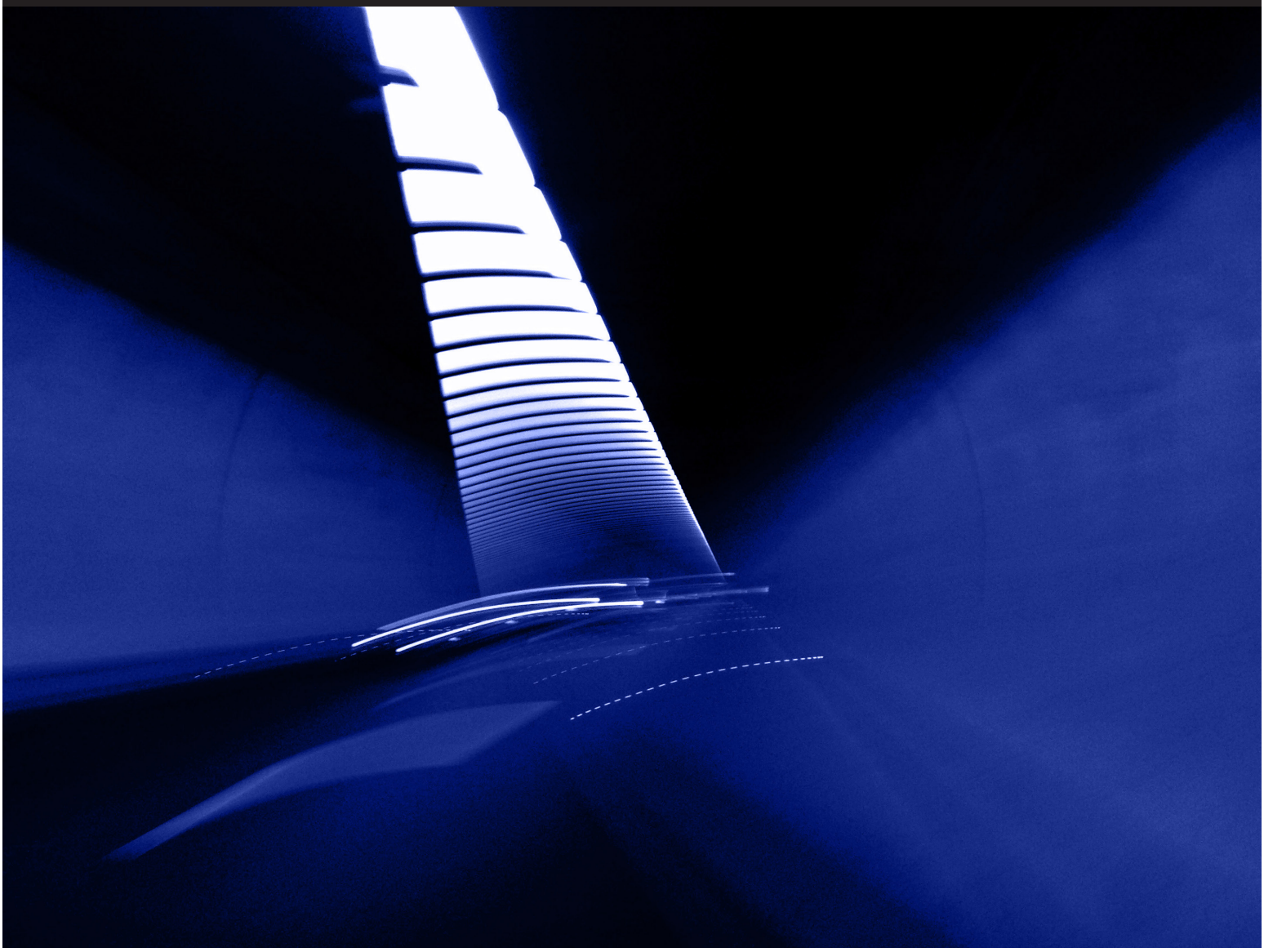
BlackBerry

White Paper



This Message Will Self-Destruct

The Power of Collaboration with an Expiration Date

The Trouble With Total Recall

A lot of technology can be occasionally ineffective, but hardly anything rivals the impotence of the "Recall Message" feature in Microsoft Outlook.

Its effectiveness is spotty when you send a message to a colleague in your own organization, but it's completely useless when you mistakenly send a message to an external recipient that you would dearly love to take back.

Email users have long lived with the fact that once a message is sent, it cannot practically be unsent. After all, the inspiration for email was snail mail, whereby a message or file sent to someone took physical form, and taking it back would involve going to their home or office and physically grabbing it.

A similar situation applies to shared files. The vast majority of shared files, even sensitive ones, have no practical means to be taken back or revoked from a recipient.

Even the United States National Security Agency (NSA) resorted to the notion of "originator control" ("OrCon" in NSA-speak), to try to control the dissemination of sensitive files. The problem with OrCon was that it operated entirely according to the honor system.

Those curious about its effectiveness need only look at the trove of documents leaked by Edward Snowden, most of which were fruitlessly stamped "OrCon" by those who wished to maintain control over how they were shared (and who dearly wished they could have taken them back from Snowden).

The Basic Power of Ephemerality

In the digital world, it doesn't have to be this way. Consider the astounding growth of Snapchat, which as of this writing has more than 100 million users, and to a lesser extent, similar apps like Wickr and Silent Circle.

Snapchat's users seized on the fact that messages, or "snaps", unlike posts on a Facebook wall or status updates, were designed for impermanence - in-the-moment social interactions that were better off disappearing.

The benefits to this kind of ephemerality were clear from the start: unless actively saved (and the sender would be alerted if the recipient took a screen capture), the messages went away. Having served their purpose, they were incapable of haunting the sender again.

The Value of Revocable File Sharing

The same should be true of most file-based collaborations, although enterprise files almost always need to last longer than a Snapchat snap.

The average enterprise user creates between 3-5 gigabytes of files, up to 80% of which will never again be accessed after they're saved to storage or a local hard drive. Much of that information is attached to emails and sent externally. But sensitive files, sent externally, using common mechanisms like email or file-sharing tools like Dropbox will not disappear unless the recipients delete them.

The cost of storing everything is also quite high. Security risks abound, as sensitive data is much harder to protect and keep track of if it does not expire in the hands of outside collaborators and is hoarded by internal users.

Information hoarding can also have staggering costs if the organization becomes involved in legal proceedings – the costs of eDiscovery rise in line with data volumes, and keeping so many files for longer than necessary results in unnecessary legal risks (see chart below).

How would file collaboration change if files did expire after a short period, by default, unless they were required to be retained for a regulatory or business reason?

e-Discovery Costs and Data Volumes

Typical file volume per employee	>	3-5 GB
Average pages per GB	>	10,000 - 75,000
eDiscovery attorney cost	>	$70 per hour
Average reviewer productivity	>	55 documents per hour
eDiscovery estimated cost	>	$380K per 1,000 employees

The Key to Expiration: Data-Centric Security

The ability to revoke access to shared files – known as information or digital rights management (IRM or DRM) – has been around in its modern form since Microsoft and Adobe implemented it a little over a decade ago. But only with the rise of online file-sharing has it become so critical.

Data-centric security embeds persistent controls in your files, so that as they are shared with internal and external parties and across multiple devices they are always protected and tracked, including post-download.

When they need to be revoked, they can disappear just like a Snap. The technical comparison, however, is not exact: while Snapchat as a mobile-only app has quite a bit of control over its data, data-centric security for files must take into account desktop, mobile and web interfaces.

Controls typically include restriction of document copy/paste, print, and sharing, and can include advanced features like dynamic watermarking and screen capture prevention. However, the key feature in this context allowing the remote wiping of data, regardless of where a file has ended up.

This is implemented, technically, by keeping files persistently encrypted and requiring users to authenticate in order to decrypt the file in memory to work with it.

If a file has been made available offline, the decryption key is typically cached for a configurable period of time, after which it expires, and the file recipient must re-authenticate online to ensure their access has not been changed or revoked. If the file has been expired or revoked, it remains in its encrypted state and as inaccessible as an old Snapchat message.

As more and more enterprises move toward collaboration methods that incorporate revocation or expiration, the enterprise file synchronization and sharing (EFSS) space is moving in that direction as well. In the final analysis, users' choices speak volumes, and the movement of consumers to Snapchat clearly presages a similar move for enterprises to EFSS tools with real expiration built in.

Security That Stays With Your Files

WatchDox® by BlackBerry® is the leading secure EFSS solution, enabling users to share, edit and control their files on every device. Only WatchDox by BlackBerry can provide the level of security organizations require—wherever files are, wherever they need to go, whoever needs to access them.

Now, stakeholders can safely access, share, sync, and collaborate on even the most sensitive files, using any device – desktop (Windows, Mac) or mobile (iOS, Android, BlackBerry 10).

Wherever the files are, and wherever they need to go, your organization stays in control. With WatchDox by BlackBerry you can establish who has permission to view, edit, print, and share each file; track who's doing what; and set content expiry dates or revoke access if you need to.

WatchDox by BlackBerry takes a unique, document-centric approach to security that allows controls and tracking to be embedded in enterprise files, with permissions that can be set at an individual user or group level.

WatchDox was positioned #1 for “High Security” in Gartner’s 2015 Critical Capabilities Report on EFSS. WatchDox also placed second in the “Mobile Workforce” and “Extranet” categories.

Gartner’s 2015 Critical Capabilities Report for Enterprise File Synchronization and Sharing

Security to Suit Every Enterprise EFSS Use Case

WatchDox by BlackBerry makes your files secure wherever they travel, through a unique data-centric architecture. With protection layered on at a file level, security stays with your content, wherever it goes – even after it's downloaded and saved locally. WatchDox by BlackBerry is the only EFSS solution that builds security into the files themselves. It's also the only solution that can address the multiple demands of enterprise environments: helping users get the job done and providing the tools IT needs to retain visibility and control of corporate information on any device, whether it belongs to an employee, a business partner, or the organization.

WatchDox by BlackBerry offers an unparalleled level of security through true digital rights management (DRM) that applies wherever files travel, and wherever they're opened. Some other solutions only apply security to files while they're open in a proprietary viewer – which doesn't give you the option to use or control files offline or within the native applications enterprise users rely on.

Control the ability to access, view, edit, copy, print, download and forward files, online and offline, on any device, even after they're downloaded from the system. Set up customized watermarks: you can splash the user's email or IP address across the document or in the viewer to deter screenshots and increase accountability. If you're giving a presentation and you're concerned about surreptitious photo-taking, you can use the spotlight feature, which blurs out the screen except where the mouse or pointer is hovering. While maintaining control has a lot to do with restrictions, WatchDox is also a productivity enabler: provide all users with access to a suite of collaboration tools, so they can manage, view, create, edit and annotate files from any device – without having to open up third-party tools unless they want to.

Encrypt files not just at rest or in transit, but in use

Files are always encrypted (via AES-256 where available, with FIPS 140-2 certification) in transit, at rest and – uniquely – in use. Truly securing a file on the desktop, for example, is not simply a matter of encrypting the file at rest or in transit. It's about controlling what can be done with the file itself – whether that's printing, editing, copying or forwarding it to someone else. And, you'll be keeping sensitive data encrypted and controlled by default, reducing the risk of a breach or loss of intellectual property.

Why Trust BlackBerry for Secure EFSS?

BlackBerry delivers proven security, trusted by thousands of companies around the world, to protect your most important assets—your privacy and your business data.

Why choose BlackBerry for secure Enterprise File Synchronization and Sharing (EFSS)?

- Leading the industry with over 70 certifications to meet your security and compliance needs*
- BlackBerry® 10 approved by NATO for classified communications up to "Restricted" level (BES10 and BlackBerry 10 smartphones were the first to receive this approval)*
- 16 of the G20 governments trust BlackBerry*
- The top 10 largest law firms trust BlackBerry*
- 5 out of 5 of the largest oil and gas businesses rely on BlackBerry*

* Current as of 10/14/2015

Learn more at www.blackberry.com/watchdox

Mobilize Your Business Simply and Securely

With Good® Secure EMM Suites, enterprises can say "yes" to their users' and business leaders' demands for anytime, anywhere productivity through secure mobile apps.

Good Secure EMM Suites provide consistent multi-platform mobile device, app management policies and controls across iOS®, Android™, Windows® 10 and BlackBerry® operating systems**, no matter the device ownership model or the user groups being mobilized.

The Good Secure EMM Suites provide a turnkey solution for rolling out collaboration apps, line of business apps, custom apps and/or leveraging your existing Microsoft® apps, all while protecting your business and your employees' privacy. Good-secured apps have consistent containerization and security policies across operating systems and devices to keep work and personal content separate. When an employee leaves the organization, only the Good-secured apps and business data are wiped from the device. All personal data remains personal and the rest of the device is left intact. Enterprises, including organizations with the highest security requirements, that are concerned about the security of their content as it moves beyond their firewall and is shared with third-parties and external partners, trust WatchDox® by BlackBerry, the leading secure Enterprise File Sync and Share (EFSS) solution, to increase the security and trackability of their business data.

WatchDox is available on its own, or bundled with the Good Secure Content Suite. For details visit www.blackberry.com/suites

About WatchDox

WatchDox by BlackBerry makes files secure and users productive. Our products enable enterprises to secure their files wherever they are against widespread threats, and to facilitate collaboration while protecting files wherever they go. Available as SaaS, a virtual appliance or a hybrid, WatchDox provides a single pane of glass to work with personal and enterprise content, uniquely combining consumer-style app interfaces with security to suit any enterprise use case. Over 150 of the Fortune 1000, including the largest civilian federal agencies, 6 of the top 12 private equity firms and most of the 6 major Hollywood studios, depend on WatchDox. For more information, visit: www.blackberry.com/watchdox.