

Acronis Cyber DeviceLock DLP

主機端資料外洩防護

唯一專為客戶設計的 DLP 解決方案，藉由自動化、客戶特定的 DLP 原則建立防止敏感資料透過週邊裝置和網路通道外洩。



讓您的 DLP 服務從競爭中脫穎而出

目前的 DLP 解決方案需要成本高昂的安全性專業經驗和客戶業務流程的深入知識，以及複雜、容易出錯、手動設定來確保客戶特定的原則。有了 Advanced DLP，您可以您需要的佈建速度和原則管理簡易性阻止客戶的資料外洩。

全方位大量受控通路

控制本機與網路通道的資料流，包括卸除式儲存裝置、印表機、重新導向的已對應磁碟機與剪貼簿、電子郵件與 Web 郵件、即時訊息、檔案共用服務、社交網路以及網路通訊協定。

透過單一主控台集中式網路防護

使用整合備份、災難復原、下一代防惡意軟體、電子郵件安全性、工作負載管理與資料遺失防護的單一解決方案，控制您的 TCO、減少管理開銷並提高利潤。

客戶特定的 DLP 原則

監控組織的傳出敏感資料流以將客戶的業務流程自動對應至針對客戶規範調整的 DLP 原則。利用最佳使用者協助實現更高準確度，並在執行原則之前請求客戶驗證。

無可比擬的 DLP 控制措施，讓您的服務脫穎而出

確保網頁瀏覽器獨立控制資料傳輸至社交媒體、Web 郵件和檔案共用服務。利用傳出即時訊息的內容檢查以及對於遠端和離線電腦上的影像的敏感資料偵測。

Acronis Cyber DeviceLock DLP Core

主機端資料外洩防護-設備連接 Port 控管

內容感知和上下文感知的 DLP 控制

防止敏感資料從客戶的組織中外洩。Advanced DLP 將偵測每次資料傳輸的寄件者、收件者、使用的通道和敏感內容，以套用原則型預防 DLP 控制措施。

封鎖覆寫支援

透過提供一次性業務相關例外來允許一般使用者在特殊情況下覆寫資料傳輸封鎖，確保客戶業務的持續性。

適應性 DLP 原則強制執行 (強制執行模式)

透過向使用者學習來實現強制執行的 DLP 原則的自動擴充。適應性強制執行選項是對新資料流的強制執行原則的自動化、使用者協助的延伸。

針對週邊裝置的資料流的內容感知控制

控制客戶組織內針對印表機、卸除式儲存裝置、已對應磁碟機等週邊裝置的資料傳輸，確保使用中的敏感資料不會經由此類本機通道外洩。

遠端連線的剪貼簿控制

透過重新導向的剪貼簿在公司電腦和 BYOD 裝置或遠端終端機之間傳輸資料時就提高警覺，在最初階段就防止資料外洩的風險。

即時警示

針對相關的 DLP 事件提供原則型即時警示，以增加 DLP 管理員的可見性並讓他們及時回應重大的安全事件。

加密卸除式儲存裝置支援

透過消除敏感資料經由未加密的卸除式儲存裝置 (例如 USB) 離開用戶端工作負載的風險, 更好地保護客戶資料。Advanced DLP 可以偵測加密的卸除式儲存裝置, 並僅允許將資料傳輸至這些裝置。

報告

藉由資訊豐富的小工具向客戶展示您的服務價值和簡化法規遵循報告, 這些小工具針對可輕鬆以報告形式傳送至客戶之可行資料外洩防範統計資料提供了清晰檢視。

DLP 事件檢視器

藉由具有快速搜尋和篩選功能、針對所有 DLP 事件的單一平台檢視, 增加服務技術人員的效率。

針對一般使用者的螢幕上通知

藉由說明特定資料傳輸被 DLP 規則阻止之原因的互動式螢幕上警告, 提高一般使用者的資料外洩防範意識, 減少 IT 管理員在調查上耗費的時間。

Acronis Cyber DeviceLock DLP ContentLock 主機端資料外洩防護-機敏內文辨識控管

預先建置的資料分類器

藉由針對個人可識別資訊 (PII)、受保護的醫療資訊 (PHI)、支付卡資訊 (PCI DSS)、「標記為機密」的文件之預先建置的資料分類器, 保護客戶的敏感資料立即可用。

自動化 DLP 原則建立 (觀察模式)

盡量減少手動工作, 並將出錯的風險降至最低, 透過針對每位客戶自動產生初始 DLP 原則來簡化佈建, 簡化服務佈建和初始 DLP 原則設定。該解決方案將觀察使用者的行爲來自動將客戶的業務細節對應到 DLP 原則, 以此建立客戶特定的 DLP 原則。

內容檢查和篩選

針對透過本機和網路通道傳輸的資料分析及篩選文字和二進位內容 (包括內嵌封存檢查), 以防洩露客戶的敏感資料。可從針對 100 多個檔案、40 多個封存以及五種列印格式的文字剖析中受益。

Acronis Cyber DeviceLock DLP NetworkLock 主機端資料外洩防護-L7網路應用層機敏辨識過濾

網路通訊控管

控制透過電子郵件、雲端檔案共用服務、Web 瀏覽器以及社交媒體等網路通道的資料傳輸。防止客戶組織內使用中的敏感資料外洩。

嚴格 DLP 原則強制執行 (強制執行模式)

對於要求進行更嚴格控制的客戶, 您可以在定義 DLP 原則時強制執行它們, 還可以阻止觀察模式期間沒有觀察到的任何全新的資料流。

支援平台: **Workstation / Server / VM**



Acronis

OFFICIAL CYBER PROTECTION PARTNER

Acronis 台灣總代理

北祥資訊股份有限公司

台北市內湖區文湖街 20號 2樓



pdcmarketing@pershingdata.com.tw



www.pershingdata.com.tw