資料外洩防護的最佳做法

白皮書

ENDPOINT PROTECTOR by CoSoSys

Protecting your entire network

目標

資料外洩防護 (Data Loss Prevention, DLP) 工具已成為資料保護策略中不可或缺的一部分。
高度彈性且適用於任何公司規模的 DLP 解決方案可以根據不同需求量身訂製，並能夠遵循新的資料保護法規運作。

本白皮書概述了公司在實施 DLP 工具時應採用的最佳做法。

背景與資料外洩防護的重要性

在現今，幾乎所有企業都保留數位記錄。從會計到市場營銷，以及基本的溝通，都在電腦和網際網路上進行。這也意味著每家公司，無論其規模大小，都會收集包括受法律保護的敏感類別在內的數位資訊，例如涉及員工、客戶或合作夥伴的個人資訊。

隨著安全漏洞和不同的網路犯罪事件不斷增加，數據被開採、獲利和轉售，不僅客戶感到愈加煩惱和憤怒，這些事件還給處理敏感數據不當的企業造成了聲譽、財務和法律損失。

因此，在當今世界，強調數據安全是每個組織的一個至關重要的因素和重大挑戰，受到更嚴格的監管和嚴厲的數據損失後果。

資料外洩防護（DLP）解決方案已成為企業網路安全策略的核心組成部分，因為它們有助於確保敏感或關鍵的業務資訊不會離開公司網路，也不會發送給未獲授權的用戶。通過DLP軟體，公司可以防止資料被竊取、遺失和外泄，同時在資料保護過程中起到作用。通過實施這類解決方案，企業可以更好地識別、管理和保護有價值的業務資訊和資產。

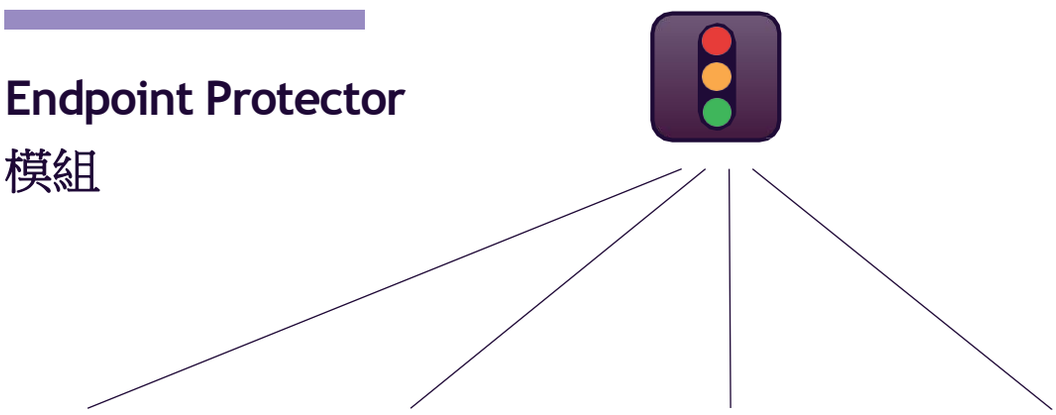
DLP解決方案帶來多項好處，幫助企業實現以下目標：

- 緩解內部威脅
- 保護知識財產權（IP）
- 保護客戶數據
- 確保法規合規性

為何使用Endpoint Protector DLP?

CoSoSys的Endpoint Protector是獲得多項殊榮的DLP解決方案目標是幫助企業保護敏感數據，阻止數據洩漏和數據竊取，最大程度地減少內部威脅，同時保持生產力，使工作更加便利、安全和愉悅。

Endpoint Protector 模組



Device Control

USB和周邊端口控制

鎖定、監控和管理設備。

根據供應商ID、產品ID、序列號等的精細化控制。

內容過濾保護

掃描在傳輸中的數據

監控、控制和阻止檔案傳輸。

透過內容和前後文檢查進行詳細控制。

強制加密

自動USB加密

加密、管理和保護USB存儲設備，通過保護傳輸中的數據。

根據密碼，易於使用且效率高。

eDiscovery

靜態數據掃描

探索、加密和刪除敏感數據。

通過手動或自動掃描執行詳細的內容和前後文檢查。

Endpoint Protector Enterprise

Endpoint Protector Enterprise 企業版解決了企業面臨的複雜資料保護策略挑戰。選擇我們的解決方案，企業可以保護個人身份資訊（PII）或知識產權（IP）等敏感類別的數據，減輕內部威脅，並滿足數據保護法規的要求，例如《歐盟通用數據保護規則》（GDPR）、《加利福尼亞消費者隱私權法》（CCPA）、《1996年健康保險可攜性和責任法案》（HIPAA）或《支付卡行業數據安全標準》（PCI DSS）。

Endpoint Protector Enterprise融合了安全性和靈活性，有助於滿足大規模數據保護的當前要求。它提供以下功能：

增強的擴展性和靈活性

Endpoint Protector Enterprise確保在不影響生產力的情況下，保護一萬個或更多的端點。

通過產品的細緻且靈活的政策，可以滿足每個部門的特定需求，而無需將相同的政策應用於整個公司。

跨平台保護

使用Endpoint Protector Enterprise，安全政策可以在實體和虛擬環境中得到相等的執行。

我們的多操作系統解決方案為Windows、macOS和Linux端點、精簡型電腦（Thin Client）以及桌面即服務（DaaS）平台提供了保護。

無縫整合

Endpoint Protector Enterprise可以輕鬆整合到企業的生態系統中，並支援分佈式部署。

這個套裝方案確保與Active Directory (AD) 和SIEM技術的整合。

對於macOS零日支援

當客戶升級到最新的macOS版本時，他們可以立即獲得對新的Endpoint Protector功能的支援，而不會延遲或對關鍵工作流程造成影響。

無KEXT代理和蘋果已經簽名的核心擴展

Endpoint Protector是市場上首家具備無KEXT代理並獲得對未來macOS版本的全面支援的DLP供應商。除此之外，Endpoint Protector的所有其他macOS客戶端版本都符合蘋果的驗證要求。

確保資料安全的最佳作法

DLP解決方案已成為資料保護策略中不可或缺的一部分。高度靈活且適應各種公司規模，它們可以根據不同需求進行定制，並支援符合新的資料保護法規，如GDPR或CCPA。

我們整理了一份最佳作法清單，將幫助企業在DLP選擇過程中，確保高效的資料保護策略。

識別並監控敏感資料

企業必須識別他們收集的敏感資料類型、它們儲存在哪裡以及員工如何使用它。

DLP工具提供了預設的敏感資料配置文件，同時允許企業根據自己的需求定義新的配置文件。

透過啟用數據監控，企業可以了解數據在內部和外部網路中的流動情況。這有助於發現數據處理中的漏洞和員工之間的不良安全操作。

實施跨平台的DLP解決方案

macOS和Linux正在逐漸趕上Windows，組織在選擇DLP工具時不應忽略它們。

像Endpoint Protector這樣的跨平台DLP解決方案在Windows、macOS和Linux之間提供了相同功能，這意味著無論電腦運行的作業系統是什麼，敏感數據都將獲得相同級別的保護。

它還允許從同一個儀表板控制公司網路上的所有端點。

建立策略並測試它們

為了控制所識別的敏感資料，DLP工具為企業提供了各種預設的規則和策略，可以在整個公司網路中執行。

這些規則和策略可以阻止敏感資料通過可能不安全的渠道進行傳輸，例如通訊應用程式、檔案共享和雲端服務。

它還可以限制敏感資料通過電子郵件發送給哪些人。

對於靜態資料，DLP解決方案允許企業在發現未經授權的電腦上出現敏感資料時刪除或加密該數據。

控制能夠連接到企業端點的設備

資料不僅可以通過互聯網洩漏，還可以通過使用可移動設備洩漏。

企業可以使用DLP解決方案來阻止設備上的USB和外接設備端口，或僅允許白名單設備連接。

強制加密也可以確保如果使用USB，所有傳輸到其中的檔案都會自動加密，只有密碼的使用者才能訪問這些檔案。

設定不同層級的授權

根據員工的職權和所屬的群組，應該限制對敏感資料的訪問和使用。

DLP工具允許管理員根據個別用戶、設備、群組或部門，在公司網路中設定不同層級的授權。

這樣一來，企業可以確保不常接觸敏感資料的員工對其有限制或無訪問權限，同時不妨礙那些日常處理敏感資料的人的工作。

建立遠程工作的DLP政策

許多組織在保護公司網路方面投入了大量資源，但一旦電腦帶回家，其中儲存的敏感資料就可能面臨遭到侵害的風險。

因此，建立遠程工作政策時應包括DLP工具，確保在公司網路之外，不論設備是否在線上，數據都會得到保護。

這樣一來，無論公司電腦前往何處，數據都能持續得到保護。

對員工進行DLP和資料安全教育

員工理解DLP工具的必要性、最佳安全作法以及資料外洩的後果至關重要。

企業可以利用DLP數據監控的結果提高對不良作法的認識，幫助員工進行改進。

對DLP重要性的理解也可以防止員工嘗試規避政策，重要的是向管理員報告可能遇到的任何問題，管理員才可以相應調整DLP政策以提高整體效率。

CoSoSys的Endpoint Protector用戶評價

4.6

產品能力

4.5

部署和整合

90%

會推薦
Endpoint Protector

過去 12 個月的評價

4.6

評估和承包

4.3

服務和支援

Gartner peerinsights™

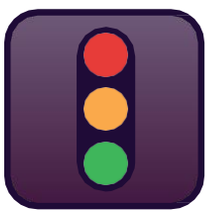
在Gartner Peer Insights 企業資料外洩保護解決方案中獲得高度評價。

總結

每年的網路攻擊數量都在增加，隨著相關法規的增多，資料保護已成為每家公司安全策略中不可或缺的一部分。資料洩露本身可能帶來災難性後果，且通常會伴隨著高額罰款、品牌損害和客戶信任流失。

DLP解決方案在受到組織青睞，因為企業正尋求降低涉及敏感資料的風險，包括資料丟失、盜竊和濫用。為了符合GDPR、CCPA、PCI DSS或HIPAA等法規要求，為了減輕內部威脅，保護知識產權和客戶資料，應當實施一個最優質的DLP解決方案。

.



關於 Endpoint Protector

Endpoint Protector by CoSoSys是一個先進的全方位DLP解決方案，支援Windows、macOS、Linux和Thin Clients，它可以防止資料外洩，保護免受惡意的資料竊取，並無縫控制移動式儲存設備。
它具有對靜態和傳輸中的數據進行內容過濾的功能，範圍涵蓋了基於字典、正則表達式的預定義內容，以及符合GDPR、CCPA、PCI DSS、HIPAA等數據保護法規的配置文件。

EndpointProtector.com

EndpointProtector.com

COSOSYS

HQ (Romania)

sales@cososys.com
+40 264 593 110 / ext. 103
+40 264 593 113 / ext. 202

Germany

vertrieb@endpointprotector.de
+49 7541 97826730
+49 7541 97826734 / ext. 202

North America

sales.us@endpointprotector.com
+1 888 271 9349
+1 877 377 6475

South Korea

contact@cososys.co.kr
+82 70 4633 0353
+82 20 4633 0354