BlackBerry

White Paper

How BlackBerry Brings Android Security To Your Enterprise

When Android first made its way into the consumer market, no one could have predicted the impact it would have. Android was an operating system developed with a simple idea at its core: Google's founders wanted smarter mobile devices that better served their users. Today, that simple idea has helped make Android the most popular mobile OS on the market, with a global share of 66%.

Android's popularity can largely be traced to its sheer diversity. Almost from the beginning, it has been an open platform, and there are countless devices from countless manufacturers that users can choose between. Therein lies the problem – due to its widespread popularity, Android finds itself targeted by criminals and malware with greater frequency than any other operating system. This means that although the OS is not inherently vulnerable, any vulnerabilities that do exist tend to be exploited if they aren't patched in a timely fashion. Moreover, because so many different vendors count themselves as players in the Android space, it's inevitable that some will lag behind with security patching. In the meantime, their devices will remain vulnerable, even as they're being used to handle sensitive business data.

"Nearly every organization supporting smartphones and tablets must have a strategy to support Android devices, despite some of the security challenges," reads a recent white paper by J. Gold Associates. "As we moved to a more mobile world over the past several years, the number of potential attack points increased dramatically, and many of them consisted of user-selected and often unsecured devices as a byproduct of BYOD," the paper continues. "The ability to secure data and prevent corporate breaches consistently ranks among the top issues both IT and general management struggle with on a regular basis. A February 2016 Ponemon Institute survey shows that 67% of companies are either certain or very likely to have had a security breach due to a mobile device."

Slow security patching is far from the only threat facing Android within the enterprise. To grant themselves additional freedoms and run certain applications, many users choose to root their devices, stripping away core security functionality in the interest of personalization. And though measures such as Samsung KNOX and Android for Work exist to separate corporate and private data, these software solutions can be fooled by a savvy enough user.

What is Rooting?

"Rooting" refers to the process by which a mobile user alters or replaces system applications or settings which are ordinarily inaccessible to them, sometimes even replacing the operating system entirely.

That's where BlackBerry comes in. Security has always been in our blood, and we've always made it our priority to protect both our clients and their data. That's why we've made our own foray into the Android device market, bringing our full security expertise to bear.

Commitment to and Leadership in Adaptive Security

BlackBerry has long set the bar for mobile security, and our approach to Android is no different. From our dedication to ongoing security patches to our superior EMM portfolio, we pride ourselves on our leadership in adaptive security.

Analyst's View

"The lack of quickly implementing updates to the latest version of the OS is often a key factor in enabling known exploits…Some manufacturers can take 60-180 days to upgrade to a new OS version after Google has made it available…This is a major security issue."*

* J.Gold & Associates

Other mobile device vendors can take weeks or months to release patches. Along with Google's Nexus devices, BlackBerry has a record of being the quickest device manufacturer on the market to deliver security updates. Do you really want to run the risk of losing critical data to an exploit such as Stagefright 2.0?

With BlackBerry, that's not something you need to worry about – we're one of the only mobility vendors with a clear commitment to security. When Google releases its security bulletin each month, we send out a Security Maintenance Release to address any flagged vulnerabilities. We also provide as-needed hotfixes for critical vulnerabilities outside those maintenance windows, such as our recent industry-leading fixes for the Quadrooter vulnerability.

Dedicated Security Response Teams

Providing world-class security has always been a significant area of focus, which is why we have several teams dedicated to furthering our leadership:

The **BlackBerry Security Incident Response Team (BBSIRT)** ensures that public and private reports of vulnerabilities are quickly received, analyzed, and mitigated to protect our clients. This team collaborates with customers, partners, vendors, governments, academics, and security researchers to monitor and address the Android threat landscape 365 days a year. This allows us to deliver a unique level of security to our customers, providing them with the guidance and tools they need to keep their businesses safe.

The **Security Research Group** is a global team of ethical hackers whose mandate is to identify security issues in the BlackBerry product portfolio and work closely with development teams to resolve them. They also conduct active research into advanced security threats and defensive technologies.

Consumer-Ready, Enterprise-Friendly

Security works best if it meshes with what the employees want – it's most effective when it's not inconvenient to connect to a security solution or use a device. Luckily, we offer three highly attractive options for business users who want to experience Android through BlackBerry; the PRIV, released in 2015, and the brand-new DTEK50 and DTEK60, ultra-sleek all-touch devices.

DTEK50 / DTEK60

DTEK50 and DTEK60 combine everything you've come to expect from BlackBerry with all the apps and great experiences of Android. They feature fantastic cameras and brilliant screens, plus the best integrated messaging experience on a smartphone. Added security lets you know when you could be at risk from hackers, so you can easily take action to protect the private details of your life.

Available at affordable, business-friendly price points, DTEK50 and DTEK60 offer stellar hardware specs, excellent battery life, and a host of productivity-oriented tools like the BlackBerry Convenience Key. Located on the right side of the phone, a single press of this key gives the user quick access to their most-used application or task. Other productivity-enabling features include:

- Gesture Controls allow for greater ease of navigation, and can be customized based on user preferences.
- Device Search and Instant Actions allow a user to execute commands through the search bar, without having to seek out or open an application.
- The BlackBerry Hub, now available as a standalone subscription service on Android, consolidates all of a user's communications into a single place, where they can then be easily organized. This includes phone calls, email, social media notifications, scheduling alerts, and text messages.
- BlackBerry's Intelligent Keyboard learns how a user types, providing word suggestions that increase typing speed and accuracy in up to three languages of their choice.

Device Security Built in from The Start

Improving the integrity of the Android OS is a cornerstone of our approach to securing Android. To that end, we've incorporated many improvements to Android's core security, locking down device capabilities that could give attackers the opportunity to compromise a device – and in so doing, your organization. From the Hardware Root of Trust to our enhanced bootloader, everything about PRIV, DTEK50 and DTEK60 is architected to protect your data, both corporate and personal.

The Hardware Root of Trust

Analyst's View

"No device should be able to boot and load its OS without first determining with certainty that the OS is authentic and not somehow modified….Not all available chips powering current devices have the ability to enable security hardware assist and thereby secure booting to verify that the OS has not been tampered with."*

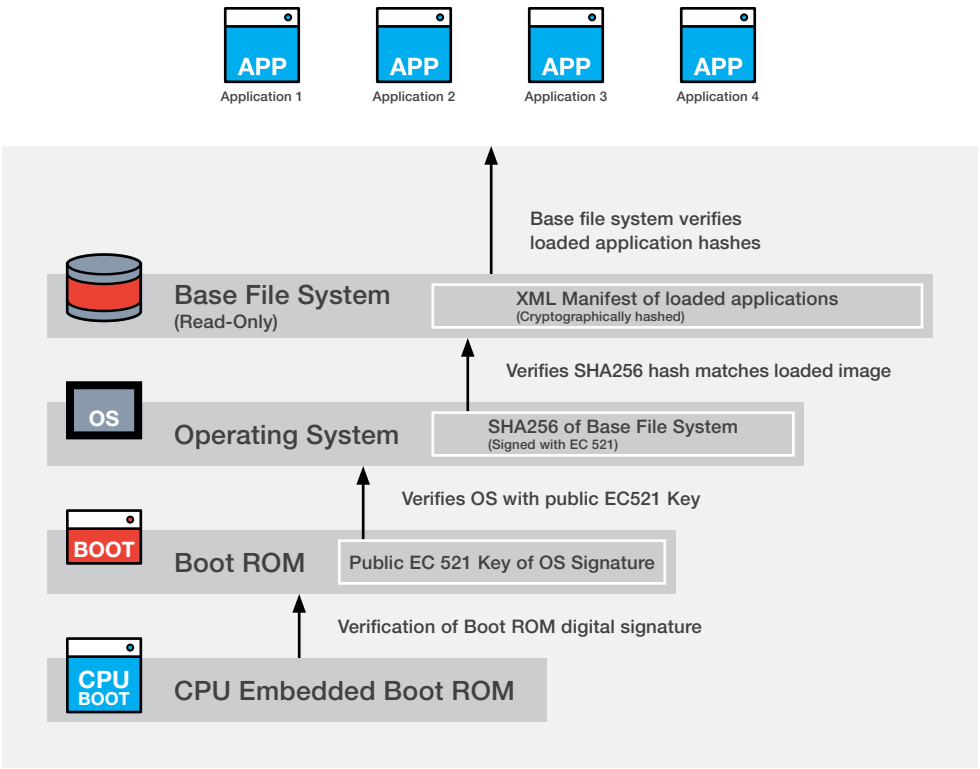
* J.Gold & Associates

Rather than layering on defenses after production, we've built security into DTEK50, DTEK60 and PRIV from the start. Our manufacturing process makes use of the Hardware Root of Trust, a proprietary technique that adds security keys to the device processor as it's built. These keys are then used to track, verify, and provision each device, ensuring their authenticity and integrity are guaranteed – along with the safety of the data they contain.

In addition to serving as the foundation of our other security measures, the Hardware Root of Trust acts as a safeguard against counterfeiting, which could expose your organization to a wide range of malware.

BlackBerry's Secure Bootloader

Built upon the Hardware Root of Trust, the secure boot chain in BlackBerry's Android makes use of multiple verification stages to ensure that the device has not been tampered with. Each stage of the secure boot chain must verify that the next component is intact before proceeding. This further protects DTEK50, DTEK60 and PRIV against tampering and ensures that rooted devices – and the security risks they represent – are not present in your organization.



BlackBerry Integrity Detection

Analyst's View

"There are many easy ways to root kit an Android device. Once done, it's impossible to look to Android and Google to provide currently verified safety…Root kitting remains one of the single biggest threats to Android device security."*

* J.Gold & Associates

BlackBerry Integrity Detection continuously monitors for events or configuration changes that may indicate a device's security is compromised. It integrates readily with EMM and third-party monitoring solutions, so that when a suspicious modification is detected it's easy to generate integrity reports and automated responses to compromised devices.

Android OS Hardening

Analyst's View

"Google is addressing the needs of many business Android users by offering an enterprise-class upgrade to Android known as Android for Work. While it does offer a significant enhancement to consumer-grade Android by providing segmented workspaces and profiles to keep corporate and personal apps and data separate, it does not completely solve the challenges of using Android in the workplace." *

* J.Gold & Associates

BlackBerry has strengthened Google's own Android security enhancements (Android for Work, user profile controls, etc.) with several of our own. For example, improved Address Space Layout randomization scrambles the operating system's code to make it harder for attackers to locate vulnerabilities. We've also hardened the Android kernel, removing unnecessary functionality which would otherwise render the operating system vulnerable.

FIPS 140-2 Compliant Full Disk Encryption

BlackBerry Powered Android devices protect their data with full-disk encryption, which is turned on automatically and cannot be disabled. BlackBerry further enhances the protections provided by this encryption through the use of a FIPS 140-2 compliant kernel. This is the same sort of encryption employed by the United States government, and allows our devices to be readily used in regulated industries; encryption keys are cordoned off within BlackBerry Secure Compound and fully write-protected. This means that even if a device is lost or stolen, your information is safe.

Control, Convenience, and Visibility

Security often seems complicated, obtuse, and troublesome for both the administrator and the end user – but it doesn't need to be. BlackBerry's Android is designed to give the end user visibility and control of their data. We make your corporate devices more secure by making security both painless and convenient.

Password Keeper

BlackBerry Password Keeper allows you to store passwords, usernames, notes, and security questions in a single location, all secured by a master password. Password strength is measured based on a proprietary algorithm, and credentials can easily be imported from other applications; this ensures that in organizations where users have to keep track of multiple logins, they can do so with ease. If someone attempts to crack a device's master password, Password Keeper is designed to erase its data after ten failed sign-in attempts. So users can spend less time sorting out authentication and more time getting things done.

DTEK by BlackBerry

Analyst's View

"Monitoring of activity that is considered a security risk, based on policies that can be set, is an important component of securing any mobile device." *

* J.Gold & Associates

A tool released exclusively for PRIV, DTEK50 and DTEK60, DTEK by BlackBerry automatically monitors a device's operating systems and applications, notifying the user when an app puts their privacy at risk. It assigns a security rating for each device based on a number of different criteria such as password strength. Alongside Android Marshmallow, it allows the user to control everything about their smartphone's privacy and security, while also giving IT an idea of which applications could prove problematic from a business standpoint.

Other Security Features

BlackBerry's Android offers a number of other diverse security options, including:

- Media Card Protection: PRIV, DTEK50 and DTEK60 control who can access a device's media card, protecting the information stored there and further separating work and personal profiles.
- Remote Device Management: Lost or stolen devices can be located through GPS positioning, and they can also be remotely locked and wiped.
- Application Sandboxing: On BlackBerry Powered by Android, applications are isolated to their own area of the device, and sandboxed off from one another to minimize the damage that might be caused by a rogue app.
- Data-in-transit protection: Information traveling over Wi-Fi, VPN, Bluetooth, and NFC connections is fully encrypted.

DTEK50 & PRIV: The Perfect Choice for Your Business Needs

From slow security patches to issues related to rooted devices, Android security is an ongoing issue within enterprise. Although many smartphone manufacturers claim to provide some degree of protection, not all devices are equally secure. In this, BlackBerry stands apart as a leader – DTEK50, DTEK60 and PRIV are the world's most secure Android smartphones, and both are a perfect choice for your business needs, whatever those may be.

To learn more about BlackBerry smartphones, visit **www.BlackBerry.com/smartphones**
You can also visit **http://web.BlackBerry.com/enterprise/enterprise-mobility-management.html** to learn more about our enterprise software.

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points – from cars to smartphones – making the mobile-first enterprise vision a reality.

Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ. For more information, visit **www.BlackBerry.com**.

Global Headquarters
+1 408 212 7500 (main)
+1 866 7 BE GOOD (sales)

EMEA Headquarters
+44 (0) 20 7845 5300

Asia / Pacific Headquarters
+1 300 BE GOOD