



WHITE PAPER

# The critical strong authentication need for privileged users

Why legacy authentication is putting your privileged users at risk



# Contents

3	<b>Privileged users are your organization's biggest vulnerability</b>
4	<b>Who really is a privileged user?</b>
5	Every user can be considered a privileged user today
6	<b>IAM and PAM considerations</b>
7	Security gaps with IAM & PAM
9	Legacy authentication is putting your organization at risk
10	How modern phishing beats mobile-based authentication
11	<b>YubiKey: Phishing-resistant MFA with a great user experience</b>
13	<b>Twitter transitions all employees to security keys</b>
13	<b>Protecting privileged access at CERN</b>
14	<b>Protecting the development environment at Facebook</b>
14	<b>Secure privileged users with the YubiKey</b>
15	<b>Best practices checklist for protecting privileged users</b>
16	<b>Summary</b>



# Privileged users are your organization's biggest vulnerability

80%



of data breaches are linked to compromised privileged credentials

53%



of organizations experienced the theft of privileged credentials

85%



accessed critical systems and/or data

Privileged access management and securing privileged user authentication is a crucial need in today's cyber threat landscape. Forrester estimates that 80% of data breaches have a connection to compromised privileged credentials such as passwords, tokens, and certificates.<sup>1</sup>

Privileged users operate at a higher level on the network, cloud, or application, giving them wider access to exploitable data or systems, including corporate IP or customer data. They may also have administrative privileges to make changes or grant access to other users. With legitimate access to critical systems and sensitive data, these accounts are a prime target for cyber criminals and malicious insiders.

Attacks on privileged credentials begin with account takeover attempts (e.g. spear phishing, man-in-the-middle attacks, credential stuffing), or may involve privilege escalation after initial entry, to broaden access laterally or vertically and ultimately gain access to the crown jewels of an organization. Between May of 2020 and May of 2021, 53% of organizations experienced the theft of privileged credentials—in 85% of those thefts, cyber criminals were able to access critical systems and/or data.<sup>2</sup>

Malicious insiders can also pose a serious security threat, either directly abusing privilege or targeting others' privileged accounts. 63% of IT professionals say that privileged users pose the maximum insider security risk<sup>3</sup>, and 90% of organizations feel vulnerable to insider attacks, either directly against confidential business information (57%) or against privileged account information (52%).<sup>4</sup>

Most organizations today leverage a wide toolset to protect privileged accounts, such as least privilege access controls, including separating user identities from admin accounts or the use of identity and access management (IAM) and privileged access management (PAM) systems. However, very few organizations adequately differentiate between access controls and protection, leaving security blindspots related to the number of privileged accounts, the level of privilege, the process of authenticating to access systems, and the separation of personal and high level account credentials.

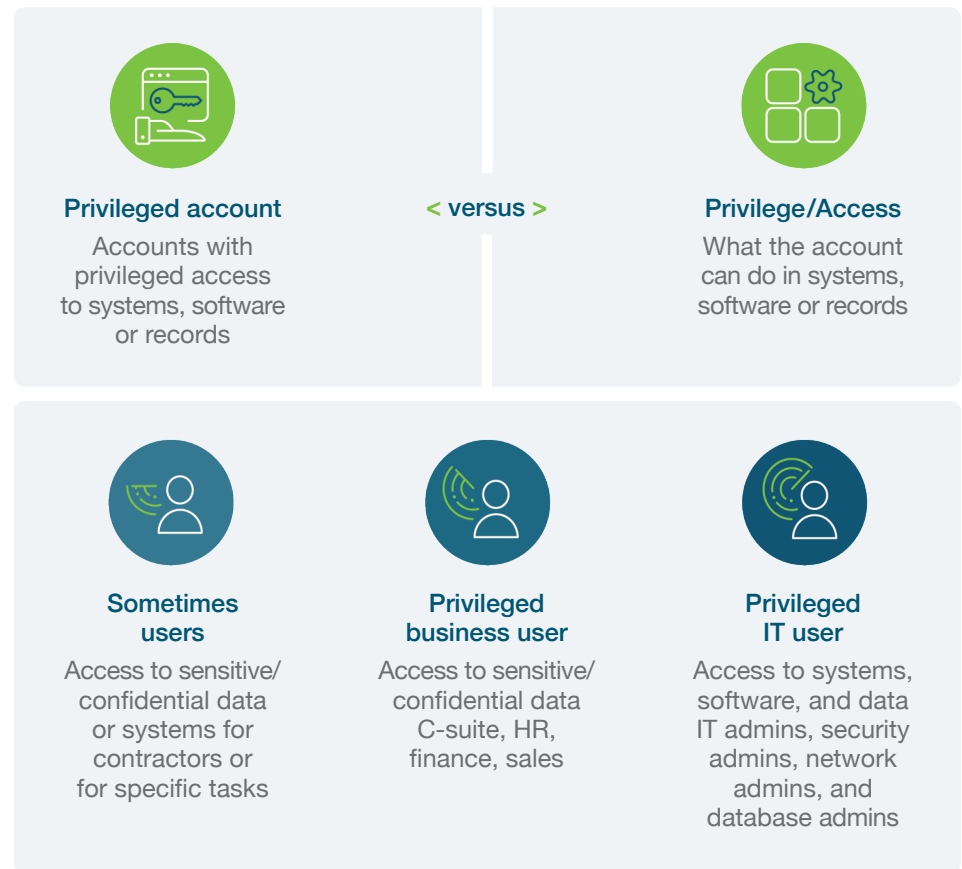
To create an effective cyber security program, the first preventative step an organization should take is to secure privileged accounts, credentials, and secrets with modern strong authentication.



# Who really is a privileged user?

23% of employees in an organization can be considered privileged users.<sup>5</sup>

A privileged user is anyone with elevated access to data or systems on the network, with wider access to corporate IP, sensitive networks and data, and critical infrastructure. According to research conducted by Ponemon Institute, an average of 23% of employees in an organization can be considered privileged users.<sup>5</sup> The number of privileged users goes up depending on the size of the organization and the sector. For example, a large engineering department in the high tech sector may have upwards of 1,000 privileged users.



A Ponemon survey indicated that **up to 49%** of organizations do not have policies for assigning privileged user access.<sup>6</sup>

Privileged users should have different levels of access based on what they are required to see and do within these systems. The concept of least privilege means to provision the least possible access (who has access to what) *and* the least possible privilege (actions that someone can take) associated with that access. For example, an HR admin and an IT admin both have privileged access to ADP, but the HR admin should have the privilege to view or add records, while the IT admin should have additional privilege to reset passwords or turn the service on or off.



# Every user can be considered a privileged user today

## Most frequently targeted privileged users<sup>7</sup>



65%

IT admins

21%

Engineers and developers

19%

C-Suite

61%

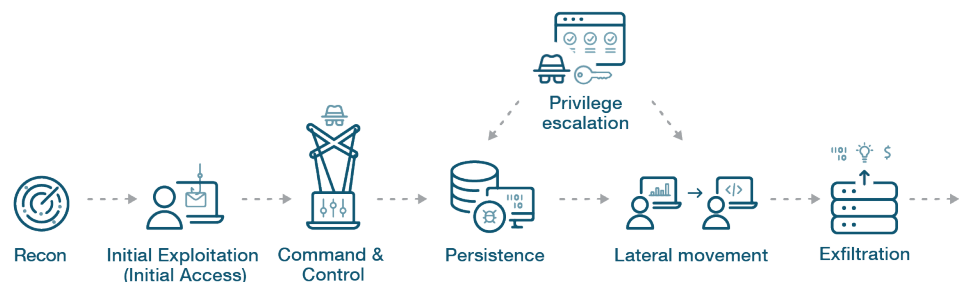


of data breaches traced back to **credentials**<sup>8</sup>

IT admins are the most frequently targeted privileged user (65%), followed by engineers and developers (21%) and the C-Suite (19%).<sup>7</sup> But in today's modern cyber threat landscape, every user can be considered a privileged user. What makes every user a privileged user? The answer — a security breach.

According to the 2021 Verizon Data Breach Investigation Report, 61% of data breaches can be traced back to user credentials.<sup>8</sup> Today's sophisticated threat actors leverage stolen credentials to move laterally on the network to search for or phish for credentials that ultimately escalate privileged access to high-value data assets and systems.

## Anatomy of a cyber attack



Traditionally, privileged users were thought of as those within IT roles who managed centralized systems and data. Today, most business activities are dependent on various types of sensitive data, increasing the number of people outside of IT who need privileged access. At the same time, digital transformation is driving more sensitive data into the cloud and across microservices, remote and hybrid work are increasing risk through unsecured devices and home networks, and shadow IT is driving more data outside the control of IT.

As the concept of privilege spreads to more business users, the same can be said in IT. In a DevOps world of continuous software development and integration, developers, operators and administrators are constantly making use of secrets that make the entire development organization privileged.

The fact of the matter is that there is a driving need to secure ALL privileged accounts, not just those traditionally considered privileged.

# IAM and PAM considerations

Up to **44%-59%** of organizations are leveraging more stringent controls for privileged password management.<sup>14</sup>

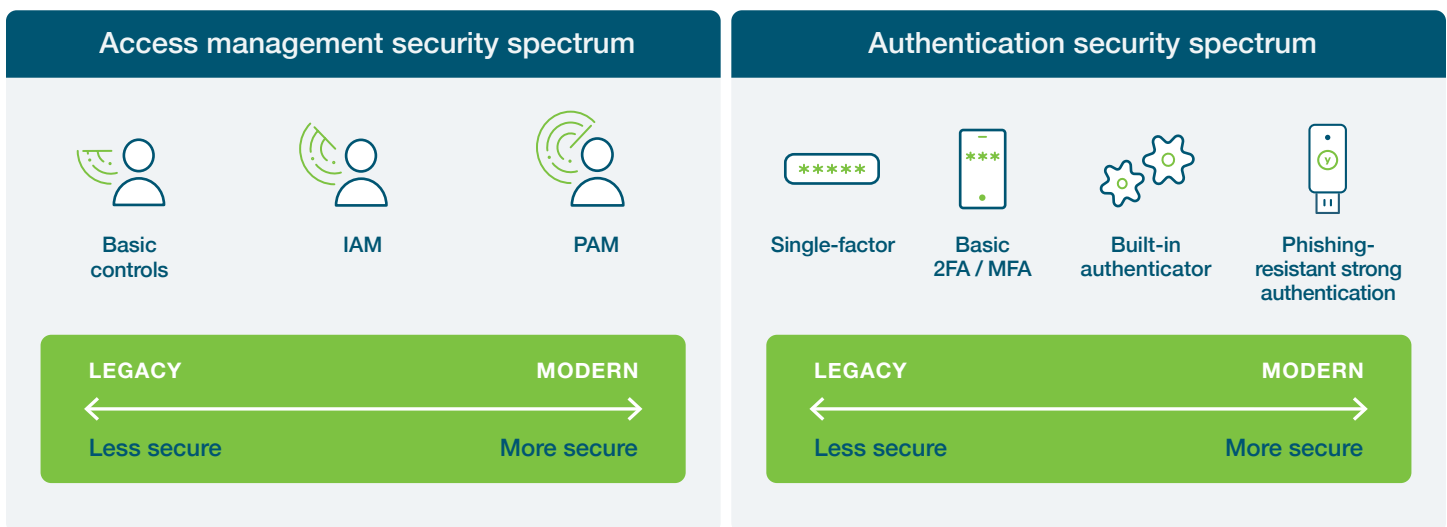
At the most basic level, organizations are securing privileged accounts with basic precautions that could include separate admin logins, often shared among teams, and often only single-factor protection such as username and password. In this scenario, privileged account credentials could be managed by IT or could be decentralized, and in some cases this “management” is in the form of a spreadsheet or paper logbook.

If you need any convincing that this is not the right approach, consider that the average employee has 191 passwords<sup>9</sup> they use at work, 73% of passwords<sup>10</sup> are duplicates, and 46% employees<sup>11</sup> share work passwords or accounts. Let's say you think these practices do not apply to privileged accounts, a shocking 40% of IT security leaders<sup>12</sup> don't change default admin passwords. Reasons such as these are why 80% of data breaches can be connected to compromised privileged credentials.<sup>13</sup>





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, but these legacy solutions were designed in a time of network-based security to specifically address the needs of privileged IT users. And most were designed to manage access — not privilege.

IAM solutions provide Single Sign-on (SSO) access to high level accounts based on group or individual identity, storing and controlling authentication within the IAM with the option to use two-factor authentication (2FA) or multi-factor authentication (MFA).





A PAM solution further protects IT privileged accounts by separating user identities from those that are more powerful to limit damage if an identity is compromised. Privileged credentials are vaulted and “checked out” for use, but these systems usually rely on the IAM for authentication, often requiring little more than a password (if anything). And, although there are barriers in place for access to the PAM, these barriers are not infallible. In an effective security strategy, the credential used for access to the IAM / PAM should not be the same as the credential that has elevated access accounts.



## Access management

Basic controls 	Identity and Access Management 	Privileged Access Management 	Governance 
Separate individual user and privileged account/admin identities.	A user identity is provided with least privilege access to systems and services upon authentication.	Privileged credentials managed separately from personal identity. Credentials are vaulted, checked out, and logged.  The least access with the least privilege granted to users for a specific request or task.	Identity Governance and Administration (IGA) where identity is at the center of IT operations, enabling and securing digital identities for all users, applications and data. This allows organizations to provide automated access to technology assets while managing potential security and compliance risks.

## Authentication

Single-factor 	Basic 2FA / MFA 	Built-in authenticator 	Phishing-resistant strong authentication 
Legacy username / password based authentication.	Legacy two-factor / multi-factor authentication such as mobile based authenticators (One-time passcode (OTP), SMS, authenticator app).	2FA or MFA with platform authenticator e.g. fingerprint, iris, facial recognition scan.	Hardware security key leveraged by all privileged users, that can be integrated with IAM / PAM. Separate credentials or security keys for privileged accounts.

## Security gaps with IAM & PAM

Many organizations face security gaps even with IAM, PAM, and 2FA/MFA. Organizations should consider the points below while building out their strategy:

- Lack of differentiation between access and privilege**  
 Occurs when access is assigned by group, with little to no attention to the level of privilege assigned to each group. Aside from over-provisioning privilege, difficulties arise in ensuring that activity is legitimate, or in redacting privilege that is no longer needed for a job or task.
- SSO vulnerabilities and privileged credential management**  
 While the goal of SSO is to reduce the burden of re-authenticating and ideally improve authentication practices around a single identity, privilege access should not be integrated with a user's standard SSO or the PAM system without deploying appropriate step-up authentication.



- **Credential sharing**

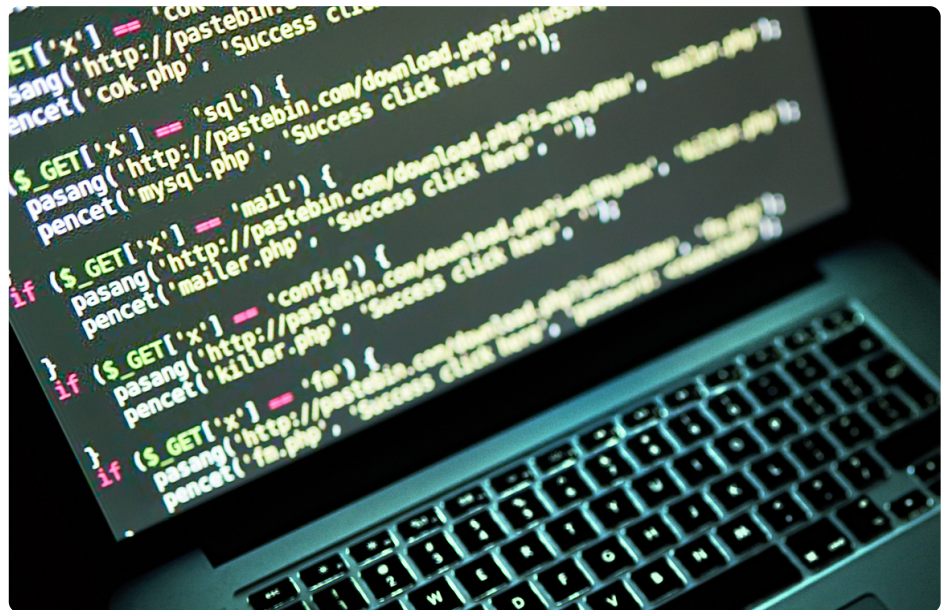
Many organizations create shared “admin” accounts that are used by multiple users. If these account credentials aren’t properly secured, it creates a security risk.

- **Unmanaged privilege**

Most organizations have some level of unmanaged privilege associated with employees or contractors no longer working for the organizations, unused identities or accounts, business or “sometimes” privilege users who are not covered by PAM, or accounts created outside the control of IT (Shadow IT).

- **Legacy authentication with IAM and PAM**

Using legacy approaches for 2FA and MFA can introduce security gaps as mobile-based authentication such as OTP, SMS, and push notifications are susceptible to malware, phishing, SIM swaps, and man-in-the-middle (MiTM) attacks.



# Legacy authentication is putting your privileged users at risk

Only **53%** of IT security professionals say their organizations require privileged users to use two-factor authentication<sup>15</sup>

Despite the elevated risks associated with privileged credentials, only 53% of IT security professionals say their organizations require privileged users to use two-factor authentication—and this only addresses access, not the level of privilege. Further, if we accept that every user can be a privileged user, only 44% of organizations require all employees to use 2FA. But the problem is not just the use, or lack of use, of 2FA or MFA, it is that not all forms of authentication are created equal.

## Not all authentication is created equal

### Risk of account takeover rates



0%

Security key

10%

On-device prompt

21%

Secondary

24%

SMS Code

50%

Phone number

#### Username & password



- Deployed everywhere
- Known usability gaps
- Costly hard to sustain
- Common target for credential phishing

#### Basic 2FA: SMS, email, mobile



- Not purpose built for security
- Uses existing technology stacks that are vulnerable to network and software attacks
- Common target for credential phishing

#### Security key



- Purpose built for security
- No network connection, stored data, or client software required
- Highly phishing resistant

While any form of multi-factor authentication (MFA) is better than no MFA, username and password or and mobile-based authentication such as SMS, one-time passcode (OTP), push notifications, and authenticator apps are all vulnerable to phishing, targeted attacks and account takeovers. Each of these authenticators rely on 'shared secrets' that can be breached by malware, man-in-the-middle (MiTM) attacks, SIM swapping, and other forms of account takeovers.

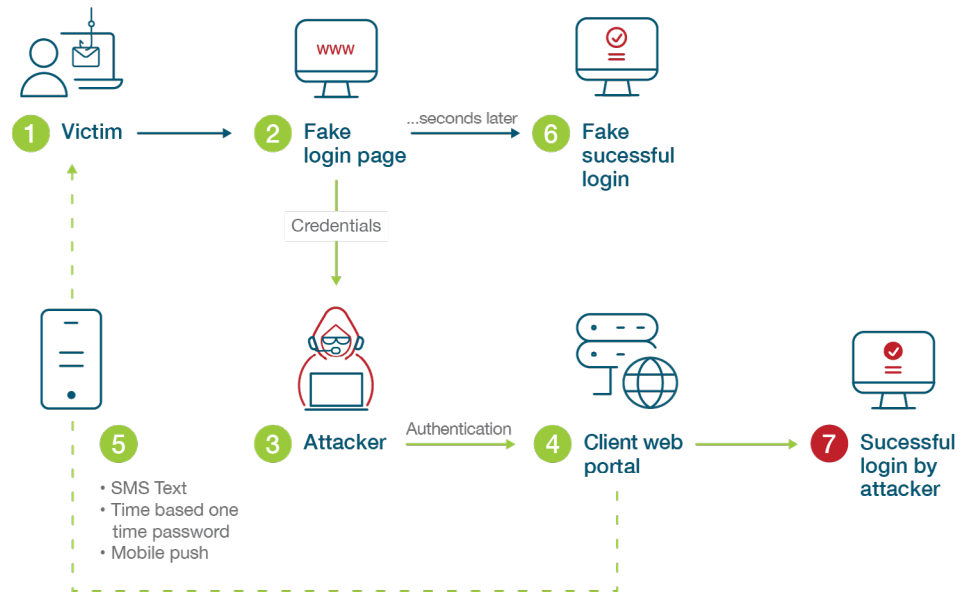
Most organizations are unaware of the risks inherent in legacy authentication. According to independent research by Google, accounts protected with SMS one-time passcodes face a 24% penetration rate—yet only 22% of respondents surveyed are aware that security could be a problem with SMS-based authentication.<sup>16</sup>

Further, many organizations are surprised by the hidden costs of mobile authentication. Organizations may be faced with carrying the costs of devices in addition to staffing and infrastructure to manage password resets (up to \$1 million each year, according to Forrester), as well as ongoing IT costs to register new devices or deal with lost devices.<sup>17</sup> Mobile-based authentication also comes with a heavy user burden, amplifying existing frustrations with passwords with a second step that is dependent on cellular network connections and battery levels. Any delay in mobile authentication decreases productivity and increases user frustration. Mobile authentication carries with it many hidden costs associated with devices, productivity, and support—not to mention the cost of a potential data breach. All together, it is estimated that the total cost of enterprise mobility can be as high as \$1,840 per owned device.<sup>18</sup>

## How modern phishing beats mobile-based authentication

Today's cyber criminals have ample and inexpensive tools at their disposal to make phishing websites, inject malware onto the device, intercept text messages or utilize SIM swapping to intercept, bypass, or otherwise thwart legacy MFA in a way that is almost undetectable to the end user:

Organizations in more highly regulated industries such as government, healthcare, energy and natural resources, and financial services may need to adhere to more stringent authentication standards in Federal Information Processing Standards (FIPS) 140-2 or National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63. These organizations have traditionally relied on legacy tokens or smart cards that rely on public key infrastructure (PKI). While these forms of authentication tick the box on security, they require heavy investments on the backend and may not always ensure user viability—they may not be appropriate for remote work, on mobile devices, or in situations with no network connectivity.



The diagram above shows an example of a successful phishing attack that is able to circumvent mobile-based two-factor authentication (2FA). In step 1, the attacker sends the victim a phishing email with a link that directs the victim to a fake login page that looks very similar to the real website. The victim enters their username and password which the attacker harvests and enters into the real website login screen in step 3. Because an OTP code is required for the second factor, the real website then sends out the OTP code to the victim in step 4, which the victim enters into the fake login page. In step 5 the attacker harvests the OTP code and enters it into the real website, gaining access to the account. The attacker usually also updates the account security settings to lock out the victim.

In this example, the end user has no idea that a phishing attempt has taken place or that their credentials have been successfully intercepted. When such an attempt targets privileged users, the potential risk for breach, ransomware, or cyber espionage increases.

If your organization relies on legacy authentication, it's time to consider that a modern threat environment requires modern, phishing-resistant authentication.



# YubiKey: Phishing-resistant MFA with a great user experience

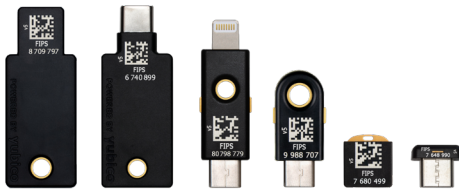
## The solution

The YubiKey is the **only** solution that is highly phishing resistant, and is proven to stop **100%** of account takeovers in independent research.<sup>19</sup>



### 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



### The YubiKey 5 FIPS Series

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



### YubiKey Bio Series - FIDO Edition

From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition

The YubiKey is a hardware security key, manufactured by Yubico, that offers easy-to-use two-factor, multi-factor, and passwordless authentication at scale.

The [YubiKey](#) uses modern protocols such as FIDO U2F and FIDO2 open authentication standards, with the hardware authenticator protecting the private secrets on a secure element, entirely eliminating phishing-driven credential-based attacks and supporting a user-friendly login flow.

Let's face it, it's frustrating to have to enter passwords or one-time passcodes all the time. And, as we all know, employees frustrated by a poor experience will not only be less productive and engaged, but also more likely to churn or circumvent the process—all of which are expensive outcomes. The YubiKey is a cost-effective and scalable solution that works out-of-the-box with leading IAM and PAM solutions, major browsers, and hundreds of applications and cloud services.

By supporting multiple authentication protocols on a single YubiKey, such as OTP, OpenPGP, and strong authentication protocols such as Smart Card, FIDO U2F and FIDO2/WebAuthn, the YubiKey offers organizations the flexibility to deploy strong authentication using a single key across a variety of legacy and modern infrastructures to support organizations no matter where they are on their passwordless journey.



The YubiKey also integrates with 3rd party systems and software that are used across enterprises for privileged access management including Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, PingID, RSA SecurID Suite, CyberArk, and others.

Organizations can separately store privileged credentials on a YubiKey, or have a separate YubiKey for privileged accounts, to provide a critical distinction between user identity access and privileged account protection.

The versatile YubiKey requires no software installation or battery so just plug it into a USB port and touch the button, or tap-n-go using NFC for secure authentication. YubiKeys don't require batteries, have no breakable screens, don't need a cellular connection, and are water- and crush-resistant.

	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
Single tap or touch to authenticate, no network or battery requirements	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

Yubico is a core contributor to the FIDO Universal 2nd Factor (U2F) and FIDO2 open authentication standards, and has contributed to open identity standards organizations W3C, IETF, FIDO Alliance and OpenID Foundation.

# Twitter transitions employees to security keys within 3 months



After a 2020 spear-phishing attack was able to bypass legacy 2FA authentication at Twitter, targeting high-profile Twitter accounts, Twitter began the process of modernizing their MFA with YubiKeys using FIDO2/WebAuthn security standards. As the New York State Department of Financial Services notes, the modern security standards of the YubiKey “would have stopped the hackers” in the 2020 attack.<sup>20</sup>

Twitter has implemented a combination of YubiKey 5 NFC and YubiKey 5C NFC across their entire workforce. Twitter relied on [YubiEnterprise Subscription](#) and [YubiEnterprise Delivery](#) services from Yubico to automate distribution of YubiKeys to over 5,500 employees within the US, Canada, and most of Europe. Employees were able to self-enroll their YubiKeys to access the single-sign on (SSO) system that is used to access internal systems, after which Twitter disabled legacy 2FA methods. The entire process took less than three months.

Twitter has taken a strong stance on the use of security keys both internally and for customers. “While any form of 2FA is better than no 2FA, physical security keys are the most effective,” notes a recent post on securing Twitter accounts.<sup>21</sup> Twitter has encouraged employees to use their YubiKeys for personal account protection, helping “promote a more secure web for everyone.”<sup>22</sup>

“We chose YubiKey because we found that it integrates rather easily with any operating system and with any client. We could therefore deploy it for all of our users, without having to change anything from the user side.

— Vincent Brillault,  
Computer Security &  
Incident Response,  
CERN IT Department

## Protecting privileged access at CERN

As a large, world-renowned research organization, CERN has many critical computing services and accelerators’ operations that make privileged account protection a top concern. In its continual evaluation of security, CERN’s CISO, Stefan Leueders, found that its administrator and operator accounts could be considered “a single point of failure.”

It was important for CERN to select an authentication solution that was simple to use and could integrate with existing systems without the need for drivers or expensive readers. CERN rolled out the YubiKey to its privileged users, starting with the Computer Security Team and later to administrators. The YubiKey is used as one of several multi-factor authentication tokens during single sign-on for web applications and for SSH login to servers.





# Protecting the development environment at Facebook

“Facebook is a very fast paced environment and we needed technologies that would allow us to maintain that pace. Because of the ease of use of Duo Security and Yubico authentication technologies, we have seen minimal support and overhead costs. Other technologies, such as traditional OTP-based hardware tokens, smart cards, and biometrics didn’t fully support our need to allow multiple and rapid logins to SSH sessions.

—John “Four” Flynn,  
Information Security  
Manager, Facebook Inc.

Facebook’s access to the personal information of billions of people make it a highly valuable target for cyberattacks. Every day, Facebook engineers initiate thousands of SSH development sessions, each one a risk point for cyber attacks to enter and move laterally through the organization.

“We wanted a 2FA solution to prevent that lateral movement,” notes John Flynn, Information Security Manager for Facebook. “So if an engineering laptop gets compromised, the attackers can’t pivot into the production environment and access critical data.”

Facebook needed a solution that would support multiple and rapid logins to SSH without the burden of needing to type in an OTP for every login. Facebook chose the YubiKey Nano combined with ecosystem partner Duo to support authentication every time a developer logs into the server. Since then, Facebook has scaled deployment globally to the rest of the company, helping future-proof the organization for today’s remote and hybrid work environment.

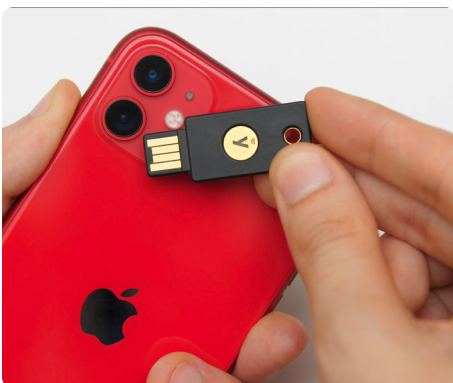
“When you have a two-factor system that’s good enough to use for every single SSH access instance, it’s easy to roll it out on your email system and VPN,” said Flynn.

## Secure your privileged users with the YubiKey



As the industry at large moves toward adopting Zero Trust security frameworks, authentication that is phishing resistant or impersonation resistant is a necessity. First, deploy YubiKeys to users your organizations consider as privileged to protect access to third-party applications and systems, including IAM and PAM. Next, roll out strong authentication incrementally to users who may not traditionally be considered privileged, including at-risk groups such as remote and hybrid workers and those outside of IT that have access to privileged data, DevOps teams, short term contractors, and those whose jobs interact with at-risk systems from time to time. Finally, strong authentication should be considered an end goal for your entire organization: employees, contractors, or even your supply chain.

Combining a YubiKey with IAM solutions such as Duo, Okta Adaptive MFA and PingID will allow for a consistent, secure and controlled authentication flow for critical applications and services across desktop and mobile. Security admins can use YubiKeys as a primary, back-up or step-up authentication factor, fully integrated into their security policies, all while allowing users to self-enroll their security keys in minutes. YubiEnterprise Delivery Services will even send the security keys to a user’s residence or workplace, across 49 countries around the world.



“Having strong authentication is a foundational security component of a Zero Trust architecture. Yubico and YubiKeys help fill the gap, for example, where weak passwords have been used, by providing validated, phishing-resistant security keys.

—John Kindervag, Creator of Zero Trust

# Best practices checklist for securing privileged users

Below are best practice considerations that organizations should consider while designing their authentication strategy for privileged users.



## Least access



Adopt a “just-in-time” access model to elevate access only for the time it is required



## Least privilege



Give the users the minimum they need for jobs or tasks



## Modern, strong authentication



FIDO U2F and FIDO2 open authentication standards



## Rotate passwords



Password rotation should be enforced



## Automate response



Ensure privileged account access can be shut down automatically in response to threats



## Risk analysis



Assess cloud environments to locate privileged identities or the presence of privileged data



## Silo credentials



Separate credentials used for access from privileged credentials



## Continuous monitoring



Track privileged account use to catch deviations



## Task automation



Reduce the need to access elevated systems by automating privileged tasks

Privilege access management best practices can also be extended beyond user roles to include machines, services, and APIs.

# Summary

Privileged users hold the keys to your organization—keys that cyber threat actors will stop at nothing to get. If your organization has done the work to set up strong access controls such as an IAM or PAM, don't let legacy authentication decisions become a \$4.24 million dollar mistake (the average cost of a data breach)<sup>23</sup>.

Deploy phishing-resistant authentication to protect your privileged users against modern cyber threats, and don't forget to include users outside of IT that aren't traditionally considered as privileged users. Define prescriptive security and policy strategies for IAM and PAM, and separate privileged accounts from users accounts. Finally, once your privileged users are secured, extend your strong authentication strategy to other parts of your organization to ensure that any risk of unwanted lateral movement and privilege escalation is minimized.



## Sources

- <sup>1</sup> Andras Cser, et. al., The Forrester Wave: Privileged Identity Management, Q4 2018, (November 2018), <https://www.forrester.com/report/The-Forrester-Wave-Privileged-Identity-Management-Q4-2018/RES141474>
- <sup>2</sup> ThycoticCentrify, More than Half of US Companies Hit with Privileged Credential Theft, Insider Theft in Last Year, (May 2021), <https://www.prnewswire.com/news-releases/more-than-half-of-us-companies-hit-with-privileged-credential-theft-insider-threats-in-last-year-301294644.html>
- <sup>3</sup> Cybersecurity Insiders' 2020 Insider Threat Report <https://gurukul.com/2020-insider-threat-survey-report>
- <sup>4</sup> Crowd Research partners, Insider Threat (2018), <http://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf>
- <sup>5</sup> Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020), <https://pages.yubico.com/2020-password-and-authentication-report/>
- <sup>6</sup> Ponemon, Privileged User Abuse & The Insider Threat, (May 2014), [https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn\\_257010.pdf](https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf)
- <sup>7</sup> ThycoticCentrify, More than Half of US Companies Hit with Privileged Credential Theft, Insider Theft in Last Year, (May 2021), <https://www.prnewswire.com/news-releases/more-than-half-of-us-companies-hit-with-privileged-credential-theft-insider-threats-in-last-year-301294644.html>
- <sup>8</sup> Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), <https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/>
- <sup>9</sup> LastPass, The Password Expose, (November 1, 2017), <https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose/>
- <sup>10</sup> Matt Bromiley, Bye Bye Passwords: New Ways to Authenticate, (July 2019), <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ>
- <sup>11</sup> Keeper, 4 Rules for Safe Password Sharing in the Workplace (April 2021), <https://www.keepersecurity.com/blog/2021/07/06/4-rules-for-safe-password-sharing-in-the-workplace/>
- <sup>12</sup> Alison DeNisco Rayome, Report: 40% of IT security leaders don't change default admin passwords, (November 2017), <https://www.techrepublic.com/index.php/article/report-40-of-it-security-leaders-dont-change-default-admin-passwords/>
- <sup>13</sup> Andras Cser, et. al., The Forrester Wave: Privileged Identity Management, Q4 2018, (November 2018), <https://www.forrester.com/report/The-Forrester-Wave-Privileged-Identity-Management-Q4-2018/RES141474>
- <sup>14</sup> One Identity, Executive Brief: Global Survey Results 2019 – Pass the Hash Attacks, (Retrieved October 25, 2021), [https://www.oneidentity.com/whitepaper/executive-brief-global-survey-results-2019-pass-the-hash-attacks8140582/?utm\\_source=none&utm\\_medium=Direct-Public%20Relations&utm\\_campaign=FY2020\\_Q3\\_Ali\\_PtH\\_exec\\_brief\\_PR&utm\\_term=&utm\\_content=](https://www.oneidentity.com/whitepaper/executive-brief-global-survey-results-2019-pass-the-hash-attacks8140582/?utm_source=none&utm_medium=Direct-Public%20Relations&utm_campaign=FY2020_Q3_Ali_PtH_exec_brief_PR&utm_term=&utm_content=)
- <sup>15</sup> Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020), <https://pages.yubico.com/2020-password-and-authentication-report/>
- <sup>16</sup> Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019), <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>; 451 Research, 2021 Yubico and 451 Research Study, (April 2021), <https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption>
- <sup>17</sup> LastPass, New Forrester Report: The Real Cost of Password Risks, (May 18, 2018), <https://blog.lastpass.com/2018/05/new-forrester-report-real-cost-password-risks/>
- <sup>18</sup> Wandera, Uncovering the True Costs of Enterprise Mobility, <https://www.clevermobile.it/risorse/file/wandera/tcwhitepaper.pdf>
- <sup>19</sup> Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019), <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>
- <sup>20</sup> New York State Department of Financial Services, Twitter Investigation Report, (Accessed September 14, 2021), [https://www.dfs.ny.gov/Twitter\\_Report](https://www.dfs.ny.gov/Twitter_Report)
- <sup>21</sup> Andy Saylor and Abbas Ali Haji, Stronger security for your Twitter account, (June 30, 2021), [https://blog.twitter.com/en\\_us/topics/product/2020/stronger-security-for-your-twitter-account](https://blog.twitter.com/en_us/topics/product/2020/stronger-security-for-your-twitter-account)
- <sup>22</sup> Nick Fohs and Nupur Gholap, How we rolled out security keys at Twitter, (October 27, 2021), [https://blog.twitter.com/engineering/en\\_us/topics/insights/2021/how-we-rolled-out-security-keys-at-twitter](https://blog.twitter.com/engineering/en_us/topics/insights/2021/how-we-rolled-out-security-keys-at-twitter)
- <sup>23</sup> IBM, 2021 Cost of Data Breach Report, (Accessed May 13, 2021), <https://www.ibm.com/security/data-breach>



## About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: [www.yubico.com](https://www.yubico.com).