Microsoft Security

Guide to Seamless Secure Access:

An Improved User Experience with Strengthened Security

Strike a balance between user productivity and secure access with the right approach to identity and authentication.

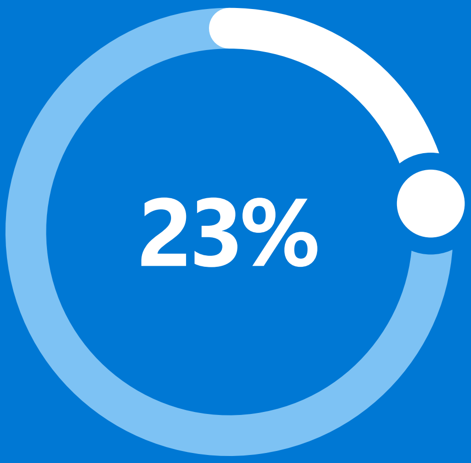
Contents

Introduction

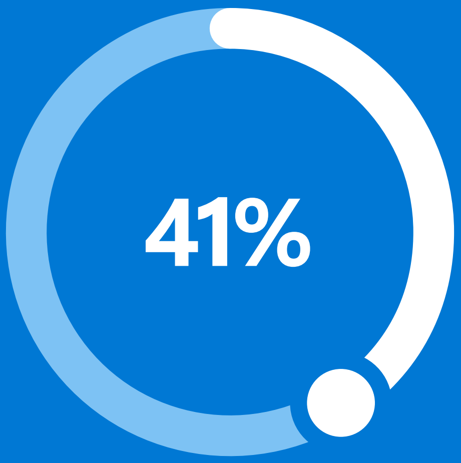
The shift to a remote workforce has caused IT and security leaders to place greater emphasis on striking a balance: They must meet user needs for seamless access to data and applications while maintaining strong security around that access.

The challenge is not going away soon. On average, CIOs believe only 23% of employees must be physically in the office for the business to be fully operational, according to the CIO Pandemic Business Impact Survey 2020. As it is, they think 41% of their workforces will permanently work remotely as of January 2021.

Organizations manage an average of 180 unique applications. At the same time, they're balancing the push and pull of modernization projects, and trying to reduce complexity for users while establishing security policies robust enough to deal with advanced threats. Adding secure remote access to the list of imperatives increases the importance of reducing barriers to productivity.



of employees must be physically in the office



of their workforces will permanently work remotely

With so many users, devices, and applications residing outside the traditional network perimeter, firewalls and virtual private networks are no longer sufficient. According to the AV Test Security Report 2019/2020, there were more than 114 million newly developed malware applications in 2019. With an average of more than 300,000 new threats appearing daily, something will eventually penetrate the perimeter.

IT needs a new approach. The Zero Trust model is an emerging path to robust security. It replaces the assumption that everything behind the corporate firewall is safe with three principles:

- ✓ **Verify explicitly**
- ✓ **Use least privileged access**
- ✓ **Assume breach**

With Zero Trust, every user, device and piece of software must be identified and authorized before communication is allowed. This approach encourages IT to take a critical view of identity and access management. With the network perimeter disappearing, identity is the control plane for security and can provide effective access control across all users and digital resources. Given that people, devices, and software are now widely dispersed for many organizations, a cloud-based model makes sense. When properly architected, a unified, cloud-based identity and authentication solution can enable strong security while providing seamless end-user experiences.

This guide examines how to provide seamless, secure access no matter where the end user is located.

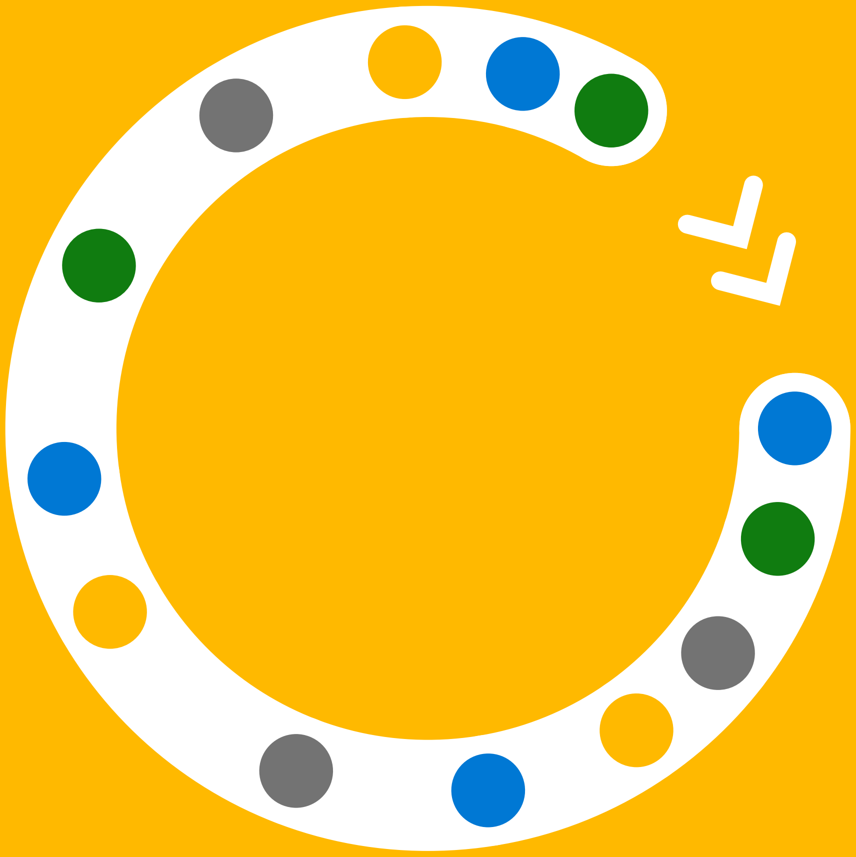
The journey takes into account:

1. **Productivity**
2. **Security**
3. **Self-service**
4. **The path to eliminating passwords**

1

Productivity

Organizations can balance security and employee productivity — and gain visibility — with the right authentication and identity verification capabilities. For example, the solution must ensure that only the right people have the right access to the right resources. This mitigates access risk by protecting, monitoring, and auditing access to critical assets.



Specifically, enterprises should seek solutions with:

Single sign-on (SSO): Users sign in once with one account to access devices, apps, and data. IT administrators should be able to easily centralize user account management, and automatically add or remove user access to applications based on group membership.

Application access: Rather than launching apps one by one, seamless access means giving users one portal from which they can easily see and open all of their apps. Even better, they should be able to personalize their app organization for easier discovery. Another important consideration is mobile access; it should be just as easy to securely access enterprise apps through a mobile device as it is from a desktop or laptop.

Access requests: In addition to auto-enrolling users in groups based on organizational policies, empower users with access requests. Simply define a safe set of apps in which users can self-enroll then make it easily discoverable from their existing app access experiences.

Guest user collaboration: Give contractors, visitors, and vendors a familiar access experience for improved collaboration. Instead of creating secondary accounts, the right access solution allows guests to use their preferred identity provider.

2

Security

Robust, frictionless security requires considerations around identity management procedures and processes. IT must be able to protect access to applications and resources across the corporate data center and into the cloud, while monitoring suspicious activity through advanced security reporting, auditing, and alerting to mitigate potential security issues. Also, consider ways to empower users to be part of the organization’s security solution by helping spot and report potential breaches to IT.

Following the Zero Trust model helps organizations achieve all of these goals.

A few important steps to take in this approach include:

Strong authentication: Verify user identities with strong authentication to verify and establish trust before granting access. Leverage multi-factor authentication (MFA) methods — such as texts, calls, biometrics, one-time passcodes, and more — to protect remote employees. Also, to aid with adoption and enrollment of MFA, allow users to register their security contact information to be shared across multiple experiences. With sufficiently strong MFA, organizations can move toward eliminating passwords for access, furthering their maturity with the Zero Trust approach.

Adaptive access policies: Enforce fine-tuned adaptive access policies, such as requiring MFA, based on user context, device, location, and session-risk information. This serves as the foundation for a robust Zero Trust strategy, where policies and real-time signals are required to determine when to allow access, block, or require additional proofs like MFA without compromising productivity.

User involvement: By giving end users the ability to review their sign-in activity, they can check for unusual behavior — such as someone trying to guess their password or a successful sign-on that they did not request. This simple step makes it seamless for users to report suspicious activity to IT.

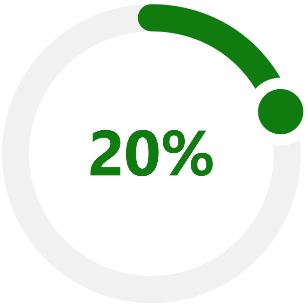
3

Self-service

Empowering users to manage their own identity not only improves their engagement with security, but it also allows IT teams to focus on more strategic security priorities. For example, giving users the ability to reset their own passwords and manage their profiles reduces friction and improves productivity.

Self-service enables IT to provide the guardrails for access, but puts the day-to-day management and security of identity in the user’s hands.

Password reset requests tend to be the largest percentage of the IT help desk workload, sometimes accounting for more than 20% of their time. With self-service password reset (SSPR) functionality, users are empowered to reset their own passwords from a web interface that can be accessed remotely. IT can also set the right level of security for their organization by dictating which forms of second-factor authentication will be required to authorize the reset.



Password reset requests tend to be the largest percentage of the IT help desk workload, sometimes accounting for more than 20% of their time.

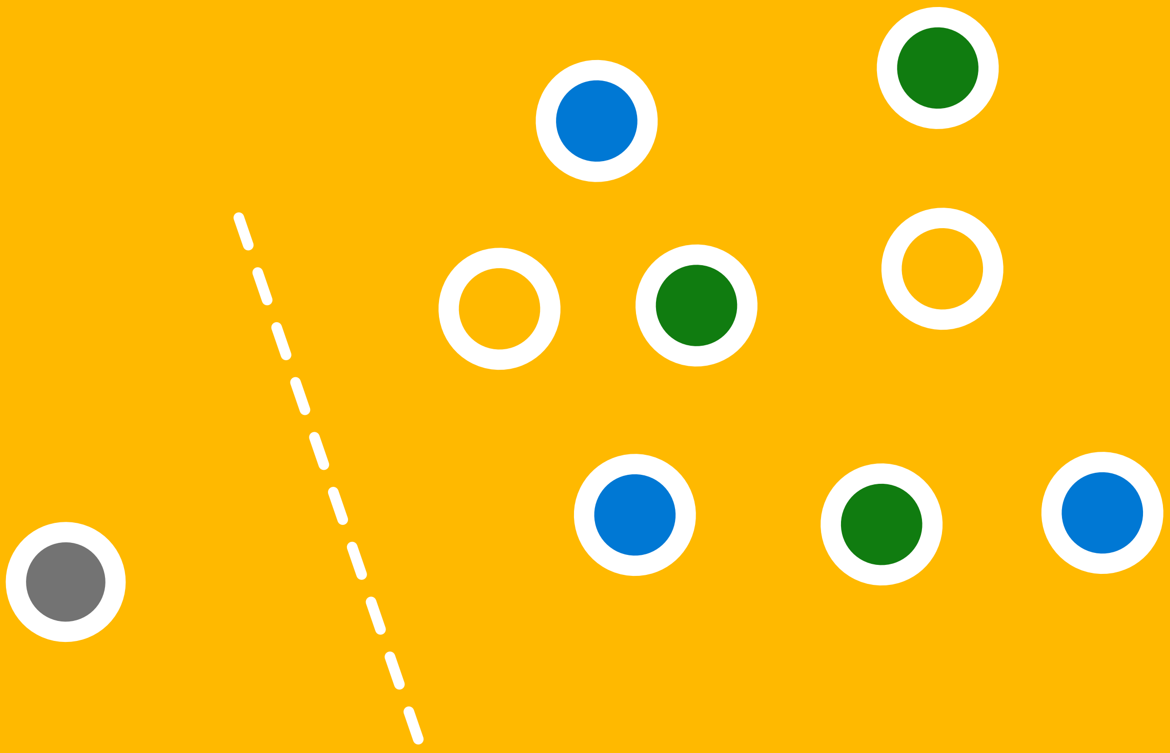
To further empower self-sufficiency and increase efficiencies, give end users the ability to manage their own identity attributes, such as resetting their security contact info, updating their authorized work devices, and reviewing sign-in information.

IT can also set the right level of security for their organization by dictating which forms of second-factor authentication will be required to authorize the reset.

4

The path to eliminating passwords

Passwords are security's weakest link. The idea of going passwordless may seem daunting, yet organizations that are already embracing seamless IT and user experiences are halfway there.



Passwordless authentication is a form of MFA that replaces passwords with two or more verification factors secured and encrypted on a user's device, such as a fingerprint, facial recognition, a device pin, or a cryptographic key. The credentials never leave the device, eliminating the risk of phishing. These alternatives are based on new technology-agnostic industry standards. No passwords are stored in the cloud. Enabling MFA blocks 99.9% of identity-based attacks.

Enabling MFA blocks 99.9% of identity-based attacks.

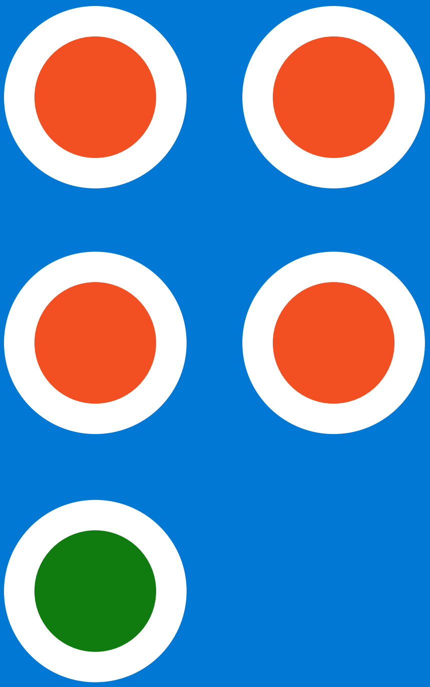
A passwordless model is a stronger and, in many cases, less cumbersome method of authentication since there are no passwords for users to memorize. After all, four in five cyberattacks involve the use of stolen credentials, according to the Verizon 2020 Data Breach Investigations Report.

While moving to passwordless authentication offers improved security and a better user experience, it requires both IT and end users to adopt a new way of thinking about security.

First step: Start with a low-risk group, explaining the benefits of eliminating passwords. Deploy MFA with a passwordless authentication option until individuals are comfortable. Then, in the background, begin replacing passwords and dependencies while continuing to educate users about the new identity solution.

4 in 5

hacking-related breaches use stolen or weak passwords.



— Verizon 2020 Data Breach
Investigations Report

Summary

A unified approach for authentication and identity provides a seamless, simple experience for users while ultimately strengthening overall security. It's a best-of-both-worlds situation: Seamless remote access for increased productivity and collaboration, while maintaining strong security.

Especially in the constantly evolving and increasingly digital workspace, organizations must increasingly protect users, data, and applications — no matter where they exist. Yet, simply adding more controls makes security harder. The right cloud-based access and identity solution matches today's digital reality with the ease of access users require to get work done and the business's need to maintain strong security.

Especially in the constantly evolving and increasingly digital workspace, organizations must increasingly protect users, data, and applications — no matter where they exist.

Delivering seamless user access and strengthened security

Microsoft Azure Active Directory (Azure AD) is a complete identity and access management solution that helps protect employees, customers and partners from cybersecurity attacks.

Whether individuals are on site or working remotely, Microsoft Azure AD enables secure and seamless access to all apps — ensuring productivity from anywhere. The solution, which manages more than **345 monthly active users** and processes over **30 billion authentications** every day, enables enterprises to provide key functionalities including:

- ✓ Workflow automation for user lifecycle and provisioning
- ✓ Self-service management
- ✓ Single sign-on
- ✓ Integration with over 3,300 software-as-a-service (SaaS) applications
- ✓ Strong authentication and risk-based adaptive controls
- ✓ A single solution to secure and manage customers and partners beyond organizational boundaries

For more information, visit microsoft.com/azuread

Microsoft