STRONG AUTHENTICATION FOR THE MOBILE WORKFORCE

THE PORTABILITY OF TODAY'S MOBILE DEVICES, WHILE CONVENIENT, PRESENTS A HOST OF UNIQUE RISKS THAT INCLUDE PHYSICAL LOSS OR THEFT, OR THE THEFT OF CREDENTIALS DURING A SESSION ON AN UNSECURED WIFI NETWORK. THE RESULTING ACCESS TO UNPROTECTED CORPORATE AND CUSTOMER DATA STORED ON THE DEVICE, OR TO CORPORATE SYSTEMS THROUGH THE VPN GATEWAY, CAN BE THE OPEN DOOR A CRIMINAL NEEDS TO ENTER YOUR NETWORK UNDETECTED AND MOUNT A SUCCESSFUL ATTACK.

WHO THIS AFFECTS

Organizations that:

- Recently implemented or currently are implementing a notebook/laptop rollout
- Are purchasing full-disk encryption for their mobile devices/notebooks
- Are rolling out "bring your own device"
  - e.g., smartphone, tablet
- Allow partners or customers to use their own devices to access the network

DETERMINE YOUR RISK

- How do you protect mobile user connections to your corporate data/systems today?
- Beyond username/password, do you have security practices in place to confirm the identities of your mobile users?
- Do your mobile users have access to sensitive customer or company information?
  - What impact/risk is tied to this data being compromised?
- Have you looked into MFA technology to protect your mobile user access?

USE CASE/ DRIVERS

- Employees carry their mobile devices that
  - Store customer data and proprietary company information
  - Provide access to the company's network and systems through a VPN gateway
- Local data and network access are exposed to a higher risk of being compromised if the mobile device is stolen or lost, or if the user's credentials are stolen during an unsecured WiFi session

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:

- Provides leading two-factor or multi-factor authentication (2FA or MFA)
- Offers multiple authentication options:
  - NEW! Mobile push and biometrics authentication capabilities
  - RSA SecurID Authentication Agent for Windows replaces vulnerable passwords with industry-leading 2FA
  - Hardware and software tokens secure VPN gateway access
- Ensures 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:
  - Hardware tokens, software tokens, riskbased authentication, mobile authentication, biometric, device-inherent technology such as TouchID
- RSA SecurID Authentication Agent for Microsoft Windows:
  - Identifies users positively before granting them access to valuable corporate resources accessed through Windows-based desktops and networks
  - Delivers a simplified and consistent user login experience

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