Secure Messaging for Mobile Device Users

VERDASYS

The business trend towards IT "consumerization" is being driven by cost savings and employee pressure to allow the use of consumer-based mobile devices to access corporate email and attachments. Businesses are quickly adapting, but are justifiably concerned about the potential for consumerization to put sensitive data at greater risk on employee-owned devices. As smartphones and tablets are allowed to access and store corporate information, a mobile data protection model is needed to overlay mobile device management (MDM) solutions to ensure sensitive data remains secure and contained when exposed to mobile environments.

Digital Guardian's technology platform for Enterprise Information Protection (EIP) extends its data-centric security model for hosts and virtual environments to include monitoring and controlling the movement of sensitive information through the Blackberry Enterprise Server (BES) and Exchange ActiveSync (EAS).

Digital Guardian's EIP Mobile solution is capable of controlling emails and attachments from being sent directly from Blackberry or ActiveSync-compatible devices. In addition, Digital Guardian forensically logs all email events generated by supported mobile users, and can send alerts to security administrators when a policy rule is triggered.

Scalable Security for Mobile Data

A specialized Digital Guardian server agent residing on the BES or ActiveSync server monitors every email event, and enforces the user's policy for accessing and sending sensitive data without the need for them to determine if an action is compliant. Digital Guardian's EIP Mobile solution provides a seamless end user experience that is transparent to authorized uses of data, while providing business owners and security administrators granular insight and control over the transfer of sensitive information beyond the corporate domain.

Managing Mobile Data Rules and Policies

Digital Guardian's data-centric architecture reduces the cost of enforcing mobile data policies by providing administrators a single interface from which to manage and deploy data usage rules that are applied automatically on a workstation, laptop, or supported mobile device throughout the extended enterprise.

EIP Mobile for BES and ActiveSync*

- ✓ Intelligently encrypts sensitive data sent to and from mobile devices
- ✓ Blocks unauthorized send, reply and forward events from mobile devices
- ✓ Automatically classifies and tags new emails based on sensitivity
- ✓ Encrypts new email bodies and attachments based on policy
- ✓ Securely delivers mail with password-based encryption

*** All functions occur on the BES or ActiveSync server**

Mobile Mail Encryption

Digital Guardian's EIP Mobile solution supports a wide spectrum of email security use cases on mobile devices for data movement inside and outside the corporate network using policy-based encryption controls that enforce data access controls with AES 256-bit encryption.

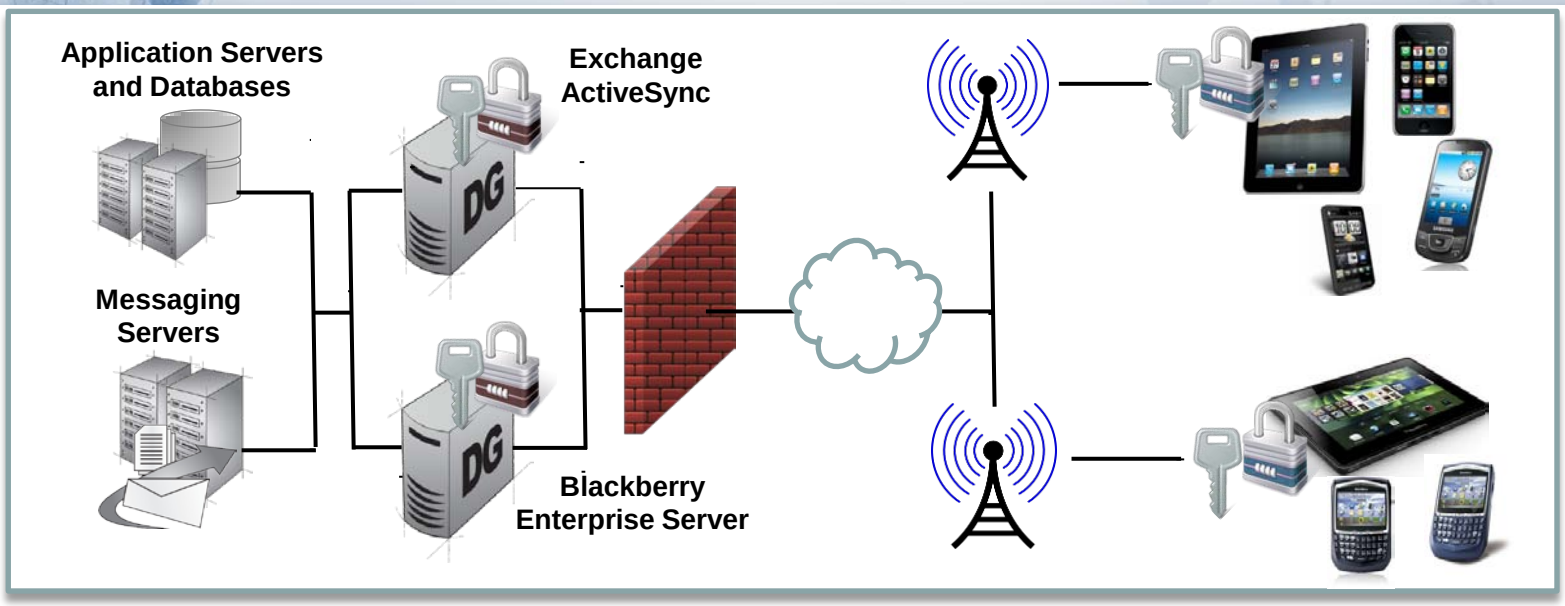
A Digital Guardian workstation or server agent can encrypt files from the moment they are created or accessed based on the their sensitivity; agents on BES and ActiveSync servers automate the encryption and decryption of messages and file attachments going to and from authorized mobile users.

Digital Guardian's mobile security model also extends beyond corporate users by supporting "portable" encryption that automatically wraps a sensitive email in a ZIP-encrypted archive as it leaves the BES or ActiveSync server. The password can be supplied by the sender or auto-generated, and accessible by the authorized recipient via a separate message automatically sent by Digital Guardian, or communicated by the sender out-of-band.

Corporate Headquarters
404 Wyman Street
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

WWW.VERDASYS.COM

EIP Mobile Secure Messaging



Rules and Policies for Secure Messaging on Mobile Devices

Digital Guardian's policies and control rules are managed and applied equally to users and data on laptops, workstations, virtual environments, mobile devices. Mobile device and user policies may be applied universally for any user connected to a specific BES and Exchange ActiveSync server(s) and/or at the user and group levels.

Silent Alert

If a mobile device user violates an email policy, an alert can be sent to security administrators and business managers without necessarily blocking the action or prompting the user.

Benefit: Silent alerting allows policy stakeholders to better understand the rate of non-compliance among mobile users – for instance, before and after policy training, or to determine if a policy rule isn't aligned with the business need – without interfering with the business process.

Email Decryption & Re-Encryption

Sensitive email content and/or attachments previously encrypted by a Digital Guardian agent can be decrypted on the BES or ActiveSync server as the message is sent to a mobile device user, and re-encrypted if it is replied to or forwarded. Digital Guardian can also auto-generate password-based encryption for secure delivery of an email outside the corporate domain.

Benefit: Digital Guardian's policy-based file encryption ensures end-to-end enterprise containment of sensitive data created or accessed from laptops, servers, removable media, email, and mobile devices.

Policy Response Notification

When a mobile user triggers a policy rule, Digital Guardian can be configured to immediately send the user an email "prompt" message to explain why a specific action was taken, or for awareness/training in response to risky or non-compliant actions.

Benefit: Providing the end user with instant policy feedback allows policy administrators to engage the user directly to increase awareness, accountability, and self-compliant behavior without increasing help desk and training costs.

User Block

Block rule policies can be based on the sensitivity of the email body and/or attachment. If a sensitive message is sent to a large distribution of users, Digital Guardian will apply the most restricted user's policy control to all recipients.

Benefit: This ensures a sensitive message is blocked if any unauthorized user is included as a recipient.

Attachment Block

A blocking policy will override any other control rule for an attachment, including an applicable encryption rule.

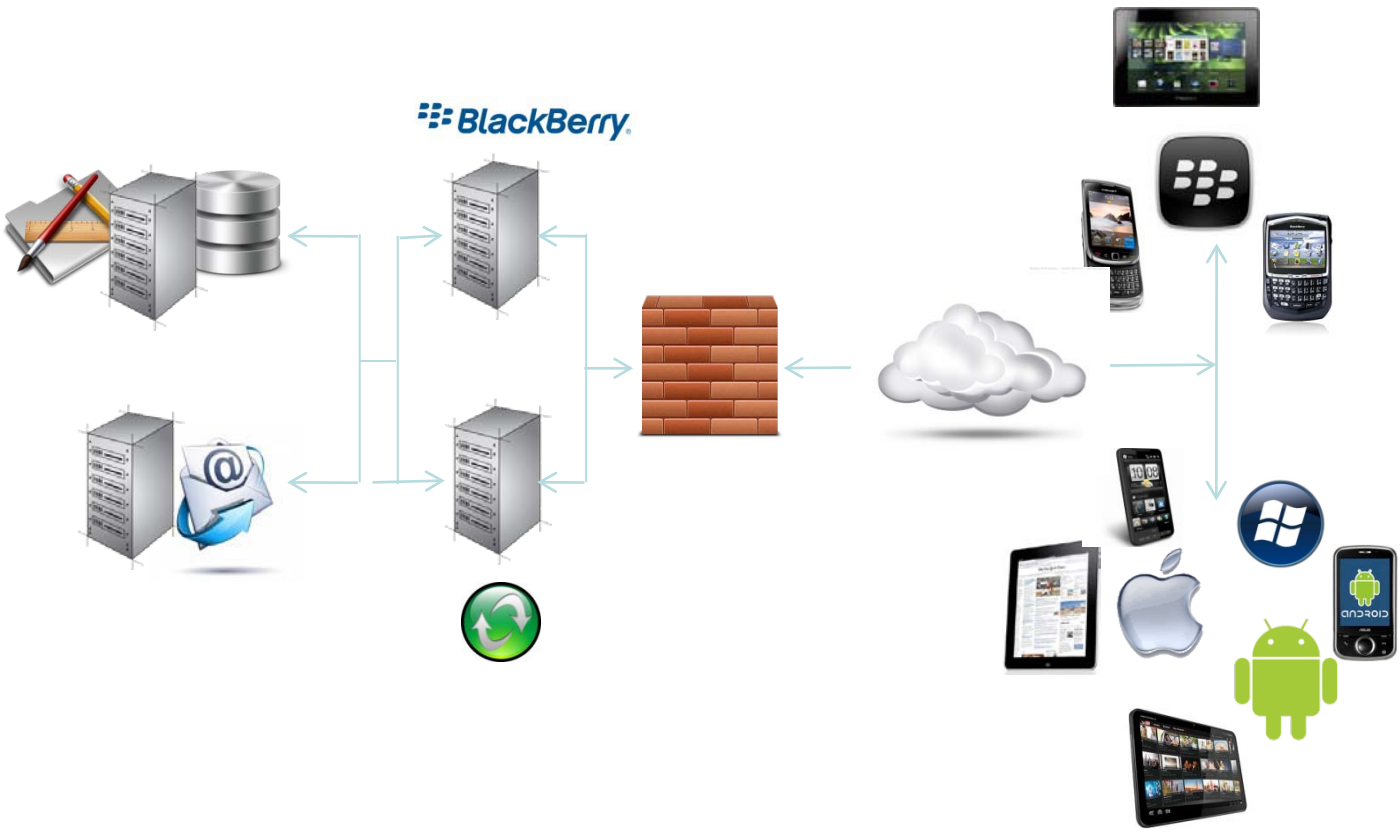
Benefit: Attachment blocking ensures that when an extreme policy condition exists, no other user privilege for the message can be invoked until the offending file is removed.

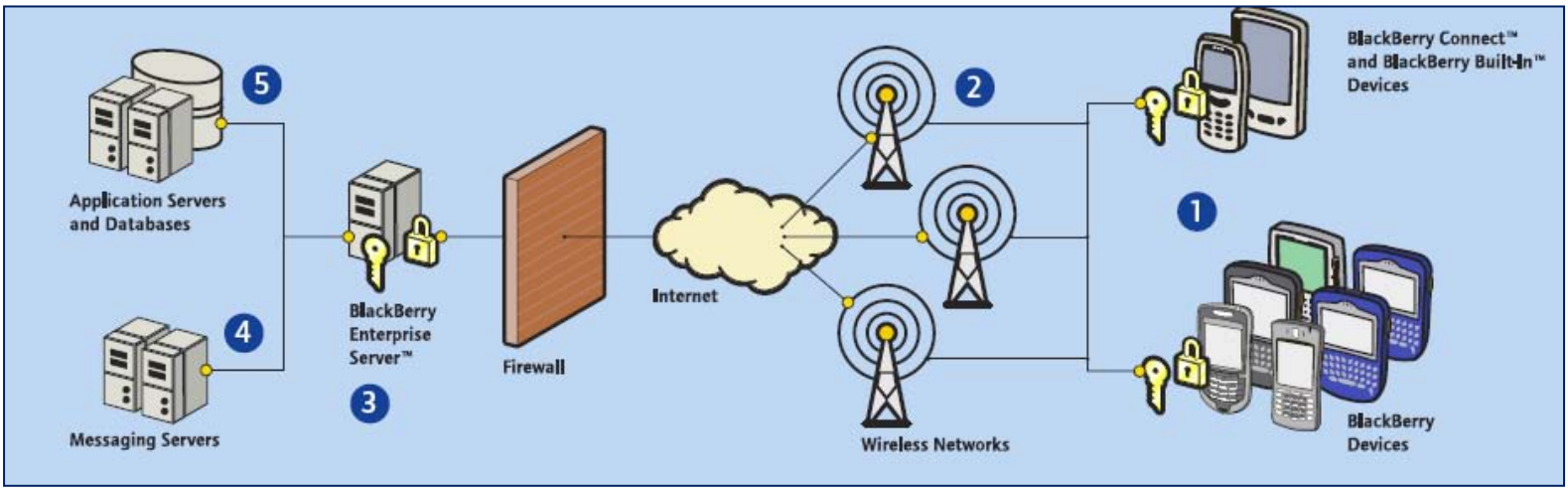
Digital Guardian BES and Exchange ActiveSync Support Requirements

Digital Guardian supports BES 4.0 and later, and Exchange 2010 and 2007. Its architecture requires a Blackberry or Exchange Active Sync server and an email server to be installed on the same physical or virtual machine.

Corporate Headquarters
404 Wyman Street
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

WWW.VERDASYS.COM


BlackBerry
ANDROID


BlackBerry Connect™
and BlackBerry Built-In™
Devices
Application Servers
and Databases
BlackBerry
Enterprise
Server™
Firewall
Internet
Messaging Servers
Wireless Networks
BlackBerry
Devices
1
2
3
4
5


DG