Magic Quadrant 安全資訊與事件管理

Gartner RAS Core Research Note G00167782, Mark Nicolett, Kelly M. Kavanagh，
2009 年 5 月 29 日

法規遵循與資訊安全需要促成 SIEM 技術廣泛使用，現在在諸如應用程式活動監視之類的領域也出現新的使用案例。

您需要哪些資訊

本文件修訂於 2009 年 6 月 2 日。

如需相關資訊，請參閱 gartner.com 上的 Corrections 頁面。

資訊安全與事件管理 (SIEM) 技術可針對網路、系統與應用程式的安全事件，提供即時監視與歷程報告。投資 SIEM 部署多半是爲了因應法規遵循報告需求，不過，組織應該也要運用 SIEM 來增強安全作業、威脅管理與事件回應功能。

SIEM 技術部署可支援以下三種主要使用案例：法規遵循報告/記錄管理、威脅管理，或涵蓋上述兩種使用案例的 SIEM 部署。大部分的組織都需要實作以上三種功能的一般 SIEM 部署，只不過在使用案例優先順序與功能需求方面各有不同。

SIEM 市場是由可針對這三種使用案例提供最基本支援的供應商與產品所組成，不過，在架構方法以及相關的安全事件管理 (SEM)、安全資訊管理 (SIM)、使用者活動監視與法規遵循報告支援等級方面各有不同。

考慮部署 SIEM 的資訊安全經理，首先應定義法規遵循報告、記錄管理、使用者與資源存取監視、外部威脅監視，以及安全事件回應等方面的需求。在定義需求方面，可能需要納入其他工作小組，包括審核/法規遵循、IT 作業、應用程式擁有者與事業單位經理。組織還應該說明其網路與系統部署拓蹼，以便可能的 SIEM 供應商能夠針對企業專有的部署情境提出解決方案。

2009 年 Magic Quadrant for SIEM 在評估技術提供者時，不僅會評估最常見的技術 選擇情境 – 投資 SIEM 專案是爲了解決法規遵循報告問題，還會評估次要需求，即獲得有效的威脅監視與 SEM。SIEM 的產品架構與部署選擇形形色色，記錄管理、SEM 與使用者監視功能也林林總總。

組織可能需要就每個象限中的供應商評估其 SIEM 產品，以因應特定的功能運作與作業需求。產品選擇決策應取決於組織在各方面的特定需求，例如 SIM 與 SEM 功能的相對重要性；部署的容易性與速度；IT 部門’ 的支援能力；以及與既有網路、資訊安全與基礎架構管理應用程式的整合。

Gartner

MAGIC QUADRANT

市場概觀

在 2008 年，SIEM 市場成長大約 30%，總營收大約 10 億美元。SIEM 需求依然強勁（投資專案數目仍在成長），但我們看到焦點比較集中在戰術面，四個象限當中第一象限的部署減少了。儘管大環境有所不同，但我們預計這個市場區隔的營收在 2009 年依然會良好成長。

目前的經濟情勢不但使得 SIEM 供應商無法獲得外部資金，大家對於以下這類私人投資供應商的可靠性也增加疑慮：

- 現金流尚未轉爲正值，而且無法獲得進一步資金
- 目前的投資人當中有部分需要撤回資金

在 2008 年，High Tower 停止營運（其資產遭 netForensics 購併），而一些小型的私有 SIEM 供應商則削減人員與通路擴充方案，以便能夠控制成本。

SIEM 供應商全貌

21 家供應商符合 Gartner' 2009 SIEM Magic Quadrant 的入選標準。其中 9 家是點解決方案供應商，有 12 家是同時銷售其他安全或作業產品與服務的供應商。現在已有眾多企業部署 SIEM 技術，因此供應商也相應改變其銷售與產品策略。大型供應商則致力於整合其 SIEM 技術與相關的產品或服務組合，以便他們可以銷售 SIEM 給現有客戶。無論規模大小，供應商皆在發展銷售通路以打入北美洲的中階市場，此外，他們也開始進軍歐洲、中東與非洲以及亞太地區，因爲這些地區的 SIEM 部署日益成長。

有些 SIEM 技術的購買決策是無法與之競爭的，因爲大型供應商在銷售這類技術時，會連同相關的資訊安全、網路或作業管理技術進行組合銷售。CA、IBM 與 Novell 整合他們的 SIEM 產品以及相關的身分與存取管理 (IAM) 產品，然後在 IAM 相關交易中一併銷售 SIEM 解決方案。NetIQ 整合他們的 SIEM 技術、安全配置管理與檔案整合監視技術。Symantec 向使用其端點安全產品的大型企業銷售 SIEM，並且整合他們的 SIEM 以及 IT 控管、風險與法規遵循產品。Cisco 將他們的「監視、分析與回應系統 (MARS)」定位成，旗下自我防禦網路的集中式監視與自動化平台，並且透過設備採購進行其大部分的 Cisco MARS 銷售。

圖 1：Magic Quadrant 安全資訊與事件管理

除了這些接受評估的 21 家供應商外，還有一些其他公司也提供' SIEM 功能，只是他們不符合我們的入選條件。不過，這些供應商有時會與此 Magic Quadrant 當中的 SIEM 供應商相互競爭。

Splunk 提供事件收集、記錄管理與搜尋技術，以便客戶有時要調查安全事件、取得部分 SIEM 技術所提供的功能，或補充他們的 SIEM 投資。Splunk 已針對資訊安全與法規遵循使用案例，發佈預先定義的報告。在 2009 年 4 月，Splunk 發表 Splunk Enterprise Security Suite - 由支持資訊安全使用案例之套裝搜尋、相關性分析、報告、儀表板、虛擬化與分析功能所構成的一組資訊安全應用程式，其中包括法規遵循報告、事件監視、事件回應、記錄管理、使用者與系統存取報告以及鑑識。Splunk 並未入選此次評估，因爲 Enterprise Security Suite 是在我們進行評估之後發表的，而且 Splunk 並非提供即時監視。

另外四家供應商未能入選 Magic Quadrant，是因爲他們的地理區或垂直市場焦點及/或 SIEM 營收規模 ：

- S21sec 在西班牙與拉丁美洲提供 SIEM 解決方案、端點保護技術與資訊安全代管服務，而且計劃朝其他地理區拓展業務。
- Tango/04 提供 SIEM、作業監視與商業程序監視解決方案，其客戶集中在歐洲與拉丁美洲。
- Tier-3 是一家總部設在澳大利亞的公司，他們在亞太地區提供 SIEM 技術，在歐洲的知名度也蒸蒸日上。
- FairWarning 專門爲醫療保健這個垂直市場，提供應用程式層次的使用者活動與資源存取監視。

有少數幾家供應商銷售以授權使用 SIEM 技術爲基礎的解決方案 。Q1 Labs 針對在本身設備上實作 Q1 Labs 技術的供應商，授權他們使用 SIEM 技術，然後整合該技術與自家的管理基礎架構 。Enterasys Security Information and Event Manager appliance（也稱爲 Dragon Security Command Console）從 2005 年就開始使用 Q1 Labs 技術，他們提供與 Enterasys Network Access Control 以及 NetSight Automated Security Manager for Distributed Intrusion Prevention 之間的工作流程整合。Juniper Networks Security Threat Response Manager 是發表於 2008 年的設備解決方案，該方案採用 QRadar 技術，並與 Juniper' 的原則管理子系統整合。Nortel 已停止供應 QRadar for Nortel 設備。

HP 提供設備型產品，其中採用 SenSage 的授權技術，現在正在累積初次安裝客戶數目。雖然 HP Compliance Log Warehouse (CLW) 解決方案是以廣泛的法規遵循與 SEM 市場爲目標，但 HP 也在其整個產品組合中，運用該技術來啓用 SEM 功能。HP 讓 CLW 成爲其 Secure Advantage 方案的核心元素，並且完成該元素與其 ProCurve 網路與安全裝置產品線以及軟體配置管理技術的整合。在 2009 年 4 月，HP 發表其中採用 SenSage v.4 的最新版 CLW 產品，該產品提供主要使用者介面與 SEM 加強功能。

客戶需求 - 法規遵循、記錄管理、資訊安全與詐騙偵測

雖然是因爲法規遵循而投資 SIEM 專案，但大部分的組織也想要增強外部與內部威脅監視功能。因此，監視主機系統的使用者活動與資源存取，以及即時的網路安全事件管理等需求是存在的。廣大的企業採用 SIEM 技術，這種情況促進了下列產品需求：可提供預先定義法規遵循報告與資訊安全監視功能，以及容易部署及支援的產品。北美洲 SIEM 市場的主要驅動因素一直都是法規遵循需求，80% 以上的 SIEM 部署專案投資，目的都是彌補法規遵循方面的落差。在歐洲與亞太地區，部署 SIEM 的主要目的是監視外部威脅，不過在這些地區，法規遵循需求也日趨強勁。

記錄管理功能之所以變成日益重要的客戶需求，都是源於下列因素：

- 美國支付卡行業資料安全標準 (PCI DSS) 要求執行記錄管理
- 詳細的歷程記錄資料分析對侵害調查與一般鑑識來說很有用
- 能夠在以 SEM 爲主的部署前方實施記錄管理，這樣可以提高事件轉遞相關性分析引擎的選擇彈性（從而降低事件管理程式的負載並增強其可調整性）

應用程式層次的詐騙偵測監視或內部威脅管理一直是 SIEM 技術的使用案例。SIEM 技術會伴隨詐騙偵測與應用程式監視點解決方案進行部署，以擴大這些解決方案的觸角。行業垂直市場（例如金融服務與電信業）中的大型企業皆已實施這類專案，以此作爲內部合理的資訊安全措施。有一些 SIEM 供應商開始將他們的技術定位成，可提供資訊安全、作業與應用程式分析的「平台」。

最佳的 SIEM 解決方案能夠：

- 支援即時收集及分析主機系統、安全裝置與網路裝置的記錄資料
- 支援長期儲存與產生報告
- 不需要延伸自訂作業
- 容易部署及維護

容易部署與容易支援的功能，以及記錄管理功能，這些功能的重要性遠高於進階事件管理功能，或可大量自訂 SIEM 部署的能力。

SIM 即服務

大部分的資訊安全代管服務提供者，在長青的 SEM 服務之外，也提供 SIM 服務。這些新服務包含收集、分析、報告及儲存伺服器、使用者目錄、應用程式與資料庫的記錄資料。SIM 服務通常會揚棄即時監視與警示，轉而專注於法規遵循導向的例外、複查與記錄報告，還有儲存及保存記錄以因應後續調查與資料保留的能力。這些產品與服務的催生者是，需要符合法規遵循要求，且正在尋找購買及實作 SIEM 產品之替代方案的客戶。在此 Magic Quadrant 中，我們並未評估資訊安全代管服務提供者 (MSSP) 的服務遞送功能。

市場定義/說明

SIEM 市場的定義者是，需要即時分析安全事件資料以進行內部與外部威脅管理’，以及收集、儲存、分析及報告記錄資料，以因應法規遵循與鑑識的客戶。SIEM 產品提供 SIM 與 SEM：

- SIM 提供記錄管理 – 收集、報告及分析記錄資料（主要來自主機系統與應用程式，其次來自網路與安全裝置），以支援法規遵循報告、內部威脅管理與資源存取監視。SIM 支援 IT 部門的特許使用者與資源存取監視活動，以及內部審核與法規遵循部門的報告需要。

- SEM 會即時處理來自安全裝置、網路裝置、系統與應用程式的記錄與事件資料，以提供資訊安全監視、事件相關性分析與事件回應。SEM 可支援 IT 安全部門的外部與內部威脅監視活動，並增強事件管理功能。

入選與排除條件

供應商必須符合下列條件才能入選 SIEM Magic Quadrant：

- 產品必須提供 SIM 與 SEM 功能。

- 產品必須支援從異質資料來源擷取資料。

- 供應商必須出現在一般使用者組織的 SIEM 產品評估清單。

- 供應商必須提供 SIEM 部署的正式作業參考客戶。

- 解決方案必須以產品形式遞送至客戶環境。

供應商若有以下情形就會遭到排除：

- 供應商提供的 SIEM 功能只能處理來自本身產品的資料。

- 供應商將本身產品定位成 SIEM 產品，但該產品並未出現在一般使用者組織的產品入圍名單。

- 供應商的 SIEM 產品營收小於 400 萬美元。

- 解決方案僅以代管服務的形式遞送。

新增廠商

此次 的 SIEM Magic Quadrant 更新未新增任何供應商。

撤銷廠商

High Tower 在 2008 年停止營運，因此從此次的 SIEM Magic Quadrant 更新撤銷。

Exaprotect 已在 2009 年 5 月被 LogLogic 購併，因此從此次的 SIEM Magic Quadrant 更新撤銷。

評估準則

執行能力

- **產品/服務**準則評估像是 SIM、SEM、記錄管理、事件管理、工作流程與補救支援，以及報告功能等領域的產品功能運作。

- **可靠性**準則包含評量組織的的財務健全性、整體公司的財務與實際成功，以及事業單位繼續投資該產品的可能性。

- **銷售執行/計價**準則評估技術提供者’在 SIEM 市場的成功，以及他們在售前活動方面的能力。這包含 SIEM 營收與安裝客戶數目、計價、售前支援，以及銷售通路的整體效益。Gartner 客戶感興趣的程度也會納入考量。

- **市場回應性與追蹤記錄**準則評估 SIEM 產品是否符合購買者在購買時所陳述的功能要求，以及供應商在市場有需要時提供新功能’的追蹤記錄。另外也會考量，供應商如何區隔本身的產品，以便與主要競爭者有所不同。

- **客戶體驗**準則評估正式作業環境中的產品功能運作或服務。此評估包括容易部署、操作、管理、穩定性、可調整性與供應商支援功能。評量這項準則時，會向供應商提供的參考客戶進行質化訪問調查。此評估採用 Gartner 客戶的回饋，這些客戶正在進行或已完成 SIEM 產品的競爭評估。

- **營運**準則評估組織的服務、支援與銷售能力。

表 1. 執行能力評估準則

評估準則	加權
產品/服務	最高
整體可靠性（事業單位、財務、策略、組織）	最高
銷售執行/計價	最高
市場回應性與追蹤記錄	最高
行銷執行	無評等
客戶體驗	最高
營運	最高
資料來源：Gartner（2009 年 5 月）	

表 2. 願景完整度評估準則

評估準則	加權
市場瞭解	最高
行銷策略	標準
銷售策略	標準
產品策略	最高
業務營運模式	無評等
垂直市場/行業策略	無評等
創新	最高
地理區策略	無評等
資料來源：Gartner（2009 年 5 月）	

願景完整度

- **市場理解**評估技術提供者瞭解購買者需求’ ，以及將這些需要轉換成產品的能力。市場瞭解程度最高的 SIEM 供應商，他們可以適應像記錄管理、簡易實作與支援，以及法規遵循報告等方面的客戶需求，同時符合 SEM 需求。

- **銷售策略**準則評估供應商如何運用直接與間接銷售、行銷、服務與營銷聯盟，以延伸市場觸角的範圍與深度。

- **產品策略**準則評估供應商的產品開發與遞送方法，其中強調他們針對目前 SIM 與 SEM 需求所提供的功能運作與功能組合。’另外，也會評估供應商接下來 12 到 18 個月內的開發計劃。

- **創新**準則評估供應商的’ SIEM 技術開發與遞送，供應商要以獨特方式解決重要的客戶需求，以便與競爭者有所區隔，我們會評估像應用程式層監視、詐騙偵測與身分導向監視等領域的產品功能與客戶使用，另外也會評估產品專有以及客戶有需要且已部署的其他功能。

領導廠商

SIEM 領導廠商象限是由符合以下條件的供應商所構成，供應商必須是 SIEM 市場中，在建立安裝客戶群與營收來源方面最爲成功的廠商，此外，還要獲得相對比較高的可靠性評等（依據 SIEM 營收或 SIEM 營收以及其他來源營收），並且提供功能運作符合一般市場需求的產品。

挑戰廠商

挑戰廠商象限是由符合以下條件的供應商所構成，供應商必須擁有龐大營收來源（通常因爲供應商擁有多種產品和/或服務線），擁有中等以上的 SIEM 客戶群，還有產品符合部分的一般市場需求。在挑戰廠商象限中，許多大型供應商都將他們的的 SIEM 解決方案定位成，資訊安全與作業技術的相關延伸。

願景廠商

願景廠商象限主要是由小型供應商所構成，他們提供符合一般市場需求的 SIEM 技術。

利基廠商

利基廠商象限主要是由小型供應商所構成，他們提供符合特定 SIEM 使用案例或部分的 SIEM 市場需求的 SIEM 技術。

供應商的優點與告誡

ArcSight

ArcSight 是最成功且知名度最高的 SIEM 點解決方案供應商，其解決方案提供廣泛的功能。ArcSight 的安裝客戶數目高於其他的點解決方案競爭者。此供應商所提供的「企業安全管理程式 (ESM)」軟體，旨在提供以 SEM 爲主的大型部署，以及一系列可獨立實作或伴隨 SEM 實作的記錄管理與收集器設備。在 2009 年 4 月，ArcSight 發表通用版 ArcSight Express，這是一種設備型 ESM 產品，適用於擁有預先配置監視與報告功能，以及簡易資料管理的中階市場。第三版 ArcSight Logger 設備系列（發表於 2008 年 11 月）特別增強報告與收集功能的效能。

優點

- ArcSight 提供廣泛的 SIEM 功能組合。
- 此供應商最近推出一種設備，其中提供比較簡化的 SEM 部署選擇。
- 在競爭評估中，ArcSight 依然是知名度最高的 SIEM 點解決方案。

告誡

- ArcSight 的 ESM 軟體適用於需要可支援安全作業中心之功能的環境，不過在某些領域，例如資料庫調整方面，需要一般使用者擁有實質專業知識。

CA

在銷售安全資訊管理 (SIM) 解決方案方面，若是以增強型審核功能銷售給本身的身分與存取管理 (IAM) 客戶，CA 的銷售算是成功的，但在需要 SEM 的使用案例中，CA 則完全不具競爭力。在 2008 年，CA 銷售兩種 SIEM 產品：CA Audit（CA 過去成功銷售給其 IAM 客戶）提供基本的主機系統記錄資料收集與分析；Security Command Center (SCC) 提供 SEM 功能。在 2009 年 4 月 20 日，CA 發表通用版 CA Enterprise Log Manager，這種軟體設備可提供記錄管理、法規遵循報告，以及應用程式 、主機、網路裝置與安全裝置分析。此產品旨在整合 CA' 的 IAM 產品組合，並且取代 CA Audit。SCC 部署並不普遍，而且需要大量自訂作業。

優點

- CA 的 SIM 解決方案緊密整合 CA 的 IAM 技術，且最常見的部署原因是監視主機系統上的使用者活動。
- CA 的 SIM 解決方案尤其適合已實作其他 CA IAM 或系統管理產品的組織。
- Enterprise Log Manager 針對需要法規遵循報告與一般記錄管理功能組合的使用案例，提供簡化的部署選擇。

告誡

- 需要 SEM 功能的組織應該也要評估其他供應商的 SEM 替代方案。

Cisco

Cisco 銷售多種以網路安全爲主的解決方案。Cisco 已爲其 Cisco Security Monitoring, Analysis, and Response System (MARS) 設備建立龐大的 SIEM 客戶群，因爲他們將此設備定位成自我防禦網路策略，並且向其以網路爲主的購買者進行銷售。此技術提供 SEM 、SIM 與網路行爲分析 (NBA) 功能組合，並且針對其所支援的平台，提供有效的現成網路安全監視與主機活動監視。除了本身的裝置外，Cisco 在擴大支援網路裝置來源方面沒有做太多努力，而且 MARS 僅限用於主機平台、安全 裝置與應用程式支援。Cisco 對於其他的 SIEM 供應商一直有很大的影響，因爲有廣大的客戶站台部署其 SIEM 技術。

優點

- MARS SIEM 設備提供「現成」的網路 SEM 功能，並且整合 Cisco Security Manager。
- 對於希望在其 SIEM 部署上增益 NBA 功能的組織來說，也應考慮採用 MARS。

告誡

- 雖然 MARS 支援基本的伺服器法規遵循監視，但對於需要高度自訂審核/報告功能的 SIM 部署而言，這並非最理想的選擇。
- 擁有異質網路裝置資料來源需求以及需要跨多重設備整合相關性分析或報告功能的的大型企業，他們會發現 MARS 對於他們的特定需要而言是不夠用的。

elQnetworks

elQnetworks 正在企業 SIEM 市場中，透過其 SecureVue 軟體與設備建立安裝客戶群。此公司將 SEM 技術授權給 MSSP，以及利用此技術爲自家產品組合建立 SEM 功能的網路安全供應商。的大型企業的 SecureVue 產品其特點是，它透過單一產品提供廣泛的功能，包括 SEM、SIM、安全配置原則法規遵循、作業效能功能，以及某些 NBA 功能。在競爭評估中，elQ 已可贏過其他的 SIEM 供應商，特別是當客戶需要這些鄰近領域功能時。

優點

- SecureVue 產品提供網路 SEM，以及容易部署的法規遵循導向 SIM 功能。
- SecureVue 提供廣泛的功能組合，包括 SIEM 、效能 、安全資產，以及配置原則法規遵循功能。

告誡

- elQnetworks 正在建立企業 SIEM 市場佔有率，不過他們需要發展更廣泛的銷售能力。
- SecureVue 的功能多半不是用於解決一般的 SIEM 問題，而且 elQnetworks 需要繼續找尋在競爭評估中看重擴充功能的潛在客戶。
- 除了作用中目錄與一般輕量型目錄存取通訊協定 (LDAP) 支援外，SecureVue 尚未整合 IAM。

IBM

IBM' 的整體 SIEM 策略就是，進一步整合其 IAM、安全與服務管理技術；利用 ISS 代管服務；以及開發設備型產品。IBM 提供三種 SIEM 產品。IBM Tivoli Compliance Insight Manager (TCIM) 著重 SIM，且主要提供使用者活動監視與法規遵循報告。Tivoli Security Operations Manager (TSOM) 著重 SEM，主要提供外部威脅管理 。Tivoli Security Information and Event Manager (TSIEM) 是寬鬆整合的 TSOM 與 TCIM 組合，其中可啓用 TCIM 的特定事件共用與一般報告功能。該公司計劃進行進一步的整合。

優點

- TSIEM 整合廣泛的 IBM 與第三方 IAM 技術及應用程式組合。
- TSIEM 提供強大的法規遵循報告功能與使用者活動監視。
- IBM 正在擴大整合其 SIEM 產品，以及其作業管理技術。

告誡

- 雖然 TSIEM 提供 TSOM 與 TCIM 之間的基本整合，但需要即時監視主機記錄事件的組織，還是需要同時部署這兩種技術。
- 雖然 TSIEM 可透過軟體實作記錄管理層，但 IBM 尚未提供記錄管理設備。

Intellitactics

Intellitactics 已重新設計其 SIEM 產品，因此在安全事件管理法規遵循與記錄管理方面，現在可提供軟體型與設備型解決方案 。Intellitactics Security Manager (ISM) 是可大幅度自訂的軟體產品，很適合用於以 SEM 爲主的大規模部署。SAFE 設備系列提供資料收集、記錄管理與基本的 SEM 。新型設備可因應目前市場上的簡易快速部署需求。

優點

- Intellitactics 目前的 SIEM 產品線提供使用者介面增強，以及擴充功能與預先定義功能，相較於先前的版本，這些新版本可減少部署與支援人力。
- Intellitactics 可爲需要自訂作業的大型部署，以及需要預先定義能與簡易部署的中型企業，提供解決方案。

告誡

- Intellitactics 必須繼續努力開發銷售通路，才能有效接觸大量的中型企業。

LogLogic

LogLogic 以前的定位是主要的記錄管理提供者，但他們現在已擴大版圖，直接挑戰更廣泛的 SIEM 提供者。LogLogic 已擴充產品功能，以包含 SEM、資料庫活動監視，以及網路安全配置管理。在 2009 年 5 月，LogLogic 完成購併 Exaprotect，後者提供 SEM 與網路安全配置管理技術。在購併行動之前，LogLogic 已發表其 Security Event Manager 設備，其中使用 Exaprotect 的授權技術。此外，LogLogic 還發表 Database Security Manager，此產品提供資料庫活動監視與安全管理。此解決方案運用代理程式技術，搭配組合特殊化設備。另外，LogLogic 也已發表 Compliance Manager 設備，此產品提供設備儀表板與工作流程。

優點

- LogLogic 購併 Exaprotect 後，已擴增其記錄管理功能，其中包含分類架構型事件相關性分析與管理。
- LogLogic 透過特殊化的代理程式技術，監視及防護 Oracle 、SQL Server 與 Sybase DBMS。

告誡

- LogLogic 需要繼續努力擴充其銷售團隊的 SEM 知識、銷售通路與售前支援。

LogRhythm

LogRhythm 的 SIEM 技術提供 SEM 與記錄管理功能，以及法規遵循與安全作業報告。在過去 18 個月中，此公司已在其主要安裝客戶群中型組織之外，擴大包含大型企業。他們的技術可以透過數種形式遞送：儀表板、事件管理程式與記錄管理程式可透過軟體映像檔、全功能設備，或多種單一功能設備等形式遞送。LogRhythm 支援代理程式型與無代理程式收集，可收集許多的主機、網路與應用程式來源，而且代理程式還提供基本的檔案完整性監視。

優點

- LogRhythm 的設備提供記錄管理與 SEM 功能組合，最適合用於需要這些功能但支援能力有限的中型組織。

告誡

- 雖然 LogRhythm 正在快速成長，但該公司在市場上仍屬於小型供應商，需要繼續開發銷售通路以維持成長。

netForensics

netForensics 是 SIEM 點解決方案供應商，擁有混合一般使用者與 MSSP 客戶的客戶群。其 SIEM 解決方案由以下三種元件組成：(1) nFX SIM One 軟體提供全功能 SEM ，一直以來都可以與像 ArcSight、Intellitactics 及 Novell 等供應商的點解決方案匹敵。(2) nFX Log One 提供記錄管理。(3) nFX Data One 提供網路型與代理程式型資料庫活動監視。nFX Log One 與 nFX Data One 可作爲軟體或設備提供，也可以獨立部署或寬鬆聯結其他的 nFX 元件。在 2009 年 1 月，netForensics 購併 High Tower 的資產，之後將 Cinxi 設備定位在中階市場的記錄管理與事件管理整合解決方案。

優點

- netForensics nFX SIM One 軟體最適合用於需要即時監視與彈性報告，但現有資源不足以應付自訂作業與支援的部署。
- nFX Log One 與 nFX Data One 設備元件擴大支援範圍，現在可支援這些需要基本記錄管理以及資料庫活動監視功能的使用案例。

告誡

- netForensics 需要在競爭評估中擴大其市場佔有率。

NetIQ

NetIQ 是 Attachmate 的事業單位。此事業單位擁有安全與作業技術組合，以及規模中等的 SIEM 客戶群。NetIQ 提供作業與安全管理軟體產品，這些產品雖然整合在一在，但通常會隨著時間變化而分別部署。NetIQ 除了向其作業管理產品安裝客戶群，也向新客戶銷售安全管理產品。NetIQ Security Manager SIEM 擁有龐大的安裝客戶群，其中主要安裝 SIM、使用者活動監視與法規遵循報告功能。此技術可以用於網路與安全 裝置來源，但實際上卻很少部署於這類使用案例，因爲 NetIQ 一般不會向網路安全購買中心進行銷售。此核心產品旨在處理經過過濾的記錄資料，不過整合記錄資料收集與保存功能，可用來收集及分析所有來源的各種記錄資料。

優點

- NetIQ Security Manager 最適合用於以分析主機上使用者與資源存取監視記錄，以及處理法規遵循報告爲主的部署。
- Security Manager 緊密整合 Change Guardian 產品線，後者提供作用中目錄的監視與變更偵測，以及主機系統的檔案完整性監視。

告誡

- NetIQ 尚未針對以網路與安全裝置事件管理爲主的部署進行最佳化。

NitroSecurity

NitroSecurity 正在從其核心的侵入偵測系統 (IDS)/侵入預防系統 (IPS) 業務逐步拓展至 SIEM 市場。此供應商將 SIEM 技術銷售給他們的 IDS/IPS 安裝客戶群，同時也向新客戶銷售上述兩種解決方案。

NitroView 的 SIEM 設備系列，採用其 IDS/IPS 產品的高速事件儲存與查詢技術。NitroView Receiver 提供記錄收集與事件相關性分析 NitroView ESM 提供跨來源相關性分析與整合備援儲存庫，以支援高速搜尋與報告。

在 2008 年，NitroSecurity 購併 Rippletech，並在其本身的 NitroView 產品中，整合後者的資料庫活動監視技術。在 2009 年初，NitroSecurity 還購併 Chronicle，並致力於在其即時監視產品中，啓用後者的網路資料分析功能。

優點

- NitroView 混合提供 SIM 與 SEM，其儲存庫可維持高度即時的事件插入率，同時還支援高效能報告產生與分析。
- 此外，還透過整合選項，提供資料庫活動監視（網路監視器與代理程式型）。

告誡

- NitroView 提供有限的內嵌式事件管理支援。

Novell

Novell 的 Sentinel 軟體產品已與 Novell 的 IAM 解決方案整合，而且 Novell 也積極銷售 Sentinel，以補足其 IAM 客戶的監視與自動化補救技術。’’ Novell 的 Compliance Management Platform 是一種整合的 IAM 與 SIEM 技術組合。’ Sentinel 的目標對象是需要廣泛且彈性之 SEM 功能的大規模部署，但是本產品不容易部署，因此不太能夠配合 Novell 向其 IAM 客戶銷售 SIEM 的策略。’ 在 2008 年底，Novell 發表 Novell Identity Audit 套件，本套件針對 Novell 的 IAM 產品提供基本的記錄管理與報告功能。’ 在本評估進行期間，Novell 正計劃發表兩項加強功能：(1) Sentinel 6.1 Rapid Deployment 選擇 - 旨在提供簡易部署與支援（2009 年第二季發表）；與 (2) Sentinel Log Manager - 作爲 Sentinel 的記錄管理層（計劃在 2009 年底發表）。

優點

- Sentinel 最適合用於以 SEM 爲主的大規模部署，其中可接受多種事件資料收集與分析。
- Sentinel 是以訊息匯流排架構作爲基礎，該架構可爲大型部署提供彈性與調整性。
- Identity Audit solution 很適合採用 Novell IAM 產品，並且需要擴充審核功能的組織。

告誡

- 需要記錄管理功能的組織必須等待 Novell 發表 Sentinel Log Manager，不然就需要採用第三方的記錄管理技術來增益其 SEM 部署。
- 發表 Sentinel 6.1 Rapid Deployment 是爲了提供簡化的部署與支援，不過在我們執行此評估時，該產品尚未發行，我們也沒有機會訪問正式作業參考客戶。

OpenService

OpenService 提供事件管理軟體，其中涵蓋系統管理與安全管理使用案例。此技術具有可調整性，容易部署，且其相關性分析方法具有區隔性。儘管技術具有區隔性，甚至擁有某些赫赫有名的大客戶，但 OpenService 在適應法規遵循需求變遷方面卻很緩慢，而且在銷售與行銷方面也效果不彰。在 2008 年，該公司獲得資金浥注，同時也有新的管理團隊進駐。OpenService 的 InfoCenter 是由 InfoCenter 主控台、ThreatCenter（風險型相關性/分析）、LogCenter（記錄儲存庫）、NerveCenter（可用性與效能監視），以及 Event Collectors 所組成。

優點

- 對於正在找尋現成 SEM 解決方案，而且其伺服器端資源需求不大的組織來說，OpenService 是很好的選擇。
- OpenService 已增強 InfoCenter 的報告與使用者介面功能。
- 風險型相關性分析會評估威脅、漏洞與資產屬性等方面的事件，它可以替代規則型方法。

告誡

- 從競爭評估得知，Open Service 在 Gartner 客戶當中的知名度仍然不高，他們必須拓展更廣泛的銷售通路合作關係。
- OpenService 需要加強其直接銷售與行銷方面的能力。

Prism Microsystems

- Prism Microsystems EventTracker 軟體的主要目標對象是，需要安全與作業管理以及法規遵循報告的中型商務企業及政府機關。Prism 一直在增強 EventTracker 的事件管理與法規遵循報告功能，而此軟體現在透過階層式或多站台部署支援可調整性。EventTracker 包含虛擬環境適用的特定監視支援。EventTracker 代理程式也提供檔案完整性監視支援。

優點

- EventTracker 軟體很適合需要一種產品就能提供記錄管理 、SEM、法規遵循報告與作法監視的中型企業。
- Prism 的 EventTracker 很容易部署及維護，特別是在 Windows 環境中，EventTracker 可支援集中式代理程式部署與管理。
- Knowledge Packs 提供 EventTracker 預先建置的相關性分析、警示與報告功能，以因應特定的法規遵循體制或作業需求。

告誡

- EventTracker 不太適合需要安全作業中心功能的實作，或其中整合配置/資產管理資料庫的實作。
- 在 EventTracker 中提供部分 Windows 漏洞評量功能，但此產品並未整合來自其他漏洞評量產品的漏洞評量資料。
- EventTracker 無法與 IAM 產品整合。

Q1 Labs

Q1 Labs' QRadar 設備系列提供 SIEM、記錄管理與 NBA 功能整合。此公司向大型客戶直接銷售、運用通路夥伴，以及將技術授權給網路與安全供應商，藉由這些方法創造快速成長。雖然 Q1 Labs 在整個 SIEM 市場中參與競爭，但他們特別將 QRadar 定位成 Cisco MARS 的競爭替代方案，並且將該技術授權給 某些 Cisco 競爭者（例如 Juniper Networks 與 Enterasys）。QRadar 技術運用 NetFlow 與直接網路流量監視，同時結合主機活動監視與記錄資料報告，藉此提供威脅環境整合檢視。QRadar Simple Log and Information Management (SLIM) 是一種記錄管理設備，可升級爲 SIEM 全功能。此供應商積極尋求需要使用者導向監視的部署，以及以法規遵循爲主的部署。

優點

- Q1 Labs 的 QRadar 提供 SEM、SIM 與 NBA 功能組合，可供 IT 安全與網路作業使用。
- NBA 功能可以應用在主機侵害探索。
- 收集層可以用來提供記錄管理功能，而記錄資料可以索引化，並且供報告功能存取。

告誡

- 正在評估是否要在以身分審核爲主之部署中採用 QRadar 的組織，也應該評估現有 IAM 供應商的 SIEM 產品。

Quest Software

Quest Software 提供 SIEM 產品，以此補足其 Active Directory 與 Windows Server 管理產品線，而且一般是已部署這些產品的客戶才會實作他們的 SIEM 產品。InTrust 的 SIEM 軟體解決方案包括資料分析、報告與記錄收集。此 SIEM 產品偏好 Microsoft 環境。部署外掛程式與其他的 Quest Software 產品，多半是爲了擴充專門供 Microsoft 平台（包括 Active Directory、Exchange 與檔案伺服器）使用的監視功能。InTrust 旨在處理主機記錄資料，但是也提供某些網路裝置與網路型安全技術支援。Quest Software 擁有龐大的 InTrust 安裝客戶群，但因爲原始檔支援狹隘，限制了部分 SIEM 技術購買者的適用性。

優點

- IT 環境中以 Microsoft 產品佔絕大多數的組織，可以在 InTrust 與相關的外掛程式中，延伸此 Microsoft 產品的原生審核功能。
- Quest Software 針對 Microsoft Active Directory、Exchange 與檔案伺服器提供大量的監視功能，這些功能可以應用在使用者活動報告。

告誡

- 需要爲安全作業中心啓用全功能安全主控台的組織，應考慮使用可在此領域中提供更多功能或靈活彈性的解決方案。
- InTrust 不太適合用於監視需求包含非 Windows 作業系統與主要 Unix 發佈版本的部署，也不太適合監視防火牆、IDS/IPS 或廣泛網路裝置爲其主要考量的部署。

RSA (EMC)

RSA（EMC 的安全部門）銷售 enVision 設備，該設備提供 SEM、SIM 與記錄管理等功能組合。enVision 擁有最龐大的安裝客戶群之一，而且 RSA 動用其直接銷售團隊與通路合作夥伴來銷售 enVision。雖然 enVision 的 SEM 能力並非最佳的點解決方案（比較複雜），但對於一般的使用案例來說已經「很好用」，而且其設備尺寸很容易部署。在 2009 年 3 月，RSA 發表 enVision v.4，其中針對外部威脅管理、特許使用者監視與系統監視，增強相關性分析功能。新的相關性分析規則充分運用 enVision 分類架構（相對於原始層次事件）。

優點

- 當需要收集所有資料並提供分析使用，以及需要單一設備能夠同時提供 SEM 和 SIM 功能時，應考慮使用 RSA enVision。
- 由於此設備很容易部署，當客戶只能動用有限的人力資源來管理 SIEM 實作當中的伺服器與資料庫時，也應考慮使用此設備。

告誡

- 與此領域的最佳解決方案相較，此設備只能提供有限的應用程式層監視。

SenSage

SenSage 解決方案經過最佳化，可針對大型記錄事件資料儲存庫進行分析及提供法規遵循報告，且該公司已成功爭取需要此能力的大型部署。另外，該公司也已成功爭取需要應用程式層和/或使用者導向監視的使用案例。在 2008 年發表的 SenSage v.4 讓該公司得以在 SIEM 市場中擴大競爭力，因爲此版本的產品解決了即時收集與事件管理功能方面的限制。此外，第 4 版產品還增強使用者介面以簡化部署與管理作業，同時也提高產生報告功能的好用程度 。SenSage 還與 Cerner（醫療設備）及 HP（HP CLW 設備）進行 OEM 合作。

優點

- SenSage 針對有以下需要的組織進行最佳化：需要進行大量事件收集、監視與分析，並且就長期收集的大量記錄資料產生報告，以供審核、法規遵循與內部調查之用。
- SenSage 保證支援 SAP、Oracle（PeopleSoft 和 Siebel）、Lawson、Cerner 與其他套裝應用程式提供者，而且其技術可支援需要精準分析的使用案例，例如詐騙偵測。

告誡

- 只需要基本記錄管理功能的組織，應考慮使用以收集與基本報告爲主的產品，這類產品比較簡易與便宜。

Symantec

Symantec Security Information Manager (SSIM) 以軟體設備的形式供應，此設備提供 SIM、SEM 與記錄管理功能。SSIM 會從 Symantec 的 DeepSight 安全研究與代管安全領域，動態更新威脅與漏洞內容。Symantec 也提供代管服務，其中運用此軟體設備來執行站上資料收集與分析。Symantec 已整合其 SIEM 與 Security Endpoint Protection (SEP) 技術，且專注於向其 SEP 客戶群銷售 SIEM 產品。

優點

- SSIM 設備提供 SIM、SEM 與記錄管理功能，這些功能不但可以調整，還很容易部署。
- 動態的 DeepSight 內容可即時識別作用中的外部威脅，以及已知的惡意來源。

告誡

- Symantec 需要增強預先定義的報告與分析功能，以兼顧 IT 安全技術領域以外的相關人士需要。

Tenable Network Security

Tenable Network Security 的 SEM 解決方案緊密整合該公司的主動式與被動式漏洞掃描程式產品，且他們的 SIEM 客戶也傾向使用漏洞掃描與配置評量技術。’’ Tenable 的 SIEM 軟體解決方案包含 Security Center 主控台環境，以及 Log Correlation Engine (LCE)。’ LCE 可以在網路上散佈以收集主機與網路裝置的記錄，而且還可以爲事件以及來自 Tenable 漏洞掃描與安全配置評量產品的資料建立相關性。 Security Center 整合 Tenable 的 Log Correlation Engine 與漏洞掃描產品，以提供統一的資產探索、漏洞偵測、事件管理記錄收集與報告。

優點

- 對於正在尋求利用單一使用者介面，同時因應掃描與記錄收集以及報告需求的購買者來說，Tenable 的 Nessus Vulnerability Scanner 與 Passive Vulnerability Scanner 產品整合是一大優點。
- Security Center 的基本 NetFlow 收集與異常偵測可用於主機侵害探索。
- 擁有充分技術專業的使用者，可以選擇運用 Scripting 功能來自訂作業。

告誡

- 對於著重主機身分與存取活動相關法規遵循報告需求的部署來說，其他的 SIEM 解決方案會更適合。
- Tenable 需要繼續努拓展其銷售能力。

TriGeo

TriGeo 針對需要現成外部威脅監視與法規遵循報告功能的中型組織，設計了設備型 SIEM 解決方案。除了用於資訊與事件管理的 Security Information Manager 之外，TriGeo 還提供用於記錄收集與網路事件收集的分散式設備，以及用於搜尋/報告的設備，其中包含來自 Splunk 的內嵌技術。

優點

- TriGeo 的設備型方法提供容易部署的 SIEM，其中包含大量預先定義的相關性分析與法規遵循報告範本。
- 用於記錄收集 網路裝置警示收集 搜尋與報告的附加設備，可讓客戶漸進地新增功能。

告誡

- 大規模的資料收集與聚集工作，或者其中包含大量自訂作業以及整合其他 IT 管理技術的部署需求，比較適合使用其他的 SIEM 解決方案。
- TriGeo 以中小企業市場爲目標，在大型競爭者開始進軍這塊區隔市場的情況下，他們必須開發更多的銷售通路以維持成長。

新增或撤銷的供應商

隨著市場的改變，我們複查並調整 Magic Quadrants 與 MarketScope 的的入選條件 。因爲會進行調整的關係，Magic Quadrant 或 MarketScope 的供應商組合可能隨時會變更。供應商若在某一年出現但下一年卻沒有出現於 Magic Quadrant 或 MarketScope，這不表示我們對該供應商的看法改變了。這可能只是反應伴隨市場變化而來的評估準則變更，或者供應商的焦點改變了。

評估準則定義

執行能力

產品/服務：供應商在所定義市場中競爭/提供的核心產品與服務。這包含現行產品/服務功能、品質、功能組合與技術，無論是原生提供或透過 OEM 安排/合作，如市場定義中所述，詳情請看次準則。

整體可靠性（事業單位、財務、策略、組織）可靠性準則包含評量整體組織的的財務健全性、事業單位的財務與實際成功，以及事業單位繼續投資該產品，並且在組織產品組合中提升該產品地位的可能性。

銷售執行/計價：供應商在所有售前活動與活動支援結構方面的能力。’ 這包含交易管理、計價與協商、售前支援，以及銷售通路的整體效益。

市場回應性與追蹤記錄：在商機形成、競爭者採取行動、客戶需要演變，以及市場動態變化時，回應、改變方向、保持彈性與達到競爭成功的能力。此準則也會考量供應商過去的回應狀況。

行銷執行：旨在傳播組織訊息，以影響市場、促銷品牌與企業、提高產品知名度，並且在購買者心目中建立正面的產品/品牌與組織形象之計劃方案，其明確性、品質、創意與功效。’ 若要推動這類「心靈佔有率」，可以靠宣傳、促銷、思潮領導、口耳相傳與銷售活動等方式同時並進。

客戶體驗：可讓客戶透過所評估產品獲致成功的關係、產品與服務/方案。具體而言，這包含客戶收到技術支援或客戶支援的方式。這也可以包含補充工具、客戶支援方案（與衍生的品質保證），提供使用者群組與服務水準協定。

營運：組織達成其目標與保證的能力。因素包含組織結構的品質，這包括技術、經驗、方案、系統，以及其他可讓組織以兼顧效益與效率之方式持續營運的工具。

願景完整度

市場瞭解：供應商瞭解購買者所想所要，以及將其轉換爲產品與服務的能力。這些供應商最能夠注意聽注意看，瞭解購買者所想所要，而且能夠透過新增願景來創造或增強這些能力。

行銷策略：在整個組織中一致傳播，並且透過網站、廣告、客戶方案與定位陳述向外傳播的一組明確與區隔的訊息。

銷售策略：運用適當的直接與間接銷售網路、行銷、服務與營銷聯盟來銷售產品的策略，上述管道可擴大市場觸角、技術、專業知識、技術、服務與客戶群的廣度與深度。

產品策略：供應商的產品開發與遞送方法，其中強調他們針對目前與未來需求所提供的區隔、功能運作、方法與功能組合。

業務營運模式：供應商的基礎業務定位其健全性與邏輯。

垂直市場/行業策略：供應商指揮資源、技術與產品，以因應個別市場區隔（包括垂直市場）特定需求的策略。

創新：透過直接、相關、補充與協同方式佈局資源、專業知識或資本，以達成投資、整合、防禦或主動出擊目的。

地理區策略：供應商指揮資源、技術與產品，以因應「母國」或發源地以外之地理區特定需求的策略，直接指揮或透過合作夥伴、通路與子公司指揮皆可，只要適用於該地理區與市場即可。