BenQ 提供更好的資料安全保護

顯示設備資安保護解決方案

BenQ 提供更好的資料使用安全性

BenQ 知道當組織引進新裝置時，總會伴隨一些風險。如果沒有充分的資訊保護，這些產品可能會導致您的網路暴露、資料洩露或隱私被侵犯等影響營運的可能性。

BenQ 致力提供您全面的安全守護策略解決方案。在顯示器方面，我們不僅提供最佳的影像清晰度、色彩準確度、絕佳的音質和互動性，也提供保護組織頂級資安保護。

我們的端對端解決方案 (從單一裝置到雲端基礎架構) 提供多個層級的安全性，協助您確認公司安全清單上的每一項安全措施。

裝置安全

網路安全

雲端安全

01 我們遵循國際標準並維護您的資料隱私權

02 我們協助您保護組織免於遭受安全威脅

03 我們對顯示器、使用者帳戶和檔案提供安全存取

01

我們遵循國際標準並維護您的資料隱私權

明基顯示器及其相關雲端服務均經過嚴格篩選。並且已通過歐盟總局施加的嚴格資料隱私標準資料保護規範（GDPR 和 GDPR-K）、《加州消費者隱私法》（CCPA）、英國產品安全與電信基礎設施（PSTI）制度、《兒童網路隱私權保護法》（COPPA）和 ISO/IEC 27001 安全標準。

GDPR　GDPR-K　CCPA　PSTI　COPPA

我們遵循國際標準並維護您的資料隱私權

符合國際規範的資料收集和使用

為了遵循 GDPR 和 CCPA 等國際資料法規，BenQ 保證，除非得到客戶許可，否則我們不會收集或儲存個人識別資訊 (PII)。

BenQ 也確保任何客戶資料 (例如其組織的使用者目錄) 僅用於雙方明確同意的目的；其中可能包括啟用和改進特定的雲端服務和裝置功能。

BenQ 不會出售或違法分享客戶的資料。

經過審查的雲端基礎架構

我們在 Amazon Web 伺服器 (位於德國法蘭克福) 上託管 BenQ 服務入口網站和資料庫，這些伺服器完全符合資料安全、隱私和可靠性的最高標準。BenQ 雲端服務定期由第三方稽核人員按照 AWS 合規計畫進行測試。

我們遵循國際標準並維護您的資料隱私權

通訊安全

BenQ 網站使用 SSL 和 HTTPS 等網路安全協定來保護您的連線、加密任何傳輸的資料，並防止攻擊者攔截BenQ線上入口網站與您的裝置之間傳送的資料。

授權便捷

BenQ Web 服務運用 OAuth2.0 和 JSON Web 權杖，這些業界標準用於跨越多個裝置進行有效授權，因此使用者完全不需要與 BenQ 共用私人憑證。

多重身份驗證

BenQ 允許使用者啟用多重身份驗證，使用者需要在登入時輸入傳送到行動裝置的安全代碼。這個額外步驟有助於驗證使用者的身分，並防止未經授權的存取，以防使用者的登入憑證遭到洩漏。

我們遵循國際標準並維護您的資料隱私權

密碼保護

使用者登入其 BenQ 帳戶時，BenQ 顯示器不會在本機上儲存密碼，降低未經授權存取顯示器和使用者資料的風險。

BenQ 顯示器也提供替代登入方法，防止使用者在螢幕上輸入憑證並確保密碼不會被公開洩露。

QR code login 登入

使用者透過行動裝置掃描 BenQ 顯示器上的 QR code，無須在螢幕上輸入帳號密碼。

NFC登入

部分機種內建NFC感應器。系統管理員可以向使用者發放已登記的NFC卡，達到管制存取和輕鬆登入的效果。

單一登入

BenQ 顯示器支援安全單一登入服務，例如Google、Microsoft Azure 和 ClassLink，這些使用加密保護的雲端服務。

02

我們協助您保護組織免於遭受安全威脅

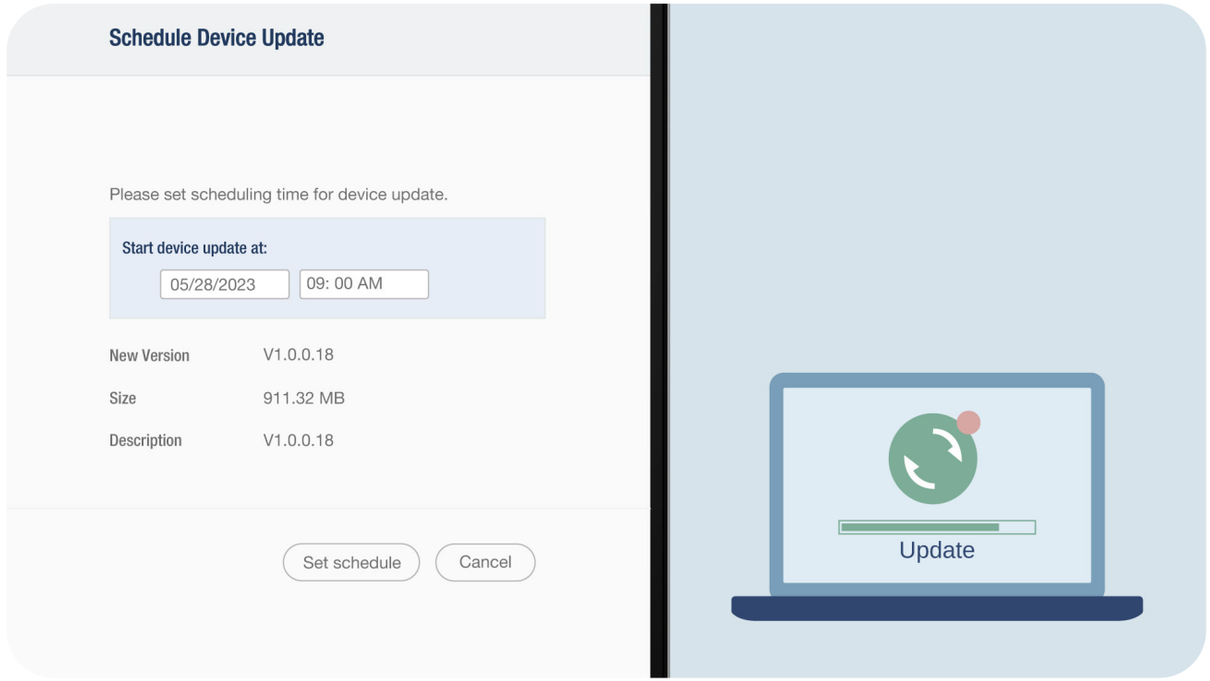
BenQ 協助學校與企業保護其系統與資料，避免惡意軟體與駭客等威脅。我們提供全面的安全選項，涵蓋不同層級的資料基礎建設。

我們協助您保護組織免於遭受安全威脅

防範入侵

BenQ 定期為顯示器的全部新舊機型提供最新的安全性修補程式和韌體更新。
管理員可以充分運用 BenQ 的雲端下載 (OTA) 更新功能，透過網際網路將修補程式遠端推送到全部顯示器中。

這不僅可以確保顯示器獲得適時的必要保護來防範網路上的入侵和相關攻擊，也有助於幫助顯示器保持在最新版的作業系統並發揮最佳效能。



我們協助您保護組織免於遭受安全威脅

靈活的網路安全選擇

BenQ 顯示器提供彈性的網路設定，幫助 IT 管理員隨時補強現有的安全策略。

企業級認證

設定 WPA2-Enterprise 進行使用者驗證和更安全的通訊。

加密資料傳輸

套用憑證來驗證其它裝置並將資料加密。

Proxy 層級保護

進行 Proxy 設定限制對有害網站進行的存取。

防範惡意軟體措施

04 系列的互動觸控顯示器可以利用 Google Play Protect 及安全瀏覽。

Google Play Protect 確保應用程式在用戶下載並安裝前已經經過仔細審查。它還會掃描並刪除任何已安裝但表現出可疑活動的應用程式。

同時，Google Safe Browsing 安全瀏覽功能可在用戶造訪涉及網路釣魚和其他網路威脅的潛在有害網站上提供保護。

Google Play Protect

Google Safe Browsing

03

我們對顯示器、使用者帳戶和檔案提供安全存取

透過 BenQ 帳戶管理系統 (AMS) 和 Identity and Access Management (IAM) 系統，我們為 IT 管理員提供建立和管理使用者帳戶的方法，管理員可以藉此防止任何未經授權的存取以及可能對 BenQ 互動觸控顯示器設定、使用者檔案和資料夾進行的竄改。

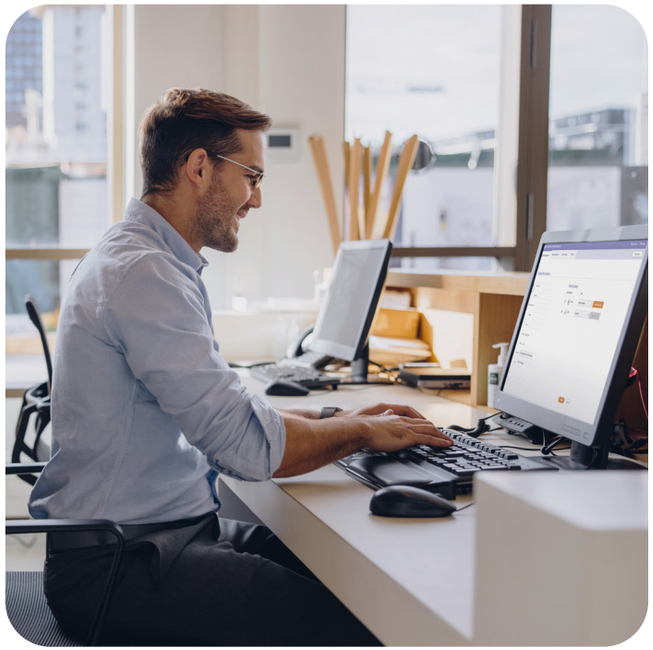
我們對顯示器、使用者帳戶和檔案提供安全存取

	訪客使用者	受限制的使用者	授權使用者
登入	不需要	需要	需要
修改設定	不允許	僅基本設定	常規用戶設定
連接裝置 (透過 HDMI or USB-C)	✓	✓	✓
公用資料夾	×	✓	✓
個人資料夾	×	✓	✓
雲端儲存	×	✓	✓
EZWrite 白板	✓	✓	✓
InstaShare 無線畫面分享	✓	✓	✓
網頁瀏覽器	×	✓	✓

深入了解 BenQ 大屏如何平衡使用者權限和資安

https://www.benq.com/zh-tw/education/edtech-blog/access-authority-security-user-roles-settings-benq-board.html

我們對顯示器、使用者帳戶和檔案提供安全存取



保護使用者存取

BenQ 提供兩種方法，可供 IT 管理員對 顯示器實施更嚴格的存取控制。

認證模式

此模式提供更高層級的存取控制，因為這能夠完全防止外部人員使用顯示器並竄改其中的設定。在 AMS 上啟用此模式可確保只有經過驗證的使用者才能使用該設備及其功能。

受限制的使用者角色

指派此角色可確保最高等級的存取控制權，因為它限制授權的使用者和群組進行更改任何關鍵的顯示器設置；但仍可使用重要功能和基本操作。

閒置工作階段登出

未鎖定和無人看管的裝置是最常見的資料洩露原因之一。管理員可以在 AMS 上設定閒置工作階段的登出時間來防止 BenQ 顯示器發生這種情況。如果使用者忘記登出，AMS 會自動登出該帳戶。

組織如何促使智慧型裝置更加安全？

以下是可以做為參考的檢查清單，確保您的智慧型設備可以安全使用。

- [ ] 組織內有智慧型設備使用指南嗎？
- [ ] 您是否能夠為設備分配和修改使用者權限？
- [ ] 您是否會收到設備的韌體更新和安全性修補程式？
- [ ] 您可以安裝安全軟體嗎？
- [ ] 您的智慧型設備是否允許您配置其網路設定以使其更安全？
- [ ] 您的智慧型裝置是否使用安全的雲端系統？
- [ ] 您的智慧型裝置及其雲端服務是否符合數據資料保護法規？