yubico

WHITE PAPER

Securing telecommunications against modern cyber threats

Modern, phishing-resistant MFA to bolster existing security approaches

Contents

$4.91 million

average cost of data breach with phishing as initial attack[1]

76%

of telecom employees **reuse passwords**[2]

82%

of data breaches tied to the **human element** social attacks, errors, misuse, credential theft[3]

The critical need for security and efficiency across telecommunications

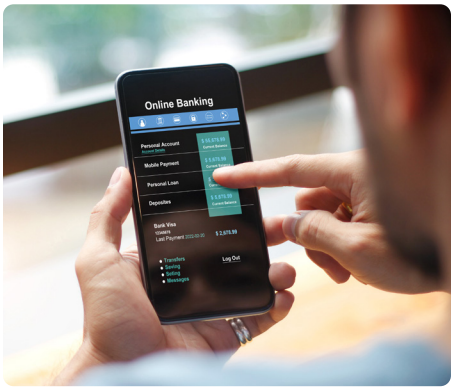
Telecommunication organizations, defined by CISA as 'The Communications Sector', provide the critical infrastructure used to support voice and data services including wired and wireless phone, satellite, cable and Internet services. These telecommunication organizations (telecoms) transmit and store vast quantities of data, increasingly making them a target for cyberattacks.

The telecom industry is increasingly subject to sophisticated cyberattacks such as ransomware, Man-in-the-Middle (MiTM) attacks, SIM swapping and account takeovers, with the purpose of stealing data, disrupting critical services, or spying on network transmissions. The combination of legacy infrastructure, third-party managed service providers, and new technologies, including 5G, cloud and virtualization, have created complex ecosystems that could make telecoms vulnerable to attacks. Further, telecom organizations who sell mobile phones, routers or other physical products have additional responsibilities to ensure the integrity of all parts used in the manufacturing process and to protect the code for any software on these products, such as custom front-end launchers on mobile devices.

Cyberattacks cause significant interruptions to critical infrastructure, result in the loss of consumer confidence, and lead to high costs, regulatory and otherwise. In fact, the telecom industry is subject to many new cybersecurity regulations, many of which now require the adoption of multi-factor authentication (MFA) and attention to the software supply chain.

Telecoms are actively seeking modern authentication solutions to improve internal and supply chain security and to address the growing number of authentication scenarios where current solutions are either inadequate or where mobile-based MFA is either insecure, not possible, or could be a source of friction for the employee or in the customer experience. Furthermore, telecoms who provision telephony or data services face additional pressure to take steps to protect consumers against mobile attacks, SIM swapping and fraud. Strong authentication leveraging the Fast Identity Online (FIDO) standard or smart cards are well placed to meet the varied authentication needs across telecoms.

> "Given that telecom companies control critical infrastructure, the impact of an attack can be very high and far-reaching. In fact, even the false claim of an attack can force a telecom company to shut down critical services that consumers and businesses rely on."
>
> —Deloitte[4]



The cyberattack landscape adds pressure to protect credentials

In June 2022, the FBI, National Security Agency (NSA) and the US Cybersecurity and Infrastructure Agency (CISA) jointly warned telecoms that hackers were increasingly targeting "overlooked" software flaws in routers, endpoint devices and other network infrastructure equipment.[5] According to a recent survey, telecom organizations, which includes the internet, are currently the most attacked industry for application-layer DDoS attacks.[6]

The telecom industry has been subject to notable attacks in the past two years, including the 2022 attack on Optus that impacted 9.8 million customers—the result of an attack that "was not particularly technologically challenging," notes Australia's Minister for Home Affairs Clare O'Neil.[7] In 2021, T-Mobile was the victim of two attacks, the first which impacted 50 million people and a more recent attack that resulted in some customers having their SIM illegally reassigned.[8]

Espionage is also a top of mind concern for telecoms operating phone or data networks. In 2021, it was revealed that the threat actor known as "LightBasin" was targeting the global telecom sector from at least 2016, stealing information including mobile subscriber identification numbers (IMSI), text message content, and call metadata—data useful for espionage.[9] The intrusions were attributed to a lack of security controls on core network and partner-managed systems, including deficiencies that allowed for credentials to be siphoned and re-used.

More recently, a phishing attack on Twilio connected to stolen credentials impacted 163 customer organizations.[10] Like many attacks, this breach involved infiltrating the organization through stolen credentials and phishing—a path that gives the attackers a path to further collect data or execute a ransomware attack. As the attacker simply logged in, they were disguised as a legitimate user.

How ransomware works

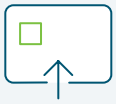
Not only did the Twilio attack highlight the weaknesses associated with credentials, Twilio is an organization that provides automated call and texting services, including SMS-based one-time passcodes (OTP)—a clear demonstration of the weaknesses associated with this legacy form of authentication. Not only could this access be used to kick off supply chain phishing attacks, the risk of SMS interception is so high that NIST called for SMS to be deprecated as a method of authentication.[11]

Evolving security regulations & cyber insurance requirements

Telecommunication organizations are subject to an increasing regulatory standard to implement MFA to protect against cyberattacks and malicious actors. The Federal Communications Commission (FCC) created guidelines to prevent SIM swapping and port-out fraud by requiring carriers to securely authenticate a customer before transferring a phone number to a new device or carrier.[12] Further, there is increased pressure to adhere to the MFA requirement of Executive Order (EO) 14028, both voluntarily as well as to secure Infrastructure Investment and Jobs Act funding. Further, in recognition of the vulnerabilities in legacy MFA solutions like SMS and push notifications, organizations should align with the new baseline requirement for phishing-resistant MFA, as detailed in OMB memo M-22-09. EO 14028 also introduces new security standards for the software supply chain for critical infrastructure, including software-based information and communication technology (ICT) products and services.[13]

What qualifies as phishing-resistant MFA?

Phishing-resistant authentication protocols



PIV/Smart Card

FIDO2/WebAuthn

Phishing-resistant MFA refers to an authentication process that is immune to attackers intercepting or even tricking users into revealing access information. The only two standards that are considered phishing-resistant are the Federal Government's Personal Identity Verification (PIV) / smart card standard and modern FIDO/WebAuthn, which enables strong two-factor, multi-factor, and passwordless authentication. All other forms of authentication, including mobile-based one-time passcodes (SMS or push app) and passwords, must be phased out.

Telecom organizations are subject to a variety of other regulations including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) and other similar state privacy laws. In the UK, the Telecommunications (Security) Act (TSA) recently became law, laying the groundwork for new cybersecurity obligations to protect data, software and equipment and take account of supply chain risks—with the potential noncompliance fines up to 10% of their turnover or £100,000 per day.[14]

As an organization that handles payment data, telecom organizations are also subject to the Payment Card Industry Data Security Standard (PCI DSS) and EU Payment Services Directive 2 (PSD2). The recently-released PCI DSS v4.0 will now require organizations to transition to the use of strong attack-resistant (phishing-resistant) MFA for all accounts that have access to cardholder data, at every instance and to implement a comprehensive information security policy to minimize cyber risk.[15]

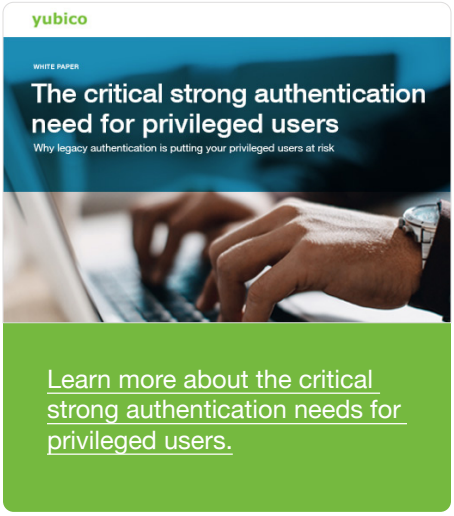
In addition to the new requirements of PCI DSS and EO 14028, FCC Chairwoman Rosenworcel recently proposed new data breach reporting requirements which would remove the waiting period for notifying consumers of a data breach and introduce new requirements to report breaches to the FCC.[16] Further, cyber insurance risk models have had to adapt to growing cyber attacks, with new minimum security requirements that require MFA.

*PCI DSS 4.0 8.3.1 clarifies that the new requirement does not apply to user accounts on POS terminals that have access to only one card number at a time to facilitate a single transaction. The new requirement would apply to privileged access on POS terminals (e.g. managers).

Common authentication scenarios and their vulnerabilities

Across telecommunications, authentication challenges can look quite different depending on the type of user and the situation or environment in which the authentication scenario is taking place. The most critical authentication scenarios are those that include access to core systems, devices, data or channels, with each additional ring representing additional authentication scenarios that bring unique challenges for telecoms.

- **Privileged users**
  Users with elevated access to data, devices, systems
- **Business & remote users**
  Business users with access to corporate systems, including remote teleworkers
- **Call center**
  In-house or third-party call center environment, sometimes mobile-restricted
- **Manufacturing & supply chain**
  Internal users and third parties with physical or virtual access to information systems, code, inputs, or intellectual property
- **Technicians**
  System technicians who log into corporate systems from off-network locations
- **Retail environments**
  Use shared devices or point-of-sale (POS) systems that tie into the brand's corporate environment for sales and customer service
- **Customers**
  Customer access to online accounts or loyalty systems



Learn more about the critical strong authentication needs for privileged users.

Privileged users

Privileged users have elevated access to systems, software, data or infrastructure, including privileged IT users such as engineers, IT admins, security admins, network or database admins and privileged business users including the C-Suite, HR, finance and sales who may have access to sensitive or confidential data. According to research conducted by Ponemon Institute, an average of 23% of employees in an organization can be considered privileged users.[17]

Further, Forrester estimates that 80% of data breaches have a connection to compromised privileged credentials.[18] Therefore, it is critical that privileged users and accounts have different levels of access based on what they are required to see and do within these systems, ideally least privilege, and that such access be protected with strong authentication and step-up authentication for the highest-risk actions.

Business & remote workers

With critical systems and PII data located across on-premises and the cloud, telecom organizations need a simple yet effective way to ensure applications and data are protected against unauthorized access. Coupled with an increase in attacks, remote work introduced new vulnerabilities such as unsecured home networks, unpatched devices, shared devices, and weak/reused passwords.

Telecom organizations are looking for secure, easy-to-use authentication solutions to ensure business and remote workers are able to securely connect to networks and applications to support productivity.

Further, as telecoms expand their digital footprint across new channels including eCommerce and social media, they need to address secure MFA to computers, servers and customer accounts, as well as create a system for secure code commits and code signing for the software being developed to support these commerce channels. As organizations leverage social media as a method to amplify their product or service offerings, strong MFA should be leveraged to secure these accounts.

Call centers

In 2015, the FCC reached a $25 million settlement with AT&T for failing to protect the privacy of its customers, prompting telecom providers to strengthen operations of in-house and third-party call centers.[19] Further, as call centers offer flexibility to staff with part-time and remote work—a trend that increased as a result of the global pandemic—the need to provision secure access to sensitive data has only increased.

Call center agents have access to PII, PCI and other sensitive data to address customer concerns or assist in customer transactions, making it important to verify call center agent identity before such access is granted. At the same time, security controls around authentication need to support response time SLAs.

To limit the risk of using mobile devices in a secure environment, or to support those call centers that are mobile-restricted by corporate policy, telecoms need a solution that will help secure a global workforce with a fast, seamless login to deliver efficient customer service.

Manufacturing and supply chain

In an industry that relies heavily on managed service-providers and third-party relationships to build and service a vast ICT infrastructure, systems and devices, a single weak point in the supply chain can result in costly consequences that put critical intellectual property (IP), infrastructure, goods and data at risk. For example, a telecom subsidiary in Australia recently breached confidential documents that included work orders, stock requisitions and business applications.[20] In fact, a recent survey found that up to 97% of organizations have had a cybersecurity breach as the result of a weakness in the supply chain.[21]

For the manufacture of telco products and equipment (phones, batteries, modems, circuit-switching systems, routers, etc.) telecoms must ensure the authenticity of all components to avoid unsolicited replication and theft, but also for quality assurance to ensure only original equipment manufacturer (OEM) parts (e.g. batteries) are included in the product. The standard approach to protect intellectual property (IP) and prevent counterfeiting in manufacturing involves the use of digital cryptographic signing keys and encryption backed by a hardware security module (HSM). Traditional HSMs are large and expensive rack-mounted devices that struggle to meet the unique manufacturing environments.

Yubico's YubiHSM 2 provides the security of an HSM but in a nano factor and a price point that allows organizations to deploy many YubiHSMs across their production lines to meet their needs. The future of securing manufacturing processes is further detailed in our whitepaper, Protecting manufacturing with highest-assurance security.

Technicians

Telecom technicians that install, operate or maintain networks and equipment need a way to access corporate systems for field updates from off-site locations without reliance on mobile networks, which may be down or unavailable in a remote location, and without a reliance on device battery.

Technicians also need access to corporate systems for corporate email, HR, or payroll systems. If these systems are used infrequently, organizations may experience a higher incidences of forgotten passwords and account lockouts, with impact on productivity and increasing IT support costs.

> "To become PCI DSS v4.0 compliant, retail environments will need to adopt MFA."

Retail environments

A customer-facing retail location may be owned and managed by the parent organization or may be franchise locations. Typically these locations have a mix of users and predominantly favor shared devices that tie into the brand's corporate environment.

It is common in telecom retail for employees to use a shared tablet or smartphone to support transactions and customer service. These shared devices are used by many people, in high traffic areas, and are prone to insecure practices around password sharing or password saving to cut down on login time necessary to be productive or to service guests. Often these positions are prone to high turnover, temporary, or seasonal workers. Further, accounts with elevated access to customer or system data (e.g. to issue refunds or access databases) are often not protected with more secure authentication. The common use of smartphones, tablets, wireless devices and near field communication (NFC) technology also introduces other mobile and wireless interception vulnerabilities. Additionally, for telcos in particular, retail employees have the capability to change a person's phone number to a new device, a level of privileged access that can easily be abused.[22]

Many of these shared devices rely only on a single authentication factor (password) or are used by multiple employees with a shared password. To address this security gap, and to become PCI DSS v4.0 compliant, retail environments will need to adopt MFA. While POS systems are highly regulated, and soon fall under the strict MFA requirements of PCI DSS v4.0 mandate, there is a wider need to optimize authentication across all of these shared device scenarios to support employee efficiency and productivity. In customer-facing scenarios, ease of authentication ties directly to customer experience (CX) goals. Learn more about protecting retail against modern cyber threats.

Customers

Most online customer accounts and loyalty programs still use legacy username and password-based authentication, which doesn't keep customers safe against phishing attacks or account takeovers. Further, as many cyberattacks now specifically target mobile devices, telcos that require MFA to confirm user legitimacy can take active steps to reduce the risk of SIM swapping.

Modernize MFA to address security, user and customer experience

Conventional MFA may be familiar, but falls short on security.

Vulnerable to attack
Every mobile authenticator can be phished

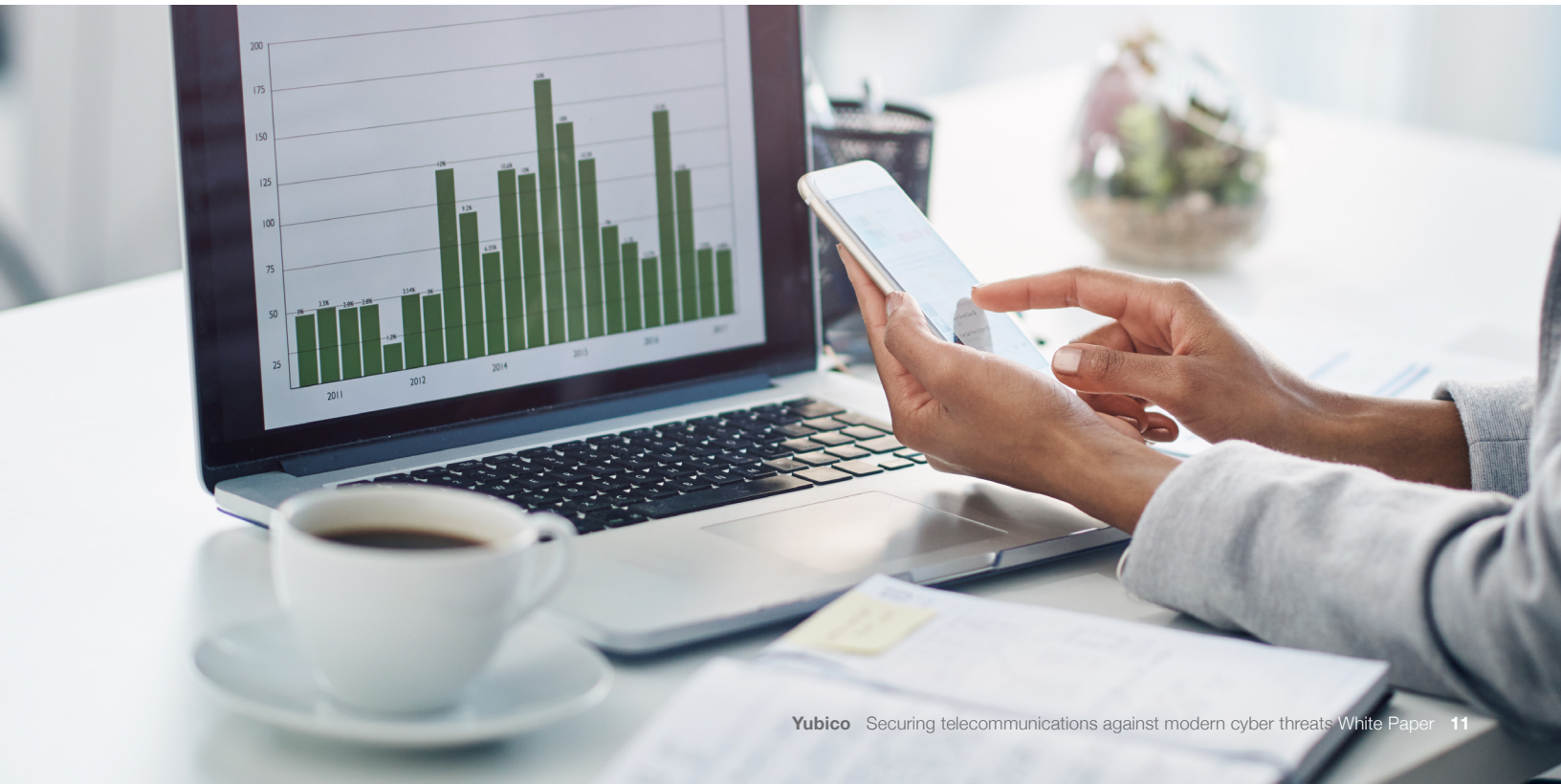
Expensive to maintain
$1840/user in enterprise mobility cost

Poor user experience
Complex to operate and manage

Security gaps
Many users can't or won't use it

Short-term solution
Legacy MFA isn't built for the future

Given the many incentives and imperatives to tighten cybersecurity postures, it's clear that traditional models of MFA fall short. Most authentication scenarios across telecoms have relied heavily on usernames and passwords, which are no longer effective to protect against modern cyber threats. However, the same can be true for more conventional MFA solutions including mobile-based authenticators such as SMS-based one-time-password or push app.



Meeting the customer experience demands of today

With a high rate of competition across telecom services, many telecoms find themselves competing on customer experience. Consumers have high expectations for service uptime, online and telephone customer service, and frictionless eCommerce capabilities. Friction and negative experiences across any of these points are likely to lead to high rates of churn. In fact, roughly 75% of subscribers signing up for services come from other networks, increasing customer acquisition costs and making it more difficult to recoup from infrastructure investments.[23] While network outages caused by cyber attacks can lead to customer churn, telecom providers have more control over variables that make up the customer experience across retail and eCommerce environments. The choice of MFA can have a significant impact on the customer experience.

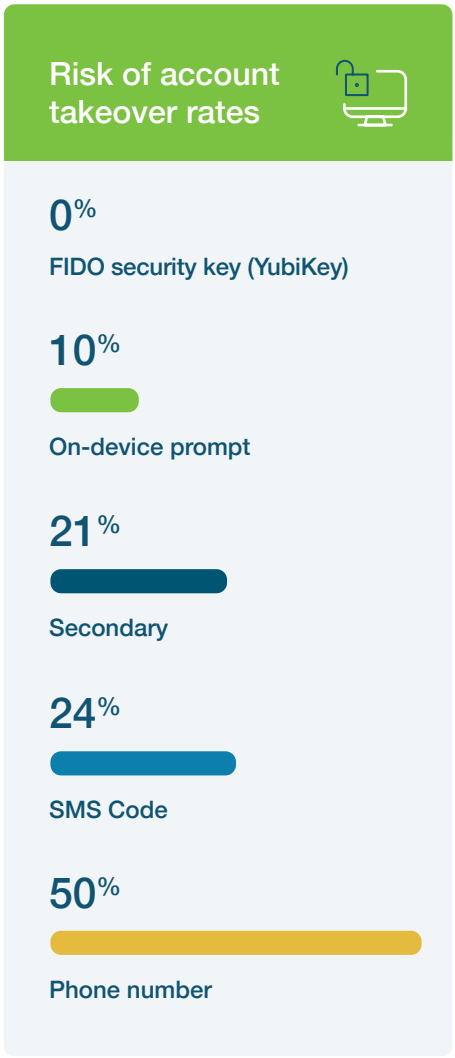
Scenario 1

Imagine, for example, if an employee had to refer to their personal mobile phone for an SMS OTP during a customer interaction? Not only does this process add delay, but it carries with it negative connotations about work ethic. Customer-facing technology must be supported by efficient, unobtrusive authentication to allow sales associates to provide a high level of attention.

Scenario 2

In an eCommerce interaction, any friction or delay in online experience of either purchasing a product and service, viewing the online account, or interacting with online customer service is likely to lead to dissatisfied customers—increasing churn and the customer acquisition cost. Every additional click and delay in the authentication experience, therefore, is costly. While customers are demanding secure online experiences, the choice of MFA must include consideration of customer experience.

In both scenarios, strong hardware-based authentication can replace the friction associated with passwords or mobile-based authentication, by offering a simple passwordless experience with the highest levels of security protection for employees, third party employees, and end customers.



Account takeover prevention rates
Google: How effective is basic account hygiene at preventing hijacking

While further ahead in security, mobile authentication actually increases the friction in the authentication experience—adding more steps and delays to authenticate. And that friction can impact the end customer, whether the friction originates during a customer-staff interaction or during customer authentication workflows to loyalty or booking systems. And as the Twilio example illustrates, mobile authentication continues to introduce an unnecessary level of risk.

Research by Google, NYU, and UCSD, based on 350,000 real-world hijacking attempts, revealed that a SMS-based OTP only blocked 76% of targeted attacks and a push app only blocked 90%.[24] That's, at minimum, a 10% penetration rate. With this approach, it's not a matter of if you will be attacked—it's a matter of when.

While considering authentication solutions for telecom environments, in addition to how effective the solution is in protecting against cyberattacks, organizations should also consider how the solution affects user productivity (account lockouts, login times), how reliable the solution is across varied environments and use cases, external variables which may negatively impact performance (e.g. cell signal and batteries) and the long-term total cost of ownership.

The future is passwordless

Given the inherent weaknesses associated with passwords, both from a security and from a usability perspective, global best practice is moving toward passwordless authentication—authentication that does not require the user to provide a password at login.

While moving from legacy MFA to passwordless authentication may seem like a big jump, it's a jump that completely bypasses the unnecessary dissatisfaction found with more conventional MFA methods and offers a solution that can bridge both legacy and modern informational technology (IT) and operational technology (OT) environments.

Modern authentication standards, including PIV/smart card and FIDO, enable strong two-factor, multi-factor, and passwordless authentication. FIDO2/WebAuthn is the most recent iteration of the FIDO standard, and uses public key cryptography for high security, where the private keys never leave the authenticator, enabling modern two-factor, multi-factor and even passwordless authentication.

Modern, phishing-resistant authentication with the YubiKey

The YubiKey delivers strong defense against phishing, convenient portable authentication and an exceptional user experience

Yubico created the YubiKey, a hardware security key that offers phishing-resistant security and exceptional user experience in a portable USB and nano form factor. With the YubiKey, users can securely and easily authenticate to more than 700 applications and services out-of-the-box including Google Suite, Microsoft Azure, and Microsoft Office 365 across a variety of devices with a simple tap or touch.

The YubiKey uses modern authentication protocols such as FIDO U2F and FIDO2 open authentication standards to help eliminate phishing-driven credential attacks. YubiKeys also support SmartCard, OTP, and OpenPGP protocols, enabling the use of a single security key across a variety of modern and legacy systems. The multi-protocol support allows organizations to leverage the YubiKey as a bridge to transition towards passwordless authentication.

The versatile YubiKey requires no software installation, battery, or cellular connection, making it ideal for shared device retail environments and for use by telecom technicians in the field. Users can benefit from a frictionless authentication workflow—providing access to accounts that is 4x faster than login with SMS. A single YubiKey conveniently works across multiple devices including desktops, laptops, mobile, tablets, notebooks, and shared workstations in manufacturing facilities.

	Username & password	Mobile-based authenticators	YubiKey
Security	Low, easily hacked.	Medium, 10 - 50% account takeover rates25	High, 0% account takeover rate[26]
Convenience	Password fatigue, account lockouts	Users that can't,won't, don't use mobile MFA	Seamless 'tap and go' user experience for MFA that is 4x faster to login than OTP, and offers a bridge to passwordless[27]
Reliability	Prone to human error	Reliant on device battery and cellular network. Not suited to mobile -restricted environments	Robust build, does not rely on cellular network or device battery
Cost	No up-front cost. High IT support cost. High potential risk.	$1,840 is the true cost of enterprise mobility per owned device28	Low cost compared to mobile MFA, and 92% reduction in support tickets[29]

Read the Forrester Consulting study

The Total Economic Impact™ Of Youbico YubiKeys commissioned by Yubico

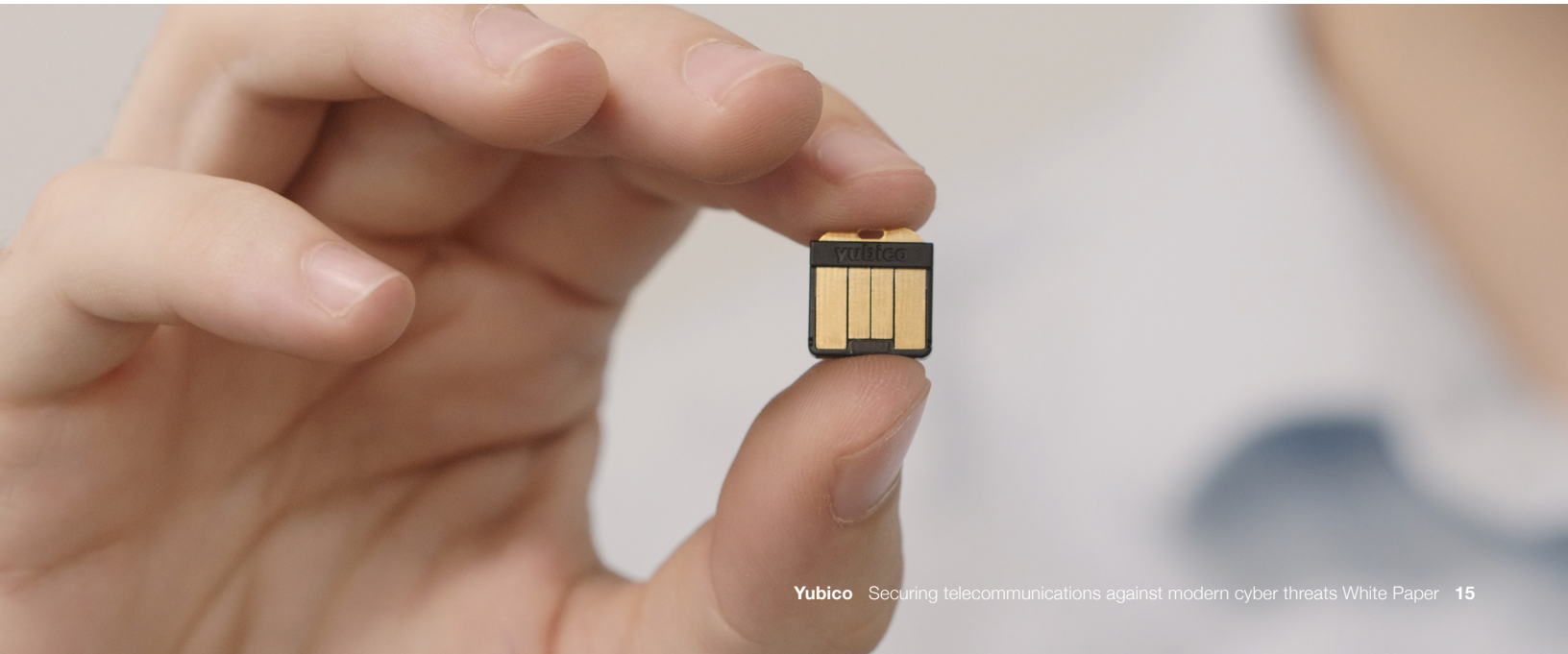
FORRESTER®

The YubiKey provides strong phishing-resistant two-factor, multi-factor, and passwordless authentication at scale, with the hardware authenticator protecting the private secrets on a secure element that cannot be exfiltrated. The YubiKey is the only solution that is proven to stop 100% of account takeovers in independent research.[30] As a phishing-resistant solution, the YubiKey helps simplify the information security policy requirements of PCI DSS v4.0 (12.1 and 12.2) while providing users with an easy to use experience that removes roadblocks that legacy forms of authentication such as passwords, mobile-based MFA provides.

For telecoms looking to drive 100% MFA coverage, the YubiKey from Yubico supports an immediate path to improved security. The Yubico Authenticator app allows you to store credentials on a YubiKey and not on a mobile phone. Further, the YubiKey allows organizations to leverage existing OTP authentication, helping organizations progress all the way to modern phishing-resistant authentication using either FIDO2 or smart card—all on one key.

Safeguarding manufacturing and the supply chain with YubiHSM 2

Telecoms must have a solution in place to protect the integrity and IP related to manufacturing and to secure external code and data (software) used in their products which includes hardware and devices such as: mobile phones, batteries, modems, circuit-switching systems, routers and others. Yubico has created the ultra-portable and low-cost YubiHSM 2, the world's smallest HSM. The YubiHSM 2 is being used to protect the manufacturing process by ensuring only certified programming stations can interface with the components, or to write digital signatures onto each component to ensure authenticity. Further, the YubiHSM 2 is ideally suited to safeguard the signing keys and certificates for signing code, helping support the secrets being shared within the supply chain. The future of securing the supply chain is further detailed in our whitepaper, Protecting the supply chain with highest-assurance security.



Yubico offers simple procurement and distribution of phishing-resistant security at scale

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.

YubiEnterprise Subscription

YubiEnterprise Delivery

With YubiEnterprise Subscription, organizations with 500 users or more can greatly simplify the acquisition and roll out of phishing-resistant authentication. Organizations can move authentication spend from CAPEX to a predictable OPEX model, and ensure security is always covered as business needs evolve, and experience benefits such as the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to deployment services, priority support and a dedicated Customer Success Manager.

Subscription customers are automatically entitled to access the Console, a web-based interface that helps organizations easily view orders, shipments, inventory status and a wide range of other information that helps with enterprise planning, and 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. Additionally, new YubiEnterprise offerings and additional enterprise capabilities will be designed explicitly for Subscription customers.

The Yubico's Professional Services team can provide tailored technical and operational guidance to help streamline your YubiKey implementation and rollout with services mapped to your needs, including:

- Technical integration services
- Deployment planning
- YubiKey lifecycle management
- User training and support
- Analytics and reporting

Yubico Professional Services can help with common questions about how to integrate YubiKeys into complex telecom environments, how to implement YubiKeys with identity providers or VPNs, and communication and education support to help support a successful YubiKey deployment. Accelerate your YubiKey adoption at scale with deployment best practices to enhance your security posture with phishing-resistant MFA.

CASE STUDY

Supporting retail POS with convenience and security

Retail Control Systems (RCS) markets and supports business management and point-of-sales (POS) systems to retailers. Subject to increasingly strict PCI (Payment Card Industry) compliance requirements, RCS sought a solution that could be used internally by RCS to secure remote admin access to systems, but also externally to protect access to sensitive data. Further, when implemented, the authentication method would need to not only scale with the growth of both the RCS customer base, but also their client's growth and needs.

Today, RCS authenticates over 11,000+ user logins with YubiKeys in a typical 48-hour period, helping protect devices as well as specific users and shared-user profiles. Their YubiKey deployment enables them to secure their endpoints, whether desktop computers, laptops, or POS hardware into a unified authentication platform that aids in security and PCI compliance.

Learn more from the Retail Control Systems' case study

Get the case study →

> "Instead of YubiKey being a highly recommended solution for our clients, we're moving towards making it a required solution. We are building it into our hosting suite, and into our user fees."

RCS

With the YubiKey

Reduce credential theft by 99.9% and helpdesk tickets by 75%, all while seeing an ROI of 203%.[31]

Summary

Telecommunication organizations face significant threats, threats that are amplified by the complexity of legacy infrastructure, a distributed workforce, and complex ICT supply chains. Telecoms require modern solutions to drive security and support complex authentication requirements.

Leading telecoms are deploying the YubiKey and the ultra-small HSM to protect against modern threats on all fronts and across the supply chain while driving compliance. The YubiKey meets and surpasses the efficiency requirements of today's telecommunication organizations, empowering users to quickly authenticate and become more productive and eliminating friction in the authentication experience that could be witnessed by customers in the retail environment. The YubiKey is a bridge solution to meet organizations where they are on their journey to passwordless, supporting legacy infrastructure and more modern PIV/smart card and FIDO2/WebAuthn standards.

Further, leading telecommunication organizations are prioritizing the safety and privacy of consumer authentication experiences to drive competitive differentiation and show their customers that they care about their digital safety.

Sources

1 IBM, 2022 Cost of Data Breach Report, (Accessed October 13, 2022)

2 SpyCloud, Telecommunications Industry Credential Exposure, (2021)

3 Verizon, 2022 Data Breach Investigations Report, (Accessed August 22, 2022)

4 Deloitte, Global Cyber Executive Briefing: Telecommunications, (Accessed October 14, 2022)

5 CISA, Alert AA22-158A, (June 7, 2022)

6 Cloudflare, Cloudflare DDoS threat report, 2022 Q3 (October 12, 2022)

7 Eileen Yu, Optus reveals extent of data breach, but stays mum on how it happened, (October 3, 2022)

8 Mitchell Clark, Another T-Mobile cyberattack reportedly exposed customer info and SIMs, (December 28, 2021)

9 Jamie Harries and Dan Mayer, LightBasin: A roaming Threat to Telecommunications Companies, (October 19, 2021)

10 Lily Hay Newman, Why the Twilio Breach Cuts So Deep, (August 27, 2022)

11 Rob Lemos, The state of two-factor authentication by text: What security pros need to know, (Accessed Sept 14, 2021)

12 FCC, FCC Proposes Rules to Prevent SIM Swapping and Port-Out Fraud, (September 30, 2021)

13 The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021)
OMB, Moving the US Government Toward Zero Trust Cybersecurity Principles, (January 26, 2022)

14 Harry Baldock, UK Telcos to Face Stricter Cybersecurity Obligations Under New Government Rules, (August 31, 2022)

15 PCI SSC, PCI DSS v4.0, (March 2022)

16 FCC, Chair Rosenworcel Circulates New Data Breach Reporting Requirements, (January 12, 2022)

17 Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020)

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

19 Karen Painter Randall, FCC Fines AT&T $25m for Data Privacy Lapse, (April 15, 2015)

20 Mihir Bagwe, Singtel Confronts Multiple Data Leaks, (October 10, 2022)

21 BlueVoyant, Managing Cyber Risk Across the Extended Vendor Ecosystem 2021, (Accessed February 2, 2021)

22 Lorenzo Franceschi-Bicchierai, How Criminals Recruit Telecom Employees to Help Them Hijack SIM Cards (August 3, 2018)

23 Arthur Hughes, Churn reduction in the telecom industry, (Accessed October 19, 2022)

24 Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)

25 Kurt Thomas, et. al, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)

26 Ibid

27 Ibid

28 Wander: Uncovering the true costs of enterprise mobility, (Accessed August 5, 2022)

29 Kurt Thomas, et. al, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)

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

31 Forrester, The Total Economic Impact™ Of Yubico YubiKeys, (September 2022)

yubico

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.