Kaspersky® Security for Storage

適用於網路連接儲存裝置的高效能網路安全防護

惡意程式能夠利用現代網路的相互操作性，以驚人的速度擴散至整個企業組織。在威脅持續成長的情況下，受感染的單一檔案在不知情的情況下放入儲存裝置，便能讓網路中的每個節點暴露在立即性的風險中。

Kaspersky Security for Storage 可以為企業網路連接儲存裝置中的貴重與敏感性資料，提供強大、高效能及可擴充的防護。透過高速通訊協定的順暢整合可以保留儲存系統的效率，維持最佳化的使用者體驗。

客戶選擇 Kaspersky Security for Storage 的原因：

- 功能強大的即時惡意程式防護，適用於 EMC、NetApp、Dell、Hitachi、Oracle 及 IBM 儲存裝置
- 由 Kaspersky Security Network (KSN) 提供的雲端輔助安全防護
- 支援多種通訊協定：CAVA 代理程式、RPC 及 ICAP
- 關鍵系統區域掃描的專屬安全工作
- 靈活且精密的設定，實現隨時啟用的防惡意程式掃描
- 可輕鬆擴充並支援容錯部署
- 可靈活利用系統資源
- 通過 VMware ™、Microsoft ™及其他供應商的認證
- 包含 iSwift 及 iChecker 防毒掃描最佳化
- 可透過 Kaspersky Security Center 進行整合管理與協調流程

商業優勢：

- 資料儲存裝置中的所有檔案均安全無虞，不需要在端點進行防毒檢查
- 透過原生 API 整合 NAS，表示對使用者生產力的影響不大
- 完整掌握整個儲存基礎結構的資料檔案網路安全

產品特性

- **功能強大的即時惡意程式防護**
  「隨時啟用」的主動式防護，是由全球安全情報提供技術支援 (Kaspersky Security Network)，適用於網路連接儲存裝置 (NAS) 解決方案。卡巴斯基實驗室功能強大的防惡意程式引擎，會檢查啟動或修改的每個檔案，尋找包含病毒、蠕蟲和木馬在內所有形式的惡意程式。進階啟發式分析甚至可辨識全新和未知的威脅。

- **最佳化的效能**
  高效能的掃描採用最佳化的掃描技術與彈性的例外設定，除了提供極佳的防護，同時可將對系統效能的影響降到最低。

- **可靠的 NAS 防護**
  採用整合元件設計的直觀架構，設計和建立時是以完美搭配運作為目標，可實現卓越的容錯能力。如此得到一個穩定的備援解決方案，在被強制關閉的情況下將會自動重新啟動，提供可靠且連續的防護。

- **管理輕鬆簡單**
  可遠端安裝在伺服器，且防護「立即可用」不須重新啟動，並可透過一個簡單的直覺式中央主控台 Kaspersky Security Center，和其他的卡巴斯基安全解決方案一併管理。

支援的平台及作業系統：

EMC Celerra/VNX 儲存體：
- EMC DART 6.0.36
- Celerra Antivirus Agent (CAVA) 4.5.2.3

EMC Isilon 儲存體：
- OneFS ™ 7.0

NetApp 儲存體：
- Data ONTAP® 7.x 及 8.x (7- 模式下)
- Clustered Data ONTAP® 8.x 及 9.x

IBM 儲存體：
- IBM System Storage N 系列

Hitachi 儲存體：
- HNAS 4100、4080、4060、4040
- HNAS 3090、3080
- 虛擬儲存平台 G 系列

Dell 儲存體：
- Dell Compellent ™ FS8600 (FluidFS 6.x)
- Dell Compellent ™ FS8600 (FluidFS 5.x)

Oracle 儲存體：
- Oracle ZFS Storage Appliance

其他 NAS
- ICAP 相容的 NAS
- RPC 相容的 NAS

功能

- **隨時啟用的主動式安全防護**
  卡巴斯基實驗室的業界領導防惡意程式掃描引擎是由全球威脅情報的專家所建立，使用智慧技術來強化偵測，進而提供主動式防護來防範新興及潛在威脅。

- **自動更新**
  防惡意程式資料庫會在不中斷掃描的情況下自動更新，可確保持續防護，並將系統管理員的工作負載降到最低。

- **雲端輔助安全防護**
  Kaspersky Security Network (KSN) 的雲端式安全防護，表示系統能夠以明顯更快的速度辨識惡意活動，協助保護資料儲存裝置不受零日威脅的攻擊。

- **例外程序和信任區域**
  掃描的效能可以透過建立「信任區域」的方式進行微調，這項功能可搭配定義的檔案格式和程序 (例如資料備份)，讓這類檔案與程序不執行掃描。

- **彈性化掃描可協助達成效能最佳化**
  減少掃描和設定的時間可對負載平衡帶來幫助，有助於伺服器效能最佳化。系統管理員可以指定和控制掃描活動的深度、廣度和時間，並定義必須掃描的檔案類型和區域。您可以在伺服器活動量較少的期間，排定依需求指定的掃描。

- **支援所有主要的通訊協定**
  Kaspersky Security for Storage 支援不同儲存系統使用的主要通訊協定：CAVA 代理程式、RPC 及 ICAP。

- **遠端集中式安裝與管理**
  您可以透過直覺的 Kaspersky Security Center 處理遠端安裝、設定與系統管理 (包含通知、更新和彈性化報告)。您也可以依據偏好使用命令列管理。

- **控制系統管理員權限**
  您可以將不同的權限等級指派給每個伺服器的系統管理員，以符合特定的企業 IT 安全原則。

- **彈性化報告**
  您可以透過圖形式報告了解報告內容，或是檢視 Microsoft® Windows® 或 Kaspersky Security Center 的事件記錄檔。搜尋和篩選工具可讓您快速存取大量記錄檔中的資料。

Kaspersky Security for Storage 搭載 HuMachine Intelligence，這是卡巴斯基實驗室的機器學習、威脅情報和專業知識的獨特組合，無論資料的來源為何，都能確保所有資料受到完整保護，而且幾乎不會對系統效能造成影響。

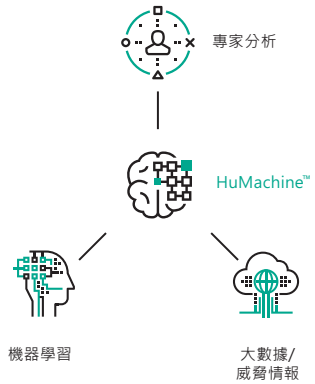
EMC²

ORACLE Gold Partner

DELL Technology Partner

HITACHI Hitachi Data Systems Technology Alliance Partner

NetApp Alliance Partner



卡巴斯基實驗室
企業網路安全：www.kaspersky.com/enterprise
網路威脅新聞：www.securelist.com
IT 安全新聞：business.kaspersky.com/

真正的網路安全
#HuMachine

www.kaspersky.com