CISCO DUO

Access Management Fails

& How to Cure Them

The wrong access management solution can create as many headaches as it solves, while leaving your individual use cases unprotected. Here's how to find relief.

Too many logins are unprotected.

Legacy systems, homegrown apps, and third-party vendors all still need protection. But most access management solutions lack integrations or coverage for these use cases.

Defense-in-depth means end-to-end coverage—even for the toughest edge cases.

	DUO	OTHERS
Mobile and hybrid workforces	✓	✓
Complex contractor, third-party, BYO access management requirements	✓	
MacOS & Windows workstations (online and offline protection)	✓	
Intricate access management compliance & insurance requirements	✓	
Servers, homegrown web apps, legacy Microsoft apps & protocols*	✓	

*Including support for SDKs, ssh, RDP, radius, LDAPS, smb file shares, and TCP connections

Zero trust remains elusive–and expensive.

You can't build a zero trust foundation without single sign-on (SSO) and passwordless authentication–among the most secure authentication available. But most vendors charge a premium for these core zero trust capabilities.

Equipping every user with features like device trust, SSO and passwordless authentication shouldn't break the bank.

Repeat after us: Zero trust is a right—not a privilege.

DUO	OTHERS
Strong MFA	Basic MFA
Device Trust	optional Device Trust
SSO	optional SSO
Passwordless	optional Passwordless
$	$$$

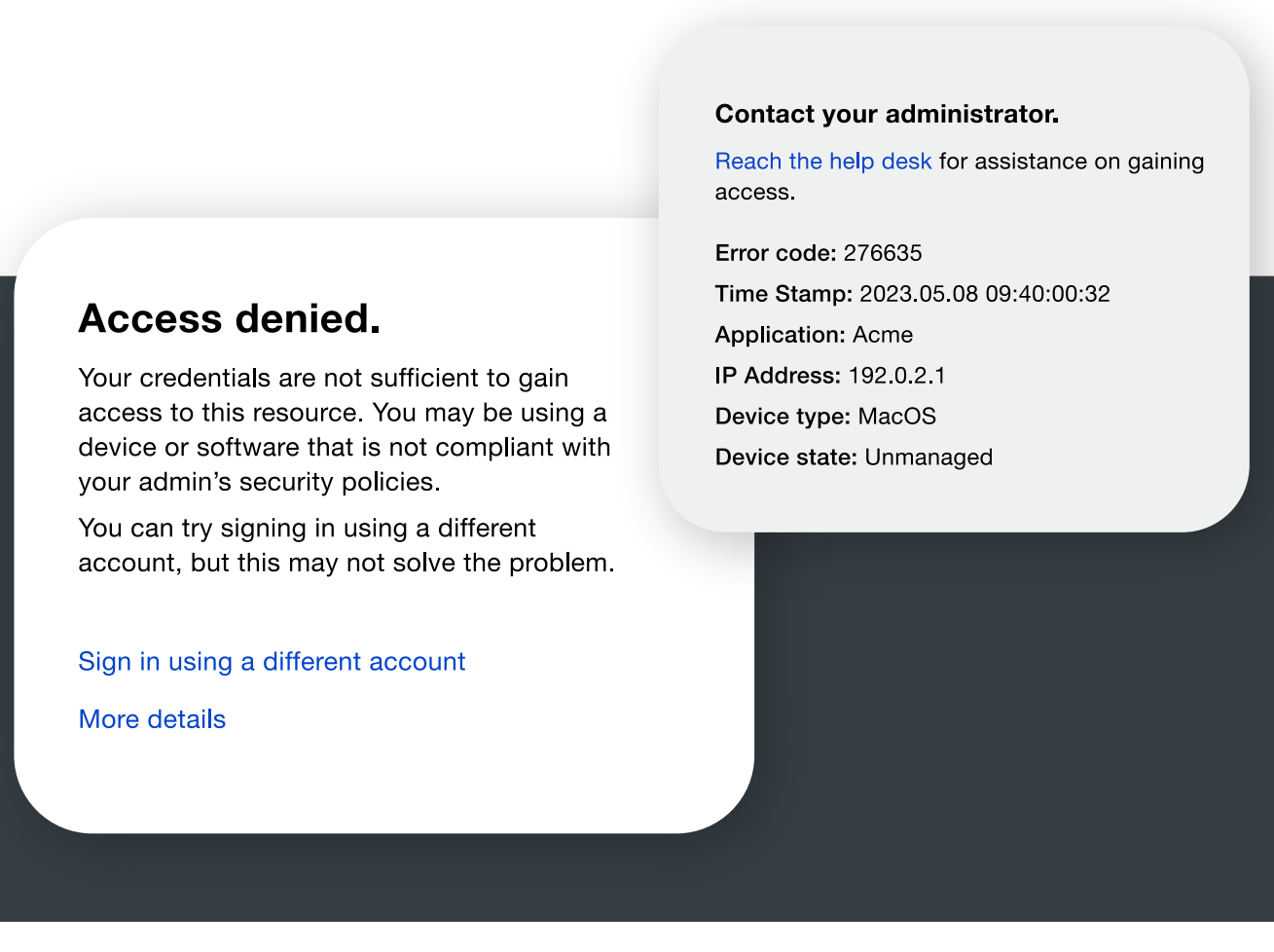
MFA is too hard to use.

With complex solutions, users can't self-remediate and IT is hounded by help desk calls. The result? IT costs soar, and some users just give up and go rogue.

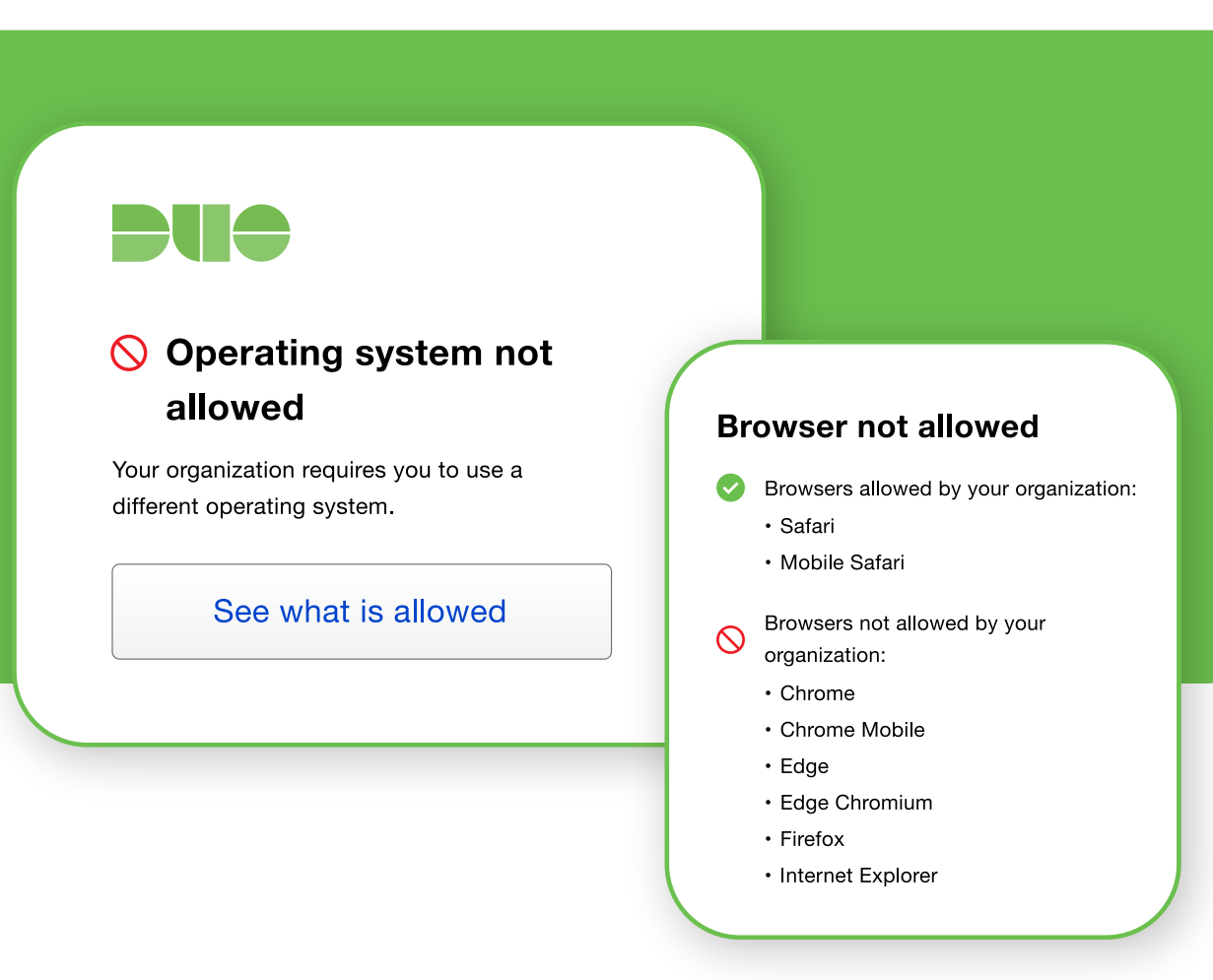
Security that's hard to use doesn't get used. Look for options that are quick to deploy and easy to manage, and that give users clear directions for authentication.

Stay protected–and productive.

OTHERS



DUO

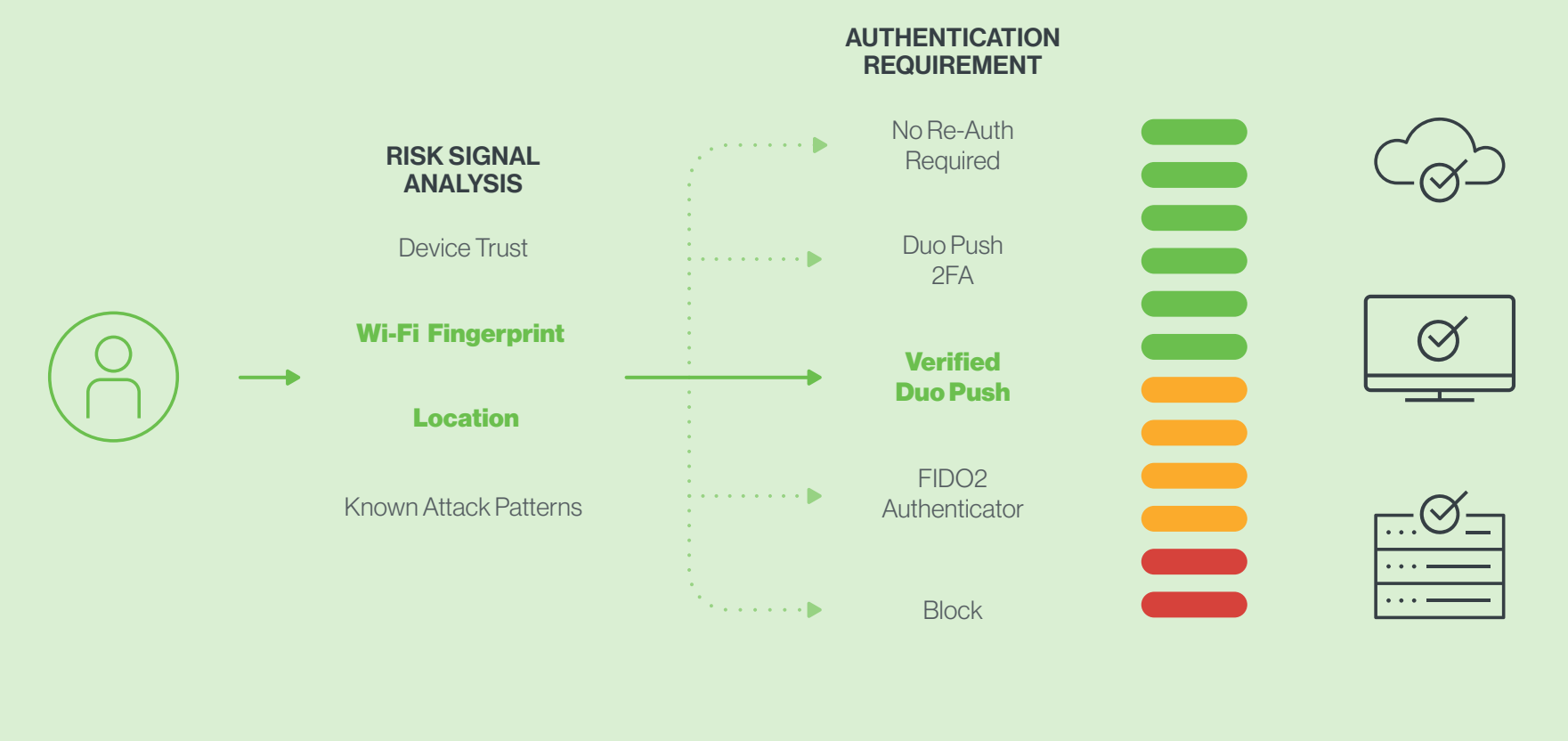


Old risk models weren't built for today's threats.

Too many vendors offer outdated technology and gauge risk based on old models–a poor fit for defending against evolving threats and MFA bypass attacks. This leaves you giving access to users or devices that could invite the next breach.

You want to evaluate logins with a combination of device signals, real-time adaptive detection, step-up authentication, risk-based authentication, and logging for all risk signals.

There are better ways to check risk.



Don't settle for just-the-basics access management.

(It's not worth the risk.)

82%

of breaches involve carelessness, negligence, and other human errors

2022 Verizon Data Breach Investigations Report

2/3

of orgs aren't prepared to defend themselves against MFA bypass and other identity attacks

Cisco Cybersecurity Readiness Index 2023

$4.35M

average cost of a data breach

Cost of a data breach, 2022, IBM

Find the one solution for your business.

Download the Access Management Buyer's Guide to learn how to evaluate and select the best secure access management solution for your business.

Get the Guide

CISCO DUO