REDWALL TECHNOLOGIES LLC

Consumer-use operating systems – a misfit for Enterprise missions

Bottom Line Upfront: There is an increasing need to deploy enterprise-grade tablet computers for telework, telehealth, logistics, maintenance, and construction applications.

These activities correspondingly involve a mobile workforce operating at remote locations often in austere settings. These use cases frequently rely upon personal, untrusted, or limited network resources for connectivity to the enterprise network. Environmental constraints such as low bandwidth or infrequent connectivity to the organizations' host networks limit the frequency and size of over-the-air authentication and operating system and application patch-updates. These oft-deployed mobile tools host mission-essential applications and connected peripheral devices that may be impacted by forced changes to the host operating system (OS), placing a premium on stability. Frequent operating system updates to fix flaws, patch vulnerabilities, and add features undermine the utility of these devices, greatly complicating and increasing the enterprise information technology (IT) support workload and cost. These impacts are magnified with software-as-a-service subscription, such as Microsoft 365® / Windows 10®.

Military use of Tablet computers for healthcare, logistics and maintenance are applications that underscore these issues. The current Microsoft Windows 10 software-as-a-service subscription model introduces complexity and instability for military use on remote bases, ships, and in tactical environments. The authentication and key management burden, exceptionally large OS/OS patch-size, over-the-air update requirements, and regular patch frequency can be highly disruptive and destabilizing-placing the mission and our service members at greater risk. Similar issues exist with Apple iOS® devices. Electronic Flight Bags (EFB) such as Foreflight® and Garmin® are deployed on iPads® and iPhones®. These mission-essential planning and navigation tools must be revalidated prior to the end user accepting iOS updates. This condition creates a conflict because vital security patches are delayed until the EFB software can be retested and validated prior to permitting the upgrade; leaving the host devices susceptible to exploits in the interim. The Android OS upgrade/update process, though less onerous than Windows 10 and iOS, can be problematic as well. Adapting a consumer-grade Tablet computer OS for an enterprise mission no longer serves enterprise needs. This OS patch "whack-a-mole" cycle *makes the end-use Tablet computer the weak link in security and stability* for Enterprise customers. An alternate approach is needed.

Windows 10 currently requires 20 gigabytes (GB) for a clean install. In addition to an ever-expanding footprint, the OS requires continual patching, with patch sizes often exceeding 1 GB. Each patch cycle requires a vigorous level of testing to ensure that the applications installed on the tablet function in accordance with enterprise needs. Windows license activation requirements present an additional level of complexity for systems that must function in austere environments that include both network-connected and standalone, closed-loop configurations. Microsoft Windows activation requires a Key Management Service for connected systems and a soft token for disconnected systems. The tablet work environment often has network bandwidth restrictions significantly increasing the risk of authentication and update failure or interference with work applications and activities.

There is a Solution: Redwall Mobile® security, from Redwall Technologies, LLC. Redwall Mobile provides a stable operating system architecture for Android OS devices that eliminates the patch and update *whack-a-mole* cycle of Microsoft Windows 10 and Apple iOS Tablet devices. Redwall Mobile is a commercially released, National Information Assurance Partnership (NIAP) certified mobile security solution that is currently shipping worldwide on Motorola Solutions LEX L11 rugged smartphones. It provides unmatched OS control, security, and privacy. Key benefits of Redwall Mobile include:

- Commercial OS: Redwall Mobile is a security solution and features enhancement to the widely supported Android open-source OS. Android boasts a large pool of global software developers readily available for app development, maintenance, and support. Redwall Mobile secures Android and stabilizes the OS at a level not possible with Windows 10 and iOS.
- Potential for 0 patching: Redwall Mobile is an industry-leading security solution that has protected the Android OS from exploitation of vulnerabilities for over five years without the need for patching or upgrades. Redwall protected mobile devices can be fielded and trusted for the entire device life-cycle, without subjecting them to security-patch whack-a-mole experienced with Windows 10, iOS and unprotected Android devices.
- Multi-level and role-based security on a single device: The Redwall Mobile architecture was specifically designed to support multi-level security on a single device. This unprecedented capability and approval for Government use via the Commercial Solution for Classified (CSfC) certification demonstrate its ability to separate classification levels. Outside of the military, this capability lends itself to configuring multiple unique Secure Personas® (roles) on a single device, each with its own profile, applications, and privacy.
- Government Purpose and End Use Licensing: Redwall Mobile is sold as a licensed product, with an End-Use License Agreement, and annual renewals that include the provision for upgrading to newer versions with additional features, at the end user's discretion. No forced OS patches or updates are required, nor is remote connectivity and attestation–in sharp contrast to Windows 10 and iOS authentication, upgrade, and patching cycles. Redwall Mobile – clearly superior!

Redwall Mobile – Clearly Superior!	Redwall Mobile	Win 10	iOS
Open Source Commercially supported OS	✓		
Reduced OS footprint and patch file size	✓		
Supports multi-level security profiles on one device	✓		
Support cryptographic and temporal isolation of user roles	✓		
Reduced frequency and volume of vulnerabilities	✓		
Reduced frequency of required patching	✓		
Reduced frequency of remote over the air authentication	✓		
OS license activation for connected and standalone devices without over the air authentication	✓		

Backed by Military Grade Security: Redwall Mobile® security is the only end-device cybersecurity solution designed specifically to protect, separate, and control classified information on mobile devices. Telework, Healthcare and Enterprise risk management, compliance and security requirements are no less stringent yet end use device security is largely reliant upon device operating system security, with its endless exploit-pay-patch cycles. *Why accept anything less that real security-and OS stability delivered when financial futures and lives are at risk?*

Redwall Technologies is the sole provider of Redwall Mobile®—demonstrably the premiere mobile device security solution featuring Secure Persona® multi-user experience providing unparalleled separation between all data and apps of each user (or user role).

About Redwall

Our mission is to provide high-quality and highly effective cyber-security expertise, software engineering, and leading-edge technology to assist public sector agencies and private sector companies in preventing and responding to emerging threats against their mobile applications and connected infrastructure. We accomplish this by applying our technology to mobile devices and delivering capability through existing distribution channels to enable rapid adoption and sustainment while providing a distinct competitive advantage to our partners and device platform providers.

Contact:

John Rosenstengel
President and CEO
Redwall Technologies, LLC

John.Rosenstengel@redwall.us
www.redwall.us