端點安全令人不安的真相

Sophos 委外對 3,100 名 IT 管理員進行獨立調查的結果

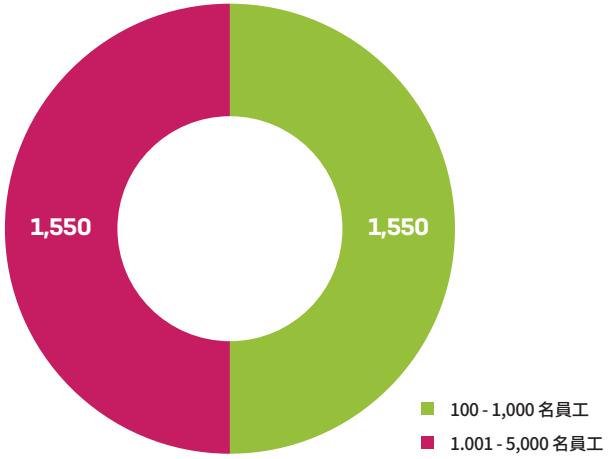
為了了解端點安全的現況，Sophos 委託獨立市調公司 Vanson Bourne 調查了全球 3,100 名 IT 管理員。從結果中，我們得到了 12 個國家和六大洲中各組織的經驗、他們關心的重點和未來計畫。報告還深入洞察了 IT 團隊面臨確保組織免受網路攻擊的日常挑戰，以及他們在端點偵測和回應 (EDR) 技術方面的經驗。

調查

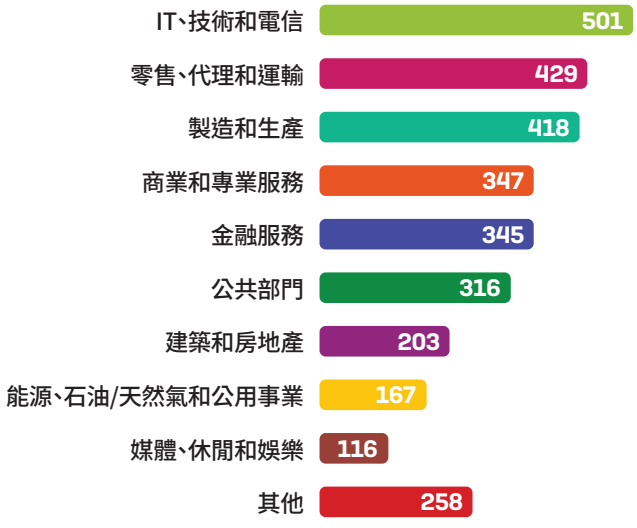
總部位於英國的研究機構 Vanson Bourne 在 2018 年 12 月至 2019 年 1 月期間採訪了 3,100 名 IT 決策者。為了在每個國家/地區提供具有代表性的樣本，受訪者平均劃分在 100-1,000 個使用者和 1,001-5,000 個使用者的組織。

每個國家/地區的受訪者人數

按組織規模劃分受訪者



按行業劃分的受訪者



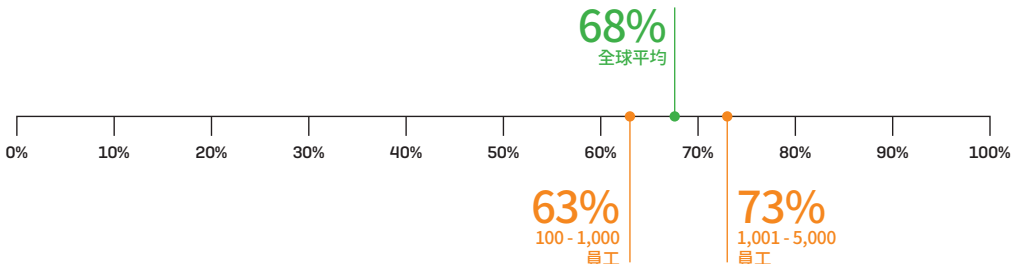
真相#1：現在成為網路攻擊受害者已是常態

超過三分之二 (68%) 的組織表示他們在去年遭到網路攻擊。較大型組織遭受的攻擊 (73%) 比較小的組織 (63%) 更多。造成這種差異有兩個可能的原因：

- 較大型組織更容易受到網路犯罪分子的攻擊，因為他們被認為是更有利可圖的受害者
- 較大型組織更能意識到受到網路威脅攻擊，因為他們擁有更多的 IT 資源來偵測和調查問題

定義：
網路攻擊的受害者

經歷過網路攻擊且無法阻止攻擊進入他們的網路和/或端點

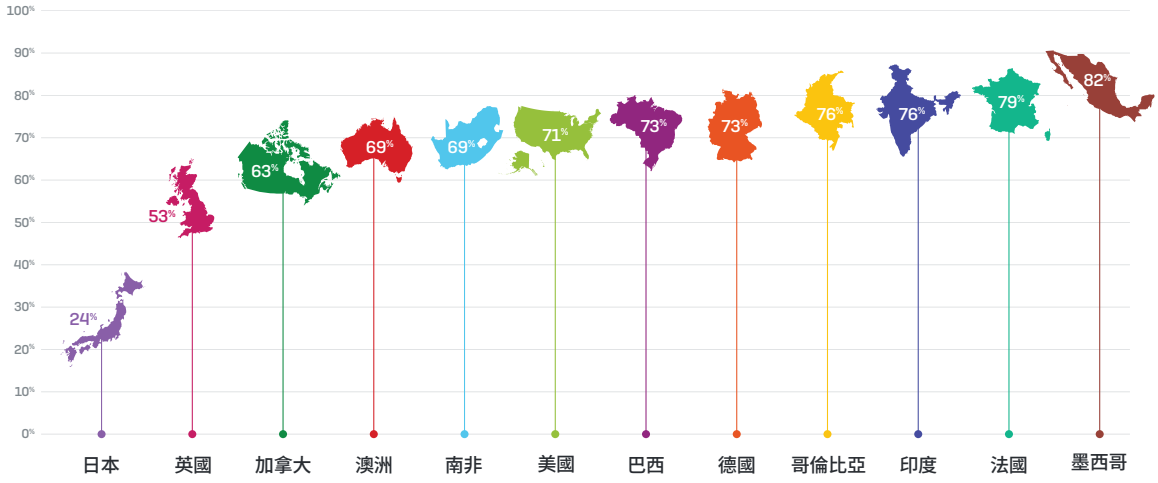


在過去一年中遭受網路攻擊的組織的百分比。詢問所有受訪者 (3,100)

當然，這些還只是被組織發現的一部分攻擊，實際數字可能會更高。

關鍵在於，**每個人都應該假定他們將會成為網路攻擊的受害者**。站在這一立場之上規劃和評估安全策略，而不是假設威脅無法入侵，或者您會僥倖躲過攻擊者的注意。

網路攻擊的等級有明顯的區域差異。日本回報遭受攻擊的次數最少，去年只有 24% 的受害者受到網路攻擊，墨西哥回報的最多，82% 的受訪者承認他們受到攻擊。



在過去一年中遭受網路攻擊的組織的百分比 (按國家劃分)。詢問所有受訪者 (3,100)

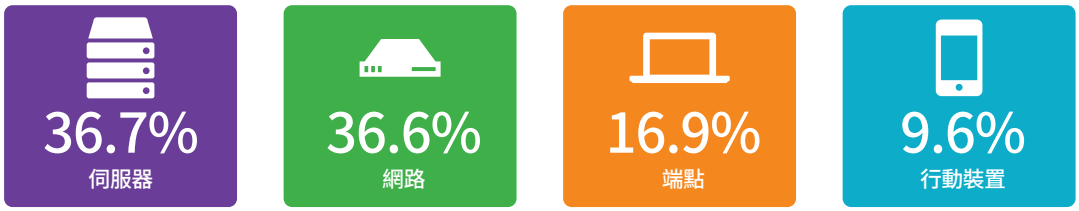
解釋之一是，網路攻擊的目標並非平均分散在全球。在檢視個別威脅時，我們經常會看到明確的地緣關係。例如，迄今為止，Emotet 特別針對美洲、北歐和西歐、澳大利亞和印度，而 WannaCry 則對烏克蘭造成最嚴重的破壞。

跟閃電不一樣，網路威脅會攻擊同一目標兩次

雪上加霜的是，遭受網路攻擊的組織平均遭受攻擊次數是 2。此外，在受訪的組織中，有 10% 在去年遭受了四次或更多次網路攻擊。這代表許多組織在自身的防禦措施方面仍然存在著可被利用的弱點。

大多數攻擊都是在伺服器或網路上發現的

實際檢視在環境中發現網路攻擊的組織，我們發現了一些有趣的現象。



去年受害組織發現重大網路攻擊的位置。詢問去年因網路攻擊而受害的受訪者 (2,109)

1.大多數威脅 (36.7%) 都是在伺服器上發現的

伺服器通常被 IT 管理員視為“安全”，因為使用者不會登入它們，但實際上數據顯示它們面臨的風險最大。現代攻擊通常從端點開始，然後橫向移動到伺服器這個價值更高的目標。組織在伺服器上攔截威脅而非端點，顯示組織對威脅鏈早期發生的事情以及端點安全漏洞缺乏可見度。伺服器上也可能會出現攻擊，因為這會對業務造成最大的影響。

2.約每10個威脅就有1個在行動裝置上發現

在行動裝置上發現 9.6 % 的威脅，數據顯示行動威脅是一個重大的危險，組織需要確保所有可以存取公司資訊的裝置得到妥善保護。

3.印度在行動裝置上發現的威脅幾乎是其他地區的兩倍

雖然全球平均9.6% 的威脅發現在行動裝置上，但在印度，這一數字幾乎是兩倍 (18.8%)。原因可能是技術和文化等因素。首先，印度的 10 支手機中有 9 個執行 Android，這是行動惡意軟體作者的首選平台，因此印度的手機特別容易受到行動威脅的攻擊。印度也是安裝不良應用程式比例最高的國家之一，導致行動裝置遭到感染的可能性提高。此外，印度完全依賴行動裝置作業務用途的比例遠高於世界上許多其他地區，因此行動裝置成為惡意攻擊目標的可能性也更高。

https://economictimes.indiatimes.com/tech/software/the-critical-flaw-in-indias-mobile-security/articleshow/65085273.cms

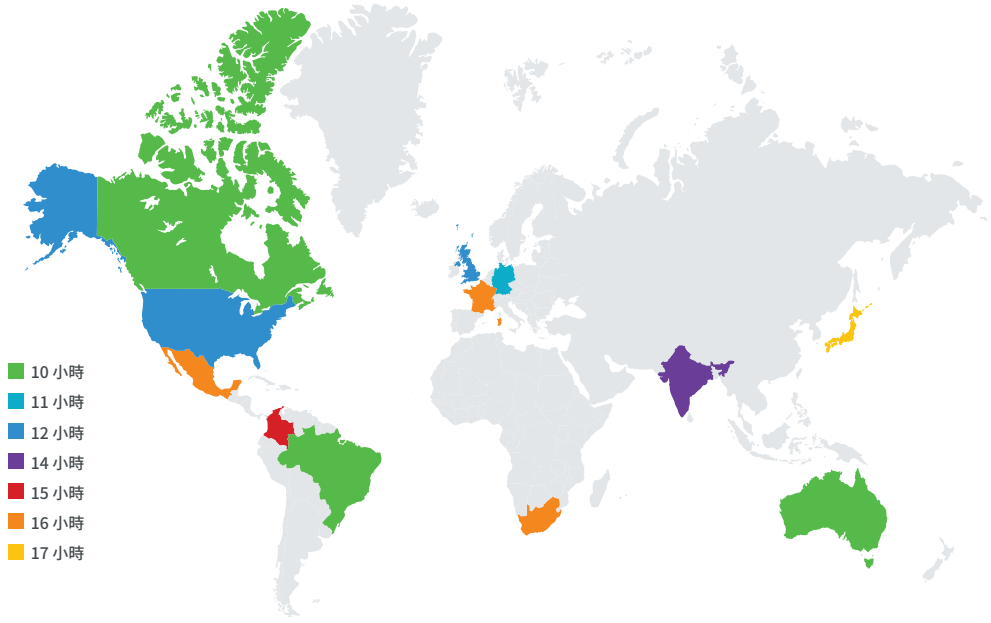
真相#2：IT 團隊缺乏對攻擊者停留時間的可見度

我們詢問組織，去年他們最長需時多久才能發現嚴重的網路攻擊。對於那些知道答案的人來說，平均時間是 13 個小時。

在被偵測出來之前，最嚴重的威脅躲藏在環境中的平均時間

顯然，13 個小時足以讓駭客不受干擾地存取您的系統和資料。在這段時間內，網路犯罪分子有機會造成重大破壞，包括外洩敏感資料、竊取憑證、安裝竊取金錢的木馬程式，以及安裝勒索軟體等。

發現威脅所需的時間因國家/地區而異：澳大利亞、巴西和加拿大最快，平均需要 10 個小時；另一方面，日本 IT 團隊平均需要 17 個小時。



嚴重威脅在被發現之前，躲藏在組織中的平均時間。詢問所有知道威脅在環境中躲藏多久的受訪者(1,744 名受訪者)

13 個小時只是冰山一角

雖然 13 個小時很長，但是請注意，這已是最好的情況。

此外，1,744 名受訪者宣稱發現組織環境中躲藏威脅的平均時間為 13 小時，乍看似乎與其他研究有出入，例如《Verizon 資料外洩調查報告》表示，68% 的資料外洩需要數月甚至更長時間才會被發現。這個數據的差異性極具意義，可以更深入地了解目前沒有專屬威脅偵測和回應團隊的組織所面臨的現實。

有 17% 的威脅，組織在被其被發現之前不知道它們已經躲藏多久。

組織只是管中窺豹。正如先前所見，大多數威脅都是在伺服器上被發現，表示端點缺乏可見度。因此，組織很可能只會看到威脅軌跡的片段，而不是完整情況，導致低估威脅在環境中存留的時間。因此，他們只使用部分資訊做出安全決策，沒有完全了解所面臨的網路風險。

組織缺乏準確評估停留時間所需的工具。對於絕大多數中小型組織而言，他們缺乏能夠完全了解組織中威脅存留時間所需的時間、工具和專業知識。

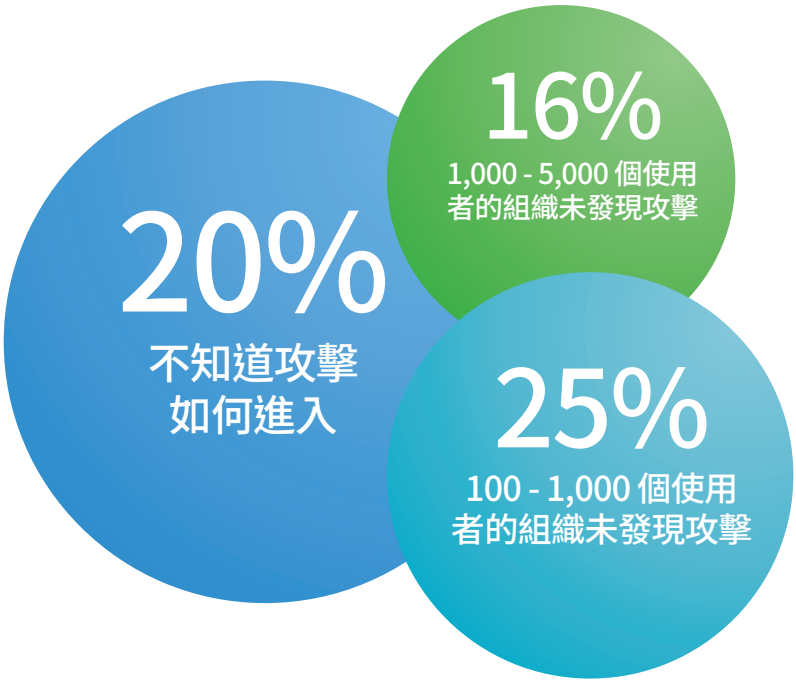
某些類型的威脅比其他威脅更容易被發現。在擴散方法、使用的技術和最終目標方面，各威脅間差異很大。一般以規模取勝 (相信如果發出足夠的攻擊，一定有一個會成功) 的撒網 (spary-and-pray) 式威脅，偽裝能力通常比不上複雜且高度目標性的隱匿性攻擊。事實上，許多這些鎖定“大眾市場”的威脅都會在幾秒鐘內被發現並阻擋。

Verizon 資料外洩調查報告僅著重在資料外洩，而 Sophos 調查的受訪者則是回報更廣泛的網路攻擊。最具影響力、最具破壞性的威脅通常最複雜，停留時間也最長。

由於今日網路犯罪分子的偽裝手法高超，IT 管理員深深意識到需要找出會造成最大損害且難纏的進階型攻擊。實際上，受訪者認為端點偵測和回應 (EDR) 解決方案中最重要的功能，就是識別可疑事件的能力。

真相#3：IT 團隊無法填補他們的安全漏洞，因為他們不知道漏洞是什麼

有效安全策略的一個關鍵要素，就是在第一時間阻止威脅進入組織。然而，五分之一的 IT 管理員不知道最嚴重的網路攻擊是如何進入組織的。因此，他們無法保護這些進入點。



受訪者中不知道攻擊其組織的最嚴重的網路攻擊是如何入侵組織的的分比。詢問在過去一年中成為網路攻擊的受害者 (2,109)

較大型組織比較小的組織更容易知道威脅是如何進入的。原因可能是因為其擁有更多的技術資源和更全面的網路安全解決方案。通常較小的組織根本沒有資源或專業知識來調查攻擊期間發生的事情，相反地，他們只關心如何清除威脅。網路犯罪分子會鎖定各種規模的組織。不過，無法識別安全漏洞，使得小型企業更容易受到攻擊。

真相#4：組織每年耗去 41 天來調查非問題的事情

平均而言，這些組織每月花費 4 天來調查潛在的安全問題，亦即每年 48 天。然而，其中只有 15% 被證實是真正的威脅。因此，組織花費 85% 的時間調查非問題的事情，相當於每年 41 天。顯然這會對財務和生產力產生顯著的影響：

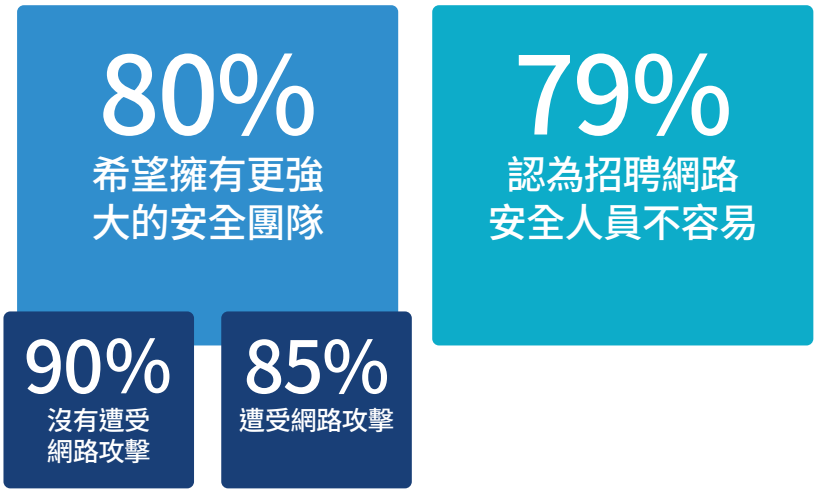
- 直接成本 - 花費大量時間調查非問題的事情所造成的財務和資源影響
- 機會成本 - 由於員工調查非問題的事情而無法進行的 IT 活動

因為其對效率的影響甚大，不難理解為什麼 EDR 最渴求的功能就是識別可疑事件。透過提供有效的工具來幫助組織識別可疑的內容，讓他們可以將有限的資源配置在正確的位置，而不是大海撈針。能夠更有效地識別可疑事件後，組織可以：

- 提高效率：更有效地利用有限的資源
- 減少暴露：更快地發現並解決實際的安全事故
- 把風險降至最低：將資源集中在最有可能使組織面臨風險的可疑事件上

真相#5：由於缺乏安全專業知識，五分之四的組織難以進行威脅偵測和回應

面對這些威脅挑戰，缺乏安全專業知識是一大問題。80% 的 IT 管理員承認他們希望擁有一支更強大的團隊來正確地偵測、調查和因應安全事件，由此可知他們缺乏網路安全技能，組織只能摸索前行。



在這一點，遭受網路攻擊 (85% 想要更強大的團隊) 和未受攻擊 (71% 想要強大的團隊) 的組織意見有別。遭受網路攻擊的組織表現出更強的意識，包括他們缺乏安全專業知識 (他們已經從威脅可以穿過防線得到教訓)，以及難以取得專業的網路安全技能來阻擋今日進階型攻擊的挑戰。

不幸的是，解決這個技術缺口並非易事。雖然組織體認到他們需要更好的協助，但將這種協助導入營運是另一回事。79% 的受訪者認為聘僱網路安全人員不容易。從這個角度來看，讓所需的團隊就緒非常不易，組織將要依靠人工智慧能等技術來填補這個缺口。

真相#6：超過一半的組織沒有認識到其 EDR 解決方案的價值

EDR 已經快速成為必備的技術。接受調查的 10 位 IT 管理員中，有超過 9 位 (93%) 擁有或計劃在其安全措施中準備 EDR。在目前沒有 EDR 的受訪者中，89% 的受訪者計劃將其新增到他們的防禦組合中，61% 計劃在未來六個月內開始著手。從前面所揭露的安全事件調查時間以及缺乏對威脅鏈的可見度來看，這些 EDR 計畫其來有自。

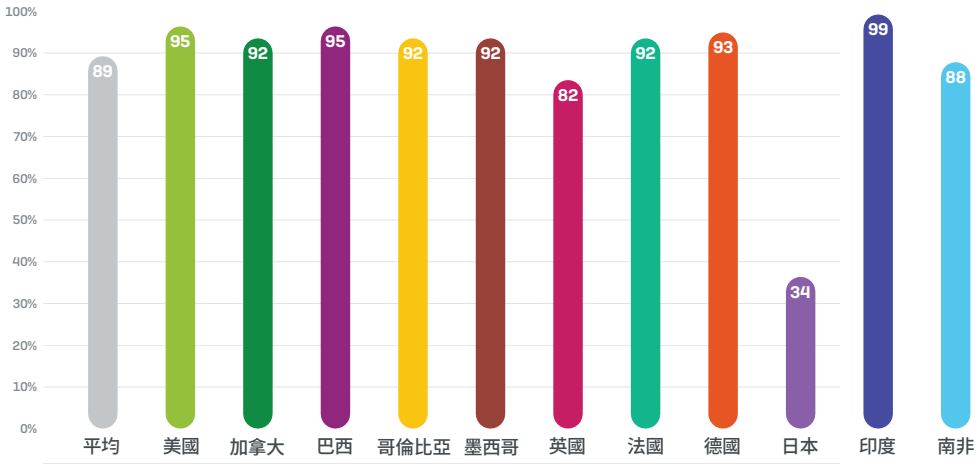
93%
想在安全策略中加入 EDR

10個裡有9個
目前沒有EDR，計劃加入這方案

61%
目前沒有EDR，計劃在6個月內加入

所有組織對於 EDR
大小企業的需求都一樣

有趣的是，我們發現小型和大型組織的 EDR 需求幾乎相等。EDR 顯然不再是大企業的專利，而是適合所有組織的工具。在所有調查的國家中，日本在 EDR 採用計畫方面有不同的見解。



受訪者計劃新增 EDR 功能的百分比。詢問所有目前沒有EDR 的受訪者 (1990)

在日本除外的所有國家中，10 個沒有 EDR 的組織中至少有 8 個計劃新增這項技術。 印度名列榜首，其中 99% 目前沒有 EDR 的組織計劃新增EDR；緊隨在後的是澳大利亞 (97%)、美國和巴西 (均為 95%)。然而，在日本，只有三分之一 (34%) 沒有 EDR 技術的組織計劃將其新增到他們的安全防禦措施中。

只擁有 EDR 不是答案

雖然 EDR 是一個可以提升網路防禦能力的強大工具，但您需要足夠的資源來有效地使用它，並讓投資發揮最大效益。不幸的是，半數以上投資 EDR 的受訪者無法做到這一點。對於 54% 的組織而言，EDR 不具效益，因為他們無法獲得解決方案的所有價值。

54%
無法完全發揮 EDR 解決方案的效益

有趣的是，雖然您會猜想較小的組織會更難從 EDR 投資中獲益，但實際上組織規模沒有影響。各種規模的組織回報的數據幾乎相同。

這些結果有兩種可能的解釋，甚至兩者都會造成一定的影響：

缺乏 EDR 管理資源。組織需要決定讓誰來管理他們的 EDR 解決方案，以確保他們可以充分利用它們。正如我們已經看到的，缺乏網路安全技能是一個普遍的問題。

可用性：員工技能不符。只有在可以有效使用的情況下，技術才能增加價值。組織應充分考慮 EDR 解決方案的易用性，以及它能如何符合現有的員工技能與資源。

真相#7：一朝被蛇咬，十年怕草繩 - 網路受害者汲取教訓

調查顯示，網路攻擊受害者和躲過駭客的組織之間，某些方面存在非常明顯的差異。過去一年中成為網路攻擊受害者的組織會：

- 更加謹慎 - 他們調查事件的次數是其他組織的兩倍
- 花更多時間在網路安全上 - 他們每個月花 4 天調查潛在的事件，對比非受害者花 3 天

可能的因素有：

1. **事件發生後，他們提高了安全性。**受害者可能會更了解網路攻擊的影響，並願意花更多的時間、精力和資源來阻止攻擊。
2. **他們對其環境的了解有限。**不良的網路防禦表示會有更多的威脅入侵，而他們調查的能力也越來越差。因此，他們需要調查的潛在事件更多，使用的工具更少，因此需要更多的時間。
3. **他們更了解要尋找什麼。**由於遭受過攻擊，這些組織對入侵跡象更有警覺性。

關於 EDR 的真相

該調查揭露全球組織在端點安全方面面臨的許多挑戰，以及 EDR 技術面臨的難題。那麼 EDR 的真相是什麼？它如何真正符合端點保護的藍圖？

現實情況是，EDR 可以幫助解決這份調查所發現的許多難題。首先要了解網路攻擊。去年，三分之二的組織遭受過網路攻擊。 但是，17% 的 IT 管理員不知道威脅在環境中存在多久，20% 的人不知道它是如何進入的。EDR 可以解答這些問題，使組織能夠確定攻擊的根本原因、威脅在系統中存在多久，以及發生的潛在影響。有了這些資訊，組織可以實施所需的防禦並填補起他們的安全漏洞。

我們還發現組織平均需要 13 個小時才能發現威脅。EDR 還可以主動識別可疑事件，使 IT 團隊能夠偵測到可能長期未被注意到的攻擊。因此，EDR 能讓組織採取有效措施，降低他們成為另一個網路攻擊受害者的可能性。

該調查的另一個見解是，組織每年花 48 天來調查潛在的安全事件。EDR 可以透過提供專家分析和引導式事件回應來縮短調查時間，以便不同能力程度的團隊都能理解和採取行動。 藉此可大大縮短偵測和回應事件所需的時間。

然而，我們也看到使用 EDR 的組織中有 54% 無法充分發揮他們的解決方案。這就是為什麼選擇適合您的 EDR 解決方案非常重要，而不是一個帶來更多工作的解決方案。正確實作的 EDR 解決方案可以幫助組織更有效地使用有限的資源。

結論

網路安全是全球各種規模的組織面臨的一項永恆挑戰。有鑑於此，我們可以從 12 個國家 6 大洲的 3,100 名 IT 管理員的經驗中學到幾個重點。

首先，在規劃網路安全戰略時，組織應該假定威脅有能力通過防禦網開始。同時，他們還應該注意到他們對威脅的有限可見度，以及導致防護網無法識別並阻止這些威脅的缺口。

其次，絕大多數組織將 EDR 視為安全戰略的組成之一。這不足為奇；EDR 是解決該調查所列挑戰的有效工具。在網路安全技能不足時，智慧型 EDR 解決方案可以提供威脅深入資訊，以及領先威脅一步所需的專業知識。

然而，正如調查所顯示的，單是購買 EDR 還不夠。對許多組織來說，他們對 EDR 的投資都被浪費了，因為他們無法充分發揮 EDR 解決方案。為避免陷入這個困境，每個組織都應充分思考 EDR 解決方案的功能和可用性，然後再將其新增到安全措施組合中。

關於 Sophos

Sophos 是端點和網路安全的全球領導者，有 150 個國家/地區的 1 億多個用戶選擇 Sophos，為複雜的威脅和資料外洩提供最佳防護。使用 **Intercept X Advanced with EDR**，組織現在可了解安全事件的範圍和影響、偵測可能沒有注意到的攻擊、分析檔案以判斷它們是否為威脅，以及在任何特定時刻都能自信地回報組織的安全狀況。內建機器學習和 SophosLabs 的威脅情報可讓您增添專業知識而非人力如需詳細資訊及開始三十天免費試用，請造訪 www.sophos.com/intercept-x。

關於 Vanson Bourne

Vanson Bourne 是科技產業領域的獨立專業市場研究單位。該公司以可靠及可信的研究分析著稱，其聲譽是建立於嚴格的研究原則，以及在所有產業領域及所有主要市場中，探求技術及業務部門資深決策者看法的能力。如需更多資訊，請瀏覽 www.vansonbourne.com。