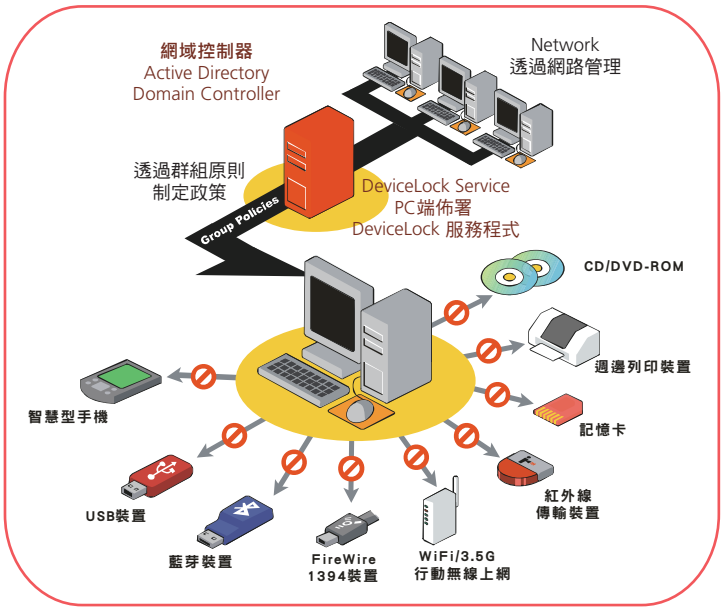
# DeviceLock®

## Proactive Network Security

## 可攜式儲存週邊裝置是資料外洩防護上最大的安全漏洞？使用DeviceLock　立即關閉它！

DeviceLock®是一套用來控管個人電腦週邊設備使用與資料外洩防護的工具軟體，系統會管制一般使用者對於電腦週邊設備的存取，杜絕員工私接隨身碟、外接硬碟、智慧手機、3G網卡、燒錄機、數位相機等可攜式儲存裝置這些可能會引起資料外洩風險的裝置。也可控管如藍牙、Wi-Fi 無線網路設備等所帶來的風險。




▲ DeviceLock　支援多種裝置管理

## DeviceLock　為系統管理者提供以下功能：

- 透過中央管理平台，依使用者、群組、時段，控管週邊設備與連接埠的存取政策。
- 根據類別（例如：可攜式儲存週邊、光碟機）或連接埠（例如：USB、藍芽、紅外線）設定存取權限，不影響如鍵盤、滑鼠等合法設備使用。
- 針對儲存裝置，透過唯讀(Read Only)的政策設定，可以讓隨身碟、外接硬碟或燒錄機變成唯讀，禁止電腦的資料複製出去。
- 對週邊的存取進行稽核紀錄並集中儲存。亦可針對允許使用的人員，將其外存的檔案陰影複製、集中備份到指定的主機，以利稽核。

## 為什麼需要建置端點資料外洩防護?

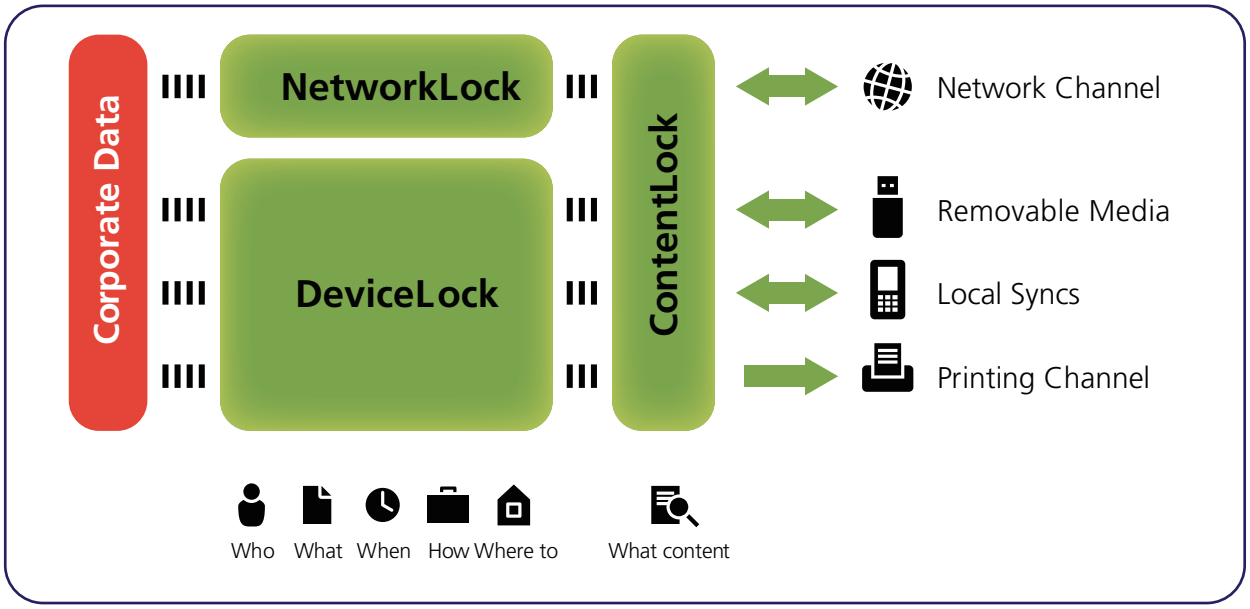
因應個資法的施行，企業對資料外洩的風險若不加以控管防護，恐將面臨嚴苛的法律責任與金額賠償。而外洩事件中，包含無心的過失以及惡意的外洩，超過80%是由於組織內部的員工導致。因此，除了惡意程式的防護之外，針對電腦的各種可攜式儲存週邊也應當實施適當的存取管控，以消弭資料外洩的風險。

如同研究機構Gartner 在其「如何解決可攜式儲存裝置的安全威脅」研究報告中指出：「漠視可攜式儲存裝置的非授權與不受控管的濫用，正促使企業逐漸將本身暴露在安全風險之中」。目前創新的週邊裝置不斷的推出，包含智慧型手機、3.5G/WiMax網卡、大容量的外接隨身碟、硬碟、記憶卡、光碟燒錄機等裝置很容易取得，且儲存容量不斷創造高峰，也對企業的資料外洩防護上帶來莫大的挑戰。

## 更多延伸功能...

### 防鍵盤側錄Anti-keylogger功能

可以偵測使用者的電腦鍵盤是否有被偷偷串接硬體式鍵盤側錄裝置。DeviceLock偵測到有這些裝置存在時，會透過專屬技術欺騙PS/2介面的鍵盤輸入訊號，使得其側錄到的指是一串無意義的亂碼。




### Network-Lock 功能 (選購)

針對端點的網路傳輸通訊進行檢查，並執行政策。該功能可以識別HTTP, FTP, IM (ICQ/AOL, MSN Messenger, Jabber, IRC, Yahoo! Messenge…), 加密的HTTPS, FTP-SSL 等通訊協定，可以依據這些協定中傳送的內容、檔案格式實施放行或阻擋的政策。也可對這些通道傳送的資訊，進行訊息重組與側錄。

### Content-Lock 功能 (選購)

Content-Lock模組可以設定內容感知相關的政策，以阻絕個資與敏感資訊的外洩。「內容感知規則」的設定，不僅預設提供的真實檔案格式識別，還可以依據關鍵字、正規化表示(Regular Expression)等，以識別出諸如身分證字號、地址、手機號碼、市話等個資資訊。

### DeviceLock服務監控

透過佈署DeviceLock Enterprise Server，得以監控分散在個人電腦端代理程式之運作狀況，並進行集中記錄與統計。

### 權限回報功能

協助您可以對內部各電腦的DeviceLock權限進行盤點與報表功能，以達到稽核目的。

### 回傳資料流量最佳化與壓縮

針對稽核紀錄與陰影複製的資料回收作業，可以制定頻寬使用限制，並可對回傳的資料流自動壓縮，以降低網路負載，減少大資料量回傳時所造成的網路衝擊。當佈署多部資料回收主機的情況下，得自動選擇辨識最佳化的回傳路徑。

### Search Server模組(選購)

Search Server模組提供針對DeviceLock Enterprise Server收回的陰影備份檔案，進行「全文檢索」方式的稽核。它可以對常用的文件格式之文字內容進行檢索查詢。這些格式包含: Adobe Acrobat (PDF), Ami Pro, 壓縮檔案(GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (documents, spreadsheets and presentations), 以及其他常用格式。

### 報表模組(選購)

網頁式DeviceLock記錄報表，讓管理者可以經由網頁介面，查詢與調閱這些週邊與檔案的存取記錄。提供依電腦、用戶帳號、存取動作、事件種類、日期時間等進行不同角度進行報表稽核。管理者除了直接於瀏覽器瀏覽報表之外，還可以自訂週期性報表，自動透過電子郵件寄送報表內容。

## 與AD&群組原則無縫整合

當DeviceLock位於有使用AD的網域環境中，得以透過Group Policy群組原則達到集中設定、儲存與政策同步內容。如此與企業中既有的網域採用相同的管理方法，可以大幅簡化管理時間與學習成本。

## 彈性且細緻的存取控管政策

存取政策可依User、Group制定對應政策，亦可對特定的電腦之所有人員(everyone)，或者本機的帳號訂定對應的權限。可依對應裝置制定政策，提供USB裝置分類，進行分類控管。政策的內容支援依時段、每週工作日區間之外，亦可針對儲存裝置制定唯讀的政策，讓企業資料無法寫出至非授權的裝置中。

## 真實檔案格式管控

支援依據檔案的真正格式制定允許或禁止傳輸的政策，不會因為使用者竄改附檔名而規避。因此您可以禁止如CAD、PSD等設計圖檔，寫出到電腦外部。DeviceLock目前支援超過3000種格式特徵資料庫。

## iPhone等行動裝置的資料外洩防護

透過DeviceLock，您可控管個人的行動裝置，如iPhone, iPad, Windows Mobile接到電腦時，行事曆、郵件、工作、記事簿還是圖片或各種檔案，哪些內容可以同步或哪些行為是禁止的。DeviceLock可以識別從USB, 藍芽, COM或IrDA紅外線所連接的裝置。

## USB裝置白名單

得以針對特定的裝置型號、裝置序號(DeviceID)進行允許或禁止。USB裝置的生產廠商會依據其取得的廠商編號、產品編號加上裝置序號合併做為DeviceID。常見的應用是單位內僅許可經過申請的特定裝置才能存取，其它裝置一律禁止。
制定時可針對產品編號整批開放，或者是針對唯一裝置序號進行放行。

## 媒體白名單Media White List

可針對特定的DVD/CD-ROM光碟片建立特定的媒體指紋，並且設定僅有特定的指紋才能使用。一旦光碟中的內容變更，則其指紋就會不同。常見的應用是在一些開放的資料查詢電腦上，如圖書館、公共展示Kiosk機等，要鎖住僅能使用特定的資料光碟，甚至鎖住光碟彈出按鈕，避免被未經授權的人員抽換。

## 暫時白名單Temporary White List

針對出差在外又臨時需要使用隨身碟者，可以透過電話向相關管理人員申請臨時性的許可權限。使用者藉由回報電腦上顯示的裝置序號，管理者即可據此產生一個臨時性開放碼。該開放碼可以指定放行的分鐘數，或直到裝置拔除。中間的溝通可透過語音電話完成，而開放期間的使用行為也可留下稽核紀錄。

## 完整裝置使用稽核紀錄Audit Log

提供裝置使用情形的完整稽核紀錄。包含事件時間、裝置類別、執行動作、執行身分、當時的程式(Process)。稽核紀錄以作業系統之事件(Event Log)格式暫存於使用者電腦上，並可設定自動回傳集中儲存於主機端，以方便報表與稽核目的。

## 提供外存檔案的陰影複製(Shadowing)

陰影複製功能可以設定來針對允許使用外接裝置的人員，將其外存的所有檔案複製、鏡射一份到集中的伺服器資料庫中，以方便稽核外存檔案的所有內容。當裝置不在內部網路時，陰影複製的資料會暫存於個人電腦端，待回到內網後會自動同步到到主機中。

## 防破壞機制的設計

為保護DeviceLock佈署於個人電腦端的防護機制被使用者破壞而造成外洩風險，因此代理程式有設計一系列的防破壞措施。包含服務無法被使用者任意停用，背景程式無法被暴力停止，即使擁有本機管理者權限者亦無法破壞。系統得以指定特定DeviceLock管理者帳號，只有管理者才能進行相關的維護與管理作業。

## 加密軟體整合應用

DeviceLock可以識別經過加密的PGP、TrueCrypt與DriveCrypt磁碟(含隨身碟等各種可攜式儲存週邊)。可以於政策指定唯有外接裝置是加密的情況下，才准許寫出檔案，如果接入的是未加密的隨身碟，則僅能唯讀，以符合企業的安全政策。

## 裝置於內、外網的政策制定能力

DeviceLock提供內外網感知能力，以制定當端點位於內部網路或外部網路時可以分別套用不同的政策設定。例如，當端點的有線網路接到內網時即禁止WiFi無線網路的連線，以避免有線、無線橋接帶來的風險。

DeviceLock® 可以為企業及各機關提供完善的行動週邊裝置安全控管解決方案，具備完整的週邊設備支援、可彈性制定權限政策，同時具備大企業與小網路均適用的管理架構，並且可以支援AD與Group Policy的管理政策指派，以及具有彈性的授權模式。

## 提供彈性多種部署方式

佈署DeviceLock® 時，可以透過以下不同的方式來進行：

- 透過管理介面針對內網的電腦進行派送
- 透過AD Group Policy(群組原則)進行軟體派送
- 支援微軟 SMS 集中佈署(提供 msi 安裝程式)
- 通過網域 Logon Script 自動化安裝
- 單機透過安裝程式逐一安裝

## 完整外接週邊裝置管控支援

藉由DeviceLock®，管理者可以制定政策阻擋非授權使用者使用各種週邊。DeviceLock® 支援針對「裝置介面(Ports)」、「裝置類別(Device Types)」以及「裝置序號(Device ID)」進行三個層級的管控。

**裝置類別 Device Types**

- 軟碟機 Floppies
- 光碟機 CD-ROMs/DVDs
- 硬碟 Hard Drives
- 磁帶 Tape Devices
- 藍芽介面 Bluetooth
- 無線網卡 WiFi Adapters
- 可攜式儲存裝置
  例如: 隨身碟、外接硬碟、記憶卡、MO光碟...等
- 智慧型行動裝置
  例如：iPhone, Windows Mobile,BlackBerry & Palm OS等裝置
- 列印裝置 包含: 本地, 網路, 虛擬印表機

**裝置介面 Ports**

- USB
- FireWire (1394)
- 紅外線 Infrared
- 串列埠(COM) & 並列埠(LPT)

**加密裝置的整合**

- PGP Whole Disk
- TrueCrypt
- Lexar SAFE

如需試用 Device Lock或是更多的詳細資訊，請瀏覽 www.docutek.com.tw

## 佈署環境需求

DeviceLock® 可以佈署於下列環境：

Windows NT/2000/XP/ 2003/Vista/2008/ 7

支援32-bit以及64-bit平台上

記憶體需求: 64MB (含)以上

硬碟空間需求: 25MB

Designed for Microsoft® Windows® XP Windows® 2000 Windows NT®

代理商

內網安控 資訊治理的極致延伸
Own Your IT Governance From Managing Insder Security Threats.
docutek 達友科技

達友科技股份有限公司
Docutek Solutions,Inc.

台北公司・Taipei Office・
11492台北市內湖區基湖路35巷11號4樓之1
TEL : 886-2-2658-8970 FAX : 886-2-2658-8670
http://www.docutek.com.tw

上海公司・Shanghai Office・
上海市徐匯區漕寶路80號803室
TEL : 86-21-6440-3373 FAX : 86-21-6440-3372
http://www.docutek.com.cn

經銷商