



與 Matrix42 合作說明與探索 最佳端點安全

MATRIX42

#KingstonIsWithYou



與 Matrix42 合作說明 與探索最佳端點安全



簡介

資料保護是今日世界中企業、政府及個人的基本考量。

資料違規、駭客及人為因素持續提醒我們全球各地的威脅及風險。資料外洩所導致的金錢與聲譽損失都是天文數字。進階的網路安全及端點 DLP (資料外洩防護) 策略需求，都仰賴可靠且有效率的儲存裝置和記憶體。

將加密、快速儲存裝置及記憶體與最佳實務、標準和原則搭配使用，是邁出的一大步。遺失的筆記型電腦和 USB 隨身碟會讓個人和公司身陷個人及私人資訊外洩的風險。Kingston 提供威脅預防解決方案，有助於緩解風險，同時還能補強現有或開發中的安全性計畫。



內容

這本簡短的電子書將介紹端點解決方案，Kingston 的加密 USB 隨身碟所採用的客製化程式與 Matrix42 EgoSecure 資料保護軟體，已協助解決了六個不同行業的挑戰，並提供滿足其業務需求的解決方案。

我們將深入研究這六個行業，並瞭解它們如何面對端點安全的挑戰。

目錄

第一部分	行業使用案例 - 公共部門	4
第二部分	行業使用案例 - 醫療保健	5
第三部分	行業使用案例 - 金融	6
第四部分	行業使用案例 - 汽車	7
第五部分	行業使用案例 - 電信	8
第六部分	行業使用案例 - 製造業	9
第七部分	Kingston 與 Matrix42 的解決方案	10
	摘要	11
	關於 Kingston	12



第一部分：行業使用案例

公共部門



狀況：

公共部門中，USB 裝置的使用非常普遍。例如執法單位必須使用 USB 線，將所拍攝的違規停車與行政違規照片，從數位相機複製到當局的系統中。警方從外部資料儲存裝置上，接收調查資料。該資料需要重寫並預防未經授權的存取。

挑戰：

由於對 USB 裝置的需求很高，因此員工經常要求採購 USB 隨身碟。出於安全理由，必須封鎖私有與未經授權的資料儲存裝置。若員工需要新的 USB 儲存裝置，則使用者服務台 (User Help Desk) 應盡快提供，以免影響工作。請務必留意，使用合適的 USB 裝置不會引起安全問題。

解決方案：

將裝置控制、資料過濾與加密結合後，可實現如下：

未知裝置通常在電腦端點上被封鎖。數位相機等資料儲存裝置僅允許使用某些功能，例如讀取圖檔。寫入操作時通常須加密，且只允許在授權的 USB 裝置上使用。所有的資料存取過程皆須記錄下來。透過客製化序號及硬體 ID，可簡化授權裝置管理。因此，Matrix42 的服務管理允許使用者透過自助服務，要求個性化的 Kingston Technology USB 隨身碟。經過核准後，將自動允許 USB 裝置使用 EgoSecure 資料保護。

“核准流程簡便，可輕鬆快速地提供新的 USB 裝置，員工們皆讚譽有加。我們對於 Kingston Technology 的客製化程式，以及 Matrix42 的服務管理和簡單的端點安全管理，感到非常滿意。”

公共部門服務台負責人

第二部分：行業使用案例 醫療保健



狀況：

員工與其他機構經常以外部儲存裝置交換資料。

例如德國的醫院必須向癌症登記中心 (Cancer registry)，提供當前癌症病例及其進展的相關資訊。為簡化流程，通常透過行動儲存裝置傳輸該資料。

醫生們也喜歡透過 USB 隨身碟將文件 (例如研究資料) 帶到各自的講座中。

挑戰：

患者的資料極度敏感，切勿落入未經授權的人員手中。因此，須提升與強化資料保護。資料載體若遺失可能會成為嚴重問題，這不僅涉及到 GDPR (一般資料保護規定)，也與患者的福祉息息相關。因此，控制、監控與加密對 USB 資料的存取非常重要。

解決方案：

EgoSecure 資料保護將一個解決方案結合多項保護措施，例如存取控制、資料稽核、過濾與加密。使 IT 管理員有權限授予特定員工存取特定裝置。例外情況則可透過序號與硬體 ID 進行處理。得力於 Kingston Technology 的客製化程式，我們可以定義這些識別碼。因此，僅需在 EgoSecure 資料保護管理中配置一個數值，即可限制經公司核准裝置的使用。由於對存取進行了加密與監控，管理工作因此大幅減少，並提高了資料安全性 (符合 GDPR、CCPA、HIPAA 等規範)。

“我們已使用 Kingston 的加密 USB 隨身碟。目前，得力於 EgoSecure 資料保護，我們還能根據 EU-GDPR (歐盟一般資料保護規定)，實現對患者資料傳輸的可溯性。”

大學醫院資訊安全長



第三部分：行業使用案例

金融



狀況：

銀行須受各種合規性要求的規範。要求之一為符合 PCI-DSS (支付卡產業資料安全標準)。PCI-DSS 的要求包括資料加密、弱點分析與資料過濾。目標是最大程度地減少或完全預防威脅與 IT 安全風險。

挑戰：

端點上存在許多 IT 安全風險。員工每天必須處理來自消費者與企業의支付卡資訊，以及來自金融機構的敏感資料。因此他們面臨著來自雲端、電子郵件、USB 與網路資料可能被惡意軟體破壞的威脅，如果資料沒得到充分保護，還可能會落入第三方的手中。就 GDPR，PCI-DSS 以及美國沙賓法案而言，這樣的事件足以對銀行的財務產生影響。此外，網路罪犯者試圖以各種方式影響或操縱銀行系統，手法也變得更具想像力。例如，最近發生的 ATM 網路犯罪，是在電源中斷後使用可開機的 USB 裝置啟動 ATM 竊取金錢。

解決方案：

IT 系統必須以多層保護措施加以保護。這可以透過應用程式控制、裝置控制、異常檢測、UEBA (使用者行為分析)、監控以及具有預啟動驗證的全磁碟加密來達成。Matrix42 可以在自動化的整體生態系統中執行此操作，故僅允許許可之應用程式和加密的 USB 裝置。此外，檢測到可疑或惡意活動時，會自動啟動進一步的措施。關於 USB 隨身碟的使用，Kingston Technology 客製化的 USB 隨身碟組合有助於確保裝置能以最低限度操作而囊括至白名單中，並且以可追溯方式對資料進行加密。如此一來，無需額外花費力氣，即可大幅提高合規性。



“借助 EgoSecure 資料保護和白名單功能，我們僅允許經核准的 Kingston 加密 USB 隨身碟。我們只會將具有個人化硬體 ID 的 Kingston 加密型 USB 隨身碟列入白名單，而不允許使用其他裝置。這會大幅減少管理工作，並提升安全性！”

金融公司資訊科技經理

第四部分：行業使用案例

汽車



狀況：

在汽車產業中，USB 裝置的使用存在於各個領域中。例如，將研究資料儲存於外部儲存裝置中，並在公司各工程師之間交換。為配置生產設備，文件要從 IT 環境傳輸到 OT 環境。所有這些資料都具高度敏感性，必須加以保護，以防止產業間諜活動及資料盜竊，否則，積累的專門技術可能落入他人之手。

挑戰：

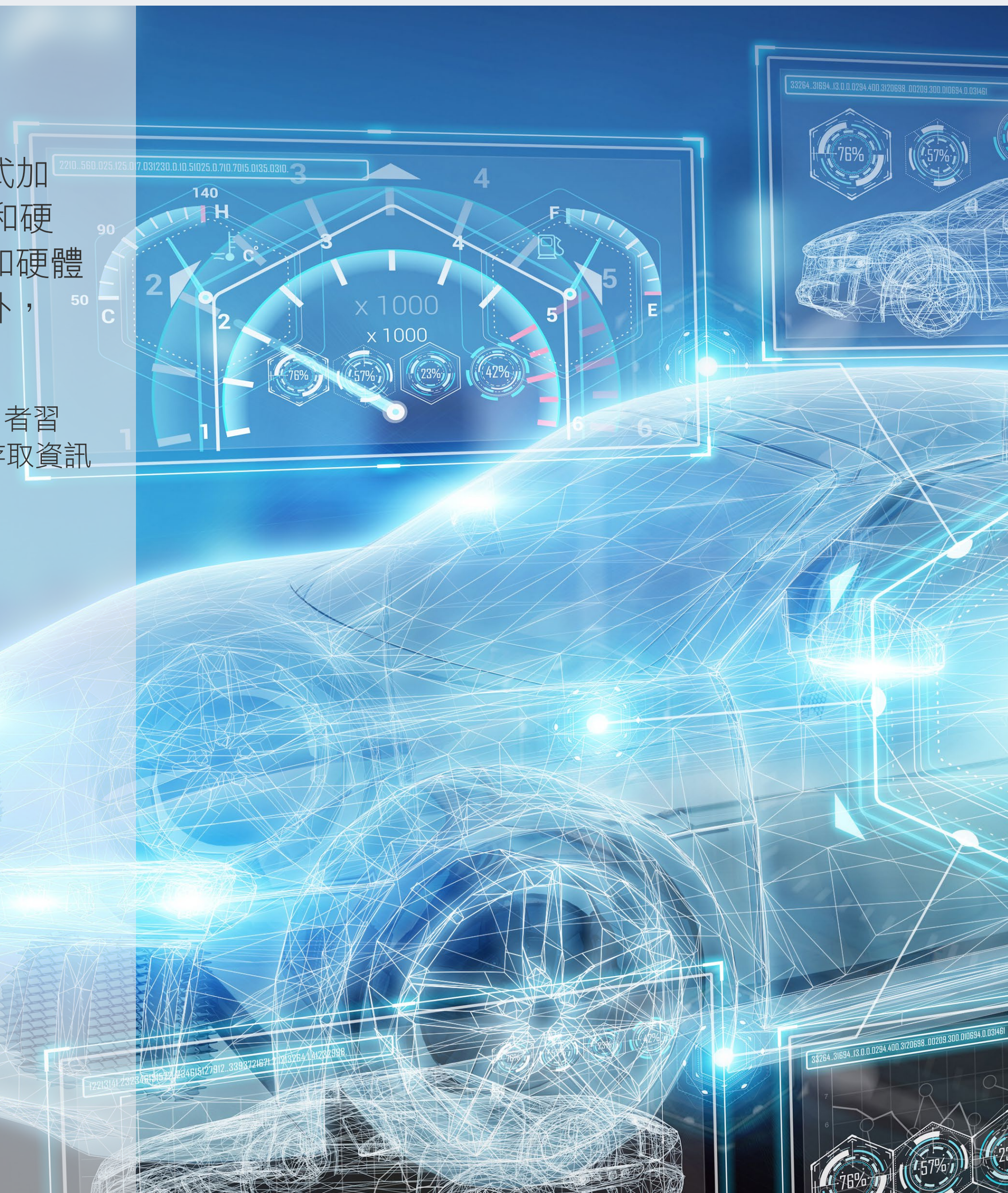
汽車產業須遵循 TISAX、原型保護、ENX、ISO27001、「第三方連接」和 GDPR 等合規性要求。在 TISAX 中，Control 9.1、9.5 和 10.1 條款規定必須對資訊存取進行控制、監控、過濾和加密。在汽車產業公司的所有領域中，亦必須遵循例如 GDPR 和 ISO27001 等其他合規要求。

解決方案：

Kingston Technology 加密型 USB 隨身碟以硬體式加密來保護資料。這些裝置可以獲取個人化序號和硬體 ID，在 EgoSecure 資料保護中使用該等序號和硬體 ID，自動地列入特定資料用途的白名單中。此外，若有任何可疑活動，可監控和分析資料移動。

“有了 Matrix42 和 Kingston Technology，無需改變使用者習慣，我們便能夠實現 TISAX 需求，例如 Control 9.5 (存取資訊和應用程式) 和 Control 10.1 (加密)。”

汽車產業供應商技術長



第五部分：行業使用案例

電信



狀況：

電信供應商持有很多客戶相關資訊。尤其是對於 GDPR 而言，這些資訊具有高度敏感性。因此，需要採取充份的措施來防止資訊遺失和資訊失竊。

挑戰：

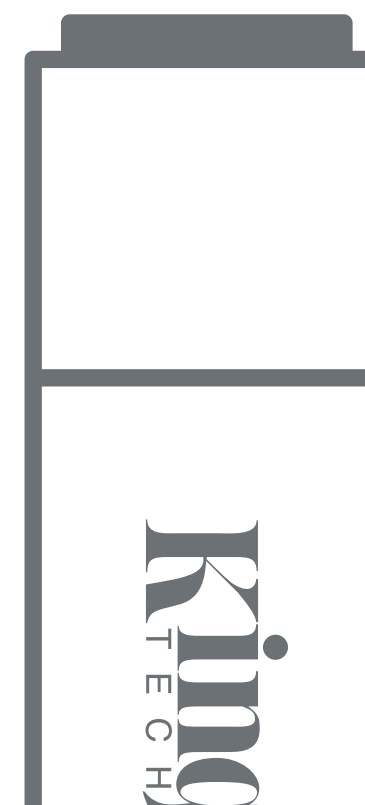
電信公司的員工每天都要處理客戶資料。大多數資料儲存在營業用應用程式中。然而，將客戶合約甚至資料庫匯出檔案儲存在端點及與其連接的外部裝置上，實具風險。為了進行資料交換，使用者經常使用外部儲存裝置。因此，檢測、糾正或保護不當的資料儲存做法相當重要。

解決方案：

為了簡化採購流程，可藉由 EgoSecure 資料保護中的預定義白名單，快速採購具有個人化產品 ID 的 Kingston Technology 加密型 USB 隨身碟，並透過 Matrix42 服務目錄進行交付。對於可能包含敏感資訊的資料儲存和匯出檔案，可藉由「使用中資料」和「靜態資料」型掃描的深度內容檢查來自動識別及補救。集中記錄資料移動。因此，員工可以在請求並核准後快速接收用於資料儲存的新硬體。這可以保證其符合 GDPR。

“ 借助 Matrix42 的自助服務入口網站，我們的使用者可以請求其所需的儲存媒體。一旦訂單獲得核准並交付後，EgoSecure 的裝置將獲准控管該裝置。Matrix42 和 Kingston Technology 的結合提升了敝公司的生產率 and 安全性。 ”

電信供應商技術長



第六部分：行業使用案例

製造業



狀況：

數位資料是未來的黃金。在製造業中，這些有價值的資料包括生產計畫、客戶及供應商的相關資料，以及公司的專門技術。如果遺失這些資料，不僅可能受到 GDPR 相當嚴厲的處罰，還可能導致指數式的聲譽問題。糟糕的是，我們每天都能在計程車、洗衣店、機場、火車站或停車場中發現 USB。

挑戰：

儲存裝置通常包含有高度敏感的資料，不幸的是，此資料通常未加密。服務技術人員使用外部資料載具來安裝生產裝置的更新，也可能存在風險。這些外部裝置存在將惡意軟體帶入工作網路的風險。

解決方案：

Kingston Technology 加密型 USB 隨身碟以硬體式加密來保護資料。這些裝置可能隨個人化序號和硬體 ID 一同交付，在 EgoSecure 資料保護中使用該等序號和硬體 ID，自動地列入特定資料用途的白名單中。此外，若有任何可疑活動，可監控和分析資料移動。

“對於我們保護自身免受資料盜竊而言，生產資料的加密非常重要。這些具高度敏感性的資料僅能透過 EgoSecure 資料保護進行檔案篩選，並由 Kingston Technology 加密型 USB 隨身碟核准後使用。在其他所有 USB 裝置中，生產資料會被鎖定，並且透過 EgoSecure 的即時加密和日誌記錄來保護對外部資料儲存的寫入存取權限。”

製造業資訊安全專員





第七部分：Kingston Technology 和 Matrix42 解決方案



將加密、快速儲存裝置及記憶體與最佳實務、標準和原則搭配使用，是邁出的一大步。遺失的筆記型電腦和 USB 隨身碟會讓個人和公司身陷個人及私人資訊外洩的風險。Kingston Technology 提供威脅預防解決方案，有助於降低風險，同時還能補強現有或開發中的安全性計畫。

Kingston Technology 加密型 USB 隨身碟

Kingston Technology 的硬體加密型 USB 隨身碟具備資料保護解決方案，以保護企業組織防火牆內外的行動資料。此隨身碟可嚴密保護您的資料，協助您遵循特定產業標準、指令及法規。產品符合 TAA 合規、已通過 FIPS 認證、最大儲存容量為 128GB，非常適合企業使用者和政府機構。



安全客製化計畫

現在您可以透過多種方式來客製化 Kingston Technology 加密型 USB 隨身碟，以滿足貴組織的需求。添加選定功能，打造獨一無二的專屬隨身碟。Kingston Technology 可讓您透過您指定的經銷商，輕鬆簡單地訂購客製化加密型 USB 隨身碟。Kingston Technology 的加密型 USB 產品包含 DTVP30、DT4000G2 和 IKD300S 系列。此計畫提供客戶最常需要的選項，包含序號、雙重密碼和客製化商標。該計畫的最低訂購量為 50 組，再次訂購量為 25 組，可準確地滿足貴組織的需求。

Matrix42 EgoSecure 資料保護

Matrix42 EgoSecure 資料保護為公司提供 360° 安全管理，以預防並保護裝置、系統和資料。該解決方案能在發生損壞的情況下，從預防至檢測到擬定對策的整個流程自動化，而不會降低生產力。

資料保護和網路安全可能讓人備感責任艱鉅。隨著員工能夠自行決定何時、何地以及使用哪種裝置來工作的變遷，對數位工作的要求已發生了巨大改變。硬體加密型 USB 隨身碟和端點軟體管理的適當組合有助於組織取得對其組織裝置的控管。因此，這可以降低資料洩露的風險，並協助其正在進行的 GDPR 合規策略。





關於 Kingston

憑藉 30 多年的經驗，Kingston Technology 擁有在不影響貴組織的前提下識別並解決端點安全挑戰的知識。

©2021 Kingston Technology Far East Corp. (Asia Headquarters), No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan.
版權所有，保留所有權利。所有商標 及註冊商標係屬於各自所有者之智慧財產權。

#KingstonIsWithYou