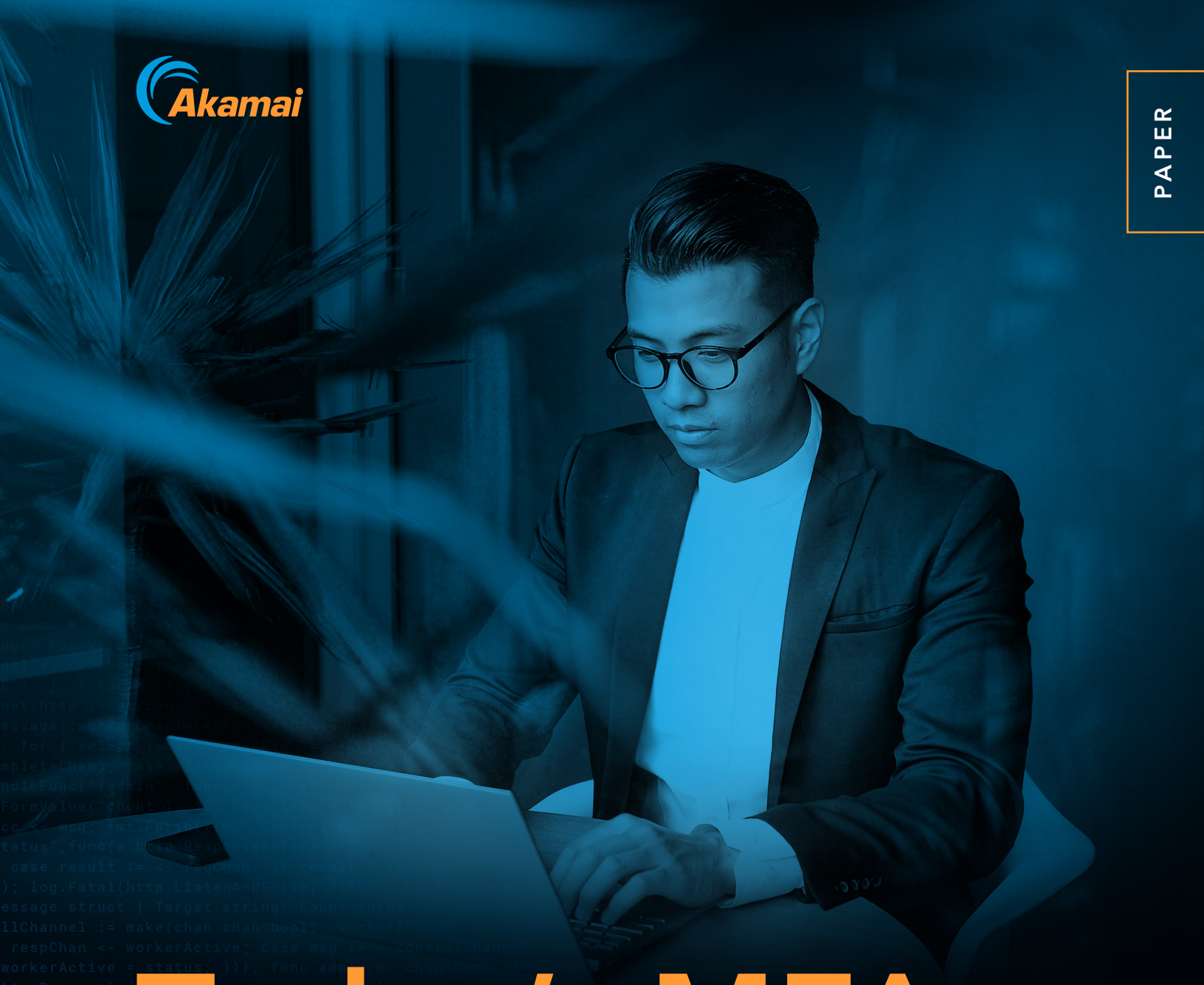
Akamai

PAPER



Today's MFA – Is It a Security Illusion?

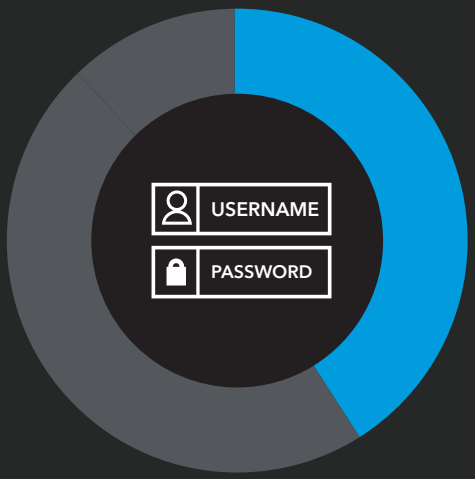
Usernames and Passwords Are Not Enough

Eighty percent of security breaches involve compromised credentials.[1] And while password hygiene is culpable in part, even complex, indecipherable passwords developed by algorithms can be problematic.[2] A recent dark web audit revealed 15 billion stolen logins from 100,000 breaches.[3]

The imperative of digital connectivity, a reliance on cloud services, and the reality of hybrid environments — coupled with a reliance on passwords — leave users vulnerable to myriad authentication attack vectors:

- **Credential stuffing**
- **Password spray and other brute-force mechanisms**
- **Local discovery and insider efforts**
- **Phishing and social engineering**
- **Keystroke logging**
- **Malicious proxy and reply campaigns**

And the global pandemic has exacerbated this status quo, showcasing the need for device- and location-agnostic secure access. When you consider that 100% of credential-related breaches occur after a user has been authenticated, it should be evident that passwords are not up to the task of accurate authentication.



Despite known weaknesses, 41% of organizations still believe usernames and passwords are one of the most effective access management tools.[4]

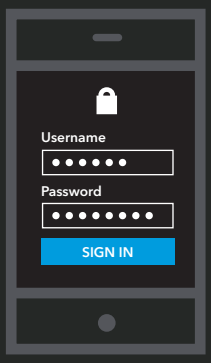
500%

Akamai has found phishing, social engineering, credential stuffing, and brute-force attacks to be on the rise. Between March and May 2020, we saw a nearly 500% increase in malware.

The Benefits of Multi-Factor Authentication

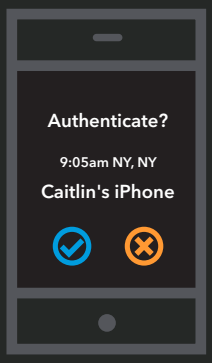
It is no surprise, then, that multi-factor authentication (MFA) technology has steadily grown in popularity. Simply put, MFA protects your enterprise by using more than one source of validation to verify identity before granting access.

MFA requires a successful combination of at least two of the following three authentication credentials:



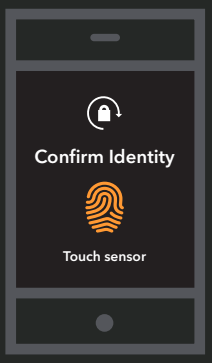
Something you know

This is knowledge-based authentication. This could take the form of a password, PIN, an answer to a security question, or even a pictograph.



Something you have

This is token-based authentication, hard or soft. This could be a smart card or key fob, or a one-time password, push notification, or SMS code delivered to a mobile device.



Something you are

This is contextual or biometric-based authentication. This might be behavioral, location signals or time, a fingerprint, facial recognition, a voice or speech pattern, or a signature.

Implementing an MFA solution significantly decreases the risk of unauthorized access and system breaches. In fact, organizations that use MFA are 99.9% less likely to be compromised than those that do not.[5] MFA enables and streamlines secure access to all environments – cloud, on-premises, web-based, SaaS, and IaaS applications. An MFA solution is also a critical component in migrating enterprise security to frameworks such as Zero Trust and SASE.

By requiring more than just usernames and passwords, unifying sign-on experience, and integrating with other cloud-native security tools, MFA technologies also have the potential to increase user productivity and usability. Furthermore, centrally managed authentication satisfies many compliance concerns and requirements.

But Traditional MFA Is Not as Secure as You Think

An MFA service built on a standard push can be easily manipulated by a hacker to achieve account takeover. Unless augmented with additional security, today's MFA technologies leave you at risk.

MFA is a form of perimeter security, but the cloud – and today's work style – has no perimeter. MFA is not designed to stop attacks unrelated to logins. It only secures sign-on at the perimeter, when the user seeks to gain system access. Cybercriminals have developed relatively simplistic yet highly effective social engineering and phishing mechanisms to circumvent this reality.

Consider this scenario:

1. **As a result of some form of social engineering, an employee enters a real username and password into a fake (phishing) site set up by an attacker.**
2. **Once these credentials are obtained, the attacker enters them into the real login portal.**
3. **This causes a push notification to be sent to the employee's phone.**
4. **The employee accepts the push notification as a natural course of login.**
5. **The attacker has now completed two forms of verification and is granted access.**

This is the critical security weakness of a standard push notification – any attacker with a set of stolen credentials can cause push notifications to be sent to an employee's phone. The only thing sitting between a security breach and business as usual is the employee's ability to discern a legitimate push from a scam. It only takes one success among thousands of employees for the attacker to get in.

Phish-Proof MFA

A truly secure MFA solution uses FIDO2 standards. At the most basic level, this means that security is provided by the technology instead of being dependent on user decisions.

How is this achieved? The FIDO2 standards use a couple of techniques that prevent phishing.

First, the request for authentication (the MFA challenge) is always sent to the workstation where the request for access originated. The browser on that workstation will direct the authentication request to any locally attached security key. Applied to the above scenario: Instead of the attacker getting the MFA service to send the push notification to the employee's phone, now the MFA challenge will come back to the attacker's workstation. Since the attacker does not have the employee's security key, no response can be made. An account takeover is prevented.

Defined: Authentication Standards and Specifications

Fast IDentity Online (FIDO) Alliance

The body responsible for the development of, use of, and compliance with standards for authentication.

FIDO2

The overarching term for FIDO Alliance's newest set of authentication specifications; standards included in the collection are CTAP1, CTAP2, and WebAuthn. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments.

WebAuthn

A web standard published by the World Wide Web Consortium (W3C) that is a core component of FIDO2. The goal of the project is to standardize an interface for authenticating users to web-based applications and services using public-key cryptography.

Client to Authenticator Protocol (CTAP)

A specification developed by the FIDO Alliance that enables secure communication between a roaming authenticator (such as a smartphone) and an internal authenticator – the client or platform.

Second, the browser sends data to the security key alongside the request for authentication. This data includes the domain name of the origin that sent the request for authentication, as seen by the browser. If the attacker simply forwarded the received authentication request to the employee's workstation, this data would contain the domain name of the phishing site. The security key would recognize the mismatch between the domain name of the site it originally registered with and the domain name requesting authentication and refuse to respond. Again, the attack is thwarted.

If more secure, phish-proof MFA is a possibility, why isn't it more widely used? Physical security keys – costly and cumbersome – are required. Or were, until now.

Next-Generation MFA at the Edge

IT has been faced with a trade-off when evaluating and implementing MFA technologies. To get the best security, they must spend more to roll out hardware, purchasing physical security keys for every employee, and managing the distribution and operation of all keys. IT must also get every user to adopt the less-than-ideal experience that keys present – another piece of hardware to use and keep track of.

The alternative is less security in the form of convenient push notifications to employee smartphones that do not add cost. The latter's ease is why push MFA is so widely used today. And it is also why so many companies are at risk of being breached.

But security no longer needs to be traded off against cost and ease of adoption.

The Akamai MFA service introduces a new authentication factor. It digitizes the security of FIDO2 with just a smartphone and a web browser, and combines it with the easy-to-use, familiar experience of a push notification — which can be used across any platform as a roaming authenticator. No physical security keys required. The solution affords the most secure functionalities of FIDO2 standards at a low cost, with ease of installation and consumption, as well as interoperability with common identity providers.

Protect your organization against phishing, credential stuffing, and account takeover with Akamai MFA. Learn more about Akamai's first-of-its-kind MFA technology and prepare for a secure, truly passwordless future.

Learn more at akamai.com/mfa.

Sources:

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://www.infosecurity-magazine.com/opinions/problem-password-everything-1/
3. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=27fa6368180f
4. https://www.businesswire.com/news/home/20200616005047/en/Weakest-Link-Prevails-Overreliance-Passwords-Continues-Compromise
5. https://www.hipaajournal.com/multi-factor-authentication-blocks-99-9-of-automated-cyberattacks/