



BlackBerry Enterprise Server: Defying the Threat of Mobile Malware

BlackBerry® Enterprise Server has built-in advanced security features to help protect your important data and IT infrastructure while communicating on the go



Malware-Fighting Features That Help You Meet Your Organization's Growing Mobile Data Requirements



Protecting Your Organization From Malware

Viruses, trojans, worms, and spyware (collectively referred to as “malware”) can seriously compromise enterprise data and create difficult IT challenges. With the BlackBerry® Enterprise Solution, Research In Motion (RIM) has taken significant measures to protect the deployment of applications and information to BlackBerry smartphones in a way that helps maintain your organization’s security policies.

Malware Containment.

In the PC world, arming an infrastructure against malware consists of two fundamental strategies: detection and containment. Detecting malware often requires a frequently updated local database, or a constant connection to an online database. While desktop computers can usually accommodate anti-virus software, wireless devices frequently cannot due to the limitations of their memory, processing power, and battery life.

The BlackBerry Enterprise Solution was designed with built-in security features that allow users access to the critical applications they need to do their job, while helping to contain malicious programs that could impact business continuity or compromise sensitive data.

BlackBerry Enterprise Solution Application Control

With over 350 IT policy controls, the BlackBerry® Enterprise Server is designed to allow IT administrators to restrict user downloads of third-party applications, as well as help maintain control over resources and data that are accessible through an application. And because administrators have the ability to specify limitations on a per application basis, they can grant elevated permissions to trusted applications.

The BlackBerry Enterprise Server provides control over many aspects of the platform, allowing administrators great command over applications, configuration and transport. The administrator can manage options centrally and update most BlackBerry smartphones virtually instantly and wirelessly.

Controlling third party application functionality on the BlackBerry smartphone

Using IT policies, the BlackBerry Enterprise Server is designed to allow IT administrators to permit or prevent the installation of third-party applications on the BlackBerry smartphone. Administrators can also restrict access to features of the BlackBerry smartphone, such as

- the phone, Bluetooth® enabled devices, USB connections, email, organizer data, as well as other data and applications
- the types of connections that a third-party application running on the BlackBerry smartphone can establish (e.g., local connections, internal connections, and external connections)

Using code signing to limit access to BlackBerry smartphone application data

While RIM does not inspect or verify third-party applications that run on BlackBerry smartphones, it does control the use of BlackBerry application programming interfaces (APIs)—sensitive packages, classes or methods—to prevent unauthorized applications from accessing data on the BlackBerry smartphone. Each third-party application requires authorization to run on the BlackBerry smartphone. Unless digitally signed by the RIM signing authority system, MIDlets cannot access the memory of other applications, or the persistent data of other MIDlets.

Before a third-party application can use the BlackBerry APIs on the BlackBerry smartphone, the RIM signing authority system must first authorize and authenticate the application code using public key cryptography.

Helping you remain protected

RIM’s proactive approach to malware protection is designed to protect the BlackBerry smartphone from damage to the hardware, applications, data, or corporate network.

RIM has also taken a proactive course of action on potential vulnerability issues. RIM’s security research and response team works with our engineering and software development teams, as well as external groups to analyze areas of possible attack on BlackBerry products. In cases where potential vulnerabilities have been identified, RIM’s security research and response team has a mandate to act quickly to determine the scope of the issue, disseminate the information to customers with possible workarounds, and develop resolutions in a timely manner. They have also developed relations with external security advisory groups to collaborate on proactive security measures.

For More Information

To obtain additional information about BlackBerry Enterprise Solution security, visit www.blackberry.com/security

To Purchase

You can purchase the BlackBerry Enterprise Solution by:

Telephone: 1-877-255-2377

Online: www.blackberry.com/go/purchase

Or by contacting your wireless service provider