yubico

Phishing-resistant MFA for privileged users

Secure data, technology, and people with YubiKey

Privileged users and their credentials should be considered maximum security assets, yet many organizations are leaving their privileged users open to attack. Forrester estimates that around 80% of data breaches are connected to compromised privileged credentials.[1] Today's sophisticated threat actors steal privileged credentials, typically through spear phishing, man-in-the-middle attacks, or credential stuffing, to gain access to critical systems or data. Or, they move laterally or vertically across the network and escalate privileges after initial entry, to reach an organization's crown jewels.

What makes privileged users such a magnet for cybercrime? And how should enterprises best protect them?

The first step in securing privileged user accounts is understanding who these users are. Step two is to discern how current access management and authentication frameworks are leaving them unprotected, and what to do to eliminate account takeovers in their entirety.

You may have more privileged users than you realize

Traditionally, privileged users were considered to be IT roles. But in today's digital world, privileged users may also be business users—anyone who operates at a higher level on the network, cloud, or application, with wide access to exploitable systems or IP such as customer, HR, finance, legal, or sales data.

This access to critical systems and sensitive data, now more ubiquitous than ever before, makes both privileged IT and business accounts a prime target for cyber criminals and malicious insiders.

Just as the number of functions who need privileged access is growing, digital transformation is driving more data beyond IT's control. Sensitive data is being sent into the cloud and across microservices. Remote and hybrid work are increasing risk through unsecured devices and home networks. If a data breach does occur, everyone in the organization suddenly becomes a privileged user—as threat actors look for credentials that will allow them to move through the network.

How IAM and PAM solutions create security blind spots for privileged users

A best practice for enterprises to strengthen security postures is by deploying identity and access management (IAM), privileged access management (PAM), and multi-factor authentication (MFA). But many organizations still find that they are vulnerable to phishing, targeted attacks, and account takeovers despite these precautions.

Access control solutions such as IAM and PAM play an important role in ensuring the right users have access to the applications and data they need. However, they still leave security blindspots that cybercriminals can easily exploit. Here are a few examples:

- Lack of differentiation between access and privilege rights
- Integrating privileged access with Single Sign-On (SSO) without deploying step-up authentication
- Unmanaged privilege accounts related to contractors, short-term, or terminated employees, or even those created outside of IT control (Shadow IT)
- Credential sharing and unsecure forms of authentication for admin accounts

Many of these gaps occur because most legacy access control solutions weren't explicitly designed to manage privilege. As a best practice for securing privileged accounts, organizations should follow the concept of least privilege. According to this concept, users should have different levels of privilege based on what they are required to see and do within a system. In other words, it calls for provisioning the least possible access (who has access to what) and the least possible privilege (actions that someone can take) associated with that access.

A PAM solution works by adding an additional layer of security by separating user account privileges and admin account privileges. This limits damage if a user identity is compromised. Privileged credentials should be vaulted and checked out for use, but these systems usually rely on the IAM for authentication, often requiring little more than a password or legacy MFA.

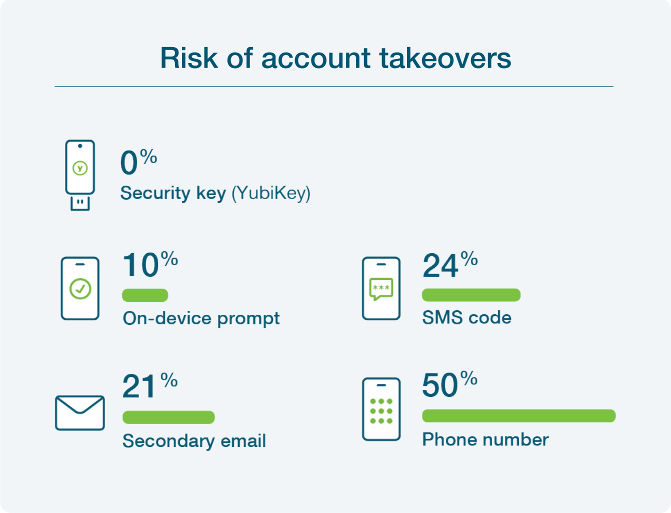
Legacy MFA further puts privileged users at risk for phishing and account takeovers

Legacy authentication methods such as usernames and passwords, and mobile-based authenticators such as SMS, OTP, and push notifications are all vulnerable to phishing, targeted attacks, and account takeovers.[2] That's because these forms of authentication rely on 'shared secrets' that can be breached by phishing attacks, malware, man-in-the-middle attacks, SIM swapping, and other forms of account takeovers. Today's cyber criminals can thwart legacy MFA in a way that's almost undetectable to the end user. When these attacks target privileged accounts, the risk for breach, ransomware, or cyber espionage grows exponentially.

To protect privileged user and admin accounts, all organizations should consider deploying phishing-resistant MFA using hardware security keys such as the YubiKey. Unlike username and password-based authentication, and legacy forms of MFA such as mobile authenticators, the YubiKey offers phishing-resistant and cost-effective authentication at scale.

YubiKeys provide 360º protection for privileged users

Yubico offers the YubiKey, a modern and high-security MFA solution designed to meet business needs to protect privileged users. Private keys are stored in the secure element on the YubiKey and cannot be exfiltrated, ensuring that privileged users and data are always protected. It's the only solution proven by independent researchers to stop 100% of account takeovers, including bulk and targeted phishing attacks.[3]



Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

	Legacy authentication	YubiKey
Security	At risk for account takeovers	Phishing-resistant strong authentication
Cost	Costs related to device and services, mobile management, password resets, plus potential data breach costs	Turnkey delivery, self-provisioning
User experience	Password + 2nd factor decreases productivity & leads to frustration, doesn't work in all situations	Single tap or touch to authenticate, no network or battery requirements
Protocol support	Single	Multiple-protocol support
Integrations	Standalone credentials per app, costly to manage	Single, interoperable credential stored on secure key
Portability	2FA can require mobile device or device readers	Portable root of trust

The YubiKey supports modern authentication protocols such as FIDO U2F and FIDO, as well as OTP, SmartCard, and OpenPGP, ensuring that a single key can work across legacy and modern infrastructures and applications. YubiKeys also offer an exceptional user experience (UX), driving adoption at scale. Users can login with just a single tap or touch of the YubiKey.

YubiKeys work out-of-the-box with leading IAM and PAM solutions, and integrate with dozens of 3rd party systems, including Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, PingID, RSA SecurID Suite and CyberArk.

Yubico offers flexible and cost-effective enterprise plans that help organizations with 500 users or more move away from legacy and broken MFA and accelerate towards phishing-resistant authentication at scale. With YubiEnterprise Subscription, organizations can benefit from a predictable OPEX model and more.

Subscription customers are also eligible to purchase additional services and product offerings, such as YubiEnterprise Delivery, a global turnkey hardware key distribution service to residential and office locations across 49 countries.

Privileged users hold the keys to any organization—keys that cyber threat actors will stop at nothing to get. Deploy phishing-resistant authentication to protect privileged users and your organization against modern cyber threats.

[1] Andras Cser, et. al., The Forrester Wave: Privileged Identity Management, Q4 2018, (November 2018)

[2] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

[3] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088