

One Device. Multiple Missions.

The practical multi-domain mobile security platform for federal, contractor, and first-responder missions.



Why Redwall Technologies was formed

Redwall's founding team worked directly with government partners to test the real-world security of mobile devices — including official, locked-down devices issued to personnel in the field. That work found a pattern: when official devices were too locked down for personal use, people turned to unsecured personal devices instead, and attackers went after the gap.

Redwall Mobile was built to close that gap, on three principles: security has to be built into the operating system itself, not added on as an app. It has to stop attacks it has never seen before. And no two personas can ever be active in memory at the same time.

What makes Redwall Mobile different

Redwall Mobile's security monitor runs above root, watching for behavior that deviates from what the system should be doing — not matching known attack signatures. That's what lets it stop new attacks without waiting for a patch. The same monitor runs real-time integrity checks on the kernel, critical memory, and key files, so tampering or privilege escalation gets caught as it happens.

On top of that platform security, temporal and cryptographic isolation mean only one persona is ever live — decrypted, active, and exposed — while every other persona stays sealed. Each persona sets its own rules for camera, GPS, Bluetooth, NFC, and network access, enforced by policy, with zero changes required to the apps themselves.

Why isolation, not promises

Nothing is impenetrable. That's exactly why True Isolation and the underlying platform protections exist. If one persona is ever compromised, it stays contained. The device, the other personas, and the data behind them stay protected.

One device. Multiple personas.

Redwall's Secure Persona® turns one device into as many isolated personas as a mission requires. Each persona has its own encrypted data store, its own set of approved apps, and its own rules for networks, Bluetooth, NFC, and sensors — managed independently, persona by persona. Switching personas wipes the previous persona's keys and memory before the next one opens.

In practice, that means a personal app can't reach official data, even by accident. A classified persona won't let an unapproved Bluetooth device join a call or let data move to a device that isn't cleared to receive it — even if a user tries.



Built on Zebra hardware already trusted in the field

Redwall Mobile runs on Zebra's rugged Android devices, including the EM45 handheld and the TC and ET series — hardware your team already knows. Most of the lineup, including the TC27, TC58, TC78, and ET65, adds hot-swap batteries, so a dead battery never takes a mission offline.

Redwall Mobile is officially signed with no unlocked bootloader, meeting federal integrity requirements out of the box. It moves to new Zebra devices without re-engineering effort and with zero changes to existing apps, whether custom-built or from the Google Play Store.

Military-grade track record. Practical every day.

More than a decade in the field. No confirmed breach of the operating system has ever been reported to us.

- Officially signed. No unlocked bootloader.
- Built for the field, not the lab.
- Hot-swap batteries on the current TC/ET lineup.
- Zero changes required to existing apps.

Built for the missions that can't fail

Different roles. Different classifications. Different rules of engagement. Redwall Mobile isolates every role and classification on a single device — for DoD, DHS, the Intelligence Community, federal contractors, and state and local police and first responders.