

YQI

System Integration Service

遠距辦公 數位企業向前行

不在辦公室 安全辦公事



COMODO
CYBERSECURITY

<https://www.yqi.com.tw>

疫情風暴來臨，企業如何實施遠距工作？



➤ 買筆電

- 雙重投資成本不低
- 市場缺貨還得搶貨
- 安裝公司軟體費時
- 員工要熟悉新電腦

➤ 建V P N環境

- 得尋求IT與廠商洽談、規劃
- 網路頻寬能否負荷
- 送預算、採購、等廠商交貨
- 不確定投資效益
- 流程跑完，疫情也過了

➤ 遠端桌面

- 網路頻寬能否負荷
- 無法控管安全
- 駭客攻擊最容易
- 公司機密資料可能外洩

疫情是測試企業軟實力和競爭力的試金石，當員工群聚感染風險提升、企業面臨營運中斷危機，提前部署數位轉型就能快速因應突發狀況下的衝擊。但企業在考量導入遠距辦公方案時，常會因為公司當前軟硬體限制、數位化程度過低及資安問題等痛點而拉長決策週期，進而錯過導入的黃金時期。

日本網路遭到攻擊！駭客侵入企業在家工作使用的VPN服務漏洞，並竊取使用者的帳號與密碼散布上網路，共有607間日本企業及行政機關受害，包含警視廳及政府觀光局。



遠距工作! 駭客入侵更容易



武漢肺炎疫情持續延燒，帶動民眾在家遠距工作或上學，但網路安全專家警告，駭客們也會跟上腳步伺機入侵各公司與機構。

由於許多企業啟動員工遠距工作，一些科技公司近來接獲網路安全協助的詢問跟著成長，思科系統公司（Cisco Systems Inc.）過去幾週相關安全支援的洽詢量就激增 10 倍。

思科旗下網路安全公司 Duo Security 高級顧問納塞爾（Wendy Nather）說，突如其來的工作型態轉變，可能意味出錯會更多，也給資訊科技人員帶來更大壓力，以及給駭客更多竊取密碼的機會。



iThome 新聞 產品&技術 專題 AI 區塊鏈 Cloud DevOps GDPR 資安 研討會

新聞

Windows 10 RDP漏洞可讓駭客綁架連線

駭客要成功利用這個漏洞，需要干擾網路連線，因此不太可能用來進行大規模攻擊，而當事者微軟評估該漏洞未達風險層級，處理態度消極，對此研究人員建議使用者應鎖定本機系統，非必要時應切斷RDP連線

文/ 林妍濤 | 2019-06-06 發表

讚 6萬 按讚加入iThome粉絲團 讚 480

Microsoft Windows RDP Network Level Authentication can bypass the Windows lock screen

Vulnerability Note VU#576688

Original Release Date: 2019-06-04 | Last Revised: 2019-06-06

遠距 / 在家辦公的安全挑戰

- 隨著駭客攻擊快速演化，即使在辦公室內，如何確保資料安全都已經非常不容易。現在，隨著Covid-19疫情升溫，如何兼顧員工在家工作與企業資安成為最頭痛的問題
- 如何確保是同仁連入？還是駭客？
- 何時連入公司？有紀錄嗎？
- 怎麼確保員工在家上網安全？避免在家裡下載病毒、木馬或勒索軟體而擴散至公司內部？如何管理雲端硬碟、WebMail的不當存取？
- 如何保護重要機敏資料，不會因為在家辦公而外洩？

- 無須額外採購設備
- 無須建置VPN
- 連入設備為辦公室電腦,熟悉度100%,不影響辦公效率
- 雙因素驗證, 帳號 + 密碼 + 動態碼三重驗證, 資安一把罩
- 完整連入使用紀錄
- 可限制檔案不落地,確保公司機敏資料不外洩

建構未來工作場域 為潛在商機超前部署

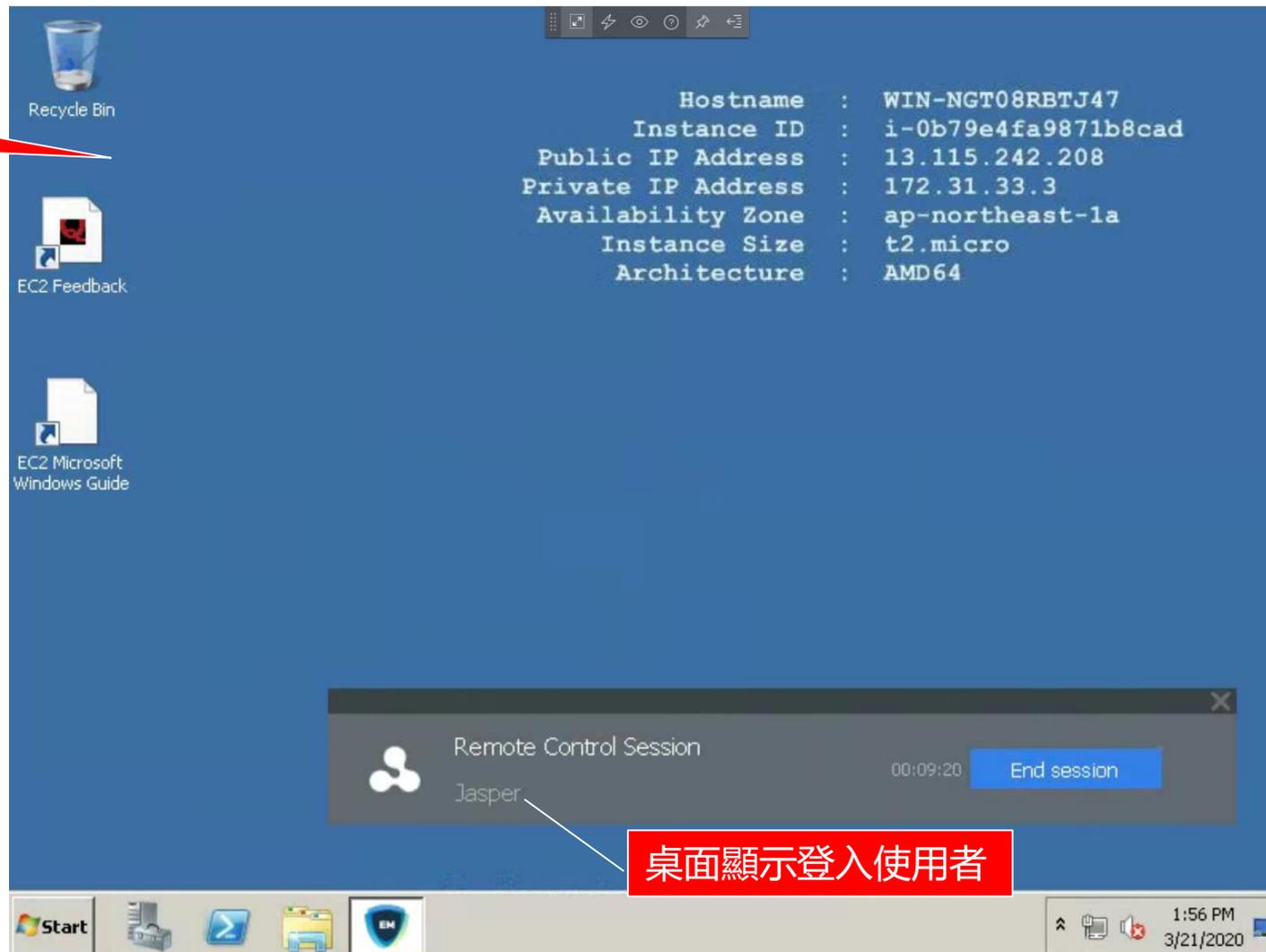
The image displays two screenshots of the Endpoint Manager web interface. The left screenshot shows a standard login page with the following elements: the 'EM Endpoint Manager' logo, a 'CONTACT' link, the heading 'INNOVATIVE AND SECURE DEVICE MA', the subtext 'WE ARE PROVIDING A SIMPLIFIED, EFFICIENT WAY TO CONF', a text input field containing 'Jasper', a password input field with masked characters, a green 'LOGIN' button, a 'Remember' checkbox, and a link for 'I forgot my password'. A red arrow points from the 'LOGIN' button to the right screenshot. The right screenshot shows the 'Two Factor Authentication - Code' page, featuring the 'EM Endpoint Manager' logo, 'CONTACT' link, the heading 'INNOVATIVE AND SECURE DEVICE MANAGEMENT SOLUTION', the subtext 'WE ARE PROVIDING A SIMPLIFIED, EFFICIENT WAY TO CONFIGURE AND MANAGE ALL DEVICES', a 'Back to Sign In' link, a 'Code' input field with a key icon, a green 'LOGIN' button, and a link for 'I don't have an authenticator app now'. The background of both screenshots includes an illustration of various devices (laptop, smartphone, tablet) connected to a cloud network.

遠距辦公使用權限限制

The screenshot displays the Comodo Endpoint Manager interface. On the left, there is a navigation menu with 'DEVICES' and 'SETTINGS'. The main content area is titled 'Device Management' and features three icons: 'Remote Control', 'File Transfer', and 'Remote Tools' (with a 'BETA' badge). A red box highlights these icons, with an arrow pointing to a red text box containing the Chinese text: '遠端連入權限可由管理政策進行限制' (Remote access permissions can be restricted by management policies). Below this, there is a search bar and a table of devices. The table has columns for OS, NAME, ACTIVE COMPONENTS, VIRTUAL DESKTOP, PATCH STATUS, CUSTOMER, LOGGED IN USER, and LAST ACTIVITY. One device is listed with the name '辦公室電腦' (Office Computer) highlighted in a red box. The table shows the device is connected to the 'Default Customer' and was last active on 2020/03/21 at 11:10:26 AM. At the bottom, there is a 'Results per page' dropdown set to 20 and a 'Displaying 1 of 1 results' indicator.

OS	NAME	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LOGGED IN USER	LAST ACTIVITY
Windows	辦公室電腦	AG CCS	Virtual Desktop	3	Default Customer	WIN-NGT08RB...	2020/03/21 11:10:26 AM

使用者電腦桌面



桌面顯示登入使用者

Audit Logs

Export

STAFF	EVENT NAME	AFFECTED OBJECT	OLD VALUE	NEW VALUE	EXTRA INFO	SESSION ID	LOG CREATION DATE
Jasper	Remote Control session summary	WIN-NGT08RBTJ47			Takeover Session ID: 17DCA559-6156-4181-9580-77A5CE857BFE Takeover Session Authentication: Allowed By Rules Takeover Session Connection Type: P2P Takeover Session Status: Finished Takeover Session Start: 03:37:16 PM Takeover Session End: 03:42:39 PM Takeover Session Duration: 5m 23s	73e89589d40444e2952ab1b3fcf98613	2020/03/21 03:42:39 PM
Jasper	Remote Control session status	WIN-NGT08RBTJ47	Connected	Finished	Takeover Session ID: 17DCA559-6156-4181-9580-77A5CE857BFE Takeover Session Duration: 5m 23s	73e89589d40444e2952ab1b3fcf98613	2020/03/21 03:42:39 PM
Jasper	Remote Control session connection type	WIN-NGT08RBTJ47		P2P	Takeover Session ID: 17DCA559-6156-4181-9580-77A5CE857BFE	73e89589d40444e2952ab1b3fcf98613	2020/03/21 03:37:24 PM
Jasper	Remote Control session status	WIN-NGT08RBTJ47	Connecting	Connected	Takeover Session ID: 17DCA559-6156-4181-9580-77A5CE857BFE	73e89589d40444e2952ab1b3fcf98613	2020/03/21 03:37:16 PM

使用者

連入電腦

連入時間

中斷時間

連線時數

稽核紀錄時間

我有問題

COMODO

Creating Trust Online™

我需要準備什麼環境？

COMODO

Creating Trust Online™



公司電腦 (安裝Comodo居家辦公套件)



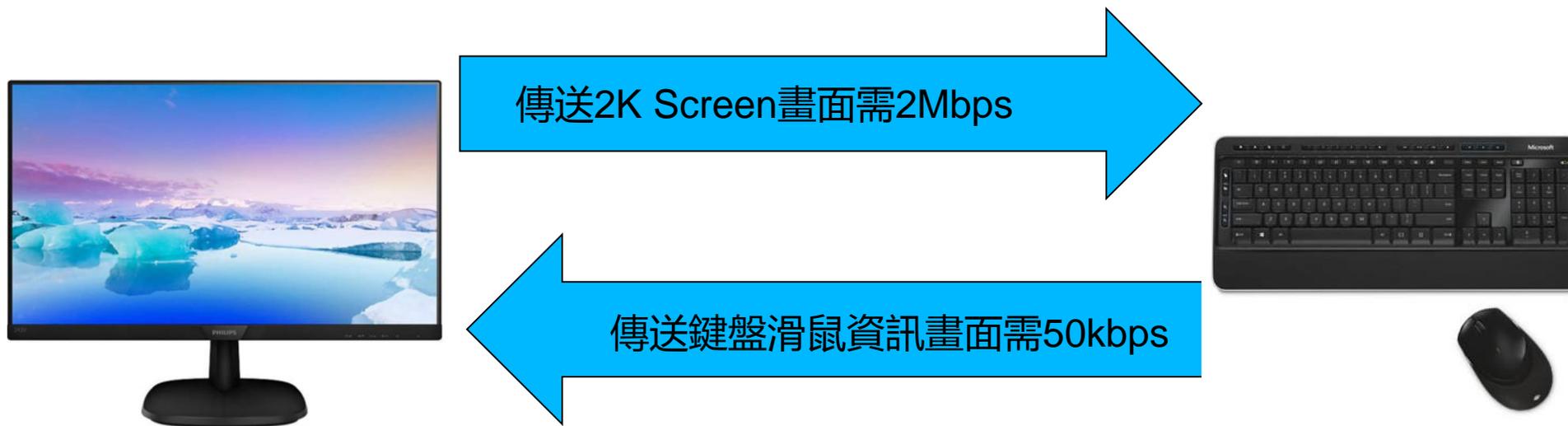
家用電腦 (安裝Comodo遙控套件)

我需要擴充網路頻寬嗎？

COMODO

Creating Trust Online™

COMODO遠距辦公網路需求



費用如何？

COMODO

Creating Trust Online™

彈性收費用多少付多少

- 2021/4/1 00:00之後新成立的客戶訂單會採取彈性的計費方式，早於此時間點成立之訂單將不受影響。
- 彈性授權啟用後，即計算至當月底天數，客戶若中途停止，恕無法辦理退款。
- 客戶授權一經啟用將自動延續至次月，若授權數量異動，請與服務人員聯繫。
- 彈性計費方式說明：
- 於2021/4/1第一次購買啟用20台居家辦公電腦授權，於2021/4/10追加10台授權，計費方式：
 - 2021/4/1授權有效期至2021/4/30，20台授權當月使用費每人300/台，使用授權費為 $20 * 300 = 6,000$
 - 2021/4/10追加10台授權，至2021/4/30授權天數為20天，不足30天，改以日計費，使用授權費用為 $10 * 300 / 30 * 20 = 2,000$
 - 合計2021/4月居家辦公使用費用為 $6,000 + 2,000 = 8,000$
 - 彈性增加之授權費用一律併入隔月授權服務費用。
- 2021/4/1 支付使用授權費 6,000
- 2021/5/1 如繼續使用30台授權，支付使用授權費用為
- $30 * 300$ (2021/5全月授權)+ $2,000$ (2021/4彈性授權) = 11,000
- 2021/6/1 無新增異動，使用授權費用計算為 $30 * 300 = 9,000$

謝謝大家!



<https://www.yqi.com.tw>

COMODO
Creating Trust Online™