DATASHEET

SorbSecurity

基於人工智慧的行為分析

雲端安全解決方案合作夥伴

SORBSECURITY

Sorb 郵件安全云(SCES)

- 99.999% 服務可用性
- 99% 阻擋垃圾郵件
- 100% 已知病毒保護
- 100% 已知钓鱼保護
- 100% 文件負載 APT 保護

SCES 安全功能

- 動態分類和控制電子郵件
- 多層次威脅保護
- 靈活的策略和內容過濾器
- 詳細的報告
- 可擴展以支援甚至最大型的組織
- 郵件存檔

SCES 優勢

- 不僅可保護垃圾郵件和病毒，還能保護免受高阶攻擊，包括網路釣魚、惡意軟體和高階持續性威脅
- 減少管理負擔
- 快速方便的報告、搜尋和調查

保護組織免受所有電子郵件威脅

SorbSecurity Cloud 電子郵件安全「SCES」透過易於使用和易於部署的基於雲端的解決方案，幫助您保護和控制收發的電子郵件。憑藉 SCES，您可以保護您的員工、數據和品牌聲譽，免受現代威脅的影響，包括但不限於：

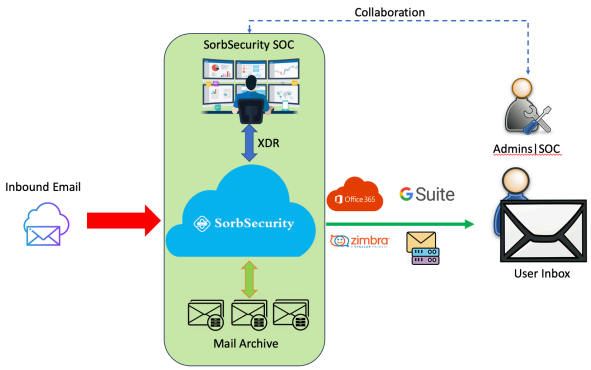
- 垃圾郵件
- 網路釣魚
- 惡意軟體
- 勒索軟體

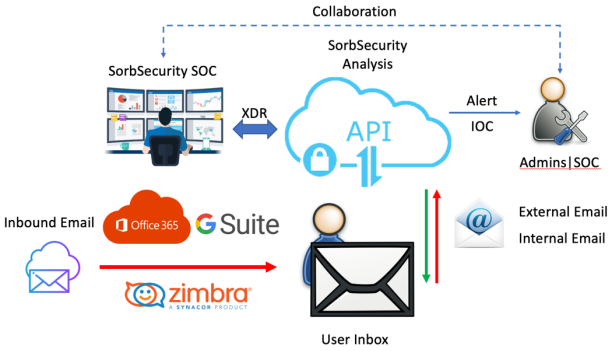
下一代電子郵件解決方案

SCES 可確保您的員工免受所有電子郵件威脅。我們靈活應對各種複雜環境，幫助我們的客戶和合作夥伴。我們支援雲端、混合、本地架構，搭配各種虛擬基礎架構（Azure、Google Cloud、VMWare、KVM 等）或物理設備。

威脅保護和預防

有效的威脅保護始於高效而精確的偵測。SCES 使用多層領先的動態行為驅動分析技術來偵測各種嚴峻的威脅，包括網路釣魚和惡意軟體。





電子郵件防火牆

阻斷式服務攻擊（DoS）防護

保護您的通訊基礎結構。使用 DDoS 郵件保護，您可以保護與同事、客戶、服務提供商和供應商之間的電子郵件交換。

SMTP 速率限制

消息節流是指對郵件伺服器可以處理的消息數量和連接數量設置的一組限制。這些限制包括消息處理速率、SMTP 連接速率和 SMTP 會話超時值。這些限制共同作用，以保護郵件伺服器免受接受和傳遞消息的壓倒性影響。

寄件者 IP 聲譽分析

我們的寄件者 IP 數據庫就像評估您的信用風險一樣，但是用於電子郵件：它測量您的電子郵件程序的健康狀況。

SMTP 交易檢查

一旦 SMTP 對話開始，您可以對遠程主機提供的命令和引數進行各種檢查。

寄件者驗證

您可以使用 SMTP 寄件者驗證來確保郵件的發件人是 SMTP 伺服器的合法使用者。

郵件路由

入站控制

為了防止不需要的郵件被接收，SCES 提供了一組控制項，讓您限制入站 SMTP 連接。入站連接控制可讓您指定 SCES 是否在 DNS 中檢查連接主機的名稱，或者如果是通過主機名或 IP 地址，則允許和拒絕連接的遠程主機。

目標控制和負載平衡

靈活的策略來控制郵件流量路由或重新路由到目標伺服器，平衡不同目標的流量。或者，甚至是密件抄送、更改收件人等。

出站來源和速率控制

出站速率控制用於防止受到垃圾郵件和大規模發送惡意軟件從受感染帳戶發出的影響。它有助於防止垃圾郵件發送者和黑客通過轉發大量郵件來破壞您的郵件伺服器。它還有助於保護我們的系統並保持我們的客戶安全。

內容安全

啟發式垃圾郵件檢測

啟發式檢測方法與簽名系統不同，它使用預測技術而非反應技術。預測性的特性是針對未知的垃圾郵件威脅和可疑電子郵件。它根據一組規則對每封電子郵件進行評分。如果一封電子郵件的得分超過指定的分數，則被識別為垃圾郵件。啟發式檢測方法有助於識別那些變化最頻繁的垃圾郵件，例如不合適或詐騙郵件。啟發式檢測方法還使您能夠阻止電子報的發送。

人工智能垃圾郵件規則

使用機器學習意味著從對垃圾郵件的模式識別轉變為自學習和優化系統。以下是人工智能工具檢測和過濾垃圾郵件的方式：

基於關鍵詞和內容的過濾：使用神經網絡、貝葉斯分類、k 最近鄰(kNN)等機器學習方法。在這裡，評估關鍵詞、短語及其分佈和頻率，制定規則以過濾垃圾郵件。
基於相似度的過濾：使用 kNN 將電子郵件分類為是否與存儲的電子郵件相似。電子郵件屬性形成基礎，根據這些屬性，將新實例作為未來電子郵件的點繪製。
基於樣本的過濾：使用機器學習算法，根據從樣本郵件中提取的訓練數據，將新電子郵件檢測為垃圾郵件或非垃圾郵件。這些樣本郵件來自合法郵件和垃圾郵件。
適應性電子郵件垃圾郵件過濾：將垃圾郵件分成組。每個組由一個令牌或標誌性文本表示。這些代表性文本由單詞、短語甚至無意義的字符串組成。收到的電子郵件會與這些代表性文本進行比較，並被歸類為垃圾郵件或非垃圾郵件。

基於聲譽的垃圾郵件分析

基於 RBL 的聲譽分析根據來源郵件的詳細信息，根據從該 IP 地址發送的垃圾郵件百分比來評估發送方的聲譽，從而投票決定該消息是否為垃圾郵件。 SCES 會為關鍵的實時黑洞名單（RBL）分配一個信任級別，該級別根據該 RBL 在阻止垃圾郵件方面的準確性進行評級。儘管大多數服務提供商使用 RBL，但 SCES 還提供了一個客戶可配置的過程，以限制虛假陽性，以確保我們的客戶在業務最小影響下獲得高水平的垃圾郵件保護。

基於類別的垃圾郵件分析

非惡意的郵件將被歸為"無"類別並具有較低的垃圾郵件得分。某些政策，例如允許發送者，會故意繞過垃圾郵件掃描，因此不會顯示這些信息。

基於發送者模式的分析

SCES 將學習發送者和接收者之間的通訊並建立模式模型。根據其模式模型，引擎將決定

內容分析和意圖識別

社交媒體中垃圾郵件的存在量大幅增加，因此垃圾郵件的檢測變得至關重要。隨著人們廣泛使用社交媒體，垃圾郵件的內容也隨之增加。人們使用社交媒體的時間越來越長，特別是在疫情期間。用戶通過社交媒體收到許多短信，他們無法辨識這些短信中的垃圾郵件內容。垃圾郵件包含惡意鏈接、應用程序、假帳戶、虛假新聞、評論、謠言等。為了提高社交媒體的安全性，檢測和控制垃圾郵件文本至關重要。涉及檢測和分類垃圾郵件的各種技術包括機器學習、深度學習和基於文本的方法。

附件保護

防病毒

防病毒引擎提供全面的實時掃描和病毒定義更新。它可以檢測到各種已知的病毒、爆發、間諜軟件、木馬、蠕蟲和惡意軟件威脅。

附件預先檢測檢查

附件預先檢測器會破解和分析異常的附件流量和附件文件類型，以預測和阻止潛在的附件威脅。

雲端沙箱

為了保護系統免受未知的高級惡意軟件攻擊，新的進階惡意軟件電子郵件和附件文件將被提交到雲端沙箱。可疑的電子郵件附件將被加密打包發送到強大的雲端沙箱中進行動態沙箱掃描。雲端沙箱提供了額外的分析層，防病毒引擎無法覆蓋。雲端沙箱為 SOC 或 IT 提供專業和全面的分析報告，以更好地了解攻擊。雲端沙箱會與雲端 URLProtect 模塊進行交叉檢查，以對樣本中的任何可疑 URL 進行全面覆蓋，以擊敗下載者攻擊。雲端沙箱支持許多文件類型，包括但不限於辦公文檔、可執行文件、存檔文件等。

釣魚郵件防護

欺騙

強大的釣魚檢測引擎可保護用戶免受以下攻擊：

- 公司身份冒充
- 魚叉式釣魚攻擊
- 電子郵件帳戶被盜用
- 釣魚郵件

動態釣魚檢測

提出了一種基於演化神經網絡和強化學習的釣魚檢測方案。通過利用學習新行為來檢測零日釣魚攻擊。使用了眾所周知的數據集進行評估。

BEC

SCES 能夠識別 BEC 郵件的危險標記（例如，回复地址與發件地址不匹配），並使用機器學習分析郵件語言以尋找攻擊的跡象。

零信任保護

零信任模型意味著不允許傳遞消息，除非它們來自一個被完全信任和清潔的電子郵件，並且已經授權發送方向該收件箱傳送消息。當涉及識別社交工程和惡意內容的趨勢時，SCES 可能是有效的，但當涉及發送者身份時，它們並不提供太多有用的信息，因為電子郵件攻擊者會迅速改變其身份。

郵件存檔(SCEA)

告別電子郵件混亂，擁抱智慧組織，與 SCEA 一起，革新您的電子郵件管理方式。 SCEA 整合了一系列前沿功能，旨在提高生產力並簡化您的溝通，徹底改變您與收件匣互動的方式。

無限儲存空間

永遠不必擔心儲存空間不足。 透過 SCEA，盡情享受無限的儲存容量，儲存您所有的電子郵件、附件和重要文件。 告別儲存限制，迎接無盡的可能性。

人工智慧助理

在您的收件匣中體驗人工智慧的強大功能。 SCEA 的先進人工智慧助理會根據您的行為學習，為您提供個人化建議、優先處理電子郵件，甚至代您撰寫回覆。 無需費力，輕鬆掌握您的通訊。

雲端存取

透過無縫雲端集成，隨時隨地存取您的電子郵件。 無論您是在辦公室、在外出行還是遠端辦公，SCEA 確保您的電子郵件安全儲存在雲端，隨時準備好在您需要時存取。