STRONG AUTHENTICATION FOR VIRTUAL PRIVATE NETWORKS (VPNS)

TODAY'S BUSINESS ENVIRONMENT IS MADE UP OF A VARIETY OF USERS, INCLUDING EMPLOYEES, CONTRACTORS, VENDORS, AND PARTNERS. REMOTE ACCESS GATEWAYS SUCH AS VPNS AND FIREWALLS PROVIDE CRITICAL ANYWHERE-ANYTIME ACCESS TO THE COMPANY NETWORKS AND RESOURCES THESE USERS REQUIRE IN ORDER TO DO THEIR JOBS. THE EMERGENCE OF IDENTITY AS A MAJOR THREAT VECTOR PLACES A PREMIUM ON ENSURING THAT THIS REMOTE ACCESS IS SECURE.

WHO THIS AFFECTS

Organizations that:

- Have purchased VPNs/firewalls recently to enable remote user access
- Have VPNs/firewalls in place
- Are not using two-factor authentication (2FA) to protect this access (i.e., are still only using usernames and passwords)

DETERMINE YOUR RISK

- Do you have remote users (employees, vendors, contractors, audit teams, etc.) that access your organization's sensitive information?
  - How are they accessing this information?
  - How do you secure access for these users?
  - How do you ensure these users are who they say they are?
- Do you leverage strong authentication, 2FA, or MFA for remote access?
- Are there regulations that require you to have 2FA or MFA for your network access?
- What type of resources would you want to improve security around user access?

USE CASE/ DRIVERS

- Mobile and remote users rely on remote access technology to connect to the corporate systems/information they need to do their jobs
- "63% of confirmed data breaches involved leveraging weak/default/stolen passwords"*
- Username and passwords are not enough and expose systems and data to cyber threats
- Many industry and federal regulations require 2FA or MFA for remote access

* 2016 Verizon Data Breach Investigations Report

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:

- Allows organizations to secure remote access gateways (VPNs, firewalls, etc.) with 2FA or MFA
- Mitigates risk by securing credentials and granting access to authorized users only
- Analyzes context to prompt users for step-up authentication as needed
- Offers authenticators for every use case:
  - Hardware, software, mobile-optimized a uthenticators, risk-based authentication
  - NEW! Mobile push and biometrics authentication capabilities

TECHNOLOGY/ INTEGRATION DETAILS

- RSA SecurID Access integrations include:
  - Cisco
  - Juniper
  - SonicWALL
  - F5
  - Palo Alto Networks
  - CheckPoint
  - SAML, WS-FED, HTTPS-FED
- For the full list of more than 500 integrations visit rsa.com/integrations and select RSA SecurID
- Access under “Tech Integrations by RSA Product”

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