



YUBICO COMPLIANCE EBOOK

Securing Your Critical Assets in an Ever-Changing Regulatory Environment

Security, Compliance and Modern Strong Authentication



Contents

2 Table of Contents

3 Global Compliance Trends

3 Changing Compliance Regulations

4 The Evolving Cyber Attack Landscape

5 Common Cyber Threats

6 Cyber Risk and COVID-19

7 Authentication in Today's Compliance Landscape

8 EU & US Cross-Industry Regulations

9 Healthcare

10 Finance

11 Energy and Natural Resources

12 Public Sector

13 Cybersecurity Frameworks

14 Modern Strong Authentication to meet Regulatory Compliance

14 What is Strong Authentication?

15 Modern MFA and the Passwordless Future

16 Modern Strong Authentication with the YubiKey

17 A Best Practice Checklist for Security and Compliance

18 Sources

Global Compliance Trends

A Cross-Industry Look at the Evolving Threat and Risk Landscape

Changing Compliance Regulations

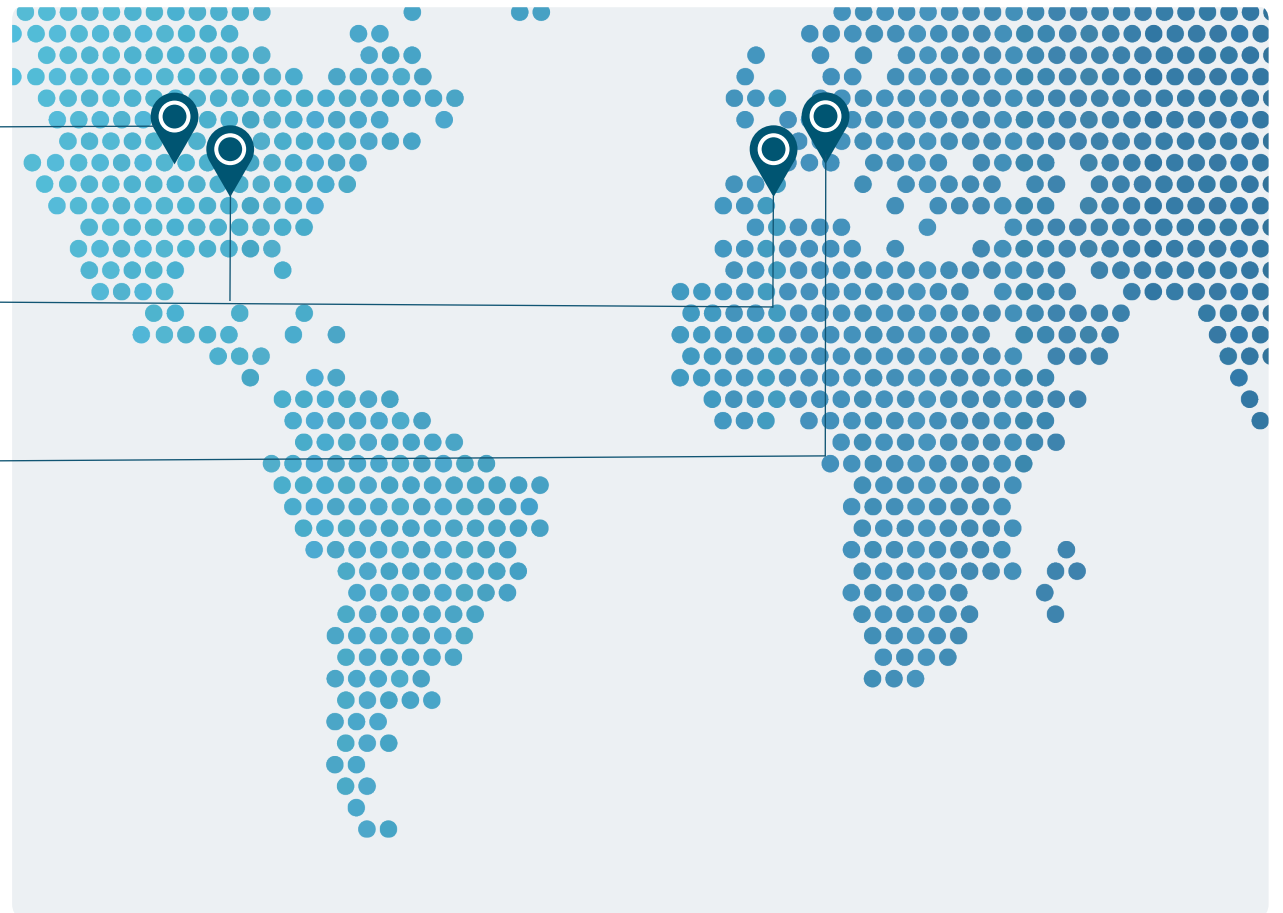
With the pace of technological change and the increasing frequency of cyber attacks, global regulators and policymakers have been enacting or modifying laws to protect sensitive and critical data at the industry, state, country, and global levels. The EU Global Data Protection Regulation (GDPR) of 2018 became the gold standard for data protection and user privacy, ushering in a rapid pace of regulatory change that has been further accelerated by the global COVID-19 pandemic.

- 27 State Data Privacy Bills introduced in the United States in 2021¹
- 4 in 5 United States voters want a Federal Data Protection Bill²

- PCI DSS 4.0 released in 2022

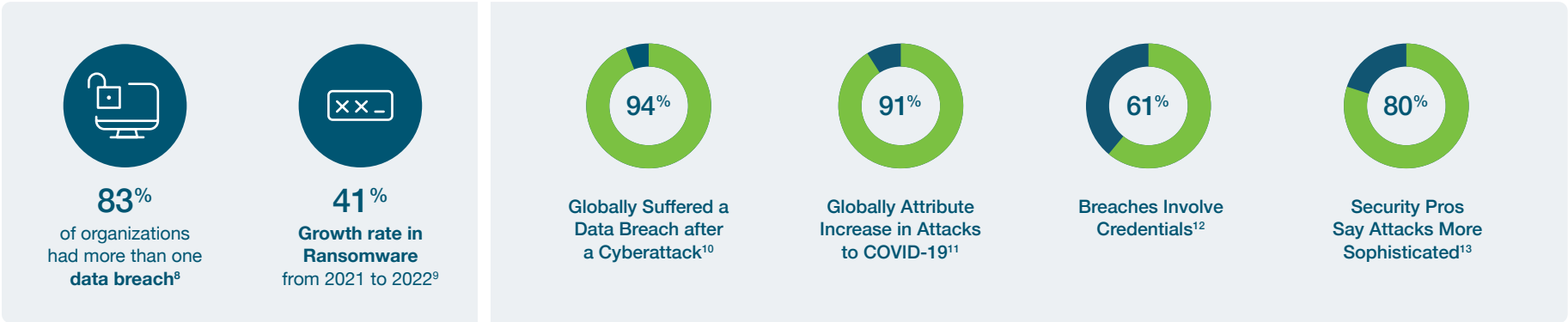
- European Union Drafts New SCCs for cross-border data transfers³
- EU's DORA to require Strong Authentication⁴

Only 47.9% of organizations believe they are succeeding at meeting compliance regulations.⁵

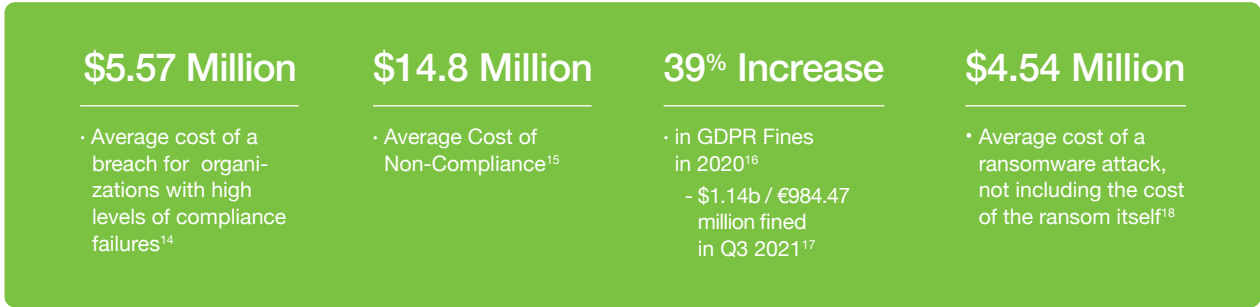


The Evolving Cyber Attack Landscape

The cyber attack landscape continues to accelerate, leveraging sophisticated technologies including machine learning and artificial intelligence. At least 13% of malicious breaches in 2020 were caused by nation state attackers, with attacks motivated by financial gain as well as a desire to disrupt and a desire to disrupt business.⁶ Cybercriminals are increasingly using COVID-19 themes in phishing attacks to more frequently target major corporations, governments, and critical infrastructure.⁷



Organizations across industries and government agencies alike continue to face rising costs associated with cyber attacks, including the loss of business, system downtime, ransomware payout and recovery costs, legal and audit costs, as well as regulatory fines.



Common Cyber Threats

Credentials are the most sought after type of data in the initial phase of a cyber attack, with threat actors leveraging this data to move laterally to find data or compromise more systems.¹⁹ Today's cyberattacks are often multi-step: leveraging a stolen credential or phishing attack to then deploy malware.

Hacking



Driven by **stolen credentials**

- 89% of hacks involve credential abuse²⁰

Many threat actors leverage stolen credentials to hack target systems, primarily web applications and mail servers.

Password spraying is a brute-force attack that uses common passwords against a large number of accounts to remain undetected.

Credential stuffing leverages breached username/password combinations.

Man-in-the-middle (MitM) attacks is a form of eavesdropping to spy, sabotage, or capture data—particularly credentials.

SIM Swap is when an attacker calls and tricks a mobile provider into changing a victim's phone number to an attacker-controlled SIM card. A 2020 Princeton study found that 17 of 140 major online services are vulnerable to SIM swapping attacks.²¹

Malware



Ransomware attacks cost **\$4.54 million**²²

Malware attacks, including ransomware and spyware, continue to rise, with a significant uptick associated with COVID-19.

Ransomware is a growing threat, with over 57% of victims making payments to recover data or prevent its exposure.²³

Leakware, unlike ransomware attacks that only encrypt data, also steals sensitive data in plaintext before it encrypts it. The ransomware actors then threaten to release the sensitive data to the public if the victims don't pay up.

Social Engineering



Phishing was the the costliest cause of a breach, averaging **\$4.91 million** in breach costs²⁴

Social attacks compromise people into taking an action that reveals credentials or opens a door for malware. Common social tactics include phishing or spear phishing and pretexting.

Phishing or spear phishing are acts of sending and emails to specific and well-researched targets while purporting to be a trusted sender. The aim is to either infect devices with malware or convince victims to hand over their information or money.

SolarWinds Attack Exposed 18,000 Customers

A Russian cyberattack created a backdoor in SolarWinds' Orion Software, installing malware to spy on government and private sector customers including Microsoft, Intel, and the Department of Homeland Security. It may be years before we realize the extent of this breach.²⁵ Investigations revealed additional vulnerabilities, including the password "solarwinds123" used to access the development server.²⁶ As a result, the Biden administration issued an executive order on protecting federal US government networks (EO 14028). This new order requires agencies, software vendors selling to the US government, and private sector organizations with access to operational technology to adopt zero trust frameworks, as well as multi-factor authentication and encryption for data at rest and in flight.²⁷

Colonial Pipeline Triggers New Regulation

A phishing attack introduced malware that shut down a gas pipeline responsible for 45% of the fuel for the east coast of the United States. After two days, and with uncertainty over the extent of the attack, CEO Joseph Blount agreed to pay a \$4.4 million ransom.²⁸

The Department of Homeland Security made rapid moves to enact cybersecurity regulations for the pipeline industry. The Transportation Security Administration (TSA) announced a new Security Directive that will require pipeline owners to identify and report on cybersecurity gaps, report on potential and confirmed cybersecurity incidents, appoint a Cybersecurity Coordinator 24 hours a day, seven days a week, and report confirmed or potential cybersecurity incidents.²⁹ Just two months later, a second Security Directive specifically directed pipeline owners and operators to implement specific mitigation measures against attacks and threats, to develop and implement a cybersecurity contingency and response plan, and to undergo an annual cybersecurity architecture review.³⁰

Cyber Risk and COVID-19

COVID-19 caused significant disruption to organizations around the world, accelerating the digital transformation toward a remote work economy—whether organizations were ready or not. Such rapid change introduced risks that are red flags for cyber security, including a blurring between work networks and home/public networks, as well as business and personal devices. According to the IBM Cost of Data Breach Report 2022, the cost of a data breach was \$1.00m higher where remote work was a factor in causing the breach.³¹

41%



of employees use their devices for both personal and work activities³²

10%



of employees lack even a basic PIN lock for their smartphone device³³

39%



of employees expect to continue to work from home post-pandemic³⁴

Authentication in Today's Compliance Landscape





After the passage of the GDPR in 2018, which became the new baseline for many data privacy regulations, global regulations have been evolving to keep pace in protecting data against increased cyber attacks and the changing technology landscape. While wide-sweeping regulations take many years to enact, we are more often seeing narrow laws, amendments, and executive orders attempting to bridge that gap. At the same time, the private sector has been stepping in to self-regulate with evolving governance and regulatory frameworks.

As the COVID-19 pandemic accelerates the global digital transformation, greater pressure is being placed on regulators and policymakers to protect the public from the risks associated with this “new normal.” That pressure is in turn transferred to security teams who must meet the burden of compliance.




Strong two-factor authentication (2FA) and multi-factor authentication (MFA) help eliminate the cyber risk associated with compromised credentials. Some regulations are beginning to spell out authentication minimums for access and control while others rely on frameworks to provide guidance. As a security professional, these are the key regulations to have on your radar.

EU & US Cross-Industry Regulations

 GDPR	 CCPA / CPRA
<p>General Data Protection Regulation (2018)</p> <ul style="list-style-type: none">• All EU data subjects• Consumer data rights• Data protection by design and default• 4% of global annual turnover or €20 million penalty, whichever is higher• “Appropriate technical and organizational measures” to protect and secure data³⁵	<p>The California Privacy Rights Act (2023) adds to the California Consumer Privacy Act (2020)</p> <ul style="list-style-type: none">• All residents of California• Consumer data rights• Data protection by design and default• \$2,500 per record (not incident) for each unintentional violation• “Reasonable security procedures and practices” to protect data³⁶

These regulations set the highest bar for general data privacy regulations across the EU and US. Following this trend, the Virginia Consumer Data Protection Act (CDPA) was signed into law on March 2, 2021, coming into effect on January 1, 2023.³⁷ On July 2, 2021, Colorado passed SB21-190, becoming the third state to pass wide-sweeping data privacy legislation, coming into effect on July 1, 2023.³⁸ Keep a close eye out for other states approving similar laws in the coming years.



 ISO/IEC 27001/2	 SOX
<p>International Organization for Standards</p> <p>Requirements for an information security management system (ISMS) and toward certification. ISO 27001 details the requirement for access controls, while 27002 introduces cryptographic controls.</p>	<p>Sarbanes-Oxley Act</p> <p>General advice to keep data “secure” and enforce access controls. However, SOX is based on SOC 2 (Service Organization Control), which favors multi-factor authentication (MFA).</p> <p>Potential for shifts in audit themes to reflect new needs (remote work).</p>
 EU Cybersecurity Act	
<p>International EU Network and Information Systems Agency (ENISA) Act</p> <p>Evolves the EU Network and Information Systems Agency (ENISA) to become the EU Agency for Cybersecurity, to establish a framework and oversee assessment.</p> <p>ENISA reports previously established 2FA as a base standard.³⁹</p>	<p>Electronic identification, Authentication and Trust Services</p> <p>Communication level “substantial” requires 2FA, “high” adds the requirement of tamper-proof authentication devices and dynamic cryptographic schemes.⁴⁰</p> <p>FIDO2 standards provide secure access compliant with eIDAS.</p>

Healthcare



 HIPAA Security Rule	 The HIPAA Safe Harbor Bill
The Health Insurance Portability and Accountability Act	HR 7898
<p>“Reasonable” physical, technical, and administrative safeguards for data security and authentication.⁴¹</p> <p>NIST is preparing to update its HIPAA guidance for the first time in 10 years.⁴²</p>	<p>This bill was signed into law on January 5, 2021 and is designed to amend the HITECH Act.</p> <p>The bill requires “recognized security practices,” further defined as those developed under the NIST framework. The bill asks regulators to consider these standards when looking at audits and fines.</p>
 CFR 21 Part 11	 EPCS
Code of Federal Regulations under the FDA for electronic records	Electronic Prescription for Controlled Substances
<p>The FDA requires certification that e-signatures in their systems are legally binding. A 2020 revision now requires that certification to use 2FA or MFA in compliance with FIPS 140-2.⁴³</p>	<p>Regulated by the Drug Enforcement Administration (DEA), the use of mobile devices requires two-factor authentication (hard token preferred), and a device compliant with FIPS 140-2.⁴⁴</p>

Financial Services



PCI DSS

The Payment Card Industry Data Security Standard

PCI DSS v3.2 required the use of multi-factor authentication to process payments.

PCI DSS 4.0 goes further by expanding the scope of accounts that require MFA, and changing password and MFA policies to align with updated MFA and InfoSec Guidance.⁴⁵



GLB Act / GLBA

Gramm-Leach-Bliley Act

Requires “administrative, technical and physical safeguards” appropriate to the size, complexity, and scope of activities.

In October 2021, the FTC released an update to the “Safeguards Rule” that requires multi-factor authentication for employee and customer access to systems.⁴⁶



FFIEC

Federal Financial Institutions Examination Council

Clearly articulates guidance stating that single-factor authentication is inadequate and that multi-factor authentication be considered.



PSD2

EU Payment Services Directive 2

Designed to produce safer and more innovative payments services, it mandates “dynamic linking” which links the payee to the user through strong authentication.



U.S. Consumer Financial Protection Bureau: Consumer Financial Protection Circular 2022-04



The August 11, 2022 Consumer Financial Protection Circular 2022-04 states that inadequate authentication, password management, or software update policies or practices are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers, and financial institutions are unlikely to successfully justify weak data security practices based on countervailing benefits to consumers or competition.

If a covered person or service provider does not require MFA for its employees or offer multi-factor authentication as an option for consumers accessing systems and accounts, or has not implemented a reasonably secure equivalent, it can trigger liability.

MFA solutions that protect against credential phishing, such as those using the Web Authentication standard supported by web browsers, are especially important.⁴⁷



Energy and Natural Resources



NIST CIP	EO 14028	TSA Security Directive Pipeline 2021-01	TSA Security Directive Pipeline 2021-01
<p>Critical Infrastructure Protection Standards</p>	<p>Executive Order on “Improving the Nation’s Cybersecurity”</p>	<p>First Directive, May 2021</p>	<p>Second Directive, July 2021</p>
<p>007-6 Enforce authentication for access controls</p> <p>005-6 Require MFA for all remote access sessions</p>	<p>SM 1.1 Use multi-factor authentication that is impersonation resistant for all users and administrators of EO-critical software.⁴⁷</p>	<p>Requires pipeline owners to identify and report on cybersecurity gaps, report on potential and confirmed cybersecurity incidents, appoint a Cybersecurity Coordinator 24/7, and report confirmed or potential cybersecurity incidents.⁴⁸</p>	<p>Requires pipeline owners and operators to implement immediate mitigation measures against cyberattacks consistent with NIST SP 800-82 standards.⁴⁹ The related GAO report directs owners to implement MFA for remote access.⁵⁰</p>

Public Sector



NIST NIST

National Institute of Standards and Technology Issues

SP 800-63 Digital Identity Guidelines

Lays out levels of authenticator assurance (AAL1-3) based on strength of authentication.

SP 800-157 PIV Credentials

Guidelines for public key infrastructure (PKI) credentials used for personal identity verification (PIV) cards.

SP 800-171

MFA required for all users who access controlled unclassified information (CUI).



FIPS

Federal Information Processing Standards

201-2 PIV Standard
MFA required to authenticate users.

140-2 Cryptographic Modules

Certiifiable security levels of private sector software or services for use by government.



DFARS

Defense Federal Acquisition Regulation Supplement

Contractors must adhere to SP 800-171 (which requires MFA).



FR FedRAMP

Federal Risk and Authorization Management Program

The Federal Risk and Authorization Management Program is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.



CMMC

Cybersecurity Maturity Model Certification

A certification framework based on DFARS.

Level 3 includes the requirements of NIST 800-171.



OMB Memos

United States Office of Management and Budget

OMB M-19-17

Allows for other strong authentication as alternatives to the PIV and CAC for contractors and citizens.

OMB M-20-19

Allows for other strong authentication as alternatives to the PIV and CAC in any use case, particularly new or remote workers.

OMB M-21-30

Amends EO 14028 to require a phased integration of NIST to protect critical software. Requires use of MFA that is impersonation-resistant.⁵¹

OMB M-22-09

On January 26, 2022, the Office of Management and Budget (OMB) M-22-09 memorandum set forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to use phishing-resistant multi-factor authentication (MFA) to reduce the threat from sophisticated attacks.

Cybersecurity Frameworks & Audits

NIST, HITRUST, & SOC 2



NIST

HITRUST



These frameworks help organizations understand cyber risks and provide organizations with a more tangible roadmap to comply with the “reasonable” and “appropriate” regulatory standards.

Both NIST and HITRUST frameworks suggest strong authentication, including a multi-factor combination of something a user owns, knows, and is. A SOC 2 report audits organizations against a number of frameworks including NIST, HIPAA, PCI DSS, ISO 27001 and ISO 27002. Two-factor authentication is considered a minimum baseline.⁵²

Two-Factor Authentication (2FA)

Combines two factors, typically one of which is a password.

Multi-Factor Authentication (MFA)

Combines two or all three factors.

Not all authentication is created equal

Username and password, and basic 2FA such as mobile-based authentication isn't strong authentication because it is highly susceptible to phishing and other remote attacks.

Modern Strong Authentication to meet Regulatory Compliance

It's clear that regulatory compliance is not slowing down cybercrime, but rather is an effort to constantly mitigate ever-evolving risk vectors. In order to do this, authentication is either explicitly or implicitly required by the major regulations, acts, frameworks, and audits, and many organizations may be ticking the box on security, but they are leaving the front door open by deploying sub-par authentication solutions. With a high rate of attacks focusing on credential theft, strong authentication holds the power to drastically reduce the success of cyber attacks.



Something you know
Password or PIN



Something you have
A physical device such as a phone or authenticator.



Something you are
A fingerprint, iris or facial scan

What is Strong Authentication?

1. Strong authentication can include 2FA or MFA. With the right strong authentication solution, and specifically modern MFA approaches organizations can achieve strong phishing resistance and robustly repel against credential phishing, man-in-the-middle attacks (MitM) and impersonation.
2. It does not rely solely on "shared secret" protocols (symmetric keys) at any point. This includes passwords and recovery questions, as well as all forms of mobile-based authenticators such as OTP, SMS codes, and push notifications.

Username and 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

YubiKey: strong authentication



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

Among the varied authentication protocols, only smart card and modern FIDO U2F and FIDO2/WebAuthn protocols satisfy the requirements of strong authentication and modern MFA.

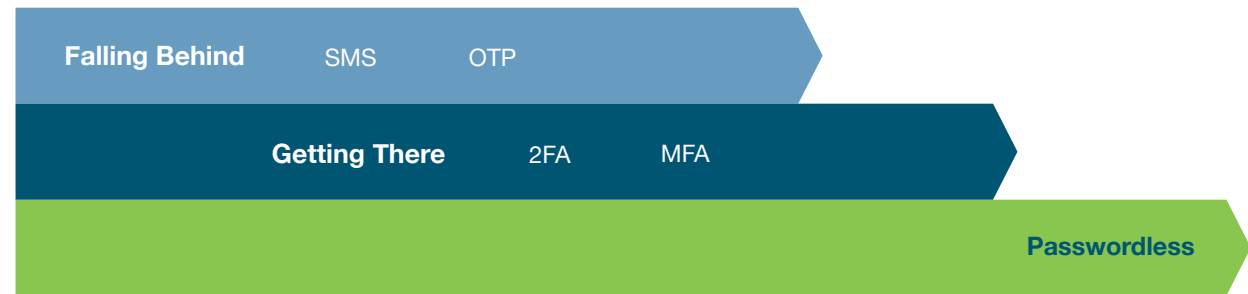
While mobile-based authentication is fairly common, they don't provide the best security or user experience. Mobile-based authenticators such as OTP, SMS codes, and push notifications are susceptible to malware, MitM, SIM swapping and account takeovers, and their usage can be impacted by device battery, network/cellular connections, and broken screens.

On the other hand, hardware security keys are purpose-built for security and are highly phishing resistant and durable. They require no network connection, store no data, and don't require any client software to be installed.

Passwordless is the Future

FIDO2/WebAuthn passwordless approach

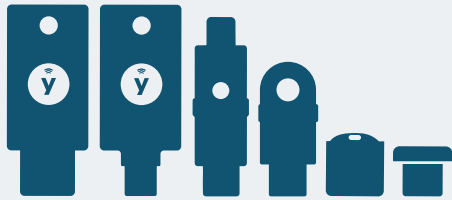
FIDO2 is the newest (introduced in 2018) FIDO Alliance specification for authentication standards, and WebAuthn is a web-based API that allows websites to update their login flow to add FIDO-based authentication on supported browsers and platforms. This is an evolving security ecosystem that will make adopting passwordless easier.



At their core, passwords are insecure—they are hard to remember, easily breached, and require validation against a server in order to work, opening up yet another avenue for breach. Passwords also require a lot of IT management and oversight such as enforcing more complex passwords, and then enforcing a change periodically per the security policies of the organization. With password-related calls to the helpdesk and downtime, this can all become very costly for the organization, not to mention still leaving it vulnerable to a breach. Therefore a move to secure passwordless account logins would eliminate much of the costs while enhancing the user experience.

Passwordless login flows often involve users entering in a PIN. However, unlike passwords that reside on a server that can be easily breached, a PIN is tied directly to a local device for authentication, but without being susceptible to remote attack. Also, unlike passwords, PINs don't need to be changed frequently and can be used for years. There are many instances of passwordless authentication, including smart cards (such as PIV and CAC cards) used in the US across the federal government.

FIDO2 is the passwordless evolution of FIDO U2F, a set of specifications around authentication. The overall objective for FIDO2 is to provide an extended set of functionality to cover additional use-cases, with the main driver being passwordless login flows.



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.

YubiKey offers a bridge to passwordless

Passwordless is a journey, not an overnight transition. With the YubiKey, organizations can implement FIDO2 passwordless, smart card passwordless or a hybrid strategy, depending on the existing infrastructure and use cases that need to be addressed. As the passwordless ecosystem continues to expand, this transitory period is what the YubiKey was designed for. Because the YubiKey supports the broadest set of security protocols, enabling a single security key to work across a wide range of applications and services, regardless of where organizations are in their passwordless journey.

Yubico offers the fastest way to meet today's complex compliance and security requirements, while accelerating your journey to passwordless. Take a stand against cyberattacks and future-proof your compliance stance with the YubiKey.

Modern Strong Authentication with the YubiKey

Yubico uses modern protocols such as FIDO U2F and FIDO2 open authentication standards to help eliminate phishing-driven credential-based attacks and satisfy the growing number of regulations that rely on the strict NIST framework.

The YubiKey is a hardware security key that provides strong phishing-resistant two-factor, multi-factor, and passwordless authentication at scale, helping organizations be compliant to MFA requirements across various industry regulations. It is the only solution that is proven to stop 100% of account takeovers in independent research.⁵³

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.



Smart Card/PIV

Out-of-the-box native integration for the Microsoft environment using Smart Card/PIV functionality based on the NIST SP 800-73 specification.



FIDO2 & FIDO U2F

Strong two-factor authentication using public key crypto to protect against phishing, session hijacking, man-in-the-middle, and malware attacks.



One time passcodes

Integrate Yubico OTP natively with the free YubiCloud authentication service or program unique TOTP or HOTP secrets.

YubiKeys offer the best of both worlds – the best available security against phishing attacks and account takeovers, as well as the best user experience. To authenticate, users simply tap/touch their security key to any kind of device, even modern devices such as mobile phones and tablets. YubiKeys also don't require batteries, have no breakable screens, don't need a cellular connection, and are water-resistant and crush-resistant.



Per the highest security requirements, YubiKey meets FIPS 140-2 certification requirements, Overall **Level 1** (Certificate #3907) and **Level 2** (Certificate #3914), Physical Security Level 3, and the highest level of assurance (AAL3) of NIST SP800-63B guidelines.

A Best Practice Checklist for Security and Compliance



Embrace zero trust

Treat each access request as a potential attack and authenticate the user before providing access to the network or any sensitive resource



Know your data

Manage your data retention policy and keep only what you need for long-term compliance mandates



Educate, educate, educate

Combine technology with employee education to spot and stop phishing and spear phishing attacks



Design security with UX in mind

Design for the new anytime, anywhere, and any device norm



Put privacy first

Most regulations are moving toward consumer rights, so be prepared to meet them



Think long term

Deploy solutions that work across legacy and modern infrastructures. They shouldn't become obsolete if existing regulations are updated, or new regulations are released

Sources

- ¹ IAPP, The Growth of State Privacy Legislation, (Accessed May 18, 2021), <https://iapp.org/resources/article/the-growth-of-state-privacy-legislation-infographic/>
- ² Sam Sabin, States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data, (April 27, 2021), <https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/>
- ³ Paul Voigt, The Draft Standard Contractual Clauses Proposed by the European Commission, (April 7, 2021), <https://www.mondaq.com/germany/privacy-protection/1055380/the-draft-standard-contractual-clauses-proposed-by-the-european-commission-legal-certainty-for-international-data-transfers>
- ⁴ European Commission, Digital Operational Resilience for the Financial Sector, (September 24, 2020), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN>
- ⁵ Cisco, The 2021 Security Outcomes Study, (Accessed May 14, 2021), https://www.cisco.com/c/m/en_us/products/security/cybersecurity-reports/security-outcomes-executive-summary.html
- ⁶ IBM, 2020 Cost of Data Breach Report, (Accessed May 13, 2021), <https://www.ibm.com/security/data-breach>
- ⁷ INTERPOL, INTERPOL report shows alarming rate of cyberattacks during COVID-19, (August 4, 2020), <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>
- ⁸ IBM 2022 Cost of a data breach report, <https://www.ibm.com/security/data-breach>
- ⁹ Tara Seals, Ransomware Volumes Hit Record Highs as 2021 Wears On, (August 3, 2021), <https://threatpost.com/ransomware-volumes-record-highs-2021/168327/>
- ¹⁰ VMware, Global Threat Report, (Accessed May 17, 2021), <https://www.carbonblack.com/resources/global-threat-report-extended-enterprise-under-attack/>
- ¹¹ Ibid.
- ¹² Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), <https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/>
- ¹³ VMware, Global Threat Report, (Accessed May 17, 2021), <https://www.carbonblack.com/resources/global-threat-report-extended-enterprise-under-attack/>
- ¹⁴ 2022 IBM Cost of a Data Breach Report, <https://www.ibm.com/security/data-breach>
- ¹⁵ DFIN, The Evolving Data Privacy landscape: GDPR, CCPA, and Similar Data Protection Laws, (March 31, 2020), <https://www.dfinolutions.com/insights/article/gdpr-ccpa-and-US-data-privacy-laws>
- ¹⁶ DLA Piper, DLA Piper GDPR fines and data breach survey, (January 19, 2021), <https://blogs.dlapiper.com/privacymatters/dla-piper-gdpr-fines-and-data-breach-survey-january-2021/>
- ¹⁷ Anna Boyce, GDPR fines of over \$1.1bn in Q3 2021 highlights the need for companies to take regulation seriously, (Oct 8, 2021), <https://bdaily.co.uk/articles/2021/10/08/gdpr-fines-of-over-11bn-in-q3-2021-highlights-the-need-for-companies-to-take-regulation-seriously>
- ¹⁸ IBM 2022 Cost of a data breach report, <https://www.ibm.com/security/data-breach>
- ¹⁹ Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), <https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/>
- ²⁰ Ibid.
- ²¹ Kevin Lee, et. al., An Empirical Study of Wireless Carrier Authentication for SIM Swaps, (January 10, 2020), https://www.issms2fasecure.com/assets/sim_swaps-01-10-2020.pdf
- ²² IBM 2022 Cost of a data breach report, <https://www.ibm.com/security/data-breach>
- ²³ Cyberedge Group, Cyberthreat Defense Report, (Accessed May 18, 2021), <https://cyber-edge.com/cdr/>
- ²⁴ IBM 2022 Cost of a data breach report, <https://www.ibm.com/security/data-breach>
- ²⁵ Isabella Jibilian & Katie Canales, The US is readying sanctions against Russia over the SolarWinds cyber attack, (April 15, 2021), <https://www.businessinsider.com/solar-winds-hack-explained-government-agencies-cyber-security-2020-12>
- ²⁶ Raphael Satter, Christopher Bing, et. al., Hackers used SolarWinds' dominance against it in sprawling spy campaign, (December 15, 2020), <https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solar-winds-dominance-against-it-idUSKBN28P2N8>
- ²⁷ David Treece, Quick Take: Executive Order on Improving the Nation's Cybersecurity, (May 13, 2021), <https://www.yubico.com/blog/quick-take-executive-order-on-improving-the-nations-cybersecurity/>
- ²⁸ Collin Eaton and Dustin Volz, Colonial Pipeline CEO Tells Why He Paid Hackers a \$4.4 Million Ransom, (May 19, 2021), <https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636>
- ²⁹ DHS, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, (May 27, 2021), <https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>
- ³⁰ DHS, Ratification of Security Directive, (September 24, 2021) [federalregister.gov/d/2021-20738](https://www.federalregister.gov/d/2021-20738)
- ³¹ IBM 2022 Cost of a data breach report, <https://www.ibm.com/security/data-breach>
- ³² Proofpoint, 2020 State of the Phish, (Accessed May 19, 2021), https://www.proofpoint.com/sites/default/files/gtd-pfpt-uk-tr-state-of-the-phish-2020-a4_final.pdf
- ³³ Ibid.
- ³⁴ HP, Blurred Lines and Blindspots, (May 12, 2021), <https://press.hp.com/us/en/press-releases/2021/hp-wolf-security-study-risk-remote-work.html>
- ³⁵ Intersoft Consulting, General Data Protection Regulation, (Accessed May 19, 2021), <https://gdpr-info.eu/art-32-gdpr/>
- ³⁶ National Law Review, CPRA Security Risk Assessments & Privacy Compliance, (November 6, 2020), <https://www.natlawreview.com/article/cpra-security-risk-assessments-privacy-compliance>
- ³⁷ Gibson Dunn, Virginia Passes Comprehensive Privacy law, (March 8, 2021), <https://www.gibsondunn.com/virginia-passes-comprehensive-privacy-law/>
- ³⁸ Meighan E. O'Reardon, Colorado's Emergent Consumer Privacy Bill Introduces Chance to Opt-Out of Data Processing, (July 8, 2021)
- ³⁹ ENISA, Authentication Methods, (Accessed May 20, 2021), <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods>
- ⁴⁰ FIDO Alliance, Using FIDO with eIDAS Services, (April 2020), <https://fidoalliance.org/wp-content/uploads/2020/04/FIDO-deploying-FIDO2-eIDAS-QTSPs-eID-schemes-white-paper.pdf>
- ⁴¹ Enzoic, Recommendations for HIPAA Password Compliance, (March 23, 2020), <https://securityboulevard.com/2020/03/recommendations-for-hipaa-password-compliance/>
- ⁴² Hogan Lovells, NIST seeks public comment to inform updates to HIPAA Security Rule guidance, (May 17, 2021), <https://www.jdsupra.com/legalnews/nist-seeks-public-comment-to-inform-7030190/>
- ⁴³ US FDA, CFR - Code of Federal Regulations Title 21, (April 1, 2020), <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?r=1311.55>
- ⁴⁴ US Department of Justice, Use of Mobile Devices in the Issuance of EPCS, (August 16, 2018), <https://www.deadiversion.usdoj.gov/GDP/DEA-DC-8%20Use%20of%20Mobile%20Devices%20in%20the%20Issuance%20of%20EPCS.pdf>
- ⁴⁵ Consumer Financial Protection Bureau, Consumer Financial Protection Circular 2022-04, <https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/>
- ⁴⁶ PCI, PCI DSS v4.0 Resource Hub, <https://blog.pcisecuritystandards.org/pci-dss-v4-0-resource-hub>
- ⁴⁷ FTC, Agency updates Safeguards Rule to better protect the American public from breaches and cyberattacks that lead to identity theft and other financial losses, (October 27, 2021), <https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial>
- ⁴⁸ NIST, Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028, (July 9, 2021), <https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf>
- ⁴⁹ DHS, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, (May 27, 2021), <https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>
- ⁵⁰ DHS, Ratification of Security Directive, (September 24, 2021) [federalregister.gov/d/2021-20738](https://www.federalregister.gov/d/2021-20738)
- ⁵¹ GAO, Critical Infrastructure Protection, TSA is Taking Steps to Address Some Pipeline Security Program Weaknesses, (July 27, 2021), <https://www.gao.gov/assets/720/715947.pdf>
- ⁵² NIST, Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028, (July 19, 2021), <https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf>
- ⁵³ IT Governance, SOC 2 Audits, (Accessed May 20, 2021), <https://www.itgovernanceusa.com/%20soc-reporting>
- ⁵⁴ 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>



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.