PONE
BIOMETRICS

Black paper
20250616

ZERO TRUST SECURITY IN THE REAL WORLD: MOVING FROM PASSWORDS TO PROOF OF PRESENCE

Pone Biometrics AS

PONE
BIOMETRICS

Black paper
20250616

REDEFINING TRUST IN A ZERO TRUST WORLD

In a world where digital identities are under constant threat, organizations must stop trusting by default. The Zero Trust Security model flips the old assumptions of perimeter-based security. It demands that every access attempt be explicitly verified, every time, for every user, on every device.

This is where Knowledge-Based Trust, meets modern innovation. At Pone Biometrics, we see Zero Trust not just as a buzzword, but as a design principle that should shape how authentication feels for real users. Our FIDO2-certified device, OFFPAD+, brings Zero Trust to life, securely, intuitively, and without compromise.

WHAT ZERO TRUST REALLY MEANS

In essence, the Zero Trust model is built on the principle that trust should never be assumed, every access request must be explicitly verified, regardless of user, device, or location. Zero Trust means:

→ Never trust, always verify.
→ Trust is not a location (e.g., on the corporate VPN), but a decision that is earned at every moment.
→ Identity is the new perimeter and it must be provable, resistant to theft, and frictionless to use.

Traditional logins fail this test. Passwords can be guessed, phished, leaked. Even one-time passwords sent via SMS can be intercepted. Zero Trust requires strong, phishing-resistant authentication, grounded in who the user actually is.

KNOWLEDGE-BASED TRUST VS BLIND TRUST

Traditional security models relied on the assumption that anyone inside the network perimeter could be trusted, granting access based on location or device rather than continuous verification. Old security models granted access based on:

→ A known device.
→ A remembered secret.
→ A network location.

The world now demands more: It builds trust through verifiable, context-aware signals—something you are, something you can prove, and something that cannot be transferred. This is where biometrics and visual feedback matter.

THE OFFPAD+ DIFFERENCE: TRUST THAT YOU CAN SEE AND FEEL

OFFPAD+ embodies our approach to Zero Trust authentication, delivering strong, passwordless security that verifies identity at every step, without compromising user experience:

→ A standalone biometric security key (FIDO2-certified)
→ With a built-in screen that tells you exactly which service you're about to authenticate
→ And a fingerprint sensor that authenticates you, and only you, in milliseconds·

WHY THE SCREEN MATTERS:

In Zero Trust, trust must be explicit and earned. OFFPAD+ shows you the service requesting authentication—so you see what you're about to trust, before you commit.
No blind approvals. No guesswork. Just informed, verifiable trust.

WHY BIOMETRICS MATTER:

Your fingerprint proves presence and intent, not just once, but every time you authenticate, many times a day. This aligns with the Zero Tust principle of continuous validation.

BUILT FOR SECURITY. DESIGNED FOR HUMANS

OFFPAD+ requires no passwords, stores no sensitive data online, and integrates with leading platforms that support FIDO2/WebAuthn. It brings security from the cloud to the palm of your hand, where it's local, secure, and controlled by you.

And because OFFPAD+ stores a template of your biometric data, not the actual fingerprint securely on the device (never transmitted, never stored in the cloud), it maintains full compliance with privacy standards, including GDPR and contributes to accessibility principles.

ZERO TRUST IS A JOURNEY. LET OFFPAD+ BE YOUR GUIDE

Whether you're protecting enterprise logins, securing privileged access, or enabling passwordless experiences for your workforce, Zero Trust starts with strong authentication—but it doesn't end there.

At PONE Biometrics, we're committed to building trust you can see, touch, and verify. Not just once. Every time.

Explore OFFPAD+ at ponebiometrics.com

PONE BIOMETRICS