DigitalArts

Information Rights Management

FINALCODE®

Protect files the moment they are created.
Make files disappear after they are sent.

Protect your files so that you maintain control on WHO can access, WHEN can access and WHAT can be done on them regardless if the file is within or outside the organization. With complete audit trail and ability to remotely delete files, FinalCode can now also automatically protect files the moment they are created on the computer.

Secure

Restrict file access
Dynamic policy modification

- No password
- Designate recipients
- Limit access count/duration
- Control print/edit
- Automatic file deletion on unauthorized access
- Print/screen watermark

Track

Persistently track file activity throughout file lifecycle

- Access log
- Unauthorized access detection
- System operation log

Remote Delete

Make files disappear AFTER they are sent

- Remote file deletion
- Remote policy modification

Advanced Technology for Strong Encryption

Confidently share files with RSA-2048 bit secure data transmission and strong 256-bit AES encryption.

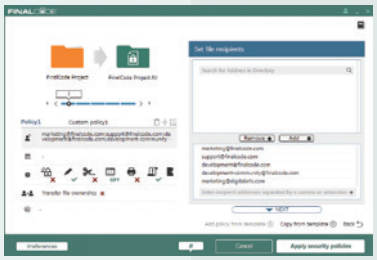
*FIPS140-2 Level 1 certified

Security Policy Settings

Extensive and granular file entitlement (open, edit, print, etc.)
based on file use and confidentiality.

User Operability

Advanced password-less encryption technology allows users to simply double-click to open and work with the secure file in the users' existing applications.



Centralized File Activity History

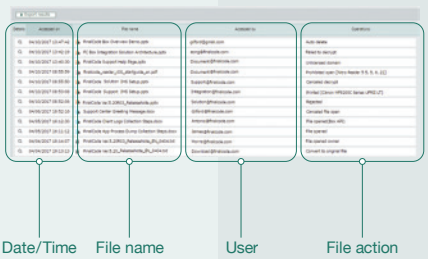
Track and log details on who, when and where shared files are opened, modified, printed, and remotely deleted even after files have been sent.

Visible Security Policy History

All file usage is logged and available to the file owner. No more oversight of inappropriate security policies.

Status Notification

File owner receives notification upon unauthorized access attempt. Instant alert of any unsanctioned file usage.

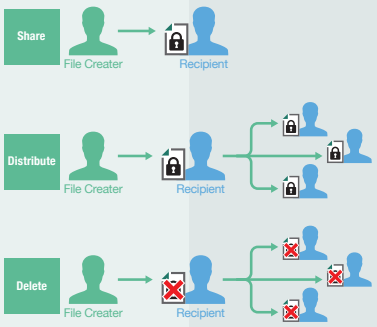


Persistent Control of Files Wherever They Go

File ownership remains with the file creator even after files have been sent. The file creators can modify security policies to change file access and permissions at anytime. Security policy updates are instantly reflected to the file.

Remote Delete Anytime, Anywhere

Trigger remotely delete on recipient's device on demand or on access attempt violation, even after files have been shared. Sensitive data remains intact even if the files were stolen or exfiltrated.



Four Checklists for Successful File Security Operations

1 Protect Information

- ☐ All files
- ☐ Customer and personal information
- ☐ Management information, IR information before disclosure
- ☐ Estimates, sales, credit information
- ☐ Research analysis data
- ☐ Resident information
- ☐ Files related to tax, pension, national health insurance, etc.
- ☐ Meeting minutes
- ☐ Information disclosed under valid RFP or NDA
- ☐ Student information
- ☐ Students lesson related files
- ☐ Other ( )

2 Protect Departments

- ☐ All departments
- ☐ Management planning
- ☐ Sales / Marketing
- ☐ Personnel, General Affairs, Finance
- ☐ Research and development
- ☐ Citizens or Residents
- ☐ Resident tax payment
- ☐ Welfare and child care support section
- ☐ Faculty and staff
- ☐ Student welfare
- ☐ Other ( )

3 Prevent Information Leak

- ☐ Targeted (malware) attacks
- ☐ Information Leakage by Internal Fraudulent Acts
- ☐ Lost / Stolen
- ☐ Tampering
- ☐ Supply chain attack
- ☐ Indirect leakage by trusted externals
- ☐ Accidental Information Leakage
- ☐ Other ( )

4 What file security do you need?

■ File Creation Security

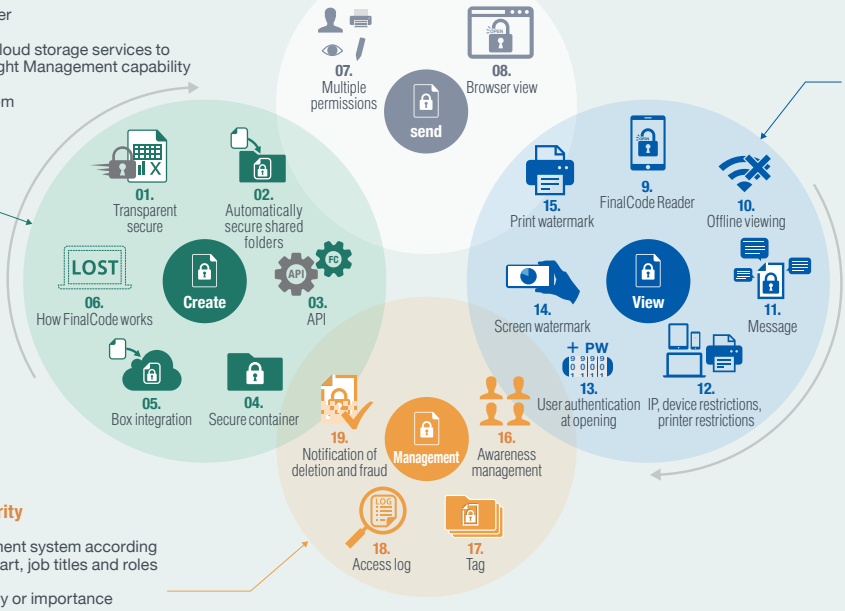
- ☐ **01.** Protect files on end users' computer automatically
- ☐ **02.** Protect files in the file sharing server
- ☐ **03.** Protect files in internal system such as document management system through integration
- ☐ **04.** Protect the entire folder
- ☐ **05.** Integration with Box cloud storage services to add on Information Right Management capability
- ☐ **06.** Disable files usage from lost computer

■ File Sharing Security

- ☐ **07.** Allowing different file usage permission for different group of recipients
- ☐ **08.** Allowing access to protected file without the need to install any software

■ File Usage Security

- ☐ **09.** View Office / PDF files safely from smartphone
- ☐ **10.** View files even in an offline environment
- ☐ **11.** Provide the latest information when viewing old files
- ☐ **12.** Prevent usage of protect files from unwanted locations and printing to unauthorized printers
- ☐ **13.** Prevent others from viewing personal files on the shared terminal
- ☐ **14.** Deter leaking of information by taking photograph of screen
- ☐ **15.** Deter leaking of information from printouts



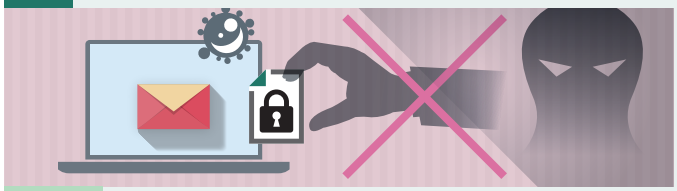
■ File Management Security

- ☐ **16.** Create a file management system according to the organization chart, job titles and roles
- ☐ **17.** Group files by category or importance
- ☐ **18.** Manage and track the file viewing / operation history
- ☐ **19.** Notification on unauthorized file access and successful remote file deletion

FinalCode solves ☑everything.

Use Cases: Solution by Purpose

Case 1 Protect files from targeted attacks



Conventional gateway security does not offer complete protection of your files against targeted attacks. FinalCode Network Folder Security option automatically secures all internal files where sensitive information remains protected, even if files are lost or stolen.

SOLUTION ▶ FinalCode Standard Edition

WHO Divisions and departments with the need to protect files in all industry, vertical, and organization size; Enterprises accredited by Privacy Mark and ISMS

WHAT Executive information, employee personal data, customer data, patents/IP and industry secrets, production planning, research data, and materials supplied by business partners

Case 2 Protect files from negligence, internal fraud, and employee turnover

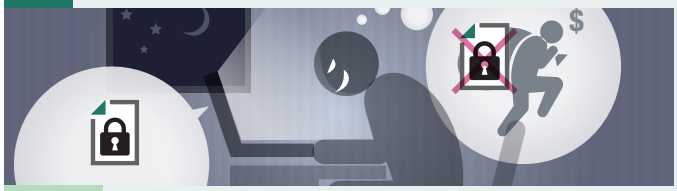
Companies and organizations lose sensitive files regularly and sustain significant damages through malicious acts, including former employee stealing files and trading information for pecuniary motives. Auto/Remote Delete and Notification option allows users to delete files wherever they are.

SOLUTION ▶ FinalCode Standard Edition

WHO Business management, sales, HR, R&D, business planning, IP, call centers, branches, and sales offices in all industry, vertical, and organization size.

WHAT Confidential documents, employee data, customer data, patents and other industry secrets, research data, pre-disclosed IR reports, and other sensitive information that could be sold to competitors/industries.

Case 3 Ensure internal file protection



Once files leave the protected data repository, data governance is lost. FinalCode API enables external solutions to call upon FinalCode functions and automatically secure all files.

SOLUTION ▶ FinalCode Standard Edition + FinalCode API

WHO Corporate departments retrieving data from Oracle®, Microsoft, Salesforce, SAP®, Marketo®, and other database, or ERP, CRM and marketing automation software.

WHAT Sales figures, personally identifiable information (PII), customer data, credit information, and HR/salary records retrieved from database and saved as CSV file.

U.S. Federal Standard FIPS 140-2 certified

FinalCode's encryption modules (FinalCode Crypto Module and FinalCode Crypto Module for Mobile) achieved FIPS 140-2 Level 1 certification and are Suite-B compliant.Federal Information Processing Standards (FIPS) are standards developed by the U.S. government for use in computer systems, which describe document securing processes, encryption algorithms and related specifications standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.

Operating environment

FinalCode Client	Windows 8.1 (32bit/64bit), Windows 10 (32bit/64bit)
FinalCode Reader	iOS 9.3 - 13.1, Android 4.1 - 4.4, 5.0 - 5.1, 6.0, 7.0 - 7.1, 8.0 - 8.1, 9.0, 10.0
Network Folder Security	Windows Storage Server 2012 R2, Windows Storage Server 2016, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019

Applications verified

Documents	Microsoft Word, Excel, PowerPoint (2003,2007,2010,2013,2016,2019) Adobe Acrobat® Reader® DC / XI / X, Acrobat® Pro DC / XI / X. Acrobat® Standard DC / XI / X JUST SYSTEM® Ichitaro ® Pro / Pro 2 / Pro 3/2014/2015, JUST Office 3 Fuji Xerox DocuWorks Viewer 7.3 / 8.0 / 9.0, Wordpad Notepad
Design/Images	Adobe Illustrator CS6 / CC (2017, 2018, 2019) , Adobe InDesign CS6 / CC (2017, 2018, 2019) Adobe Photoshop CS6 / CC (2017, 2018, 2019) , Microsoft Paint
Video	Windows Media Player (wma, wmv, avi, mpg, mpeg, mp3, mp4, etc.,)
CAD	AutoCAD® 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016 / 2017 / 2018 / 2019, AutoCAD LTTM 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016 / 2017 / 2018 / 2019 DWG TrueViewTM 2013 / 2014 / 2015 / 2016 / 2017 / 2018 / 2019, SolidWorks® 2013 / 2014 / 2015 / 2016, iCADMX V7L6 ,SolidMX V3.2

Please check our website for the latest information. Https://www.finalcode.com/jp/product/spec/

Contact Us

T : +65-6549-7879 E : inquiries@finalcode.com W : https://finalcode.com

FINALCODE®

DigitalArts