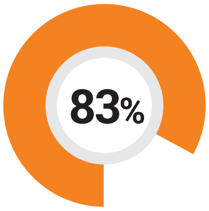
FINALCODE®

PRODUCT BRIEF

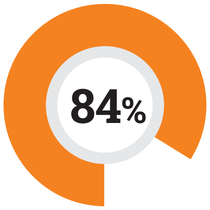
The FinalCode Platform

The Easy, Flexible and Persistent Way to Secure Sensitive Files Wherever They Go

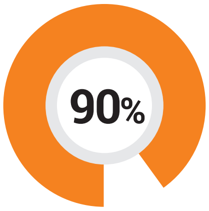
Companies face the monumental challenge of establishing strong and persistent data protection to ensure files containing sensitive, regulated and confidential information remain protected. Unfortunately, the ease and varied instruments to share files and the diversity of recipients and device types have grown exponentially - particularly with the adoption of bring your own device (BYOD), enterprise mobility, cloud-based collaboration and Enterprise Content Management (ECM) systems.



*Experienced a file data leakage incident**



*Lack confidence in file security controls**



*Concerned with files leaving cloud and container apps**

At the same time, targeted attacks and advanced malware have increased the probability of network, application, and system breaches, as well as the risk of ensuing unauthorized data access. Lastly, mounting data breach incidents and publicity within government and business sectors continue to drive additional legislative and commercial data privacy requirements. These factors have placed greater demands on IT and information security professionals to re-examine their file security controls and fortify information resource management (IRM) capabilities. The challenge is how to ensure that file protection remains active across file sharing mechanisms and infrastructure while supporting existing workflow and business collaboration.

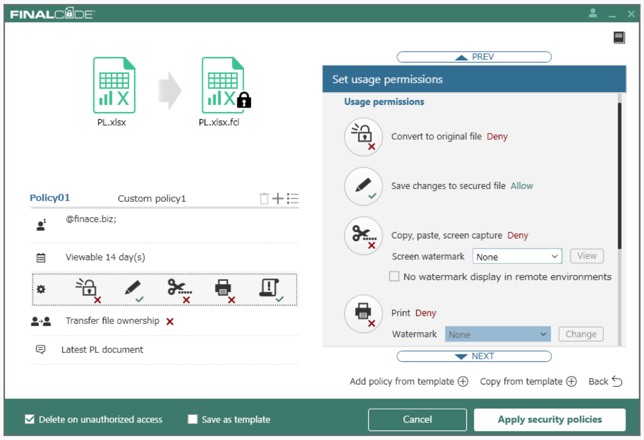
Effective File Security At Your Fingertips

The FinalCode persistent file security platform provides organizations with an easy, comprehensive and scalable means to protect sensitive files within and outside the corporate network – even after the files may become further exposed due to: inappropriate or unsanctioned collaboration, unauthorized network folder access, inadvertent email, lost or serviced devices, and removal of files from cloud- and container-based applications.

Conventional enterprise IRM and content management systems are presumed to offer strong file security and tracking since they are "behind the firewall." External cloud-based file storage and collaboration services are also presumed to offer security when files are managed within cloud, device and application containers. This protection breaks down once a recipient takes the file outside the protected confines of the managed corporate perimeter or cloud, device and application containers.

FinalCode makes file security intuitive, rapidly deployable and readily scalable with an approach that separates file security management from file storage, distribution and content management. The solution allows files owners and administrators to apply strong file encryption and a full range of usage controls locally, according to policy, and prior to sharing a file internally or externally. Once secure, security remains enforced at the file, operating system and application level, even after the file leaves the file owner's hands. The platform centralizes security management and provides for dynamic file permissions setting, lifecycle auditing and the ability to remotely delete files after they have been distributed.

FinalCode preserves user work flows, file storage and collaboration platform investments while persistently protecting files across all communication channels: trusted, untrusted, private or public.



Policy01 Custom policy1

@finace.biz;

Viewable 14 day(s)

Transfer file ownership ✗

Latest PL document

Set usage permissions

Usage permissions

Convert to original file Deny

Save changes to secured file Allow

Copy, paste, screen capture Deny

Screen watermark None View

□ No watermark display in remote environments

Print Deny

Watermark None Change

☑ Delete on unauthorized access

□ Save as template

The FinalCode persistent file security platform is comprised of two components; the FinalCode Client and the Server. The FinalCode Client resides on file owner's system and is activated once a sensitive file is designated by the file owner to be protected. The user is presented with an intuitive interface to allow for manual or template-based application of file recipient access and usage permissions. Once the FinalCode Client has secured the file locally, only the security metadata [keys and entitlement] are securely sent to the FinalCode Server. The resulting FinalCode protected file can be shared using any storage, distribution, application or content manager system. Only authenticated recipients can open the protected file using the FinalCode Client. The FinalCode Client will request access policy from the Server and the policy will be enforced at the operating system and application level. The policy can be dynamically modified, and provides for the ability of remote file unlocking and deletion. All file access and usage, both authorized and unauthorized, is logged in the server and available to the file owner and enterprise. The entire system is designed for automated onboarding for file owners and for both internal and external recipients.

*© 2015 EMA- State of Secure File Collaboration Report, September 2015 Sponsored by FinalCode.

The FinalCode Platform

PRODUCT BRIEF

Granular Entitlement Control

- Apply multiple policies per file
- Enforce policy online and offline
- Ad hoc or template-based policy setting
- Designate authorized users
- Directory-service integration
- Access duration; time, period…
- Read-only, no edit or save
- Edit/save only in encrypted file
- Allow / deny copy, paste, screenshot
- Allow / deny printing
- Printing with custom watermark
- Overlay watermark on an application window
- On-demand dynamic permission change
- Automatic email invitation to recipient
- Restrict user device type
- User template management
- Multiple policy server support
- Secure files in local or cloud folder
- Auto-secure files in network folders
- Application whitelisting
- File usage audit log and search
- Remote delete, on-demand
- Remote delete, unauthorized access
- App and OS level file-IRM control without relying on MS-Azure RMS

Powerful Security Management

- FIPS 140-2 Level 1 validated
- Suite-B compliant
- AES 256 file encryption
- RSA 2048 PKI - based user authentication
- TLS/SSL communication between client and server
- AWS KMS integration
- Automated, secure on-boarding
- Lightweight Client install does not require admin privileges
- Supports remote deployment tools
- Web management console
- Policy hierarchy aligned to organization structure
- Global user management
- Roles-based access control
- Define function scope for user types
- Custom administrator roles
- Template policy management
- Enforce template use by role
- Restrict user and device type
- Network share folder monitoring
- Restrict file access by IP address
- Restrict file printing by IP printer
- User and device authentication
- Global file activity, violation logs supporting CEF format and SYSLOG
- Comprehensive SDK available

Extensive File IRM Coverage

- Microsoft Excel 2016, 2013, 2010, 2007
- Microsoft Word 2016, 2013, 2010, 2007
- Microsoft PowerPoint 2016, 2013, 2010, 2007
- Microsoft Access 2016, 2013, 2010, 2007
- Microsoft Visio 2016, 2013, 2010, 2007
- Microsoft Viewer Word, Excel, PowerPoint
- Microsoft Windows Media
- Microsoft WordPad, Paint, Notepad
- Adobe Reader DC XI, X
- Adobe Acrobat, Pro/Std. DC XI, X
- OpenOffice.org Writer, Cal, Impress 4.1, 4.0
- Libre Writer, Calc, Impress 5,2, 5.1, 5.0, 4.4, 4.3, 4.2, 4.1, 4.0
- Microsoft Windows Picture and FAX Viewer, Photo Gallery, Photo Viewer
- Broad Photo, Video and Music format support

CAD Option:

- AutoDesk AutoCAD 2016-2010
- AutoDesk AutoCAD LT 2016-2010
- AutoDesk DWG TrueView 2016-2013
- Dassault SolidWorks 2016-2013

Abbreviated list, subject to change

FinalCode Client

Client for Windows OS

- Windows 7 Ultimate/Professional SP1 32bit/64bit
- Windows 8.1 Pro/Enterprise 32bit/64bit
- Windows 10 Home/Pro/Education/Enterprise 32bit/64bit
- Windows Server 2012 R2
- Windows Storage Server 2012 R2

Client for Mac

- Mac OS 10.12 Sierra

PDF Reader App for iOS

- iOS 9.3 – 10.2

PDF Reader App for Android

- Android 4.0, 4.1, 4.23.3, 4.4

Network Folder Security

- Windows Server 2008 R2 SP1 64bit
- Windows Storage Server 2012 R2
- Windows Server 2012 R2
- Windows Server 2016

FinalCode Server

SaaS and Virtual Appliance server options are available

SaaS for Cloud

- Running on Amazon Web Services (AWS)

Virtual Appliance (VA) for On-Premise

- Hypervisor: VMware vSphere 5, 6
  Windows Server 2012, 2012 R2 Hyper-V
- Database: Microsoft SQL Server 2014
  MySQL 5.6, 5.7
  Oracle Database 12c
  PostgreSQL 9.3

Take the Next Step

With FinalCode, your employees can share sensitive files internally and externally with confidence, knowing that unauthorized recipients will not have access. Better yet, your company can rapidly implement strong file protection, entitlement and auditing capability that preserves user expe-rience and your investment. FinalCode's persistent file security platform provides an easy and flexible approach allowing you to use your existing file share, enterprise content management, cloud storage and collaboration platforms. Visit the FinalCode website to schedule a demo or get a free trial license.

www.FinalCode.com

FINALCODE®