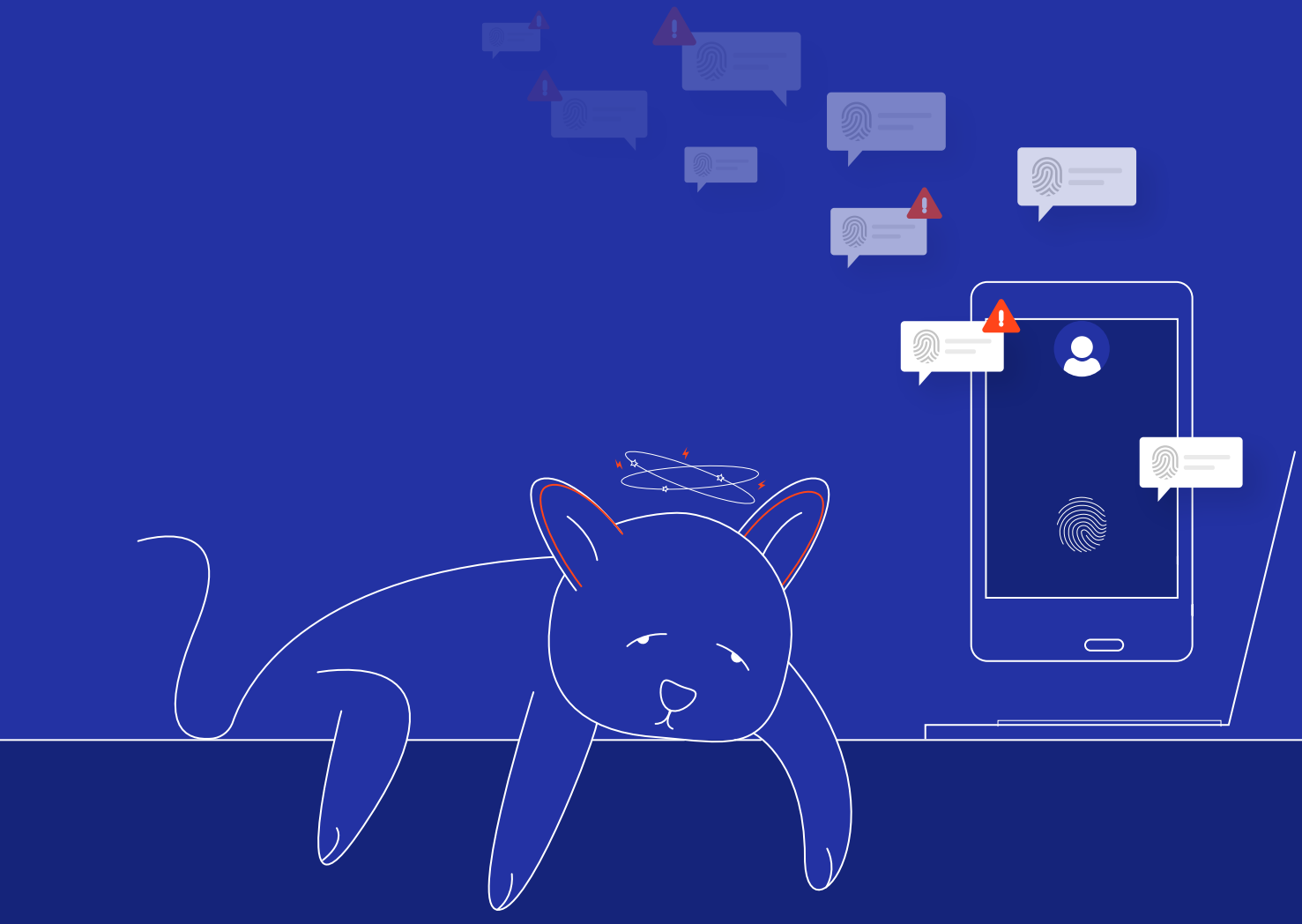
ManageEngine
AD360

A GUIDE TO

SECURING ORGANIZATIONS FROM MFA FATIGUE



www.manageengine.com/active-directory-360/

Table Of Contents

Introduction

Multi-factor authentication (MFA) is not new to data protection, but it has become more prominent with the rise of remote work, and attackers are exploring new ways to get beyond this line of defense. Attackers prefer to manipulate the human element of security to circumvent MFA controls, using various kinds of phishing and social engineering tactics. According to the 2022 Verizon Data Breach Investigations Report,

82% of breaches in 2021 involved a human element.

Identity security gaps in network infrastructures pave the way for attackers to gain control of high-risk identities and break into networks. A popular tactic among attackers to bypass MFA is MFA fatigue. Read on to learn what MFA fatigue is, how it works, and what organizations can do to protect against this sinister attack.

What Is MFA?

Obtaining usernames and passwords is not hard for attackers. As the name implies, MFA requires not just one but two or more factors of authentication, like email, SMS, or OTP verification. This combination makes the authentication process more secure, as it is less likely for an attacker to crack multiple factors.

What is MFA fatigue?

MFA fatigue, also known as MFA prompt bombing, is a technique used by attackers to spam a user's authentication app with repeated MFA push notifications and annoy the user until they eventually approve the request. The goal is to inflict a sense of fatigue in users with an endless barrage of push requests.

As continuous notifications roll in, making it impossible for the user to use their phone for anything else, fatigue ultimately drives the victim to approve the request, either knowingly or unknowingly. MFA fatigue follows a brute force approach to circumvent MFA security controls.

How does MFA fatigue work?

- The attacker has already obtained the user credentials in other ways, such as phishing or credential stuffing, or the attacker found them on the dark web.
- The attacker now tries to log in to the user account with the stolen credentials.
- If the user account is MFA enabled, the actor makes repeated sign-in attempts, sending out a flurry of MFA requests.
- The attacker might also send an authentication link over an email or SMS, pretending to be someone from the organization's admin or IT team.
- The frustrated user accidentally clicks any of these links or taps Approve instead of Deny on the request window.

That's all it takes to make MFA fatigue successful for attackers.

Recent MFA Fatigue Attacks

MFA fatigue has been increasingly spotted in recent times and is proven to be rewarding for threat actors to carry these out on large organizations such as Microsoft, Cisco, and recently Uber. In 2021, **Russian attackers** bombarded Microsoft 365 users with push notifications in an attempt to bypass MFA.

In the **Cisco breach** of August 2022, the attacker stole internal network credentials that an employee had synced with Google Chrome; the attacker then tried voice phishing the employee, pretending to be calling from many trusted sources, until eventually the Cisco employee was convinced to accept the push notification.

In the recent **Uber breach** in September 2022, an 18-year-old hacker said that he spammed an Uber employee for over an hour, contacted them later on WhatsApp claiming to be from the Uber IT team, and told the employee that they would need to accept the request if they wanted the notifications to stop. The employee then accepted the request and the attacker successfully invaded Uber's internal servers.

What Organizations Can Do To Strengthen Their MFA

When it comes to preventing MFA fatigue, the most important thing is to stay informed of the different methods attackers use to invade. Below are some recommendations to fend off MFA fatigue and fortify the security posture of your organization.

1. Educate users about the common attack techniques

Malicious MFA push notifications can be identified by the following characteristics:

- Unexpected notifications during non-business hours
- Notifications from unfamiliar locations
- Suspicious calls, emails, or SMS messages from someone claiming to be from a trusted organization
- Multiple MFA push notifications in succession

2. Restrict the number of MFA prompts

Check with your MFA solution provider if the solution can limit the number of MFA push notifications that can be sent within a timeframe or if the time limit in between prompts can be increased. This will largely help in preventing MFA fatigue in the first place.

3. Implement SSO

The more users have to go through MFA for every single service, the more likely they are to experience MFA fatigue, resulting in higher chances they'll fall victim to MFA fatigue attempts by attackers. Reduce the overall number of logins by deploying a single-sign-on (SSO) solution with passwordless authentication and ease login fatigue.

4. Require additional context

Ensure the authenticator app provides complete details about the approval request to the end user by presenting the location, IP address, device information, and the application context. This will help the user to detect if something is fishy and report the login attempt.

5. Automate stale account cleanup

Many organizations don't realize the importance of disabling and deleting orphaned or expired user accounts. The MFA apps and devices of these accounts are more vulnerable to attack. Deploy an IAM solution that automates user provisioning and deprovisioning and ensures user accounts are kept updated across all systems.

6. Enable MFA number matching

Instead of making the users tap Allow or Deny, make the technique for the attackers tougher. Deploy an MFA solution that shows a series of numbers on the login screen and asks the user to enter this number in the authenticator app. This way, the attacker cannot successfully log in without providing the exact number.

How ManageEngine Can Help Combat MFA Fatigue

ManageEngine AD360 is an integrated, holistic identity and access management solution with an intuitive interface and powerful capabilities to combat MFA fatigue attacks. Let's take a closer look at how AD360 strengthens MFA with its identity security features.

AD360 offers an extra layer of security to MFA by providing users with over 20 different authentication methods, ranging from biometrics to time-based one-time passcodes (TOTPs). Organizations can enable any of the available authentication methods for users and enforce user enrollment to be able to prove their identity. AD360 MFA provides a high level of identity assurance for access requests.
Below are some of AD360's features that help thwart MFA fatigue.

1. Adaptive MFA

With AD360, access control decisions to the IT environment are automatically made based on a user's IP address, device, time of access, and geolocation without admin intervention. Configuring conditional access can help in implementing security measures in critical scenarios like:

- Mandating MFA for privileged users.
- Blocking access to high-risk actions like password reset requests from untrusted IPs or unknown devices.
- Enabling endpoint MFA for machine logins (Windows, macOS, and Linux systems; RDP and VPN logins; enterprise application logins through SSO; and Outlook Web Access (OWA) logins.

Automating access control policies based on user context will require the attacker to satisfy the enforced conditional access rule, thus ensuring security without disrupting user experience.

2. Authentication workflows

AD360 enables IT administrators to trigger a preconfigured authentication workflow once a user initiates a password self-service request, utilizes SSO, or logs in on an endpoint. Using this workflow, IT admins can enforce different authenticators for different sets of users based on their OU, domain, and group memberships.

Implementing an authentication workflow for business-critical operations helps prevent attackers from accessing sensitive organizational data.

3. Passwordless authentication

With AD360's passwordless authentication, users don't have to enter a password to verify their identity. Instead, they're authenticated using biometrics or a TOTP, which is safer because these factors cannot be stolen easily

Going passwordless with AD360 helps in eliminating password-based attacks and also enhances the user experience.

4. Stale account cleanup

AD360 offers a broad range of reports that collect data on the last logons, users who have never logged on, users who have not logged on recently, inactive users, and more. It helps to automate operations like move, disable, enable, delete, password reset, and account unlock for the predefined scenarios exhibited by user accounts.

Checking for stale user accounts periodically helps in minimizing the risk of inactive accounts being compromised or misused.

Conclusion

MFA fatigue can be the most challenging attack to deal with in the evolving cyberthreat landscape. Organizations need to understand the risks associated with such attacks and plan their security infrastructure accordingly. MFA is an excellent additional layer of security when used in conjunction with other security measures to strengthen cyberdefenses. Review the current MFA settings in your organization today and ensure you stay protected from the rising MFA fatigue.