FINALCODE®

Solutions By Role

職務別: 行政人員CIO，首席技術長，首席信息安全長，首席財務長，首席運營長

文件共享是組織業務的正常部分。文件在設備，存儲，通信渠道，基於雲的應用程序以及環境內外的收件人之間快速而廣泛地移動。這種動態協作會導致敏感文件經常不受保護，容易受到數據洩漏和不當使用的影響。EMA研究調查顯示，83%的中型和大型企業遇到了文件數據洩漏事件，50%經歷了頻繁事件。

隨著系統違規和數據隱私洩露持續增加，未經授權訪問您組織的文件包含受限制的，受監管的和機密的數據可能會影響您的底線，引入重大責任並損害您的商業信譽。面臨的挑戰是如何根據需要啟用文件安全性，利用當前的基礎架構和工作流程，並允許內部甚至外部用戶迅速採用。

FinalCode提供經過驗證的，可互操作的文件安全平台，以簡單，可擴展和持久的方式應對這些挑戰。我們基於文件的信息權限管理（IRM）解決方案允許您的組織或部門和用戶在共享文件時輕鬆應用文件加密和使用控制。通過將文件安全性與文件存儲，傳輸和內容管理分離，文件無論走到哪裡都會受到保護。使用端到端IRM控制，只有授權用戶才能根據臨時或根據公司策略設置的權限訪問該文件。組織不僅可以獲得完全可見性，而且即使在文件離開您的環境後也可以撤消訪問權限或更改使用控制。最好的是，訪問被拒絕，如果文件最終落入壞人手中，文件將被自動刪除。存儲所有文件安全活動以用於合規性和調查目的。

FinalCode 適用於您現有的內容管理投資，因為它與您當前的基礎架構集成。它的應用程序，基礎架構和設備無關，因此支持您的工作環境以及外部用戶的工作環境 - 使FinalCode比典型的IRM解決方案更具成本效益。為部門，辦公室甚至整個組織內的特定應用程序部署它。這種受控的持久文件保護可以增強您組織內外共享文件的數據丟失防護功能; 使您能夠保護敏感信息，更好地遵守保密義務並支持數據保護合規性標準。

職務別: 資訊安全人員，MIS

您的任務是保護信息資產，但在文件安全方面，您的警衛已經失敗。根據EMA研究報告，75%的中型和大型企業調查受訪者表達了對文件數據洩漏風險的高度關注。在動態環境中維護網絡文件夾和內容管理訪問具有足夠的挑戰性，但是一旦授權用戶從存儲庫中刪除敏感文件，外圍控件就會丟失。因此，50%的EMA受訪者經常遇到文件數據洩漏事件就不足為奇了。

當從安全本地容器中刪除文件時，使用基於雲的文件共享和內容管理平台會大大增加此風險。在同一份EMA調查中，90%的人擔心文件會離開基於雲的平台和設備容器。典型的文件安全解決方案通常需要復雜的公司範圍部署，這些部署成本過高且管理複雜 - 尤其是在保護要與組織外部用戶共享的文件時。

到現在。FinalCode允許您通過提供簡單，靈活且經濟高效的持久性文件安全平台，立即解決文件數據洩漏和數據隱私合規風險。FinalCode與基礎架構，應用程序和設備無關，允許您的團隊快速實施。由於FinalCode管理文件安全性而不是文件存儲，傳輸或協作，因此它適用於現有的內容管理投資，不會干擾用戶工作流程。它可以在幾個小時內部署，以支持特定用戶，部門或業務需求，或者可以輕鬆支持企業範圍的實施，而不會影響用戶體驗。它是一個可擴展的平台，隨著需求的變化適應您的公司。

FinalCode系統從加密管理和策略設置中抽象和自動化各種管理任務，以允許組織內外的用戶自我配置。由於文件安全性由用戶應用或由系統自動應用於網絡共享文件夾，因此僅需要名義上的最終用戶交互。用戶只需將安全控制應用於他們想要共享的文件，指定授權的收件人，進行即時策略更改，接收權限請求等等，直觀的GUI。組織及其文件所有者對共享文件具有端到端的可見性，並且即使在分發後也可以更改控制和刪除文件。跟踪文件安全活動和文件使用情況，並隨後記錄以用於各種分析和取證目的。

FinalCode可以快速部署，輕鬆管理，並且與傳統的信息權限管理（IRM）解決方案相比，顯著降低了總體擁有成本。現在，您可以使您的組織能夠以經濟高效的方式輕鬆保護包含敏感，受監管和機密數據的文件，這不會破壞您的基礎架構投資或增加您有限資源的負擔。

職務別: CISO，安全架構師，資料保護官

雖然協作是業務必需品，但數據隱私和數據洩漏風險仍然是執行和董事會層面關注的問題。不恰當地共享環境內外的文件，發送給錯誤收件人的文件或通過系統違規獲得的文件會對您的業務構成持續威脅，並使組織面臨合規風險和責任。遺憾的是，在一份針對中型和大型企業的EMA研究報告中，超過84%的受訪者對其安全控制和審核保護文件的能力表示中等甚至不信任。

確保適當的數據保護和治理的分層方法包括資源訪問控制，Web過濾，數據丟失預防和保護靜態數據。在同一個EMA調查中，超過50%表示文件數據洩漏的最大影響是由於與公司外部的其他人不恰當地共享的文件，惡意軟體或駭客洩露的文件以及受信任的內部人員竊取的文件。雖然政策制定和法律執行是最佳做法，但大多數組織計劃進行技術投資並實施更強大的文件加密和使用控制軟體。

FinalCode提供基於文件的信息權限管理（IRM）平台，該平台以有效，可管理和可用的方式應用經過驗證的標準加密和使用控制，允許任何組織輕鬆保護包含敏感，受監管和機密數據的文件。它提供了一種持久的方法來確保文件所有者或公司政策調用的技術控制無論在何處都可以保持活動狀態。所有文件安全活動（包括控制的應用，後續訪問嘗試和實際使用）都保存在審計日誌中，用於趨勢分析，取證和支持數據洩露安全港的證據。由於FinalCode管理文件安全性，而不是文件存儲，傳輸和協作管理，因此可以快速部署它以便以內部和外部用戶都可以輕鬆採用的方式支持通用的基礎架構，設備和應用程序。

我們的平台管理密鑰，用戶配置和身份驗證，策略設置和實施以及日誌記錄。它允許文件所有者使用256位AES加密來加密文件，應用細化權限，並確保文件只能由授權用戶根據設定打開和使用。系統還可以自動將策略應用於本地和網路共享文件夾。當文件跨網路（受信任，不受信任，私有或公共），設備以及文件和雲共享服務移動時，文件安全控制最終將在接收者系統的操作系統和應用程序級別保持強制執行。收件人和權限，包括解鎖，撤銷訪問或通過數據覆蓋遠程刪除文件，即使在分發後也可以動態更新。未經授權的嘗試打開文件或未經批准的使用可能導致文件自動從系統中刪除。

使用FinalCode，組織可以安全地共享文件，同時保留信息可用性，完整性和機密性以及機密性。