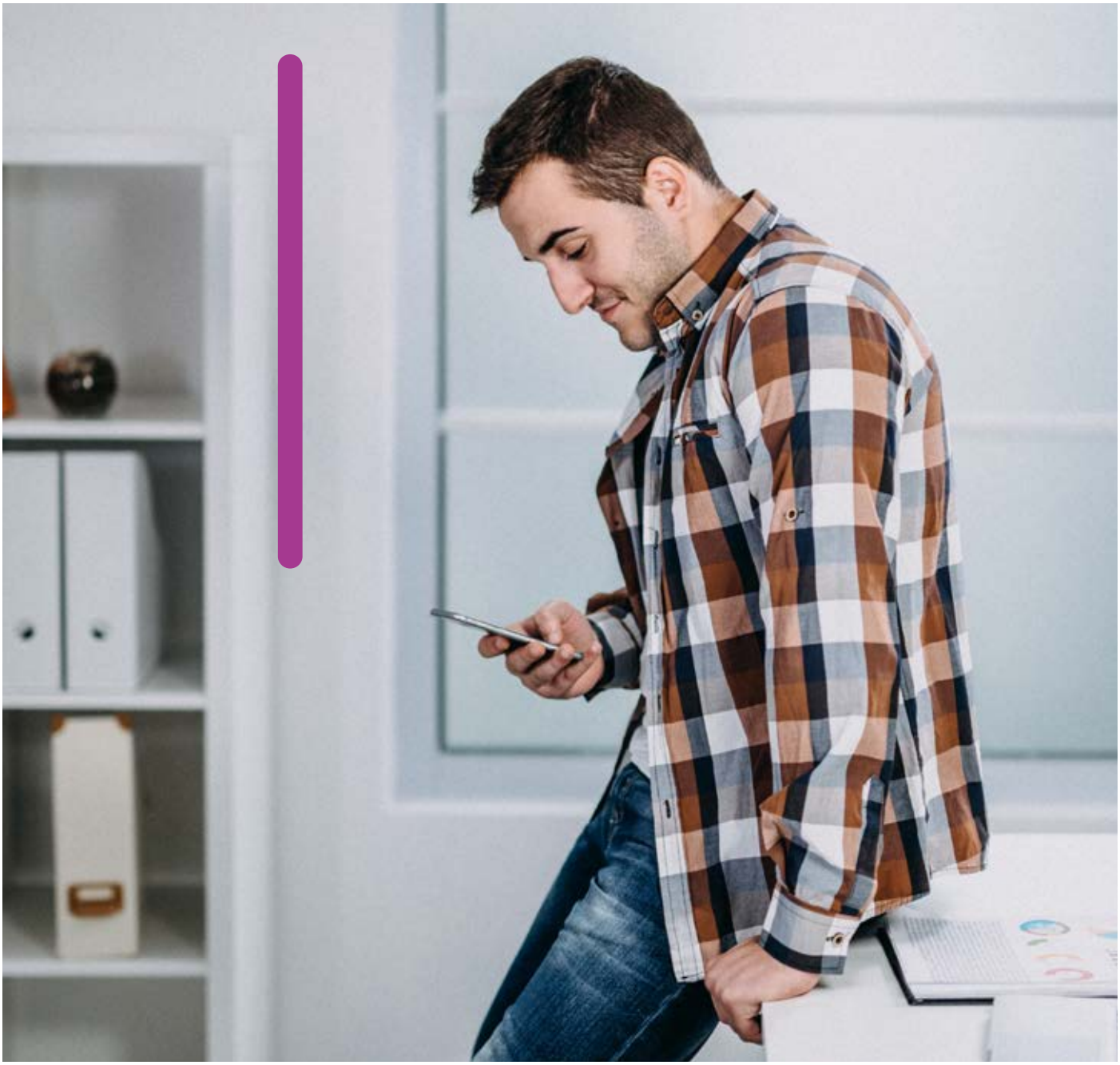
# FinalCode® for Multifunction Devices

Your data secured. Everywhere it goes.



FUJI Xerox

# Why FinalCode for Multifunction Devices?

Today's digital marketplace poses an enormous challenge for data security. In addition to preventing intentional security breaches, companies have the high probability of accidental losses to contend with. Research shows as many as 68% of business users have sent an email to the wrong person by mistake. Of all breaches in data security, 35% are due to human error.

More and more business processes rely on the sharing of data, not just between employees but also with customers and partners. Unfortunately, business partners are implicated in 32% of all breaches. With sensitive data being sent outside organisations every 49 minutes, it is getting more difficult to keep track of sensitive files.

According to research1, while 75% of organisations are highly concerned about data leakage risks, only 16% expressed confidence in their security controls.

Unauthorised distribution of digital media and end users copying or leaking sensitive content and documents can be averted by adopting Information Rights Management (IRM). Organisations who adopt an IRM policy in the workplace can protect IP with a systematic approach for complete copyright protection.

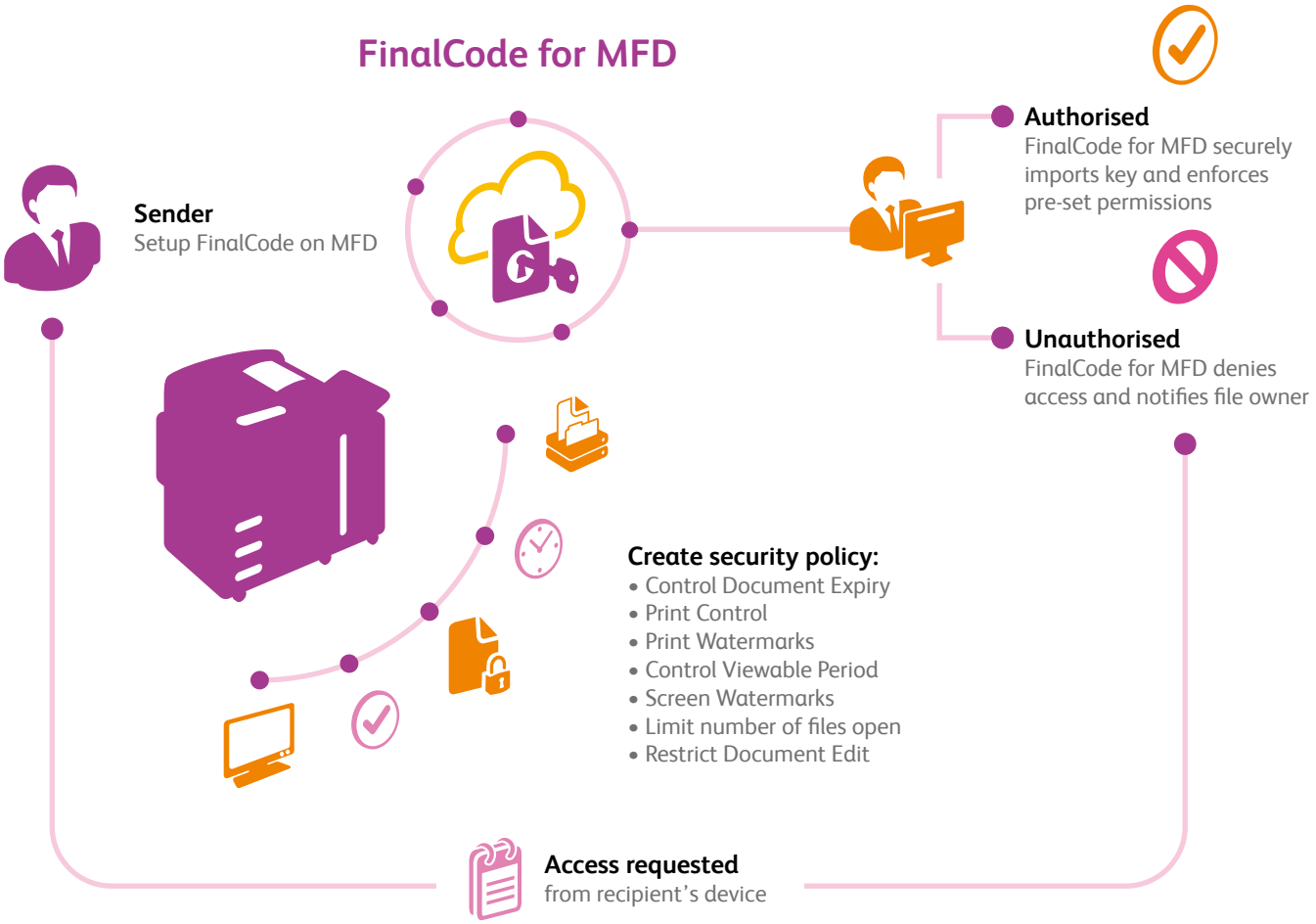
@2015EMA – State of File Collaboration Report September 2015, Sponsored by FinalCode*.

## YOUR DATA SECURED, EVERYWHERE IT GOES

FinalCode for Multifunction Devices (MFD) secures your files wherever they go. You are in control of exactly how each file is accessed and used throughout its lifecycle. Our unified solution consistently protects your data across communication channels. It's easy to use, scalable and cost effective.

*FinalCode® delivers a file security platform that allows any business to persistently protect sensitive files wherever they go inside and outside of their organisation. Available as a SaaS or virtual appliance offering, FinalCode makes securing file collaboration easy, flexible and cost-effective and in a way that works with popular applications, platforms and devices while preserving user experience and workflow. The solution applies strong encryption and granular usage control on demand or by corporate policy with the ability to remotely delete files on unauthorised access and usage attempts. As a result, companies can confidently share files and reduce data leakage risks. Headquartered in San Jose, California, FinalCode offers its solutions through its global network of authorised partners.

# How it works?




Use your existing or new MFD's to set up a security policy for your document. The MFD's communicates with the FinalCode cloud server, where all encryption keys are stored and managed. Once the document is scanned it is encoded with the policy selected from the MFD user interface. Recipients are allowed or denied access according to the policy, and pre-set usage permissions are enforced throughout the file's lifecycle.

### SECURE IT

Set precise access and usage permissions to encrypt the file locally. Security policies are stored and managed on the FinalCode cloud, reducing traditional on premise software and hardware costs.

**Human error risk: minimised**

### SHARE IT

Send the encrypted file via email communication channel – trusted or not, private or not – and FinalCode for MFD's will securely import the key for the recipient, decrypt the file and enforce permissions, even on mobile devices.

**Data leakage risk: minimised**

### TRACK IT

FinalCode for MFD's keeps a record of all file activity, giving you full control throughout the file's lifecycle. If an unauthorised user tries to access it, FinalCode for MFD's will deny decryption and log details of the attempt.

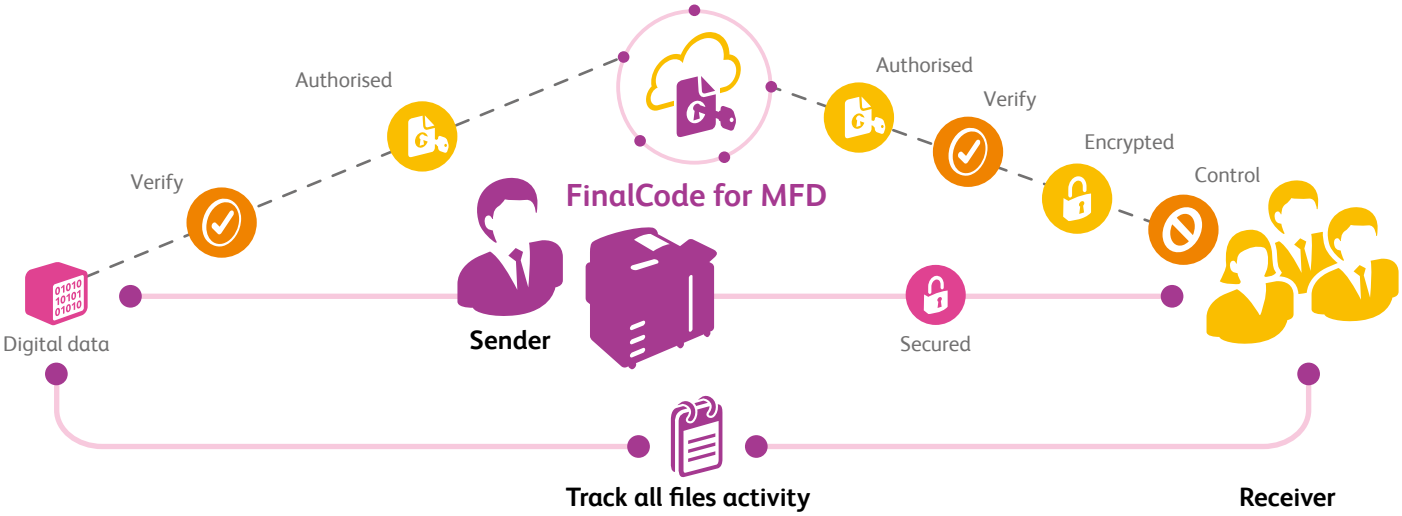
**Lost file risk: minimised**

# FinalCode for MFD in action

## PREVENT DATA MANIPULATION

With advanced technology, FinalCode for MFD's keeps a record of all file activity, protecting sensitive information such as quotes, sales figures, experiment data and clinical data from manipulation.

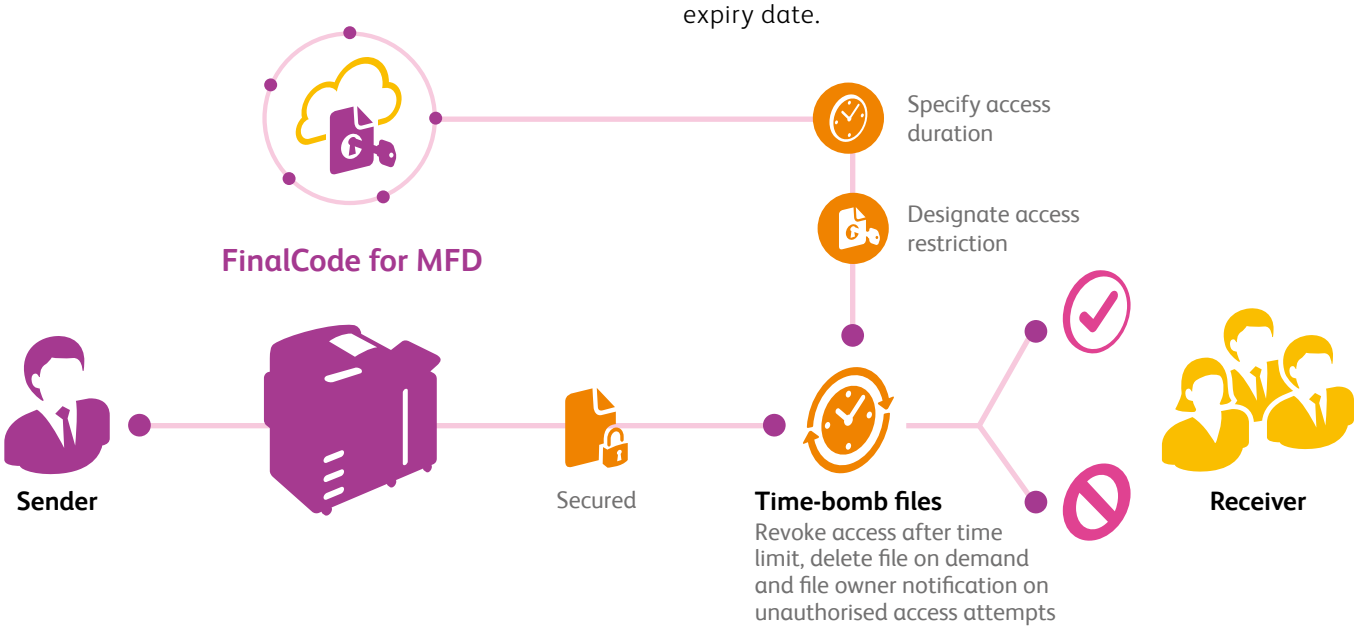
For industries requiring data integrity, including banking and securities, machinery, chemicals, food, precision devices, pharmaceuticals, construction, public services, healthcare, and agriculture. Application usage amongst others can include quotes, sales figures, credit information, experiment/ measurement/ observation data, design data, production data and clinical data.




## CREATE "TIME-BOMB" FILES

Set a window of time for the file to be used and FinalCode for MFD's will automatically revoke access when time is up, ensuring files such as requests for proposals, e-catalogues and NDAs are secured.

For division and departments involved in production and distribution of deliverables, including R&D, IT, general affairs, sales, and desktop publishing, across all industries and organisation sizes. Applicable to files with sensitive information (i.e. proposals, e-catalogues, disclosed information based on non-disclosure agreements) that could lead to a major data breach if accessed past the expiry date.



# Supported devices

| Model | Series |
|---|---|
| ApeosPort-VI | C7771/C6671/C5571/C4471/C3371/C3370/C2271 |
| DocuCentre-VI | C7771/C6671/C5571/C4471/C3371/C3370/C2271 |
| ApeosPort-V | C7776/C6676/C5576/C4476/C3376/C3374/C2275 |
| DocuCentre-V | C7776/C6676/C5576/C4476/C3376/C3374/C2275 |
| ApeosPort-V | 3065/3060/2060 |
| DocuCentre-V | 3065/3060/2060 |
| DocuCentre-V | C2265/C2263 |

For more information or detailed product specification, please call or visit us at


## Fuji Xerox Australia Pty. Ltd.

8 Khartoum Road, Macquarie Park NSW 2113
Tel. 13 14 12
**http://www.fxap.com.au/**




The information is as of March, 2018. PIC-0095 A(1510)