SecureAge

使用透明加密
戰勝 12 種常見資料外洩問題

SecureAge 2020 年白皮書

全新的網路安全界線

長久以來，網路界線的保護措施一直被視為不足。在當今的區域網路、連網裝置和雲端應用程式環境中，各個組織使用了零信任 (Zero Trust)、軟體定義界線 (Software Defined Perimeter) 和微分區 (Microsegmentation) 等安全技術來應對資訊安全的相關問題。這些方法和相關技術旨在防止資料容器（即檔案）受到未經授權的存取。控制檔案的存取即是新的安全界線。

儘管有這些控制措施，資料外洩仍頻傳

據報導，2019 年仍有 123 億筆資料記錄遺失或遭竊，證明了資料竊取仍然是一個普遍存在的問題。作業系統、網路硬體和其他裝置中始終存有缺陷，能夠躲避網路安全的控制，並可能遭到利用以對檔案進行未授權的存取。

人為因素同樣也是關鍵。除了外部攻擊者以外，內部人員和相關的第三方，無論他們是有意或無意的，都是資料遺失的主要因素，原因在於他們也是獲得授權存取資料。

> Microsoft SMBv3 安全漏洞可能使未經授權的攻擊者在目標伺服器或用戶端電腦執行程式碼，導致資料立即遭到存取。

這給上述提到的技術帶來了一個嚴重問題：它們無法區分「經授權的資料存取」和「未經授權的資料使用」之間的差異。這一點至關重要，由於這些系統無法保護檔案中的資料，這些檔案內的重要資訊可能會遭到合法使用者的外流，因為他們具有獲得授權的存取權限。

資料外洩的 4 個途徑

以下是資料大幅遺失或遭竊的 4 個主要途徑：

A. 內部人員竊取資料
在此情況下，看似合法的使用者竊取了資料。

B. 特權使用者竊取資料
特權使用者能夠存取大量的資料，且較容易導致資料外流。

C. 駭客駭取資料
駭客時常透過遭竊或購買的使用者憑證、惡意軟體或網路漏洞駭取資料。

D. 人為錯誤
人為疏失在所難免，資料外洩也因此容易發生。

文件結構

根據以上 4 個資料外洩的途徑結構，我們檢視了一系列的資料竊取情境。這些情境皆使用了相關技術，能夠避開現有網路安全工具對於防止未經授權存取資料的防護。我們將針對每個情境描述資料是如何成功外流，並介紹 SecureAge 能夠如何對抗威脅。

以資料為導向的網路安全做法

在檔案中的資訊是不受到保護的，不論是機密資訊還是智慧財產，每年遭竊或遺失的數十億筆資料記錄皆包含在檔案中，一旦從組織外流以後即完全不受保護。

SecureAge 的 SecureData 採用了以資料為導向的安全做法，透過最基本的檔案加密來保護其中的資料。相較於其他能阻止未經授權的檔案存取或是對資料選擇性保護的網路安全產品，SecureData 採取了不同的方式，以加密的形式在本質上保護檔案中的所有資料。

檔案一旦遭竊，使用 SecureData 加密的遭竊檔案，竊取方將無法為其解密，且無法進一步使用其中的資料。只有這種做法才能確保遭竊的資料得到保護，即使資料是經由獲得授權可存取的內部人員外流，外人也無法存取該資料。

資料竊取情境 A
內部人員竊取資料

1. 使用者帳號被盜

使用者的登入帳號和密碼被盜。犯罪分子在被盜的使用者筆記本電腦上進行操作，或者透過遠端或虛擬桌面存取了公司帳號。犯罪分子（也許是內部人員）因此有權限可以存取被盜帳號能夠取得的所有資料。這些資料可能包括個人身分識別資訊、智慧財產等其他敏感資料。顯然該使用者的帳號因其業務角色的需求而有權限存取這些資訊。

> 三名外國人為了竊取和出售未決併購交易的相關內線資訊，成功地滲透了兩家紐約律師事務所的網路，非法收益超過 4 百萬美元。

現有的網路安全工具會根據登入的使用者身份提供敏感資料檔案的存取權限，但無法確定存取意圖是否合法或出於惡意。檔案一旦遭竊，內容將不再受到任何保護，外人因此可以輕易存取其中的資訊。

解決方案

透過 SecureAge 的 SecureData，檔案可以隨時在所有存儲媒介上保持加密狀態。SecureData 的本質在於不干擾使用者操作，檔案在後台進行加密時使用者也不會察覺到。

即使犯罪分子登入使用者帳號後能夠查看檔案，SecureData 仍可確保在檔案被複製到新的存儲位置（例如 USB 隨身碟）後，檔案仍然會保持加密狀態。因此，檔案一旦被帶到組織外部即無法再被使用。如果有啟用token-based身份驗證，加密金鑰會儲存在token上，即使犯罪分子使用竊取來的憑證登入，在沒有token的情況下也將無法查看檔案內容。

2. 使用者從應用程式中擷取資料

合法使用者將應用程式資料複製或匯出到本機檔案中。在此情況下用，應用程式本身的安全性將不再適用，因此新檔案中的資料將不受保護，並容易遭到竊取。

> 英國威廉莫里遜超市公司的一位資深稽查員出於個人恩怨，洩露了約 10 萬名員工的工資資料，試圖損害公司運作。

解決方案

SecureData 內建的檔案層級加密在檔案建立時便默默進行加密，進而在檔案的整個生命週期中維持保護狀態。如果將資料從應用程式複製或匯出到新的或現有的檔案中，系統會就地將檔案加密，即使被授權使用者帶回家中處理，檔案還是受到保護。然而，該檔案在組織外部將無法解密。

其他檔案加密產品是依賴使用者主動決定是否要進行加密。有的是根據指定狀態來加密檔案的資料類別的作法，或是像 Microsoft EFS 會直接對檔案或資料夾進行加密。無論哪種方式，讓使用者自己做出相關決定都是有風險的，因為（一）他們可能不知道做出的選擇會為隱私和安全性帶來哪些影響，並且（二）他們做的選擇可能只是基於便利性而非安全性。

3. 資料庫日誌檔和暫存檔遭竊

包含敏感資訊的資料庫日誌檔或暫存檔案被複製到 USB 存儲裝置上，由於不被權限管理軟體歸類為重要檔案，日誌檔和暫存檔因此不會受到保護。此外，非結構化檔案以及日誌檔和暫存檔不受資料庫透明資料加密 TDE（Transparent Data Encryption）產品的保護，因此該技術不能阻止資訊被竊取的問題。

> Peekaboo Moments 應用程式的開發商 Bithouse Inc.未成功保護超過 7,000 萬個日誌檔案，其中包括電子郵件地址、地理位置資料、行動裝置的詳情資料以及照片、影片的連結等資訊。

解決方案

SecureData 透過對每個存儲位置中的所有檔案加密，可確保所有資訊都受到完整保護。如此一來，任何遭竊的日誌檔或暫存檔都將維持加密且無法使用。除了資料庫以外，許多應用程式都會產生包含可能有敏感資訊元素的暫存檔，例如 Microsoft Office 系列的應用程式。

權限管理或分類解決方案會將暫存檔案和日誌檔視為不重要的檔案資訊。但是，它們通常包含主要檔案中的許多資料。SecureData 無縫加密檔案的做法對使用者和應用程式都是透明的，不會因為資料進出記憶體且通過加密引擎進出而對性能造成影響。此外，它在 CPU 中使用 AES-NI 指令集可確保加密流程比 I/O 更快。

4. 無效的第三方安全性

處理敏感資料的第三方合作夥伴公司或顧問方無法對資訊保有充分的安全性，由於第三方無法獲得您的控制與持續監督，因此極有可能會造成資料遺失。

> Nedbank 與第三方服務提供商發生的安全漏洞事件影響到 170 萬筆客戶資料。儘管資料是透過 SSL/TLS 傳送到第三方，卻未以加密的形式儲存。

解決方案

強制要求第三方使用 SecureData 可避免此問題。如此一來，任何從第三方或顧問方竊取的資料都將被加密，無法使用。除了佈署 SecureData 之外，由於檔案加密技術的低調性質，第三方的工作也不會受到影響。您的資料將保持加密狀態，但可以根據需要加以存取、修改和管理。

透過安全管理伺服器（Security Management Server），您可以持續掌握第三方端點資料的使用情形，還可以使用加密金鑰確保資料的持續掌控，並且可以透過安全管理伺服器變更適用的策略來撤銷對資料的存取權限。

資料竊取情境 B

特權使用者竊取資料

5. 特權使用者存取未經授權的檔案

特權使用者運用個人的存取權限來竊取檔案（包括他們不應看到的資料）。如果某一方因職務需求擁有對檔案的合法存取權限，他即有可能竊取檔案。

管理員擁有管理檔案的權限，例如將檔案從一個伺服器移至另一個伺服器，或者是還原備份，這種權限通常意味著他們也可以看到這些檔案的內容。儘管您可以透過稽核日誌登錄和監視來了解事件發生後的情況，但是仍無法防止資料遭到竊取。

> 愛德華•斯諾登 (Edward Snowden) 利用其管理員的身份從美國國家安全局成功竊取約 170 萬份文件。

解決方案

SecureData 按照每位使用者的檔案層級做加密，因此，只有獲得授權的使用者才能為檔案解密。管理員仍然擁有移動檔案和管理的權限，但是他們不能解密和存取檔案內容。在這種情境下，特權使用者仍然可以執行工作，但是他們無法查看管理的檔案內容。此外，當有檔案解密失敗時，SecureAge 安全管理伺服器皆會記錄下來。

6. 管理員從備份中竊取檔案

特權使用者存取備份媒介並竊取包含智慧財產的檔案，管理員必須有對備份媒介內容的存取權限，才能在需要時還原檔案。備份經常受到加密保護，但管理員需要有存取備份的解密金鑰才能還原備份的檔案。

> 駭客透過錯誤留在 GitHub 儲存庫的憑證取得 Amazon 網站伺服器的存取權限，導致數百萬筆 Uber 用戶資料遭竊，被竊的檔案內包括了客戶資料的備份。

解決方案

透過 SecureData 按照每位使用者的檔案層級加密，所有備份中的個別檔案都會被單獨加密。

管理員仍然可以從備份媒介中還原這些檔案，但他們不能解密和存取檔案內容。

資料竊取情境 C
駭客駭取資料

7. 惡意軟體

內部人員成功將惡意軟體佈署在您的網路上，或是內部使用者成為網路釣魚攻擊的受害者。惡意軟體在休眠一段時間後，再將其找到的資料洩漏出去，最後再將所有內容加密，並要求贖金贖回資料。社交工程、魚叉式網路釣魚、深度偽造等技術日漸成熟複雜，因此防詐教育也無法保證忙碌的專業人士不會錯誤點擊到有害的連結，或打開惡意文件。

> 受到勒索軟體的攻擊後，長達好幾個星期的時間，Travelex 的業務流程不得不退回人工處理。不僅商務客戶無法提供貨幣服務，消費者的荷包更是失血。據報導，該公司的客戶資訊也因此遭竊。

惡意軟體的設計是基於利用技術與人性弱點，規避企業防護線控制和內部安全措施。取得存取權限後，檔案滲透便很容易。此外，只要成功一次後，駭客就可以再進行成千上萬次的攻擊。然而，組織卻必須抵禦所有駭客的攻擊。

解決方案

未經授權的惡意軟體程式在網路上的存在令人十分不樂見。即便如此，SecureData 還是能確保所有遭竊的檔案都是保持加密的狀態，讓攻擊者發現偷來的檔案毫無用處。此外，SecureAge 的 SecureAPlus 也是一款結合應用程式控制和白名單功能的工具，可以確保只執行經授權的程式，即使是授權使用者也無法啟動惡意軟體。

如果使用者不小心點擊到有害的連結或檔案，無論是執行檔、無檔案攻擊、指令碼還是巨集相連的惡意軟體，都會被封鎖且無法執行，因為該程式不在授權的程式清單中。在此情境下，使用 SecureAge 產品將確保任何資料竊取和擾亂組織的行為都無法成功。

8. 使用者帳號被盜

外部人士使用竊取的使用者憑證遠端存取目標網路，並在自己的機器上操作。在這種情況下，外部人士可以存取被盜使用者的帳號，並且能夠取得的所有檔案，這些檔案便很容易從企業網路被複製到外部人士的桌面上。

> 在一次資料外洩事件中，魁北克近 36 萬名老師的個人資料遭到外流。駭客竊取了一名使用者代碼和密碼，進而存取資料並加以竊取。

解決方案

使用 SecureData，儘管外部人士可以存取被盜的使用者帳號，但無法有機會存取使用者的加密金鑰。由於 SecureData 能夠確保隨時為所有檔案進行加密，因此外部人士無法對任何檔案解密。由於 SecureAge 安全管理伺服器（Security Management Server）會收集稽核資料，任何將檔案（已加密）複製到外部的動作都會記錄在日誌檔內，能夠用於任何將來對不成功的數據竊取嘗試進行鑑識分析。

9. 檔案分類錯誤

使用者對敏感文件錯誤分類，將導致對資料的保護不足。自行分類資訊時，使用者可能會因為對隱私和資訊安全後果的誤解而作出錯誤的分類決定。自動分類工具可以掃描檔案，然後根據其內容進行分類。但是，這些系統的有效性取決於其配置。如果沒有掃描所有儲存的資料，或者資料匹配過濾器不周全，那麼分類錯誤將成為一個存在的問題。

請務必知道，今天的「普通」資料可能成為明天的「敏感」資訊，看似不重要的資訊也可能會遭受濫用。這會讓針對網路安全進行分類規則的配置，變得十分困難。

> Gekko Group 是歐洲首屈一指的飯店預訂平台，由於資料庫的安全性不周全，洩露了超過 1TB 的顧客、客戶和合作夥伴資料，使他們落入帳號接管、身份盜用和財務欺詐的風險之中。

例如，在 Facebook 外洩 5,000 萬個帳號的事件中，那些看似無害的資料可能會被用來破解安全問題、建立假帳號並詐騙使用者。資料分類在許多方面很有用，但將其作為安全措施卻有待商榷。

解決方案

SecureData 的透明檔案層級加密可以保護所有檔案，透過專門的設計，不會干擾使用者或應用程式的運作。由於所有檔案都經過加密，您不必再擔心某些資料會因分類錯誤或未分類而變得不安全。

資料竊取情境 D
人為錯誤

10. 雲端資料庫不再安全

雲端服務中的資料庫，有些並沒有正確地做好安全設定。有許多媒體報導指出，雲端資料庫沒有受到安全保護。無論是已經正式上線的環境或是開發環境中的資料庫，都容易發生安全方面的人為錯誤。無論是在什麼情況，以這種不安全的方式儲存敏感資訊時常會導致資訊遭竊。

> Desjardins Group 的一名不良員工使用其合法使用者憑證竊取了大約 290 萬筆顧客帳號資料等記錄。我們推斷該系統有安裝 DLP （資料外洩防護），但卻未能偵測到此類敏感資料被匯出。

解決方案

使用 SecureData 時，資料庫內的所有檔案都會經過加密。如果這些檔案遭受盜取，將不會導致任何資料的遺失，由於這些檔案持續保持加密狀態，因此對竊取資料的人士來說是毫無用處。

儘管透明資料加密 TDE 之類的資料庫加密解決方案也可以減輕資料庫檔案的竊取問題，但是這些系統既不會加密關聯的非結構化檔案，也不能加密日誌檔、暫存檔和報告檔。使用了 SecureData 後，所有這類的檔案都將自動加密。

11. 雲端儲存裝置配置錯誤 / 誤用

雲端服務被用於文件儲存和管理，雲端基礎架構的配置不正確，造成安全漏洞。駭客或惡意內部人員可以利用基礎架構配置的錯誤來存取和竊取檔案。

另一個問題是，雲端服務提供商有他們自己的系統管理員，他們有可能有權限存取您的檔案。GDPR 或 CCPA 等資料保護法規規定，相關人士必須獲得必要的存取權限，以處理個人身份識別資訊。雲端管理員是無需查看此類的資料。

> 一名 Amazon 工程師竊取了儲存在 AWS 中的 1 億筆 Capital One 顧客記錄。他藉由配置錯誤的防火牆，遠端存取 700 多個資料夾的資料。這樣的竊取行為持續了足足 4 個月。

解決方案

SecureData 按照每位使用者、檔案等級加密的功能，
確保所有資料都予以加密。如果我們考慮使用像 OneDrive 或 G-Drive 這樣的資料複製服務，那麼可以使用 SecureData 將檔案加密儲存在本機系統磁碟機上，複製到雲端的副本也會被加密。SecureData 的檔案加密可確保應用程式在運作期間，唯一未加密的資料就是只有在記憶體中操作的資料。

這意味著內部人員、雲端管理員或外部攻擊者竊取的檔案將會保持加密狀態，對竊取資料的惡意人士並沒有用處。此外，雲端管理員也無法查看檔案的內容。

12. 從 BitLocker 保護的虛擬桌面伺服器中竊取的檔案

提供虛擬桌面服務的伺服器已啟用 BitLocker，以確保對磁碟上的所有資料進行加密，檔案卻被內部人員竊取。

像 BitLocker 的全磁碟加密（FDE）功能僅在未運作的系統上有效。BitLocker 的即時系統以未加密的形式，將所有資料傳遞給請求它們的所有處理程序–無論是合法或是惡意。FDE 非常適合保護遺失的筆記型電腦上的資料，但有時候使用是為了讓「是否已佈署加密？」 勾選框可以被勾選並生效。FDE 在一直運作的伺服器上是沒有效用的。由於文件以未加密的方式傳遞，因此惡意員工、被盜的使用者帳號或特權使用者可以輕鬆地竊取他們在系統上可以找到的任何資料。

> MGM 飯店的 1,060 萬筆房客詳細資料遭人在駭客論壇上發佈。這些資料是透過未經授權存取的雲端伺服器收集而成，可想而知，該伺服器早已啟用全磁碟加密（FDE）功能。

解決方案

SecureData 固有的檔案金鑰加密可保持持久性加密，只有在授權人員使用其加密金鑰存取時才會解密資料。即便如此，磁碟上的資料也會始終保持加密狀態，即使複製到其他位置亦同。由於加密 / 解密過程是透明的，因此使用者（和應用程式）並不知道此作業。這是檔案級加密成為實用安全解決方案的關鍵原因。

結論

我們討論了一系列的資料盜竊場景及相關案例報導。在每種情況下，資料都可以成功遭到利用，因為資料一旦被盜並且在組織的控制結構之外，被竊取的檔案內容即不會受到保護。

如果檔案遭到竊取，有了 SecureAge SecureData，竊取者完全無法存取資料內容。如果要緩解資料洩露造成的損壞，讓遭到竊取的資料在組織外變得毫無用處是一個有效方法。包括法規、品牌損害、法務、業務復原等，SecureAge 的做法可確保知識財產權、敏感和機密的資訊不外洩。每一份文件隨時隨地都受到保護，不論每次以任何方式操作文件，都能讓文件保持受保護的狀態。

SecureAge Technology

總部位於新加坡的 SecureAge Technology 是一個真正同時將安全與實用並列，提供資料安全解決方案的公司。SecureData 以 PKI 的安全技術為改進基礎，於 2003 年首次推出供新加坡政府使用。SecureAge 將以 PKI 為基礎的專利加密技術做為資料保護固有且無形的一部分，很快就成為其他政府機關和公共單位的首選資料加密合作夥伴。這些長期和高度整合的關係為 SecureAge 帶來了保護大型複雜組織資料的豐富經驗。

SecureAge 的資安解決方案讓公共單位與私營企業能夠全面掌握網路內部的資料移動，使他們能夠在任何時間、任何位置掌控任何文件。

SecureAge 的資安產品是需要最高等級資料保護的組織首選。我們的客戶包括新加坡、香港和日本政府的多個機構，英美煙草公司、索尼、成田機場技術公司、泰國政府儲蓄銀行和 GRG 銀行等，都是我們的擁護者。

SecureAge Technology: 掌握資安的作法

主動保護，亦即：

資料安全性

資料安全性意味著全面性的加密。資料應以最基本的獨立單元形式進行保護，也就是檔案。其他競爭廠家的解決方案有時僅能保護部分資料，其關注的是法規遵循而非安全性，或是會增加風險的複雜性。由於使用者（也是任何系統中最易受攻擊的部分）已經在內部，因此僅靠外圍防禦措施是不夠的。

應用程式完整性

應用程式完整性就是將白名單和資料綁定到應用程式以進行控制，只有經授權的處理程序才能為特定目的存取特定的資料。傳統的反惡意軟體系統代表被動保護，並且過於緩慢。他們專注於先前已知的惡意軟體，並試圖阻止已經啟動的惡意處理程序。

可用性

可用性意味著固有和無形的技術。解決方案應該完全消除人為因素，而不是試圖解釋或改變它。培訓和監控並非永遠有效，如果解決方案不符合自然需求，人們將自創（非安全的）替代方法。使用者應該能夠按照自己的意願或需要來工作，也不需要有額外的顧慮與考量。

沒有權衡取捨

對 SecureAge 來說，這些原則之間不應有權衡取捨，可用性更不應該為了要增強資料的安全性而犧牲。SecureAge 產品設計的基本原則是：當「正確」的方式不容易被遵循時，人們就會尋找其他的替代方式。

進一步了解

如果您想更加了解 SecureAge 的企業資訊安全解決方案，歡迎與我們聯絡。我們很高興能與您分享 SecureAge 改善資安問題的方法，並為您安排免費試用。

歡迎參閱網站 www.secureage.com

SecureAge

新加坡 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
英國 74 Mackie Avenue, Brigton, BNI 8RB, 公司編號 11734665
日本 1-16-6, Toranomon, Minato-ku, Tokyo 105-0001, Japan
北美 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA
台灣 2F 32 Dong-Mem Street, Banqiao District 22055 New Taipei City, Taiwan