Attack Vectors Decoded: Securing Organizations Against Identity-Based Threats

Attack Vectors Decoded: Securing Organizations Against Identity-Based Threats

Table of Contents

Threat Landscape

Improving Your Security Efficacy

How Duo can help

Threat Landscape

MFA-Targeted Attacks

As organizations put up stronger defenses around their sensitive resources, attackers find new ways to get around them. These attackers are not lone individuals working in isolation in their basement as we might see in the movies. They are organized cybercriminals that run their operation like a business. One way in which cybercriminals collaborate with each other is through attack kits that make circumventing security controls simple. These kits enable attackers with minimal technical expertise to launch sophisticated attacks.

That means our security solutions must continue to evolve, just like attackers' tactics. In the past, we might have thought a strong password with strange letters and numbers was a sufficient defense. Then, adding other factors to authenticate, such as verifying with a code over text message, was good enough. But now we know we must provide holistic solutions that enable easy access for our trusted users while putting roadblocks in the path of attackers.

So, what are cybercriminals doing to gain access? The good news is we have a lot of information on how these attack vectors work. The nonprofit MITRE has developed a knowledge database of attack tactics and techniques to help organizations understand how bad actors gain fraudulent access. While there are hundreds of attacks logged in the MITRE knowledge base, there are a few key types of attacks that focus on targeting end users. These methods can exploit weaknesses in MFA technology if not deployed correctly. They include:

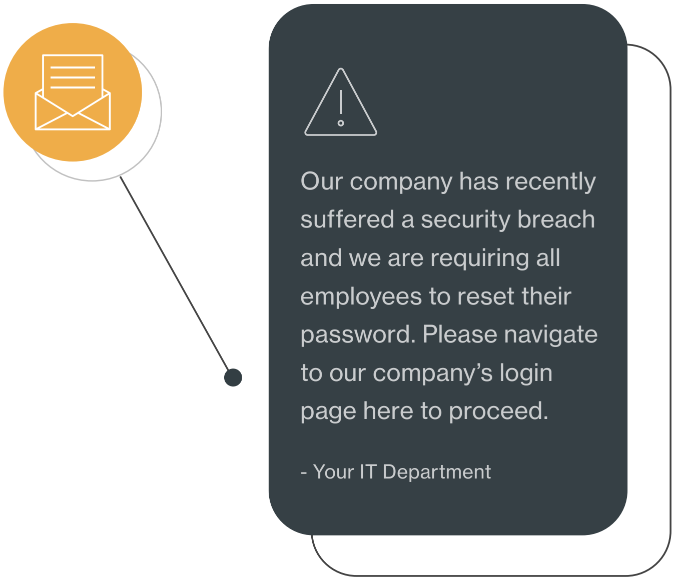
- MFA Interception (MITRE ID T1111): An attacker steals a one-time code that is sent through an SMS (short message service) or email and proceeds to log in with the user's credentials and MFA code.
- Device Registration (MITRE ID T1098.005): An attacker uses stolen credentials to register a new, fraudulent device to the MFA account to gain persistent access.
- MFA Request Generation (MITRE ID T1621): An attacker with stolen credentials sends repeated MFA requests to a trusted user in the hopes that they accidentally grant access, or the authentic user caves and accepts the request to stop the harassment due to MFA fatigue.
- Adversary-in-the-Middle AiTM (MITRE ID T1539): An attacker steals an authenticated user's session cookies to gain unlimited access posing as the trusted user and bypassing the need for MFA at all.

Many of these tactics can also include a form of social engineering, where a bad actor will impersonate an employee or IT team to trick someone into granting access. Social engineering can happen in general phishing attacks, or in spearfishing where a specific individual or company might be targeted using personal information from social media. Recently, there has been an increase in voice spearfishing attacks where an attacker might pose as an employee calling an IT help desk to bypass the company's security protocols.

The Attack Playbook

We've all seen news headlines where a company suffers a breach and has to scramble to protect and preserve its data, communicate to the public with PR teams, work to reduce the financial impact, and minimize the overall damage. While each attack is a little different, here's how a typical attack might play out:

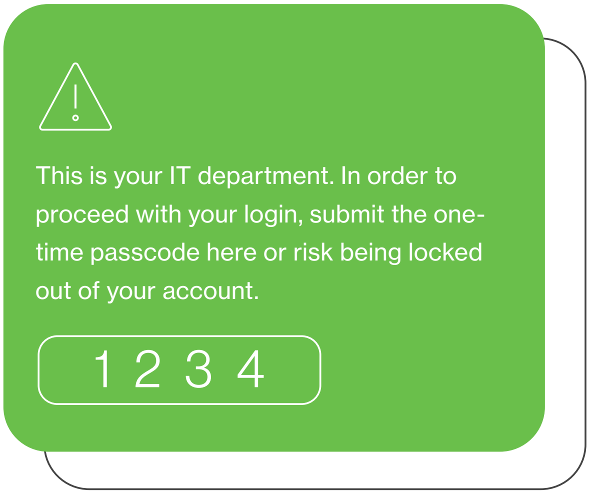
1. The attacker sends a spear phishing email posing as the company's IT team to capture an authentic user's credentials.



Our company has recently suffered a security breach and we are requiring all employees to reset their password. Please navigate to our company's login page here to proceed.

- Your IT Department

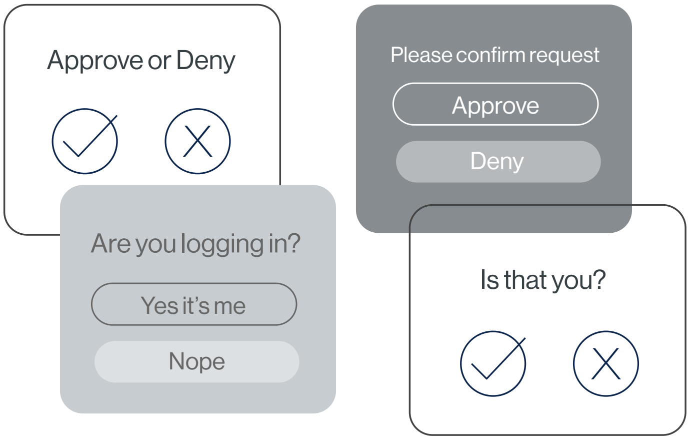
2. Through social engineering, the attacker tricks the user into sharing a onetime passcode (OTP) to bypass the MFA requirement.



This is your IT department. In order to proceed with your login, submit the one-time passcode here or risk being locked out of your account.

1 2 3 4

3. If OTPs are blocked as an authentication option, the attacker might send repeated MFA requests that get accepted due to MFA fatigue.



4. Once they gain access, the attackers can enroll their device and escalate their privileges and steal sensitive data or hold it ransom.

Unfortunately, this story is not unique. The Cybersecurity and Infrastructure Security Agency (CISA) has found that 90% of attacks begin with phishing. And with the rise of AI, phishing has become more realistic and believable. Emails that were once filled with typos can now sound professionally crafted, as well as mimic the tone and style of colleagues we know. An employee would need to be extremely vigilant to not fall for these tricks and it's not fair to expect them to be cyber experts. We need to move beyond blaming users for being victimized by cybercriminals and find ways to protect them.

Improving Your Security Efficacy

Pre-Requisite: Modernize Environment

Before organizations can access advanced access management security features, they must upgrade the authentication protocols used in their environment, which is a common step in the cloud-adoption journey. To unlock many of today's newest security features, applications must use upgraded authentication protocols including SAML or OIDC, rather than legacy protocols, such as LDAP and RADIUS.

LDAP is an authentication protocol that verifies user identities and grants access to on-premises applications by communicating with a directory on the network. When a user requests access to an application, LDAP checks whether the user's credentials match the information in the directory and if the user is authorized to access those resources. RADIUS also has an on-premises component as it enables users to access a remote network.

Modern protocols operate differently. SAML and OIDC function by establishing trust between the identity provider (IdP) and the application. These are the key protocols that enable single sign-on (SSO) and MFA to function and rely on encryption technology. Modern protocols are more secure than legacy protocols because they were built to support authentication to cloud and web-based applications. In addition, legacy protocols rely on a single factor, like a password, to gain access and can have a poor user experience.

Definitions:

- **SAML:** Security Assertion Markup Language
- **OIDC:** OpenID Connect
- **LDAP:** Lightweight Directory Access Protocol
- **RADIUS:** Remote Authentication Dial-In User Service

So, what needs to be done to modernize? For homegrown apps using legacy protocols, it's a question of dedicating internal resources to build that capability within the organization. For external applications it's a matter of understanding which authentication options are supported, and if modern options are not supported yet, what the roadmap is to get that support.

Once applications are using a modern infrastructure, that opens new opportunities to protect against bad actors and better position your organization to deal with the threat landscape today and in the future.

What are those new capabilities you can utilize to better protect your organization? There are different paths you can take to safeguard your users and applications. In the following sections we will outline the key categories to consider that include enhanced security features to provide the following benefits:

Lowest lift

Strongest Authentication

Most Secure

Best Visibility

Lowest Lift Winner: What you can do to upgrade security right now

The attack playbook has made it clear that users need additional protection beyond a password and a second authentication factor. Users need an authentication factor that can recognize and stop common MFA targeted attacks.

One solution that organizations can implement tomorrow is to upgrade a traditional push request to require a unique code, also known as a verified push request. This unique code is input into the authentication application and is different from a one-time passcode that might be sent through a text message or email. It requires that the end user enter the code from the access device (like a laptop) into the authentication device (typically a mobile phone). If the user is not really logging in, it will not be possible for them to enter the correct code into the authentication app.

However, trusted users who are logging in to do their jobs might be frustrated about having to input a code every time they login. Therefore, organizations can also consider a risk-based approach. In this approach, the authentication technology can consider risk signals and context to adjust user requirements at login. For example, if a user is in a trusted scenario, like on a corporate laptop or on a familiar Wi-Fi network, then they can decrease the number of times the user must authenticate.

If the user context changes, such as moving locations, then they might be prompted to authenticate again. More importantly, if there are authentication requests that resemble an attack pattern, like multiple push requests in a row from an unknown device, then you can step up the authentication method to a verified push to stop the attack.

Strongest Auth Winner:

Journey to passwordless

The philosophy of multi-factor authentication has always been to protect a user with at least two of the following factors:

1. Something you know
2. Something you have
3. Something you are

Traditionally, that has looked like a user logging in with a username and password (something you know) and authenticating through an application on a mobile device (something you have). This relies on a shared secret, the password, that is in your head (or a sticky note) and in the application's database. It also requires a second step, like accepting a push notification, to confirm your identity while logging in.

New, innovative technology is changing the way we log in, for the better. Passwordless solutions rely on something you are (like a fingerprint) and something you have (like a device).

This removes passwords from the equation, which are difficult to remember, easily stolen, and not very secure.

The "something you are" + "something you have" unlocks a private-public keypair that enables access in one step. Because the private key never leaves the user's device it is strongly protected, unlike passwords.

Passwordless technology is supported by the **FIDO Alliance** (Fast Identity Online), a consortium of companies dedicated to improving authentication and overseeing development of **FIDO2 standards**, including **WebAuthn**, or Web Authentication API. When a user first logs in, the WebAuthn protocol sends a username to that application. The application sends the username through the browser to the user's authenticator (device or security key). The user confirms their identity with a biometric or device PIN, and that device stores the user's newly created private key using encryption technology. The public key gets sent back to the application with the username. It can remain public because it is worthless without the private key that is being protected on the device.

Something you are:

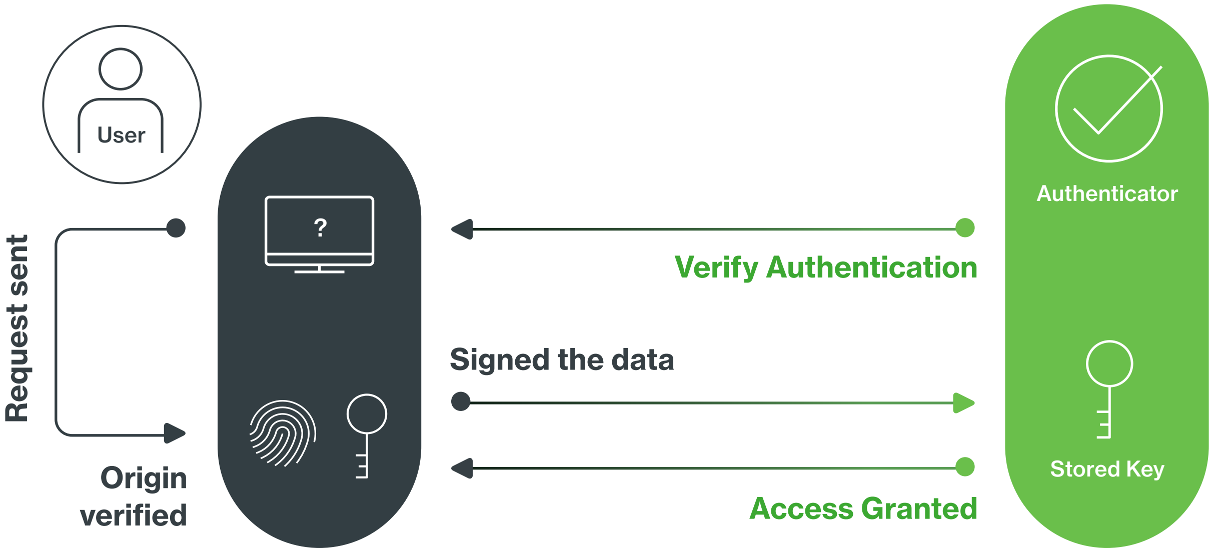
Biometrics (face ID, fingerprint)

+

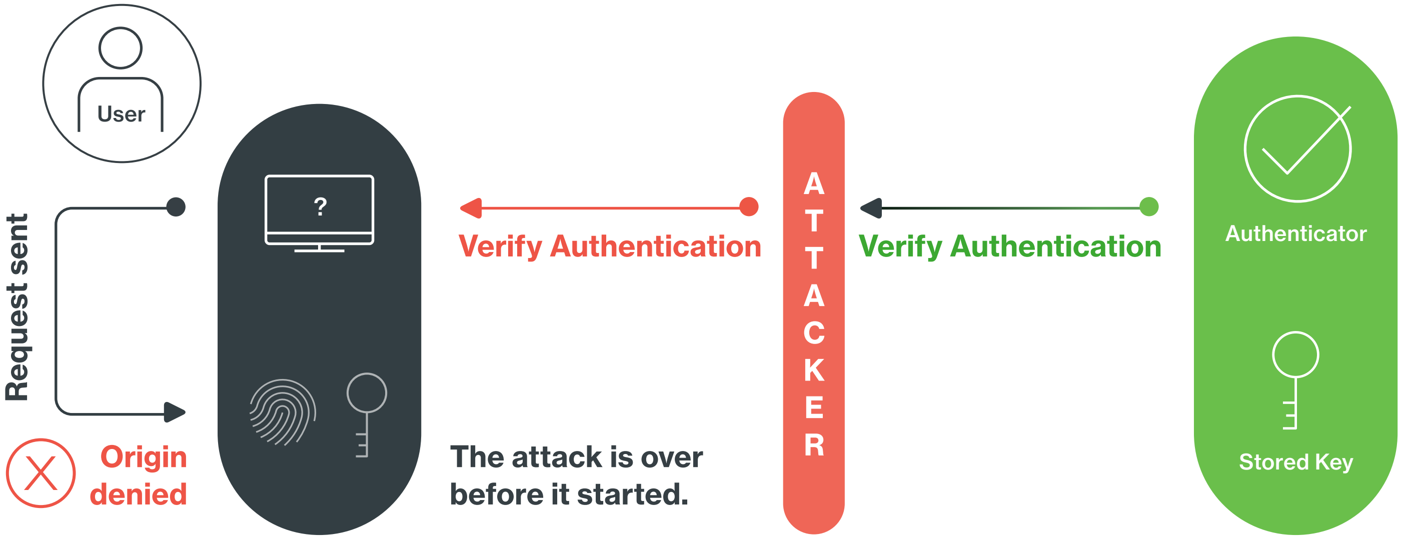
Something you have:

Device, security key, mobile apps

When the user goes to login in the future, the biometric unlocks the private key which is paired with the public key. This private-public keypair becomes the core credential, instead of a username and password. The use of passkeys makes passwordless even easier, as it enables users to access FIDO sign-in credentials across devices so users do not have to re-enroll biometrics.



This form of authentication is known as “phishing-proof” because it is impossible for an attacker to steal the user credentials. For example, in an Adversary in the Middle scenario, the attacker can steal a user’s session cookies through a proxy (a malicious website that sits between the user and the real website, so it looks like everything is normal). When the user authenticates, instead of through acme.com it might be coming from evil-acme.com But, if WebAuthn is deployed, the browser can’t lie about what is prompting the authentication and where the session request is coming from, as the authenticator is only registered with the secure domain. Therefore, the authentication request is rejected before the attack can even begin.



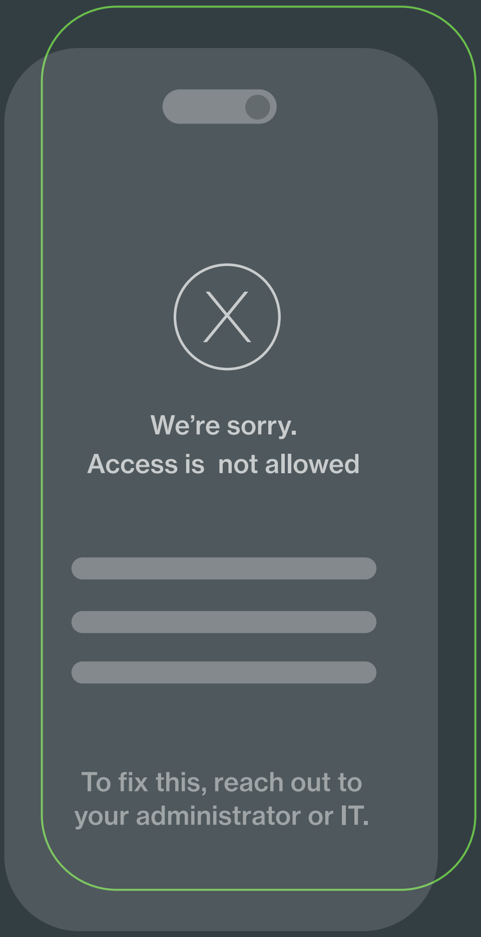
However, implementing passwordless is no small task, especially when you're dealing with large user populations, a substantial number of apps, hybrid infrastructures and complex login flows. Achieving a completely passwordless environment is a journey that involves a phased approach as technology continues to evolve and user adoption increases.

Most Secure Winner: Combine device and authentication security

While passwordless represents the most secure authentication option, one way to improve its efficacy is to pair strong authentication with device trust policies. Organizations can approach this by registering all devices, managed and unmanaged, that should have access to their organization's resources. If a device is not recognized, then that device would not be able to begin an authentication request.

Behind the scenes, the browser and device would be working together to confirm a user's identity through an application on the device. During an authentication, the browser can talk directly to the device application, and, out of band of the user request and browser, the device can say "yes, this device is secure" and "yes, this device should be given access."

Alternatively, if the device is not recognized, it is a non-starter for an attacker. It doesn't matter if they have a user's credentials; the attack is stopped before it can begin. That means that the attacker never interacts with the end user. This eliminates push fatigue, stops push harassment attacks, and prevents a social engineering attempt to get the user to enter the code in their authentication app.



We're sorry.
Access is not allowed

To fix this, reach out to
your administrator or IT.

Best Visibility Winner: How to use reactive tools

Proactive tools are essential for improving your organization's security posture. However, the reality of the threat landscape means organizations must also have the tools to respond if a bad actor is able to make their way past those defenses. That's where reactive measures can come into place to analyze authentication and login data to surface any anomalies.

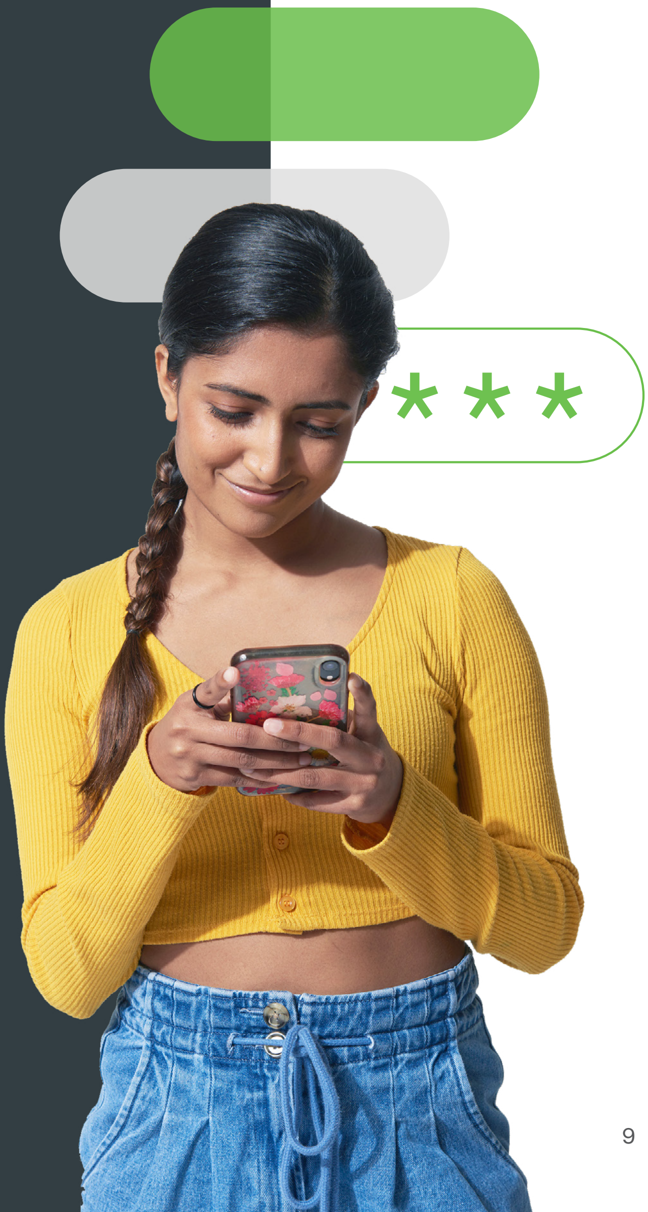
This can be difficult for organizations because there is so much data around users, devices, and locations. While one worker might access work resources at home most of the time, if they bring their work computer when they travel for a long weekend, that is not inherently a risk. And to flag it as a risk can overwhelm security teams with false positive alerts. In this case, it is still a trusted user, but in a new situation. However, if there is a user logging in to a new device, in a new location, at a strange time, that might be important to flag.

Organizations need a solution that understands their end users' behavior and can surface events that require attention and action. Then, when a threat is detected, security specialists need the tools to isolate and remove the threat from their environment. Reactive tools require user data to understand baseline behavior, an investigation to better understand if it is a true threat or false positive, and the ability to take action. These features enable organizations to improve visibility into their workforce and ensure they are protected.

Organizations need a solution that understands their end users' behavior and can surface events that require attention and action.

How Duo can help:

Wherever your organization is on your security journey, Duo can meet you where you are and help improve the efficacy of your security tools today.

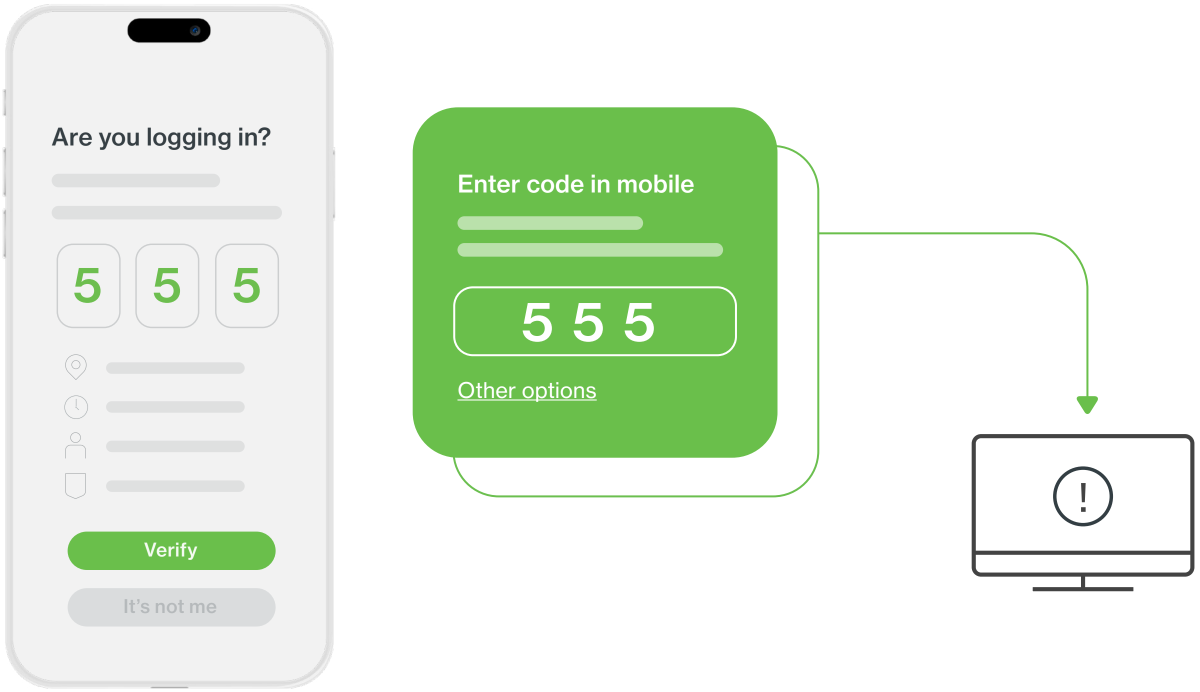


Pre-Requisite:
Modernize your environment

Duo's Universal Prompt offers many of the enhanced security features that are designed to protect against threats that target users. There are some helpful first steps your organization can take to modernize your environment, including taking an inventory and assessment of applications that support SAML or OIDC protocols. This can improve both the end user experience of accessing applications and set your organization up to improve your overall security posture.

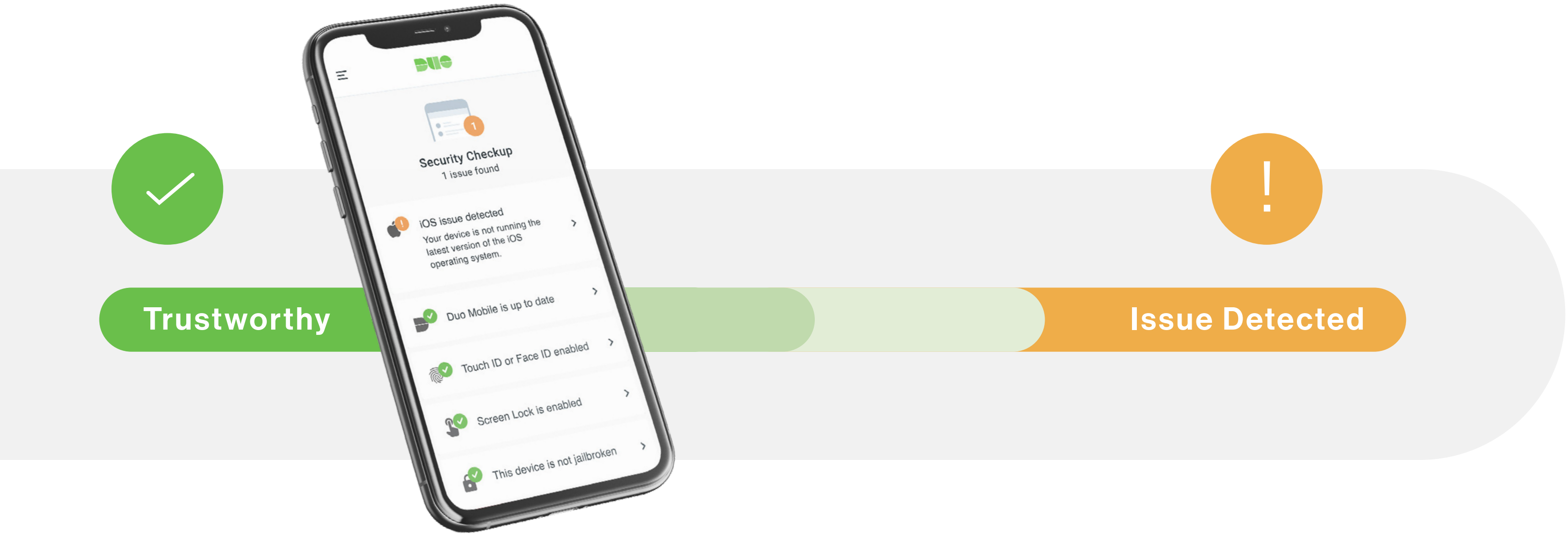
Lowest Lift Winner:
What you can do to upgrade security tomorrow

Verified Duo Push is an enhanced version of the traditional Duo push request, as it requires a 3-to-6-digit code, provided on the access device, to accept the authentication request. For customers with all editions of Duo (Essentials, Advantage, and Premier), customers can upgrade the Duo push to a Verified Duo Push for specific users, specific



For customers worried about MFA fatigue or pushback from employees about the extra friction, a great alternative is Duo's Risk-Based Authentication solution, available in the Advantage and Premier packages. Duo utilizes advanced algorithms to assess, in real-time, the risk associated with each login attempt by considering factors such as user location, device reputation, and network context.

If the user is in a trusted situation, they can easily gain access to the resources they need. If there is a change in context, Duo can prompt the user to reauthenticate. And if there is an attack from a cybercriminal, like MFA push harassment, Duo can step up the authentication requirements to a Verified Duo Push. The goal of Duo's Risk-Based Authentication solution is to prioritize security while ensuring a seamless user experience.



Security Checkup
1 issue found

iOS issue detected
Your device is not running the latest version of the iOS operating system.

Duo Mobile is up to date

Touch ID or Face ID enabled

Screen Lock is enabled

This device is not jailbroken

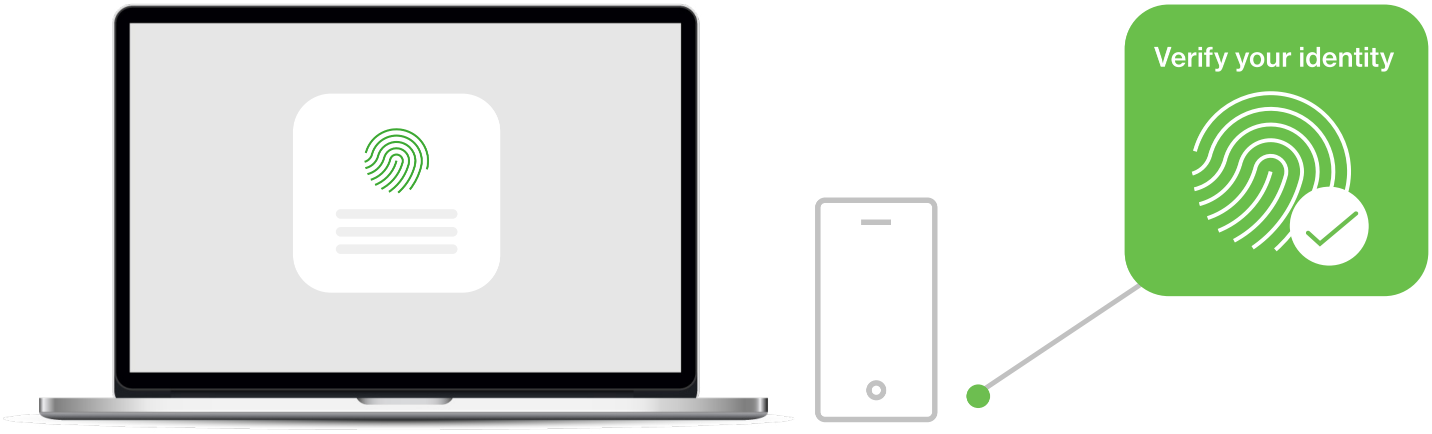
Strongest Auth Winner:

Journey to passwordless

Duo's Passwordless solution, available in all Duo editions, eliminates the need for passwords and employs WebAuthn protocols. Passwordless supports flexible authentication options, including utilizing passkeys. Passkeys are unique cryptographic keys generated for each user and are securely stored on a device or within a trusted platform. When a user logs in, the passkey is used to verify their identity, providing a secure and password-free authentication experience.

Duo makes it easy for organizations to deploy passwordless technology by supporting a diverse set of end-user authenticators and passkeys, including Windows Hello, Touch ID, and FIDO2 security keys such as YubiKeys.

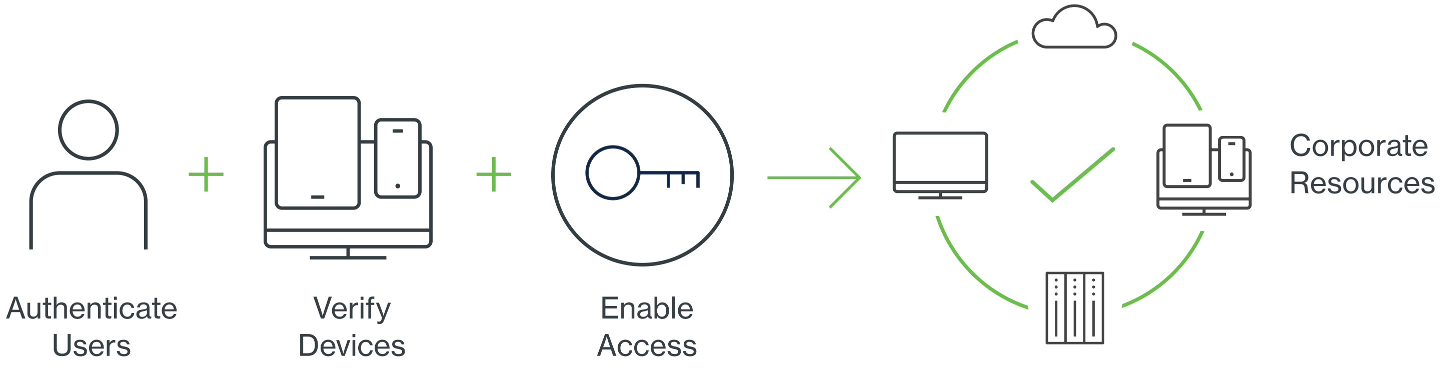
For some more tips on how to get started at your organization, the Duo Admin's Guide to Passwordless: Your Passwordless Rollout provides details for a phased approach to make passwordless a reality.



Most Secure Winner:

Combine device and authentication security

The gold standard of strong user protection is combining strong authentication factors with device policies. At RSAC 2023, Duo announced a significant change in packaging, enabling all customers to take advantage of its Trusted Endpoints technology. Powered by Duo Desktop, Trusted Endpoints lets organizations define trust for every endpoint, whether managed or unmanaged, company-issued, contractor-owned, or personal. Duo mobile app also enables organizations to check for a mobile device management (MDM) solution to verify that mobile users should gain access.



Through Duo policy, administrators can determine which users, applications, and devices should be granted access, or enable the policy at a global level for their entire organization.

The dynamic duo of strong authentication factors with device trust policies puts the necessary barriers in place to prevent cybercriminals from using the most common attack vectors. This also ensures that trusted users have a seamless experience because when accessing resources on trusted devices, most users will not even realize the technology is running in the background.

Best Visibility Winner:

How to use reactive tools

Duo Trust Monitor is a Duo threat detection feature focused on surfacing valuable and actionable security events to Duo administrators in the admin console. It creates a baseline of normal user and device access behavior by analyzing and modeling Duo authentication data. The feature considers questions like who, what, why, where, and when users access applications.

Because Trust Monitor compares user behavior to that user's historical context, it can help flag true suspicious behavior and not distract teams with false positives. And in the event of an actual attack, Trust Monitor enables Duo administrators to lock out a user while they investigate the potential threat.

Cisco Duo protects against breaches with a leading access management suite that provides strong multi-layered defenses and innovative capabilities that allow legitimate users in and keep bad actors out. A trusted partner to more than 40,000 customers globally, Duo quickly enables strong security while also improving user productivity.

Interested in learning more about Duo Security? **Sign up for a free trial.**