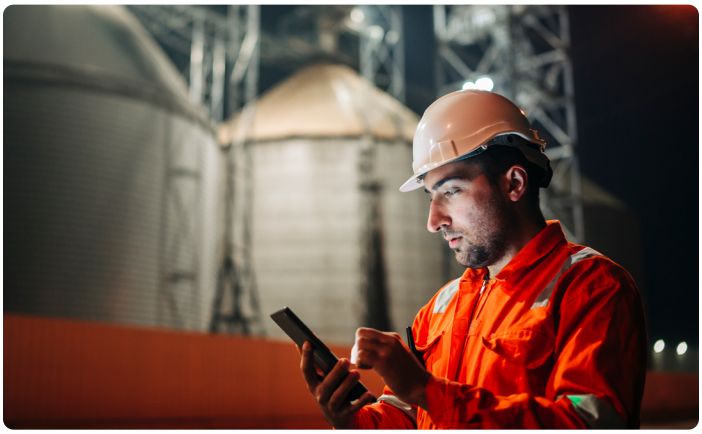
yubico

Securing energy and natural resources with phishing-resistant multi-factor authentication



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 was a turning point, triggering 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.

With the average cost of a data breach across the energy sector being $4.65 million, it's imperative that organizations adopt modern phishing-resistant MFA to secure critical IT and OT infrastructures, while ensuring compliance to new and evolving regulations.

In addition to security, it's also important to consider usability, portability, and scalability, as key requirements across OT environments. Poor user experiences, low portability, and lack of scalability can result in MFA gaps, low user adoption, and an increased risk of a breach.

Phishing-resistant MFA and compliance 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.[2]

Risk of account takeovers

0% Security key (YubiKey)

10% On-device prompt

24% SMS code

21% Secondary email

50% Phone number

With the YubiKey, energy, utility, and oil and gas companies can deploy highest-assurance security across both IT and OT environments. 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.

[1] https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

[2] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

YubiKeys come in portable USB and nano form factors, and require no battery or cellular connectivity. They are also highly durable (IP68 certified)—dust proof, crush resistant, and water resistant. YubiKeys with NFC capability, in combination with wearables, are highly suited for no spark and low voltage OT environments.

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). These 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, offering a portable root of trust for field workers and employees in such environments.

3. Drive compliance to industry regulations

The FIPS 140-2 validated YubiKey is impersonation resistant and highly suitable for regulated environments. 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

Reliance on supply chain vendors and outsourced partners require critical IP handoffs that can result in major vulnerabilities if your supply chain doesn't follow the same Zero Trust and phishing-resistant MFA approach. Weak links in the chain can lead to costly consequences such as disruption to normal operation, 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.

Easily procure and distribute YubiKey authentication solutions at scale

Yubico helps organizations simplify procurement and distribution of YubiKeys for employees at scale.

With YubiEnterprise Subscription, organizations receive a service-based and affordable model for purchasing YubiKeys with benefits such as predictable spending, upgrades to the latest offerings, choice of form factor, customer support, and more. This is especially beneficial for organizations experiencing frequent employee turnover.

With YubiEnterprise Delivery, organizations receive turnkey service with shipping, tracking, and returns processing of Yubico products handled seamlessly by logistics experts. This allows organizations to focus on what matters—securing internal and customer assets.

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.

YubiKeys are produced in the USA and Sweden, maintaining security and quality control over the entire manufacturing process.

The YubiKey 5 Series

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

The YubiKey 5 FIPS Series

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

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088