Whitepaper

BlackBerry Workspaces Appliance-X

Published: 2016-12-18
SWD-20161218072621822

Contents

Overview..... 4
Design requirements..... 5
Architecture..... 6
Security..... 8
Legal notice..... 9

Overview

1

Workspaces is a document-centric security platform that allows enterprise users to easily and effectively access, share and control all their important documents across the extended enterprise on any tablet, smartphone, or PC – even those beyond IT's control.

The Workspaces next-generation virtual appliance is typically installed on-premise by customers, or deployed in a cloud or managed hosting environment by managed service providers.

Feature	Description
Control	Restricts who can view, print, edit, or forward documents.
Tracking	Provides visibility into who views, forwards, edits, or prints organizational documents, where and when they use the documents, and maintains a full audit trail for compliance purposes.
Remote document wipe	Workspaces administrators can remove access to documents at any time, even after they have been downloaded.
Device optimized access	Render documents in high fidelity, and with platform-neutral controls that allow access of documents on PCs, mobile devices, or using a web browser.
Workspace	You can create a site, such as a virtual data room, to allow for document collaboration.
Quick Send	Securely share documents using Microsoft Outlook, or a web-based GUI.
File Sync	Provides real time updates of all documents accessed through the various Workspaces end user interfaces.

Design requirements

2

Based on extensive experience in deployment of virtual appliances in the field, Workspaces developed the next-generation appliance to meet several design requirements.

Table 1: Virtual appliance design requirements

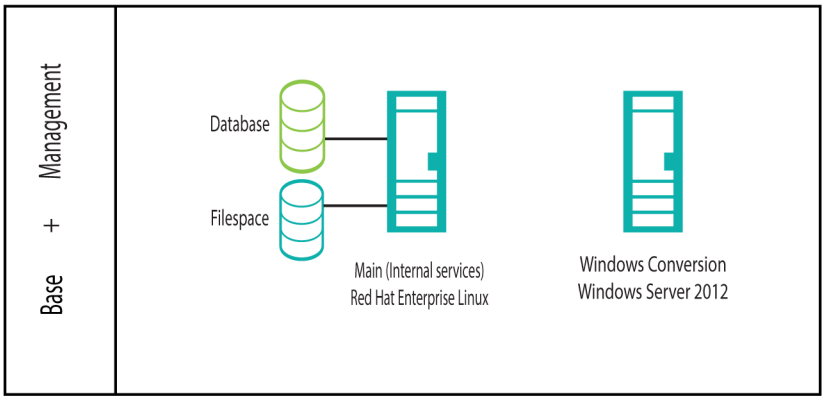
Design Requirement	Description
Simple deployment and upgrade	You can deploy the Workspaces virtual appliance in a variety of virtual environments within a matter of hours.
High-level security	The virtual appliance meets the highest security and compliance criteria, and provides rich functionality to protect documents stored and shared using the Workspaces system.
Scalability	You can deploy the Workspaces server on varying hardware resources and easily scale out.
Built-in high availability	You can configure the Workspaces virtual appliance with built-in high availability, running multiple front-end web servers and redundant software modules, thereby ensuring there are no single points of failure. If you run multiple front-end web server, an external load balancer is required.
Inegrate with enterprise systems	The Workspaces virtual appliance integrates with existing document repositories, such as SharePoint, Windows File Shares and cloud storage services. It also integrates with other key enterprise IT and security systems, such as Active Directory and identity management providers, DLP systems, log management systems, hardware security modules, and more. Workspaces supports OAuth 2.0 and SAML protocols.
Support for multiple hypervisors and stacks	You can deploy the Workspaces virtual appliance in a way that is agnostic to the underlying hypervisor, whether it is based on VMware, Hyper-V or KVM.
Single and multiple-tenant options	Customers, MSPs and OEMs can use the Workspaces next generation virtual appliance to provide secure file sharing and sync services to multiple organizational units or to multiple customers.

Architecture

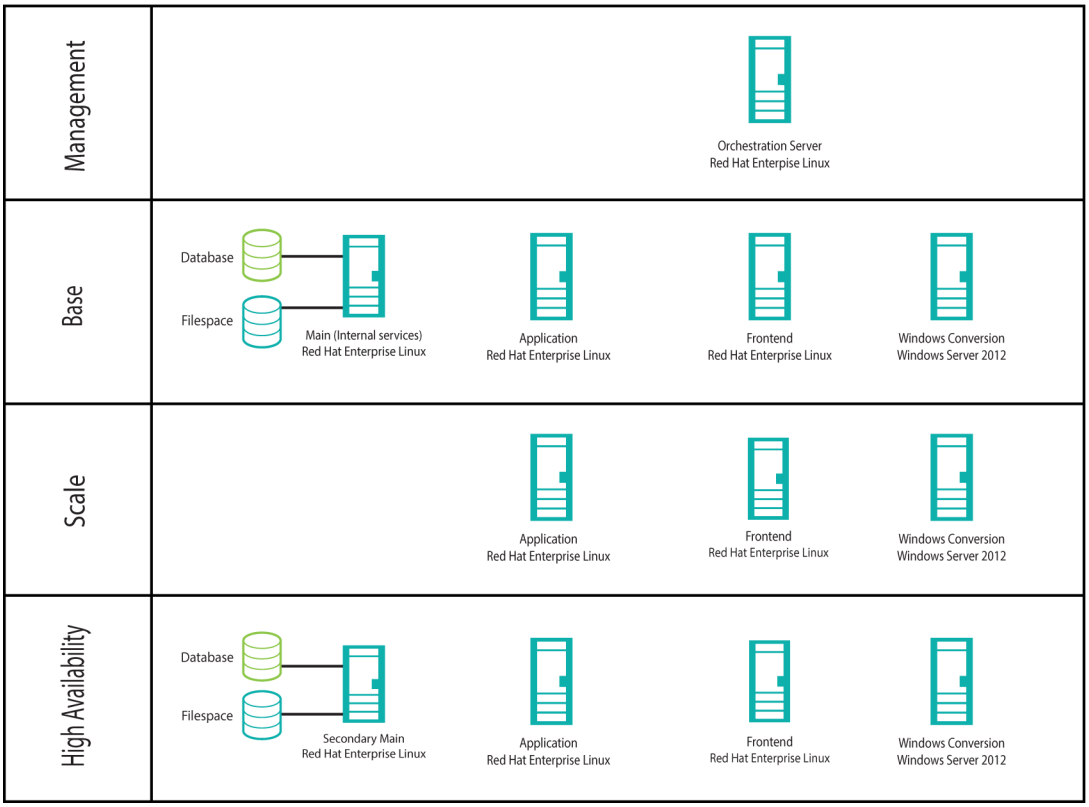
3

The Workspaces next-generation virtual appliance is a composite system consisting of multiple virtual machines. These virtual machines are responsible for the system's front-end web and management interfaces, load balancing, document converters, and other internal components.

Appliance-X (Basic)



Appliance-X (Advanced)



The Workspaces virtual appliance virtual machines run hardened Redhat Enterprise Linux and one or more instances of Windows Server.

File storage for the virtual appliance installation is a NAS, SAN, NFS, or an externally deployed Object-Storage. This component stores the encrypted customer files and the permissions database data.

The virtual appliance optionally supports a set of connectors to enterprise repositories, such as SharePoint, Windows File Shares, and various cloud storage services. Additionally, RESTful APIs provide connectivity to virtually any other enterprise systems.

You deploy and manage the next-generation virtual appliance using an orchestration server, which is based on SaltStack. SaltStack is a modern configuration management and remote execution platform that allows quick and easy deployment of a standard configuration. Alternatively, you can customieze the SaltStack orchestration component to run on different hypervisors, granularly deploying a variable number of modules on a variable number of virtual machines, as required by scalability and security policy considerations.

Security

4

The Workspaces virtual appliance is a multi-tier application with strict separation between the web application serving the users, the database that contains the system meta-data, and a secure file system that contains the encrypted documents.

Workspaces web applications employ Role Based Access Control security methodology. The software's security layer restricts users according to security permissions, with no ability to move across unauthorized boundaries. Using compartmentalized software architecture, The Workspaces server components use compartmentalized software architecture to protect against outside intrusion.

Encryption

Workspaces uses the industry-standard Advanced Encryption Standard (AES), used by businesses and governments to protect sensitive information. All user data transmissions over the Internet to and from the Workspaces servers are sent using HTTPS, and are encrypted using SSL that employs strong keys (128-256 bit, depending on the browser capabilities. 256-bit minimum can be set).

All key data fields that contain data from user input, registration, content, and policies are encrypted. The storing of the documents and meta-data in encrypted form ensures that even if intruders obtain the actual physical disks on which they reside, they will not be able to read or modify them.

Each document is stored encrypted using its own unique cryptographic key, and thereby gaining access to one key does not invalidate the security of the rest of the documents in the system. The keys are stored in secure keystore. You can connect an additional hardware security module (HSM) to the Workspaces virtual appliance, storing the system’s keys externally, with the highest level of security.

Secure document boundaries

The Workspaces web application is further separated into components that handle meta-data and components that handle users' documents. These components each reside in their own security context with a strict interface and communicate betwee themselves over SSL utilizing APIs. This architecture ensures the protection and separation of users' documents, even in the face of maliciously crafted documents.

Encrypted documents are stored in a manner that prevents association between the document itself and meta-data information such as the document’s owner, recipients, or the original file name.

Identity management integration

In addition to its built-in authentication mechanisms, Workspaces intefaces with Active Directory or any SAML or OAuth compliant identity provider to provide SSO, identity federation, and multi-factor authentication.

DLP integration

You can integrate Workspaces with DLP systems using the ICAP protocol, or you can integrate into the DLP discovery and classification to provide actionable protection to files classified as confidential by the DLP system.

Logging

You can configure the virtual appliance to report events captured by varios SIEM solutions.

Legal notice

5

©2016 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Adobe Reader, Acrobat, and Adobe PDF Maker are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Apple App Store, Mac OS, Safari, Finder, Office for Mac 2011, iPad, and iPhone are trademarks of Apple Inc. iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. Android, Google Chrome, and Google Play are trademarks of Google Inc. Microsoft Active Directory, Internet Explorer, Microsoft Excel, Microsoft Office, Microsoft Outlook, Microsoft PowerPoint, Microsoft SharePoint, Microsoft Windows, and Microsoft Word are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Mozilla Firefox is a trademark of Mozilla Foundation. "LibreOffice" is licensed under the Mozilla Public License v2.0 and is a registered trademark of its registered owners and is in actual use as a trademark in one or more countries. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY

LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada