SECUREAUTH
Welcome to Better Identity.

Get The **Access Management** You Need For **Office 365**

Prevent Attackers from Using Stolen Credentials to Compromise Your Cloud Data

Best Practices Guide

Table of Contents

Executive Summary

Office 365 has eclipsed all other cloud applications to emerge as the most widely used enterprise cloud service by user count. It's easy to understand why: With Office 365, organizations no longer have to pay for hardware or resources to manage software in their own data centers, and their users always have the latest versions of applications.

But Office 365 comes with significant security concerns, especially as organizations store more and more sensitive and business-critical data there. One study reports that virtually every organization experiences at least one cloud-based threat each month — and the average has soared to nearly 6 incidents every week.

What can organizations do to protect their Office 365 environments? We know that 81 percent of breaches involve misuse of stolen credentials, so one critical strategy is to stop relying on the traditional username + password — which, unfortunately, is the only type of authentication that most older Office 365 and third-party clients support. Instead, organizations need a solution that enables them to detect and block the misuse of valid credentials before attackers can compromise their critical data and systems.

Adding a second authentication factor is a good start. But two-factor authentication (2FA) is not as secure as many organizations think, and many 2FA solutions impose multiple disruptions on each user's daily routines, which can seriously hurt productivity. SecureAuth® Identity Platform has a comprehensive, multi-layered approach to authentication that delivers far more security than 2FA — without most users even knowing it's there. This white paper explains how Multi-Factor Authentication (MFA) with risk analysis (Adaptive Authentication) can help you properly control access to your Office 365 environment, including detecting and blocking attackers with stolen valid credentials.

Office 365: Popular with Users — and Attackers

Office 365 is the most popular and used service in the world, with over 100 million users and growing. An analysis of more than 20,000 cloud-based services found that 58.4% of sensitive data — business plans, medical records, financial forecasts, etc. — in the cloud is stored in Microsoft Office documents.

This wealth of valuable data makes Office 365 an appealing target for attackers. According to the Q4 2016 Cloud Adoption & Risk Report report by Skyhigh Networks, nearly all corporate Office 365 users (93.5%) have at least one insider threat per month, and more than half (57.5%) have at least one privileged user threat.

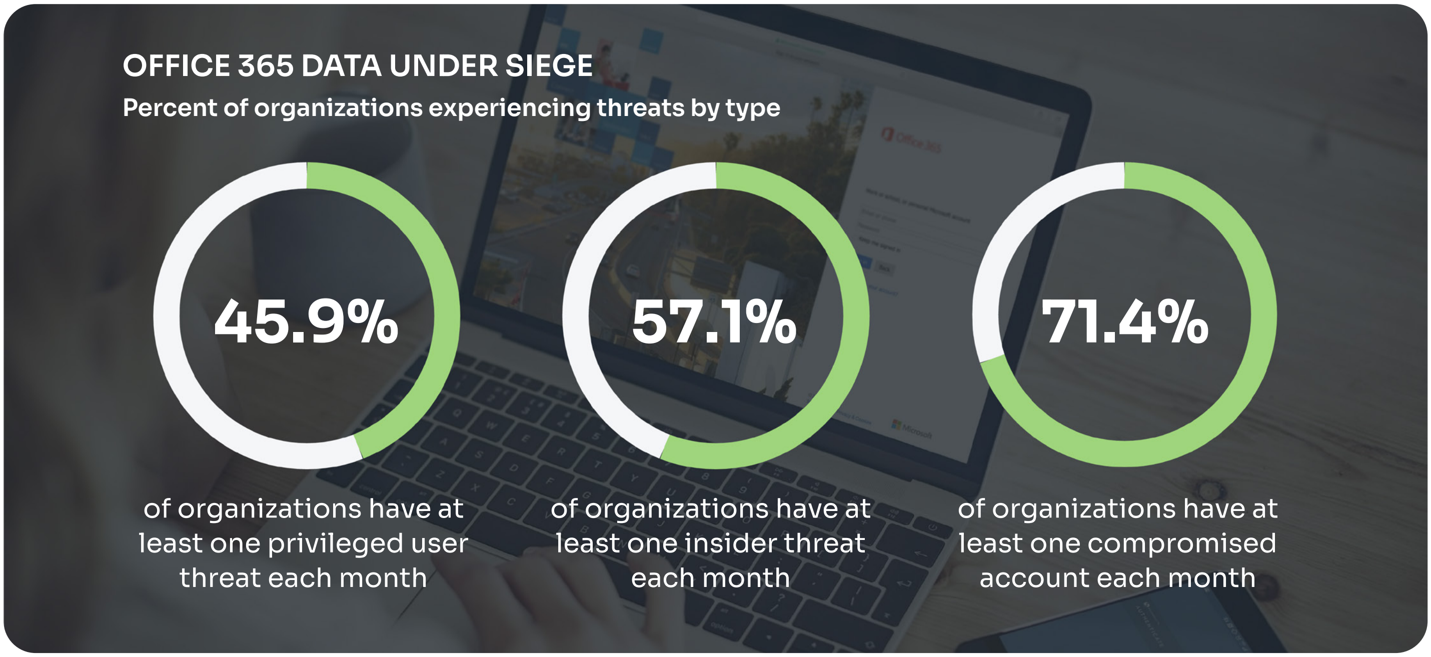


Figure 1. The valuable data organizations store in Office 365 is under constant attack (Source: SkyHigh Cloud Adoption & Risk Report).

Attackers are Walking in Your Front Door with Legitimate Credentials

One of the most common attack vectors putting your Office 365 at risk is stolen credentials. The Skyhigh Networks study reports that more than three quarters (79.1%) of Office 365 environments experienced at least one compromised account each month, and the Verizon Data Breach Investigations Report says that 81 percent of attacks on organizations leveraged weak, default, or stolen credentials.

These remarkably consistent findings make one thing abundantly clear: Single-factor authentication is woefully insufficient for protecting your Office 365 environment. Valid credentials are fairly easy to steal through social engineering and other methods, and hundreds of millions of them are readily available for purchase on the dark web. Chances are, some of your user's credentials are out there in a database controlled by an attacker. Moreover, users frequently re-use their passwords for convenience and simplicity, so when attackers acquire someone's password for one site, such as Facebook, they can often access other sites the person frequents — such as your Office 365 environment.

If your assets are protected by single-factor authentication only, attackers who acquire valid credentials can walk right in your front door and gorge themselves on a veritable buffet of your sensitive and business-critical data.

Nearly Half of Assets Are at Risk

Organizations and analysts alike have recognized for some time that the password alone is no longer effective at protecting resources. Nevertheless, a survey by Wakefield Research that SecureAuth recently commissioned found that, on average, companies are protecting only 56% of their assets with either 2FA or MFA. That means nearly half of assets are protected only by passwords, or by nothing at all!

And once attackers have breached your perimeter, they can take their sweet time lurking in inside your network, looking for what they want and elevating their privileges to access it. In fact, Mandiant's M-Trends 2024 Report finds more than 30% of breaches go undiscovered for more than 6 months! Giving plenty of time for attackers to damage or steal your valuable assets and cover their tracks.

> **"nearly half of assets are protected only by passwords, or by nothing at all"**

The Stakes are High

Attackers are continually refining their craft, and security solutions need to evolve just as quickly. What worked 2 or 3 years ago may no longer be nearly as effective as it once was. Consider what's at stake:

Your company's bottom line — The average cost of a US breach in 2023 was 9.48 million, according to IBM Security.
Your company's reputation — After a breach, how likely are customers to stay and prospects to come?
Your continued revenue — Will your customers leave for a competitor they perceive to be safer or more responsible? Given that studies show that it's three to ten times as hard to find a new customer as it is to keep an existing one, customer attrition is serious risk.
Your job — Will a breach cost you and your team their jobs?

Two-Factor: Better than Passwords, but Not Nearly Good Enough

Two-Factor Has Its Weaknesses

Organizations recognize the very real risks they are facing, and a mad rush is on to put 2FA in front of everything. In fact, the Wakefield survey found that 99% of decision-makers feel 2FA gives them the protection required to prevent breaches.

But while two-factor authentication is much better than relying on passwords alone, it is not nearly good enough to protect your critical assets. Table 1 shows how attackers are getting around the most popular 2FA methods.

2FA Method	Why It's not Secure
OTP via SMS	Attackers have compromised SMS multiple times and the National Institute of Standards and Technology (NIST) no longer recommending 2FA with SMS without certain controls.
Push-to-accept	Users have become conditioned to routinely accept without being in an authentication process, simply to remove the notification from their screen.
Knowledge-based questions (KBAs)	Answers can be guessed or easily obtained though social media, even if you're using credit bureau or LexisNexis services.
Hard tokens	Well documented cases existed where hardware tokens have been compromised in numerous ways.

Learn more about other 2FA methods that have been circumvented by attacker
Identity 101: Why two-factor authentication is not enough

2FA is Disruptive

In addition to failing to provide proper security, many two-factor authentication methods suffer from a serious second flaw: They are inconvenient for users. People don't like having to carry hard tokens and may not have them available when they need them (and of course they are expensive for the organization as well). Soft tokens are a bit more convenient — unless you're stuck in an airport somewhere and your phone is still on your bedside table at home, or the battery has died. Users can even get themselves locked out trying to remember which childhood friend they picked as their bestie, or whether they specified “Buffalo NY” or “Buffalo, New York” or just “Buffalo” as their birth place. As a result, legitimate logons get blocked, and your vital business operations suffer.

Even when users aren’t denied access, constantly having to provide a second factor hurts their productivity — and your bottom line — more than you might think. Suppose you have 3,500 employees with an average salary of $50,000. If each one has to spend just 3 minutes a day supplying 2FA, that lost productivity will adds up to over a million dollars a year.

Detect and Block Attackers with Adaptive Access Management

Adaptive Authentication: More Secure Than Two-Factor Alone

The best way to secure your Office 365 environment is to layer together multiple contextual risk layers to gain an increasingly accurate picture of who is a legitimate user and who might be an attacker. Think of a bulletproof vest; no single layer can stop a bullet (or an attacker), but together they form an impenetrable barrier.

The more layers you have, the more difficult you make it for attackers to gain a foothold in your network, and the more likely they are to seek the path of least resistance and move on to another target. SecureAuth offers more risk checks than any other vendor so you can create a custom bullet-proof vest that fits your needs. Here are just a few of the checks you can include in your security strategy:

+ **Device Recognition** — Creates one or more unique device profiles for each user, using settings like web browser configuration, language, installed fonts, browser plug-ins, IP address, screen resolution and more. Attackers who have obtained valid credentials will be blocked because they’re using the wrong device.
+ **Threat Service** — IP reputation data (blacklists of IP addresses) can be used to deny or step up authentication. For example, your organization might choose to deny authentication if the IP address of a user’s machine is part of the Tor anonymity network or a known botnet, or an IP/subnet associated with known bad actors such as cyber-criminals, hacktivists, or particular nation states.
+ **Phone Number Fraud Prevention** — Attackers often impersonate legitimate user’s phone number attempting to trick authentication safeguard and by pass phone-based authentications. SecureAuth can block access from phones numbers coming from carriers in countries where they have no employees, partners, or customers. The SecureAuth platform can also block by phone type (landline, VoiP, mobile, toll-free) and if the phone number has recently been ported.

- **Geo-Location** — If an access request is coming from a location where the organization has no known employees, contractors, business partners, or customers, the SecureAuth platform can deny the request or automatically step up to multi-factor authentication.

> **"SecureAuth offers more risk checks than any other vendor so you can create a custom bullet-proof vest that fits your needs"**

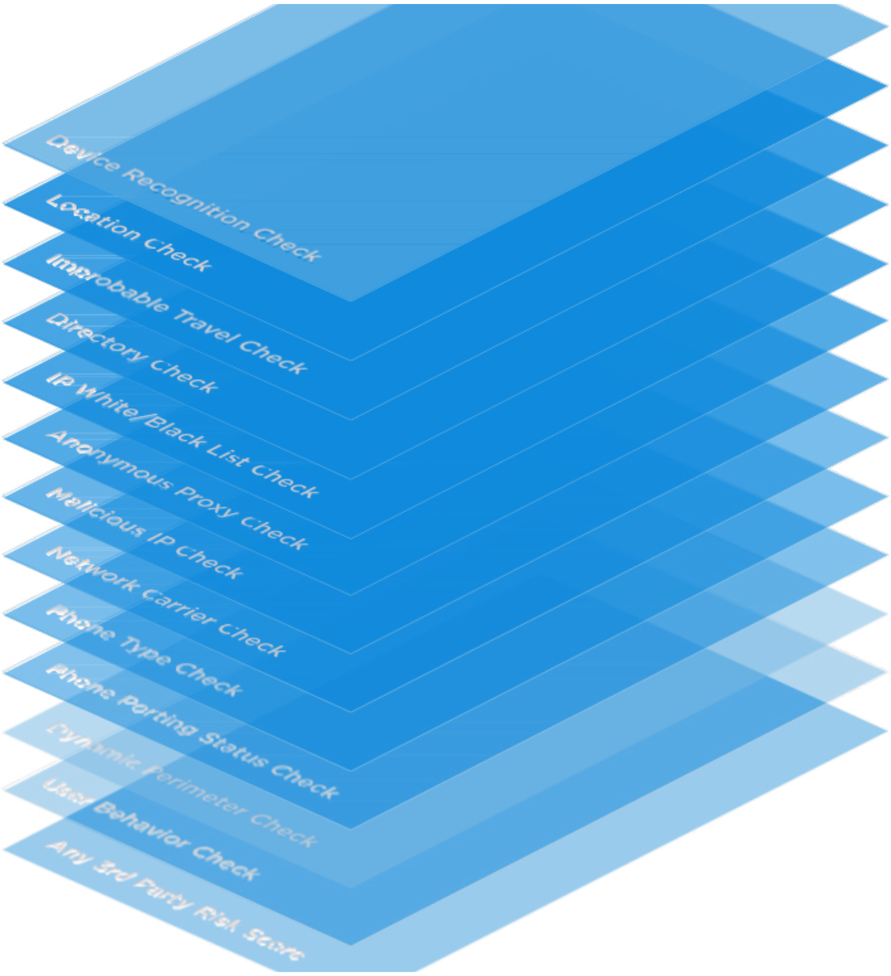


Figure 2. Pre-authentication risk-checks for complete protection

Deliver a Seamless User Experience

What's more, the SecureAuth Identity Platform's strong adaptive authentication actually streamlines the user experience instead of setting up more roadblocks that hurt productivity. When a user attempts to authenticate, the solution evaluates the risk of that attempt based on the set of factors you choose. The vast majority of authentication attempts will be legitimate, and they will be approved without the user even being aware that the risk checks took place.

But if the risk is too high, the solution will either challenge the user for another authentication factor, block it entirely, or redirect the user to a honey pot for further investigation. How high is “too high”? You get to decide. You can even set different thresholds for different users or groups of users. For example, you might set the risk bar lower for financial department staff, who have access sensitive data, than for salespeople.

And you might set it lower yet for your most senior IT administrators, since having an attacker successfully access your systems using their powerful credentials could be disastrous. Most of the time, these users will also sail through the authentication process, but they may be challenged for 2FA authentication more often, such as when they get a new device or travel to a new location — an acceptable trade-off for the increased security.

You get a wide range of choice about what authentication methods to offer for those infrequent challenges. SecureAuth supports nearly 30 authentication methods, including SMS, telephony, email one- time passcodes (OTPs), push notifications, USB keys, and push-to-accept, just to name a few.

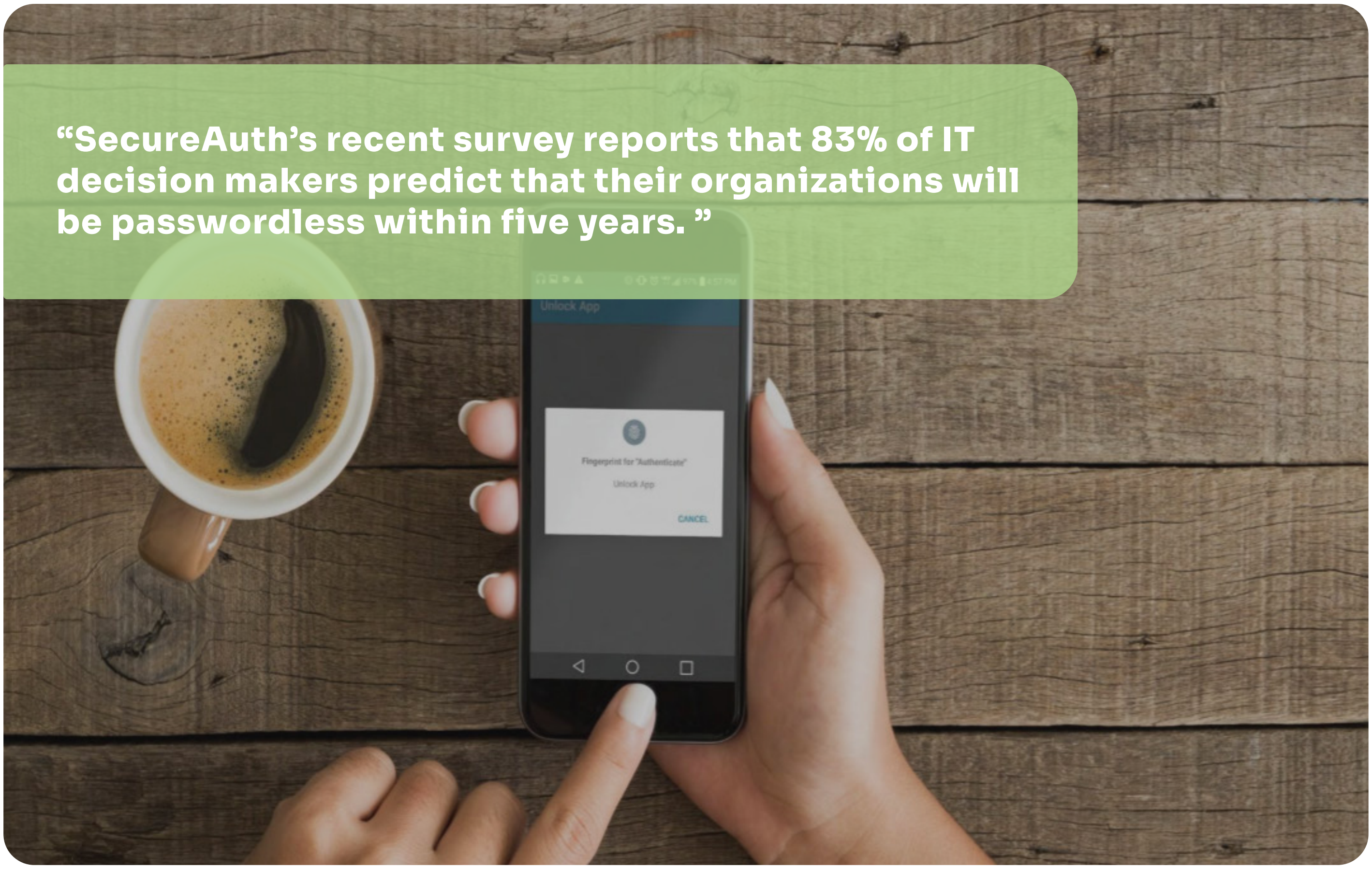
Reduce Security Risk in Using Legacy Office 365 Clients

In addition to providing the most comprehensive protection for browser access to Office 365 covered above, the SecureAuth solution also provides adaptive security for all Office 365 clients – including legacy Microsoft Outlook and third party clients, such as Apple Mail. Although recently released Office 365 clients support Multi- Factor Authentication and Adaptive Authentication, organizations whose users access Office 365 via older Outlook or third-party clients remain at high risk. Most older Office 365 clients support only username and password authentication, and even the popular two- factor methods behind newer clients have been proven to have significant flaws. Only Multi-Factor Authentication together with adaptive access control offer the multiple layers of protection and detection needed

Go Passwordless

Adaptive MFA is so powerful that you can actually dispense with passwords altogether, and thereby eliminate the possibility of passwords being stolen and used by attackers. Passwordless authentication is clearly the approach of the future — the not-too-distant future. SecureAuth’s recent surveys report that 83% of IT decision makers predict that their organizations will be passwordless within five years.

With SecureAuth, you can be ahead of the curve, enjoying the security of dozens of risk checks silently streamlining the workflows of your legitimate users, putting up a roadblock of 2FA for slightly suspicious authentication attempts, and blocking clear attacks outright — all while eliminating the hassle and risks associated with obsolete password use and maintenance.



“SecureAuth’s recent survey reports that 83% of IT decision makers predict that their organizations will be passwordless within five years. ”

Additional Benefits

In addition to the security and convenience of adaptive MFA, SecureAuth offers Single Sign- on (SSO), so users can authenticate just once to gain access to multiple systems. Behind the scenes, the platform will continue watching and will challenge or block the user if risk factors emerge that suggest something is amiss. SecureAuth also provides self-service options that enable users to enroll their devices, reset their own passwords, unlock their own accounts, and update their personal information, which can dramatically improve user satisfaction and productivity while slashing your helpdesk workload.

What’s more, SecureAuth solutions are built using industry-leading, standards-based technologies and do not require a rip-and-replace exercise. They fit right into your infrastructure, tying to your enterprise directories, applications, web servers, and VPNs while utilizing the same IDs, profile information, and policies you use today. You even get the flexibility of hybrid, on-prem, or cloud deployment options.

Conclusion

To protect the increasing amounts of valuable and sensitive data you store in Office 365, you adaptive, continuous authentication and authorization. Unfortunately, older Office 365 clients and many third-party solutions support only username and password authentication — leaving organizations that rely on those clients at risk. And although recently released Office 365 clients do support multi-factor and some adaptive authentication, they can't match the security and convenience that SecureAuth delivers. When it comes to Office 365 security, you don't have to compromise. With SecureAuth, you get both strong security and a seamless user experience.

About SecureAuth

More security shouldn't equal more obstacles. And, with Identity Management solutions from SecureAuth, leading companies worldwide find it easier than ever to create experiences that are as welcoming as they are secure.

Our AI-driven Risk Engine helps you deliver dynamic – and often invisible – authentication and authorization for your users, combined with a data privacy framework that protects their information and ensures their consent.

It all adds up to a virtual handshake at the digital door to your company. Making you more effective than ever at eliminating bad actors or incorrect authorizations. And giving your employees and customers the seamless and safe access they deserve.

Learn more at www.secureauth.com

SecureAuth. Welcome to Better Identity.

SECUREAUTH

Welcome to Better Identity.

©2024 SecureAuth Corporation. All Rights Reserved. www.secureauth.com

SecureAuthTM IdP is a trademark of SecureAuth Corporation in the United States and/or other countries.