



Yubico and IBM Consulting

Frictionless, Phishing-resistant Identity at Scale

The Executive Imperative: Identity Has Become the Primary Risk Surface

Digital transformation, with its shift to hybrid work, cloud, SaaS, and AI, has eliminated traditional perimeters, making identity the enterprise control plane. Meanwhile, advanced threats bypass legacy multi-factor authentication (MFA) such as SMS, push, or one-time passwords, via Adversary-in-the-Middle (AiTM), MFA fatigue, and social engineering. The challenge for CISOs and CIOs is to close the identity risk gap—securing the environment without adding friction, reducing productivity, or increasing costs.

The Partnership: Hardware Root of Trust Meets Enterprise Transformation

Yubico and IBM Consulting have joined forces to tackle identity risk. Yubico provides phishing-resistant, hardware-backed authentication (FIDO2, WebAuthn) and has pioneered passkeys to eliminate vulnerable credentials and passwords.

IBM Consulting brings global expertise in enterprise transformation, focusing on designing and implementing Zero Trust architectures, identity governance, regulatory compliance, and change management across multiple industries.

This partnership bridges the identity risk gap by combining strong authentication with enterprise-wide implementation. IBM creates and manages the secure digital framework, while Yubico ensures that only verified identities can access it.



Strategic Outcome: Frictionless, Phishing-Resistant Identity at Scale



The collaboration between Yubico and IBM Consulting is not simply an authentication upgrade. It is a strategic transformation of identity assurance. Together, we enable enterprises to:

- Eliminate the primary vector of credential-based breaches and operationalize Zero Trust architectures
- Reduce operational overhead and help desk burden and improve workforce productivity
- Achieve regulatory alignment while future-proofing authentication against evolving threats

By combining hardware-rooted trust with enterprise-scale transformation expertise, Yubico and IBM redefine digital trust for the modern enterprise—delivering frictionless, phishing-resistant identity at global scale.





Eliminating Credential-Based Breach Vectors

More than 90% of breaches involve compromised credentials, often due to legacy MFA's vulnerability to phishing, AiTM attacks, and credential replay. By deploying hardware-backed, phishing-resistant authentication (passkeys), enterprises eliminate these primary attack vectors. The passkeys cryptographically bind authentication and signing events to the user and device. IBM ensures consistent deployment across all hybrid environments, from legacy systems to modern SaaS platforms.



Compliance by Design and Future-Proofing Identity

With growing regulatory mandates for phishing-resistant, hardware-backed authentication (especially in finance, government, and healthcare), the partnership ensures a "compliant by design" posture. IBM manages compliance with global frameworks, while Yubico provides the high-assurance authentication with auditable proof mechanisms, future-proofing strategies against evolving regulations.



Reducing Operational Overhead While Improving Security

Deploying YubiKeys significantly reduces operational overhead. A Forrester Total Economic Impact™ study found a **265% return on investment** and up to a **90% reduction in password-related help desk tickets**, resulting in a **99.99% reduction in addressable credential theft risk**. Eliminating password dependency frees IT teams from reactive maintenance and allows them to redirect focus toward strategic initiatives.



265%
return on investment



99.99%
reduction in addressable credential theft risk



For more information, please visit yubi.co/contact



Enterprise-Scale Deployment Without Productivity Loss

For multinational organizations, the Yubico and IBM Consulting partnership ensures frictionless deployment at scale. Yubico's YubiKey as a Service, combined with IBM's change management expertise, allows employees to receive keys securely and authenticate immediately. This approach minimizes "Day 1" productivity dips and reduces transition support burdens, making identity modernization an enabler of workforce productivity.



Resilience Across Constrained and High-Security Environments

YubiKeys offer resilience in constrained and high-security environments, such as mobile-restricted or air-gapped locations. Functioning without batteries, cellular, or Wi-Fi, they ensure consistent, offline authentication where app-based MFA is impractical.

