

# Powering stronger cyber defenses in the energy sector

Stop account takeovers and secure your critical infrastructure with phishing-resistant authentication

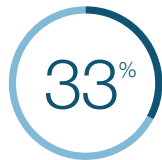
## The energy sector faces constant cyber threats

Without the essential services provided by the energy sector, none of us would be able to work, learn, travel, or conduct most of our daily activities. But because of the critical nature of these services, utilities, energy and natural resource organizations are a top target for cyber attacks including ransomware, which tends to originate from phishing attacks, in order to steal credentials and breach systems. Cyber criminals and nation-states seek economic gain and mass disruption from these attacks. A breach can impact distribution of these critical services that enable society to have heat, electricity, fuel, and all that comes with it.



of the world's top energy companies have suffered third-party data breaches in the past year

[Source](#)



of energy companies scored a C or lower in security, indicating a heightened breach risk within the sector

[Source](#)



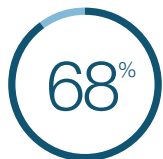
Phishing is the most popular attack technique used against the energy sector worldwide

[Source](#)



The average cost of a data breach in the energy sector

[Source](#)



of all breaches involve a non-malicious human element, like a person falling victim to a phishing attack or making an error

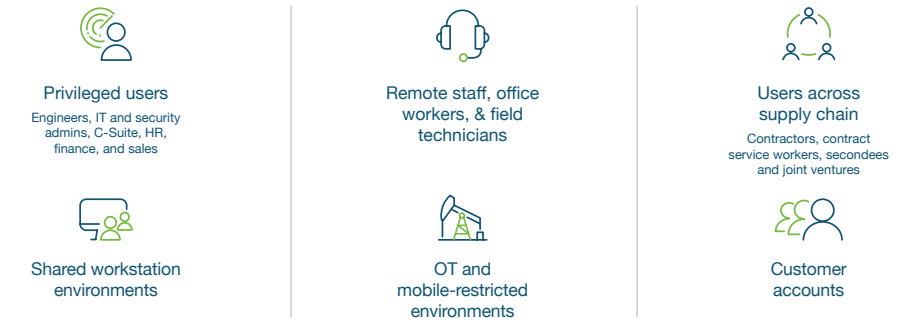
[Source](#)

## Modern protection for an ever-evolving cyber threat landscape

While multi-factor authentication (MFA) is foundational in protecting this critical infrastructure, not all forms of MFA are created equal. According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, only two forms of authentication currently meet the mark for phishing-resistant MFA: Smart Card/PIV and FIDO2/WebAuthn.

Historically, the energy sector has relied on Personal Identity Verification (PIV) Smart Cards to meet strict security guidelines. While PIV satisfies the needs of traditional perimeter-based and desktop authentication requirements, advancements in technology have made operational technology (OT) and systems connected to the internet much more vulnerable to remote attacks, creating a need for phishing-resistant options beyond Smart Cards to FIDO2-based solutions.

It is critical that modern phishing-resistant MFA be the first line of defense with a comprehensive strategy across the upstream, midstream and downstream that includes:



# Accelerate Zero Trust with modern phishing-resistant authentication to combat cyber threats



The YubiKey is a modern hardware security key that offers phishing-resistant multi-factor and passwordless authentication so organizations in the energy sector can secure critical systems and it is the only technology that complements Smart Card/PIV. YubiKeys cultivate phishing-resistant users, providing authentication that moves with users no matter how they work across devices, platforms, systems and locations including wind and solar farms, offshore drilling sites, and beyond.

## Why choose the YubiKey for phishing-resistant authentication?

- Reduce risk of credential theft by 99.9% and stops account takeovers while delivering 203% ROI  
[Source](#)
- Reduce help desk costs by up to 75% with self-service password resets  
[Source](#)
- Help lower cyber insurance premiums by 30%  
[Source](#)
- Provide secure user access at scale on any device with the best user experience
- Drive business continuity, be cyber resilient, and ensure the best security and user experience for employees and end-customers alike.
- Does not need battery or cellular connectivity to function
- Bridge to modern passwordless with multi-protocol support for Smart Card/PIV, FIDO2/WebAuthn, FIDO U2F, OTP and OpenPGP on a single key
- Deploy the most secure passkey strategy: device-bound that is purpose-built for security, FIPS 140-2 validated and Authenticator Assurance Level 3 (AAL3) compliant
- Satisfy cyber insurance and drive regulatory compliance to BSI-KritisV, CCPA, E8MM, eIDAS, FedRAMP, FERC, GDPR, NERC-CIP, NIS2 Directive, PCI DSS v4.0.1, PSD2, SOCI Act, SOC2, SOX, TSA.



“ You can already see the extremely low probability of phishing-attacks with Naftogaz-Bexreka. It is through using YubiKeys and Microsoft Azure, where we link our keys, that users no longer need to use passwords. In my opinion, we are the most secure company in our group.”



Oleksandr Tarasov  
Head of Security Controls  
at Security Operation Center  
[Read our case study](#)  
[yubi.co/Naftogaz](https://yubi.co/Naftogaz)



“ 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  
[Read our case study](#)  
[yubi.co/SchneiderElectric](https://yubi.co/SchneiderElectric)



Yubico also offers the YubiHSM that ensures enterprise-grade high cryptographic security and operations that protects servers, applications, and computing devices. Its ultra-portable nano form factor allows for flexible deployment.

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 passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

For more information, visit: [www.yubico.com](https://www.yubico.com) © 2024 Yubico



Contact us  
[yubi.co/contact](https://yubi.co/contact)



Learn more  
[yubi.co/energy-wp](https://yubi.co/energy-wp)

yubico