Market Share

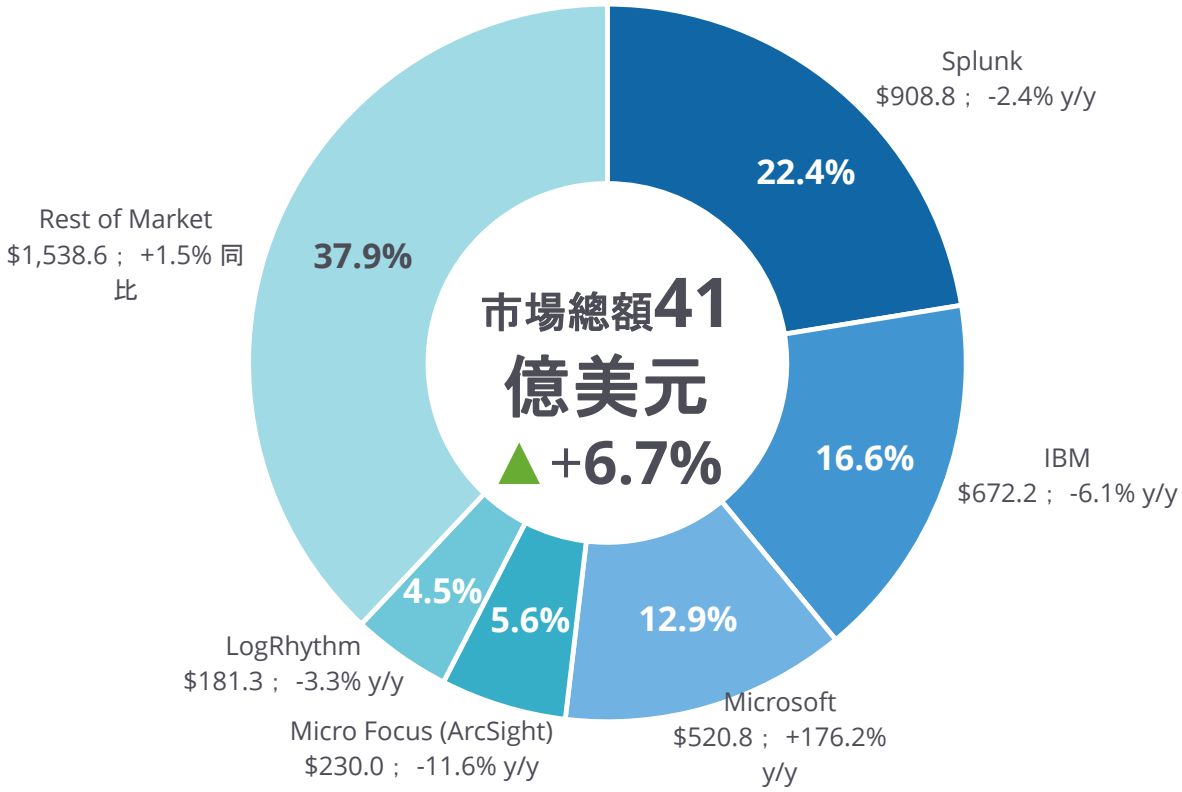
2020 年全球安全資訊和事件管理（SIEM）解決方案市佔率：以 SaaS 為重點的崛起

Michelle Abraham　　Christopher Kissel

IDC 市佔率資料

圖 1

2020 年全球安全資訊和事件管理（SIEM）解決方案市佔一覽



注：2020 年市佔率（%）、收入（百萬美元）和成長率（%）

資料來源：IDC，2021 年

本節摘錄

本節內容直接摘錄自《2020 年全球安全資訊和事件管理（SIEM）解決方案市佔率：以 SaaS 為重點的崛起》（文件#US46350821）。本節摘錄包括以下全部或部分章節：執行摘要、對技術供應商的建議、市佔率和市場背景等專門與 Splunk 有關的部分，以及與 Splunk 有關的任何數字和或表格。

執行摘要

安全資訊和事件管理（SIEM）是一個正在轉型的產品，從內部部署到 SaaS，以及從日誌管理、基於規則的告警和合規性報告等基本功能到新增更多遙測源、告警優先順序和基於機器學習（ML）進行異常檢測的次世代平台。新的擴展檢測和回應（XDR）工具是否會對 SIEM 市場產生影響仍是未知數。

除了更新 SIEM 以保持領先於開源日誌管理工具外，SIEM 供應商還需要提供更穩定的價格，這樣客戶就不必因為負擔不起獲得所有資料的費用而進行艱難的取捨。供應商還應當提供開箱即用的整合和定制服務，盡可能讓客戶輕鬆獲得所需資料。

雖然 Splunk 仍然在 SIEM 市場上佔據著領先地位，但微軟 Azure Sentinel 的快速崛起，也分食其市佔率。新玩家正在對於 SIEM 市場帶來改變，並有望取代傳統的 SIEM 供應商，如果傳統的 SIEM 供應商不轉向 SaaS 解決方案並持續更新功能集，很可能會遭到淘汰。2020 年，新玩家取得了收入的增長，而傳統的供應商則面臨收入減少、市佔率降低。

疫情也很可能為 SIEM 供應商的收入造成影響。隨著資安設備的發展，SIEM 變成了一套非常昂貴的工具，企業許可證價格高達 8 萬美元，甚至更高。概念驗證（POC）需要一些內部部署的工具，且客戶和供應商雙方的高層皆將參與採購週期，其中許多合約因疫情隔離導致的工人無法到崗而被擱置。不過要注意的是，隨著 SIEM 供應商轉向 SaaS 模式和改善儲存的計價模式，對於員工人數在 500-2500 人的公司來說，SIEM 將成為一個更可行的方案。

這項 IDC 研究提供了 2020 會計年度安全資訊和事件管理（SIEM）的全球市佔率資料。

SIEM 合約常在兩個面向受到質疑。首先，SIEM 可以提供的遙測資料（從使用者行為分析（UBA）到網路情資再到工作流程）正在受到 XDR 平台的挑戰；第二項挑戰則是對於日誌管理的支援能力。這使得公有雲服務商成為 SIEM 市場中更有力的競爭對手，如 AWS、微軟 Azure（雲端內支援，而不僅僅是其 SIEM）和 GCP 可以提供更多的安全相關服務。

「SIEM 市場正處於一個不確定的時期，供應商們正在釐清在 SIEM 與 XDR 平台上應該提供哪些功能」Security and Trust 部門研究總監 Michelle Abraham 表示。「哪些功能對於未來大多數客戶是必需的，目前還沒有定論」

對技術供應商的建議

SIEM 根本上仍然是一種收集日誌資料的技術，日誌資料是組織中發生的任何事情的唯一真實來源。SIEM 還能夠對於日誌進行關聯性分析，提醒分析人員應該注意的事件，幫助資安維運中心（SOC）的分析人員瞭解事件、確定事件優先順序，並生成合規報告。因此，IDC 提出以下建議：

- **給客戶提供多使用再多購買的理由。**我們特意先強調「多使用」，然後才是「多購買」，SIEM 供應商有很完善的分析平台，但透過獲得的數據量來計費，導致了 SIEM 一直以來面臨的難題，即客戶因為價格因素，無法把所有方案都投注於此一平台。因此，若依據每 GB 數據獲取量來計價，將使那些想要獲得更多日誌資料的客戶望而卻步；同時，訓練機器學習模型也需要歷史資料，因此供應商亦應建議客戶勿將日誌資料用完就刪除。
- **使定價穩定且可預測。**在可能的情況下，將資料留在原處，以避免從雲端移動資料時產生的出口費用，並幫助客戶瞭解在他們想要獲取得所有日誌資料來源以及於儲存期間內，所需的預算為何。

- **確保日誌資料獲取不會為客戶帶來阻礙。**隨著企業的資料分散於內部部署、公有雲和 OT 環境，資安團隊想要獲得的數據量有增無減，聰明的供應商將幫助客戶盡可能獲取更多的資料來源，SIEM 供應商不會希望因為自己不支援獲取某種類型的資料，而失去上牌桌的資格。供應商應確保資料可以與其他資安工具共用，以實現 SOC 的高效率運行。SIEM 與 XDR 之主要差異在於資源來源，XDR 解決方案僅能獲取端點資料，此將限制 SIEM 解決方案的對於威脅檢測的能力。
- **透過內建或整合 SOAR 功能，為客戶自動區分應採取行動之告警與無效告警。**增加提供回應的能力，以自動化的方式修復威脅，從而提高資安團隊的效率。例如，SIEM 供應商 Micro Focus，將 SOAR 整合至 SIEM 的功能中，而不是作為附加模組。
- **開發設計精良、易用的介面，無需大量的維護工作或專業知識，特別是現今許多 SOC 皆面臨人力短缺的挑戰。**與其他資安供應商的預先整合，將使得實施 SIEM 方案變得更為容易、開箱即用，且不會增加客戶的成本。
- **同時使用監督式和非監督式的機器學習，因為前者為客戶提供了開箱即用方案，而後者可以針對特定的客戶環境進行調整**。這兩種類型的告警和統計彙編都應該整合基於邏輯的分析功能，從而更快地生成資訊。使用者和實體行為分析（UEBA）不應該再是一個新增模組，而是整合在產品中。
- **確切地與 MITRE 框架相符。**要獲知競爭對手的進展，MITREATT&CK 框架可以算是業界標準，現在許多網路安全公司的控制台就運用到了 MITRE ATT&CK 的許多技術要素，也許在不久的將來，MITRE Shield 框架也將被許多網路安全公司採用。在任何情況下，藉由 ATT&CK 框架將攻擊階段可視化有助於 SOC 分析師確定收集哪些資訊，以及在何處設定屏障以阻止不法分子的入侵。
- **在 SIEM 方案中加入威脅情資以豐富日誌資料，確定告警優先順序。**許多 SIEM 供應商有內部的威脅情資來源，同時也可以從第三方供應商處獲得威脅情資。這一領域的併購活動熱度高漲，例如，Rapid7 以 3.35 億美元的現金加股票併購了 IntSights、Splunk 則併購了 TruSTAR。
- **從風險的角度來考慮異常情況。**風險可以被認為是在不久的將來很可能造成危害的漏洞，風險評分是指根據資產對目前發生的惡意軟體攻擊的敏感程度、資產的關鍵性以及針對資產的告警權重，對資產進行的風險評分。Devo、LogPoint、Micro Focus、NetWitness、Splunk 和 Sumo Logic 皆具有個別資產風險評估之能力。

市佔率

2020 年 SIEM 領域的頭條事件是微軟的突然崛起。2019 年 7 月底，微軟宣佈推出 Azure Sentinel SIEM 服務。IDC 估計，微軟在 2019 年獲得了 1.886 億美元的收入，2020 年微軟獲得 5.208 億美元的收入，維持強勁的成長動能。（微軟僅正式宣佈其 SIEM 保護了 9000 個工作負載）。

2020 年，微軟的崛起在 SIEM 市場中受到高度的關注，從各方面來看，基於雲端的 SIEM 供應商（Sumo Logic、Securonix 和微軟）分食了 SIEM 的市場，對於提供企業許可證的傳統供應商，其市佔率所剩無幾。（Exabeam 是一個例外，不過它已經轉向雲端解決方案以尋求新客戶）

2020 年，Splunk 的 SIEM 收入為 9.09 億美元，相較於 2019 年的 9.31 億美元有所下降，部分原因可能是轉向雲端計價模式所造成。2019 年 Splunk 簽訂的企業授權合約平均為期三年，以預付費為主；現在，合約期限為一年，按月計費，每月自動遞增，因此要到 2025 年初，才能入帳全部的合約金額。Splunk 的年度經常性收入（ARR）正在增長，Splunk 也積極尋求續約，據其公司報表，每份合約實現了 41%的增長。

SIEM 總收入包括硬體、軟體(軟體許可證與 SaaS)以及維護和支援。在本分析中，我們未納入託管 SIEM 服務，如 Alert Logic 公司的服務（見表 1）。

表 1

2019 年和 2020 年，全球安全資訊和事件管理(SIEM)供應商收入（百萬美元）

等級	供應商	2019 年	2020 年	2020 年市佔率（%）	2019-2020 年成長率（%）
1	Splunk	930.9	908.8 年	22.4	-2.4
2	IBM	715.6	672.2	16.6	-6.1
3	微軟	188.6	520.8	12.9	176.2
4	Micro Focus (ArcSight)	260.1	230.0	5.7	-11.6
5	LogRhythm	187.5	181.3	4.5	-3.3
	其他	1515.5	1538.6	37.9	-1.5
	合計	3,798.2	4,051.7	100.0	6.7

注：資料包括 SIEM 軟體收入達到 2000 萬美元以上的公司。

資料來源：IDC，2021 年 9 月

年度合作夥伴

我們選擇了 2020 年收入份額最高的 SIEM 供應商 Splunk，以及其他幾家在 2020 年收入高速增長的供應商，作為我們的年度合作夥伴。

Splunk

鑒於客戶事先不清楚要擷取多少資料，無法確定合約金額，因此最大的 SIEM 供應商 Splunk 調整了其定價模式。Splunk 推出了基於受保護裝置需求的雲端方案套餐，客戶亦可以選擇基於工作負載的套餐，其定價則是基於對搜尋、分析和資料處理資源的使用量，而不是資料獲取量，已有超過 50%的客戶選擇了 Splunk Cloud。

2020 年，Splunk 的 SIEM 收入為 9.09 億美元，相較於 2019 年的 9.31 億美元有所下降，部分原因在於從軟體許可到雲端服務的轉變。2019 年 Splunk 簽訂的企業授權合約平均為期三年，以預付費為主；現在，期限為一年，按月計費，每月自動遞增，因此要到 2025 年初，才能入帳全部的合約金額。

2021 年 5 月，Splunk 併購了 TruSTAR，以獲得對客戶外部情資來源進行標準化與管理的能力，並將其與 SIEM 整合，以生成關於優先指標和威脅的告警。客戶不再需要浪費時間去手動整合來自多個來源、入口網站和 API 的情資，客戶表示該解決方案將使回應時間更快。

Splunk 的長項一直是它獲得非結構化資料的能力，其解決方案支援超過 1000 種不同的資料來源，其中許多是來自其社群和合作夥伴；所有資料來源皆可於任何格式下被擷取，無需預定義的模式。大型客戶每天需獲取並分析 PB 級的結構化和非結構化資料，透過聯合搜尋，可以在資料所在的位置存取資料。UEBA 可用於企業內部和雲端部署，在即時獲得資料時對資料進行行為分析，以實現即時檢測。

2021 年 6 月，Splunk 宣佈推出 Splunk Enterprise Security（SES）6.6。SES 6.6 的主要新功能和改進包括：

- **改進的事件審查。**SES 6.6 的一個細微改進是能夠根據 UEBA、資產的價值、優化的網路效能分析和告警鏈等方面的異常情況來衡量風險。雖然這些特徵是非連續的，但技術之間的相互關聯很重要，SES 6.6 將整合所有的 IOC 情報，以輸出高保真的告警，並強化對於事件的可視性，包括將基於風險分析（RBA）的事件時間軸視覺化。
- **基於安全隔離區的架構。**透過安全隔離區，Splunk 客戶可與資安資訊共享與分析中心(ISAC)和資安資訊共享與分析組織(ISAO)共用遙測資訊，以實施更大的防禦網。
- **擴展開放框架。**Splunkbase 現在可容納 1200 多個應用程式。為了使 Splunk 在安全方面更具價值，開放框架包括一個開放的參考 API，供其他單點資安產品建立自己的服務模組。

同樣在 2021 年 6 月，Splunk 宣佈 Splunk Security Cloud 和 Splunk SOAR Cloud 作為新增模組。對於使用 AWS 並希望獲得更簡單解決方案的客戶，Splunk 提供了 Splunk Security Analytics for AWS；簡化版本的 Splunk Security on AWS 將對小型 SOC 團隊有幫助，這些團隊無法在 SIEM 上投入太多預算，也沒有時間使用所有的功能。

在 2022 會計年度第一季，Splunk 超過 50%的軟體預訂收入是來自於雲端而非軟體許可證，其雲端收入正在急劇攀升，同比增長 73%，1/3 的雲端 ARR 來自於全新的客戶。SIEM 和可觀察性都有助於其雲端服務模式的發展，Splunk 一直專注於 DevOps、ITOps 和 SecOps 客戶，希望幫助組織中的這些團隊進行協作，消除過去的資料孤島。

最後，還有兩件值得注意的事項。2021 年初，Splunk 雲端平台取得了 SOC2 合規性認可；2021 年 8 月，Splunk 正式宣佈 Splunk Phantom 的淡出，現在將該平台稱為 Splunk SOAR。該公告既是一種宣傳，更是表明可同時於於企業內部和雲端環境中提供 Splunk 安全協調服務。

市場背景

基於已知規則的 SIEM，由於其缺乏機器學習(ML)、圖形化能力、行為分析(UEBA)和其他分析能力，正在被能夠檢測未知事物的 SIEM 所取代。SIEM 解決方案現在基本都包含使用者行為分析功能，要麼是內建功能，要麼是新增模組，視供應商而定；具備 ML/AI 功能的供應商將領先於 SIEM 開源方案，企業也可以利用 Spark 等大數據技術建構自己的 SIEM，或者在使用 SIEM 的同時使用大數據平台。

如果平台足夠靈活，允許開發團隊自己完成所有的整合，則可以進行自訂設定(DIY)或使用開源 SIEM，然而自訂設定平台可能需要更多的支援，使其比常規商用方案更為昂貴。由於缺乏安全人員，公司往往不願意自己建構和管理 SIEM，但開源方案在小型組織中永遠有一席之地，因為開源日誌管理已經足夠完善；而大型企業擁有自己的開發團隊，則可在開源 SIEM 的基礎上建立日誌管理能力。

企業也正在將 SaaS 工具納入其安全堆棧。隨著包括資安團隊在內的工作人員轉向遠端工作，擁有 SaaS 模式的 SIEM 供應商在 2020 年表現出色；而傳統的 SIEM 供應商通常擁有一些客戶仍然需要內部部署的解決方案，此為僅提供 SaaS 模式的 SIEM 供應商所無法滿足的市場。

對於那些選擇不使用託管安全服務的小型客戶，一些供應商可提供包含日誌管理、報告和搜尋功能的基礎型的 SIEM。新的 SaaS 產品，如 Splunk Security Analytics for AWS 即針對此類客戶提供服務。

SIEM 已經不僅僅是收集日誌資料並基於規則發出告警，還能實現威脅檢測和威脅獵捕。通常 SIEM 會納入威脅情資功能，使其獲得的日誌資料具有關聯性，而威脅情資可針對特定的垂直領域進行定制，如合規性報告。

一些組織不止使用一個 SIEM，可能是一個用於雲端環境，一個用於特定用例。要開發一個為每個垂直領域客戶提供所有功能的 SIEM 十分困難，所以組織使用專門定制的 SIEM 也是可以理解的。SAP Enterprise Threat Detection 和 LogPoint for SAP 專為使用 SAP 的企業設計，使 SAP 使用者能夠輕鬆地將資料映射到 SIEM，以提供告警。在一篇部落格中，Orange Business Services 的一位分析師提

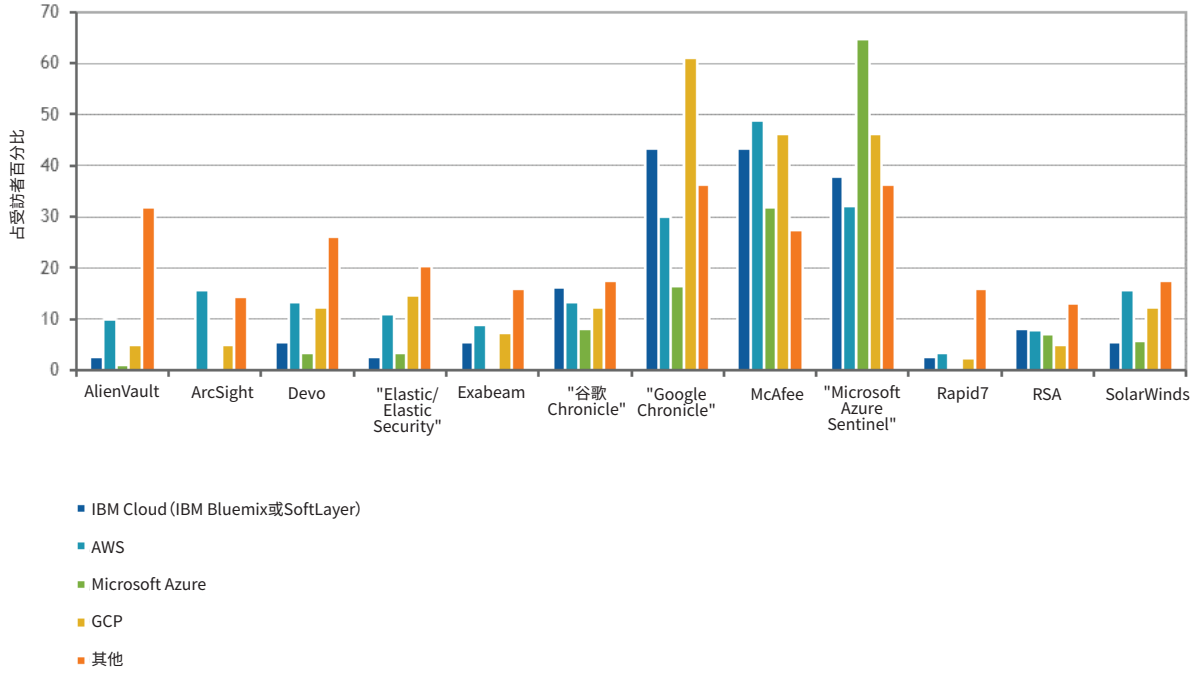
到，可以將 Elastic SIEM 新增至之前的 SIEM，因為該 SIEM 方案使用的是第一代關聯引擎。我們認為，新的 SIEM 更有可能與傳統的 SIEM 一起運行，至少在開始時是這樣。

基於 IaaS 雲端供應商提供的 SIEM 在其自家環境中的效能往往是無法比擬的，因此一些客戶將這些 SIEM 用於他們的雲端環境，並將不同的 SIEM 用於遙測，並將所得資料彙集到主 SIEM 中。非 IaaS 供應商的 SIEM 解決方案提供商計劃在能夠獲得和監測所有類型的工具、基礎設施、網路和應用程式方面維持其中立性，以彙集所有資料進行分析。

IDC 在 2020 年 12 月發佈的*《雲端安全調查》*介紹了企業是如何選擇方案來監控其雲端環境的（見圖 2）。Google Chronicle 最常被用來監控 GCP IaaS 環境，而 McAfee 在 AWS 方案中的市佔最高，在 Azure 方案中，Azure Sentinel 的佔比最高。

圖 2

安全和資訊事件管理用於管理和監測主要 IaaS 供應商的警報



n = 403

資料來源：IDC 的*《雲端安全調查》*，2020 年 12 月

重要的市場發展情況

SIEM 平台需要分析大量的資料集，因此，一些具有大數據背景的供應商看到了安全市場的機會。這些供應商的優勢在於能夠即時獲得一個組織的所有資料，並轉換資料以利查詢，以及使用 ML/AI 進行進階分析。

Datadog 宣佈在 2020 年 4 月全面推出其安全監控產品 Security Monitoring，目的是促進資安分析師和 DevOps 團隊的協作；Security Monitoring 則彙集了來自 450 多個開箱即用的整合安全日誌檔和資料，

透過威脅情資豐富遙測資料後，用一個基於規則的引擎生成告警，以便在數據流中進行即時檢測，而該平台是按分析日誌的數據量(GB)定價。

供應商正在決定是否將 XDR 打造為其平台的一個核心功能。有些人認為傳統的 SIEM+UEBA+SOAR 是新的或下一代的 SIEM，與 XDR 方案相同。無論哪種情況，SIEM 和端點供應商都需要不斷發展以滿足目前對 XDR/次世代 SIEM 的要求。隨著供應商自身對 XDR 的定位，已經出現了一些併購案例，例如，2021 年 2 月，CrowdStrike 併購了 Humio，以獲取其資料擷取和分析之能力。

目前來說，XDR 和 SIEM 的發展前景如何，我們不得而知。XDR 的資料分析和資料規模將與 SIEM 相當？還是 XDR 將成為輕量級的 SIEM？XDR 是否能夠處理 SIEM 所擅長的合規活動？還是說，在 SIEM 方案下，將 SOAR 功能整合到 XDR 中，就像 UBA 一樣？一些 SIEM 客戶將他們的 XDR 資料納入 SIEM，就像他們之前對 EDR 資料執行的操作一樣。

微軟已經在 SIEM 領域大放異彩，未來我們可能還將看到 Google 和 AWS 的身影。雖然我們今日未將 Google Chronicle 算作 SIEM，但它確實已經具有 SIEM 的許多特性和能力，能夠大規模地擷取、儲存和分析來自許多其他資安工具的遙測資料，它沒有合規報告功能，而是與 Cyderes 合作，在 Chronicle 之上建構該功能層；在計價方式上，Chronicle 採用的是基於員工數量的固定價格，並且具備擴展性以處理海量資料。

7 月，Google 宣佈將 Looker 和 BigQuery 整合至 Chronicle 安全分析平台。Looker 能夠藉由建立儀表板與生成報告將工作流程視覺化，而 BigQuery 資料湖則有助於結合資料集進行分析。Google 的 Autonomic Security Operations 解決方案堆棧以 Chronicle 為基礎，包括藍圖、整合和產品功能，以幫助客戶將 Google 的工具和專業知識用於自己的資安維運，且 Chronicle 的使用環境並不僅侷限於 GCP。。

AWS 提供 Amazon GuardDuty 威脅檢測功能，以分析來自 AWS 環境的遙測資料，並與其他 AWS 安全服務功能（如 Amazon Detective、Amazon Inspector、Amazon Macie 和 AWS Security Hub）協作。企業可能選擇 Google 或 AWS，而不是其他 SIEM 平台，使得目前 SIEM 供應商的佔比降低。如圖 2 所示，企業通常使用 IaaS 供應商作為其雲端環境中的 SIEM 方案供應商，這減少了非 IaaS SIEM 供應商的收入機會。

一些供應商可以對 SIEM 中的資料進行加密，使篡改日誌資料變得更加困難，若客戶需要此功能或監管規定需具備此功能，其他供應商應該也會跟進。

方法論

網路安全市佔率文件是所有 2020 年報告的彙總，並反映了 2021 年 5 月初已知的市場趨勢。首先需要說明的是，我們基於全球資安市場(Worldwide Security Tracker)作出了收入估算。

在本研究中，IDC 關注了幾個主要市場。這意味著，一個 SKU 產生的收入只能計算一次（例如，不能在 SIEM 和策略與合規性方面重複計算收入）。其次，在這些市場收入估算中，有來自實體設備的收入（IDC 的 Software Tracker 報告中沒有列出這些收入），儘管這些收入在整個行業中只占很小的一部分。

IDC 的軟體市場規模和預測基於的是商務軟體收入。IDC 使用*商務軟體*一詞來區分商用軟體和定制軟體，商務軟體是任何類型的程式或代碼集，可透過銷售、租賃、出租或即服務(as a service)的方式獲取收入，其收入通常包括初始和持續使用商務軟體許可證的費用，這些費用可能是合約中不可分割的一部份，包括獲得產品支援和/或其他與使用權許可費用，或者這種支援可能需另外收費；升級可能涵蓋在持續使用權中，也可能另外收費；商務軟體必須可用於競標。這些用例被 IDC 算作商務軟體收入。

商務軟體收入不包括來自訓練、諮詢和系統整合的服務收入，這些服務與使用權許可是獨立的（或未組合的），但確實包括透過不同定價方案提供軟體功能的服務中包含的軟體隱含價值。它是指進一步分配到市場、地理區域，有時還包括作業環境的商務軟體總收入。有關詳細資訊，請參閱 *IDC 的《2021 年全球軟體分類法》*（IDC #US47588620，2021 年 4 月）。

作為本文件的一部分，如前所述，IDC 向本研究所涉及的公司發送了收入估算，供其審查和提出意見。在任何情況下，IDC 都不會披露供應商為某一特定收入估算規定的透明度。許多公司可能會提供精確的收入估算，或為分析師提供 10-K/10-Q 或相關報表，有些公司是私人公司或未予置評，其他公司則提供了大概的估算值。此外，安全和產品團隊與大的 Tracker Group 協作，以特定供應商的總收入為基礎，對收入進行了調節。（換句話說，將不同技術收入相加，等於一家公司的軟體總收入）。分析師可以使用的其他工具包括得標合約、新聞稿和雇員人數。此外，損害參與供應商的保密性是不公平和不道德的行為。

本研究中呈示的資料只是 IDC 的估計。

注：由於四捨五入，本文件中的所有數字可能並不精確。

市場定義

安全資訊和事件管理涉及以日誌為中心的平台，用於策略和合規性保證，以及啟動安全調查。SIEM 解決方案旨在從多個來源彙總資料，以識別潛在的攻擊、入侵、濫用或失敗的事件模式。事件關聯透過將告警和錯誤日誌整合到一個簡短且易於理解的方案中，簡化並加快對網路事件的監控。產品還可以整合和儲存由 SIEM 處理的日誌資料，這項技術包括收集和傳播威脅情資、提供威脅預警服務、提供對策資訊，以及來自 SIEM 產品的資料被提供給策略和合規性解決方案，以獲得一致的報告。

SIEM 的正式定義很重要，有幾個原因，主要是為了確保透明度，這麼說有一點模糊，但 IDC 認為一個平台被認為是 SIEM 平台的標準之一是，其必須像 SIEM 方案一樣促進資料處理，包括必須接收各種日誌和流程，配備專門用於威脅調查的儀錶板，並能夠進行合規性報告。因此，SIEM 不同於安全分析產品，使用安全分析產品，使用者可以靈活地指定特定的安全框架並針對該框架運行資料，以更好地進行資料分析。SIEM 與威脅情資產品也不同，威脅情資產品旨在接收各種威脅情報源，並為企業提供一個平台，以對照各種不同的威脅情報源，然後進行資料分析。通常情況下，企業會將商業智慧（BI）平台與開源平台相結合來索引資料，但 IDC 並沒有將其歸類為 SIEM 方案。然而，理想情況下，SIEM 結合了安全和威脅分析、威脅情資、商業智慧和資料庫管理等功能，以提供搜尋、儲存、索引服務，以及最重要的是，提供促進事件檢測和回應的資料。

相關研究

- *2021-2025 年全球安全資訊和事件管理預測：日誌的功能性是否過時？*（IDC #US46350721，2021 年 9 月）
- *IDC 市場概觀：SIEM，2021 年第三季*（IDC #US48166021，2021 年 8 月）
- *2020 年全球 SIEM、漏洞管理、策略和合規性以及 AIRO 支援技術的市佔率：在疫情期間測試、調整和驗證*（IDC #US47724120，2021 年 6 月）。
- *2021-2025 年全球網路安全分析、情報、回應和協調預測：傳統的 SIEM 和漏洞管理技術—它們將如何生存並繼續茁壯成長*（IDC #US47081021，2021 年 6 月）
- *2021-2025 年全球安全即服務預測*（IDC #US47956921，2021 年 6 月）
- *當今的 SOC 方案中使用了哪些安全工具？*（IDC #US47681521，2021 年 5 月）

關於 IDC

國際資料公司（IDC）是面對資訊技術，電信和消費者技術市場的市場情報，諮詢服務和活動的全球領先供應商。IDC 幫助 IT 專業人士、企業高級主管和投資機構制訂以事實為基礎的技術採購決策和業務發展策略。IDC 在全球擁有 1,100 多名分析師，為 110 多個國家/地區的技術和行業機會與趨勢提供全球、區域和當地的專業知識。在 IDC 超過 50 年的發展歷史中，眾多企業借助 IDC 的策略分析實現了其關鍵業務目標。IDC 是全球領先的技術媒體，資料和行銷服務公司 International Data Group（IDG）的全資子公司。

全球總部

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
推特帳戶：@IDC
blogs.idc.com
www.idc.com