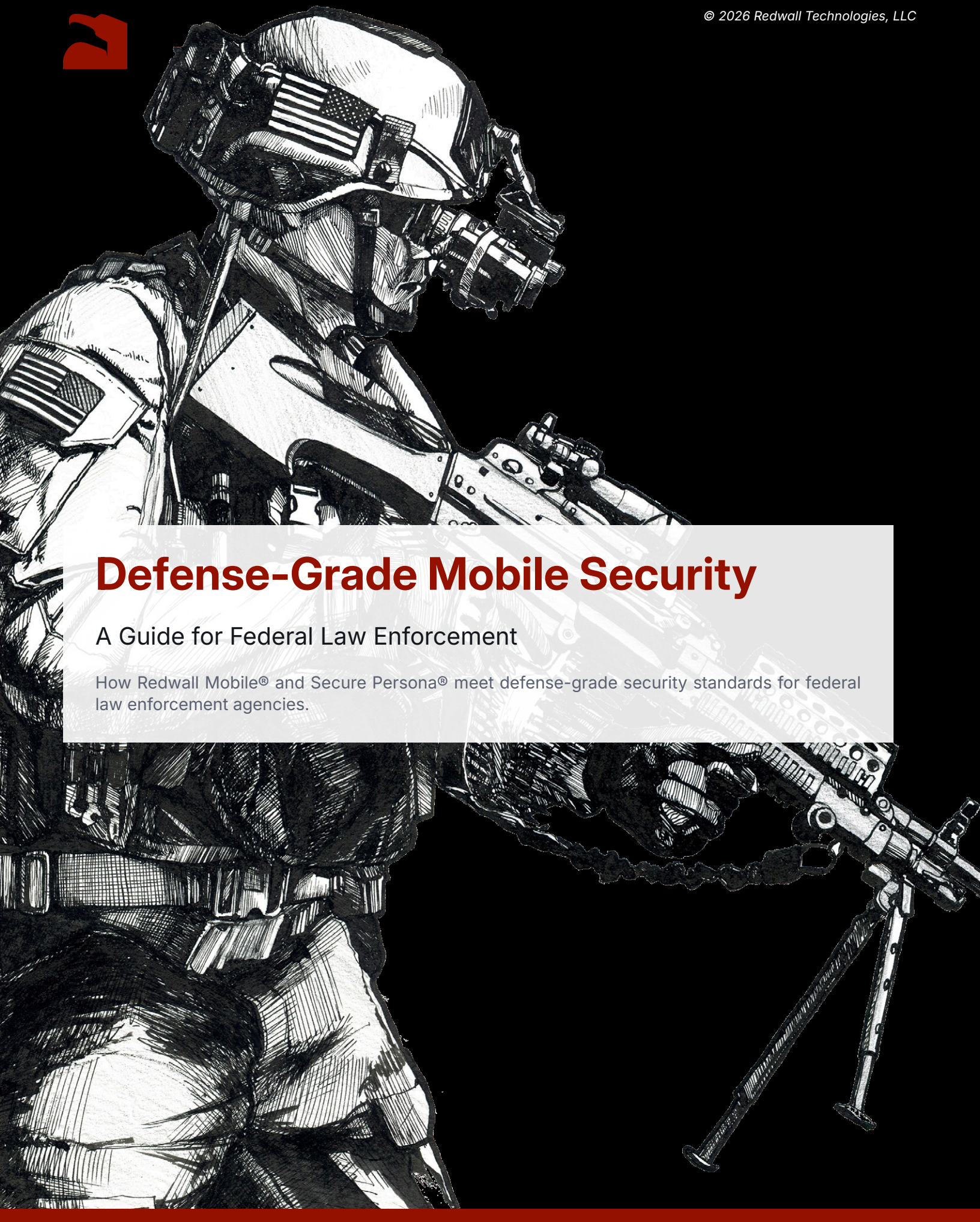

Defense-Grade Mobile Security

A Guide for Federal Law Enforcement

How Redwall Mobile® and Secure Persona® meet defense-grade security standards for federal law enforcement agencies.

The Weakest Link

Mobile devices are everywhere: indispensable to our personal lives, and increasingly to our professional ones. Public and private-sector organizations equip their workers with mobile computers and tablets to streamline processes, boost productivity, and improve communication. But the shift to a connected workplace comes with its own risks.

For federal law enforcement and other government agencies, the biggest challenge is fortifying mobile-device ecosystems against a constant threat of cyberattacks. A majority of public-sector organizations report having experienced a mobile-related security compromise, and most agree mobile-device security deserves to be taken more seriously. Mobile devices aren't always the target. They're a convenient entry point to back-end systems holding sensitive or classified data.

Mobile devices that rely on OS-level security protections and frequent patches are the weakest link in security and data protection, leaving agencies vulnerable to zero-day attacks and other potentially devastating threats.

Mobile Policies: Limited Options

Government employees using mobile devices face a range of threats: advanced nation-state attacks, organized crime using fraud technology, and simple theft of a phone. Attackers targeting government agencies often use the same methods they use against consumers: call interception, location tracking, social engineering, ransomware, identity theft.

When agencies mix enterprise and personal devices on their networks, security tradeoffs are unavoidable. Do you allow personal devices on duty and accept the risk, or prohibit them and invite unauthorized shadow devices instead? However a BYOD policy is written, the stakes for government agencies are too high for "good enough."

There's no policy that resolves this tradeoff on its own. It takes a device built to make the tradeoff unnecessary.

Real-World Implications

When government employees carry multiple mobile devices to separate work from personal use while on duty, it creates unnecessary security risk, and it's a burden for the user. What happens when IT leaders can't strike the right balance between performance and security in their mobile networks? A few examples:

1

Venue managers, law enforcement personnel, and first responders often lack the capacity to coordinate securely in real time, compromising their ability to manage threats and mitigation.

2

Agencies unable to share real-time information securely while staying isolated from cyber threats have one option: power through and accept the risk.

3

Critical-infrastructure operators locked out of immediate-action communications when away from a desk put vital resources at risk.

4

Agencies overpay for hardened, specially-approved networks that still end up with limited real-world capability.

5

Case files and evidence handled on an officer's personal device, because the official system was too locked down, put chain of custody and the case itself at risk.

A significant share of public-sector organizations with a mobile-related compromise also suffered reputational damage or faced regulatory penalties.

Every scenario above shares the same root cause: mobile-device security bolted on after the fact, instead of built into the device from the start.

Achieving Complete Protection

Building and maintaining a fortified mobile-device network is complex, but purpose-built solutions exist for government agencies in the age of BYOD. With the right combination of enterprise-grade hardware and software, agencies can protect their devices, applications, and connected infrastructure. When evaluating security solutions, here are the factors that matter:

1. Built into the operating system

Any solution that runs on top of the OS as an app, or is installed after the device ships, has to rely on that OS never being compromised. A truly effective solution is built in by the manufacturer, booting as part of the native device OS.

2. Dual persona isn't the answer

Dual-persona approaches partition a device to separate IT-controlled work apps from personal data, but sensitive data still sits in shared memory, leaving the device vulnerable. Dedicated single-purpose devices aren't the answer either. The right solution consolidates every feature of a locked-down, defense-grade device with multiple personas into one device.

3. Never trust the OS

Operating systems carry a huge surface area of code from many developers. That's the primary source of publicly acknowledged hacks. An effective solution protects even against processes with root permissions, based on a use-case-specific policy.

4. Nation-state-grade security

Cybersecurity "solutions" are everywhere, and most fail regularly. Law enforcement and other government agencies should accept nothing less than a proven, defense-grade solution.

5. Keep memory separate

Never accept a solution that leaves sensitive data in memory at the same time as lower-security uses, including hypervisor solutions, regardless of their claims. Choose a solution that keeps each use case completely separated.

Consolidating to a single mobile device can eliminate security risks and reduce cost and complexity.

"Government mobile devices represent an avenue to attack back-end systems containing data on millions of Americans, in addition to sensitive information relevant to government functions."
U.S. Department of Homeland Security, Study on Mobile Device Security

Redwall + Zebra Technologies

Redwall Technologies brings a unique approach to mobile security, giving agencies the tools to reduce mobile-device operating costs, strengthen device security, and gain greater functionality. Redwall enhances Zebra's rugged, best-in-class mobile computers to support the highest levels of performance, durability, and security for any application. With Redwall Mobile® and Secure Persona®, government agencies achieve complete mobile-device protection. Every device ships officially signed, with no unlocked bootloader and no custom ROM. Redwall is built into the device as it leaves the factory, not bolted on afterward.

Redwall Mobile: unmatched device control and security

Redwall Mobile protects, separates, and controls information on mobile devices from beneath the operating system. It operates at a higher privilege than the OS, controlling it and making protected devices fully configurable at the feature and function level. Agencies can stop zero-day attacks and prevent privilege escalation by users, apps, or the OS itself.

- Stops new attacks without waiting for an OS patch cycle
- Officially signed. No unlocked bootloader, ever
- Policy-driven activation and deactivation of device functionality prevents accidental compromise
- Custom configurations deploy in minutes
- Protects against unauthorized data access, surveillance, and device tracking

Secure Persona: unmatched role-based privacy

Secure Persona lets one device serve as many, extending the value of mobile devices and solving the BYOD dilemma for government agencies. Only one persona is ever live. Each has its own security settings, authentication requirements, and policy controlling access to system features, drivers, files, and networks.

- Easily configure devices for highly compartmentalized roles: multi-level security, law enforcement on-duty/off-duty
- Unique controls and settings per persona maintain complete separation and isolation
- Every Redwall Mobile control feature is available by persona
- Multi-SIM operation by role or persona

Suggested modes for law enforcement

Personal
Officer's own use. Not agency-tracked. No path to duty systems.

Duty
Full agency control, including location and policy. Day-to-day operational tools and networks.

Restricted
Same complete separation, configured tighter by the agency: approved apps and networks only. For higher-sensitivity work.

Each mode has its own storage, settings, security policy, apps, data, VPN, and network rules. Only one mode is live at a time.

Military-grade track record. Practical every day.

Nothing is impenetrable. That's why isolation exists: if one mode is ever compromised, it stays contained, and the device, the other modes, and the data behind them stay protected. More than a decade in the field, with no confirmed breach of the operating system ever reported to us.

www.redwall.us | sales@redwall.us | (937) 477-0424

REDWALL TECHNOLOGIES LLC

Recommended Hardware

Redwall software is compatible with a wide range of devices and technologies, but it has to be built in. You need a device that already has Redwall's platform integrated into its operating system. Redwall Mobile and Secure Persona are designed to provide maximum benefit when deployed on Zebra's next-generation mobile computers. **www.redwall.us/zebra**

EM45

Zebra's primary Redwall Mobile-ready device: a rugged, everyday handheld built for field-first agencies that need one device to cover every mission.

TC53/TC58

Rugged handheld computers built for workers who need enterprise-grade durability without sacrificing a familiar, phone-like form factor. Hot-swappable batteries mean a dead battery never ends a shift.

ET60/ET65

Rugged tablets for vehicle-mounted, office, and field-based computing, with a shared accessory ecosystem across configurations. Hot-swappable batteries keep a shift going.

All three run Redwall Mobile and Secure Persona out of the box: officially signed, no unlocked bootloader, ready for federal deployment.