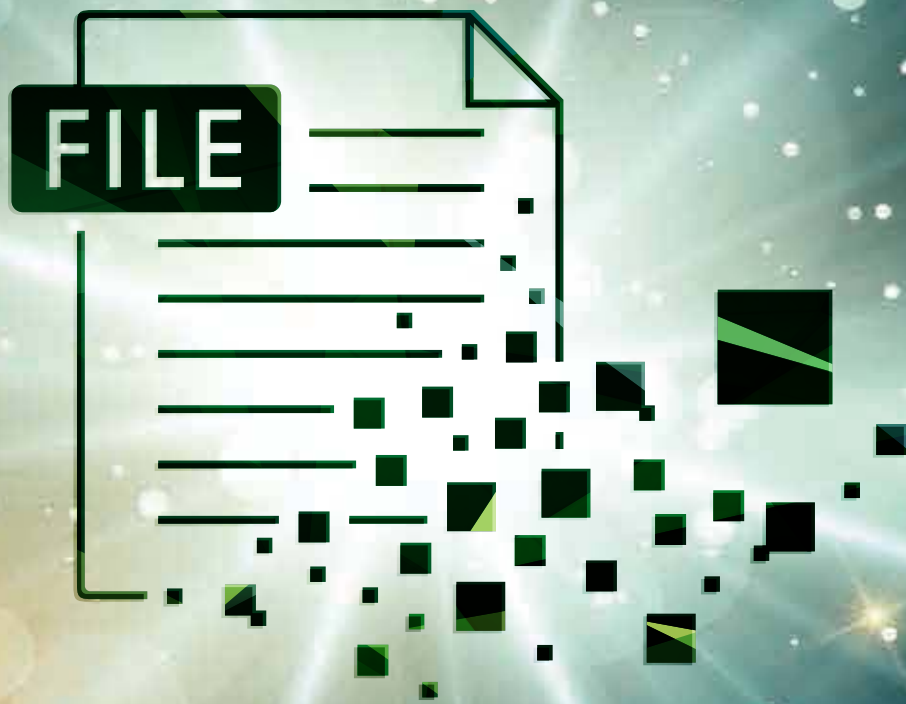




新世代數位版權管理系統



**全面掌控
外送檔案的使用狀態！**

使用FinalCode保護的檔案，檔案擁有者將檔案傳送後可將檔案遠端刪除，如同魔術般讓它消失不見！

我們每天都會建立及分享資料，並在修改後傳送給他人。

檔案會持續不斷在企業內部與不同企業間來回交換，特別是在資訊無國界的現代。

在這個全球化的年代，我們該如何確保檔案能獲得妥善保護呢？

FinalCode 目標是努力不懈地確保您在日常商務中的檔案安全，並在企業內外隨時隨地提供保護。

只需使用 FinalCode，即可將檔案存取權限授予給授權接收者、在檔案生命週期全程進行稽核，以及依照需求修改遠端檔案存取政策。



安全

限制檔案存取
遠端修改政策

- 🔒 無需密碼
- 🔒 指定接收者
- 🔒 限制存取次數/期間
- 🔒 控制列印/編輯
- 🔒 自動刪除非經授權的檔案，或防止未經授權的存取
- 🔒 列印/螢幕浮水印

先進強化的加密技術

透過 RSA-2048 位元安全資料傳輸及強大的 256 位元 AES 加密，在保密的情況下分享檔案。

* FIPS 140-2 Level 1 認證

安全性政策設定

根據檔案使用情況與機密性，針對檔案權限(開啟、編輯、列印等)選擇一般或進階設定。

使用者操作性

先進的無密碼加密技術，讓使用者只需在其現有的應用程式中用滑鼠點兩下，即可開啟和處理受保護的檔案。



追蹤

在檔案的生命週期中
全程追蹤檔案活動

- 🔒 存取記錄
- 🔒 偵測未授權的存取
- 🔒 系統操作記錄

集中式檔案活動 歷程記錄

追蹤並記錄開啟、修改、列印及遠端刪除已分享檔案的人員身分、時間及地點，即便是已傳送的檔案也不成問題。

透明的安全性政策歷程記錄

所有檔案使用情形皆會受到記錄並提供給檔案擁有者。再也不會因安全性政策制定上的失誤而出錯。

狀態通知

檔案擁有者會在有人嘗試存取未授權的檔案時收到通知。
任何未經批准的檔案使用情形皆會警示記錄。



遠端刪除

在檔案傳送後
可讓檔案消失無蹤

- 🔒 遠端刪除檔案
- 🔒 遠端修改檔案存取政策

無論檔案去了哪裡， 仍可持續的監控

即使已經傳送檔案，檔案所有權仍保留在檔案建立者手中。
使用者可以隨時修改安全性政策，以變更檔案存取使用權限。
檔案安全性政策可遠端更新，並立即套用在受保護的檔案上。

隨時隨地遠端刪除

即使已經送出的檔案，仍可依照需求或在違反存取規則時，遠端刪除受保護的檔案。即便檔案失竊或被盜用，機密資料仍受到完整保護。

使用案例

適用於各種用途、
角色及產業的解決方案

案例 01

保護檔案免於因疏失、內部員工惡意竊取及員工流動而造成資料外洩



企業因人為的疏失、內部員工惡意資料竊取或是人員流動等種種因素，造成企業機密資料外洩。FinalCode提供受保護檔案遠端刪除的功能，不論您受保護的資料在哪裡，檔案擁有者或是系統管理員皆可遠端刪除受FinalCode保護的檔案。

對象

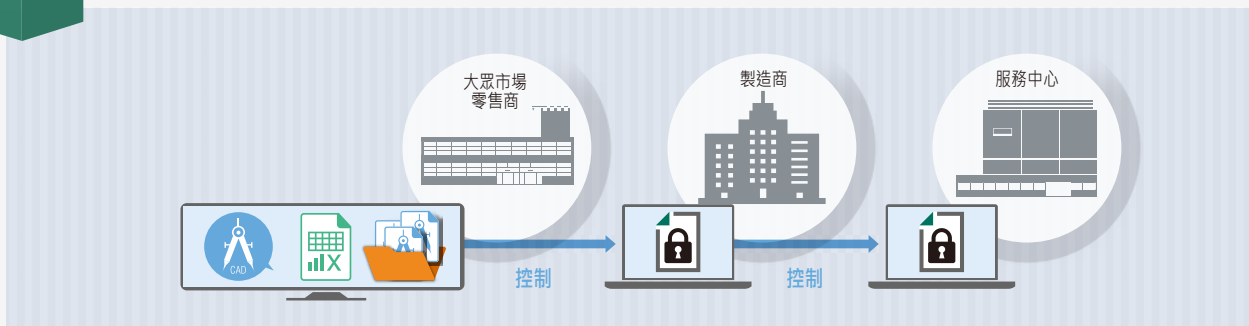
企業中接觸到機密資料的單位，包括財務、法務、業務、R&D、HR、行政管理部.....等等。

內容

機密文件、員工資料、客戶資料、專利及其他產業機密、研發資料、以及其他可能售予競爭廠商/產業的機密資訊。

案例 02

保護與客戶及商業合作夥伴分享的檔案



企業之間主要透過共享關鍵機密資訊來共同合作，如個人資訊、財務資料或與設計有關的文件，因此必須解決資料遺失、竊取和遭人破解等的重大議題。FinalCode 讓企業能輕鬆設定檔案存取權限及使用政策、追蹤檔案被使用的狀況，以及不限地點遠端刪除任何檔案。

對象

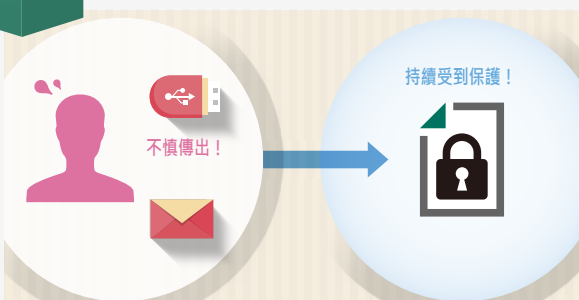
物流、運輸、零售、電信、大眾服務以及其他服務區塊和相關供應鏈；處理個人識別資訊 (PII) 的部門，包括服務、物流、商業支援、行政管理及客服中心。

內容

企業之間必須被交換的機密資料。

案例 03

保護資料免於因疏失而外洩



機密資訊經常會因意外寄出的錯誤收件者電子郵件、可攜式裝置遺失、未被記錄的檔案傳輸，以及未經授權的人拿取印表機中的文件而外洩。FinalCode 的專利技術提供進階的使用權限並可在發生未經批准的使用情形時觸發遠端刪除，保證能持續確保檔案的安全。

對象

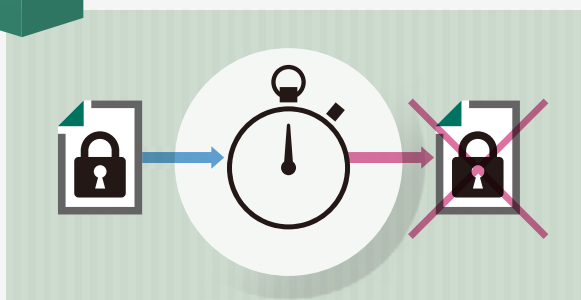
企業內所有需要保護的機密檔案；尤其以通過隱私標章 (Privacy Mark) 及 ISMS 認證的企業。

內容

遺失或遭破解時，可能對公司、供應鏈及客戶造成不可預期影響的資訊。

案例 04

建立「限時閱讀」檔案



特定文件需要對存取設下時限，例如徵求提案說明書 (RFP)、電子型錄及根據 NDA 公開的資料，使用FinalCode可以設定檔案存取的時段。系統會在時間結束後自動撤銷存取權限、根據需求刪除檔案，以及在有人嘗試未經授權存取時寄發通知給檔案擁有者。

對象

所有企業中需要和其他夥伴交換機密資料的使用者，包括研發 (R&D)、IT、總務、銷售等。

內容

具有時效性資訊的檔案，若在到期日後遭人存取，可能引發重大的資料外洩事件，包括徵求提案說明書 (RFP)、電子型錄及根據 NDA 公開的資訊。

取得進階權限的控制能力

- 根據政策確保多個資料夾及檔案的安全
- 依檔案/資料夾套用多個政策個
- 線上及離線狀態強制執行政策
- 個別指定或以範本為基礎的政策設定
- 指定授權使用者
- 整合 Active Directory(AD)
- 存取期限：時間或期間
- 使用者開啟 FCL 檔案時進行驗證
- 僅可檢視，不可編輯或儲存
- 僅可在加密檔案進行編輯/儲存
- 控制檔案複製、貼上、螢幕截圖
- 控制檔案列印
- 列印時加入自訂浮水印
- 在應用程式視窗中加入螢幕浮水印
- 根據需求遠端變更使用權限
- 自動寄送電子郵件邀請給檔案接收者
- 限制檔案接收者裝置類型
- 使用者政策範本管理
- 支援多重政策伺服器
- 確保本機或雲端資料夾的檔案安全
- 自動加密網路共用資料中的檔案
- 應用程式白名單
- 檔案使用情形稽核記錄 (支援 CEF 及 LEEF)
- 依照需求遠端刪除受保護的檔案
- 發生未授權存取時遠端刪除受保護的檔案
- 應用程式及作業系統層級的檔案 IRM 控制

強大的安全性管理能力

- FIPS 140-2 Level 1 認證
- 符合 Suite-B 規範
- AES 256 檔案加密
- RSA 2048 PKI - 以使用者驗證為基礎
- 用戶端與伺服器間以 TLS/SSL 通訊
- 整合 AWS KMS
- 輕量化用戶端安裝，不需要管理員權限
- 支援遠端部署工具
- 網頁管理主控台
- 支援階層式的管理架構
- 以角色為基礎的存取控制
- 對使用者類型定義功能範圍
- 自訂管理員角色
- 範本政策管理
- 強制使用者套用檔案保護範本
- 限制接收者及裝置類型
- 網路共用資料夾監控
- 依 IP 位址限制檔案存取
- 依 IP 印表機限制檔案列印
- 使用者及裝置驗證
- 全域檔案活動、違規記錄，支援 CEF 及 LEEF 格式

廣泛支援的檔案類型

- 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、小畫家、記事本
- Adobe Reader DC XI、X
- Adobe Acrobat、Pro/Std.DC XI、X
- Adobe Illustrator CS6 / CC (2017)
- Adobe Photoshop CS6 / CC (2017)
- OpenOffice.org Writer、Calc、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 及 FAX Viewer、影像中心、相片檢視器
- Broad Photo、視訊及音樂格式支援 CAD 類型：
- Autodesk AutoCAD 2016-2010
- Autodesk AutoCAD LT 2016-2010
- Autodesk DWG TrueView 2016-2013
- Dassault SolidWorks 2016-2013
- 本表為簡表，更多詳細支援的檔案類型可造訪FinalCode官方網站

FIPS140-2 Level 1 認證

FinalCode 的加密模組及行動加密模組 (FinalCode 採用的 AES256 加密模組) 已獲得美國國家標準暨技術研究院 (National Institute of Standards and Technology, NIST) 頒發聯邦資訊處理標準 (Federal Information Processing Standards, FIPS) 140-2 Level 1 認證。

FinalCode 用戶端

Windows 作業系統支援平台

- Windows 7 Ultimate/Professional SP1 32 位元/64 位元
- Windows 8.1 Pro/Enterprise 32 位元/64 位元
- Windows 10 Home/Pro/Education/Enterprise 32 位元/64 位元
- Windows Server 2012 R2
- Windows Storage Server 2012 R2
- Windows Server 2016

Mac 作業系統支援平台

- Mac OS 10.12 Sierra

iOS 版 PDF Reader 應用程式

- iOS 9.3 – 10.2

Android 版 PDF Reader 應用程式

- Android 4.0、4.1、4.2.3、4.4、5.0、5.1、6.0、7.0、7.1

網路共用資料夾支援平台

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

FinalCode 伺服器

提供SaaS與Virtual Appliance(VA)兩種模式

- SaaS管理平台運作於Amazon Web Services(AWS)；Virtual Appliance(VA)於本地端自行架設管理系統
- 虛擬化平台：
VMware vSphere 5、6
Windows Server 2012、2012 R2 Hyper-V
- 資料庫：
Microsoft SQL Server 2014
MySQL 5.6、5.7
Oracle Database 12c
PostgreSQL 9.3、9.6

邁向下一步

FinalCode 能讓您的員工放心地在企業內外分享機密檔案，因為未授權的接收方絕對無法獲得存取權限。更棒的是，您的公司能快速實施強大的檔案保護、權限以及稽核功能，以保全使用經驗及您的投資。FinalCode 使用的檔案安全性平台提供簡便且彈性的方法，在不改變您現有的檔案交換機制上保護企業機密資料。

想得到更多FinalCode的訊息，請您和FinalCode台灣總代理倍網資訊聯繫

FinalCode 台灣總代理倍網資訊：電話：(02)2563-2386 | 電子郵件：sales@pronet-info.com.tw | 網址：www.pronet-info.com.tw