DeviceLock
AN ACRONIS COMPANY

Acronis DeviceLock

全方位端點資料外洩防護（DLP）

在簡化業務程序與支援遠端工作雙重需求的推動下，資料的易用性正日漸提升。然而，隨著資料更容易被廣為存取，員工無意或蓄意將敏感、機密資訊外洩予組織外部未經授權方的風險，也因此大幅增加。

90% 的組織感到易遭受內部威脅攻擊，原因為有許多管道可能會發生資料外洩，包括透過本機週邊裝置和連接埠（例如印表機和 USB），以及經由網路途徑如電子郵件、社交網路、即時傳訊工具，或是雲端型檔案共享。如果敏感資料落入未經授權方手中，可能會導致嚴重的財務和信譽損失、商業機密損失以及高昂的違規罰款和訴訟。某些資料的存取和傳輸作業是合法的，但需要嚴加保護，確保不會因使用者疏忽造成不慎外洩。若有人威脅要與未經授權的第三方共享敏感資料，即必須全面阻止。

ACRONIS DEVICELOCK DLP

Acronis DeviceLock DLP 是一套端點資料外洩防護解決方案，能顯著降低內部相關資料外洩的風險。這套解決方案結合了內容分析與篩選功能，執行極度細緻的關聯式控制（依據使用者驗證、安全群組成員資格、資料類型、裝置類型或網路通訊協定、資料流方向、媒體狀態或 SSL 加密、日期和時間以及其他因素），以阻止或允許資料存取與傳輸作業。Acronis DeviceLock DLP 由多個具互補與特定功能的元件組成，允許客戶依據安全需求和預算選擇最佳設定。

優點

簡單：降低複雜度

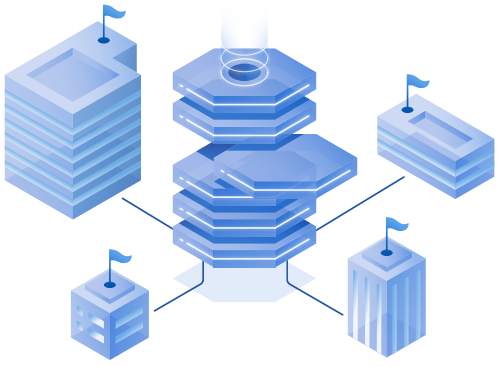
- 集中管理
- 與 Active Directory 整合
- 模組化架構 – 透過僅購買您需要的功能，將總持有成本減至最低

高效：提高生產力

- 將內部程序對應到使用者必須遵循的管理員強制原則，進而順利推動內部程序轉換
- 監控和記錄使用者活動，以利進行後期分析
- 藉由強大的報告功能提高察覺度及合規性

安全：防止資料外洩

- 透過本機和網路管道，降低內部相關資料外洩的風險
- 阻止未經授權的資料存取和傳輸作業
- 僅允許業務程序所需的合法作業



Copyright © 2002-2022 Acronis International GmbH.

Acronis DeviceLock Core

一種基本元件兼獨立產品，可在受到保護的系統上，針對本機資料管道執行細緻的關聯式控制以及事件記錄、資料陰影和警示。本機資料管道內容包括週邊裝置和儲存空間、連接埠（USB、FireWire、COM、LPT、IrDA）、連接本機的行動裝置、重新導向連接埠、遠端終端機對應的磁碟機、螢幕截圖和剪貼簿作業。對於其他功能模組，Acronis DeviceLock Core 也提供了基礎平台以及所有集中管理和系統管理元件。

Acronis NetworkLock 附加元件

一款 Acronis DeviceLock Core 的選用附加元件，可依深度封包檢查（DPI）對網路通訊（包括 Web、電子郵件、即時傳訊工具、雲端儲存服務、檔案共享、網路通訊協議等）提供關聯式控制。DPI 型的控制不限於在受保護電腦上執行的特定應用程式或瀏覽器，它也允許控制來自任何 Web 瀏覽器、任何 SMTP 電子郵件用戶端、任何 FTP 用戶端以及任何 Torrent 代理程式的流量。Acronis NetworkLock 的連接埠獨立式通訊協定偵測以及完整的工作階段資料重建和擷取，皆允許靈活的篩選、事件記錄、警示與資料陰影。

Acronis ContentLock 附加元件

一款 Acronis DeviceLock Core 的選用附加元件，可針對傳輸到卸除式媒體和隨插即用裝置的文字和二進位內容，以及來自網路通訊、由 NetworkLock 和 DeviceLock Core 重建並傳遞給該元件的各種資料物件，實施分析和篩選。內容分析引擎可擷取超過 150 種檔案格式和資料類型的文字資料，然後套用有效、可靠的內容篩選方法。結構化資料的內容會依據預建的規則運算式（RegExp）模式範本和產業專用的關鍵字字典（HIPAA、PCI 等）進行偵測，而非結構化文字和二進位內容則通常採用資料指紋偵測。Acronis ContentLock 也可以識別以及依據 Boldon James Classifier 產品指派給文件和檔案的分類標籤進行篩選。此外，該模組含有內建的光學字元辨識（OCR），可偵測跨存於檔案、螢幕截圖、文件和電子郵件中超過 30 種圖表格式的影像型文字內容。

Acronis User Activity Monitor（UAM）附加元件

一款具有監控使用者活動功能的選用附加元件，可將使用者在螢幕上的動作、按鍵輸入內容擷取為影片，並取得錄製時使用者在電腦上執行的應用程式相關資訊，以便進行證據收集、安全調查和稽核。安全管理員可以透過內建的檢視器，查看及分析錄製的使用者活動。

Acronis DeviceLock Discovery

一款單獨的功能元件，針對組織整體 IT 環境中的公開敏感待用資料，提供察覺度與防護。自動掃描位於網路共用、儲存系統、Elasticsearch 資料庫和 Windows 端點上的資料，尋找含公開敏感內容的檔案，並提供含修復措施的保護選項。Acronis DeviceLock Discovery 還可以啟動事件管理程序，對安全資訊和事件管理（SIEM）系統或組織中的 IT 安全人員發出即時警示。

Acronis DeviceLock Search Server（DLSS）

一款選用的附加元件，可對集中陰影處理和事件日誌資料庫中的資料，進行索引與全文搜索。Acronis DLSS 的開發目的是讓資訊安全合規性稽核、事件調查以及鑑定分析等勞力密集型的程序，能更加精確、方便與省時。

集中管理

Acronis DeviceLock DLP 是為了簡化勞力密集型、耗用資源的部署與管理 DLP 解決方案程序而開發。它提供一組靈活的集中管理主控台（依管理員需求），不僅具有相同的 GUI 外觀，同時可依任何組織（從小型到大型企業）的需求量身打造：

Active Directory（AD）環境

Microsoft 群組原則管理主控台的自訂 MMC 嵌入式管理單元，是 Acronis DeviceLock DLP 最廣為使用的管理主控台。這種原生整合模式可採用現有 Active Directory 安裝中的群組原則，對 Acronis DeviceLock 代理程式進行部署與全面管理，無須單獨的 DLP 原則伺服器或管理平台。

非 Active Directory 環境

Acronis DeviceLock Enterprise Server（DLES）可用於將 DLP 原則發佈到所有託管的 Acronis DeviceLock 代理程式。在這種情況下，在另一部電腦上執行的原生 Windows 應用程式 Acronis DeviceLock Enterprise Manager，即成為提供客戶全面支援的另一個管理主控台。

無目錄安裝（例如在 Windows for Workgroups 網路中）

自訂 Acronis DeviceLock MMC 嵌入式管理單元可以遠端管理每個端點上的代理程式。這個選項也用於管理 Acronis DeviceLock Discovery。

Copyright © 2002-2022 Acronis International GmbH.

ACRONIS DEVICELOCK DLP 功能

為了確保對使用中、運行中與待用的敏感資料進行全面防護，Acronis DeviceLock DLP 提供了全方位的功能，可大幅降低資料外洩風險，同時支援資訊安全性稽核以及合規性相關工作。

適用於 BYOD 裝置的虛擬 DLP

在使用領先業界的桌面和應用程式虛擬化解決方案（如 Citrix XenApp/XenDesktop、Microsoft RDS 以及 VMware Horizon View）時，防止內部資料經由 BYOD 裝置外洩。DeviceLock 在 VDI 主機或終端伺服器上執行，用於將關聯式、內容感知的端點 DLP 控制機制「遠端」至連接的裝置，藉此建立虛擬端點 DLP 代理程式，以防止未經控制的資料在工作階段與本機週邊裝置、託管應用程式以及裝置的網路連線進行交換 。

主機駐留光學字元辨識（OCR）

Acronis DeviceLock 代理程式、Acronis DeviceLock Discovery Server 和 Acronis DeviceLock Discovery 代理程式中內建的 OCR 引擎，可針對文件與圖表式檔案中的圖片，快速而準確地擷取、檢查文字資料。OCR 引擎對於本機與網路型資料流的 30 多種圖表格式，可從中識別超過 30 種語言。

防竄改

可設定的 Acronis DeviceLock DLP 管理員功能可以防止 Windows 與 macOS 上的 Acronis DeviceLock 原則設定遭竄改，即使具有本機系統管理權限的使用者也列為禁止對象。唯有透過 Acronis DeviceLock 主控台或群組原則物件編輯器指派的 Acronis DeviceLock 管理員，才能解除安裝或升級代理程式，或以任何方式修改 Acronis DeviceLock DLP 原則。

精確檔案類型控管

Acronis DeviceLock 會查看檔案的二進位內容，藉以判定確切的檔案類型（不是僅經由檔案名稱和副檔名判斷），並依據套用的原則，強制執行防止、記錄和警示操作。

剪貼簿控制

Acronis DeviceLock DLP 選擇性地控制使用者與群組存取剪貼簿中各種資料類型的物件，包括檔案、文字、影像、音訊片段，甚至是無法識別的資料類型。透過剪貼簿複製的檔案、文字以及影像中的文字資料內容，都能監視與篩選。此外，Acronis DeviceLock DLP 也可以透過 Windows PrintScreen 鍵盤功能與第三方應用程式，控制使用者和群組擷取螢幕截圖的權限。

允許清單

授權使用特定的 USB 裝置或裝置模型。為便於離線工作，可以透過發行存取碼製作臨時允許清單。允許清單列出有權存取 DVD、藍光或 CD-ROM 磁碟的使用者和群組，並以資料簽名為唯一識別。您也可以依據 IP 位址、位址範圍、子網路遮罩或是網路連接埠及其範圍，指定網路通訊的允許清單，簡化管理工作。

稽核

Acronis DeviceLock DLP 的稽核功能可用於追蹤本機電腦上指定裝置類型、連接埠與網路資源的使用者和檔案活動。這項功能可以依使用者/群組、天數/小時數、連接埠/裝置/通訊協定類型、讀取/寫入以及成功/失敗事件，預先篩選稽核活動。Acronis DeviceLock DLP 採用標準事件記錄子系統，並將稽核記錄寫入 Windows 事件日誌、DeviceLock 日誌以及含有 GMT 時間戳記的 Syslog。日誌可以匯出為多種標準檔案格式，或經由 Syslog 傳送而匯入其他報告機制或產品。DeviceLock 日誌會從遠端電腦自動收集，並集中儲存於 SQL Server 中。即使具有本機管理員權限的使用者，也無法以編輯、刪除或其他方式將設定竄改為傳輸到 Acronis DeviceLock Enterprise Server 的稽核日誌。

資料陰影處理

Acronis DeviceLock 代理程式自動收集，並經由違反 DLP 原則的序列埠、平行埠和網路連接埠列印、傳輸、複製到外部儲存裝置的鏡像資料。檔案的完整副本可儲存於供鑑定審核而填入的集中 DLP 日誌資料庫。陰影資料可依使用者/群組、天數/小時數、檔案類型和內容預先篩選，以縮小擷取與收集的範圍。稽核與陰影處理功能透過串流壓縮、服務品質（QoS）流量塑形、本機配額設定及最佳 Acronis DLES 伺服器自動選擇，達到有效使用傳輸與儲存資源的開發目標。

警示

用 SNMP、SYSLOG 和 SMTP 警示功能，對使用者於網路上受保護 Windows 端點進行的敏感活動，發出即時通知。

Copyright © 2002-2022 Acronis International GmbH.

卸除式媒體加密整合

Acronis DeviceLock DLP 對於將資料加密到卸除式媒體採用開放式的整合方法。客戶可以選擇使用最適合其安全情境的加密解決方案，包括Windows BitLocker To Go、macOS FileVault、Sophos SafeGuard、Symantec Drive Encryption、SecurStar DriveCrypt、TrueCrypt、Infotecs SafeDisk 和 Rutoken Disk 軟體產品，以及用於預先加密卸除式媒體的 Cardwave SafeToGo USB 快閃磁碟機。任何預先加密卸除式媒體在嚴格強制使用方式的情況下，都可以選擇性列入白名單。

報告

Acronis DeviceLock DLP 可以產生型式多元的報告以供合規性與資訊安全性稽核，包括：

圖表式報告

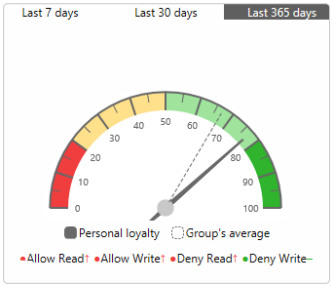
依據稽核與陰影日誌製成的圖表式報告。

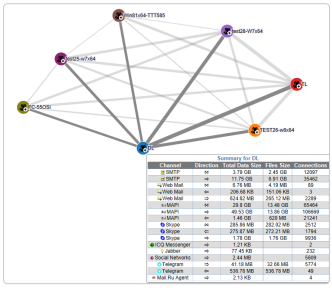
權限報告

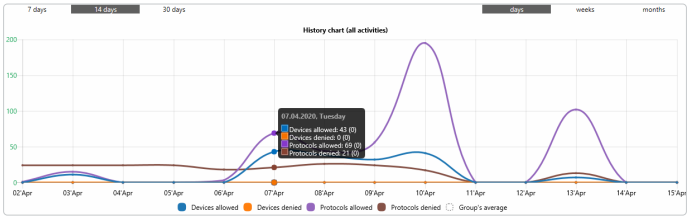
顯示對網路所有端點設定權限與稽核規則內容的權限報告。

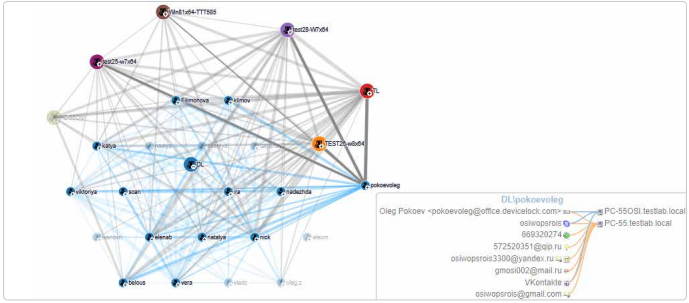
隨插即用裝置報告

隨插即用裝置報告顯示目前或以往在網路中連接端點的 USB、FireWire 和 PCMCIA 裝置。









使用者操作記錄

使用者操作記錄為依據陰影與事件日誌，在單一使用者卡片中以圖表格式呈現的使用者動作統計資料集。這些統計資料會依排程自動更新，或在伺服器負載較低的期間自動更新。使用者操作記錄包含某段指定期間內使用者活動的歷史圖表以及忠誠度儀表板，內容呈現了各種活動於報告期間與基準線期間的平均值相對偏差、在本機或網路管道中拒絕及允許作業的數量、最常見作業的資料，以及使用者通訊頻率的視覺化關係圖。

系統需求

Acronis DeviceLock Agents 和 Management Consoles

- Windows XP/Vista/7/8/8.1/10（最高支援至 21H1）/Server 2003-2019（32/64 位元）
- Apple macOS 10.15 - 11.2.3（32/64 位元）
- Microsoft RDS、Citrix XenDesktop/XenApp、XenServer、VMware Horizon View
- VMware Workstation、VMware Player、Oracle VM VirtualBox、Windows Virtual PC

Acronis DeviceLock Enterprise Server、Discovery Server、Search Server

- Windows Server 2003-2019（32/64 位元）
- Microsoft RDS、XenServer、VMware vSphere Desktop

目錄整合

- Microsoft AD（完全原生）
- NetIQ（Novell）eDirectory 任何 LDAP（物件匯入）

資料庫

- Microsoft SQL Server/Server Express 2005 或更高版本
- PostgreSQL 9.5 或更高版本

Copyright © 2002-2022 Acronis International GmbH.著作權所有，並保留一切權利。Acronis 和 Acronis 標誌均為 Acronis International GmbH 在美國及/或其他國家/地區的商標。其他所有商標或註冊商標皆為個別擁有者的財產。技術性變更與例證歧異均為保留之權利；但錯誤除外。2021-07