yubico

Securing Operational Technology with Yubico

Hardening OT access to protect safety, uptime, and continuity

How expanded connectivity is reshaping cyber risk in operational technology

Operational Technology (OT) supports critical infrastructure including manufacturing, energy, healthcare, and government. These OT environments consist of large-scale machines and Industrial Control Systems (ICS), including Distributed Control Systems and SCADA, to manage physical processes including machine-to-machine and human-to-machine communication.

Historically, these environments were designed to prioritize safety and uptime, rather than secure connectivity. By their nature, these systems are often considered shared workstations with multiple users resulting in shared accounts and passwords with limited access controls. OT systems have commonly been isolated or airgapped from external networks delivering a degree of physical security. However, as OT systems become increasingly connected to IT networks, cloud platforms, and third parties, their exposure to cyber threats grows due to insecure legacy industrial protocols that lack basic authentication.

Legacy systems not built for external connectivity are now prime targets, where stolen credentials, ransomware, and remote access abuse can lead to operational disruption, physical damage, and significant financial impact.

180,000+	ICS/OT systems are exposed monthly to the Internet. Source
72%	of attacks targeting OT systems originate from IT as the entry point. Source
3,300	industrial organizations had data posted to ransomware leak sites in 2025. Source
42%	of intrusions (i.e. phishing, malware, ransomware) had operational outages that impacted revenue. Source

A unified international approach to secure OT connectivity

In January 2026, cybersecurity authorities from the Five Eyes alliance (United States, United Kingdom, Canada, Australia, and New Zealand), alongside Germany and the Netherlands issued a new guidance called Secure Connectivity Principles for Operational Technology (OT).

The guidance stresses that OT–IT connectivity is essential but must follow a secure-by-design model. It outlines eight principles to help organizations modernize connectivity while minimizing exploitable risk across industrial environments. Among these, hardening the OT boundary is identified as a strategic priority.

Principle 5: Why hardening the OT boundary is now a strategic imperative

The OT boundary is the critical contact point between these trusted operational systems and external networks. As connectivity expands, it becomes a prime target where attackers can gain control, compromise affected devices, move laterally and, eventually, elevate privileges to disrupt critical devices or functions.

A core component of hardening the OT boundary is ensuring that the identity of anyone accessing the environment is legitimate, along with ensuring secure machine-to-machine authentication. **Principle 5** of the international guidance highlights the use of **phishing-resistant multi-factor authentication (MFA)** for external and human-to-machine access to prevent credential-based attacks and unauthorized control actions. This new OT guidance spotlights phishing-resistant MFA which mirrors the Essential Eight, NIS2, PCI DSS, NERC CIP, NIST AAL3, OMB M-22-09 and more.

Phishing-resistant MFA requires hardware-backed public key cryptography on a Trusted Platform Module (TPM) along with user intent. The most effective method uses FIDO2 (Passkey) or PIV (Smart Card) protocols bound to a specific device, such as a YubiKey.

> “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 the user’s accounts, so they don’t need six different TOTPs.”

OT Security Specialist
Anonymous State-Owned Energy Company
Learn more

Harden the OT boundary with hardware-backed security from Yubico

Hardware passkeys, such as YubiKeys from Yubico, are the recommended MFA method that ensures portability, phishing-resistance, and independence from mobile signals.

The YubiKey enables organizations to deploy phishing-resistant authentication that supports secure access across both IT and OT environments at scale. Designed for industrial durability, the YubiKey is dustproof, crush-resistant, and water-resistant with IP68 certification.

Hardware-based cryptographic protection for industrial systems

While the YubiKey secures user access at the OT boundary, a hardware security module (HSM), like the YubiHSM from Yubico secures the cryptographic foundation within OT systems, machine-to-machine communication and integrity.

An HSM delivers enterprise-grade cryptographic security in a compact device, performing sensitive operations inside a dedicated hardware boundary and isolating keys from host systems to reduce the risk of compromise—even if surrounding systems are breached.

With the YubiKey, using the NFC interface, utilize wearables like rubber bracelets or gloves with a slot, so users can authenticate with a simple touch or tap, without having to remove protective clothing.

The YubiKey Family

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

Secure human-to-machine user access with the YubiKey

A modern hardware security key that offers phishing-resistant multi-factor and passwordless authentication.

- Reduce risk of credential theft by 99.99% and stops account takeovers while delivering 265% ROI[1]
- Embrace multi-protocol support on a single YubiKey: phishing-resistant protocols FIDO/Passkeys and Smart Cards(PIV), also supporting legacy OTP with an authenticator app
- Deploy the most secure passkey strategy: device-bound that is purpose-built for security and Authenticator Assurance Level 3 (AAL3) compliant
- Bridge to modern FIDO2 passwordless authentication
- Does not need battery, power, or cellular connectivity to function

Protect machine-to-machine communication across devices, servers and more with the YubiHSM

A hardware security module (HSM), that ensures enterprise-grade high cryptographic security and operation.

- Safeguard intellectual property, corporate secrets and secure manufacturing assembly lines
- Can be applied to any process where secrets and the authenticity of components needs to be managed
- Ultra-portable nano form factor allows for flexible deployment to any USB slot on servers, databases, robotic assembly lines, applications, and IoT devices

A call to action: Leading the shift toward secure-by-design OT connectivity

As OT environments continue to evolve, organizations must align with best practices and take proactive steps to make operational boundaries phishing-resistant and protect critical systems from credential-based attacks. Yubico is ready to partner with organizations and move toward a secure-by-design future where OT connectivity does not come at the cost of security. With exclusive enrollment and delivery services available through YubiKey as a Service, Yubico is here to help you deploy phishing-resistant MFA globally.

Trusted by

T-Mobile · Schneider Electric · Mitsubishi Electric · Naftogaz Group

Contact us yubi.co/contact | **Learn more** yubi.co/yk5

[1] Forrester TEI study, The Total Economic Impact™ Of Yubico YubiKeys

Yubico (Nasdaq Stockholm: YUBICO) is a modern cybersecurity company on a mission to make the internet safer for everyone. As the inventor of the YubiKey, we set the gold standard for secure, simple login, stopping account takeovers with phishing-resistant, hardware-backed authentication.

Our technology secures people in over 160 countries, delivering fast, passwordless access. Dual-headquartered in Stockholm and Santa Clara, we believe strong security should be within everyone's reach. Learn more at www.yubico.com.