GLOBAL X ETFs研究

網絡安全簡介

作者：
Pedro Palandrani
研究分析師

日期：2019年10月29日

話題：技術

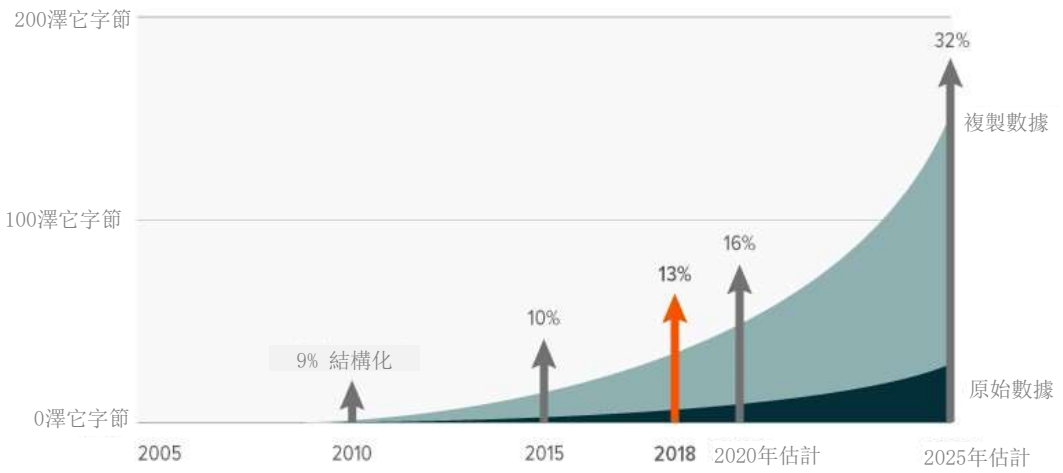
隨著全球變得數碼化，保護有價值和敏感的數據變得越來越重要。技術將有形物件帶入數碼全球和自動化手動流程，以提高生產力。然而，隨著越來越多物件和過程離開實體世界並進入數碼領域，這些技術為新型罪案打開了大門。到2021年，網絡罪案每年可令全球損失6萬億美元，促使個人、公司和政府投入大量資金向網絡安全公司購買複雜的軟件和服務，以保護其專有數據。[1]因此，我們認為網絡安全是一個強大的主題，並將進一步為生產、利用或連接數據正切領域的發展所推動，例如機器學習、雲端計算和物聯網。

大數據的興起

不久以前，地址、健康記錄和財務報表等關鍵資料都儲存在文件櫃中，裏面裝滿按字母順序排列的文件夾。然後，電腦和互聯網的出現建立了一種新的數碼範式，開始以1和0收集和儲存大量資訊，仿佛在一夜之間，技術讓我們只需點擊滑鼠即可輕鬆獲得數據。然而它並沒有就此止步。將舊數據從實體記錄轉化為數碼數據是第一階段，但現在，我們所做的幾乎所有事情都會留下數碼軌跡：我們購買了什麼、我們觀看了什麼、我們與誰交談以及我們去了哪裡都被各種平台收集。據估計，全球每天產生超過2.5萬兆字節（2.5×10^{18}）的數據，相當於過去兩年產生所有數據的90%。[2] 從另一個角度來看，2020年全球每天產生的數據字節將是可觀測宇宙中星體數量的40倍。[3]

各種數碼技術的出現進一步推動這種數據爆炸，包括：1）物聯網，將從洗碗機到電視等日常設備連接互聯網，以收集和傳輸數據；2）雲端計算，提供廉價、可擴展和高效的數據基礎設施服務，減少企業向更依賴數據轉型的障礙；3）機器學習和人工智能，讓人們可以從龐大的數據集中發現深刻的見解，使數據變得前所未有的有價值。

每個IDC收集/創建/複製的新數據（數據量、年度、全球（澤它字節））
資料來源：Bondcap，2019 年互聯網趨勢。注意：1 PB = 100 萬 GB； 1 澤它字節(ZB) = 100萬拍字節。結構化數據表示數據已被組織，以易於搜索。複製數據= 源自原始數據的數據。



數據激增 = 網絡威脅激增

但是，隨著更多有價值的數據被創造，網絡犯罪分子越來越有動力竊取並在黑市出售數據、持有數據以圖勒索贖金或暴露私人資料。最常見的是網絡犯罪分子利用數碼手段竊取專有或私人數據、知識產權(IP)和金錢。隨著技術的發展，網絡威脅也在不斷發展。例如，當物聯網將日常物品連接互聯網時，它為網絡犯罪分子創造了新的運作途徑。交通燈被非法入侵、汽車被盜或個人健康設備被操縱現在都變得有可能。

一間網絡安全公司每天可攔截超過1億個威脅，[4] 相當於每秒攔截千多個威脅。但是，只要一次泄露就可對公司和用戶造成嚴重損害。

2013-14年，雅虎！全部30億個帳戶分別被兩次攻擊非法入侵，可說是21 世紀最嚴重的數據泄露事件。這些泄露事件暴露了用戶的姓名、電子郵件地址、出生日期、電話號碼、密碼和安全問題。
令人不安的是雅虎！於2017年才證實這些襲擊，即事件實際發生3至4年之後。

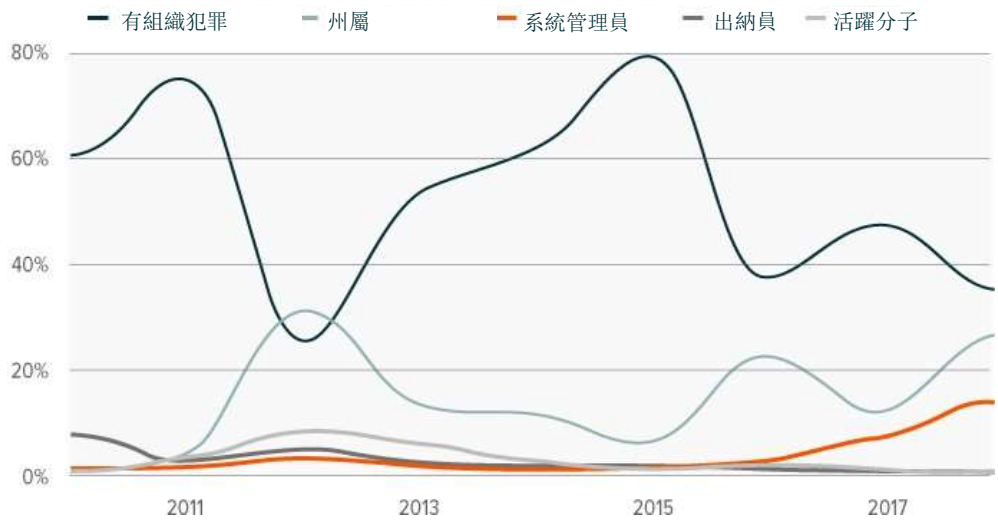
2017年，美國最大的徵信機構之一Equifax宣布數據泄露，包括社會安全號碼、出生日期和駕駛執照號碼，影響1.43億消費者。2018年底，萬豪國際宣布發生數據泄露事件，包括護照號碼等個人資料，導致5億個帳戶受害。

通常，外部行為者是網絡犯罪的罪魁禍首。襲擊雅虎！的是由國家資助的行為者，這種情況並不罕見；全球數據泄露中約23%由外國政府贊助的黑客進行襲擊，[5] 另外 39%為有組織犯罪。

但外部行為者並非唯一的問題，內部泄露也會發生：為了個人或經濟利益，或者有時只是人為錯誤。

數據激增 = 網絡威脅激增（泄露）

資料來源：威訊無線，2019年數據泄露調查報告。



需要一個解決方案生態系統

防禦網絡威脅是一個行業。網絡安全服務專注於保護網絡的所有層面，包括網關、身份、電子郵件、雲端、網絡安全和端點。網絡安全公司利用不同的技術打擊未經授權和惡意活動，可能包括以下任何一種技術，或更可能是以下各種技術的組合：[6]

- 身份驗證和授權：利用權限識別和驗證用戶活動的過程。
- 密碼學：允許以數學函數保護通信的過程
- 合法使用模式的自動分析：用於提醒管理員異常行為的自動使用模式分析
- 入侵偵測和風險緩解：防止惡意行為者滲透系統的主動方法
- 數據完整性驗證：進行分析以確保數據保持完整，並評估被損壞或更改的範圍
- 電腦取證：追蹤網絡威脅和犯罪的反應機制，以確定事件發生的方式和原因

我們預測主動預防機制將演變為包括人工智能(AI)和機器學習(ML) 的方法。AI和ML可以幫助偵測網絡釣魚，識別試圖看似合法的虛假網站和鏈結。視覺識別技術的進步是AI和ML可以幫助下一代網絡安全公司偵測潛在威脅的另一個領域。當然，AI和ML機制的發展需要存取大量數據，包括用於訓練目的的惡意軟件等惡性數據。

網絡安全投入資金必然上升

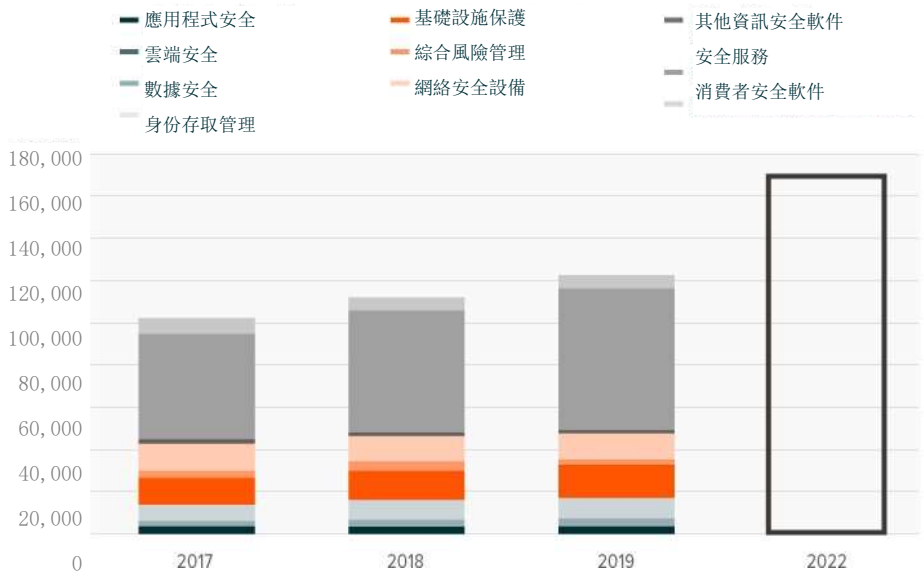
網絡安全是資訊科技支出增長最快的類別之一。美國各地的首席資訊官(CIO)都將網絡安全列為他們的優先支出。[7] 公司在網絡安全上投入數百萬美元是可以理解的：2019年，公司數據泄露的平均總成本為390萬美元，其中36%的成本由失去客戶信任所致。[8]

隨著被發現惡意程式數量達到創紀錄的9.25億，到年底，全球在安全相關軟件、硬件和服務上的支出可達1,240億美元。[9,10] 到2022年，全球總支出可達1,704億美元，五年複合年增長率 (CAGR)達10.9%。[11] 由於網絡威脅激增，擔心攻擊成本和後果的組織現在通常視網絡安全為一種成本節約措施。

同樣，政府在網絡安全實施上的支出亦持續增長。歐盟《通用數據保護條例》(GDPR)於2018年5月生效，提倡以確保安全以及提供保護和透明度的方式處理個人數據。

在美國，網絡安全是優先事項，監管機構朝著類似GDPR的立法方向持續努力。2019年聯邦預算中有150億美元用於網絡安全，比2018年增加了 5.834億美元，即4.1%。[12] 網絡安全也是州級問題。加利福尼亞州於2018年通過了一項數碼私隱法，授予人民控制他們資料的權利。此類立法對企業造成緊迫感，以迅速加強其網絡安全，並避免任何潛在的醜聞。

2017-2022年全球分類安全支出（單位：百萬美元）
資料來源：高德納諮詢公司。2019-2022年為預測數據。



結論

所有行業向數碼化轉型意味著配備網絡安全的能力不能被動。主動確保安全是必須的。防止數據泄露事件發生可以減輕不良的經濟和政治後果。數以百萬計並日益複雜的網絡威脅說明網絡安全公司服務需求有機會持續上升。網絡安全扮演核心的角色，利用更強大的安全和私隱措施及政策保護全球公司、消費者和政府機構。

1. Cybercrime Magazine, “Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021”(2017-2021 年全球網絡安全支出預計將超過 1 萬億美元), 2019年6月10日。
2. Domo, “Data Never Sleeps 5.0”, 2017年。
3. Domo, “Data Never Sleeps 7.0”, 2019年。
4. 註：從 Zscaler Cloud Activity Dashboard 檢索的數據（於10/11/2019獲得）。這是一個數據不斷變化的實時工具。
5. 威訊無線, “2019 Data Breach Investigations Report”(2019 年數據泄露調查報告), 2019年。
6. 註：由卡尼基美隆大學語言技術研究所開發的網絡安全分類法。分類只考慮了網絡安全的技術範疇。於2019年10月15日獲得。
7. IDC, “Developing Your Security Fabric: A Transformational Approach for State Government” （開發您的安全架構：州政府的轉型方法), 2019年5月。
8. IBM, “Cost of a Data Breach Report 2019”(2019年數據泄露成本報告), 2019年。
9. 高德納諮詢公司, “Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019” (高德納預測2019年全球資訊安全支出將超過1,240億美元), 2018年8月15日。
10. Palo Alto Networks, “2019 Analyst Meeting”(2019年分析師會議), 2019年9月4日。
11. 高德納諮詢公司, “Forecast Analysis: Information Security, Worldwide, 2Q18 Update”(預測分析： 全球資訊安全, 2018年第二季更新), 2018年9月14日。
12. 白宮, 網絡安全資金。於2019年10月24日獲得。