CISCO DUO

5 Critical Security Callouts to Know in 2024

Taken from the 2024 Duo Trusted Access Report

Organizations today must navigate a treacherous digital landscape and an increasingly complex security environment to find success. With that in mind, the 2024 Duo Trusted Access Report reveals a new frontier for access management and identity security. Here are five key takeaways from our findings.

01

In the last year, Duo recorded a **41%** global increase in multi-factor authentications
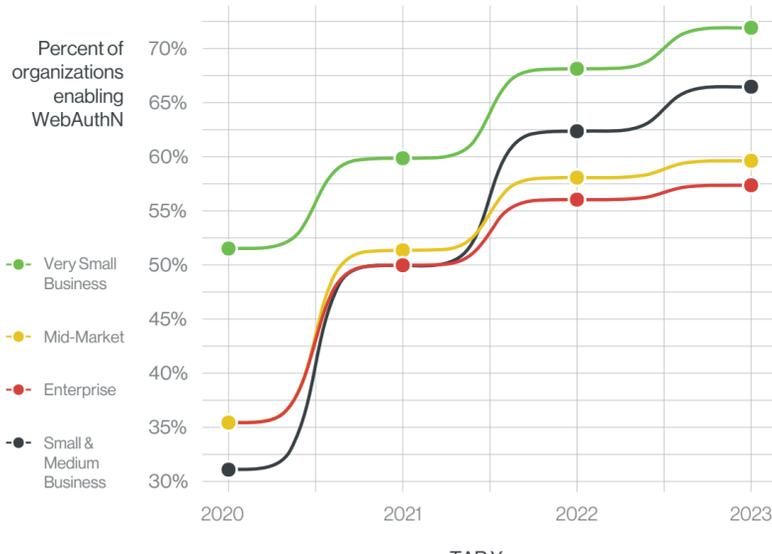
Why it matters: With the rise in more sophisticated forms of cyberattacks, organizations need more dynamic methods of protecting themselves from disaster. Multi-factor authentication (MFA) is a great start, as it adds an extra layer of protection in which users are required to verify their identity beyond simply entering a password.

Germany
+52.3%

Japan
+28%

Brazil
+26.3%

Phillipines
+24.9%

Australia
+16.9%
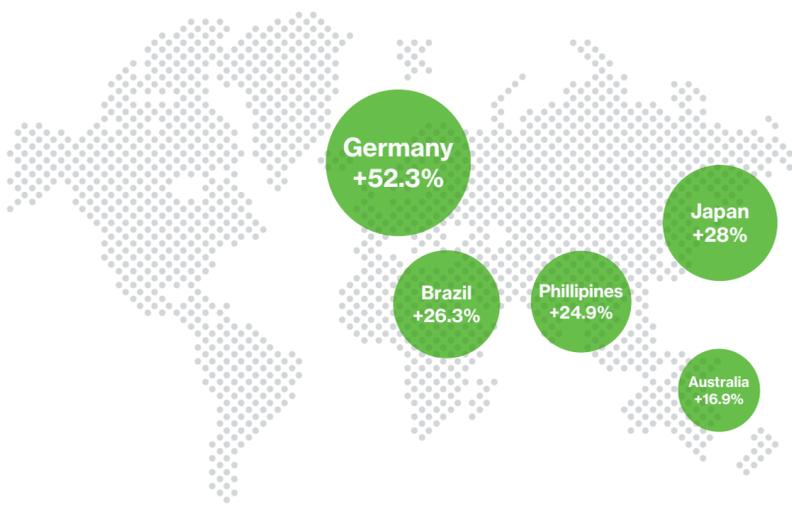
02

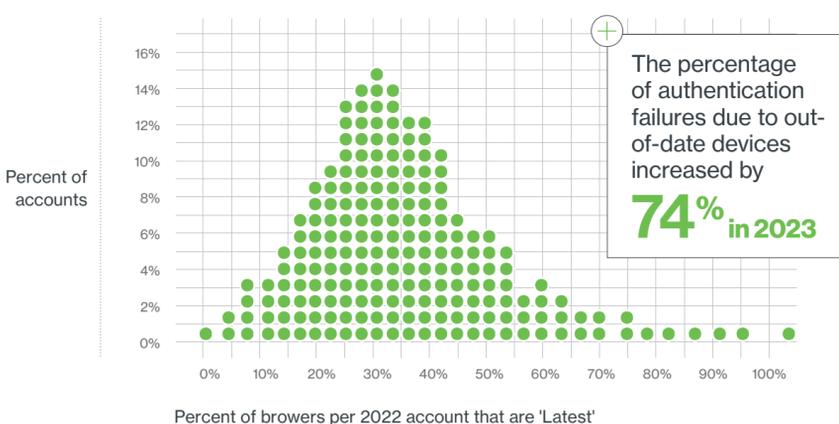### Less secure authentication methods continue to decline in usage

Why it matters: Due to the relative ease of being intercepted by attackers, SMS (short message service) and voice calls are not considered very secure authentication methods. Our research shows users are catching on, with a 22% decrease in these methods from 2022. You can read more about this in our blog post.

Percent of organizations enabling WebAuthN

- ● Very Small Business
- ● Mid-Market
- ● Enterprise
- ● Small & Medium Business

70%
65%
60%
55%
50%
45%
40%
35%
30%

2020   2021   2022   2023

TAR Year

03

Outdated devices continue to be a strain on security

**Why it matters:** The use of invalid or outdated devices poses a significant risk, especially in diverse and expanding IT environments.

Percent of accounts

16%
14%
12%
10%
8%
6%
4%
2%
0%

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

Percent of browers per 2022 account that are 'Latest'

The percentage of authentication failures due to out-of-date devices increased by **74%** in 2023

Policies addressing geo-restrictions, unsecure devices, and granular per-user or per-application access can help reduce complexity and increase security coverage.

04

Organizations see over **500 attacks** on inactive accounts each year
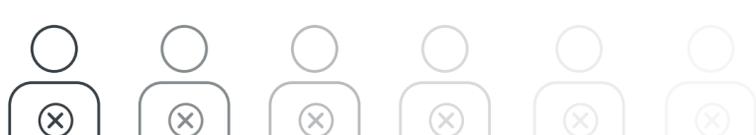
Why it matters: Employees may have multiple digital identities across various systems, applications, and platforms. Without proper visibility, threat detection, and response, identity infrastructure left unchecked provides ample opportunity for attackers to gain entry to critical systems.

05

5,600 more Duo customers took extra steps to protect themselves from MFA-targeted attacks

Why it matters: 2023 saw an increase in MFA-targeted attacks, such as push fatigue or push harassment. Over 5,000 more Duo customers rolled out Duo Verified Push, which provides an extra layer of protection from such attacks. These customers not only prevented identity-based breaches but also strengthened their overall security posture.

Navigate Complexity

The **2024 Duo Trusted Access Report** delves into the evolving landscape of access management and identity security. Focusing on data-driven insights, the report provides a comprehensive analysis of authentication trends and identifies key challenges and opportunities for organizations today.

Get the full report at **duo.com**