications, the RSA SecurID Access solution allows you to set a single access policy and have visibility across your enterprise into who is accessing what.

Risk analytics set the RSA SecurID Access solution apart. After all, how can you protect your organization from today's advanced threats without the presence of a sophisticated risk engine ready to evaluate in real-time user authentication requests and step up/challenge or block users that don't meet the required identity assurance? That is exactly what RSA SecurID Access does. Using a combination of device, location, network, role and other factors, the risk analytics evaluate every user login to ensure the user has reached the requisite security level and that the context of the user is appropriate to grant access. It's a powerful technology that can stop a sophisticated attacker with a stolen password dead in their tracks.

NO SINGLE AUTHENTICATION METHOD CAN SATISFY ALL YOUR USERS.

This is why we have greatly expanded the multi-factor authentication options available to you, providing a wide range of convenient mobile, biometric and traditional options to fit any user or use case. For example, some users might prefer a simple mobile-based push notification as an authenticator. In other scenarios, that same user may be asked to provide a one-time password (OTP) generated from a mobile application for greater security. For your most secure applications, the traditional RSA SecurID hardware or software token or a biometric fingerprint or eyeprint may be required.

The point is, these multi-factor authentication methods are all available and when combined with the risk analytics, your business rules can be applied to authentication and followed by all users, i.e., step up a user to a biometric authentication method if working off premises or from a remote country.

With RSA SecurID Access, organizations can:

- Provide strong, secure and convenient access to legitimate users from anywhere to anything, including web and SaaS applications, native mobile apps and traditional enterprise applications and resources (including VPNs, firewalls, virtual desktops and Windows or Linux servers) whether deployed on-premises or in the cloud.
- Apply consistent and centrally-enforced risk and contextual access policies to configure user access in real-time, based on the business areas they operate in, location, application sensitivity, session and network information, and device type.
- Reduce business risk by using convenient and secure access controls (such as multi-factor authentication, risk analytics and real-time context) to verify that the people trying to access your systems are who they say they are.
- Increase business agility, security and user convenience by providing the broadest range of authentication solutions.

RSA® IDENTITY GOVERNANCE AND LIFECYCLE ACT WITH INSIGHT TO DRIVE INFORMED SECURITY AND RISK DECISIONS

RSA Identity Governance and Lifecycle solutions protect your organization from the identity and access risks that arise in today's boundary-less world and enable your dynamic user population to get the access they need when they need it. With RSA, you know where your greatest risks are and can mitigate them quickly.

RSA Identity Governance and Lifecycle enables the ability to act with insight to reduce identity-based risks and drive informed security decisions. RSA Identity Governance and Lifecycle simplifies how access is governed and streamlines access requests and fulfillment to deliver continuous compliance by automating the management of user entitlements throughout the user's lifecycle.

ONE SOLUTION, MULTIPLE OPTIONS

RSA® Identity Governance simplifies how user access is governed across the enterprise. RSA Identity Governance makes it possible to achieve sustainable compliance by fully automating the monitoring, reporting and certification and remediation of user entitlements.

RSA® Identity Lifecycle streamlines access request and fulfillment processes using business language to ensure users, both new and those changing roles, gain timely and appropriate access to the resources they need in accordance with compliance objectives.

RSA® Data Access Governance provides visibility, monitoring, certification and reporting of user access permissions to unstructured data resources stored on Microsoft Windows, Linux, and UNIX file servers, network-attached storage devices and Microsoft Sharepoint servers. It is available as an add-on option with the RSA Identity Governance and Lifecycle solution.

RSA IDENTITY GOVERNANCE

IMPROVE AUDIT PERFORMANCE AND MINIMIZE RISK

With RSA Identity Governance, organizations can:

- Gain an extraordinary enterprise-wide visibility into all your user access privileges, improving the ability to safeguard access to information assets by quickly identifying orphan user accounts, inappropriate user access, and violations of policy, such as segregation of duties that introduce risk to the business.
- Engage the line-of-business for user access review and certification processes thereby empowering the business to take responsibility and assume accountability, helping to ensure compliance with regulatory requirements and IT controls.
- Manage and audit all entitlement changes through integration with enterprise-wide access fulfillment and enforcement systems that speeds compliance reporting.

RSA IDENTITY LIFECYCLE

SIMPLIFY AND AUTOMATE THE ACCESS REQUEST PROCESS

RSA Identity Lifecycle simplifies and automates how access is requested, approved and delivered. RSA Identity Lifecycle combines a business-friendly interface for access request and approval with an innovative approach to provisioning user access changes automatically across all target systems. RSA Identity Lifecycle can be layered on top of existing provisioning systems, extending their value.

With RSA Identity Lifecycle, organizations can:

- Provide a business-relevant, easy-to-use service for requesting and approving access that uses a single repository which houses complete information about identities and data resources, as well as policies around compliance controls, birthright, and user transfer and termination events.
- Execute user access changes rapidly and reliably, across all key applications—whether on premises or SaaS—without manual effort—that provides end users with an easy-to-use system and encourages its use.
- Enforce policies and ensure sustainable access compliance through preventative controls, enforced at the time of access request.

- Efficiently onboard, offboard, or transfer users, ensuring that users quickly obtain appropriate access through suggested entitlements based on similar users' attributes and job roles.
- Connect quickly to commercial or custom applications via configuration-based adapters, avoiding long and expensive deployment projects.
- Leverage existing provisioning systems instead of ripping and replacing them thereby protecting your prior investment.

REIMAGINE YOUR IDENTITY STRATEGY WITH RSA

Reimagine your identity strategy for the modern workforce with RSA SecurID Suite, the industry's most innovative identity and access assurance solution. RSA gives your users the fast, convenient access they need to innovate and succeed, anytime, anywhere, from any device and gives you the visibility and control minimize risk.

Choose RSA SecurID Suite. Your users and your business will love you for it. Learn more at rsa.com/iam.

The information in this publication is provided "as is." Dell Inc. or its subsidiaries 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.

Copyright 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA, 04/17, Solution Brief, H15848

Dell Inc. or its subsidiaries believe the information in this document is accurate as of its publication date. The information is subject to change without notice.