RSA

5 Ways to Protect and Optimize Your Workforce

Identity Management for the Dynamic Workforce

As workforces have become increasingly dynamic and remote, managing the risk associated with the "new normal" has become increasingly important. The combination of supporting a greater number of remote workers and accelerating digital transformation initiatives has generated the requirement for workforce optimization. Today, more than ever, you need to protect and optimize your workforce.

How can you ...

- Enable remote workers to be both productive AND secure?
- Accelerate digital transformation initiatives by moving identity 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

The surge has shone a light on the importance of enabling remote workers to be productive by making authentication simple, frictionless and easy to manage. Workers want to use devices and login options that they're used to using in their personal lives, such as fingerprint, face recognition or FIDO® authentication. As your enterprise adopts these authentication methods, however, you need to ensure devices are both safe and easy to manage.

What to 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, whereas increased security for privileged users may be best addressed with hardware authentication.
- **Frictionless experience.** It's likely that workers are accessing both software-as-a-service (SaaS) and on-premises applications, yet the experience of moving between them needs to be seamless to increase productivity.
- **Self-service.** Enable employees to be self-reliant when it comes to onboarding and emergency access services. Solutions that provide balanced credential lifecycle management can increase worker productivity and reduce IT costs.

2. Broader protection for ubiquitous coverage

The perimeter has changed now that many workers who previously worked on-site in an organization-managed location have gone remote. This increased complexity makes it difficult to ensure workers are who they say they are, introducing additional risks.

What to look for …

- **Ground-to-cloud coverage.** Modern organizations may be interested in protecting logins for web-based and SaaS applications, but it's important to remember that most organizations still rely on on-premises and legacy applications for many of the systems that workers access. Identity management systems 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 automatic updates with the latest features and functionalities. It's also where many 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?

What to 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 "no fail-open" 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.

What to look for …

- **Best of both worlds.** Seek identity management platforms that include all of 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. Save time, resources and costs while reducing risk as you drive forward 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 you for tomorrow's opportunities. With the right solution, investments made today can be leveraged for the future, lowering your total cost of ownership.

What to look for ...

- **Broad integrations.** Flexible platforms provide connectors, application programming interfaces (APIs) and standard agents for a wide variety of 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 share best practices, a vision for the future, the fortitude for regular product enhancements and the skill to make upgrades to the newest capabilities simple.

Ready to take the next step?

Are you ready to protect and optimize your workforce? RSA has been a trusted advisor for thousands of customers of every size, across every industry for decades. Here are just a handful of ways that **RSA SecurID Access**, a part of the comprehensive **RSA SecurID Suite**, can help you 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.

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

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. Recent advancements include: FIDO authentication and enhanced security with biometrics for Andriod devices.

True "no fail-open" offline authentication for both Microsoft Windows and macOS laptop users who are not connected to a network. While other solutions may provide limited offline access, RSA ensures that users are fully authenticated to sign in, even offline; it provides truly secure access with a seamless experience.

Conditional Access and Threat-Aware Authentication enhances detection of abnormal user, device and network activities inside or outside of the corporate premises. With threat intelligence, organizations can mitigate the risk of insider threats and data breaches, and ensure stronger, continuous authentication.

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

About RSA SecurID Access

RSA SecurID Access, part of the **RSA SecurID Suite**, enables businesses to empower employees, partners and contractors to do more without compromising security or convenience. Embracing the security challenges of today's blended cloud and on-premises environments, bring your own device, and mobile, RSA SecurID Access ensures that users have timely access to the applications they need—from any device, anywhere and ensures that users are who they say they are, with a modern, convenient user experience.