SecurID

WHITE PAPER

5 Ways to Protect and Optimize Your Workforce

Identity and Access Management for the Hybrid Workforce

As the workforce has increasingly become a mix of on-site and remote workers, managing the risk associated with this hybrid workforce has become increasingly important. The combination of supporting more remote workers and accelerating digital initiatives has created the need for workforce optimization. Today, more than ever, you need to protect and optimize your workforce.

How can you:

- Enable the remote workforce to be both productive and secure?
- Accelerate digital initiatives by moving identity and access management to the cloud?
- Ensure that the technologies you implement today will secure your organization for tomorrow?

Here are five ways to protect and optimize your workforce.

1. Greater productivity with modern MFA

To enable remote workers to be productive, you have to make authentication simple, frictionless and easy to manage. People who are working from home want to use devices and login options that they're accustomed to using in their personal lives, such as biometrics (fingerprint or facial recognition) and FIDO authentication. As your organization adopts new authentication methods, however, you need to ensure devices are both safe and easy to manage. Look for:

- **Flexibility and choice.** Identity management solutions should support a wide variety of modern multi-factor authentication (MFA) methods to address the organization's appetite for risk, as well as different worker requirements. Some methods, such as biometrics, may be better suited to mobile device users with limited resource access. Other methods, such as hardware authentication, may be better for a scenario such as addressing increased security for privileged users.
- **Frictionless experience.** Workers today are likely to be using both software-as-a-service (SaaS) and on-premises applications, rather than one or the other. The experience of moving between them therefore needs to be seamless to increase productivity.
- **Self-service.** Enabling workers to handle onboarding tasks and emergency access requests on their own, without help from IT, increases convenience and saves time. It also improves productivity and saves on IT costs.

2. Broader protection for ubiquitous coverage

The perimeter that once protected sensitive data, applications and other resources is disappearing now that many workers who once worked on-site have gone remote. This makes it difficult to ensure that people who seek access to those resources are who they say they are, introducing more risk. Look for:

- **Ground-to-cloud coverage.** Modern organizations need to protect logins for web-based and SaaS applications, but it's also important to remember that many organizations still rely on on-premises and legacy applications for many of the systems that workers access. Identity and access management capabilities should cover all applications and make the experience seamless for users.
- **Detect abnormalities.** Solutions that offer conditional access based on contextual or behavioral analysis provide greater protection across endpoints, reducing the risk associated with authenticating users from unknown locations, devices and networks. By automating and detecting abnormal user and machine activities, as well as network anomalies, organizations can enrich authentication policy decisions.

3. 24x7 online and offline availability

The cloud provides many conveniences, such as automatically updating software with the latest features and functionalities. It's also where many of the applications that workers need to access are hosted. But what happens if access to the cloud slows or goes down? Similarly, how do users log in when there's no internet connection? And if access is granted, what assurance is there that users are who they say they are? Look for:

- **Convenient cloud services backed by on-premises assurance.** Reliability is critical for remote workers to access applications, and always-on security is critical to alleviating organizational risk. With a hybrid identity management approach, organizations can enjoy the benefits of the cloud combined with the availability and assurance of an on-premises system, and workers won't notice if (or when) the cloud becomes unavailable.
- **Consistency online and offline.** Authentication should not only function efficiently when a user is online but also be effective when the internet is unavailable. Seek solutions that offer offline authentication for a variety of operating systems and endpoints. This approach provides a frictionless user experience and ensures that workers are truly authenticated to sign in, even when they're offline.

4. Hybrid model to accelerate cloud adoption

Recent disruptions have likely accelerated your cloud adoption projects and digital transformation initiatives. However, if your organization's risk tolerance is low, a hybrid approach to identity and authentication management is recommended. Look for:

- **Best of both worlds.** Seek identity management platforms that include all the components for on-premises and cloud authentication. Not only does this approach enable modern MFA options and provide higher availability than cloud-only options, it also allows organizations to efficiently move to the cloud when they're ready. It's a way to save time, resources and costs—and reduce risk—while moving forward with cloud initiatives.

5. Dynamic platform to future-proof investments

The best way to optimize your workforce is to invest in solutions that solve today's challenges and provide ongoing innovations to prepare for tomorrow's opportunities. With the right solution, investments made today can be leveraged for the future, lowering total cost of ownership. Look for:

- **Broad integrations.** Flexible platforms provide connectors, application programming interfaces (APIs) and standard agents for a variety of operating systems and applications, such as Windows, macOS, Linux, Citrix and more. Vendors who have a track record of supporting a broad range of integrations will ensure you're ready for the next wave of technology adoption.
- **Continuous customer-centric innovations.** Trust identity management vendors that have the experience to advise you in an informed way as you pursue your identity journey, including sharing best practices with you. It's also important to find a vendor that provides regular product enhancements and makes it easy to upgrade to the newest capabilities.

Ready to take the next step?

Are you ready to protect and optimize your workforce? SecurID has been a trusted resource for thousands of customers of every size, across every industry, for decades. Here are just a handful of ways that SecurID can help protect and optimize your dynamic workforce.

An unrivaled hybrid approach that not only simplifies cloud adoption, but also ensures that modern authentication methods protect both cloud and on-premises resources.

The broadest range of easy-to-use authentication methods coupled with self-service options. This enables you to select the authenticators that work best for your organization and/or users, while reducing strain on IT.

Conditional access and threat-aware authentication to enhance detection of abnormal user, device and network activities inside or outside the traditional perimeter. With threat intelligence, organizations can mitigate the risk of insider threats and data breaches, and ensure strong, continuous authentication.

24x7 authentication availability and protection, and the confidence to move to the cloud.

Offline authentication for both Windows and macOS laptop users who are not connected to a network. While other solutions may provide limited offline access, SecurID ensures that users are fully authenticated to sign in, even offline. It provides truly secure access with a seamless experience.

Continuous innovations and a direct upgrade feature that enable next-generation capabilities, eliminate time-consuming multi-step serial upgrade processes, and improve total cost of ownership (TCO).

About SecurID

SecurID, an RSA business, is the trusted identity platform for 13,000 organizations around the world, managing 50 million identities and providing secure, convenient access to 30 million users. SecurID 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, SecurID connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to securid.com.

SecurID
An RSA Business