作者：

Pedro Palandrani
研究分析師

日期：2021 年 2 月 2 日
題目: 主題式

GLOBAL X ETFs 研究

引領網絡安全興起的四間公司

今時今天，公司發生重大網絡事故可能只是遲早的問題。軟件管理公司 SolarWinds 便在 2020 年 12 月發生事故了。有些人描述這是美國史上最大的網絡攻擊，犯案者在該公司的 Orion 軟件中引入了一個漏洞，可以讓攻擊者破壞運行該軟件的伺服器。可怕的是，這次襲擊打擊了關鍵的聯邦機構和組織，也許損害了國家安全。早期估計有大約 250 個機構受到影響。

網絡威脅事件在美國和全球變得日益普遍和精密複雜。網絡攻擊數字的上升趨勢預計將導致全球保安支出從 2020 年的約 $1,250 億美元增加至 2024 年的 $1,750 億美元。[1] 向雲端遷移的加速促成了這種增長。目前只有三分之一的工作利用雲端計算科技進行。產品或服務的訂購續訂率下降或波動，或知識產權的失去或受損可能會對利潤產生不利影響。

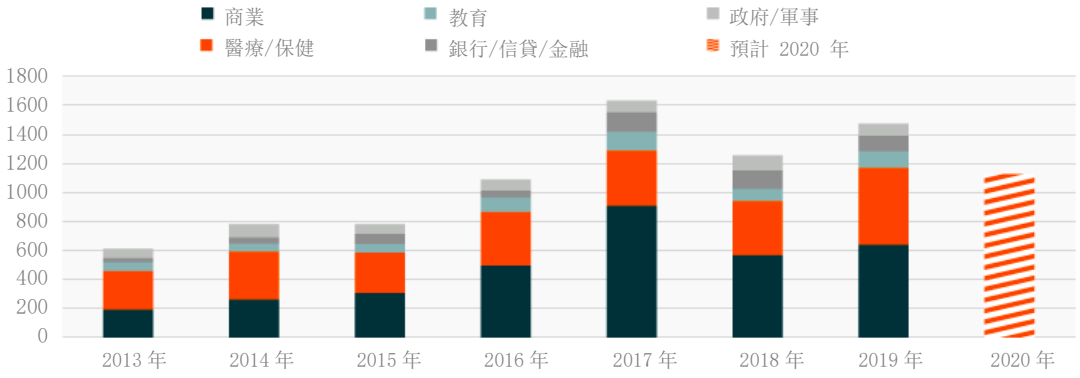
我們將在本文中重點介紹在網絡安全主題中扮演關鍵角色的四間公司：

- CrowdStrike: 領先的終端防禦平台
- Zscaler : 提供安全網關的雲端原生平台
- Okta: 身份和存取管理領域的主要參與者
- Mimecast : 檢測和阻截惡意電子郵件的頂級解決方案提供商

預計 2020 年有超過 3.8 億人的數據被洩露[3]

美國的資料外洩數字

資料來源：身份盜竊資源中心，2020 年。



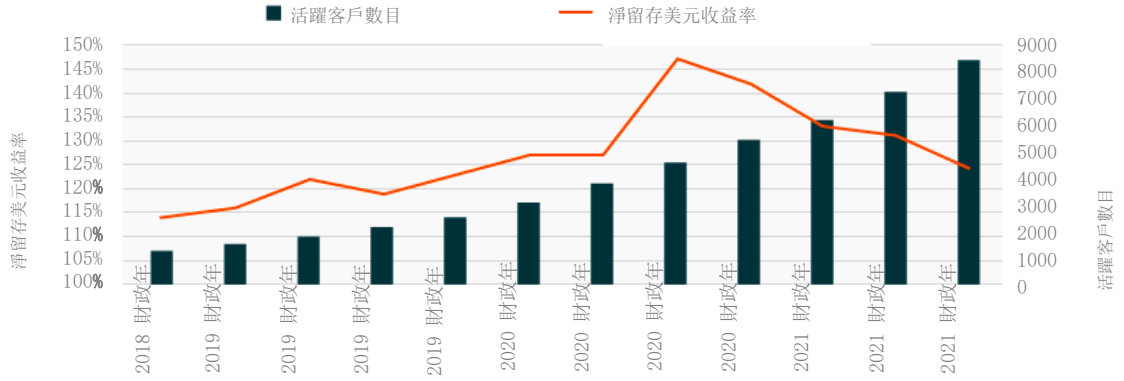
CrowdStrike: 領先的終端防禦平台

CrowdStrike 是終端防禦平台（EPP）的領先網絡安全公司之一，幫助客戶保護終端用戶設備（如流動設備、筆記本電腦和伺服器）的安全。CrowdStrike 採用軟件即服務（SaaS）解決方案，可持續工作，以檢測和分析威脅。該解決方案是 100% 以雲端為本的體系結構，與傳統非雲端計算的公司相比，CrowdStrike 具有競爭優勢。該公司可以在許多不同的資訊科技環境中快速而有效地設置其解決方案。例如該公司在 2020 財政年度第四季內以短短10天就吸納了 Target 成為新客戶。

過去，本地防病毒軟件通過監視和掃描終端文件中的已知威脅來防止網絡攻擊。但是該安全層在很大程度上是被動的。現今最好的產品都利用人工智能。CrowdStrike 的人工智能產品稱為 Threat Graph，是該公司人工智能網絡安全解決方案背後的主腦。Threat Graph 幫助 CrowdStrike 每周處理 4 萬億個網絡事故，每分鐘作出 5,000 萬個決策。[4]數據集在 CrowdStrike 的雲端中進行處理，從而產生網絡效應。分析的客戶數據越多，Threat Graph 人工智能技術就會變得越完善。

雲端為本的解決方案可以轉化為可觀的經常性收入。截至 2020 財政年度第四季，CrowdStrike 的總收入來自訂購。[5]另外，值得注意的是自 2019 財政年度第一季以來，CrowdStrike 的淨留存美元收益率一直高於 120%。[6]比率大於 100% 意味著通過價格上調或向上銷售機會，現有客戶群實現了淨增長。

CROWDSTRIKE 淨留存美元收益率（左軸）和活躍客戶（右軸）
資料來源：Global X ETF，CrowdStrike 公司文件。



Zscaler: 安全網關的領先機構

Zscaler 是另一個 100% 以雲端為本的網絡安全平台，因此無需購買或管理硬件，並且該平台不斷進行更新。Zscaler 每天作出 175,000 次雲端安全更新。[7]Zscaler 的安全網關（SGW）解決方案主要專注於通過其Zscaler Private Access（ZPA）為客戶提供對內部管理應用程式（如公司電子郵件）的安全存取，以及通過 Zscaler Internet Access（ZIA）為外部應用程式提供解決方案，例如客戶關係管理（CRM）軟件。安全網關可防止不安全的流量通過外部網絡應用程式進入內部網絡。Zscaler 就像一個中間人，將用戶直接連接應用程式，而無需通過他們的網絡。

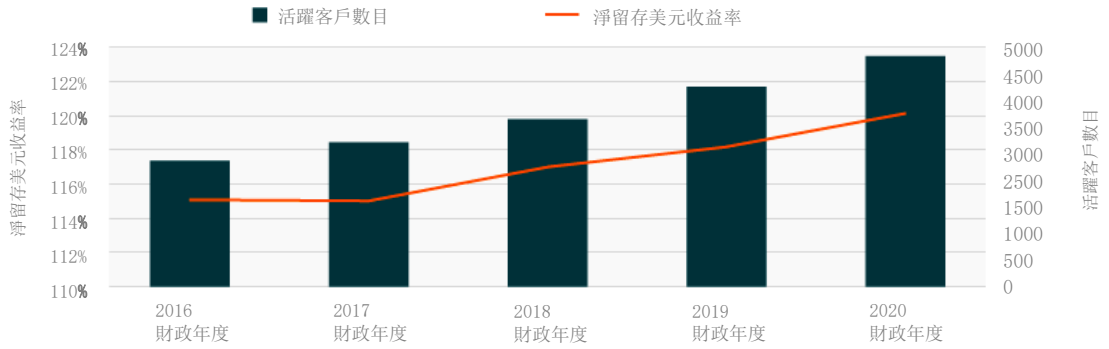
Zscaler 提供的功能最終可能會淘汰虛擬專用網絡（VPN）技術。與傳統的 VPN 解決方案相比，該公司的 ZPA 解決方案更易於調動和管理，而且更安全。ZPA 用戶可以存取內部應用程式，而無需連接到一間公司的網絡或在互聯網上暴露這些用戶。該體系結構還完全限制網絡攻擊於進行侵害期間在網絡上水平移動的能力。該公司將該架構描述為零信任網絡，並且從來不會將網絡擴展到所有用戶。本質上，網絡變得不再受重視，而互聯網則成為新的公司網絡。[8]

現在，確保利用筆記本電腦、智能手機和其他物聯網（IoT）設備存取內部和外部應用程式的安全是組織的首要考慮，尤其是在遠程和混合工作逐漸成為主流的背景之下。根據研究公司 Gartner 的調查，2023 年將有 60

% 的企業逐步淘汰大部份遠程存取 VPN，轉而採用零信任網絡（如Zscaler 的產品）。[9]

截至 2020 財政年度末，Zscaler 的淨留存美元收益率達到 120%，表示其現有用戶群持續增長。[10]重要的是，該公司相信僅 ZIA 和 ZPA 的現有客戶就可帶來 6 倍的向上銷售機會。[11]

Zscaler 的淨留存美元收益率（左軸）和活躍客戶（右軸）
資料來源：Global X ETF， Zscaler 公司文件。



Okta：發展迅速的身份和存取管理公司

Okta 是身份和存取管理（IAM）領域的領先網絡安全公司。其垂直結構專注於讓正確的個人和員工以正確的理由在正確的時間存取正確的資源。[12]公司越來越多地利用多因素身份驗證（MFA）、應用程式編程接口（API）存取管理和單點登入（SSO）等身份解決方案來確保正確的用戶被授權存取各種應用程式。

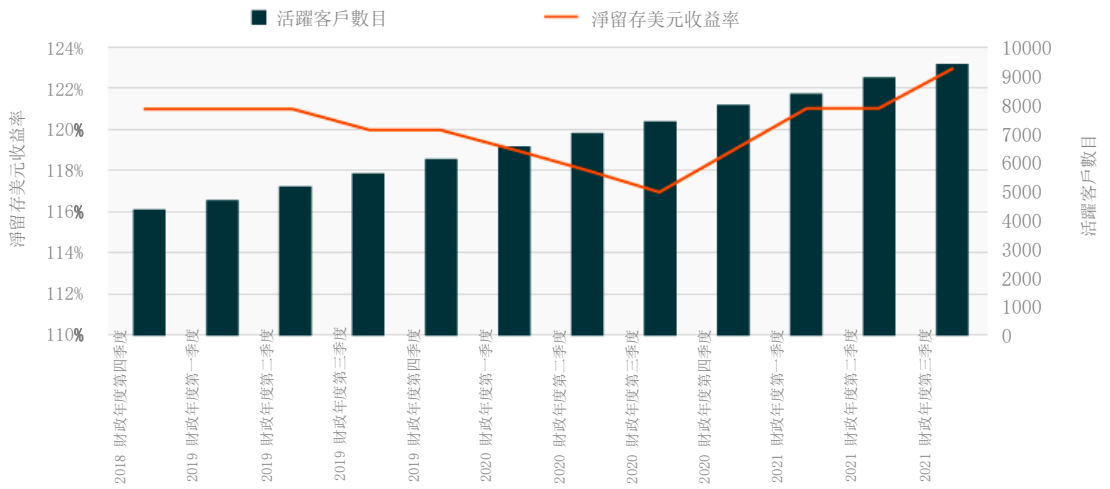
IAM 垂直結構的公司也有望受惠於向遠程和混合工作環境的轉型。通過讓員工在多個地點工作，並利用不同的設備進行連接，IAM 可以讓資訊科技部門監察誰人在指定時間內存取特定應用程式。IAM 還可以幫助公司監察和保護向必須存取某些內部應用程式的承包商或客戶授予的接觸點。

從終端用戶的角度來看，Okta 的 IAM 解決方案讓他們存取單個門戶中的所有應用程式。此功能將有關登入的服務台查詢減少了 50%，並使用戶登入和使用新應用程式的速度提高了 50%。[13]Okta 估計，勞動力身份的總潛在市場價值達 $300 億美元，客戶身份的市場價值 則達 $250 億美元。[14]

與 CrowdStrike 和 Zscaler 相似，Okta 的解決方案是雲端原生的。由於訂購服務產生的收益，該公司 94% 的收入是經常性的。Okta 是另一間擁有穩定淨留存美元收益的公司，在 2021 財政年度第三季之前的 12 個月中錄得 123%，較上一季度增長 2%。

OKTA 的淨留存美元收益率（左軸）和活躍客戶（右軸）

資料來源：Global X ETF，Okta 公司文件。



Mimecast: 電子郵件安全的頂級提供商

在可能是最為人熟悉的網絡安全垂直結構種類——電子郵件安全閘道中，Mimecast 處於領先地位。95% 的網絡攻擊利用電子郵件進行，使其成為機會性和針對性攻擊的首選渠道。[15]全球約有 10 億商業電子郵件用戶，故此 Mimecast 的商機是巨大的。[16]現今，該公司擁有約 1,500 萬用戶，全球市場滲透率為 1.5%。[17]

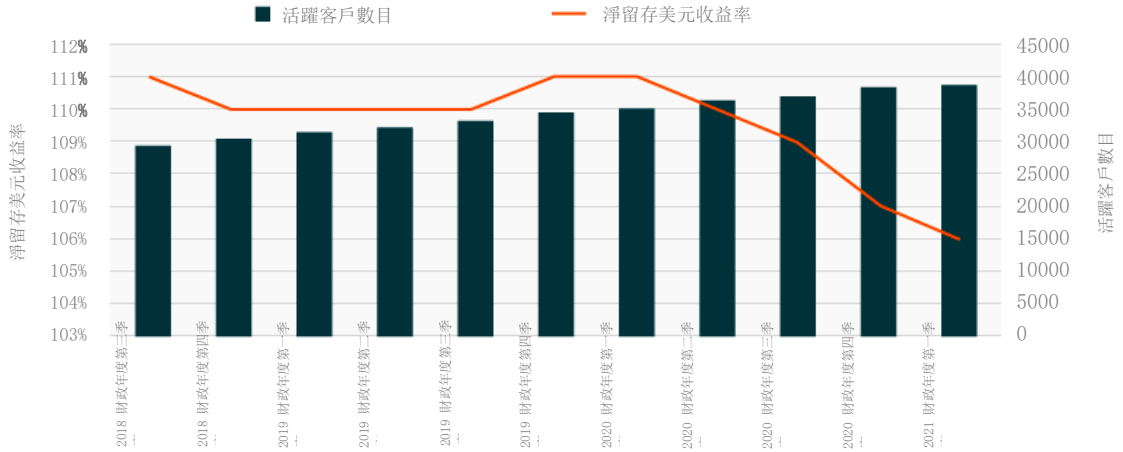
大規模網絡釣魚和針對性魚叉式網絡釣魚攻擊的目標是通過與收件人產生共鳴並強迫他們採取行動的電子郵件來吸引收件人。[18]攻擊者希望竊取金錢或知識產權等關鍵資料。FBI 估計，在 2013 年 10 月至 2018 年 5 月期間，電子郵件外洩造成了 $120 億美元的損失。[19]現今，電子郵件網絡釣魚和假冒欺詐一直存在，但是由於新冠肺炎大流行，人們花在網絡上的時間越來越長，為更多此類行為提供了成熟的環境。實際上，僅在新冠肺炎的首 100 天內，電子郵件網絡釣魚和假冒欺詐就增加了 30%。[20]

Mimecast 提供的解決方案可以檢測和阻截包含已知或未知惡意軟件、惡意 URL 以及假冒高級職員或第三方組織（如銀行、聯邦機構甚至客戶和供應商）的電子郵件。Mimecast 通過人工智能功能對傳統檢測技術進行了補充，例如深度學習以識別對工作不安全的圖像和徽標、機器學習以檢測電子郵件中的異常風險模式以及監督學習以對高風險鏈結進行分類。

Mimecast 還採用了雲端原生架構，為吸引的業務模式增添靈敏度。過去幾年，該公司的淨留存美元收益率保持在 100% 以上，為網絡安全公司的商業模式增添實力。[21]

Mimecast 的淨留存美元收益率（左軸）和活躍客戶（右軸）

資料來源：Global X ETF，Mimecast 公司文件。



結論

最近，網絡安全不僅成為了頭條新聞，而且預算也日益增加。網絡攻擊的數字不斷上升，加上其對全球各行業和政府的潛在影響，對於組織進行橫跨多種業務功能的安全營運，網絡安全工具變得不可或缺。無論是電子郵件、身份管理、存取內部和外部應用程式還是保護終端用戶設備，這裡重點介紹的四間公司對於日益數碼化的世界變得更加安全扮演著關鍵的角色，並體現了網絡安全行業的多面性本質。

註：

1. 2020 年 8 月 13 日 IDC “Ongoing Demand Will Drive Solid Growth for Security Products and Services, According to New IDC Spending Guide”（根據新的 IDC 支出指南，持續的需求將推動安全產品和服務的強勁增長）。
2. 2020 年 6 月 8 日 IDG “2020 IDG Cloud Computing Survey”（2020 年 IDG 雲端計算調查）。
3. 2020 年 10 月 14 日身份盜竊資源中心 “Identity Theft Resource Center's 2020 Q3 Data Breach Analysis and Key Takeaways”（身份盜竊資源中心的 2020 年第三季度數據外洩分析和重點）。
4. 2020 年 12 月 CrowdStrike “Corporate Overview”（公司概述）。
5. 同上。
6. CrowdStrike，（n4）。
7. 於 2021 年 1 月 19 日獲得的 Zscaler “Investor Relations: Cloud Stats”（投資者關係：雲端數據）。
8. 於 2021 年 1 月 19 日獲得的 Zscaler “An Introduction to Zero Trust Network Access”（零信任網絡存取簡介）。
9. 2020 年 6 月 Zscaler “VPN Alternative”（虛擬專用網絡替代方案）。
10. 2021 年 1 月 11日 Zscaler “Zscaler 2021 Analyst Day”（Zscaler 2021 年分析員日）。
11. 同上。
12. 於 2021 年 1 月 19 日獲得的 Gartner “Identity and Access Management (IAM)”（身份和存取管理（IAM））。
13. 於 2021 年 1 月 19 日獲得的 Okta “Single Sign-On”（單一登入）。
14. 2020 年 12 月 2 日 Okta“Q3 FY 2021 Results”（2021 財政年度第三季業績）。
15. 2021 年 1 月 19 日獲得的 Mimecast “The 2020 Gartner Market Guide for Email Security”（2020 年 Gartner 電子郵件安全市場指南）。
16. 2020 年 11 月 Mimecast “Mimecast Investor Presentation”（Mimecast 投資者介紹）。
17. 同上。
18. 於 2021 年 1 月 19 日獲得的 Mimecast “Email Security That Protects Your Organization”（保護您組織的電子郵件安全）。

19. 2018 年 7 月 12 日 FBI “Business E-mail Compromise The 12 Billion Dollar Scam”（企業電子郵件外洩: $120 億美元騙局）。
20. 2021 年 1 月 19 日獲得的 Mimecast “The State of Email Security: Download Hub”（電子郵件安全狀態：下載中心）。
21. Mimecast，（n16）。

.