Proximia

Technical Overview

Proximia replaces passwords with something fundamentally stronger: verified human presence. Users sign in with a biometric check and stay signed in only while they are physically present — the platform continuously confirms that the authenticated person is still at the workstation and locks the session the moment they step away. There are no passwords to phish, reuse, or steal, and no unattended sessions to hijack.

The result is a security posture aligned with Zero Trust principles that is also faster and simpler for users: sign-in takes seconds, and the help-desk burden of password resets disappears.

(844) 438-7769

sales@proximia.com

proximia.com

PROXIMIA®

The Problem: Trust Granted Once Is Trust Misplaced

Modern organizations face a fundamental contradiction: the tools designed to protect access are often the same ones that attackers exploit to breach it. Passwords, MFA tokens, and session cookies are all compromisable artifacts. Yet most identity and access management (IAM) systems continue to rely on them as the primary basis of trust.

Industry breach reports consistently identify stolen credentials as the leading initial access vector. The root cause is architectural. Traditional systems verify identity once, at sign-in, and then assume the session remains in the right hands until sign-out or timeout. That model creates three exploitable gaps:

- **No session continuity —** After sign-in, nothing confirms the same person is still present. A stolen session token grants full access to whoever holds it.
- **No presence awareness —** Systems cannot tell when a user walks away, leaving live sessions exposed to anyone nearby.
- **A persistent attack surface —** As long as passwords exist anywhere in the chain, they can be phished, guessed, or replayed. Add-on MFA reduces risk but introduces its own attack vectors.

Authentication, Reinvented

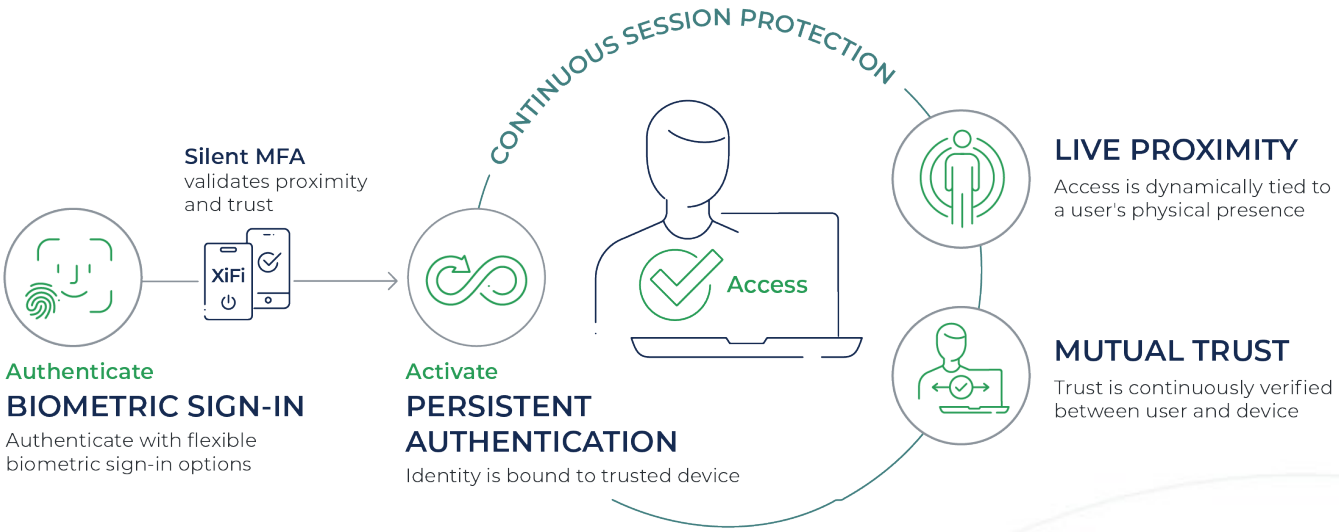
Built Different From the Ground Up

Proximia was built to address these gaps at the architectural level. Rather than layering security controls on top of a credential-based model, Proximia eliminates password credentials entirely and replaces point-in-time authentication with persistent, presence-aware verification. Identity is bound to the user's physical presence, not to a static token or remembered secret. The session is protected continuously, not just at the front door. The result is an authentication model where there are no password credentials to steal, no sessions to hijack without physical presence, and no friction tax on users to achieve it.

How Proximia Works

Proximia binds each session to a verified person and their trusted device, then keeps verifying for as long as the session lasts:

- **Biometric sign-in —** Users authenticate with facial recognition or their device's native biometrics. Biometric matching is performed locally; raw biometric images are never stored or transmitted.
- **Continuous presence verification —** A trusted device — a Proximia XiFi Card or the user's phone — communicates with the workstation over an encrypted, mutually authenticated wireless channel with cryptographic distance verification. Live proximity sensing confirms the user is physically present throughout the session, not just at sign-in.
- **Mutual Trust —** Both the user and device continuously verify each other. A found or stolen XiFi Card cannot unlock anything on its own — the user's biometric is always required, and the device must prove it remains trusted and uncompromised.
- **Automatic lock on departure —** When the user moves outside the administrator-configured proximity zone (typically five to thirty feet), the session locks within seconds. Re-entry requires the user's biometric.



Legacy Protocol Support — Where underlying systems require password-format credentials — Windows login, RDP, and VDI — Proximia generates and injects them automatically. Users never see, know, or manage them. There is nothing to phish, reuse, or steal.

Attack Vectors Eliminated

Proximia is designed to structurally eliminate the three most exploited attack vectors in modern identity security.

Credential-Based Attacks

Credential-based attacks exploit user-managed passwords and static MFA to gain initial access — through phishing, credential stuffing, password reuse, replay attacks, MFA fatigue, and SIM swapping.

Proximia eliminates the password credential attack surface entirely. Users never create, manage, or enter passwords — there are no password credentials to phish, reuse, or steal. For Windows login and RDP/VDI sessions that require password-format credentials at the protocol layer, Proximia generates and injects system-managed credentials automatically — users have no knowledge of them and they cannot be extracted.

Session Hijacking and Post-Sign-In Exploits

Once authenticated, traditional systems offer no ongoing verification of presence or session integrity — leaving sessions vulnerable to token theft, credential replay, lateral movement, and access to unattended workstations.

Proximia introduces persistent session protection. Authentication continues throughout the session via continuous BLE proximity detection and mutual device trust. A stolen session token is useless without the user's physical presence and registered proximity device. Access is continuously earned, not permanently granted.

Insider Threats and Physical Security Risks

Insider and physical risks include shared workstation misuse, shoulder surfing, lost or stolen proximity devices, and abandoned sessions — attacks that succeed because traditional systems cannot distinguish between the registered user and anyone else at the same workstation.

Proximia addresses this through biometric identity verification combined with proximity-based session enforcement. Every session requires a biometric match; proximity devices are useless without it. Workstations lock the moment the authenticated user steps away, and shared workstations support per-user session isolation — each user authenticates independently with no shared credentials.

Why Existing Solutions Fall Short

Password managers and SSO reduce friction but don't eliminate passwords. Credentials remain in vaults that are high-value breach targets. SSO still pushes password-format credentials into underlying systems during federation. Both fall back to passwords when something fails, and neither provides any protection after sign-in.

Traditional "passwordless" solutions use phone-based authenticators as a substitute for password entry — but maintain passwords as a backend fallback. Push-based MFA introduces fatigue and SIM-swapping risks. And like all point-in-time systems, they offer no session protection after sign-in.

FIDO2 and passkeys eliminate passwords at sign-in and represent a meaningful step forward. But they address the sign-in event only — no session continuity, no presence detection, and no protection against unattended workstation access. They also typically require a phone or hardware key, limiting deployment in restricted environments.

	Proximia	Imprivata	Windows Hello	Okta / Duo
Biometric-bound passwordless Windows sign-in	✓	✗	✓	✗
Continuous session protection after sign-in	✓	⚠ *Phone required*	✗	✗
Presence-based auto-lock on walk-away	✓	⚠ *Phone required*	✗	✗
Shared workstation support	✓	✓	✗	✗
Phone-free option	✓	⚠ *Initial Badge + PIN Major security gaps*	✗	✗
Offline / disconnected support	✓	⚠ *Badge + PIN*	✓	✗
RDP / VDI support	✓	✗	✗	✓
Zero Trust enforcement beyond sign-in	✓	✗	✗	✗
Easy deployment	✓	✗	✓	✗

They added Zero Trust language. We built the architecture.

Technology Architecture

Proximia is engineered end to end — from embedded firmware to cloud services — rather than assembled from third-party authentication components. That vertical integration is what makes continuous, presence-aware authentication practical at enterprise scale.

Backend services	Service-oriented backend with an enterprise relational database; REST APIs for integration.
Admin console	Web-based administration console with role-based access control
Windows agent	Native Windows service and credential provider, integrated directly with Windows logon, RDP, and VDI.
Mobile apps	Fully native iOS and Android applications; platform biometrics, hardware-backed keystores, background proximity.
XiFi Card	Ultra-low-power embedded firmware on a hardened real-time operating system, with motion-based power management.
Cloud platform	Cloud-native, container-orchestrated services on AWS; fully reproducible infrastructure-as-code; centralized observability and immutable audit logging.

Proximity and Presence Technology

- **Bluetooth Low Energy (BLE) —** provides the always-on proximity foundation — present in virtually every modern laptop, desktop, and phone, with no additional infrastructure required.
- **Cryptographic distance verification —** Proximia implements BLE Channel Sounding–based distance estimation, a defense designed specifically against relay attacks: an attacker who forwards radio traffic cannot fake the round-trip physics of the measurement.
- **Rotating ephemeral identifiers —** prevent the XiFi Card from being tracked or correlated across locations by passive observers.
- **Layered verification —** Proximity alone never grants access — it is continuously combined with biometric identity, mutual device authentication, and session integrity checks, mitigating the classic weaknesses of any single radio technology (interference, spoofing, relay).

Cryptographic Architecture

- **Hardware-rooted device identity —** Each registered device holds a unique P-256 key pair generated and stored in hardware — Apple Secure Enclave, Android StrongBox/Keystore, or protected platform key storage on Windows. Private keys never leave the hardware.
- **Mutual authentication by design —** Mutual authentication by design. Sessions are established with a mutually authenticated key exchange built on a well-audited, standards-based design family, the same class of construction used by leading secure-messaging and VPN protocols. Both sides prove identity before any data flows.
- **Authenticated encryption —** All session traffic is protected with AES-256-GCM authenticated encryption using ephemeral per-session keys, providing confidentiality, integrity, and replay protection.
- **Crypto-agility —** The key architecture is algorithm-agnostic, designed to adopt NIST post-quantum cryptography standards without re-architecting the platform.

Security and Privacy by Design

- **Zero Trust alignment —** Built to support NIST SP 800-207 and the NSA's pillars of Zero Trust: every access decision is verified continuously, with no implicit trust.
- **Biometric privacy —** Proximia never stores or transmits raw biometric images. On mobile platforms, biometric validation is handled entirely by the operating system; Proximia has no access to the underlying data. On Windows, biometric matching runs locally and capture data is discarded immediately after verification.
- **Credential security —** System-generated credentials are created on demand and are never visible to or accessible by users.
- **Auditability —** Session-level audit logging — including authentication events, proximity changes, and credential activity — provides full traceability for compliance and incident response.

Certifications and Standards

- **SOC 2 Type II certified —** Proximia is independently audited against the AICPA Trust Services Criteria.
- **HIPAA —** Audit logging, access controls, and encryption aligned with HIPAA requirements for healthcare deployments.
- **NIST SP 800-207 —** Architecture designed around the NIST Zero Trust model, mapped to the NSA's seven pillars of Zero Trust.
- **Open identity standards —** FIDO2/WebAuthn, OpenID Connect, OAuth 2.0, and SCIM 2.0.

Compliance reports and security documentation are available through the Proximia Trust Center at trust.proximia.com.

Enterprise Integration

Proximia is built on open identity standards and is designed to extend — not replace — existing IAM investments:

- **Identity standards —** OpenID Connect, OAuth 2.0, SCIM 2.0 user provisioning, and FIDO2/WebAuthn
- **Directory services —** Active Directory and Microsoft Entra ID, including automated user lifecycle management via SCIM
- **Remote access —** RDP, VDI, and terminal-server environments with the same continuous-authentication model
- **APIs —** REST APIs for provisioning, policy management, session monitoring, and audit-log retrieval, enabling SIEM and SOC integrations

Where Proximia Fits

- **Regulated and high-security environments** — meeting regulations and strict audit requirements with zero tolerance for unauthorized access
- **Remote and distributed workforces** —passwordless RDP/VDI and presence enforcement that follows the user, regardless of network location
- **Shared-workstation operations** — fast user switching with per-user isolation and automatic locking

Implementation

Every new account is assigned a dedicated Customer Success Manager who guides deployment from start to finish. Proximia is available as a fully managed cloud deployment or via Flex Mode, which supports phased rollouts by allowing selected users to retain passwords during migration. Initial configuration typically completes in under two hours using standard enterprise management tools, with workstation deployment scripted or per-device at your team's discretion. User onboarding averages six minutes per person — biometric enrollment plus XiFi Card provisioning.

Authentication, Reinvented.

The world’s first persistent, presence-aware authentication platform.

proximia.com | sales@proximia.com | (844) 438-7769