

PASSWORDS ARE DEAD:

Comprehensive MFA & Advanced Identity Systems - Your Cybersecurity Essentials

Passwords have long been a weak point in security, easily breached and often reused. Cyberthreats have evolved exponentially, and it is no longer enough to rely on passwords alone to protect your data. Multi Factor Authentication (MFA) and advanced identity management systems are now best practices.

A QUICK REFRESHER...

Think of MFA as using both a key *and* a passcode to enter your house. Advanced security systems, on the other hand, are like having a smart home that recognizes your face, voice, and behavior before letting you in. While advanced systems include MFA, they go beyond by employing more sophisticated methods to safeguard your digital identity.

* MFA STATS:

99.99%

of MFA-enabled accounts remain secure.

99.22%

risk reduction across the board using MFA.

98.56%

reduction in the risk of leaked credentials for accounts that have MFA enabled.

*Source: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1661D>

DATA BREACH INSIGHTS:

50%+

of data breaches involve compromised credentials.*

88%

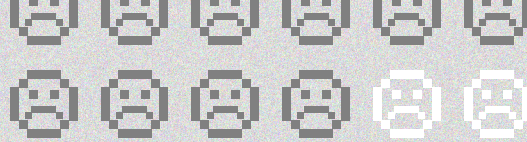
of data breaches could be prevented with basic cybersecurity practices like MFA.**

*Source: Verizon 2023 DBIR **Source: Symantec

STILL RELYING ON PASSWORDS ALONE? HERE'S WHAT YOU RISK

81%

of hacking-related breaches are due to weak or stolen passwords.*



THE MOST COMMON PASSWORDS REMAIN...

123456 123456789 qwerty password

Users also continue to manage passwords unsafely – often leaving them on scraps of paper, storing them in easily accessible files, or sending passwords via text or email.

- Executives and shared accounts often bypass MFA due to perceived urgency, a false sense of security, convenience in shared access, inconsistent policies, lack of awareness about cyber threats, and a culture that prioritizes speed over security. This makes them prime targets.
- One unprotected account can lead to massive breaches.

MOST ACCOUNT COMPROMISE ATTACKS CAN BE BLOCKED WITH COMPREHENSIVE AND ADVANCED MFA. IT'S TIME TO UPGRADE YOUR SECURITY MEASURES!

*Source: <https://www.zippla.com/advice/mfa-statistics/>

NOT ALL MFA IS CREATED EQUAL:

Weak vs. Strong MFA

77%

of accounts use SMS (texting) as their two-factor authentication (2FA), which is considered a weaker form of MFA due to vulnerabilities.

Push-based MFA attacks happen when attackers send fake login approval requests to users. In 25% of cases, users mistakenly approve these fraudulent notifications, allowing unauthorized access.



MFA IS GREAT—IF YOU USE THE RIGHT KIND. BASIC MFA LIKE SMS AND EMAIL HAS ITS FLAWS, BUT ADVANCED OPTIONS LIKE BIOMETRIC SCANS AND AUTHENTICATOR APPS ARE SIGNIFICANTLY MORE SECURE.

PASSWORDS ARE DEAD.

MEET THE NEW KEYS TO YOUR SECURITY.

PASKEYS: Stored on your device and encrypted, passkeys eliminate passwords and are nearly impossible to hack, offering strong protection even if data is breached.

TWO-WAY CHALLENGE-RESPONSE MFA: Ensures both the device and user are authenticated, providing top-tier security.

THESE SYSTEMS ARE PAVING THE WAY FOR A MORE SECURE FUTURE—ONE WHERE YOU DON'T NEED TO REMEMBER 15 DIFFERENT PASSWORDS.

PASSWORDS MAY BE DEAD

But Compliance Isn't

REGULATIONS LIKE HIPAA AND PCI STILL REQUIRE THE USE OF PASSWORDS, EVEN THOUGH STRONGER ALTERNATIVES, LIKE PASKEYS, ARE CONSIDERED MORE SECURE TODAY.

More than

55%

of enterprises use MFA to protect security but only

28%

of SMBs actually require MFA to be implemented.*

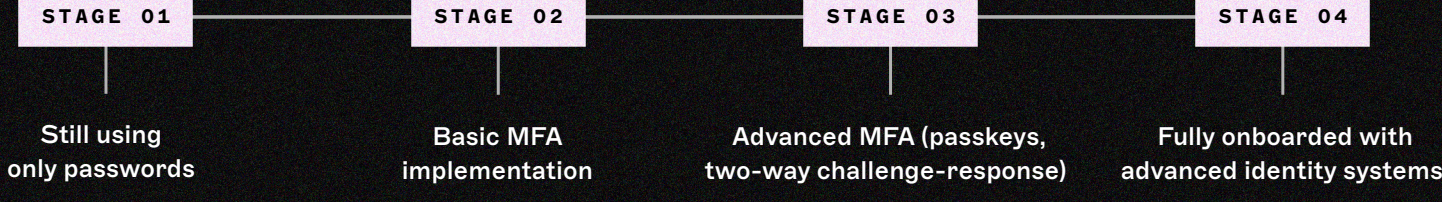
Looking ahead → The global multi-factor authentication market is projected to reach

\$20 BILLION BY 2025**

*Source: <https://www.okta.com/identity-101/why-mfa-is-everywhere/#:~:text=More%20than%2055%20percent%20of,that%20number%20rises%20each%20year.>

**Source: <https://www.adroitmarketresearch.com/press-release/multi-factor-authentication-mfa-market>

YOUR SECURITY JOURNEY: FROM PASSWORDS TO ADVANCED IDENTITY SYSTEMS



87%

organizations have deployed MFA, but only

18%

of SMB employees are required to use it.

38% of large organizations still don't use MFA, highlighting a significant gap in adoption.*

Every organization is at a different stage of the security journey. Understanding where you are—and where you need to go—will help protect your business from threats.

*Source: <https://www.zippla.com/advice/mfa-statistics/>

IT'S TIME TO MOVE ON:

Embrace MFA And Advanced Security

MFA can reduce the risk of identity-related breaches by **70%**



Consistent, advanced MFA across all accounts is the key to locking out threats.



The future of authentication is here. Let's put passwords to rest once and for all.



IT'S IMPORTANT TO SECURE EVERY ACCOUNT WITH MFA



Our advanced cybersecurity team is here to make sure businesses of all sizes get the protection they need, backed by enterprise-level expertise.

LET'S CHAT ABOUT HOW WE CAN HELP!