RSA

SOLUTION BRIEF

IAM and the Hybrid Workforce

Secure, Convenient Access No Matter Where It Happens

The access management challenges the hybrid workforce presents are formidable.

How do you secure access for a workforce that's as likely to be at home or on the road as on-site?

The accelerated move to remote work in 2020 ushered in a new age in access management, with the on-premises VPN perimeter giving way to a perimeterless reality of multiple devices, multiple access points, and users connecting to resources from their own individual networks. This perimeterless reality isn't going away, as organizations allow for varying levels of remote work. The access management challenges the hybrid workforce presents are formidable: How do you secure access for a workforce that's as likely to be at home or on the road as on-site? How do you make accessing resources in the cloud as secure as accessing on-premises resources? And how do you ensure access is as convenient as possible, to maintain a positive user experience while keeping the IT support burden low? As you develop strategies to support secure access everywhere people work, the following guidelines will help.

Adopt a "least privilege" model to minimize access risk

The principle of "least privilege" has been around for years, but in today's perimeterless environment, it is more important than ever. The US Cybersecurity and Infrastructure Agency (CISA), in a document published in 2005, defined it as assigning "only the minimum necessary rights" to those requesting access. Best practices include conducting privilege audits of existing accounts, starting new accounts with the least possible privilege and enforcing separation of privileges.

Protect resources in the cloud with MFA

In addition to the rise of the remote workforce, increased use of cloud resources will continue to make secure access more challenging. Ensuring secure access to these resources starts with understanding exactly what's in the cloud; think beyond customer service and sales applications, and look at other areas like messaging and unified communication that are also likely to contain confidential, proprietary information. Protect all cloud resources containing sensitive data with multi-factor authentication (MFA), and authenticate directly to each one rather than via VPN, using single sign-on (SSO) to speed and streamline the process for users.

Take a broader view of the value of MFA

Having more than one factor of authentication is, of course, important for access security, but there is even greater value in an approach to MFA that also prioritizes user convenience. Choose an MFA solution that gives users a range of ways to authenticate easily, with minimal IT support—even when they're offline—to keep their experience positive and reduce the need for IT intervention. For example, passwordless and biometric options for authentication mean not only decreased cybersecurity risk, since there are no passwords to steal, but also greater user convenience, since there are no passwords to remember.

Lay a solid foundation for identity governance

Knowing who has access to what is critical to secure access. It's the basis for governing user identities and ultimately being able to better deliver a secure yet seamless access experience through automated provisioning and risk-based authentication. Implement a methodology to review who has access to what, as well as whether their level of access reflects what is required to do their job.

RSA: MFA and identity governance to secure access for today's remote workforce

Trusted by security-sensitive organizations around the world, RSA provides the identity management platform that empowers users to do more without compromising security or convenience, with:

- **A range of choices for how to authenticate**, with hardware, software and mobile options, to deliver the same level of secure, convenient access to remote or on-site users, in the cloud or on-premises, working on any technology platform
- **A full complement of modern authentication methods** including FIDO, push-to-approve, biometrics (fingerprint or facial recognition), "bring your own authenticator," and hardware tokens that represent the gold standard in authentication
- **A centralized platform to simplify authentication and credential management**, including unified identities, access points and applications to ensure a consistent approach
- **Capabilities to build out rules and risk evaluations** to lay the groundwork for dynamic management of access and authorization to applications, which simplifies processes for both granting access and requesting it

Learn more about how RSA can help you secure remote workforce access to critical resources on-premises and in the cloud.

About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to RSA.com.

RSA