



SECURE



Why Multi-Factor Authentication Demands Single Sign-On

Discover how adopting
single sign-on supplements
multi-factor authentication
efforts to reduce risk



The bridge to possible

Table of Contents

- 03 Introduction
 - Never assume trust – always verify
 - Moving from reactive to proactive security

- 05 Multi-factor authentication is just the start
 - MFA and SSO: Two critical components of secure access management
 - Helpful definitions

- 08 SSO: Much more than convenient

- 10 SSO and MFA: A dynamic duo
 - Together, these two defenses can help your team
 - Checklist: What to look for in an SSO solution

- 14 Duo's long-term vision for SSO
 - Frictionless secure access with SSO & MFA
 - SSO + MFA: Unlock security simplicity
 - Administration made easy

- 18 Why Duo?
 - Is Duo Single Sign-On right for you?

Never assume trust – always verify

What does it mean to operate in a zero-trust world? It means eliminating unauthorized entry points and reducing risk at every turn by first verifying the user and the health of the device they're using.

There's never been a better time for zero trust. For the last few years, organizations have been pummeled with a rise in attacks stemming from stolen credentials and weak passwords. Hackers target people because people are fallible, and because using them as an attack vector works. In 2022, 82% of breaches involved the human element.

One factor that increases cyber risk is a reliance on traditional security tools and infrastructures – siloed data and signals, manual vulnerability management tools, and antiquated access management solutions. These outdated approaches saddle organizations with a reactive security posture, leaving them to try to manage blows as they're dealt. This passive approach is a costly one, resulting in damage that can far exceed the direct cost of today's average breach. According to Cisco's 2022 Security Outcomes Report, Volume 3: Achieving Security Resilience, 40% of information security and privacy professionals around the globe reported that their organizations are grappling with lasting brand damage in the wake of a past security event.



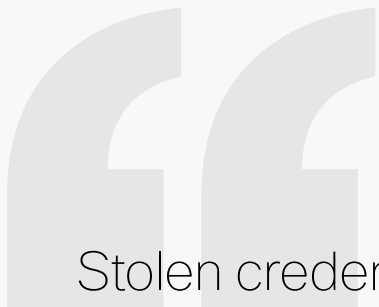
**of breaches involved
the human element**

Moving from reactive to proactive security

These painfully expensive security breaches have begun to alert organizations that it's time to adopt a proactive security strategy. Teams increasingly are implementing multi-faceted defenses to shrink their attack surface, close off potential attack vectors, and create nothing but frustration for would-be hackers. Laying the groundwork for a zero trust environment allows teams to take back much of the deciding power regarding who and what accesses their environment.

Meaningful zero trust measures often include leveraging first- and third-party threat intelligence, unearthing new opportunities for automation such as AI-driven threat detection and remediation, and evolving the old "trust, but verify" adage into "never assume trust – always verify."

In today's hyper-connected climate where every user or device is a potential thoroughfare for attackers, modern secure access management solutions are vital for resilience-minded, proactive defenders intent on getting ahead of the next attack.



Stolen credentials are involved in more than 80% of breaches from web application attacks.”

Verizon 2022 Data Breach Investigations Report

Multi-factor authentication is just the start

The use of multi-factor authentication (MFA) – which adds two or more identity-checking steps to user logins – has soared as organizations work to better protect user login credentials. For example, a 2022 analysis of more than 13 billion authentications from almost 50 million different devices found that MFA use rose 39% during a 12-month period.

Taking note in this jump in popularity, attackers are getting creative by establishing a new, highly trafficked attack vector: they're looking to bypass MFA protections themselves. With the average enterprise managing as many as 1,000 cloud applications, coupled with the rise of the hybrid workforce and the careless but common habit of reusing passwords, logins have become rife for exploits from attacks targeting MFA environments. These attacks are emerging, thanks to widely accessible tools that help hackers target authentication codes and device enrollment, and take advantage of MFA user fatigue. When threat actors use these tools, it results in headaches and laborious fixes by IT and security teams and can ultimately impact an organization's bottom line.

MFA and SSO: Two critical components of secure access management

But organizations heeding the call for security resilience are looking for ways to reinforce – rather than restrict – their MFA implementations. For them, the answer to fortifying against MFA-targeted attacks, not to mention broader efforts to steal credentials, is to strengthen MFA implementation by requiring strong and phishing-resistant authentication where possible, while streamlining access management by deploying cloud-based single sign-on (SSO) and applying application-specific access policies. With SSO, users log in once to access network resources and web applications.

This eBook examines how these two crucial elements of secure access management work together to provide organizations with even stronger authentication protection, while improving the user experience. It also outlines how Duo combines MFA and SSO into a cohesive solution that makes SSO much more than a convenience for your users, but a policy enforcement point and an essential part of a zero trust environment.



Worried about password-based and MFA-targeted attacks?

Duo integrates strong and phishing-resistant MFA options with robust, cloud-based SSO to help security teams stop password-based and MFA-targeted attacks.

Before we continue, let's make sure we're aligned on definitions.

Multi-factor authentication (MFA):

An access security product used to verify a user's identity at login by adding two or more identity-checking steps via secure authentication tools. Traditional MFA relies on something you have, like a mobile device, and something you know, like a password, to verify your identity

Phishing-resistant authentication:

A form of authentication immune to different types of phishing attacks such as spear phishing, brute force attacks, man-in-the-middle attacks, replay attacks, and credential stuffing. One common example is a Fast Identity Online (FIDO) security key, a small device or application that enables two-factor authentication and binds the user login to the origin, mitigating phishing risks.

Passwordless authentication:

A method of verifying a user's identity without use of a password; passwordless login still uses something you have (like traditional MFA), but it replaces the password with something you are, like a biometric such as a fingerprint or face ID. Passwordless authentication still uses two factors to verify identity, but both factors can be established in a single gesture – simply by picking up a device and performing the swipe or scan needed to verify your identity.

Single sign-on (SSO):

An authentication process that provides users with one easy and consistent login experience across all applications, eliminating the need to supply user credentials with every application or access request.

Zero trust:

A comprehensive approach to secure all access across your applications and environment, from any user, device, and location, allowing you to mitigate, detect, and respond to risks across your environment. The 2022 Cisco Security Outcomes Report, Volume 3: Achieving Security Resilience found that implementing a mature zero trust environment can improve [security resilience by 30%](#).

SSO: Much more than convenient

With SSO, employees only need a single set of credentials to log into multiple websites and applications, both in the cloud and on-premises. Not only does this simplify their user experience and eliminate the need to manage and maintain multiple passwords, it also provides administrators a centralized way to manage all accounts and more easily govern which users have access to them.

SSO is about more than convenience. Adopting technologies such as SSO can make it easier for employees to work on what matters most to them, while at the same time mitigating login risk. The benefits are catching on. In 2020, 20.6% of all authentications were made to SSO applications. In 2021, that number rose to nearly one in four (24.8%) of all authentications.

As complexity increases, so does the need for simplification

Grappling with blurred boundaries and the effects of increased connectivity and complexity, more security-minded organizations are deploying SSO solutions to establish order and help rein in their burgeoning environments.

SSO benefits both user and administrator, while making life harder for hackers.

Here's what organizations like yours can expect from adopting SSO.

- Users only need to remember one password. Although they may be required to enter credentials for other systems occasionally, there's significantly less signing in needed.
- SSO helps reduce reliance on passwords to: improve the user experience, since users get seamless access without all the special characters; reduce IT overhead, because fewer passwords means fewer password resets; and strengthen security posture, since attackers can't steal a password if there's no password to steal.
- SSO saves users time and effort. And it might not seem like much, but when the average enterprise uses hundreds of applications, it adds up quickly.
- Fewer passwords equal less risk. SSO also relieves some of the pressure on users to flawlessly follow strict cyber hygiene habits.
- SSO results in fewer calls to the service desk for password resets, reducing IT support resource needs.
- SSO enables your organization to start on its journey to passwordless authentication, using technologies like W3C's WebAuthn (FIDO2) standard for using public key-based credentials for secure application access, to further improve security and the user experience for all employees.



SSO doesn't only enhance the user experience but it also increases the security of the environment."

HANS PRUIM
ICT Adviser, ZorgSpectrum

SSO and MFA: A dynamic duo

It's possible you may think of SSO and MFA as two separate (or even conflicting) solutions. But these two solutions are complementary. They work together to fortify identity and access management initiatives – and, in the process, your entire cybersecurity infrastructure.



Together, these two defenses can **help your team:**



Reduce overall risk and optimize resources

- Reduce risk of data breaches
- Decrease risks associated with password reuse and weak passwords
- Reduce IT and help desk burden and costs of helping users reset passwords



Provide a frictionless user experience without sacrificing security

- Eliminate need for multiple sets of credentials for all business-critical apps
- Minimize cybersecurity burden on users
- Layer in strong authentication to verify user identity



Support a heterogeneous workforce

- Easily manage permissions and shifting access needs for permanent and temp workers
- Lock down access for managed and unmanaged devices
- Accommodate remote and mobile users on a case-by-case basis

What to look for in an SSO solution



Mature and enterprise-ready

Look for a solution that: offers strong security; can be used by all employees, including partners and contractors; is available in different regions; supports a variety of apps, including cloud and on-premises, web, and client-based apps; and supports common protocols such as Security Assertion Markup Language (SAML) and OpenID Connect (OIDC).



Identity and access management (IAM) platform

An SSO solution should ideally be integrated with a flexible MFA solution that supports phishing-resistant authentication options. Think of SSO and MFA as modules of a secure access management platform that work together to authenticate and help enable user access to federated applications, all based on granular conditional access policies. If you want to minimize risks associated with passwords altogether, SSO helps you transition to passwordless authentication for use cases that permit it, with an eventual goal of moving to desktop SSO.



Simple, not simplistic

Choose a solution that's easy to deploy, simple to manage and administer, and helps your users stay productive by enabling them to get up and running quickly without sacrificing security. You want a solution that frustrates threat actors, not users.



Resilient and scalable

Select an SSO solution that offers high availability and uptime with strong SLAs and the ability to scale quickly for enterprise rollout and long-term growth.



Honor data sovereignty and compliance regulations

Validate that the SSO solution has obtained security certifications such as SOC 2 and ISO 9001. Certifications provide assurance that data is protected.



Long-term vision for SSO solution

Because rolling out an SSO solution requires planning and support, try to ensure security investments and human resources devoted to the solution stay relevant for years to come. Always think about the long-term goals of the technology you're deploying.

Any SSO solution should also keep pace with rapidly evolving cyberthreats and adversary tactics. When migrating applications to SSO, you should see continuous improvement in support and capabilities.

Duo's long-term vision for SSO

Duo believes SSO is a baseline security need. That's why Duo Single Sign-On offers an open, integrated solution for teams looking to future-proof their business, proactively defend their organization against emerging threats, and build security resilience. It's important to select an SSO solution that's built to meet the unknown demands and threats of tomorrow, while at the same time exhibiting the flexibility needed to scale with the business, respond to changing market and cyber threat conditions, and meet the demands of evolving regulations.

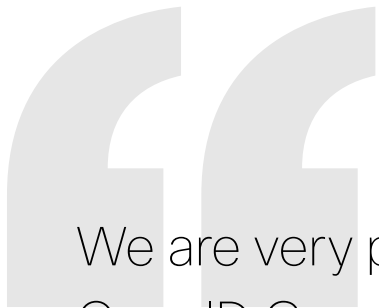
Frictionless secure access with SSO & MFA

Duo Single Sign-On meets all these requirements. But when combined with Duo's Multi-Factor Authentication or Passwordless Authentication solution, IT security professionals can deliver a frictionless access experience for their users without compromising security. Deployed together, SSO and MFA streamline the user experience, drive down password-associated risk, ease the support burden on IT, and save time and money. This combination also helps organizations proactively defend themselves against all types of exploits, especially password-based and MFA-targeted attacks.

SSO + MFA: Unlock security simplicity

With Duo Single Sign-On, users can verify their identity and use only one set of login credentials to securely access a range of apps, services, and platforms, including:

- Proprietary apps (APIs)
- Microsoft environments
- Cloud services
- Unix devices (SSH sessions)
- Internal applications (VPNs)
- Cloud applications
- Web applications
- SAML 2.0 applications
- OpenID Connect (OIDC) applications



We are very pleased that Duo SSO now supports OpenID Connect which allows us to secure more applications that our employees access on a regular basis. **We use Duo SSO for securing access to Microsoft 365, Cisco AnyConnect VPN, and IFS Aurena, our ERP system. We will ... expand usage to 50x more users over the next few months.** We are glad we chose Duo for securing access to modern apps that our hybrid workforce depends on.”

CARLOS CORTES

Business Systems Administrator, ASO Worldwide

Without SSO



With SSO



Administration made easy

Earlier, we noted how simple administration and management should be part of any SSO solution. Duo meets this criterion with Duo Central, a single, user-friendly, web-based portal that provides users access to permitted applications. This powerful administration tool enables security teams to direct users straight to the frictionless login workflows established by IT and security. You can configure Duo Central to provide each employee access to only those applications they need – in keeping with “least privilege” best practices – enabling you to control security at the application level and ensuring that only employees with the verified permissions can access sensitive information.

Additionally, Duo's self-service portal, available either as a direct link or via Duo Central, saves time for both administrators and end users by eliminating the need to contact IT staff for authentication device changes. Users can add, edit, and remove authentication methods via the traditional Duo prompt or Universal Prompt while logging in to protected applications.

Instead of relying on IT support, users can reset their expired Active Directory passwords themselves while authenticating through Duo SSO. After a user attempts to log into Duo SSO, they'll be informed that their Active Directory password has expired and can update their password after authentication.

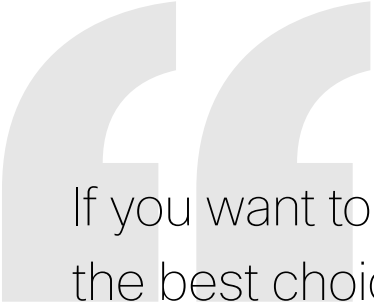


Why Duo?

The answer is simple (and secure).

You don't need to put your networks, data, and applications at risk merely to make security simple to use and administer. Duo's entire portfolio of secure access solutions is built to help you work toward your own zero trust environment without the headaches, workarounds, and compromises that come with piecemeal environments stitched together from disparate solutions that were never meant to work together. After all, anything that throws up roadblocks to user adoption increases your risk – especially since users are threat actors' favorite target.

MFA and SSO environments work together to protect those users – and by extension, everything they access. In a world where workers access enterprise systems from any location or device, where threats grow increasingly sophisticated and effective, and where breaches can impose lasting damage on operations and brands, why make security harder than it needs to be?



If you want to implement MFA very quickly, Duo is the best choice. We chose Duo because of its many features like Duo SSO that are easy to use and cost effective. One person was able to implement it quickly for 24,000 people in our complex environment.”

ALEXANDER STANOVY
Senior Security Architect, Diebold Nixdorf

Is Duo Single Sign-On right for you?

Pick the benefits that help build your business case.



Achieve greater security with less complexity

- Paired with Duo's robust MFA or passwordless authentication
- Integrated device trust
- Customizable, granular policy controls
- Deep breadth of application support



Create a seamless user experience

- One password (or no passwords) to manage
- Accessible from any device or location
- Paves the way for going passwordless



Save time and cut costs

- Implementation achieved in minutes
- Reduced overhead costs
- Free with all paid editions



Lessen the demand on IT

- Self-service capabilities for end users
- Extensive documentation
- Flexibility to add federate applications with ease
- Expedited on-boarding and off-boarding

Now that we have outlined how Duo SSO and MFA work better together, try them both, free for 30 days. In fact, we believe in this combo so much, that we always include SSO in our free trials. Give it a try, on us.

Try Duo free for 30 days



Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform.

Learn more at cisco.com/go/secure.



Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo is a trusted partner to more than 40,000 customers globally, including Yelp, Box, Generali, La-Z-Boy, Eastern Michigan University, Sonic Automotive and more.

Try it for free at duo.com.