



Proximia Addresses all 7 Pillars of Zero Trust

The Gold Standard of Cybersecurity

Proximia adheres to the strict guidelines of Zero Trust Architecture (ZTA). Zero Trust means trust nothing and verify everything, creating a digital fortress around your data.

1 USER:

Continually authenticate users and monitor their activity to govern access while protecting every interaction.

Proximia assigns a digital ID using secure biometrics. Authentication persists across sessions and devices through bi-directional trust and proximity. Every event and interaction is monitored and protected inside the Proximia ecosystem.

2 DEVICE:

Verify that every device accessing resources is located, authenticated, authorized, and evaluated against security policies.

Proximia verifies device identity through the user's digital ID, then tracks location, login patterns, device proximity, and trust signals. Risky conditions (lost biometrics, distance, mutual trust failure) can trigger lockout.

3 APPLICATIONS & WORKLOADS:

Secure applications, hypervisors, containers, and virtual machines.

Biometrics, mutual trust, and dynamic proximity grant initial access, then persistently enforce protection across all workloads and sessions based on the organization's access policies and individual user profiles.

4 DATA:

Enable transparent visibility and secure all data through enterprise encryption, standards, and logging.

Proximia applies full end-to-end encryption, logs all authentication events, and exposes an API for monitoring, analytics, and asset tracking.

5 NETWORK & ENVIRONMENT:

Segment, isolate, and control network environments with granular policies and access controls.

By combining cyber and physical authentication, Proximia secures every session beyond login. Persistent biometrics and proximity reduce user error and complexity while maintaining segmented network benefits.

6 VISIBILITY & ANALYTICS:

Analyze events and behaviors using context and AI/ML to improve detection and reaction time.

All authentication events flow into Proximia's REST API, giving full visibility into user behavior, devices, network access, and enabling stronger security decisions.

7 AUTOMATION & ORCHESTRATION:

Automate security responses using rules and AI — blocking actions or triggering remediation when needed.

Proximia logs all identity events in real time, enabling automated processes, alerts, and actions driven by user behavior and organizational policies.