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
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 authenticators, 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.