yubico

Phishing-resistant MFA for energy and natural resources

Protect critical IT and OT systems

Energy, utilities, and oil and gas are increasingly under cyber attack

The 2021 Colonial Pipeline attack highlighted how vulnerable energy, utilities, and oil and gas sectors are to modern cyber attacks. Using a single compromised password, attackers disrupted the fuel supply to the eastern U.S region for days. This attack triggered widespread regulatory change. On May 12, 2021, the White House Cybersecurity released Executive Order #14028 on Improving the Nation's Cybersecurity mandating Zero Trust and impersonation-resistant multi-factor authentication (MFA). The Department of Homeland Security released TSA Security Directives 2021-01 and 2021-02, requiring pipeline owners and operators to implement special mitigation measures to protect against ransomware and other cyber threats. 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).

Increasing threats from nation-states, cyber criminals, and hacktivists seek to cause security and economic dislocation. In addition, expansive and increasing attack surfaces arising from geographic and organizational complexity, and interdependencies between physical and cyber infrastructure, especially operational technology (OT) systems, create key security vulnerabilities in this sector.[1]

Legacy authentication is creating risk

Implementing multi-factor authentication (MFA) can be a strong first-line of defense to protect against modern cyber threats. But not all forms of MFA are created equal. Legacy authentication such as usernames and passwords can be easily hacked, and mobile-based authentication such as SMS, OTP codes, and push notifications are highly susceptible to modern phishing attacks, malware, SIM swaps, and man-in-the-middle attacks (MiTM).

With the average cost of a data breach across the energy sector being $4.78 million,[2] it's imperative that organizations adopt modern phishing-resistant MFA to secure critical IT and OT environments, while ensuring compliance to new and evolving regulations.

[1] McKinsey & Comapny, The energy-sector threat: How to address cybersecurity vulnerabilities
[2] IBM, Cost of a Data Breach 2023 Report
[3] Google: New research: How effective is basic account hygiene at preventing hijacking

In addition to security, it's also important to consider usability, portability, and scalability, as key requirements across IT and OT environments that exist within the upstream, midstream and downstream flow of natural resources. Poor user experiences, low portability, and lack of scalability can result in MFA gaps, low user adoption, and an increased risk of a breach.

Safeguard critical infrastructure, people, and data with the highly durable YubiKey

To protect against modern cyber attacks, Yubico offers the YubiKey, for phishing-resistant two-factor, multi-factor, and passwordless authentication. The YubiKey is FIPS 140-2 validated and impersonation-resistant, making it highly suitable for regulated environments.

YubiKeys are proven to offer the highest levels of security against account takeovers in independent research, preventing targeted attacks.[3] With the YubiKey, energy, utility, and oil and gas companies can deploy highest-assurance security across both IT and OT environments.

Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

A single YubiKey can be used across a variety of applications, services and devices, with multi-protocol support for SmartCard, OTP, OpenPGP, FIDO U2F and FIDO2/WebAuthn. They are also highly durable (IP68 certified)—dust proof, crush- and water-resistant.

Common uses cases the YubiKey solves for the energy, utility, oil and gas sector

1. Secure IT and OT environments

YubiKeys offer a cohesive and effective way to ensure that your entire IT and OT environment—across corporate, field, and remote locations—is protected against unauthorized access. Secrets are stored in the secure element on the YubiKey which cannot be exfiltrated, unlike legacy MFA approaches. YubiKeys also integrate seamlessly with existing IAM solutions such as Microsoft, Okta, Duo and Ping, while providing secure authentication for hundreds of applications and services.

2. Secure shared workstations, mobile-restricted areas, and isolated networks

Legacy authentication such as mobile-based MFA isn't suitable for mobile-restricted environments or isolated networks (air-gapped, SCADA). They are also burdensome for field workers to carry in OT environments or remote locations such as plants, off-shore rigs, and remote vessels.

YubiKeys come in USB and nano form factors and require no battery or cellular connectivity, offering a portable root of trust for field workers and employees in such environments. YubiKeys with NFC capability, in combination with wearables, are highly suited for no spark and low voltage OT environments.

3. Drive compliance to industry regulations

The YubiKey is highly suitable for regulated environments and they are FIDO2/WebAuthn compliant. It meets NIST SP 800-63B Authenticator Assurance Level (AAL) 3 requirements, enabling energy, utilities, and oil and gas entities to comply with EO #14028, the TSA Security Directives, and other government regulations like Sarbanes-Oxley (SOX), the Federal Energy Regulation Commission (FERC), and North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) standards. YubiKeys offer a bridge to passwordless, ensuring that your MFA strategy is future-proofed from a compliance and technology perspective.

4. Secure your supply chain

If your supply chain vendors and outsourced partners don't follow the same Zero Trust and phishing-resistant MFA approach as you do, this can result in costly consequences such as disruption to operations, and national and regional critical infrastructure outages. With the YubiKey your supply chain vendors and partners can also deploy phishing-resistant MFA, minimize your cyber risk, liability, and damage to your brand reputation. Authentication of users is vital along the supply chain, but so is authentication between systems and machines, which is provided by the world's smallest hardware security module (HSM), the YubiHSM 2.

Seamlessly procure and distribute YubiKeys at scale and empower your users rapidly

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 can benefit from a predictable OPEX model, 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 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.

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

Key questions Yubico can help you with:

- ☐ Which YubiKey should my organization use?
- ☐ What is the best way to integrate YubiKeys into my environment?
- ☐ How can I get YubiKeys to my globally distributed workforce?

Contact the Yubico sales team today to add phishing-resistant MFA to your security ecosystem.

Trusted authentication leader

Yubico is the principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO alliance and is the first company to produce the U2F security key and a multiprotocol FIDO2 authenticator.

The YubiKey Family

The YubiKey is available in multiple form factors for desktop, laptops and mobile devices.

Contact us
yubi.co/contact

Learn more
yubi.co/energy

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries. For more information, visit: www.yubico.com.