REDWALL
TECHNOLOGIES LLC

Why was Redwall Technologies formed?

While working with the government to determine vulnerability of mobile devices, Redwall's Chief Architect found that the existing security approaches were easily hacked. A new approach was clearly needed. So, Redwall Mobile was envisioned as a new security paradigm developed from the perspective of a professional hacker.

Everyone has a mobile security product these days. Why is Redwall Mobile in a class by itself?

Every competitor has created their solution based on the flawed architectures of their failed predecessors.

By way of example, Samsung's security product, KNOX, relies on “hardware-level” security and the NSA-backed Security Enhancements for Android (SE Android) to provide a “best in class” container solution. In no time, Towelroot was posted on the internet, allowing anyone to hack a Samsung secure phone and get whatever data they wanted. Redwall Mobile running on the same Samsung phone was completely invulnerable.

The fact that Silent Circle's Black Phone was hacked within minutes shows that no amount of marketing buzz can provide actual protection. Similar hacker toolkits exist for several "secure" mobile devices, including those designed specifically to support national security users (Good Technologies, MobileIron, etc.).

Redwall Mobile's patent pending architecture and security enhancements provide a demonstrably clear level of security that no competitor can touch.

Additionally, Redwall effectively turns one phone into any number of separate phones, each with the data and apps needed to match whatever role the user takes on throughout the day. Basically, sometimes you are a private person and sometimes you are an employee. Redwall keeps these completely separated, such that, if a Redwall phone is ever successfully hacked while in personal mode, all of the company data is 100% separated and secure. The same separation can be used to keep your financial data completely protected while you are downloading a game app that may contain malware.

Mobile

With more smartphones and tablets on the planet than people, attackers are turning their attention towards mobiles with frightening speed and success. The mobile security market is already over $1B, and expected to more than quadruple in the next four years. Redwall is partnering with carriers, device manufacturers, and integrators to address smartphone and tablet security in industries like corporate enterprises, financial services, medical, and defense. Through highly successful demonstrations, proof-of-concept deployments, and SBIR contracts, Redwall is already quickly gaining ground in the US and FVEY mobile defense and intelligence markets.

Public safety communications

Public safety networks are undergoing historic transformations, with the public safety LTE device market expected to reach $7B annually in this decade. Efforts such as FirstNet may expand this market even further by building dedicated public safety networks . By working with Motorola Solutions and other top providers and manufacturers in this space, Redwall is poised to become the de facto security base which public safety devices rely on for security.

Unmanned vehicles

UAVs and drones represent a burgeoning market where the security implications are just beginning to come to light. Redwall is poised to work with defense and commercial partners to help define and implement the security of such devices and vehicles, capturing part of a $5B market.

Critical National Infrastructure (CNI)

One of the most significant threats to national security today is the lack of security in critical national infrastructure such as power distribution, traffic controls, etc. The number of “nodes” (small computers similar to those in a cell phone) involved in CNI is enormous. Because this will be a huge future market, Redwall has filed a patent specifically for this market. As the nation gains resolve to fix our CNI, Redwall will identify partners to address this $10B market.

Internet of Things (IoT)

The IoT market is forecast to grow to $7.1 trillion in this decade. As IoT deices, wearables, and sensors permeate our homes and streets, security and privacy of the kind Redwall provides will be tantamount to marketplace acceptance of these devices. Redwall is partnering with device manufactures and network providers in order to establish ourselves as a key player in this market.

How does Redwall stack up against some of the competitive approaches like specialized phones or containers?

Redwall is a new approach to mobile security, and as such , it's difficult to easily place the Redwall Mobile product into a convenient box or existing category. In comparing Redwall's benefits and technology to existing device security solutions, many would-be competitors are more appropriately viewed as complimentary technology, with Redwall enabling their underlying claims or enhancing their capabilities. Despite this potential synergy, there exists very significant competition for mind-share and perceived benefits in a market feverish for anything and everything to solve the immediate GRC issues and address both real and perceived mobile threats. This section summarizes the different approaches products have taken to date, and illustrates the key differences between them and Redwall

Application-level defenses

The key weaknesses of these defenses are that they are completely moot if the platform is compromised in any way, and that as apps, they are limited in their influence and access to the device. Their key advantage over Redwall is that they are available on app stores like iTunes and Google Play. Actual usage, however, is often extremely complex, requiring IT-level device knowledge, training, enterprise support, and cooperation with app authors to port their apps to the proprietary API of the various solutions. Examples of these technologies include:

- Containers/sandboxes (e.g. Good, MobileIron)
- Anti-virus/malware scanners (e.g. McAfee, Bitdefender)
- Security apps (e.g. AirWatch, Lookout)
- MDM/MAM (e.g. Symantec Mobile Mgmt Suite, Google Divide)

Since Redwall Mobile secures the device without the need for these applications to change in any way, all of these apps will run even better on a Redwall Mobile device. With Redwall Mobile protecting the underlying system, these apps can perform their functions with much higher assurance.

OS-level defenses

Like Redwall, these technologies require integration with the operating system, albeit much deeper than Redwall's. The key weaknesses are the engineering overhead and NRE that must go into each device, and their need for vendor-proprietary source code. Many vendors, especially device manufacturers, are unwilling or, due to licensing constraints, unable to share the source code with third parties like virtualization vendors. Furthermore, once integrated, maintaining across the vendors becomes problematic and complex, often requiring significant NRE and calendar time to keep the technology up to date. In the fast-paced mobile world, hardware may be obsolete by the time such an effort is complete. And while these solutions lack some of Redwall Mobile's core features, and do not represent feature/benefit or technology competitors, they are well-funded and well marketed. Examples of these technologies include:

- Hypervisors and virtualization (e.g. VMWare, Samsung Knox)
- Hardened OS (e.g. Invincea, Optio)

Most hardened OS solutions are fully compatible with Redwall. For example, Redwall Mobile has integrated with SE Android. Although SE Android polices may be more challenging to

create, they are completely compatible with and run well on a Redwall Mobile enabled device (as demonstrated by the recent MSI/Redwall integration).

Hardware-level defenses

These technologies offer either complete devices, or hardware peripherals that are added to existing devices. They offer clear partnership opportunities for Redwall more so than competition, and in fact Redwall is in the early stages of integrating some of these products. Examples of these technologies include:

- Peripherals (e.g. MSI CRYPTR micro, Spyrus Rosetta)
- Full device (e.g. Silent Circle Blackphone, Boeing Black)

Full devices, including Samsung devices using Knox, lack Redwall Mobile's n-persona, full integrity checking, and easily management policies that include feature-level ACLs beyond Android's own capabilities, but they are heavily marketed as complete solutions. As such, a small number of them represent serious competitors for mindshare in the mobile security space, but do not represent true alternatives or technical competition.

Remote access

Remote access technologies are a re-incarnation of remote desktop technologies, but for mobile devices. Their key weaknesses are their requirement for constant, reliable high-bandwidth connectivity, the need for very significant infrastructure, and the fact that they can expose authentication information. Like other app-based solutions, their advantage over Redwall is their ability to be installed from an app store on an arbitrary device. Examples of these technologies include:

- Virtualization (e.g. VMWare, Citrix)
- Cloud-based

Since very little data is stored on the device, the market is starting to embrace these technologies to assist with GRC issues or to relegate those issues to cloud vendors. While the benefit from the combined buzz of "mobile" and "cloud" keywords, there is not likely to be significant overlap with Redwall Mobile target customers.

What are some key Redwall Mobile features the competition cannot match?

We have seen that Redwall Mobile is compatible with a wide variety of devices and technologies, which in and of itself sets it apart from narrower solutions. There are features, however, that even combinations of all available technologies cannot match without Redwall Mobile.

- Behavioral vs taxonomic analysis
  Rather than looking for specific threats or porting specific parts of a system into a trusted container or cell, Redwall Mobile uses policies to define acceptable behavior, and treats any aberrations as a policy violation. And since Redwall Mobile handles violations with graduated responses based on the mode or persona, there is no need to lock down a device to the point where it becomes unusable. There are also no pattern definition files or threat definitions to maintain.

- Policy-driven security model enforced from TEE in secure memory
  Redwall Mobile creates a secure memory region wherein it executes a trusted monitor, called the trusted execution environment or TEE. Competing solutions must take over any trusted code, which adds cost when apps need to be ported to vendor-specific APIs, and grows the trusted computing base to rival the complexity of the untrusted base, making the division of little use. Redwall Mobile's TEE can monitor and enforce separation among different apps with zero changes to those apps.

- Temporal isolation in addition to cryptographic and other methods
  Sandboxing or virtualization cannot provide this level of isolation en in theory, let alone in practice. Those solutions suffer from the shortcoming that trusted and untrusted data co-exist in memory, making them highly vulnerable. Dedicated devices like the Blackphone are even worse, requiring users to cary multiple devices for different roles or different levels of security. Redwall Mobile consolidates all the features of a locked-down secure device with an off-the-shelf device suitable for personal use, reducing cost and complexity, not to mention and weight burden and power usage.

- Biomorphics
  Redwall Mobile adds diversity between devices and processes while the device is running. This can reduce or more likely eliminate the ability of an attack to propagate from one device to another, as attackers must hit a moving target.

- Device support
  Redwall Mobile moves easily to new devices without the re-engineering efforts involved in porting virtualization or hypervisor solutions. And it does so with zero changes to existing apps or their frameworks, including both custom apps and Google Play Store apps.

- No hardware requirements (e.g. TrustZone not required)
  Redwall is agile, not tied to a single version of a single device or ODM, and we are eager to meet any custom requirements.

REDWALL

HTTP://WWW.REDWALL.US