**RSA** BUSINESS-DRIVEN SECURITY™

FOUR TIPS TO SECURE DIGITAL WORKSPACES WITH MFA

MAKING DIGITAL WORKSPACES MORE SECURE

Faced with managing more and more mobile and BYOD programs, organizations are turning to digital workspaces to help them deliver and manage any app on any device.

For end users, digital workspaces such as VMware Workspace™ ONE™ serve as one-stop shops for an organization's entire application portfolio, wherever users are and whatever device they're using. Because virtual workspaces give users such easy access to so many applications, they generally merit a level of security beyond basic authentication. Mobile Multi-Factor Authentication (MFA) from RSA SecurID® Access uses risk and behavioral analytics to confirm users' identities, providing an experience that's both convenient and secure.

1 Verizon, _2018 Data Breach Investigations Report_.
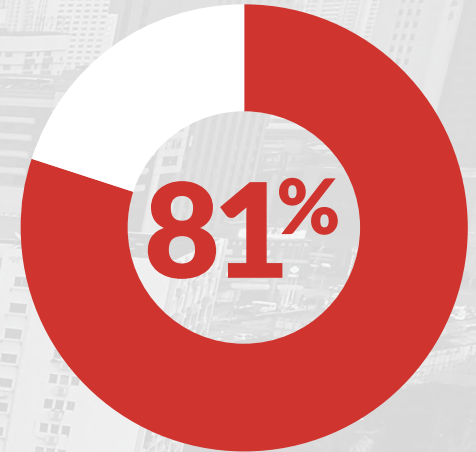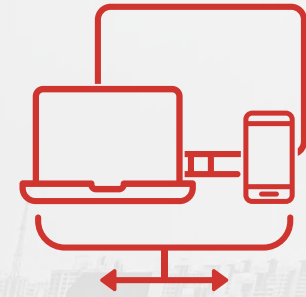
81%
OF HACKING-RELATED BREACHES LEVERAGED **STOLEN OR WEAK PASSWORDS**[1]

WHAT'S THE BEST WAY TO SECURE YOUR DIGITAL WORKSPACE?

We've identified four tips for securing the digital workspace.

1 **REALIZE THAT USERNAMES AND PASSWORDS ARE NOT ENOUGH**

Deliver convenient and secure front-door access to your entire application catalog, via machine learning-based risk assessments.

2 **TAKE A RISK-BASED APPROACH TO ACCESS CONTROLS**

Trigger step-up authentication based on user risk and application sensitivity, for specific applications or an entire platform.

3 **PROVIDE SIMPLE, CONVENIENT ACCESS**

Give end users a consumer-simple experience that doesn't impede productivity.

4 **USE A SINGLE MFA SOLUTION**

Cover all your digital workspace, on-premises, and cloud security needs with one authentication solution.

TIP 1 REALIZE THAT USERNAMES AND PASSWORDS ARE NOT ENOUGH

It's very easy for bad actors to get credentials from their own hacking activities or from the dark web—and once they're in your network, they're free to roam.

You need more than usernames and passwords as your first line of defense. Consider adding MFA to your digital workspaces to protect front-door access. Next, ensure that your policies are flexible enough to step up MFA to users or applications as required. The goal is simple, convenient MFA—whether biometrics or push notifications—that can increase security while easing friction.

TIP 2 TAKE A RISK-BASED APPROACH TO ACCESS CONTROLS

A risk-based MFA solution will ask for additional authentication only when it detects a high enough level of risk to warrant it, based on your defined security policies. The best approach combines behavioral analytics, business context, and geographic and technology signals (IP address, browser type, etc.) to automatically understand each user interaction and gauge the degree of risk posed by an access attempt.

If the solution has machine learning capabilities, this information can become something it "knows" and automatically takes into account for each user—further reducing the need to ask for additional authentication unless anomalous behavior warrants it.
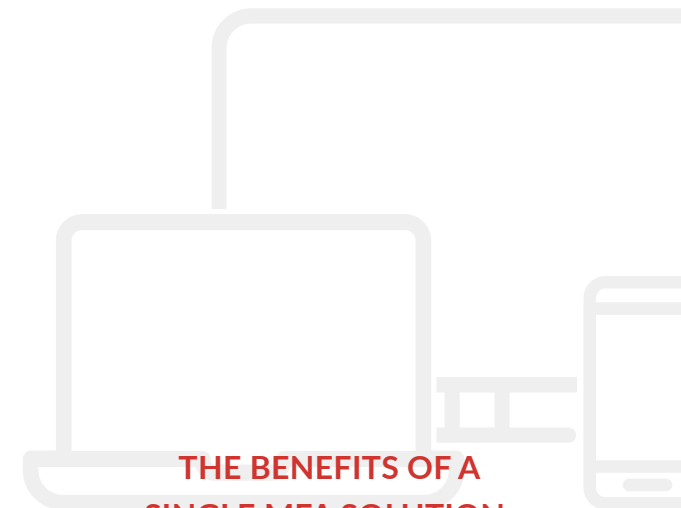
Follow these tips to provide users with the full benefits of the digital workspace, without compromising security or convenience.

TIP 3 PROVIDE SIMPLE, CONVENIENT ACCESS

Give end users a consumer-simple experience across all mobile devices and environments, while allowing only authorized, compliant users and devices access to corporate information and resources. With RSA, you can choose from a full spectrum of MFA options—from mobile push notification to biometrics— to support the widest range of user and use case authentication challenges.

THE BENEFITS OF A SINGLE MFA SOLUTION:

Ease of use for administration
Only one set of tools to manage.

Ease of use for end users
No need to navigate multiple applications for MFA.

Infrastructure and economy of scale
Maximize your MFA investment —for example, build on your investment in RSA hardware and software tokens.

TIP 4 USE A SINGLE MFA SOLUTION

Digital workspaces are great tools for managing a wide variety of applications. But because most enterprise organizations still have some resources on premises, it's best to have a single MFA solution that's flexible enough to accommodate multiple authentication types and deployment models. Ideally, you want a single solution that can protect and secure your digital workspace cloud and legacy environments.
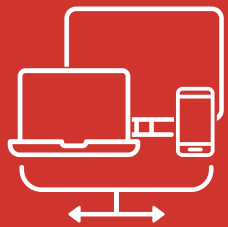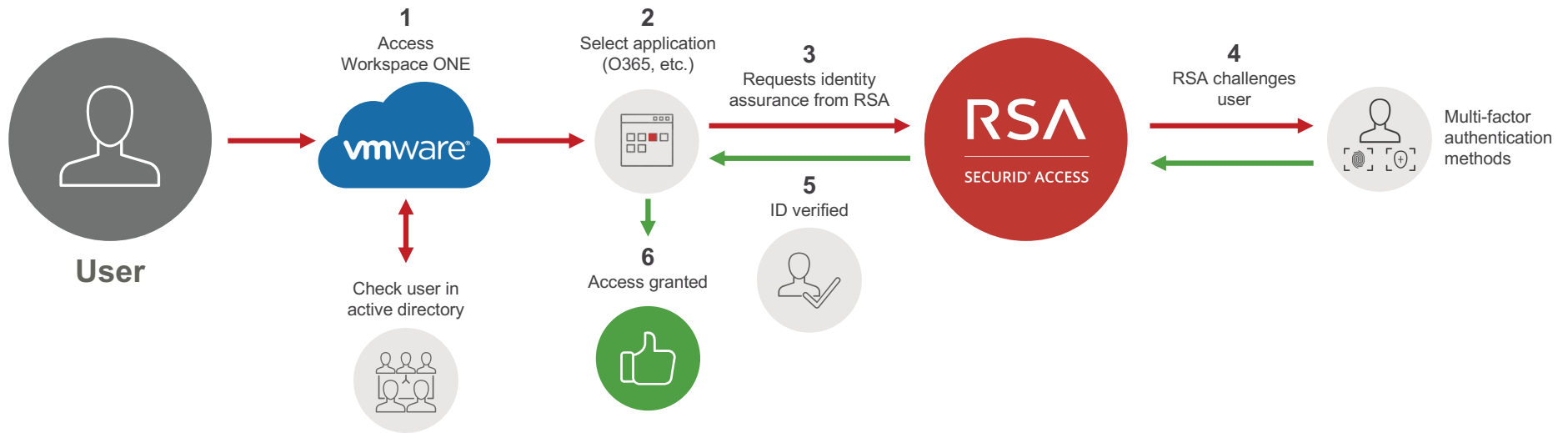
HOW IT WORKS

1 Access Workspace ONE

2 Select application (O365, etc.)

3 Requests identity assurance from RSA

4 RSA challenges user

5 ID verified

6 Access granted

User

Check user in active directory

Multi-factor authentication methods

RSA SECURID ACCESS

RSA SecurID Access enables businesses to empower employees, partners and contractors to do more without compromising security or convenience. Embracing the security challenges of today's blended-cloud and on-premises environments, bring-your-own-device trends and mobile policies, RSA SecurID Access ensures that users are who they say they are—and that they get timely, convenient access to the applications they need—from any device, anywhere.

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, visit **rsa.com**.

RSA