yubico

Proactive Security for Privileged Users

Building cyber resilient financial services

Every privileged user across the organization should be a maximum security asset, yet many organizations leave privileged users and their businesses open to attack. Forrester estimates that around 80% of security breaches involve privileged credentials[1], and according to Gartner 56% of IT leaders in enterprises have attempted a Privileged Access Management (PAM) rollout but failed to meet goals[2]. Today's sophisticated GenAI driven cyber threats can easily exploit users and gain access to critical systems or data if privileged users and privileged credentials are compromised.

You may have more privileged users than you realize

Privileged users were once considered to be IT and network admin roles. But privileged users are any user that operates at a higher level on the network, cloud, or application, with wide access to exploitable systems, IP or customer PII and financial data. These could be your C-suite, HR, bank tellers, call center workers, and others across the organization.

IAM and PAM solutions create security blind spots

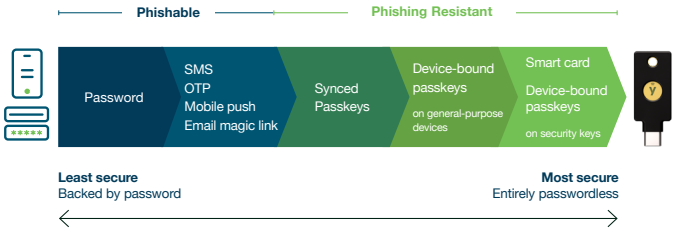
A best practice for financial organizations to strengthen security postures is to deploy identity and access management (IAM) and privileged access management (PAM). IAM and PAM play an important role to ensure the right users have access to the applications and data they need. However, they can leave 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 using legacy authentication for admin accounts

These gaps occur because legacy access control solutions weren't designed to manage privilege. Organizations should follow the concept of least privilege where users have different levels of privilege based on what they are required to see and do within a system — 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 IAM for authentication, often requiring little more than a password or legacy multi-factor authentication (MFA).

Legacy MFA further puts privileged users at risk

Legacy authentication such as usernames and passwords, and mobile-based authenticators such as SMS, OTP, and push notifications are all vulnerable to phishing and account takeovers. When these attacks target privileged accounts, the risk of a breach and ransomware grows exponentially. To protect privileged user and admin accounts, all financial services organizations should deploy modern, phishing-resistant passkeys across the enterprise because when it comes to a breach, every user is a privileged user.

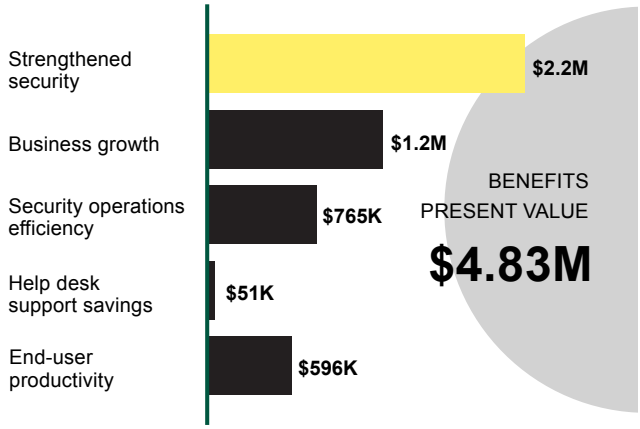


Deploy proactive security with the YubiKey

YubiKeys are hardware passkeys, the most secure form of passkey, that are also portable, allowing users to work across multiple devices including shared workstations, tablets and mobile devices that are common across financial services call centers and retail locations.

YubiKeys are the only solution proven by independent researchers to stop 100% of account takeovers, including bulk and targeted phishing attacks[3]. They also drive a 203% total return on investment and a 75% reduction in password related help desk tickets[4]. To use the YubiKey to authenticate, users login with just a single tap or touch, increasing productivity and offering the best experience and regulatory compliance for client-facing roles.

YubiKey by the numbers



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, helping bridge to a passwordless future.

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

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.

Getting started is easy

Don't put your users and business at risk of being hacked, get started with YubiKeys today!

To make it easy to deploy phishing-resistant authentication at scale using hardware passkeys, Yubico offers YubiKey as a Service and YubiEnterprise Delivery for easy procurement and delivery of Yubikeys.

- With YubiKey as a Service, organizations receive a service-based and affordable model for purchasing YubiKeys in a way that meets their technology and budget requirements. This service also provides priority customer support, ease of form factor selection, backup key discounts, and replacement stock benefits.
- With YubiEnterprise Delivery, organizations receive a cloud-based service that streamlines the distribution of YubiKeys to end-users, serving both domestic and international locations including residential addresses.
- Yubico also offers the Yubico Enrollment Suite, delivering a complete registration experience for easy enrollment of YubiKeys on behalf of users, with support for Microsoft and Okta currently, and additional Identity Provider (IdP) support planned to come on board.

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
yubi.co/finance

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.