PROXIMIA®

Eliminate 90% of Modern Attack Vectors

Current Identity and Access Management (IAM) systems stop at login — trusting users for the rest of the session. Proximia continuously verifies identity, proximity, and device trust to **eliminate the three most exploited attack surfaces behind the majority of modern breaches.**

100% Threat Elimination from Compromised Passwords

Credential-Based Attacks

Proximia neutralizes the most common entry point for attackers by eliminating passwords and static MFA entirely.

ELIMINATES: Phishing · Credential theft · Password reuse · MFA fatigue · Replay attacks

How Proximia stops them:

- **Passwordless architecture:** Removes passwords and user-managed secrets, ending phishing and password reuse.
- **Dynamic, ephemeral credentials:** Each authentication generates short-lived, rotating tokens that can't be intercepted or replayed.
- **No phone dependency:** Removes push fatigue and SIM-swap risks common in mobile MFA.

Session Hijacking & Post-Login Exploits

Proximia closes the post-login security gap every other IAM leaves open, securing the session from start to finish.

ELIMINATES: Session hijacking · Credential replay · Lingering access after login · Unattended session takeover

How Proximia stops them:

- **Persistent, presence-aware authentication:** Continuously validates user proximity and trust throughout the entire session.
- **Automatic session lock:** Instantly locks when the verified user steps away or proximity is lost.
- **Mutual trust model:** Both the user and the device must continuously validate one another — preventing stolen-session abuse.

Insider & Physical Threats

Protects critical on-premise systems in environments like hospitals, courts, utilities, and industrial facilities — even inside the perimeter.

ELIMINATES: Shared-workstation misuse · Shoulder-surfing risks · Lost-badge exploitation · Unauthorized local access

How Proximia stops them:

- **Biometric identity verification:** Ensures only the authorized user can activate or continue a session.
- **Proximity-based access enforcement:** Keeps sessions active only when the user and trusted device remain present.
- **Automatic lock on absence:** Prevents opportunistic misuse when users step away.
- **No visible credentials:** Removes PINs and passwords that could be observed or memorized.

ZERO passwords. phishable credentials.

Fastest Login. Longest Protection.

TRUE ZERO TRUST ARCHITECTURE

proximia.com | sales@proximia.com

(844) GET-PROX or (844) 438-7769

PROXIMIA®