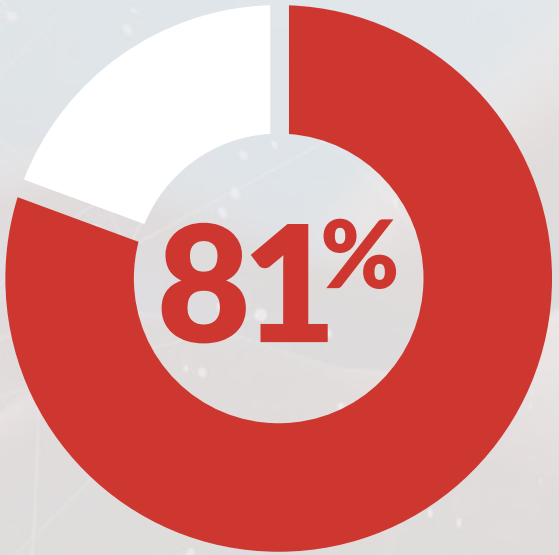
RSA BUSINESS-DRIVEN SECURITY™

FIVE WAYS TO TRANSFORM ACCESS AND SECURE THE DIGITAL ENTERPRISE

SECURE ACCESS CHALLENGES FOR TODAY'S DIGITAL ENTERPRISE

The days of securing a well-defined perimeter around your organization are gone. The cloud, mobile technologies, the internet of things (IoT) and diverse user groups freely exchange data across digital ecosystems, network and economies. This fluidity, however, means that organizations must secure access at multiple points throughout the organization, or risk letting in intruders seeking to hijack data.

To manage the increasingly diverse digital landscape of mobile user populations, hybrid environments and BYOD programs, IT and security managers need to move beyond usernames and passwords, expanding their use of multi-factor authentication (MFA) to help provide secure and convenient access to the critical data and systems users need.

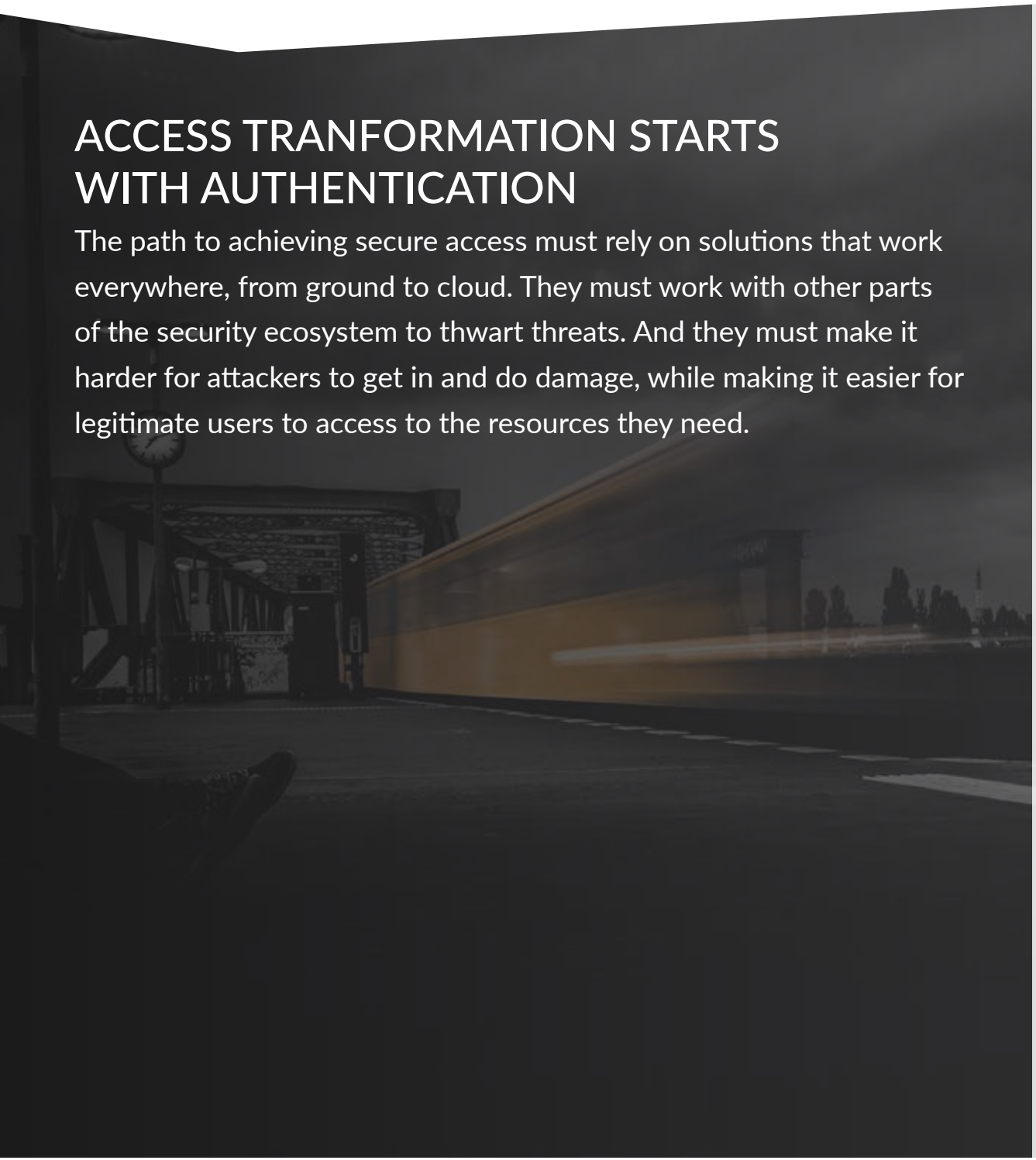


OF HACKING-RELATED BREACHES LEVERAGED **STOLEN OR WEAK PASSWORDS**[1]

Source: Verizon, 2017 Data Breach Investigations Report.

ACCESS TRANFORMATION STARTS WITH AUTHENTICATION

The path to achieving secure access must rely on solutions that work everywhere, from ground to cloud. They must work with other parts of the security ecosystem to thwart threats. And they must make it harder for attackers to get in and do damage, while making it easier for legitimate users to access to the resources they need.



Protecting against attacks means making authentication:

Pervasive
Enabling secure access at all points across applications, devices, users and environments.

Connected
Sharing information and insights across the security ecosystem to strengthen security.

Continuous
Constantly collecting and analyzing information to stop attacks.

And doing it all without adding friction to the user experience.

FIVE FOCUS AREAS FOR SECURE ACCESS TRANSFORMATION

Here are five common ways you can transform access with multi-factor authentication (MFA) throughout your organization:

VPN access

Cloud applications

Privileged access

Custom and legacy apps with next-generation firewalls

Digital workspaces

Read on to learn how MFA can transform how you provide secure access—to any application, from any device, anywhere, at any time.

EVOLVING ACCESS TO THE VPN

Back in the day, when only a handful of users accessed your VPN, it was easy to control access and enhance security; you may have deployed a token to that core group. Today, with more and more people using VPNs, too many organizations still rely on basic usernames and passwords. And that leaves you vulnerable. Instead, you need to provide easy, frictionless and secure access to a diverse and growing population of VPN users—including employees, contractors, vendors, customers, audit team members, and partners. And you must have confidence that they are who they say they are, and have the appropriate levels of access.

Modernize access to your VPN in three ways:

Use modern MFA tools, such as push-to-approve authentication and biometrics, on users' mobile devices for easy, secure access.

Leverage risk and behavior analytics to provide more complete identity assurance that users are who they say they are.

Keep it simple for users—provide one authentication solution for all access points, including VPN, as well as applications that live outside the VPN like cloud and third-party apps.

DID YOU KNOW?

More than tokens

RSA has the **broadest range of authentication solutions**, including mobile MFA via push notification, biometrics, OTP, SMS, and of course, hard and soft tokens.

SECURING CLOUD APPLICATIONS

Third-party cloud applications such as Microsoft Office 365, Salesforce, and Workday are critical productivity tools, used daily by employees and vendors alike. When you look at all the sensitive data that sits in these applications—from personally identifiable information (PII) and health information to payment data and corporate secrets—it's clear that it needs to be protected. And access security must do so without disrupting your employees' ability to do their jobs. Plus, some emerging regulations and corporate policies may require that you protect this data with something stronger than a password.

Here are three ways MFA can help secure access to your cloud applications:

Provide users a choice of authentication methods. Allow users to choose methods most convenient for them, such as mobile-optimized MFA, including push-to-approve and biometrics.

Challenge only according to the level of risk. Ask for step-up authentication only when a user or situation presents a risk, based on user and risk analytics further reducing access friction

Make it easy for users and administrators. Many cloud application providers also offer MFA capabilities, but that means more applications and tools for the end user to remember, and more MFA solutions for you to manage. Keep it simple with one authentication solution that covers all your apps, from the ground to the cloud.

DID YOU KNOW?

Standards-based interoperability
RSA SecurID® Access supports **500+ certified apps** out-of-the-box and works seamlessly with thousands more.

PROTECTING THE MOST CRITICAL ACCESS WITHIN THE BUSINESS

While any compromised identity can have real consequences for organizations, privileged accounts pose the greatest security threat. In the wrong hands, privileged credentials can allow attackers to take control of IT infrastructure, disable security controls, steal confidential information and commit fraud.

Many organizations have implemented tools and processes for managing privileged credentials, including Privileged Access Management (PAM) solutions and password vaults. That's a big step toward more secure data.

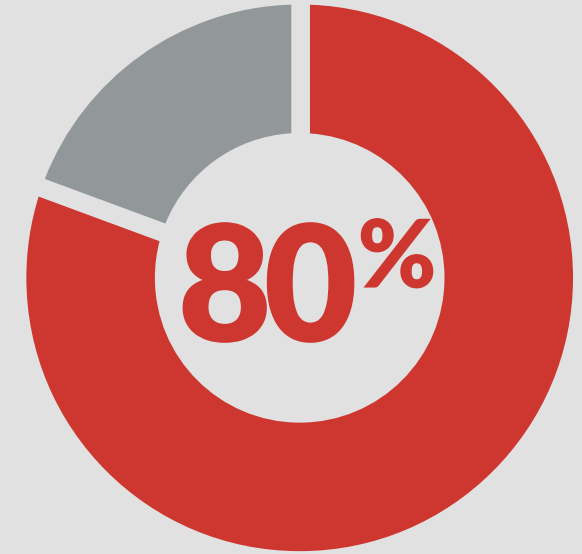
What's surprising is how many organizations using PAM to protect privileged credentials still rely on usernames and passwords to secure those vaults and tools. Here are three ways to strengthen identity assurance with privileged users:

Require strong authentication with MFA to protect access to PAM solutions, plus critical infrastructure including Amazon Web Services, Microsoft Azure, firewalls, and VPN.

Combine MFA with a robust risk and behavioral analytics engine to enhance your security posture and detect suspicious access attempts on these critical assets.

Think beyond traditional admin accounts to include privileged accounts across third-party applications and cloud providers—wherever users have access to sensitive and privileged assets.

Source: Jeff Edwards, "**By the Numbers: Privileged Access Management**" Identity Management Solutions Review, July 2016.



OF SECURITY BREACHES
INVOLVE PRIVILEGED CREDENTIALS[2]

SECURING CUSTOM AND LEGACY APPS WITH NEXT-GENERATION FIREWALLS

Behind the firewall, custom and legacy applications contain critical information needed to run the business. As authentication becomes more pervasive, you also need to evaluate security inside the firewall, assessing how each application is protected. If a username and password gets compromised, hackers can move laterally throughout the network, often undetected, accessing multiple critical applications. Historically, it's been difficult and costly to secure access to custom and legacy apps using MFA. But now there's a way to give them the same level of protection, integrating MFA with next-generation firewalls to apply MFA to these legacy apps. Specifically, you can:

Secure access at the network level. This approach gives you more control over access, without spending the time and money required to develop integrations for each legacy or custom app.

Protect against compromised credentials. Network-level MFA covers all applications, with more protection against stolen or compromised usernames and passwords.

Strengthen firewall administration. Group firewall administrators into low, medium and high assurance levels based on their roles and permissions.

Be more compliant. MFA deployed at the network level helps provide the security you need to better comply with regulatory compliance mandates, including PCI DSS and HIPAA.

PROTECTING DIGITAL WORKSPACES

To help deliver and manage access to any app on any device, organizations are turning to digital workspaces like VMware Workspace One. Add MFA to the front door of these digital workspaces to provide strong security as users access the mobile apps they need to stay connected and productive. Use additional step up authentication based on the level of risk of the application and individual to further hone access and reduce user friction. To start securing your digital workspaces:

Reduce user friction by challenging users based only on the level of risk each poses. Use machine learning to understand behaviors. When you're confident that user A is user A, let him in. Extend this convenience to all users, while maintaining strong security.

Provide simple, convenient access. When you do have to step up and ask for additional authentication, leverage modern mobile authentication for simple access. Give users a consumer-simple experience that doesn't impede productivity.

Use a single MFA solution. Cover all your digital workspace, on-premises, and cloud security needs with one solution vs. various point authentication solutions that can cause user confusion and duplicative administration.

DID YOU KNOW?

Future ready
RSA SecurID Access **scales across millions of users, apps, and devices** from ground to cloud and whatever comes next.

IDENTITY ASSURANCE, FOR SECURE AND CONVENIENT ACCESS FROM GROUND TO CLOUD

At RSA, we've transformed our offerings to meet today's modern authentication needs. Advanced analytics and machine learning technologies allow us to provide the most convenient and secure user access possible across a wide range of authentication options—from traditional hardware and software tokens to mobile-optimized biometrics and push notifications. And we make it easy for customers to extend traditional methods with more modern ones to improve overall security posture.

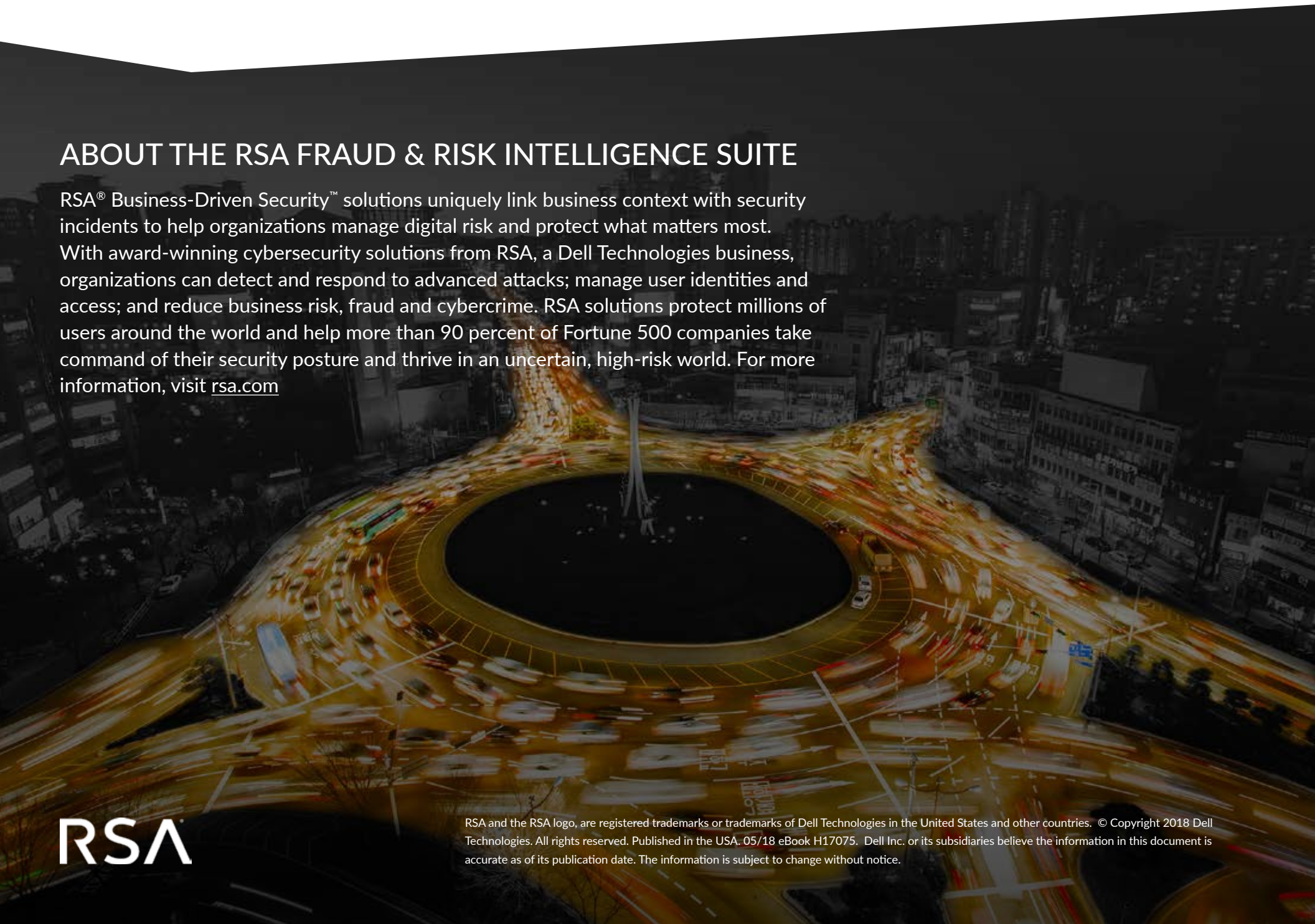
Deliver convenient, secure access to your extended enterprise with RSA SecurID® Access, the leading multi-factor authentication and identity assurance solution. Whether you deploy it as a service in the cloud or on premises, RSA SecurID Access protects both SaaS applications and traditional enterprise resources with a full range of authentication methods and dynamic, risk-driven access policies. Learn more at www.rsa.com/authentication.

DID YOU KNOW?

Assurance you can count on
RSA SecurID Access offers a risk-based **approach** that provides seamless security for a diverse set of users without compromising convenience.

ABOUT THE RSA FRAUD & RISK INTELLIGENCE SUITE

RSA® Business-Driven Security™ solutions uniquely link business context with security incidents to help organizations manage digital risk and protect what matters most. With award-winning cybersecurity solutions from RSA, a Dell Technologies business, organizations can detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA solutions protect millions of users around the world and help more than 90 percent of Fortune 500 companies take command of their security posture and thrive in an uncertain, high-risk world. For more information, visit rsa.com



RSA