yubico

WHITE PAPER

Securing energy and natural resources against modern cyber threats

Modernize MFA and go passwordless to protect critical infrastructures and resource flow

Contents

The critical need for security and efficiency across energy and natural resource organizations

$5.29 million

cost of data breach in energy[1]

$442 million

is approximately the amount that the cyber insurance market for energy is anticipated to grow by 2030[6]

Energy and natural resource services are an invaluable part of critical national and international infrastructures, making them an ideal target for cyberattacks that can cause operational disruption. Cyberattacks not only cost energy and natural resource organizations an average of $5.29 million,[1] but can also result in loss of production time, intellectual property, product integrity and potentially cause an impact to life. The unique landscape of information technology (IT) and operational technology (OT) that exists within the upstream, midstream and downstream flow of natural resources only exacerbates the many touchpoints and handoffs that need to be secured against modern day cyber threats. Additionally, what makes this sector a key target is because many utilities may fall under the cybersecurity poverty line, which refers to those below the poverty line who do not have enough budget or human resources to implement security measures.[2]

Attacks across this sector have become commonplace around the globe. The 2021 Colonial Pipeline attack which caused tens of millions of USD dollars of damage and impacted millions of people in the Eastern United States all because of one compromised password,[3] only magnified that energy and natural resources organizations are prime targets for sophisticated ransomware and advanced persistent threat (APT) adversities such as phishing, SIM swaps and Man-in-the-Middle (MiTM) attacks. In February 2022, a cyberattack on the European oil refining hubs of Amsterdam-Rotterdam-Antwerp (ARA) disrupted the loading and unloading of refined product cargoes amid a continental energy crisis.[4]

The Colonial Pipeline attack along with the 2020 SolarWinds attack were also drivers of regulatory change mandating the use of phishing-resistant multi-factor authentication (MFA). Since the energy industry falls under the purview of several federal agencies, this has resulted in a variety of standards and regulations that need to be met, such as the Security Directives from the Transport Security Administration (TSA): TSA Security Directives 2021-01 and 2021-02. These require that pipeline owners and operators implement special mitigation measures to protect against ransomware and other cyber threats. Many of these practices outlined in the directives are designed for information technology systems found on traditional computer networks, not operational technology—hardware or software that monitors or controls equipment such as pipeline safety valves and water pumps.[5] This means that operators who rely on these OT shared resources are not provided adequate guidelines to implement strong security measures.

Additionally, the Oil and Natural Gas Sector Coordinating Council (ONG SCC) and the Federal Energy Regulatory Commission (FERC) strongly back compliance to National Institute of Standards and Technology (NIST) which has stated that legacy forms of MFA such as SMS codes should be deprecated.

So why the increased focus on MFA specifically? The answer is that current, legacy authentication and security solutions, such as usernames and passwords and mobile-based authenticators, are no longer effective to protect organizations against modern cyber threats. Research by Google, NYU, and UCSD, based on 350,000 real-world hijacking attempts, revealed that a SMS-based one-time-password (OTP) only blocked 76% of targeted attacks and a push app only blocked 90%.[5] 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.

Furthermore, most cyber insurance providers today require MFA, and some phishing-resistant MFA, to be deployed. The market for cyber insurance in the energy sector is anticipated to grow to $442 million by 2030, at a compound annual growth rate (CAGR) of 18%.[6] It is becoming apparent that without strong MFA in place, cyber insurance will be impossible to obtain.

Common authentication scenarios and associated vulnerabilities

Across the three sectors within energy and natural resources, a unique set of challenges and common authentication scenarios has resulted in security not keeping pace with the cyber security attack landscape as shown in the table below.

Upstream	Midstream	Downstream
Privileged users and accounts in IT and OT environments	Contractors, contract service workers, secondees and joint ventures	Shared workstation environments
OT and mobile-restricted environments	Field IoT devices	Physical access security

Privileged users and accounts with access to critical IT and OT systems

Every energy and natural resource organization has a subset of users or accounts with privileged access to critical IT and OT systems. A privileged user or account is any user or login credential with elevated access to critical data or systems on the network, or to critical infrastructure. Privileged users and accounts should have different levels of access based on what they are required to see and do within these systems, ideally least privilege. The principle 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. According to research conducted by Ponemon Institute, an average of 23% of employees in an organization can be considered privileged users.[7]

Username & password

*****

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

A privileged user may also be a user that is not a full time employee i.e. a contractor, secondee, supply chain vendor etc. 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.[8] Organizations must identify and authenticate every user who has access to inputs, IP, or to the systems involved across the entire supply chain. Even SCADA systems, which control and monitor the transmission of electricity, transportation of gas and oil in pipelines, and other functions,[9] need to have access monitored because if the capabilities and control get into the hands of a user with malicious intent, the results could be catastrophic. Therefore, it's vital to grant access to only those users to applications and services associated with the specific user credentials, while authenticating quickly and reliably to support productivity.

Additionally the idea of "privileged users" has ultimately expanded to include any business users who possess access to exploitable systems or IP such as customer, HR, finance, legal, or sales data. This level of access makes any user a desirable target for credential theft, but directly attacking such users isn't the only way cyber criminals can gain access to your critical systems. These threats can be costly and harmful to the business especially these essential energy and natural resource services.

Types of privileged users

Sometimes users

Access to sensitive/ confidential data or systems for contractors or for specific tasks

Privileged business user

Access to sensitive/ confidential data C-suite, HR, finance, sales

Privileged IT user

Access to systems, software, and data IT admins, security admins, network admins, and database admins

Cyberattacks targeting ICS and SCADA systems

Energy organizations are now being warned about malware targeting Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA) devices which can be deployed through phishing or compromised remote access. Attackers can gain control, compromise affected devices, elevate privileges and move laterally within an OT environment, and disrupt critical devices or functions.[10] This malware is also known as 'Pipedream,' because it can "disrupt, degrade, and potentially destroy industrial environments and processes" according to a Dragos report.[11]

Contractors, contract service workers, secondees, and joint ventures

Across the energy sector not everyone has access to company provided devices used for authentication. In comparison to employees who may have a device given to them by the organization; contractors, contract service workers, secondees, and joint ventures most likely do not. Contractors can be numbered in the tens of thousands, or more, and can also change per month in size and individual users. People in those roles fallback on legacy authentication, usernames and passwords and in doing so, creates risk because if those credentials are compromised the risk is magnified. This heightens the need for strong authentication that will not be phished. The need for education and awareness training should also be considered among the non-technical community so that people can recognize threats and vulnerabilities.

Shared workstation environments

Shared workstations are devices, kiosks, or computing environments that are used by multiple users, sometimes called 'roving users', with multiple people authenticating to the same workstation. These systems are critical to the day-to-day operations and often have a direct link to critical systems and data which amplifies the insider threat, whether malicious or negligent, and present additional security risks when used in high-traffic areas.

Mobile-restricted environments

- Call centers
- Airgap environments
- High-security sites
- Industrial (no connection, oil rigs, etc)

OT and mobile-restricted environments

A mobile-restricted environment is an scenario where mobile devices cannot be used, either due to factors related to the environment itself such as specialized equipment (air-gapped or SCADA) or isolated networks, harsh environments, offline or offshore locations, high-security sites, or due to restrictions imposed either by regulations, unions, or where mobile devices are simply discouraged by company policy. There may also be a subset of users within an organization that do not wish to use personal mobile devices for work purposes, requiring a different authentication method. Mobile-restricted environments often include shared workstations, and those stations may have special login and logout requirements.

For energy and natural resource organizations to ensure secure workflows in mobile-restricted environments, while accelerating business, they need to consider an MFA solution that can easily overcome the unique security and productivity challenges.

Field IoT devices

The Internet of Things (IoT) is transforming this industry by increasing automation and efficiency of equipment used in oil and gas extraction to the tools used for monitoring an end-user's consumption.[12] Through the use of IoT devices and the data collected from them, the energy sector has been able to create intelligent networks, 'Smart Grids,' allowing the devices and assets that are connected to the network to be optimized providing increased flexibility to manage the systems.[13] Controlling strict access into these networks is essential because if anyone is able to access the data collected, or obtain control, it can cause grave damage by disrupting services.

Undoubtedly this network of connected end-points including the data collected across it, needs to be secure and encrypted throughout the end-to-end cycle. This is why hardware solutions such as hardware security modules (HSMs)—which offer maximum security even in the most hostile, rugged environments–are needed to protect IoT devices.

Physical access security

Threats may be cyber or physical, which is why insider threats must also be considered. With vast amounts of highly expensive equipment and sensitive information, physical security is still a principal concern—as an example, a targeted sniper attack on a California grid caused about $15 million in damages, which disrupted service among others.[14] Controlling who has access to enter physical locations is vital to ensure that sensitive information and access is only given to the individuals whose job requires it.

The rise in cyberattacks and the amplification of mandates across various federal and public-serving agencies, highlights the massive need to invest in security that provides holistic protection for all critical infrastructure and systems within energy and natural resources. In order to protect against malware, like 'Pipedream,' and phishing attacks, it is vital to understand the role and impact of quality authentication.

94%

of data breaches in energy are traced back to **credentials**–higher than any other industry[15]

Risk of account takeovers

0%
Security key (YubiKey)

10%
On-device prompt

21%
Secondary email

24%
SMS code

50%
Phone number

Secure access with modern, phishing-resistant MFA

Drawbacks of legacy authentication

Not all forms of MFA are created equal at protecting against cyberattacks nor in terms of offering the optimal balance of strong security with a fast and simple user experience (UX) that enables high productivity. It's important to note that while any form of two-factor or multi-factor authentication offers more security than passwords alone, legacy authentication still relies on passwords as the first factor—still insecure, still inefficient, still a source of employee frustration. Insecure practices around credentials only compound these data breach risks.

With legacy MFA, the second factor is often tied to a mobile device. Mobile authenticators increase the number of steps in the authentication process, requiring users to wait for OTP or push app codes, or in case of users in energy and natural gas organizations—to remove heavy duty gloves for the authentication process. Safety concerns are one of the most important reasons why cell phones may not be used in certain situations aboard an oil rig[16] and many companies and local local laws prohibit the use of personal phones and other smart devices on oil rigs.[17] Among those concerns there are many red flags, including aspects listed below:

- There can be availability challenges with mobile devices sending codes in a timely manner due to poor connectivity or unreliable services.
- There is no real guarantee that the private key ends up on a secure element on the mobile device.
- The OTP or private key could be intercepted in some way (such as via SIM swapping)

Replacing legacy single-factor authentication (username and password) and mobile-based authentication with phishing-resistant MFA is the first step in improving security practices to secure IT and OT environments.

What are passkeys?

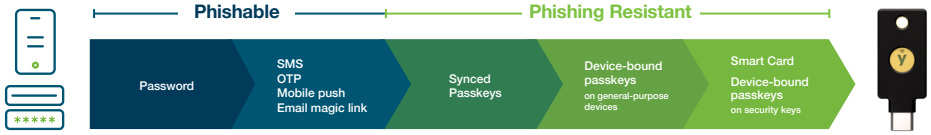
Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.

Device-bound passkeys offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across industries.

What is phishing-resistant MFA?

Phishing-resistant refers to an authentication process that is immune to attackers intercepting or even tricking users into revealing access information. According to NIST Special Publication (SP) 800-63-4 currently, only two forms of authentication meet the mark for phishing-resistant MFA: PIV/Smart Card and the modern FIDO2/WebAuthn authentication standard, also known as passkeys.[18] This also is indicated by the Office of Management and Budget Memo M-22-09.



The future is passwordless

Ultimately the actions of the user are the biggest weaknesses in legacy authentication, and multi-step authentication is a big contributor to user dissatisfaction which is why, the global best practice is moving toward passwordless authentication—authentication that does not require the user to provide a password at login.

Traditional smart cards do offer high security, but generally require high capital expenditure (CapEx) for smart card readers, physical cards, in addition to backend management platforms. Due to this, the industry as a whole is moving toward a passwordless login flow leveraging modern authentication standards such as FIDO2/WebAuthn that work well with the cloud, resulting in lower ongoing costs even as enterprises scale up.

The FIDO (Fast IDentity Online) modern authentication standard enables 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. For energy and natural resource organizations that have legacy OT systems and a low tolerance for non-productive tasks, FIDO2 hardware security keys, such as the YubiKey offer multi-factor and passwordless authentication with high security and exceptional user experience and provides multi-protocol support for SmartCard, OTP, OpenPGP, FIDO U2F and FIDO2/WebAuthn on a single key.

YubiKeys

- Proven to stop 100% of account takeovers[19]
- Ensure tap-and-go experience
- 4x faster to login than OTP[20]
- Do not rely on cellular network or battery
- Highly durable, IP68 certified: dust proof, crush-resistant, and water-resistant

YubiKey offers phishing-resistant MFA helping cultivate phishing-resistant users

The YubiKey from Yubico is a purpose-built, hardware security key that contains the highest assurance passkeys. The YubiKey provides modern strong authentication at scale across the supply chain, helping energy organizations and their suppliers implement robust, easy-to-use authentication for any user who has upstream access to the network or at critical IP handoffs. It is the most secure and user-friendly option for protecting all users across business units; providing authentication that moves with users no matter how they work across devices, platforms and systems.

With the YubiKey, energy and natural resource organizations can deploy phishing-resistant, multi-factor, and passwordless authentication at scale, with the hardware security key protecting the private secrets on a secure element that cannot be easily exfiltrated. The YubiKey is FIPS 140-2 validated and impersonation resistant, making it highly suitable for regulated environments and surpassing evolving regulations such as the Executive Order 14028 and the Office of Management and Budget (OMB) Memo M-22-09, to strengthen cyber security with Zero Trust frameworks including the deployment of phishing-resistant MFA.

YubiKeys comes in a variety of form factors and a single key can be used across multiple devices, a variety of modern and legacy IT and OT environments, as well as with thousands of applications and services. They are specifically designed to work in some of the most rigorous locations: shared workstation, mobile-restricted environments, isolated areas and offshore rigs. Users can benefit from a frictionless authentication workflow—plug the YubiKey into a USB port and touch a button to authenticate, or simply tap the YubiKey using NFC against a device (highly suited for no spark environments).

To further improve the user experience and speed of authentication, Yubico also offers the YubiKey Bio Series—FIDO Edition supporting FIDO U2F and FIDO2, which delivers the hallmark security that all YubiKeys are known for, with a new biometric-based passwordless experience.

Cultivating phishing-resistant users

The only effective approach to remove phishing from an organization's threat landscape is to ensure that every user within the organization becomes phishing-resistant—and that resistance must move with the users no matter how they work, across devices, platforms and systems. Deploying phishing-resistant authentication across the entire credential lifecycle, including the registration, authentication and recovery processes, is what creates a phishing-resistant user.

The YubiKey cultivates phishing-resistant users which then creates phishing-resistant enterprises.

“We introduced YubiKeys in our power operation SCADA systems to increase security with MFA. This process allows an operator to come on shift, authenticate quickly, and to take actions when appropriate, without any system interruptions. MFA ensures only authenticated users can gain access to operate the system.”

Chad Lloyd, Director of Cybersecurity Architecture for Energy Management, Schneider Electric

Learn more at
yubi.co/SchneiderElectric

Securing the supply chain and critical system integrity

In energy and natural resource organizations the continuous movement of critical resources is crucial in supplying these resources out to the world. One of the risks inherent in supply chain security is the possibility of compromise to the integrity, quality, or reliability of the product, software or service being delivered. Being able to authenticate equipment and machines is also an integral component in ensuring secure operations. The interconnectedness between the 3 main sectors–upstream, midstream, downstream—and the vast organizations that exist between all impact the quality of security because they are as secure as their weakest link.

Ensuring the highest integrity of your product parts and IoT devices

It is crucial to ensure that all components involved in an end to-end process are authentic to avoid unsolicited replication and theft, but also for quality assurance. As a result, there must always be a solution in place to protect the integrity and intellectual property of all components and resources across the upstream, midstream and downstream processes.

The traditional approach to protect intellectual property (IP) and prevent counterfeiting involves the use of digital cryptographic keys and encryption. Cryptographic keys would be stored either in software, which is highly vulnerable, or a hardware security model (HSM). Unfortunately, traditional rack-mounted and cardbased HSMs are large and expensive, making them impractical on oil rigs, industrial facilities, in caged data centers, or for IoT devices. When considering IoT devices, the diverse data, including environmental information, and credentials stored inside them needs to be controlled and secure through encryption and decryption. If a malicious actor disrupts or modifies the data flow between the IoT devices this could raise regulatory issues or put a company in a severe or compromised state. As a result, these devices need security measures that safeguard that data and protects these potential failure points.

Securing external code and data

Organizations that use software in their products, must have a method of secure code-signing for ingesting code or data from external sources. The need for secure code signing solutions has increased in the recent past, as demonstrated in the aftermath of the SolarWinds attack. In that attack, hackers exploited a breach in the SolarWinds code signing system, which allowed them to fraudulently distribute malicious code as legitimate updates to more than 18,000 installations of the SolarWinds Orion product across the world.[21] Further, the strength of the cryptographic solution you're using is only as strong as your supply chain partner's attestation method. It's therefore vital that those partners can show a chain of custody for code that runs all the way back to the original developer's computer.

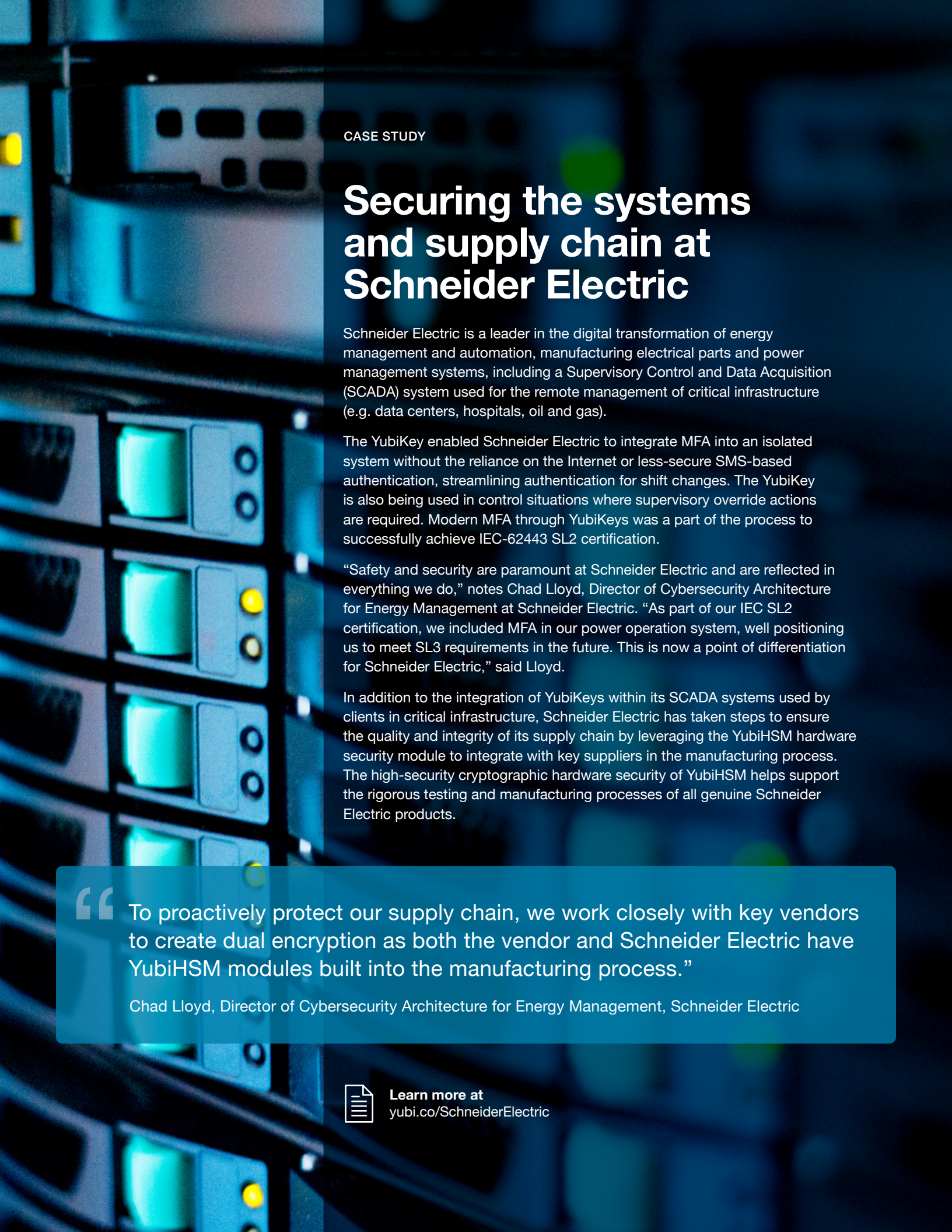
Safeguarding IP, product and device integrity with YubiHSM 2

Not only is the authentication of users vital, but also authentication between IT and OT systems which includes product parts and machines. Yubico created the ultra-portable and low-cost YubiHSM 2, the world's smallest HSM that comes in a nano form factor. The YubiHSM 2 enables secure, tamper-resistant key storage and operations, by preventing the copying and distribution of cryptographic keys, and remote theft of keys stored in software. The YubiHSM 2 can be applied to any process where secrets and the authenticity of components needs to be managed, and where tampering needs to be prevented. This solution secures the data and credentials stored within IoT devices and keeps them protected through encryption which creates additional layers of security. The compact size of the YubiHSM 2, minimal power requirements, and the fact that it can be plugged directly into equipment without requiring rack mounted gear makes it flexible to use and deploy.

YubiHSM 2 can protect and be easily deployed to any:				
USB slot on servers	Databases	Robotic assembly lines	Applications	IoT devices in the field

The YubiHSM 2 ensures only certified programming stations can interface with the intended components, or to write digital signatures onto each component to ensure integrity. In both scenarios, the added security of the YubiHSM 2 helps to maintain a company's reputation and gives them peace of mind. It is ideally suited to safeguard the signing keys and certificates for both signing code and creating digital signatures, helping support the secrets being shared within the supply chain. But even besides these use cases, organizations are freed up to innovate and solve for a wider range of business scenarios with the YubiHSM2 than ever possible before. For organizations that need to meet the FIPS 140-2 requirements, there is also the option of the FIPS 140-2, Level 3 validated YubiHSM 2 FIPS to ensure the highest levels of data protection in addition to strict levels of compliance.

It's important to note that the cryptographic keys used to sign and/or certify components are never exposed outside of the YubiHSM 2 hardware, ensuring a high level of assurance and security. To illustrate this point with an example, even if a remote attacker is able to compromise a network or specifically the computer connected to the device, there are still no obvious attack vectors as keys cannot be extricated. On the other hand, if the same attacker is able to gain full underlying access to a software equivalent, they might be able to at least run analysis on the memory, connected database or even local files for potential weaknesses or patterns.



CASE STUDY

Securing the systems and supply chain at Schneider Electric

Schneider Electric is a leader in the digital transformation of energy management and automation, manufacturing electrical parts and power management systems, including a Supervisory Control and Data Acquisition (SCADA) system used for the remote management of critical infrastructure (e.g. data centers, hospitals, oil and gas).

The YubiKey enabled Schneider Electric to integrate MFA into an isolated system without the reliance on the Internet or less-secure SMS-based authentication, streamlining authentication for shift changes. The YubiKey is also being used in control situations where supervisory override actions are required. Modern MFA through YubiKeys was a part of the process to successfully achieve IEC-62443 SL2 certification.

“Safety and security are paramount at Schneider Electric and are reflected in everything we do,” notes Chad Lloyd, Director of Cybersecurity Architecture for Energy Management at Schneider Electric. “As part of our IEC SL2 certification, we included MFA in our power operation system, well positioning us to meet SL3 requirements in the future. This is now a point of differentiation for Schneider Electric,” said Lloyd.

In addition to the integration of YubiKeys within its SCADA systems used by clients in critical infrastructure, Schneider Electric has taken steps to ensure the quality and integrity of its supply chain by leveraging the YubiHSM hardware security module to integrate with key suppliers in the manufacturing process. The high-security cryptographic hardware security of YubiHSM helps support the rigorous testing and manufacturing processes of all genuine Schneider Electric products.

> “To proactively protect our supply chain, we work closely with key vendors to create dual encryption as both the vendor and Schneider Electric have YubiHSM modules built into the manufacturing process.”
>
> Chad Lloyd, Director of Cybersecurity Architecture for Energy Management, Schneider Electric

Learn more at
yubi.co/SchneiderElectric

CASE STUDY

Securing critical infrastructure at an Asia-Pacific energy company

For this leader in electricity distribution in Asia-Pacific, serving millions of customers, much of the responsibility for protecting operations from cyberattacks falls to the OT Security Specialist, a job which sits at the border between IT and OT.

During the procurement process of an authentication solution, the energy company had to balance multiple requirements. It was important that the product would also integrate easily with existing infrastructure, without requiring additional software. This ruled out one possible solution—Smart Cards—which require specific drivers and Smart Card readers to function. The OT Security Specialist was also keen to find a solution that was user-friendly.

The OT Security Specialist was most attracted by how YubiKeys balanced security and usability: “if you’ve got to physically touch the button, you know a user is physically there using it. We could set up one YubiKey as MFA for all a user’s accounts, so they don’t need six different TOTPs.” To protect the hardware and live equipment upon which distribution relies, the organization chose the YubiKey to secure all users who access the operational environment—offering a balance of security. Further, the flexibility of YubiKey as a Service helps guarantee the highest level of protection into the future.

> “My personal opinion is that they’re more convenient to use than a token off your phone, especially when your YubiKey is next to you. I don’t like having to grab my phone and look for an app to get a token out of it or unlock it to approve a request. It’s a lot quicker to just hit a button on the USB stick.”
>
> OT Security Specialist, Anonymous State-Owned Energy Company

Learn more at
yubi.co/EnergyCo

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.

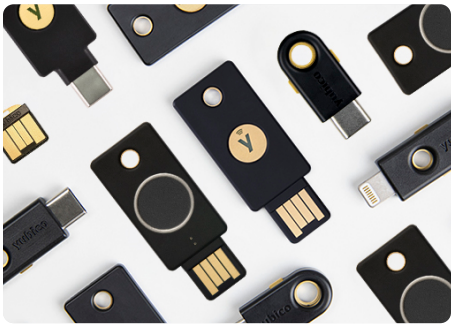
YubiKey as a Service

YubiEnterprise Delivery

With YubiKey as a Service, 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.

YubiKey as a Service 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 YubiKey as a Service customers.

Yubico's Professional Services team can provide technical and operational guidance to help streamline your YubiKey implementation and rollout with services mapped to your needs.



Economic benefits of the YubiKey

Outside of technological and security benefits, there are also economic benefits of the YubiKey. This section showcases an example authentication problem and suggested calculations that energy and natural resource organizations can use to generate estimated expected economic benefits of deploying YubiKeys for strong two-factor, multi-factor, or passwordless authentication.

SITUATION

Let's consider Energy and Natural Resource Company X:

Company breakdown: 10,000 employees and 10,000 contractors (that change each month) who work on the energy production and distribution process across upstream, midstream, and downstream. Unlike employees, contractors do not have access to mobile devices provided by the company, therefore they do not have access to mobile-based MFA that employees currently use. Within the energy production and distribution process exists several critical systems that require secure access for data access and system controls.

What keeps them up at night: Growing concerns over repeated cyberattacks, as well as reports of poor authentication user experience that challenges worker productivity, drives up support costs, which may also be tied to longer time to market.

Unproductive authentication: Employee feedback states that the current two-factor authentication process used across the corporate IT environment that includes a username and password as well as a TOTP token code, is inefficient for the multiple times through a workday when employees must authenticate to leverage IT and OT systems and workstations. Additionally username and password based single-factor authentication used by contractors does not provide security against modern day cyberattacks, and leads to delays in production and increased IT costs when workers forget their password and need to contact the help desk.

END STATE: MIGRATION TO PASSWORDLESS AUTHENTICATION

The office of the CISO is now exploring the means to migrate to a passwordless authentication environment for both employees and contractors for two primary reasons. The first is to reduce exposure to outside threats that are typically well funded from domestic cyber attackers as well as known nation states, and designed to disrupt critical infrastructure and the supply chain. The second reason is to improve the user experience in order to drive efficiency and productivity.

With the dangerous risks of having mobile phones in OT environments such as oil rigs or energy plants, mobile-based authentication is not suitable here making Company X look for a solution that offers high security against modern threats, a simple user experience and high durability across OT environments. Company X's strategic priority is to incorporate a FIDO2 based passwordless strategy using a hardware security key like the YubiKey that would add significant incremental value to the organization across both IT and OT environments for their employees as well as contractors, contract service workers, secondees, joint ventures. For the purpose of this ROI exercise below the term "user" will be used to reference employees, contractors, contract service workers, secondees, or joint ventures.

ROI FORECAST AND GOALS

It is predicted that a migration to Yubico's YubiKeys with NFC capabilities that supports modern FIDO2 authentication protocol will address all of the above stated challenges.

The goal is to calculate reasonable, achievable, and believable hard dollar return on investment (ROI) that has been in proof of concept and positively reflects a commitment and investment in a long-term authentication strategy. For the purpose of this exercise this means a standard, enterprise-wide method of verifying user identities without the use of a password. The ROI calculations will show annual returns across upstream, midstream and downstream processes, of the YubiKey versus a username and password authentication that is often used by contractors and contract service workers, as well as returns of the YubiKeys versus a TOTP authentication solution often used by employees.

After comparing costs for purchasing YubiKeys using perpetual licensing and YubiKeys using YubiKey as a Service-based licensing, it is predicted that a migration to Yubico's YubiKey as a Service including YubiKeys with NFC capabilities that supports modern FIDO2 authentication protocol will address all of the above stated challenges and deliver the best return on investment ROI.

ROI EXECUTIVE SUMMARY

Improved authentication experience and productivity gains: With the YubiKey's simple tap/touch login and ease of use this drives expectations that the average authentication/login time for users will dramatically decrease per user overtime logging into IT and OT systems allowing them to redirect their productivity elsewhere. While considering the diverse locations of contractors, contract service workers, secondees, and joint ventures (corporate office, out in the field) they need an always-available MFA solution.

Help desk cost reduction: A majority of the calls to the IT help desk at Company X are related to password resets. IT management would like to reduce the costs and time spent on password reset calls by moving toward a self-service model and eventually a passwordless environment.

Threat remediation and loss of business continuity: Given the fact that the highest volume of credential theft is from successful phishing attacks, Company X anticipates a significant reduction in costs related to cyber threat mitigation and remediation efforts including threat analysis, thus decreasing related security operations center (SOC) analyst FTE cost, and importantly reducing risks to brand exposure. Additionally, having their facility shut down because of an attack, can lead to loss of business, critical disruption to end customers, regulatory fines, and attack related legal and payout costs.

ROI CALCULATIONS

After a comprehensive review of the above use cases, Company X has determined to move forward with YubiKeys. Company X will arrive at a homogeneous FIDO2 based passwordless strategy by the end of 2024. The chosen YubiKey as a Service offering includes Priority Support Services, as well as a 25% YubiKey overhead for employee churn.

Company X is currently using both username and password-based authentication, and TOTP-based authentication across their organization. Replacing username and password-based authentication with FIDO2 based passwordless using the YubiKey with YubiKey as a Service licensing, for contractors, contract service workers, secondees and joint ventures would result in an annual return of approximately $6,208,333.33. Replacing TOTP authentication for employees would result in an annual return of approximately $17,617,333.33. Both scenarios include a significant reduction in authentication time, redirection of employee time to other priorities (productivity gains), reduced support calls to IT help desk, and in a similar manner, reduced successful phishing threats to the end users, resulting in fewer cases to resolve by the security operations center. The annual returns for both authentication scenarios does not include the profit costs related to reallocation for user time to higher priority deliverables. It is believed that the resulting economic data, as shown below, is a conservative proposed estimate.

ROI CALCULATIONS

A roll-up of each estimated economic impact calculated against individual use case goals is shown in Table 1.

Table 1: ROI executive summary

USE CASE: ENERGY PRODUCTION & DISTRIBUTION PROCESS | AUTHENTICATION				
Details	**Number of users**	**Current username and password cost**	**Current TOTP cost**	**Cost with YubiKey**
Authentication experience and redirected user productivity gain	10,000	$ 5,692,000.00	$11,386,000.00	$ 2,846,000.00
Help desk costs	—	$ 58,333.33	$ 58,333.33	—
Threat remediation costs	—	$ 864,000.00	$ 864,000.00	$ 0.00
Total Annual Cost	—	$ 6,614,333.33	$ 12,308,333.33	$ 2,846,000.00
YubiKey Licensing Cost (perpetual)				$ 1,110,000.00
Annual YubiKey Licensing Cost (YubiKey as a Service)				$ 420,000.00
Estimated Annual Return YubiKey perpetual versus username and password				$ 5,518,333.33*
Estimated Annual Return YubiKey as a Service versus username and password				$ 6,208,333.33**
Estimated Annual Return YubiKey perpetual versus TOTP				$ 17,127,333.33*
Estimated Annual Return YubiKey as a Service versus TOTP				$ 17,617,333.33**

*Current Cost + Productivity Gain - (Cost with YubiKey + YubiKey Perpetual Licensing Cost)
**Current Cost + Productivity Gain - (Cost with YubiKey + YubiKey as a Service Licensing Cost)

Table 2 shows inputs and calculations of migrating from username and password and TOTP authentication to FIDO2 or smart card based passwordless with the YubiKey, specifically the comparison of current required time for those processes and its comparison to the upgraded YubiKey authentication experience along with the cost saving and benefit of going with YubiKey as a Service.

Table 2: Authentication experience inputs & calculations

COMPANY X INPUTS		
Number of users in use case	10,000	Input value
Mean hourly pay rate (user)	50	Input value
Mean minute pay rate (user)	0.83	Input value
Work days per year	200	Input value
Hours per work day	8	Input value
Application log-in time (in minutes) per user per year with username and password only	1,253	Forrester benchmark: 1253 mins a year equals 3.43 mins a day spent accessing applications on average
Application log-in time (in minutes) per user per year with TOTP	2,506	Assuming it doubles the time from base time entering username and password so 1253 x 2
Application log-in time (in minutes) per user per year with YubiKey	626.5	Google Stat: YubiKey is 4 times faster than typing in an OTP (Google Authenticator)

AUTHENTICATION COSTS	Current username and password cost	Current TOTP cost	Cost with YubiKey	
Application log-in time (in minutes) per user per day	3.43	6.86	1.715	Input value from above
Cost per authentication/employee/day	$ 2.846	$ 5.693	$ 1.423	minute rate of user * total daily avg time to auth
Total daily cost to authenticate (per total users in use case)	$ 28,460.00	$ 56,930.00	$ 14,230.00	cost per auth/emp/day * #number of users
Total annual authentication experience costs	**$ 5,692,000.00**	**$11,386,000.00**	**$ 2,846,000.00**	total daily cost to authenticate * work days per year

ESTIMATED YUBIKEY COSTS PERPETUAL		
Cost of licensing YubiKeys for 10,000 users	$ 1,100,000.00	YubiKey License (YubiKey 5C NFC $110 for 2 pack)
Annual support services cost considering Priority Support	$ 10,000.00	Yubico Priority Support Costs
Total Estimated YubiKey Costs (perpetual licensing)	$ 1,110,000.00	YubiKey licensing + support costs

ANNUAL ESTIMATED YUBIKEY COSTS YUBIKEY AS A SERVICE		
Annual cost of licensing YubiKeys for 10,000 users (primary key)	$ 240,000.00	YubiKey as a Service cost (YubiKey 5C NFC) $24
Annual cost of licensing YubiKeys for 10,000 users (backup key)	$ 180,000.00	YubiKey as a Service cost for backup key (25% discount)
Annual support services cost considering Priority Support	—	Free with YubiKey as a Service licensing
Total Annual Estimated YubiKey Costs (YubiKey as a Service licensing)	$ 420,000.00	Annual cost of primary keys for all users + annual cost of backup keys for all users

Table 3 shows inputs and calculations of migrating from username and password and TOTP authentication to FIDO2 or smart card based passwordless with the YubiKey, and the outcome of a greatly improved user experience which returns time back per authentication/login attempt, multiple times per day across the energy production and distribution process.

Table 3: Redirected user productivity gain inputs & calculations

AUTHENTICATION COSTS	Current username and password cost	Current TOTP cost	Cost with YubiKey	
Application log-in time (in minutes) per user per day	3.43	6.86	1.715	Input value from above
Number of work minutes per year		96,000		Number of work days per year * number of hours per work day * number of minutes per hour
Application log-in time (in minutes) per user per year	686	1,372	343	Application log-in time (in minutes) per user per day * number of work day
Application log-in time (in hours) per user per year	11.43	22.86	5.71	Application log-in time (in hours) per user per year / 60
Total recouped time (hours) per user per year YubiKey vs. username and password	–	–	5.72	Application log-in time (in hours) per user per year [username and password - YubiKey]
Total recouped time (hours) per user per year YubiKey vs. TOTP	–	–	17.15	Application log-in time (in hours) per user per year [TOTP - YubiKey]
Total recouped time (hours) per year YubiKey vs. username and password	–	–	57,200	Total recouped time per user per year * number of users
Total recouped time (hours) per year YubiKey vs. TOTP	–	–	171,500	Total recouped time per user per year * number of users
Productivity cost per year YubiKey vs. username and password	–	–	$ 2,860,000.00	Total recouped time (Hours) per year * mean hourly pay rate (user) [username and password - YubiKey]
Productivity cost per year YubiKey vs. TOTP	–	–	$ 8,575,000.00	Total recouped time (Hours) per year * mean hourly pay rate (user) [TOTP - YubiKey]

Organizations can use the formulae below to calculate the estimated cost savings for use case goals: Help desk cost reduction, and Threat remediation savings.

Help desk cost reduction:

Inputs and calculations of migrating from username and password and TOTP authentication to FIDO2 or smart card based passwordless with the YubiKey, and the elimination of “password reset” tickets, reduction in new hire education, and ongoing support of all users pertinent to the improved authentication experience. See appendix for input data values used.

Total cost = Fully loaded help desk worker FTE hourly cost X number of help desk employees addressing password/ authentication tickets X time per employee per ticket X number of tickets per employee

Threat remediation costs:

Inputs and calculations of migrating from username and password-based authentication and TOTP authentication to FIDO2 or smart card based passwordless with the YubiKey, and its impact on cyber threats and threat remediation due to non-shared-secret, asynchronous methods that stops credential phishing, malware, and Man-in-the-Middle driven cyberattacks. TOTP based authentication is not considered to be phishing resistant per NIST guidelines, so threat remediation costs using username and password-based authentication, and TOTP based authentication, will be the same using the consideration that TOTP can be phished. Current calculated cost does not include data breach related to production downtime, legal fees, ransomware payout, cyber insurance premiums, or regulatory fines. See appendix for input data values used.

Total FTE cost per remediation analysis/fix = Fully loaded security analyst FTE hourly cost X number of analysts involved in remediation efforts of suspected credential theft reported or detected X number of hours invested per investigation

Appendix

Number of help desk employees (in use case)	10	Input data
Help desk employee mean hourly FTE	50	Input data
Help desk employee mean minute FTE	0.83	Input data
Help desk employee work days/year	200	Input data
Cost per help desk employee per day	29.17	Total hours per day per employee * hourly rate
Total cost per day for password reset	291.67	Cost per help desk employee per day * number of help desk employees
Total annual cost for password reset	58,333.33	Total cost per day for password reset * work days per year
Number of password reset requests per day to help desk	5	Input data
Avg minutes required per password reset request	7	Input data
Total minutes/day required for password reset requests	35	#requests * avg min per
Total hours/day required for password reset requests	.58	#daily mins / 60
Number of SOC analyst employees (in use case)	10	Input data
SOC analyst mean hourly rate in threat remediation	90	Input data
SOC analyst mean minute rate in threat remediation	1.50	Input data
Work days/year of SOC analyst in threat remediation	200	Input data
Number of unresolved phishing attempts per day	6	Input data
Average minutes required per analysis and remediation	48	Input data
Total minutes/day per SOC analyst	288	#daily unresolved * avg min per analysis
Total hours per day per SOC analyst	4.80	total minutes / 60
Daily SOC analyst cost	432.00	Total hours per day per SOC analyst * SOC analyst mean hourly rate in threat remediation
Total daily SOC analyst cost	4,320.00	Daily SOC analyst cost * number of SOC analyst employees
Total annual threat remediation cost	864,000.00	Total daily SOC analyst cost * work days/year of SOC analyst threat remediation

Takeaway

The YubiHSM 2 and YubiHSM 2 FIPS

From left to right: YubiHSM 2 and YubiHSM 2 FIPS

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

Due to the ever-evolving sophistication of cyberattacks, the need to modernize authentication could not be more timely and necessary. As a result, leading organizations are deploying passwordless authentication and ultra-portable and flexible HSM to protect against modern cyber threats. These solutions need to be both user-friendly and cost-effective at scale, while being highly durable to meet the diverse work environments users are in such as out in the field, in a corporate environment, or on an oil rig.

Being proactive and securing your data, people, and critical infrastructures with the right security solution can help you mitigate attacks, minimize attack penetration rates, and protect your invaluable resources that impact the world.

Modern cyber threats require Yubico's security solutions. The YubiKey and YubiHSM 2 are secure, portable, adaptable and easy-to-use solutions designed to meet the diverse needs of energy and natural resource organizations where they are, helping to seamlessly support legacy infrastructure as well as bolster them into modern, cloud-based systems.

Stay ahead of the ever-evolving threat landscape with best-in-class security that sets you up for success not only now, but also into the future.

Sources

[1] IBM, 2024 Cost of Data Breach Report, (Accessed November 20, 2024)

[2] Bloomberg, Hackers Breached Colonial Pipeline Using Compromised Password, (June 4, 2021)

[3] Industrial Cyber, WEF weighs in on cyber attacks targeting European energy sector, (February 8,2022)

[4] Politico, TSA has screwed this up': Pipeline cyber rules hitting major hurdles, (March 17, 2022)

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

[6] PR Newswire, Guidehouse Insights Anticipates the Cyber Insurance Market for Energy to Grow at a Compound Annual Growth Rate of Nearly 18% by 2030, (March 10 2022)

[7] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020)

[8] BlueVoyant, Managing Cyber Risk Across the Extended Vendor Ecosystem 2021, (June 1 2022)

[9] Onlogic, What is a SCADA System and How Does It Work?, (April 20 2022)

[10] CISA, Alert (AA22-103A), APT Cyber Tools Targeting ICS/SCADA Devices, (May 25 2022)

[11] CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS), (April 13 2022)

[12] Trusted Computing Group, Protecting the energy sector's industrial IoT, (January 24 2022)

[13] Nexus Integra, IoT in the energy sector: monitoring and analysis of variables, (Accessed July 1 2022)

[14] Rich Castagna, Energy Grid Security Gets More Challenging With IoT, (August 18 2020)

[15] Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2022)

[16] Arnold & Itkin, How Offshore Workers Communicate with Loved Ones, (Accessed May 25, 2022)

[17] Ibid.

[18] NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022)

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

[20] Ibid.

[21] SEC, Form 8-K SolarWinds Corporation, (December 14, 2020)

yubico

About Yubico

Yubico (Nasdaq Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA. For more information on Yubico, visit us at www.yubico.com.