BlackBerry

Data Sheet

Integration With Data Loss Prevention (DLP)

Introducing BlackBerry Workspaces™ to an enterprise workforce kick-starts secure collaboration and true mobile productivity. With powerful security controls centered on files, content that includes intellectual property or Personal Identifiable Information (PII) can now be accessed on BYOD mobile devices, or shared with external business partners without fear. The ability to control, revoke and track corporate files provides unprecedented Data Loss Prevention.

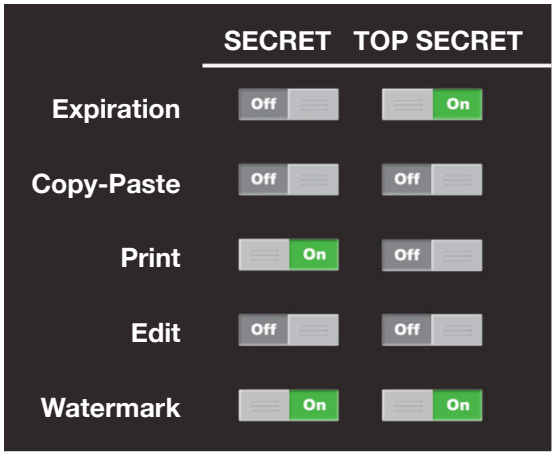
In addition to the protected distribution of sensitive files, Workspaces provides two additional pillars in the world of Data Loss Prevention.

The Solution

Leveraging Workspaces APIs

One powerful aspect of Data Loss Prevention products is the ability to discover sensitive files in sites such as file shares or Microsoft SharePoint. An enterprise organization that has deployed a DLP solution for document discovery will be able to locate sensitive documents. For example, regulated financial documents, intellectual property-rich strategy presentations or spreadsheets with customer credit card information could be flagged as sensitive and classified according to corporate policy (e.g. “Secret” and “Top Secret”).

With document classification in place, CIOs and CISOs can now take action to apply file-centric security to these sensitive documents. Using APIs from Workspaces and integrating them with the DLP solution, the classified sensitive documents can be protected and then made available for easy, secure access and sharing, even on mobile devices or with external collaborators. In addition to protection through encryption, various file controls (e.g. who has access, allow print, don’t allow copy/paste, expire access after a specific date, etc.) can be applied based on classification categories of the DLP discovery product.



For example, the following document controls can be made to each classification category, as illustrated in the graphic above.

Workspaces APIs allow the organization to programmatically use the classification requirements to enforce how sensitive information is accessed and used. Files in unsecure environments may now be migrated to a secure environment with encryption, access controls, rights management and detailed audit trails.

Prevent Distribution of Specified Sensitive Content

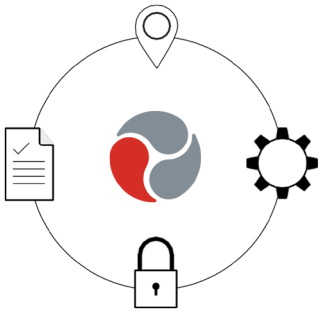
Combining Workspaces and Data Loss Prevention also provides visibility, remediation and alerts for CIOs and CISOs when files are sent and shared with Workspaces

Via an ICAP integration, Workspaces can route files to a Network DLP solution to perform content scanning, providing visibility to the contents of the files shared through Workspaces and the ability to remediate via blocking or allowing. Furthermore, the DLP solution can also be configured to generate alerts based on the policies that are triggered.

The combination of visibility, remediation and alerts through the ICAP DLP integration means that, for example, a merchant card processor can scan for files with payment card data, block them from being uploaded into Workspaces and generate alerts for audit reasons. Likewise, a sports equipment company may allow a shoe design document to be shared but still generate alerts to interested parties in the firm.

Enabling the Three Pillars of Data Loss Prevention

Workspaces has information security in its DNA and understands the needs of both the business user and the security-conscious enterprise.



By combining Workspaces with DLP solutions, an enterprise has the most comprehensive set of tools to enable secure collaboration. The powerful combination of file protection and mobile security, visibility and alerts, and discovery and remediation allows organizations to seamlessly extend the compliance regimes they've established on their internal networks with DLP to the mobile, collaborative environment of modern organizations.

PROTECT THE DISTRIBUTION OF SENSITIVE FILES

"My employees need to share files for business reasons but we need to protect the content wherever it goes."

Workspaces provides mobile security and Digital Rights Management

PREVENT DISTRIBUTION OF SPECIFIED SENSITIVE CONTENT

"I have a company policy that restricts content of certain types from being shared. I need to be compliant with company policy through visibility, remediation and alerts."

Workspaces provides ICAP-based integration with DLP solutions

DISCOVER AND PROTECT SENSITIVE CONTENT

"I have discovered files with sensitive content on PCs and file systems. I now need to encrypt that content."

Workspaces provides API integration with DLP Discovery tools

Learn more at www.blackberry.com/workspaces

About Workspaces

BlackBerry Workspaces

BlackBerry Workspaces makes your content secure wherever it travels. With Workspaces, all stakeholders can safely access, share and collaborate on even the most sensitive files, using any device — desktop (Windows®, Mac®) or mobile (iOS®, Android™, BlackBerry® 10). By combining a user experience that's as easy and intuitive as any consumer solution with a unique datacentric architecture (which embeds protection right in your files), BlackBerry Workspaces is designed to meet the needs of your organization, IT team, and users. To learn more, visit www.blackberry.com/workspaces.