Enhance Remote Access Security With Multifactor Authentication and Access Management

Published 6 May 2020 - ID G00724227 - 22 min read

By Analysts Ant Allan, Michael Kelley, Rob Smith

The COVID-19 pandemic has suddenly hastened the move toward remote work and thus the need to implement secure remote access for large workforce populations. Security and risk management leaders should invest in MFA and access management for all kinds of remote access, and plan for rapid scaling.

Overview

Key Challenges

- Secure remote access to on-premises and cloud applications requires identity and access management (IAM) controls that a VPN, virtual desktop infrastructure (VDI)/desktop as a service (DaaS), zero trust network access (ZTNA) or cloud access security broker (CASB) alone cannot provide.
- Multifactor authentication (MFA) is an essential control to establish trust in a remote user's identity and reduce account takeover (ATO) risks, but it is difficult to rapidly provision robust MFA options at scale.
- Modern access management (AM) tools represent the future for remote worker access, but legacy applications represent a significant hurdle to the workforce of the future.

Recommendations

Security and risk management (SRM) leaders responsible for identity and access management should:

- Liaise with other SRM and infrastructure and operations leaders to determine remote access requirements and to identify what remote access tools are and will be used.

- Implement or expand use of MFA across all remote access use cases. Enable out of band (OOB) SMS as an interim solution only; migrate users to mobile push or hardware tokens, prioritizing by risk. If using OOB SMS is unavoidable, seek compensating controls.

- Standardize on modern identity protocols — Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and OAuth — for single sign-on (SSO) to securely provide access for remote workers to applications and data.

- Categorize critical applications according to support for modern identity protocols, and enable legacy web apps with identity-aware proxies (properly secured) and agents.

- Follow the “response, recovery, renewal” action plan to address MFA and AM requirements during the COVID-19 pandemic and subsequently.

Strategic Planning Assumption(s)

Through 2021, enterprises that rapidly expand remote access without implementing MFA will experience five times as many ATO incidents as those that use MFA.

Introduction

Occasional or permanent remote work is increasingly the norm for a large part of the workforce in many enterprises and can be supported via a range of technologies including VPN, ZTNA and CASB.

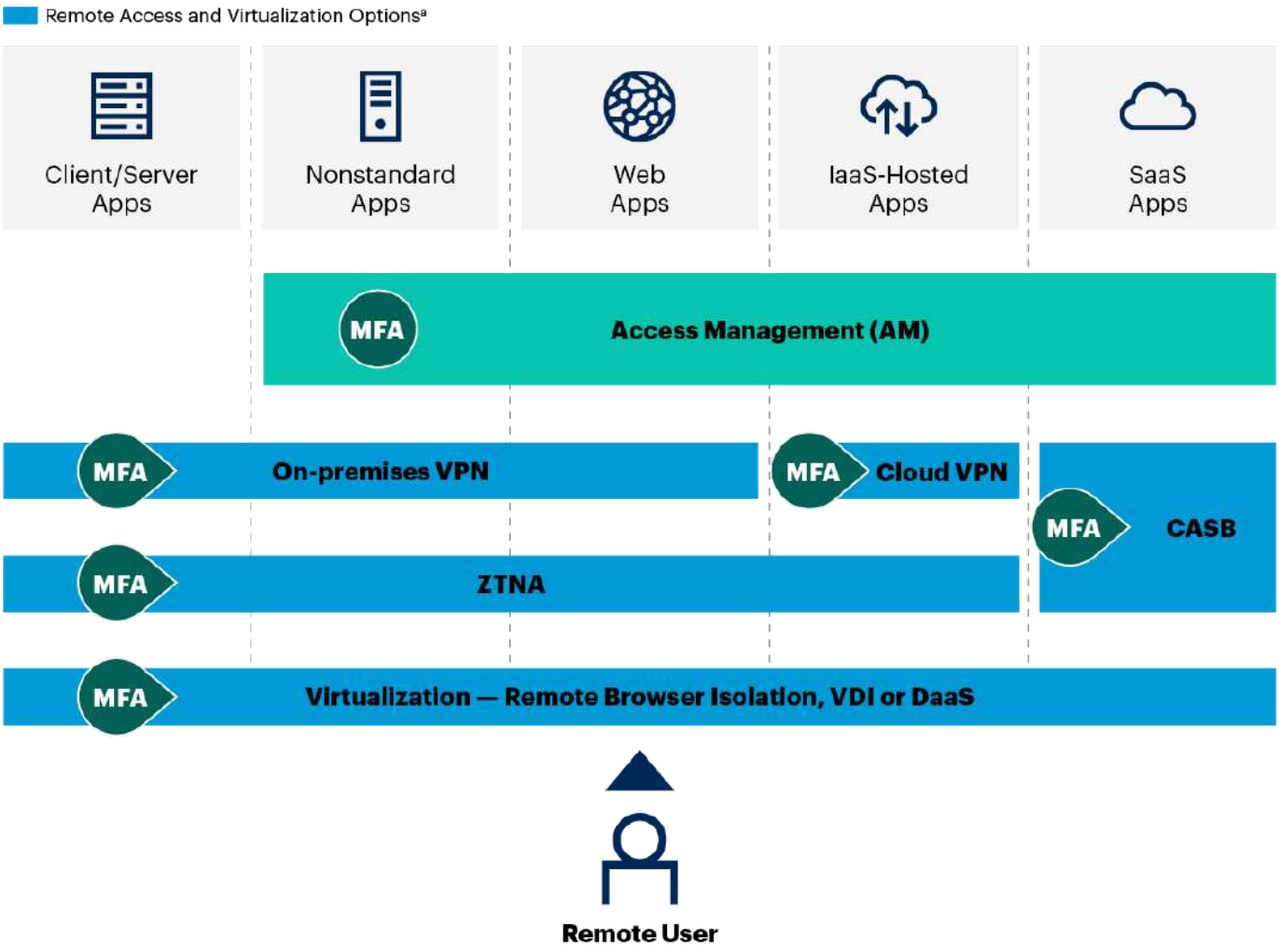
However, secure remote access to on-premises and cloud applications requires IAM controls that these tools cannot natively provide. Now, the COVID-19 pandemic has suddenly created a demand for remote work at unprecedented scale.

Thus, there is an urgent need to rapidly expand the use of MFA for any kind of remote access and, particularly for SaaS and other public cloud access, to enforce additional corporate controls using an AM tool.

What can SRM leaders responsible for IAM (“IAM leaders”) do to address these needs? This research offers IAM leaders technology and policy guidance for enhancing remote access security through MFA and AM (see Figure 1).

Figure 1. MFA and AM for Remote Access

MFA and AM for Remote Access



Source: Gartner
[a] see "Solving the Challenges of Modern Remote Access" (G00722990)

724227_C

Analysis

Determine Remote Access Requirements and Tools

One of the largest mistakes Gartner sees organizations make when enabling any remote access technology is not defining requirements before purchasing and deploying products.

This often results in poor performance, user dissatisfaction, and lesser security as users try to circumvent deployed security solutions in order to have better usability.

To mitigate this, we recommended building user personas based on the following four variables:

1. Who is the user and what is their job function? All users are not equal.

- Executives and mission-critical employees, as well as those who have intense data analysis needs, may require more bandwidth than an average user who simply checks email.

2. What kind of device is being used and who owns it? Usability and security vary widely across the universe of devices. A corporate-owned PC is much easier to secure than a personally owned smartphone.

3. What kind of applications and data do users need to access and are these applications and data located on-premises or in the cloud?

   - For example, for users accessing only SaaS applications, an always-on VPN to the corporate network delivers poorer performance than direct access via a CASB.

4. Where in the world is a user located? A wide array of data security, labor, and privacy laws spread across countries and local jurisdictions complicates offline data storage choices.

Once user personas have been defined, it is possible to decide among the remote access and virtualization options illustrated in Figure 1 (see "Solving the Challenges of Modern Remote Access").

Implement or Expand Use of MFA

Given the greater exposure to phishing attacks and stolen passwords in all remote access scenarios, MFA is required to establish trust in a user's identity and reduce ATO risks.

Smartphone apps and other phone-as-a-token methods can be quickly rolled out to new remote workers; OOB SMS modes are easiest to ramp up, but are not as secure as other approaches.

Choosing Among Common Authentication Options

Most MFA and almost all AM vendors offer phone-as-a-token methods or one-time password (OTP) hardware tokens that are used in addition to legacy passwords. These methods dominate across many market segments and use cases.

Many enterprises are still using legacy OTP hardware tokens such as RSA SecurID, typically when their needs are limited to remote access via VPN to the corporate network by a fraction of their workforce.

However, hardware tokens tend to be costly to procure and distribute, more so the more widely users are spread geographically. Clients tell us that people don't value these tokens and can readily share them.

The limitations of hardware tokens are felt even more keenly in enterprises that are scaling up the use of SaaS apps and extending remote work to the majority of the workforce.

Thus, over the past 10 years or more, IAM leaders and other buyers have increasingly preferred phone-as-a-token methods for most, if not all, of their workforce needing MFA for remote access.

There are several different phone-as-a-token options, the most common of which are:

- OOB authentication, in which users and authentication servers exchange authentication information across a different channel from that between endpoints and servers via:
  - Automated voice calls
  - SMS text messaging
  - Push notification via a smartphone app
- OTP apps for smartphones which emulate legacy OTP hardware tokens

Legacy OOB SMS and voice modes are the least secure and have been compromised by a variety of attacks. Most of these have been in retail online banking, but workforce remote access is not immune.

Gartner clients increasingly prefer OTP-less OOB push ("mobile push") modes, which are more secure than OOB SMS and voice modes and have better user experience (UX) than OTP apps.

The need to use a smartphone for mobile push can be problematic when users don't have corporate phones; some people (typically 5% to 15% of the workforce among North American clients) might not be willing to use their personal phones.

The common robust alternative to mobile push modes are OTP hardware tokens. Clients increasingly prefer Yubico YubiKeys to legacy display tokens for their portability and UX, and these are widely supported.

FIDO Universal Second Factor (U2F) and FIDO2 security keys (from FEITIAN Technologies, Google and others, as well as Yubico) are another alternative that offers improved security, but is less widely supported.

Note that enrolling users for any additional factor requires more robust identity corroboration than authentication using the AD password that will typically be used in conjunction with that method for MFA.

Supporting Rapid Scaling of Remote Access

Quickly scaling up MFA deployments to support a sudden shift to remote access in response to the COVID-19 pandemic or any mundane business continuity scenario poses many challenges.

Few if any enterprises will maintain an inventory of tokens to support such a contingency and quickly procuring tokens at volume will be difficult. This becomes impossible in the face of international crises.

It's much easier to scale up use of phone-as-a-token methods. OOB SMS is easiest: All that's needed is knowledge of the users' mobile phone numbers, likely already on record as their emergency contact numbers.

If not all users have mobile phones, landlines can be used with OOB voice modes, and, where telcos offer text-to-speech services, with OOB SMS modes. Some users might still need OTP hardware tokens.

But, while OOB SMS (and voice) modes can be quickly scaled up, the weakness of these modes means that this should be regarded only as an interim solution and replaced when the need extends beyond two weeks.

Migrate users to mobile push or hardware tokens, prioritizing by risk. Among other classes of users, senior management and business users with access to sensitive and critical systems should be quickly migrated.

A further option is to use OTP software tokens for Windows PCs. These are not as widely used as the methods discussed above, as they are less transportable and less secure; nor are they as widely available.

Nevertheless, for people who will be permanently working from home from a corporate laptop, they might provide an acceptable level of trust and protection from ATO attacks, at least on a temporary basis.

System administrators and other IT staff with privileged access should already be using MFA. If not, implement robust MFA methods straight away; OOB SMS is strongly deprecated here.

If use of OOB SMS persists for some low-risk users in the longer term, note that users' mobile phone numbers are now security-sensitive, so change procedures, including self-service, need to be made more robust.

Whatever methods are used, rapidly scaling up MFA can have significant cost implications. However, some vendors allow temporary increases in usage at no cost and others are willing to defer subscription increases.

In response to the COVID-19 pandemic, several vendors are offering free "introductory" periods. See the Consider MFA and AM Vendors' Free or Low-Cost Options section for more details.

Taking Advantage of Conditional and Adaptive Approaches

Conditional and adaptive access approaches provide a way to skip MFA and reduce friction for users while still mitigating ATO risks.

Tools evaluate a variety of contextual or other signals that can increase (or decrease) confidence in a claimed identity. For example:

- Rule-based approaches provide conditional access at login, typically based on location, network or device identity: Can the person bypass a prompt for MFA (typically, just the second factor: "+1FA")?
- Analytics-based approaches dynamically evaluate a richer set of signals throughout a session (i.e., not just at login) to enable continuous adaptive responses (e.g., step-up authentication).

Many AM tools support conditional access (the term is explicitly used in Microsoft Azure AD Premium), and some support full-blown continuous adaptive access.

ZTNA tools implement conditional access by default, as part of the zero trust approach. In addition, some tools use cryptographic tokens to provide device identity, which might qualify as a "hidden" second factor.

Some ZTNA tools remain in-line for the duration of the session to provide adaptive access.

Some stand-alone MFA tools support conditional access, although most evaluate only recognition signals, unbalanced by risk signals, and lack visibility throughout a session needed for continuous adaptive access.

While the UX benefits of these approaches have clear advantages in strategic remote access projects, they might seem an unnecessary sophistication for contingent remote access deployments.

However, given that most people in contingent deployments will be working from home using a known device, even conditional access can minimize the need for MFA, and ameliorate an additional scaling hurdle.

For any long-term contingencies, as well as planned remote access deployments, full continuous adaptive access, consuming behavior analytics and anomaly detection, provides more resilience.

Tinkering With Password Policies and Password Reset Procedures

Remote access should not depend on passwords alone but all the MFA options discussed previously are really only "+1FA," adding a single factor to a legacy password — i.e., passwords persist.

Adding a second factor does not mean that password policy can be "relaxed" in any way, because:

- Reducing password strength will reduce the overall strength of the aggregate MFA implementation.

- In the context of conditional access, lower-risk logins (e.g., from a trusted corporate network) can skip MFA, leaving the password as the only authentication factor.

- The password can persist as a single-factor in use cases where MFA is not used at all.

Ideas about what a good password policy looks like have changed over the past three years. However, many enterprises are subject to regulations or auditors requirements that enshrine traditional practices.

Remote access creates additional risks for password use and creates additional urgency for the following recommended controls:

- Implement password block-listing. Many “password policy” tools provide this, often using the same public corpus of “known bad” passwords. Some vendors build block lists based on their own analytics.

- Advise people to change their passwords whenever they have logged in from a shared public device or if they know or suspect that their passwords have been discovered.

- Set up automatic, real-time notifications to prompt an immediate password change when monitoring or analytics indicates the potential compromise of a person’s account.

This guidance should be reflected in password policies, but the new controls should be implemented as soon as possible when there’s a need to quickly scale up remote access; defer the paperwork.

Robust password reset procedures are an urgent requirement in a remote work scenario; it is harder to differentiate between attackers and legitimate users when the users are working from home.

Callback on a registered phone number is vulnerable to spoofing attacks (compare with some of the vulnerabilities of legacy OOB modes) and using security Q&A (knowledge-based verification) is woefully fragile.

A common approach in self-service password reset (SSPR) tools, less commonly used at the service desk, is to use single-factor phone-as-a-token authentication, typically using OOB SMS.

Apart from the weaknesses of OOB SMS itself (see the Choosing Among Common Authentication Options section), there’s a flaw in using a phone-as-a-token method for password reset, when the same method is being used with that password for MFA.

If attackers can compromise the phone-as-a-token method (e.g., having possession of the person’s phone), they can use it to change the password and then use that password plus the phone for ATO.

Gartner projects the use of independent identity proofing tools for SSPR and service desk calls, and other “identity recovery” events. But few tools are geared for enterprise use yet and few enterprises use them.

Our interim recommendation is to use corroboration methods that are independent of MFA methods and their components and to combine orthogonal channels, despite the overheads and UX penalties.

Provide Secure Remote Application Access Through AM Tools

AM tools facilitate SSO to cloud (SaaS) and on-premises (internal) resources, and can help provision accounts (see “Critical Capabilities for Access Management” for a full functional description).

Modern identity protocols like SAML, OIDC and OAuth 2.0 provide a secure SSO mechanism for workforce users to remotely access SaaS and internal applications in lieu of a VPN.

System for Cross-Domain Identity Management (SCIM) can provide a uniform open-standards approach for identity provisioning for applications.

Using an AM tool for central policy management and control of applications enables IAM leaders to leverage additional security controls including contextual and adaptive access and MFA.

Enterprises have a choice for how they leverage SSO for remote workers. Alternatives include:

- Advertising a portal from which staff can access SaaS and internal applications and be seamlessly logged on without having to authenticate multiple times.
- Using application-initiated SSO, which redirects the user to the identity provider (IdP; i.e., the AM tool).

Using AM to Provide Better Secure Than VPN or VPN Alternatives

VPN essentially provides “wire” access: A user is joined to the network just as if they were accessing the network from a PC in their workplace, potentially exposing all assets on the internal network.

However, by providing access via an AM tool, only applications a user is authorized to access are visible to the user. Thus, other applications are not exposed, reducing the attack surface for remote access.

AM tools become the root of trust and attest on behalf of a user requesting access to an application. Essentially, the application “outsources” authentication to the AM tool, which specializes in authentication.

After the AM tool authenticates the user, it is then responsible for providing the user with secure access to the applications for which it manages access.

That secure access typically uses encrypted single-use tokens, which is far more secure than password- based application login. IAM leaders should adopt modern identity protocols, specifically:

- SAML, which has been used for secure access to applications on the internet for nearly a decade.
- OAuth2.0 and OIDC, which are more modern and flexible API-based approaches.

When securely implemented, these protocols can mitigate security concerns like ATO and inappropriate access, because they use tokens constructed specifically for that user, that application and that session.

Password vault and forward can be used as an exception for difficult applications (i.e., those don't support modern identity protocols), but it is unsecure and thus strongly deprecated.

Focusing on Applications: The Key Consideration for an SSO Project

The success of providing secure application access to remote users is the ability to integrate required applications into the AM tool.

Many AM tools have catalogs of common applications that have been preintegrated for SSO; those are helpful for popular applications like Concur and Workday.

However, application integrations can be challenging, and in providing secure remote access to users, IAM leaders must prioritize:

- First according to business need (all applications required to support remote work).
- Then according to the three categories of applications, in the order as discussed below.

IAM leaders should feel confident in publicly exposing applications on the internet using this framework. But there are a number of considerations on the application side that must be accounted for.

Understanding the architecture of the applications will drive decisions for both vendor selection and implementation. Divide the applications that remote users need access to into these three categories:

1. "Standard" web applications; HTML-based applications that can communicate via open identity protocols (such as SAML, OIDC and OAuth) as part of fully federated SSO.
    - Many, but not all, SaaS applications fall into this group, as do many software-delivered applications. These apps are simple for AM platforms to integrate.

2. “Nonstandard” web applications; HTML-based applications that *can’t* communicate via open identity protocols.
    - These applications require “translators,” proxies or agents, which can help the application communicate with the AM tool.
    - Although doable, these application integrations take time, and SRM leaders must explore the proxy and agent capabilities of AM tools when choosing a vendor.
3. Legacy applications; for thick-client or Lightweight Directory Access Protocol (LDAP)-based applications, proxies and agents are limited, although some applications will accommodate them.
    - The best strategy is to plan an eventual retirement of the application in favor of a standard web application.
    - Another possibility for legacy applications is to modify the application to accommodate modern identity protocols.
    - Password vault and forward for these applications is also an alternative, but, for the reasons outlined earlier, should be used only as a last resort.
    - Other technologies such as ZTNA and VDI can enable secure access to these types of applications.

Using Session Management Along With MFA to Improve UX

Session management can loosely be thought of as a time-limited relationship between a user, the AM tool (as an IdP) and an application.

The IdP is essentially a butler, with keys to all the applications. So once a user authenticates to the IdP, the IdP will provide secure access through access tokens, without reprompting for credentials — classic SSO.

The IdP sets time-limited sessions with applications for that user by issuing time-limited tokens. Once that user’s session has expired, the IdP will have to reauthenticate that user, and generate a new access token.

Traditionally, using MFA for applications was onerous for users as they would be presented with an MFA challenge for each application they accessed.

However, by coupling MFA with session management, once the user successfully authenticates, the IdP will now have a set of MFA-authenticated credentials to provide to any application requiring MFA.

Thus, just as SSO reduces the overhead of multiple logins in the first place, coupling MFA with SSO likewise provides strong authentication for all applications that require it, without additional user impact.

Supporting Rapid Scaling of Access Management

There are a number of challenges for quickly scaling up AM to support large numbers of remote workers. Whether in response to the COVID-19 pandemic or in response to any other business-interrupting disaster.

From a licensing perspective, SaaS AM tools are somewhat simple: An IAM leader needs only expand the enterprise's subscription to cover the new pool of remote users.

For software-delivered solutions, additional infrastructure (physical or virtual servers) may be necessary, along with additional licenses for the new users.

As noted previously, application integrations are the largest component of success for remote work, and those integrations can take considerable time and effort.

Prioritize "standard" applications: many will be already available in an AM tool's catalog of preintegrated applications. If not, they are simpler and quicker to integrate than other types of applications.

Next, consider which "nonstandard" applications are business-critical and use proxies or agents to integrate those applications for SSO and MFA. This may mean acquiring additional components from the AM vendor.

For some nonstandard applications, password vaulting and forwarding is the only option for SSO. Treat these as exceptions and mitigate the security risk by always requiring MFA for access to these applications.

Finally, given that remote access can be less secure, assess signals such as geolocation, time and device information to provide context for access decisions and to increase confidence in the user's identity.

In responses to the COVID-19 pandemic, several vendors are offering free "introductory" periods. See the Consider MFA and AM Vendors' Free or Low-Cost Options section for more details.

Understanding the Necessary AM Components

At minimum, to provide secure remote access to SaaS and internal applications, these components are required: An identity repository (a modern directory solution), SSO, MFA and session management.

In addition, depending on the makeup of the application portfolio, there might be a requirement for an identity-aware proxy for nonstandard applications (see "Magic Quadrant for Access Management").

Consider MFA and AM Vendors' Free or Low-Cost Options

Several MFA vendors already offer free time-limited extensions to product licenses or subscriptions, enabling customers to extend MFA to larger populations in business continuity situations.

In the current crisis, where many enterprises unexpectedly have to support remote work, several vendors in the market are newly offering "free" time-limited access to their MFA or AM services.

Gartner has also seen vendors providing free time-limited upgrades to premium services, specifically those including conditional access, as a way of limiting the need to provision everyone for MFA initially.

Once the time has expired, customers are expected to begin paying for the services or stop using them.

Even given the urgent need for MFA or AM, IAM leaders should choose a vendor in the same way as in a planned selection process: Define an RFP and weigh vendors against your needs.

By taking this approach, an AM leader can make a more confident decision about continuing to use that service once the "free" period is over, taking account of the residual change in remote working patterns.

In many enterprises, IAM leaders will likely need to plan for a new normal, where the number of remote workers will fall from crisis levels but remain rather higher than it was prior to the COVID-19 pandemic.

As of the date of publication of this research, the following vendors had advertised "free" offers. Note that this is not an exhaustive list.

MFA time-limited offers

- Cisco (Duo)
- Ping Identity (for existing Ping Identity customers)
- RSA

AM time-limited offers

- Idaptive
- Microsoft
- Okta
- OneLogin

- Ping Identity
- SecureAuth

COVID-19 Action Plan

Much of the guidance in this research is relevant to planned remote access needs as well as contingent business continuity needs. However, currently the urgent need for nearly all clients is driven by the COVID-19 pandemic.

Not only is the pandemic creating a business continuity need for all enterprises globally, but it will likely have longer-lasting impacts on working patterns and business models.

> **"The work-from-home genie is out of the bottle."**
>
> — *A vendor customer's IAM leader*

Table 1 summarizes the urgent first (and possibly temporary) actions, the consequent stabilizing actions and the long-term strategic, durable actions that IAM leaders should take.

Table 1: Action Plan: Response, Recovery and Renewal

Response ↓	*Recovery* ↓	*Renewal* ↓

Response ↓	Recovery ↓	Renewal ↓

■ Extend your existing MFA or use your AM vendor's MFA or choose a new vendor.
■ Implement MFA for all remote access on a risk-prioritized schedule:
  ■ Deploy mobile push or hardware tokens for new privileged MFA users
  ■ Deploy OOB SMS or voice for other new MFA users
  ■ Implement conditional access to minimize need for and user impact of MFA
■ Update password management processes to reflect remote user risks
■ Increase AM subscriptions, or add licensing/infrastructure to accommodate higher volume
■ Migrate all critical applications to the AM tool
■ If nonstandard applications are within scope, procure and deploy necessary proxies, agents, etc.
	■ Consolidate MFA for remote access, favoring the chosen AM tool
	■ Migrate users off OOB SMS or voice-to-mobile push or hardware tokens on a risk-prioritized schedule
	■ Refine conditional access policies and explore continuous adaptive access approaches
	■ Consolidate all remote access into a single AM tool for all applications; explore the additional benefits of SaaS-delivered services for AM
	■ Plan for renewal:
	  ■ Estimate long-term increases in remote workers (industry estimates are 20% to 30%)
	  ■ Account for additional subscriptions, licensing or infrastructure in budgeting and forecasting
		■ Assess postcrisis changes in working patterns and business models
		■ Focus on providing a favorable remote work experience as a competitive advantage for recruiting and retention
		■ Review strategic vision for MFA and AM across all use cases for workforce and partners (and optionally for customers) through a continuous and adaptive risk and trust assessment (CARTA) lens:
		  ■ Review MFA options to exploit new methods and alternatives such as bring your own identity (BYOI)
		  ■ Review identity recovery processes
		  ■ Identify where AM can wholly replace VPN or ZTNA
		■ Evaluate incumbent vendors against that vision and plan to consolidate; replace or add vendors as necessary
		■ Execute on your plan

Source: Gartner (May 2020)

Evidence

This research is based on hundreds of interactions with Gartner clients and MFA and AM vendors over the past few years and many interactions over the past months regarding rapid scaling of remote access.