STRONG AUTHENTICATION FOR VDI ENVIRONMENTS

ORGANIZATIONS ARE EMBRACING THE BRING YOUR OWN DEVICE (BYOD) TREND, AND THE USE OF VIRTUAL DESKTOP INFRASTRUCTURE (VDI) SOFTWARE IS HELPING TO MITIGATE BYOD'S TRADITIONAL RISKS. WITH VDI, THE VIRTUAL DESKTOP LOADED WITH SENSITIVE COMPANY DATA AND APPLICATIONS REMAINS WITHIN THE SECURITY OF THE COMPANY'S DATA CENTER. THE DEVICE USED TO CONNECT TO THE VIRTUAL DESKTOP THEN OPERATES SIMPLY AS A REMOTE MONITOR/KEYBOARD: A THIN CLIENT THAT STORES LITTLE TO NO DATA. THE REAL RISK WITH THIS DELIVERY METHOD? VERIFYING THE IDENTITY OF THE USER FOR AUTHORIZED ACCESS TO THE VDI ENVIRONMENT.

WHO THIS AFFECTS

Organizations that recently purchased:

- A VMware View VDI environment
- A Citrix VDI environment

DETERMINE YOUR RISK

- How sensitive is the data that users access through your VDI environment?
- How are you protecting access into your VDI environment currently?
- Are you utilizing MFA to access your VDI environment?
- Are you required to comply with any regulations with regard to accessing your VDI environment?

USE CASE/ DRIVERS

- VDI mitigates the risks of allowing users to access sensitive company data using their own device
- VDI delivers user convenience and productivity and saves the company money
- Little data is stored on the endpoint device with VDI; the device simply acts as a remote monitor for the virtual desktop
- The risk of VDI is ensuring that end users are who they say they are in order to comply with regulations such as HIPAA

RSA SecurID® Access

A Complete Access Solution for On-Premises, Cloud, and Mobile

Assures Identity
Risk-based and context-aware authentication deliver security and convenience

Provides Options
A broad range of multi-factor authentication (MFA) methods support an increasingly diverse set of users and use cases

Bridges Islands of Identity
Provides consistent visibility and enforces access and authentication policies across cloud, mobile, and on-premises applications

Enables the Business
Seamlessly connects users to all of the resources they need most — anytime, from anywhere, with any device

Preserves Existing Investments
Benefit from a cloud and mobile access product that integrates with your existing on-premises security solutions including RSA Authentication Manager and web access management solutions

VISIT RSA.COM/TRYSECURID TO SIGN UP FOR A FREE TRIAL

RSA

BE SECURE IN THE KNOWLEDGE THAT RSA SecurID ACCESS:

PROVIDES
World-leading two-factor authentication

PROTECTS

- 25,000+ organizations
- 55 million users

EXTENDS SECURITY

- Cloud
- Mobile
- BYOD
- Web Portals
- Traditional VPNs

CONTROLS ACCESS
Based on the context or risk of the situation

DELIVERS
Convenient and secure access for any user, from anywhere, to anything

LEARN MORE
RSA.COM/ACCESStheSOLUTION

THE RSA SOLUTION

RSA SecurID Access:

- Integrates two-factor or multi-factor authentication (2FA or MFA) with leading VDI solutions
- Provides multiple authentication options for an extra layer of protection over user credentials:
  - Hardware, software, and mobile-optimized, authenticators, risk-based authentication
  - NEW! Mobile push and biometrics authentication capabilities
- Ensures that credentials are secured and access is granted only to authorized users

TECHNOLOGY/ INTEGRATION DETAILS

RSA SecurID Access provides:

- Market-leading 2FA and MFA with authenticators for every use case
- More than 500 tested, out-of-the-box integrations with on-premises and cloud-based applications for a seamless integration process and end-user experience
- For the full list of more than 500 integrations visit rsa.com/integrations

SECURE ACCESS CAN'T WAIT.
VISIT RSA.COM/CONTACTUS
GET THE CONVERSATION STARTED.