BEYOND IDENTITY + YUBIKEYS

Beyond Identity

Secure Desktop Access

Beyond Identity removes the weakest link in desktop authentication: shared secrets. With native support for hardware-bound credentials like YubiKeys using the PIV standard, Beyond Identity enables phishing-resistant login to Windows desktops, without relying on mobile phones, networks, or passwords.

Product Features

Secure hardware-backed login

Leverages FIPS-validated YubiKeys with PIV credentials for local login. No mobile device or password required.

Offline access

Login works even when disconnected from the network, making it ideal for field operations and emergency scenarios.

Built for high-security environments

Perfect for regulated industries, shared workstations, manufacturing floors, and clean rooms — anywhere mobile phones aren't allowed.

Device trust

Use device signals like firewall, antivirus status, and risk signals from your MDM, EDR, and ZTNA in access decisions to block risky, non-compliant devices.

Key Differentiators

Phishing-resistant authentication

Hardware-bound keys eliminate credentials that attackers can steal or intercept.

No mobile dependency

Works seamlessly in secure zones, shared workstations, and facilities where phones are prohibited.

Strong compliance posture

Uses FIPS-validated hardware and meets MFA requirements under CJIS, HIPAA, PCI DSS, and NIST.

Works offline

Authenticate without relying on Wi-Fi, LTE, or VPN access, all critical for operational continuity.

Immutable audit logs

Prove who did what, when, and how for investigations and audits by tying access to a hardware-bound credential.

Business Outcomes

- Make phishing and other credential-based attacks impossible
- Meet mandates like CJIS, HIPAA, and PCI DSS
- Secure access for frontline workers and field agents, even in mobile-free and offline zones
- Eliminate login friction and reduce IT tickets
- Simplify investigations and audits