MENLO SECURITY

Phishing Isolation 產品型錄

重要功能

- 以隔離技術保護電子郵件中的連結網址，消弭偷渡式下載的入侵方法
- 防範帳密的釣魚攻擊，防止身分竊盜
- 利用即時、可自訂且動態的使用者教育訊息，加強網路釣魚意識培訓
- 簡易的安全佈署架構，不需安裝端點代理程式，而且能夠與現有的郵件伺服器基礎架構輕鬆整合

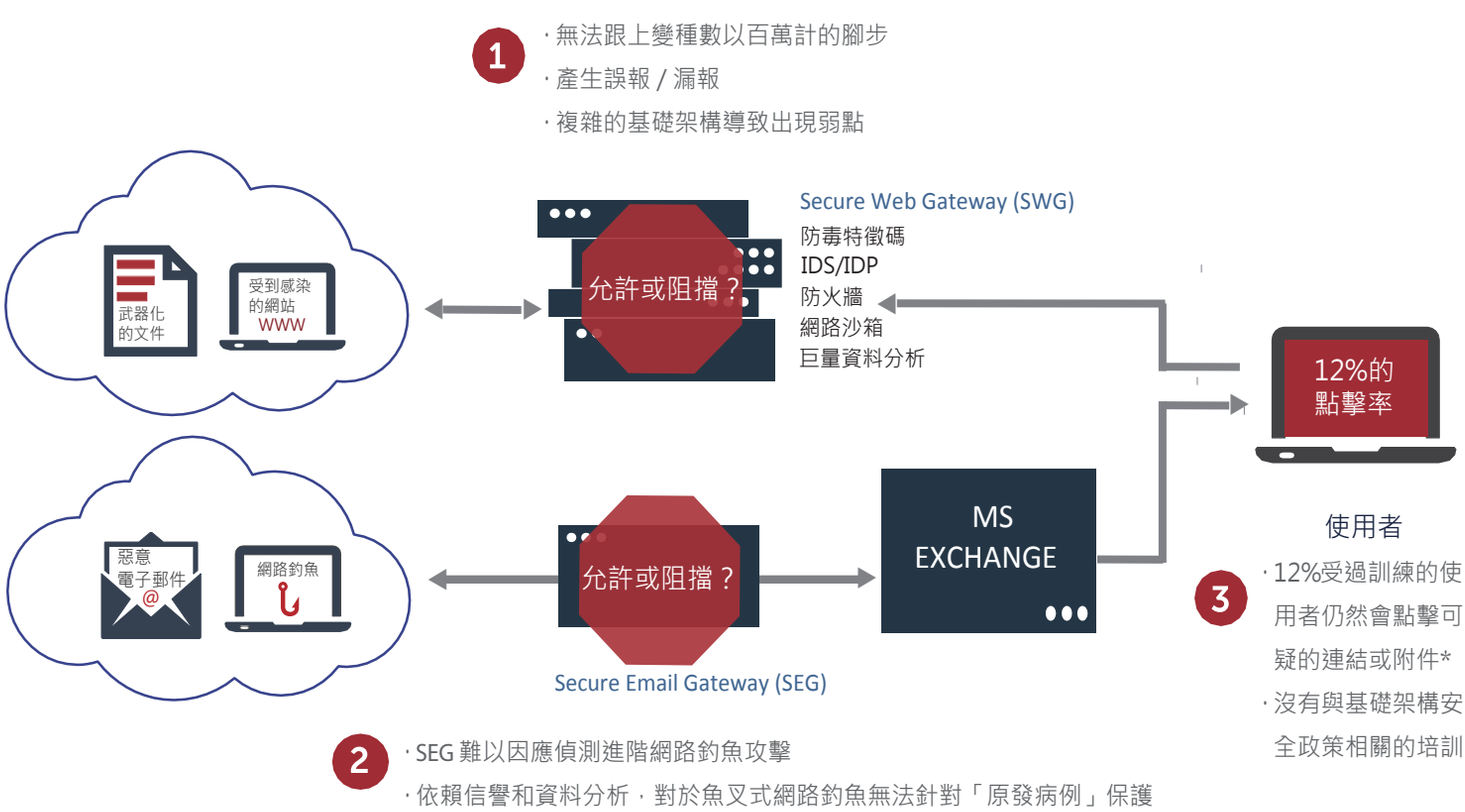
防範網路釣魚和偷渡式入侵威脅

網路釣魚已經成為網路犯罪分子的首選武器。儘管運作了全面性的電子郵件安全解決方案 (包括反垃圾郵件、防毒、沙箱，以及加密方案)，企業仍然受到魚叉式帳密釣魚、目標式APT攻擊、社交工程惡意程式攻擊，以及身份竊盜...等一系列的資安風險。

傳統的電子郵件安全解決方案依賴第三方情資或內部特徵來研判每封信「有沒有問題」來決定要不要阻擋。APT釣魚信件經常個人化的手法，每封攻擊內容通常是獨一無二的。因而無法仰賴情資與特徵來準確研判。一旦使用者點選或開啟就會造成感染。

即使佈署了最先進的沙箱檢測，先不論可用來規避沙箱的駭客手法越來越多，前所未見的檔案需要等待沙箱的行為觸發進行事後通知，而無法即時的識別與阻擋。此時會造成資安界所謂的「原發病例(Patient-Zero)」。甚至使用者直接連到釣魚網站輸入帳密，為了參加報名輸入個資，或點選超連結而造成感染...等。一個錯誤就可能會導致成本高昂且具破壞性的網路攻擊。

因此我們需要新的方法。



*Verizon 的 2016 資料外洩調查報告

網路釣魚統計數據總覽

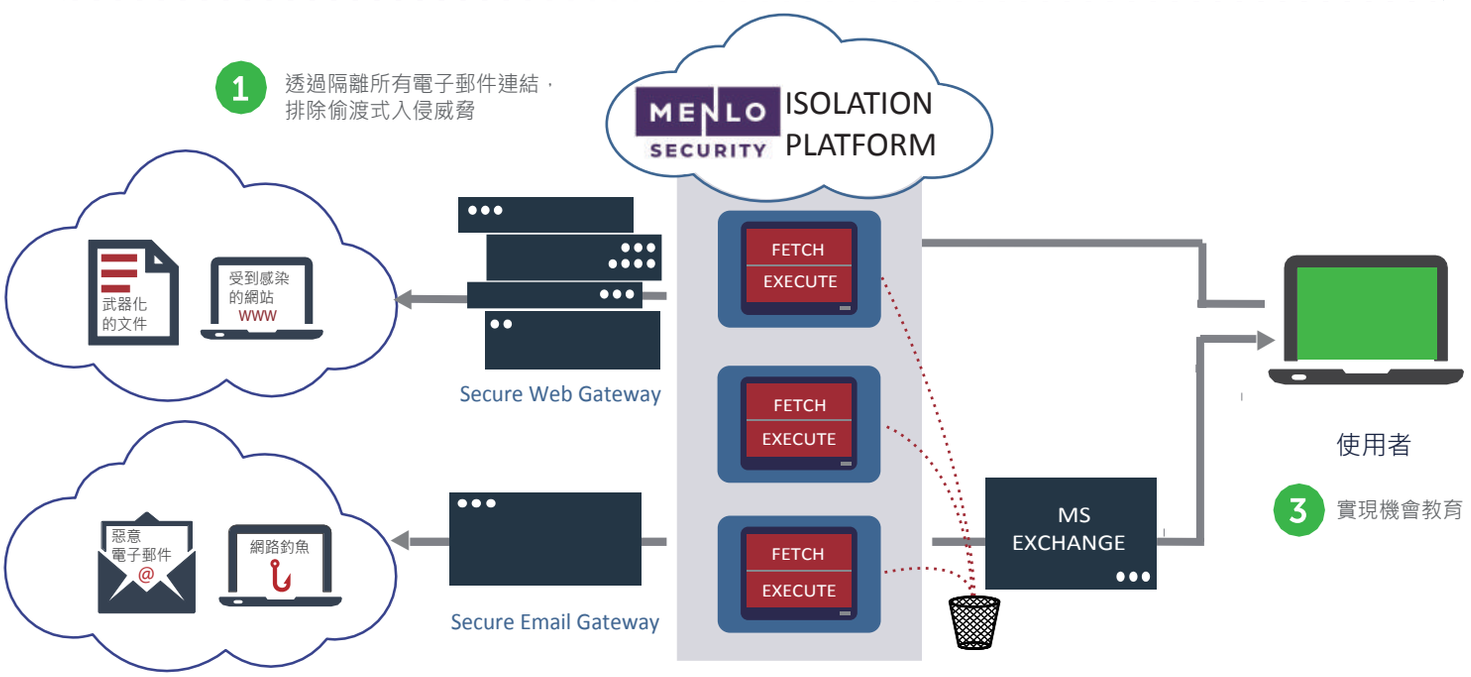
- 網路釣魚是網路攻擊最常見的針對性方法[1]
- 將近 50% 的使用者會在第一小時內開啟電子郵件並點擊網路釣魚連結[2]
- 12% 的使用者儘管受過訓練，仍然會點擊可疑的連結或附件[2]
- 網路釣魚攻擊的數量和複雜程度日益增加，導致停機時間和直接財務欺詐[3]
- 網路釣魚攻擊的主要犯罪份子是犯罪集團組織和國家附屬行為者[3]

1/Gartner 的 Fighting Phishing:Optimize Your Defense (2016 年 3 月 17 日出版)
2/Verizon 的 2015 資料外洩調查報告
3/Verizon 的 2016 資料外洩調查報告

解決方案：Isolation / 隔離

Menlo Security 的 Phishing Isolation 解決方案可消除電子郵件攻擊所引起的認證竊取和偷渡式入侵威脅。透過整合雲端式 Phishing Isolation 和現有的郵件伺服器基礎架構 (例如 Exchange、Gmail 和 Office 365)，就可以轉換所有電子郵件連結以通過 Menlo Security Isolation Platform。當使用者按一下電子郵件連結時，他們會與所有惡意軟體威脅 100% 隔離，包括勒索軟體。網站也可以用唯讀模式(Isolate + Read Only)呈現，以防個人將敏感資訊或帳密輸入有惡意意圖的網頁表單。

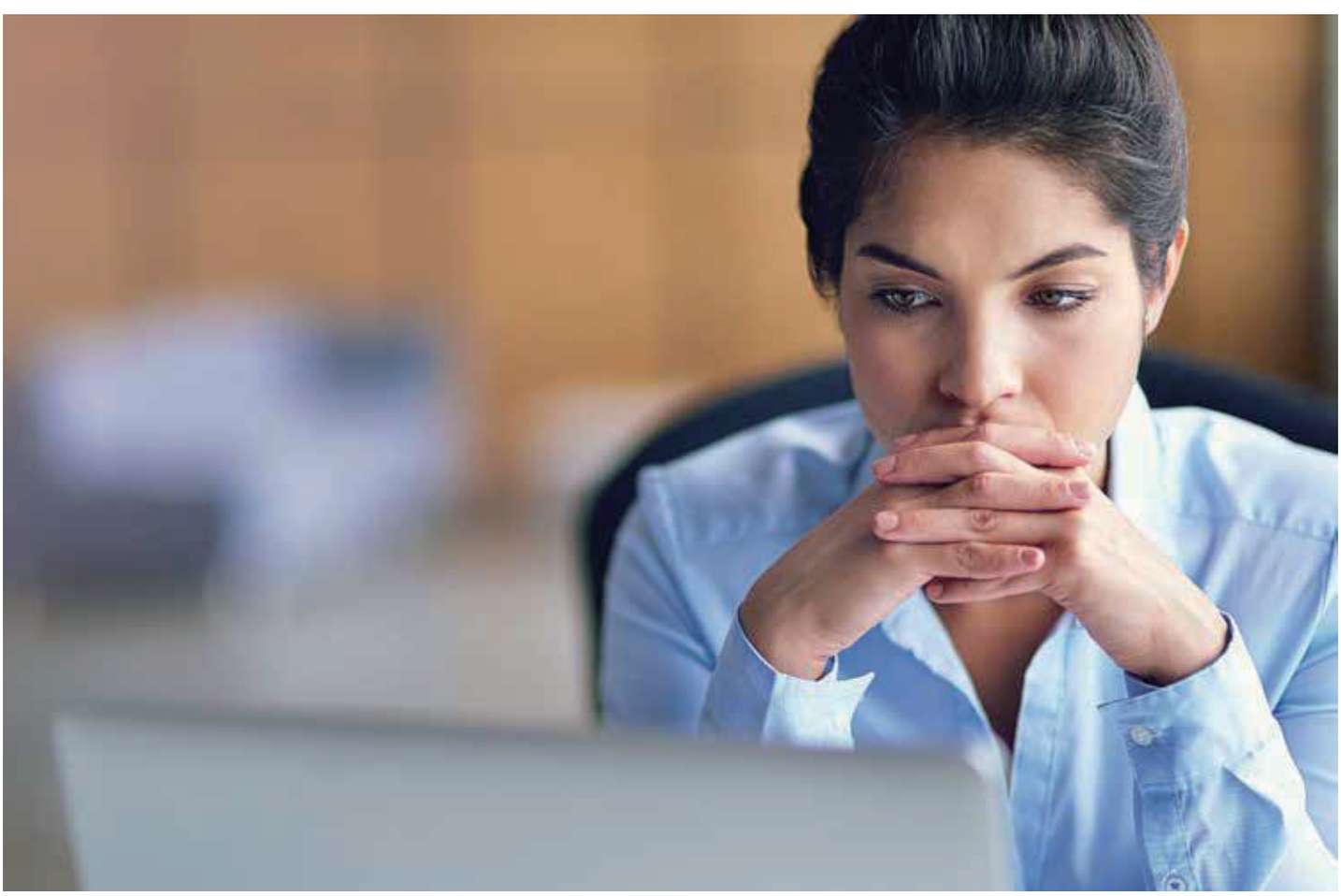
系統管理員可以將其使用者安全的隔離，藉以監控點選可疑連結的行為統計資料，並提供可自訂的點擊時網址保護 (time-of-click) 訊息，加強反網路釣魚意識訓練。系統管理員也可以透過工作流程，針對群組或個人設定政策來放寬 Web 輸入限制。Menlo Security Phishing Isolation 完全不依賴諸如資料分析等容易誤判或漏報的傳統威脅偵測方法，是創新的電子郵件安全解決方案，可即時保護所佈署的每個電子郵件使用者。



2 MSIP 可以透過在安全隔離工作階段中開啟所有電子郵件連結，
以保護每位使用者不受針對性魚叉式網路釣魚和偷渡式入侵作為的攻擊，
因而排除「原發病例」感染

Phishing Isolation 的主要效益

- 透過隔離所有電子郵件連結，防範網路釣魚並排除偷渡式入侵威脅。MSIP Phishing Isolation 提供業界唯一的解決方案，可防止認證遭到竊取，同時 100% 排除偷渡式惡意軟體入侵作為。
- MSIP 讓電子郵件中的超連結點選都導引到隔離平台中，並且開一個獨立的工作階段，以防範針對性魚叉式網路釣魚和偷渡式入侵威脅，而不依賴容易出錯的威脅偵測方法。
- 不需要端點軟體或設備，而且能夠與現有的郵件伺服器基礎架構輕鬆整合。MSIP Phishing Isolation 是第一個零依賴端點軟體或設備的雲端式 (公用或私有) 解決方案。
- 此解決方案可與現有的郵件伺服器基礎架構 (例如 Exchange、Gmail 和 Office 365) 輕鬆整合。
- 可提供使用者行為統計資料和可自訂的資安意識加強提示功能，實現機會教育。由於網頁工作階段會通過隔離平台，因此 MSIP Phishing Isolation 可以提供對使用者行為的能見度，協助系統管理員判斷哪些使用者正在點擊可能危險的連結。即使使用者的確點擊了惡意連結，所有網站還是受到安全隔離，而且具有輸入欄位的限制。系統管理員可以使用這項資訊創造機會教育，方法是，提供能夠提供額外企業網路釣魚意識培訓的可自訂且即時的警告訊息。



關於Menlo Security

Menlo Security 將透過隔離讓您安全點擊，並排除網路和電子郵件中的惡意軟體威脅，以防止組織受到網路攻擊。Menlo Security 的 Isolation Platform (MSIP) 可在雲端隔離所有使用中的內容，讓使用者安全地與網站、連結和文件線上互動，而不會犧牲安全性。

Menlo Security 受到一些全球最大的企業信任，其中包括 Fortune 500 大企業和金融服務機構。此公司是由安全產業資深人士以及加州大學柏克萊分校的知名研究者合作創立。Menlo Security 由 General Catalyst、Sutter Hill Ventures 和 Osage University Partners 為後盾，其總部位於加州的門洛公園。

如需詳細資訊，請造訪 menlosecurity.com 或透過contact@docutek.com.tw 聯絡

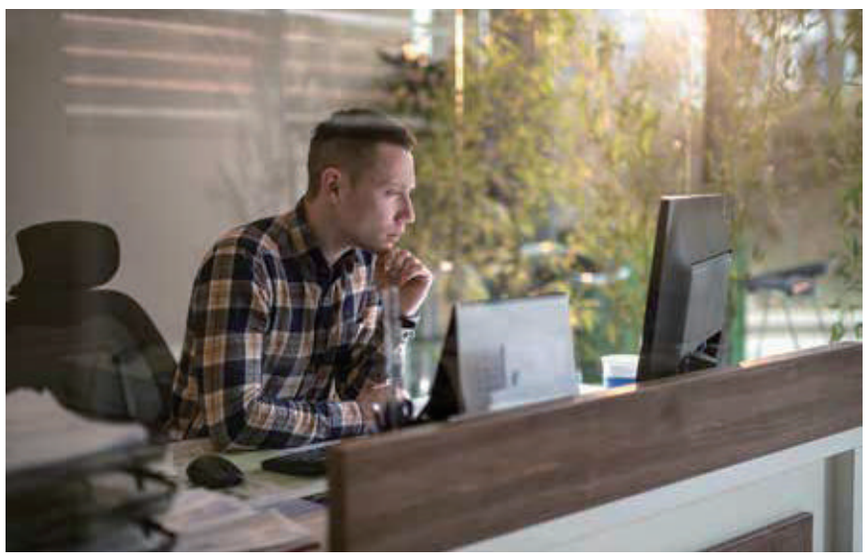
MENLO SECURITY

docutek 達友科技

總結

由於網路釣魚成為網路犯罪份子散發惡意軟體日益普遍的一種方法，因此，Menlo Security Isolation Platform (MSIP) 提供了業界唯一的 Phishing Isolation 解決方案，可防止認證遭到竊取，同時 100% 排除偷渡式惡意軟體入侵威脅。

MSIP Phishing Isolation 使用網路隔離的方法，防止使用者遭到可能會造成惡意軟體感染或引導至網路釣魚網站的惡意電子郵件連結攻擊。使用者可以透過這個獨特的方法，安全地檢視具有輸入欄位限制的網站，同時可設定的訊息能夠提供額外的企業網路釣魚意識培訓。MSIP Phishing Isolation 不需要端點軟體或設備，而且能夠與現有的郵件伺服器基礎架構 (例如 Exchange、Gmail 和 Office 365) 輕鬆整合。



代理商 docutek 達友科技 Content・Intelligence・Security

02-2658-8970 www.docutek.com.tw
contact@docutek.com.tw
台北市內湖區基湖路35巷11號4樓之1