

作者：

Jon Maier

日期：4/22/2022

話題：Conversational Alpha

# Conversational Alpha：網路安全技術從錦上添花到必不可少

當今數碼世界，把握資料便是擁有黃金，越來越多黑客欲在這個金礦中分一杯羹。近日就有兩間重量級科技公司，向偽裝成執法官員的黑客提供了客戶資料，證明這些公司的網路防禦並未有如預期中強大。<sup>1</sup>此等事件引發外界擔憂，自普京襲擊烏克蘭的網路後，這種擔憂進一步加劇，因每個人、公司及政府都在思考可有黑客潛伏在他們的網路中，令大眾緊張不安。對此，拜登政府警告了一眾與西方實施的製裁及緊張地緣政治有關，並較可能面對網路犯罪的企業。<sup>2</sup>在這種環境下，沒有人可以逃脫網路攻擊，然而仍可以努力阻止這些事情發生。因此，我們預計網路安全支出將繼續增加，網路安全公司將因其經常性收入模式而吸引投資者的興趣。在我們看來，這些因素以及網路安全主題有助於管理投資組合中地緣政治風險的能力使得這種風險敞口至關重要。

## 關鍵要點

- 我們預期協助防止網路犯罪的公共及私人計劃的範圍擴大，並導致在網路安全方面的支出持續增加。一間領先的研究公司預測，2021 年至 2025 年間，全球網路安全支出累計將超過 1.75 萬億美元。<sup>3</sup>
- 拜登政府增加了向美國企業發出緊急訊息的次數，提醒它們需要預防網路攻擊，以免對政府、政府承包商及私營企業等造成影響。下游影響可能是更多的網路安全支出。
- 投資於網路安全主題，會帶來具防禦性的持續經常收入，以及與公營及私營部門為應對日益複雜的網路犯罪相關的增長潛力。

## SolarWinds 黑客事件警示外界需作出行動

2020 年 12 月發現的 Solar Winds 黑客事件是網路安全轉捩點。這個黑客被認為是俄羅斯外國情報局所為。順帶一提，當時約有 100 間公司與十幾個政府機構遭到入侵，包括美國財政部、司法部和能源部以及五角大樓。<sup>4</sup>這次攻擊敲響了警鐘，讓人們意識到黑客影響的侵入性及廣泛性，尤其是當攻擊者破壞高度使用的軟件時。拜登政府瞭解現代化網路安全防禦，並與美國政府簽約的組織更新安全要求的必要性。<sup>5</sup>鑑於俄羅斯對烏克蘭的侵略，拜登政府向美國企業發出了關於防範網路攻擊的緊急訊息。下游影響可能是更多的網路安全支出。

## 戰爭爆發與增加網路安全方面的支出

近日針對烏克蘭銀行與政府部門的網路安全威脅，將網路安全主題帶到了戰爭的前線。為了幫助保護烏克蘭免受網路攻擊，歐盟提供了一個由來自立陶宛、克羅地亞、波蘭、愛沙尼亞、羅馬尼亞和荷蘭的專家組成的網路快速反應小組。私營部門也在伸出援助之手。就在普京入侵之前，微軟的威脅情報中心發現了針對烏克蘭政府部門和金融機構的異常活動，並迅速參與揭露。<sup>6</sup>Alphabet 也是防止烏克蘭網路攻擊的關鍵。<sup>7</sup>



這些反應類似於拜登政府啟動的公營及私人行動計劃，以保護美國的電力、管道及供水部門，並利用政府權力強制實施新的網路安全和網路防禦措施。<sup>8</sup> 政府實現網路防禦現代化的目標，同時包括與眾多國際盟友與合作夥伴繼續合作，以阻止勒索軟件攻擊並公開歸因網路犯罪活動。<sup>9</sup>

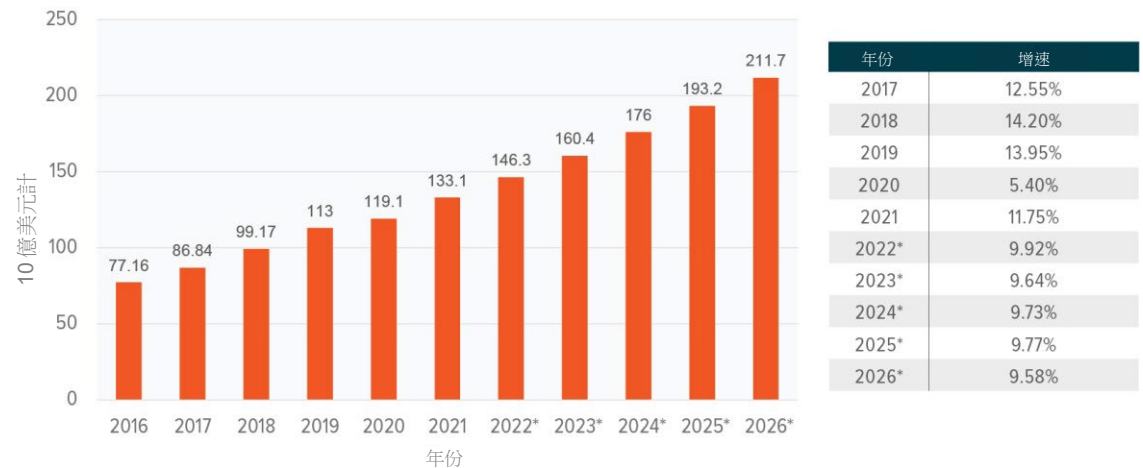
科技界別與烏克蘭政府、歐盟及北大西洋公約組織 (NATO) 的密切協調，在範圍及速度上是史無前例。此回應說明了網路科技的進步及其在全球經濟中發揮的關鍵作用。我們預計此類合作將繼續下去，並可能增加網路安全支出，因為網路犯罪是一種持續存在的風險。

### 網路安全可能是高增長機會

烏克蘭戰爭及相關的地緣政治陰謀，進一步引起人們對強大網路防禦重要性的關注。行政命令與白宮新的網路安全策略，或會進一步被採用，特別是在政府制定監督計劃及規定最低標準的規則時。<sup>10</sup> 我們認為，將網路安全從自願投資轉變為開展業務所需的受監管投資，可能會在美國、歐洲和其他地方加快採納。<sup>11</sup> 考慮到資料安全性及可訪問性之間直接權衡，決心提供對資料的絕對保護，但網路安全支出可能會繼續增長，用於降低風險，在建立更廣泛的投資組合時應該考慮這一主題。

### 全球網路安全收入

資料來源：截至 2022 年 3 月的 Statista 資料



\*預測資料

註：顯示的資料尚未反映俄烏戰爭對市場的影響。

### 網路安全 ETF 可能會增加投資組合的韌性

網路安全科技致力主動抵禦可能的攻擊，同時減輕和修復已發生的攻擊所造成損害。網路攻擊的發生率和嚴重性增加表明對網路安全支出的長期需求。對於網路安全公司來說，這種日益重要的需求創造了一種能夠產生強勁經常性收入的商業模式。因此，透過在這個主題的更廣泛層面上進行投資，投資者可以分散他們在企業之間的風險敞口，因為推動採納度這個因素不太可能快速消失。

在任何領域或主題中挑選贏家總是很困難。雖然需要詳細資料才能有效選擇能夠擊敗市場的個別公司，但投資主題可能會引導投資者選擇 ETF，皆因它們有助分散風險。與網路安全相關的股份，在出現大規模黑客攻擊後，價格往往會上漲；但當應用程式開發人員成為大規模入侵的受害者時，其股價亦可能下跌，因此 ETF 或許是不錯的多元解決方案。



腳註：

- <sup>1</sup> 白宮情況說明書 (White House FACT SHEET): 立即行動以防止潛在的網路攻擊, 2022 年 3 月 21 日 (Act Now to Protect Against Potential Cyberattacks, 3/21/2022)
- <sup>2</sup> 白宮情況說明書 (White House FACT SHEET): 立即行動以防止潛在的網路攻擊, 2022 年 3 月 21 日 (Act Now to Protect Against Potential Cyberattacks, 3/21/2022)
- <sup>3</sup> Cybersecurity Ventures, 由 2021 年到 2025 年, 全球網路安全支出將超過 1.75 萬億美元, 2021 年 9 月 10 日 (Cybersecurity Ventures, Global Cybersecurity Spending to Exceed \$1.75 Trillion From 2021 -2025, 9/10/2021)
- <sup>4</sup> 全國公共廣播電台, 「最可怕的噩夢」網路攻擊: SolarWinds 黑客攻擊事件不為人知的故事 (A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack), 2021 年 4 月 16 日
- <sup>5</sup> 全國公共廣播電台, 「最可怕的噩夢」網路攻擊: SolarWinds 黑客攻擊事件不為人知的故事 (A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack), 2021 年 4 月 16 日
- <sup>6</sup> 網路安全和基礎設施安全局, 烏克蘭破壞性惡意軟件攻擊組織, 2022 年 3 月 1 日 (Cybersecurity & Infrastructure Security Agency, Destructive Malware Targeting Organizations in Ukraine, 3/1/2022)
- <sup>7</sup> 商會商業新聞, 隨著威脅的增加, 專家評估政府和私營部門對網路攻擊的準備工作, 2022 年 3 月 24 日 (Chamber Business News, As threats grow, experts assess government and private sector preparation for cyberattacks, March 24, 2022)
- <sup>8</sup> 紐約時報, 惡意軟件著坦克進入烏克蘭 (NYT, As Tanks Rolled Into Ukraine, So Did Malware)。微軟亦加入戰團, 2022 年 2 月 28 日 (Then Microsoft Entered the War, 2/28/2022)
- <sup>9</sup> CSIS, 共同責任 (CSIS, A Shared Responsibility): 網路安全公私合作, 2022 年 3 月 22 日 (Public-Private Cooperation for Cybersecurity, 3/22/2022)
- <sup>10</sup> 麻省理工學院技術評論, 解決美國無休止的網路安全問題計劃, 2022 年 3 月 18 日 (MIT Technology Review, Inside the plan to fix America's never-ending cybersecurity failures, 18 March 2022)
- <sup>11</sup> 路透社, 歐盟在網路安全擔憂中為歐盟機構提出網路安全規則, 2022 年 3 月 22 日 (Reuters, EU proposes cybersecurity rules for EU bodies amid cybersecurity worries, 22 March 2022)

投資涉及風險, 包括可能損失本金。焦點集中的投資或會帶來更大波幅。

科技主題投資可能會遭受科技的日新月異、激烈的競爭、產品和服務迅速被淘汰、知識產權保護的喪失、不斷演變的行業標準和頻繁出現的新產品生產以及商業週期和政府法規的變化影響。

ETF 的股票以市場價格 (而非資產淨值) 進行買賣, 並且不會從基金中單獨贖回。經紀佣金將減少回報。

本材料代表對特定時間點市場環境的評估, 並非對未來事件的預測, 亦非對未來結果的保證。此資訊無意作為個人或個性化的投資或稅務意見, 並且不得用於交易目的。有關您的投資及/或稅務情況的更多資訊, 請諮詢財務顧問或稅務專家。

Global X Management Company LLC 擔任 Global X 基金的顧問。

