PRODUCT BRIEF

FINALCODE®

Persistent File Security

Use FinalCode to make files disappear AFTER they are sent. It's magic.

Companies today face a monumental challenge as they try to protect sensitive or confidential information as it is used and distributed across their value chain. Companies are generating more data than ever, as mobile workforces use a proliferation of smart devices to do their jobs; lines of business develop and run their own apps; companies leverage cloud services and enterprise content management (ECM) systems; and the IoT revolution gains strength.

Secure
Track
Remote Delete
Log

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

Effective File Security At Your Fingertips

At the same time, targeted attacks and advanced malware have increased the probability of unauthorized data access and application, system, and network breaches. Lastly, legislative and commercial data privacy requirements are growing in response to increased cyberattacks and data breach incidents. All of these business, technology, and regulatory developments are causing IT and information security professionals to re-examine their file security controls and strengthen information rights management (IRM) capabilities. The challenge: ensure persistent file protection across diverse file sharing and distribution mechanisms and infrastructure while supporting existing workflow and business collaboration.

Effective Security That Protects Files Wherever They Go

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 stolen devices, and removal of files from cloud- and container-based applications. Conventional IRM and ECM 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 by separating file security management from file storage, distribution, and content management. FinalCode 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.

Gain Strong Policy Controls and an Audit Trail for Regulatory Purposes
Once FinalCode protection is applied, 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 enables 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.

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 that enables 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 [the keys and IRM permissions] 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 locking/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 in enterprise.

The FinalCode Platform

PRODUCT BRIEF

Gain Granular Entitlement Control

- Secure multiple folders and files according to policy
- Apply multiple policies per file/folder
- Enforce policy online and offline
- Ad hoc or template-based policy setting
- Designate authorized users
- Active Directory-service integration
- Access duration: time or period
- Authentication of users on opening FCL files
- View-only, no edit or save
- Edit/save only in encrypted file
- Allow / deny copy, paste, screenshot
- Allow / deny printing
- Printing with custom watermark
- Overlay screen 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 (supporting CEF and LEEF) and search
- Remote delete, on-demand
- Remote delete, unauthorized access
- App and OS level file-IRM control

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 and LEEF format
- Comprehensive SDK available
- ISO/IEC 27001:2013
- ISO/IEC 27017:2015

Extensive File IRM Coverage

- Microsoft Excel/ Microsoft Word / Microsoft PowerPoint / Microsoft Access 2021, 2019, 2016
- Microsoft Visio 2021, 2016
- Microsoft Windows Media
- Microsoft WordPad, Paint, Notepad, zip Adobe Reader
- DC (2022,2021) (32bit, 64bit) Adobe Reader DC (2020,2019,2018,2017)(32bit version only)
- Adobe Acrobat Pro / Adobe Acrobat Std DC (2023-2017)
- Adobe Illustrator, Photoshop, InDesign CS6 / CC (2019,2018,2017)
- OpenOffice.org Writer, Calc, Impress 4.1, 4.0
- Libre Writer, Calc, Impress 4.0 – 5.2
- Microsoft Windows Picture and FAX Viewer / Photo Gallery / Photo Viewer / Windows Write
- Broad Photo, Video and Music format support

CAD Option :

- Siemens Solid Edge 2022
- AutoDesk AutoCAD 2022-2018
- AutoDesk AutoCAD LT 2021-2018
- AutoDesk DWG TrueView 2021-2018
- Dassault SolidWorks 2020-2017
- Dassault SolidWorks Composer Player / Dassault eDrawings (2020-2019)

FinalCode Client

Client for Windows OS

- Windows 10 Home/Pro/Education/Enterprise 32bit/64bit
- Windows 11
- Windows Storage Server 2012 R2 / 2016
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

FinalCode Reader App for iOS

- iOS 12.54 – 16.1.1, iPad OS 13.7 – 16.1.1

FinalCode Reader App for Android

- Android 10-13

Network Folder Security

- Windows Storage Server 2012 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Storage Server 2016
- Windows Server 2019
- Windows Server 2022

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 6, 7
- Windows Server 2012/2012 R2/2016/2019/2022 Hyper-V
- Nutanix AOS 5.5

Database:

- Microsoft SQL Server 2014, 2017, 2019
- MySQL 5.7, 8.0
- Oracle Database 18c, 21c
- PostgreSQL 11, 13, 14

FinalCode API

- Red hat Enterprise Linux 7,8 (x86_64)
- CentOS 7 x64
- Windows 10 x86
- Windows 10 x86_64
- Windows Server 2012 R2
- Windows Server (2022, 2019, 2016)

About FinalCode

FinalCode delivers a file security platform that allows any business to persistently protect sensitive files wherever they go inside and outside of the organization. Available as a SaaS or Virtual Appliance, FinalCode makes securing file collaboration easy and cost-effective and in a way that works with popular applications, platforms and devices while preserving user experience and work flow. The solution applies strong encryption and granular usage control on demand or by corporate policy with the ability to remotely delete files. The company's patented CryptoEase™ technology streamlines on boarding, encryption and administration, making deployment rapid and scalable.

www.finalcode.com

FINALCODE®