RSA®

REIMAGINE YOUR IDENTITY STRATEGY

Keep your business soaring
with identity and access assurance

BUSINESS-DRIVEN SECURITY™

INNOVATE WITHOUT LIMITATIONS

Remember when you were a kid? A cardboard box was a rocket ship ready to blast off to the moon. Intricate castles emerged from the sand. And just about anything—from blankets to tree branches—could become a secret fort.

What if imagination and creativity flowed as freely in your business? Unhindered by fear or insecurity, you'd have the courage, ambition and hope to reach new users, deploy new technologies and grow your business faster. You could conquer the world (or at least the marketplace).

Your identity strategy should be the wings that keep your business—and your users—soaring.

Reimagine your identity strategy with the RSA SecurID® Suite, the industry's most advanced identity and access assurance solution that helps minimize risk and accelerate business. With the RSA SecurID Suite, you're free to explore a world of limitless possibility.

THE NEW TECHNOLOGY PLAYGROUND

The digital revolution has enabled widespread business growth and innovation, but it's also exposed your business to new vulnerabilities and risks, which threaten it daily. To address ever-increasing security and compliance demands, organizations must ensure the identities of employees inside their protected network along with millions of users outside their walls—while providing convenient access to systems, applications and data that exist on premises and in the cloud.

Your identity strategy must accelerate your business and mitigate risk by effectively managing:

Multiple user identity types, from both inside and outside the company

Access to systems, applications and data, both on premises and in the cloud

User access from anywhere, on any device

ARE YOU PROTECTING YOUR IDENTITY KINGDOM?

The threat landscape is expanding—and traditional identity and access management (IAM) technologies and approaches leave IT security and operations teams ill equipped to simultaneously ensure convenience and strong security without compromise.

The perimeter is being disrupted, rendering traditional security controls ineffective. Employees have gone beyond the traditional on-premise applications to leverage, for example, SaaS applications and file sharing services that reside in private and public clouds.

Access blind spots and islands of identity are growing, especially due to the shadow IT phenomenon. To increase productivity, business users go around IT and deploy SaaS applications. These islands of identity create control blind spots as user access is increasingly managed at the cloud application or system level, rather than centrally.

Business managers are checking the compliance boxes. Ineffective governance and user lifecycle controls have left users over-provisioned, increasing the number of unused accounts and the risk of insider threats. This creates vulnerable identity islands open for attack. To try to address this problem, many organizations have implemented some form of identity governance, often requiring regular access oversight. However, such periodic access reviews can quickly become rubber-stamping exercises when business managers are faced with lengthy reports, looming deadlines and an overall lack of business context surrounding IT-provided data.

THE RESULT?

Identities are under attack. Users often replicate credentials, creating "one key to access the kingdom" —and generating an attack surface that malicious actors can easily take advantage of to impersonate users, move undetected, and access critical data. According to recent research, 63% of confirmed data breaches leveraged weak, default or stolen passwords[1]—making identity the single most consequential attack vector.

63%

of confirmed data breaches leverage weak, default or stolen passwords[2]

Users are frustrated.

Users expect ready access to the data and applications they need to do their jobs. Repeated prompts, requirements for complex and constantly changing passwords, incorrect access and other barriers to convenience create friction in the user experience. Users are led to bypass security controls, jeopardizing compliance.

IT is losing control.

IT can be slow to put identity and access risk into a business context, so users go around IT and deploy cloud applications—increasing the likelihood of failed audits and security breaches.

Business growth is hindered.

Lack of identity and access assurance slows a business's ability to deliver information to users and roll out new technologies—ultimately affecting growth.

[1,2] Verizon 2016 Data Breach Investigations Report.

IDENTITY & ACCESS MANAGEMENT THAT PREPARES YOUR BUSINESS FOR TAKEOFF

To give your business the oomph it deserves, you need to reimagine your identity strategy. What if identity and access management could not only strengthen security, but also enable growth and innovation?

The right identity and access management technology can help you:

Strengthen security and mitigate risk. Prioritizing security activities based on risk makes it easier to mitigate the risk of stolen identities and failed audits.

Replace fear with confidence. Be sure that users are who they say they are, and can access what they need to do their jobs (and nothing more).

Keep pace with the business, with an approach that's intelligent, proactive and continuous—leveraging identity risk analytics to make better access decisions.

Make life easier for everyone, with access that's seamless, frictionless and nearly invisible to users. Users quickly and easily get what they need, while security and compliance remain both achievable and demonstrable.

A NEW APPROACH TO IDENTITY & ACCESS MANAGEMENT

It's time for a new approach to identity and access management. This requires evaluating your current approach, understanding what you need to be successful and making sure you have the right technology to help you reach your goals. Carefully consider your approach in three key areas:

1

Identity governance

Are you able to see across all your islands of identity—who has access to what? Can you gain actionable insights into your riskiest areas? Are you sure that users have the right levels of access to do their jobs, and no more? Are you sure enough to certify audit reports? If you're not completely sure, it's time to reimagine your identity governance strategy and solution.

2

Identity assurance

Look at how you authenticate your users today. The goal isn't to simply authenticate each user, but to keep security strong while providing fast, convenient access. When you grant access, how sure are you that users are who they claim to be? Are you giving your users more security hurdles to jump over when they travel, work from a mobile device—or simply need to do multiple tasks at once? Are you matching authentication methods to their particular needs? If you have any hesitation, it's time to reimagine your approach to authentication—and move toward identity assurance as the end goal.

3

User lifecycle management

Are you able to manage user onboarding and offboarding in the most efficient, user-friendly and risk-aware way possible? Are you automating "birthright" entitlements for your users from the start? How easy is it for users to get fast access to the data and systems they need?. Are you leveraging automation and risk intelligence to keep governance controls in place while speeding up the access provisioning process? Do you know who requested and approved access for your users? If you aren't satisfied with your execution in any of these areas, it's time to reimagine your identity lifecycle approach and technology.

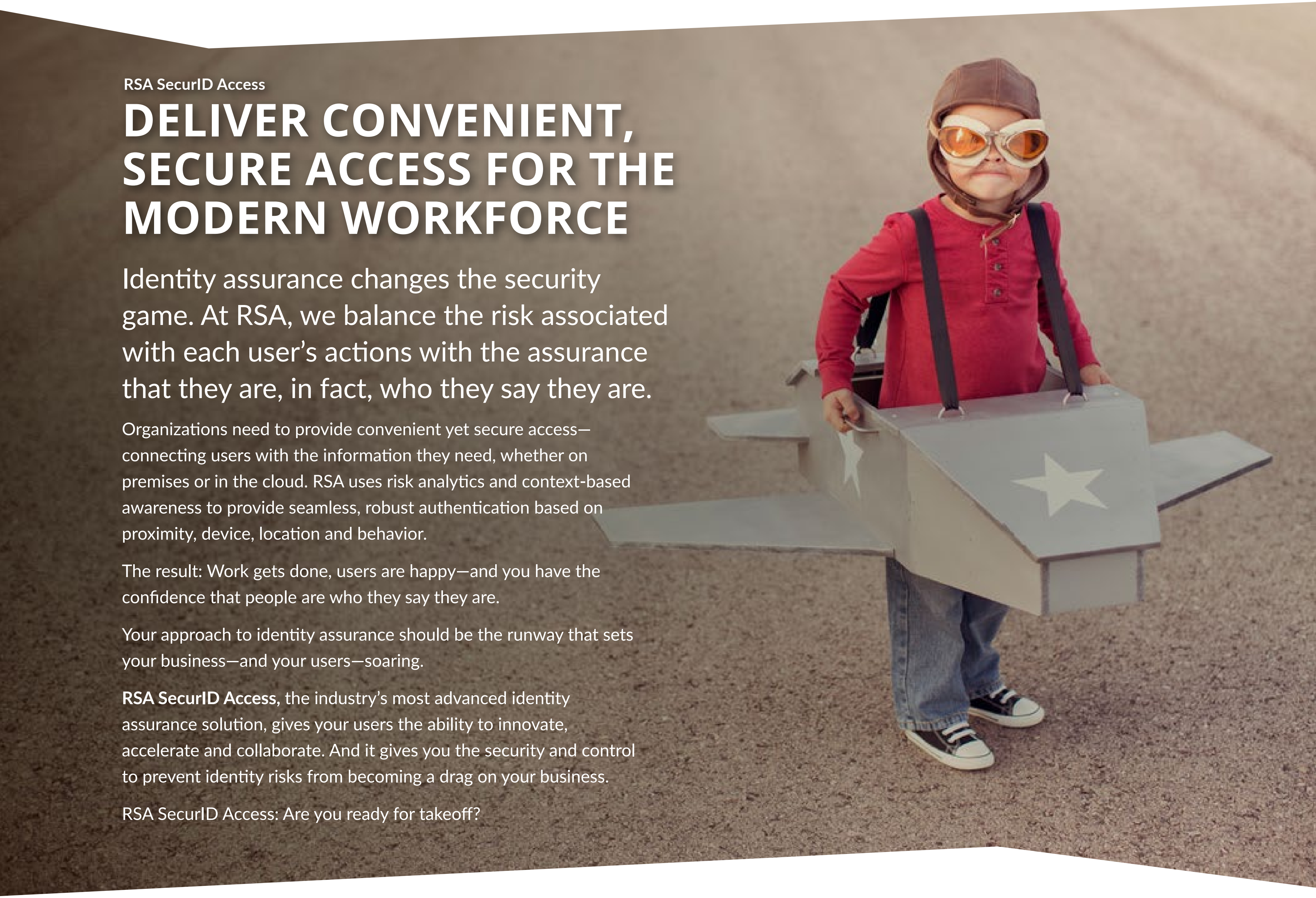
MANAGE IDENTITY BASED ON RISK & BUSINESS CONTEXT

RSA helps organizations reimagine the possibilities for identity and access management. Our business-driven technology can improve identity and access assurance, while making access simultaneously easier for the users and more secure for the business. RSA provides full visibility across all applications and users, bringing everything together for a holistic view of identity.

RSA's approach to identity and access assurance leverages risk and context—weaving them into the fabric of your identity infrastructure to help assess, automate, streamline and prioritize access delivery and identity risk mitigation.

RSA SecurID Access

DELIVER CONVENIENT, SECURE ACCESS FOR THE MODERN WORKFORCE



Identity assurance changes the security game. At RSA, we balance the risk associated with each user's actions with the assurance that they are, in fact, who they say they are.

Organizations need to provide convenient yet secure access—connecting users with the information they need, whether on premises or in the cloud. RSA uses risk analytics and context-based awareness to provide seamless, robust authentication based on proximity, device, location and behavior.

The result: Work gets done, users are happy—and you have the confidence that people are who they say they are.

Your approach to identity assurance should be the runway that sets your business—and your users—soaring.

RSA SecurID Access, the industry's most advanced identity assurance solution, gives your users the ability to innovate, accelerate and collaborate. And it gives you the security and control to prevent identity risks from becoming a drag on your business.

RSA SecurID Access: Are you ready for takeoff?

RSA® Identity Governance & Lifecycle

BRING IDENTITY RISK INTO FOCUS WITH ACCESS ASSURANCE

Everywhere you look, boundaries are blurring. Sometimes it can feel a little unsettling. Access assurance helps protect your business from risks that arise in today's boundaryless world, while ensuring that your dynamic user population can get the access they need when they need it. Access assurance lets you implement stronger access controls, gain enterprise-wide access visibility, and streamline delivery of user access via automated processes while minimizing risk.

With **RSA Identity Governance & Lifecycle**, you know where your greatest risks lie and can mitigate them quickly. As you plan for growth, you can rest assured that your user access is more secure and your business more compliant.

IDENTITY & ACCESS ASSURANCE THAT FUELS BUSINESS GROWTH

RSA identity and access assurance solutions leverage contextual insights and risk analytics to support the access management, authentication, identity governance and lifecycle management capabilities of the RSA SecurID Suite.

Centralized visibility and control across islands of identity. RSA SecurID Suite works across all applications, for all users interacting with your business.

A risk-based approach to focus on what's important. Prioritize identity governance efforts by identifying and addressing your biggest identity and access risks, then eradicating threats before they become problems. Use identity risk analytics and context-based authentication to speed access delivery and governance.

Frictionless security. RSA makes security seamless at a user's point of entry. Making security a natural and intuitive step in a user's daily activity keeps productivity high while continually protecting against new threats.

Continuous assurance. Risky or unlikely access scenarios automatically trigger additional authentication or controls, adhering to rigorous security and compliance requirements.

The RSA SecurID Suite gives enterprises the confidence to open their walls to employees, customers and partners—and to grow quickly and successfully while managing identity and access at the speed of business.

REIMAGINE IDENTITY WITH THE RSA SECURID SUITE

Reimagine your identity strategy for the modern workforce with the RSA SecurID Suite. RSA gives your users the fast, convenient access they need to get the job done—any time, anywhere, from any device—while giving IT the visibility and control it needs to minimize risk.

With the RSA SecurID Suite, you can do more and grow your business more quickly, minimizing risk of a breach or noncompliance—and delighting your users with convenient, easy access to the systems and data they need. Identity and access management become frictionless, automated, continuous and risk aware, helping your business accelerate.

ABOUT RSA

RSA offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to rsa.com/reimagine.

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.