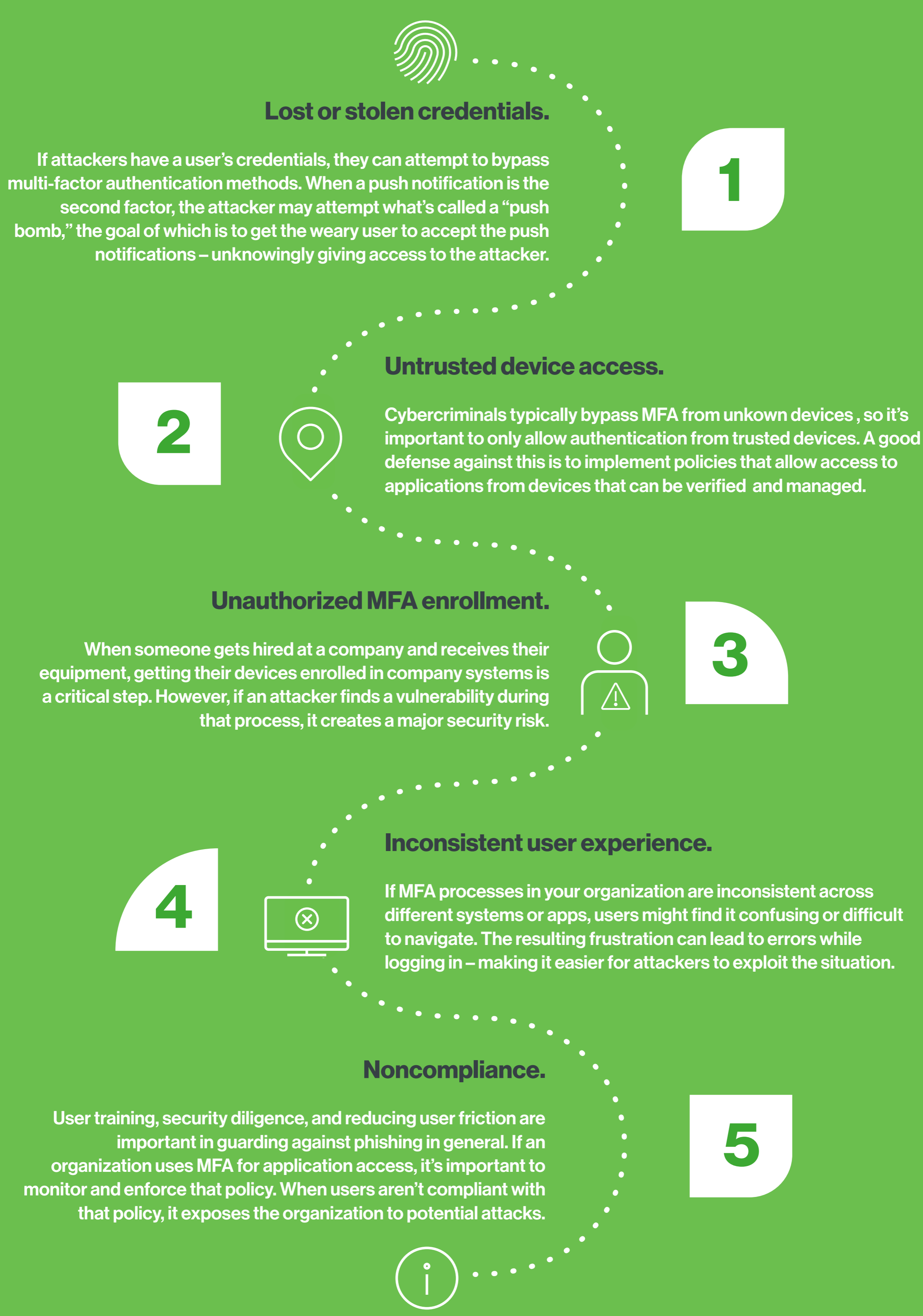


# Staying Vigilant Against MFA Attacks

## What is an MFA fatigue attack?

Multi-factor authentication (MFA) fatigue attacks refer to types of cyberattacks that attempt to frustrate or overwhelm the user during the authentication process. When a user experiences friction upon trying to log in, they're more likely to look for a shortcut or workaround, which creates a major security risk.

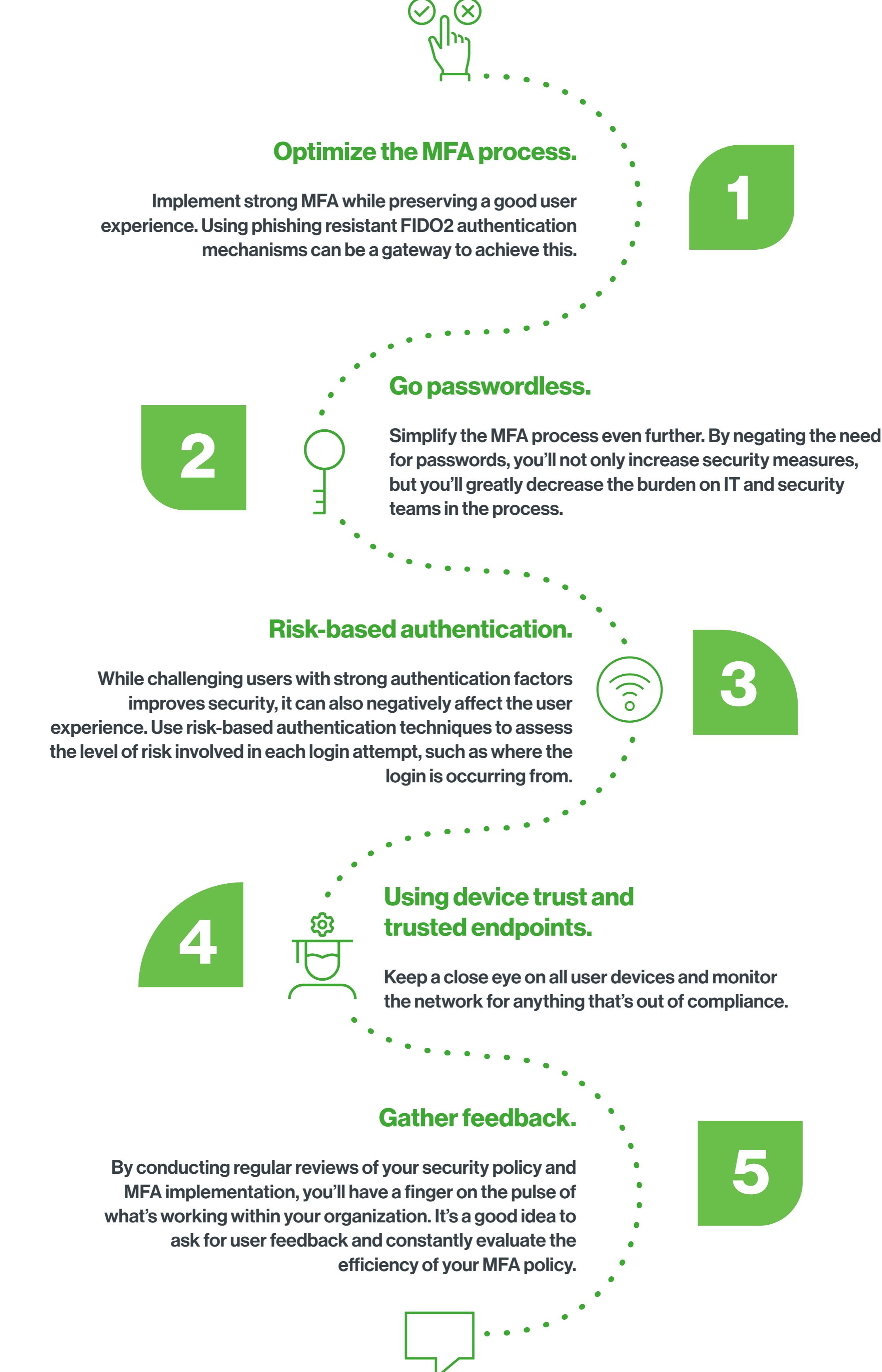
Here's a quick look at factors that can lead to an MFA attack:



## How can you stay protected from MFA fatigue attacks?

Make no mistake, attackers are always finding new ways to exploit, attack, and steal sensitive data. MFA fatigue attacks are just one of the ways attackers continue to evolve their methods. Therefore, to stay safe from these attacks, individuals and organizations alike must take every measure they can. It's no longer enough to rely on a single method alone – you need to develop a strategy and stick to it.

Here are some ways to stay protected:



## Get the strongest protection against MFA attacks

Stay one step ahead of attackers with one access management solution: **Cisco Duo**.

With **strong MFA protection** and multi-layered defenses, Cisco Duo keeps bad actors at bay. It also uses risk-based evaluation methods, allowing users to indicate if they received a push notification they didn't initiate. This is one of the strongest and most effective ways to stay protected against MFA fatigue attacks.

Duo can also distinguish between unmanaged and managed endpoints to prevent attackers from attempting verification on their rogue devices using **Duo Trusted Endpoints**.

Additionally, Duo takes the headache out of remembering passwords with **passwordless** authentication. This feature is fully compliant with the FIDO2 (Fast Identity Online) industry standard and adds yet another layer of protection with phishing-resistant authentication.

What's more, Cisco Duo also features **Verified Duo Push**, which sends a PIN to the user's device. If an attacker sends that request from their own device, the user won't see it – ensuring your users stay much less susceptible to MFA fatigue attacks.

[Try Cisco Duo](#)