

Secure Enterprise File Sharing and Mobile Content Management



Organizations need to share files. BlackBerry Workspaces™ makes enterprises more mobile and collaborative, while reducing the risk, complexity and cost of sharing information across and beyond your organization. Workspaces provides file-level encryption and user access controls, so you maintain control over your content even after it leaves your firewall. Workspaces also embeds digital rights management (DRM) protection in your files, so you can control what the recipient is able to do with the file once they gain access to it.

Workspaces increases file security while increasing the productivity of your organization. Users are able to view, edit, comment and collaborate on files on all major device platforms. Our deep integration with Microsoft Outlook, Microsoft Office, Office 365 and OneDrive means that your employees can continue to use their existing apps and workflows while seamlessly integrating Workspaces file secure sharing.

Workspaces allows your employees to work more effectively and safely with outside contributors. This is critical in a world where core business operations are being outsourced and vendor, partner and customer ecosystems are growing rapidly. Workspaces flexible security policy model allows you to create secure collaborative workspaces, control access and assign file permissions at the user, group and domain level. You can extend your security perimeter outside your firewall and collaborate with outside users without risk of losing control of core IP or exposing sensitive information such as personnel records or product designs.

Only Workspaces delivers the features users want and the control that IT needs.

Secure, Mobilize and Share Files



The Functionality Users Want

Share Files: Workspaces allows you to create workspaces for ongoing collaboration or simply share a link to a file via email, messaging or other means

File Synchronization: The latest version of a file is automatically synced to and available from all the user's devices.

Mobility: Access, synchronize, share and control files on all platforms: web, mobile (iOS, Android™, BlackBerry® 10), and desktop (Windows®, Mac®).

Productivity: Access, create, edit, annotate (highlight, comment, draw, erase), search (folders, files and content) and share files on any device.

Internal and External Collaboration: Share files with anyone (internal and external), anywhere, on any device, without losing visibility or control.

Large File Transfer: Share extremely large files with colleagues, partners and third parties easily.

Protect, Externalize and Track Files and File Usage

The Functionality IT Needs

File-Level Security and Enforcement: Keep sensitive files encrypted and controlled - at rest, in transit and on the device - reducing the risk of a breach or loss of intellectual property. Apply dynamic watermarks or use the spotlight feature to deter screenshots and increase accountability. Track, revoke, wipe or expire file access at any time - even after the document has left your security perimeter.

Authentication and Encryption: Enforce enterprise-level security policies including mobile passcode, jailbreak detection, remote document control, always-on AES-256 encryption (in transit, at rest, and in use) and advanced key management (optional HSM).

Easy-to-Use DRM Controls: Restrict what users and recipients can do with a file. Easily set and manage users' permissions to download, edit, copy, print and share Microsoft Office, PDF and image files.

Visibility and Reporting: Workspaces tracks all file activity so you know WHO, did WHAT, WHEN and WHERE they did it and WHAT DEVICE they used. This data is archived within Workspaces and can be used to monitor intrusions in real-time or to provide compliance reporting on demand.

Flexible Deployment Options: Choose to deploy BlackBerry Workspaces in the cloud, on-premises or as a hybrid solution.

Integration and Secure Access: Workspaces provides connectors for Microsoft content repositories (SharePoint, SharePoint Online, OneDrive for Business) and Windows File Shares (CIFS) as well as any CMIS-compliant Data Store such as OpenText, Alfresco, HP Trim, IBM FileNet and many others. This allows you to mobilize, externalize and share documents from your existing repositories securely and within your existing infrastructure. There's no need to migrate your files to the cloud or onto someone else's servers.

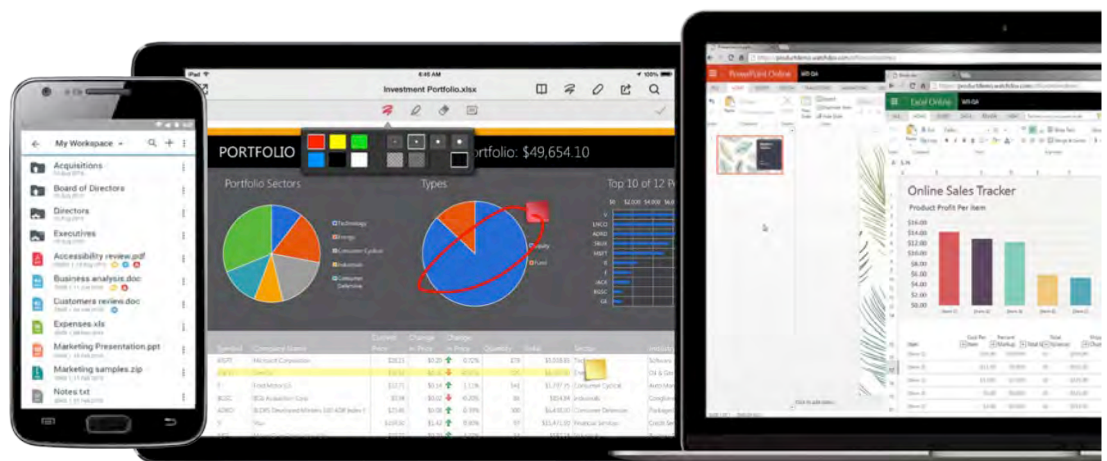
Recent Product Enhancements

There are a number of recent enhancements to Workspaces, including:

- Office Online Integration
- Inline Commenting, @mentions and alerts so that your collaboration activity stream lives alongside your documents
- Revised and Refactored SDK for easier integration with existing applications and workflows
- DocuSign Integration puts digital signatures on Workspaces files enabling new business workflows
- Mobile App Features – Be more productive on your mobile device
- File Locking – Avoid versioning conflicts while collaborating

Email Protector

BlackBerry Workspaces Email Protector is a standalone solution that automatically applies file-level encryption, user access and DRM controls to outbound email attachments, based on controllable policies such as recipient or file type. This means that system administrators can ensure that all files leaving the corporate firewall are protected by Workspaces file security. Email Protector can be purchased and deployed separately from, or alongside, Workspaces EFSS



Workspaces in the Enterprise

Virtually every business has sensitive information and documents that need to be shared. Hundreds of global companies in nearly every industry have deployed Workspaces for a wide variety of use cases:

- Replace consumer-grade file sharing systems with a secure alternative
- Securely mobilize patient health records and allow doctors to access them anywhere, from any device – all while meeting HIPAA compliance requirements
- Securely share sensitive personal information within the company and with outside vendors and agencies – contact information, credit and financial information, fingerprints, background checks, etc.
- Protect intellectual property, such as blueprints, product specs, formulas, scripts and screenplays while providing controlled access to upstream and downstream partners
- Enable executives and board members to securely view, edit and annotate highly sensitive documents on their personal iPads and other devices
- Exchange files through secure data rooms for M&A and other business transactions
- Integrate with SharePoint, Windows file shares (CIFS) or any CIMS-compliant content management system to leverage existing investments and get a single view of all content
- Extend compliance reach to mobile devices and external collaborations – for SOX, PCI, HIPAA, FINRA, GLBA, 21 CFR Part 11, ITAR, POPI and other information security regulations

Enabling Technology Transformation, Securely

BlackBerry Workspaces was built to secure information in the collaborative and mobile world of modern IT. It is designed to provide the granular, flexible and powerful security required by IT, while still delivering an elegant and intuitive user experience across web browsers, desktops, mobile devices and tablets.

Where endpoints, networks and technology infrastructure fall short in providing persistent protection, Workspaces uniquely controls and tracks all sensitive corporate assets wherever they go in the course of business.



About Workspaces

BlackBerry Workspaces secures your enterprise content wherever it travels. With Workspaces, all stakeholders can safely access, share and collaborate on even the most sensitive files, using any mobile (iOS, Android, BlackBerry) or desktop (Windows, Mac) device.

BlackBerry Workspaces also provides the flexibility to deploy as you want: cloud, on premises or a hybrid. For more information, visit www.blackberry.com/workspaces.

Combining an easy, intuitive user experience with a unique data-centric architecture (which embeds protection right in your files), BlackBerry Workspaces is designed to meet the needs of your organization, IT team and users.