yubico

Secure Privileged Users and Accounts against AI cyber threats

Securing privilege users and accounts is table stakes

With Generative AI and Agentic AI accelerating the speed and scale of cyberattacks, securing privileged access has become an urgent need. Privileged accounts—including administrators, service identities, and cloud operators—remain prime targets; as do users across C-suite, HR, finance, marketing, and sales that have access to critical data.

AI agents are a new class of privileged identity — also called Non-Human Identities (NHIs). Like service accounts, they hold credentials and interact with sensitive systems, but they are able to make autonomous decisions at machine speed and can spawn sub-agents, multiplying both capability and risk. Zero trust principles should apply but the classical privileged access management (PAM) tool chain wasn't designed for multi-hop delegation chains or the latency requirements of agentic workflows. The governance gap isn't just who has access, but proving that a human authorized a specific decision in an auditable, tamper-evident way.

IAM and PAM can create security blind spots

Identity and access management (IAM) and PAM can strengthen cyber hygiene, but can also create security blind spots:

- 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 using legacy authentication for admin accounts

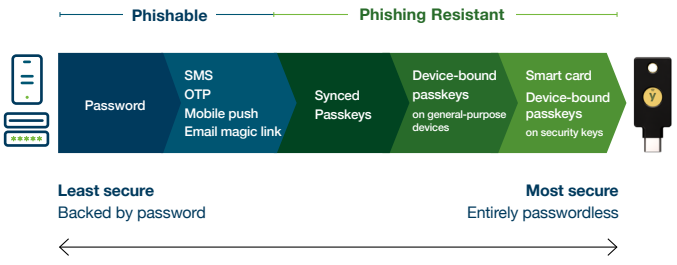
Organizations should follow the concept of least privilege — provisioning the least possible access (who has access to what) and the least possible privilege (actions that someone can take).

A PAM solution works by adding an additional layer of security by separating user account privileges and admin account privileges. Privileged credentials should be vaulted and checked out for use and also require phishing-resistant authentication.

Modern cyber threats demand modern security

Legacy authentication such as usernames and passwords, and mobile-based authenticators such as SMS, OTP, and push notifications are vulnerable to phishing attacks and account takeovers, and fail at scale against AI-driven cyber attacks.

The YubiKey, a hardware security key that contains the most secure passkey, is the modern industry standard for identity security, offering phishing-resistant multi-factor and passwordless authentication. By requiring a physical phishing-resistant security key with human authorization, account access is blocked against unauthorized remote access.



19 of the top 20 technology companies

8 of the top 10 media companies

9 of the top 10 financial services

8 of the top 10 retail companies

Securing privileged users and accounts with the YubiKey

YubiKeys are the only solution proven by independent researchers to stop 99.99% of account takeovers[1], including bulk and targeted phishing attacks. They also drive a 265% total return on investment and a password reset related help desk savings of over $450,000.[2]

To use the YubiKey to authenticate, users simply login with just a single tap or touch, increasing productivity with a 80% faster time to authenticate.

Total Economic Impact of YubiKeys

The Numbers You Can Achieve

265% ROI
Return of investment

8-month
Payback Period

Reduced security risk	Business growth	End-user productivity
$1.6M	$1.9M	$2.2M
Security operation efficiency	Help desk savings	Retired legacy MFA costs
$1.6M	$476K	$321K

YubiKey by the numbers[4]

The YubiKey supports modern authentication protocols such as FIDO2 and FIDO U2F, as well as OTP, SmartCard, and OpenPGP, ensuring that a single key can work across legacy and modern infrastructures and applications, helping bridge to a passwordless future.

Privileged users and accounts 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 privileged accounts and your organization against modern AI-driven cyber threats.

[1] Forrester The Total Economic Impact™ Of Yubico YubiKeys
[2] Ibid
[3] Forrester The Total Economic Impact™ Of Yubico YubiKeys
[4] Ibid

> “Attacks are becoming privileged-based, identity based and pretty much every report reinforces that identity is the real number one problem. Once the YubiKey started to be adopted, it became a very strong case for the right way to do things to protect the organization”
>
> **Morey J. Haber**,
> Chief Security Officer, BeyondTrust

Fast and frictionless deployment of passwordless at scale

To make it easy to deploy passwordless authentication at scale to secure digital identities against modern AI-driven threats, Yubico offers YubiKey as a Service for fast and frictionless deployment of enterprise-grade security

With YubiKey as a Service, organizations can benefit from simple and scalable global deployments of YubiKeys for their workforce, supply chain, and end customers. YubiKey as a Service offers customers a choice of form factors, replacement stock, and priority customer support, all for less than the price of a cup of coffee per month.

Customers also have access to turnkey Enrollment and Delivery services that help IT get users quickly onboarded and get YubiKeys shipped to end users across the world.

Users can even experience self-service ordering of YubiKeys, giving them the freedom to have the keys shipped to their preferred address anytime they need. YubiKey as a Service customers receive continual enhancements to available and new services assuring a smart and future-proofed security investment.

The YubiKey 5 Series

From left to right: Yubikey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano

Contact us
yubi.co/contact

Learn more
yubico.com

Yubico (Nasdaq Stockholm: YUBICO) is a modern cybersecurity company on a mission to make the internet safer for everyone. As the inventor of the YubiKey, we set the gold standard for secure, simple login, stopping account takeovers with phishing-resistant, hardware-backed authentication.

Our technology secures people in over 160 countries, delivering fast, passwordless access. Dual-headquartered in Stockholm and Santa Clara, we believe strong security should be within everyone’s reach. Learn more at www.yubico.com.