OPSWAT.

客戶

柏林機場如何保護關鍵基礎設施免受網路攻擊

OPSWAT 技術正在幫助防範可能影響地面和空中安全的惡意軟體攻擊。

BER FLUGHAFEN BERLIN BRANDENBURG

關於柏林勃蘭登堡機場 (BER)： BER 於 2020 年 10 月 31 日開放商業交通，取代了滕珀爾霍夫、舍訥費爾德和泰格爾機場。它現在是唯一一個服務於柏林和周邊勃蘭登堡州的商業機場，該地區共有 600 萬居民。

這是怎麼回事? 柏林勃蘭登堡機場 (BER) 面臨著全球企業都熟悉的挑戰：接收大量檔（每天超過 9000 個檔）並將檔無威脅地返回系統。在採用之前，只有一個防病毒引擎掃描檔 OPSWAT 技術，機場無法確保進入其系統的檔不包含潛在威脅。現在，使用 OPSWAT 的 MetaDefender ICAP Server，整合 OPSWAT BER採用多重掃描 技術和8個防病毒引擎，可以有效地管理其大型檔流，同時防範隱藏在檔中的任何潛在威脅。瞭解如何整合 OPSWAT MetaDefender 該技術顯著提高了惡意軟體檢測率，並縮短了 BER 的爆發檢測時間，使其基礎設施更加安全和高效運營。

工業：
運輸

位置
Schönefeld， 德國

使用的產品：
MetaDefender ICAP Server

關鍵技術：
OPSWAT 多重掃描
配備8個防病毒引擎

越來越多的數據和檔湧入給全球企業帶來了越來越大的壓力，因為公司正在努力管理大量數據，同時確保流入和流出其系統的檔沒有潛在的惡意軟體。機場存在獨特的高風險，因為上傳到其伺服器的檔會影響乘客安全、地面運營和機載資產。

如今的現代機場與小城市共用許多相同的關鍵基礎設施元件，包括電力、供水、污水處理、交通、技術中心和通信。雖然這使得全球各地的機場每天能夠為數百萬人提供服務，但它也在其網路中產生了特別容易受到網路攻擊的壓力點。維護這些系統並提供免費的檔傳輸，同時保持安全和服務，是一項持續的挑戰。

OPSWAT 柏林勃蘭登堡機場已經實施了解決方案，以加強其網路安全並防止網路攻擊。

最近，我們有機會與 Ronny Querfurth 進行了交談，他是 IT 柏林勃蘭登堡機場的解決方案和平臺。作為平臺的一部分，以及 IT 管理，Querfurth 的工作是確保機場的伺服器資產以及關鍵基礎設施保持安全，並確保機場運營保持正常運行。

Querfurth很快指出，與世界各地的城市一樣，機場的安全威脅也在不斷變化，這要求不斷更新協定以應對新的挑戰。值得慶幸的是，像這樣的解決方案 OPSWAT 正在幫助機場保護其關鍵基礎設施。

最新文章

OPSWAT 保護加拿大政府服務免受檔上傳威脅
3月7， 2024

國土報：在威脅到達目的地之前檢測到威脅。
3月6， 2024

OPSWAT 更新 - 2024 年 2 月
3月6， 2024

增強 MetaDefender Linux 上對 CMC 反惡意軟體引擎的平台支援和 Cloud
3月6， 2024

活動總結：2024 年 CNME CIO 領導力獎
3月4， 2024

> 我們以前的解決方案不再適合我們日益增長的要求。跟 OPSWAT，在存取我們的內部網路之前，我們會主動掃描檔。
>
> **羅尼·奎爾福特**
> IT解決方案和平台顧問，
> 柏林勃蘭登堡機場

不斷變化的環境中的主要挑戰

不斷變化的數字威脅迫使安全防禦不斷適應。根據 Querfurth 的說法，直到十年前，大多數中小型組織只需要一個有效的防火牆來保護他們的關鍵資產。然而，今天，國際犯罪組織、駭客和流氓國家採用更複雜的方法來滲透關鍵系統。

作為回應，柏林勃蘭登堡機場等組織採用了一種多層次的深度防禦安全方法，利用多個防火牆、端點檢測和回應以及高階威脅防護來保護其系統免受潛在威脅。

然而，對於柏林勃蘭登堡機場這樣複雜的組織來說，改造系統以實現如此高的安全性是一項巨大的挑戰：

- **他們的網路非常龐大**——BER 有多個分散的、封裝的網段，必須從各個方面進行保護——不僅要通過防火牆從 Internet 存取，還要通過 VPN 進行 GSM 連接。
- 通過機場系統傳輸的檔量是幾年前的兩倍，這增加了包含惡意負載**的檔**通過的幾率;因此，需要在入站檔到達網路之前掃描它們。
- 雖然保護他們的系統是重中之重， **但機場員工還必須能夠完成他們的工作**，其中不僅包括使用互聯網，還包括傳輸檔、上傳影片以及與第三方供應商共享資訊。有些來源是可信的，有些則不可信。因此，他們的系統需要提供針對來自多個媒介的威脅的保護。
- 就像一個城市可能因網路攻擊而失去關鍵服務一樣， **不安全的機場會帶來嚴重的公共安全風險**。除了數據丟失和旅行延誤之外，未能保護機場還威脅到空中和地面人員的安全。
- **遵守** 德國聯邦法律和 IT 保險強制執行。
- 除了今天的威脅之外，BER還必須 **為未來的挑戰做好準備**，包括基於人工智慧的麻煩、社會工程助長魚叉式網路釣魚攻擊等等。

設計氣密系統

正如 Querfurth 所解釋的那樣，“我們以前的解決方案不再真正符合我們的性能要求，需要更新。它落在性能和速度上，因為它只有一個防病毒引擎掃描檔。另一個關鍵點是，以前的解決方案只能在檔進入網路後對其進行掃描。

柏林勃蘭登堡機場現在使用 MetaDefender ICAP Server，隨插即用解決方案，以確保每天通過其系統的檔沒有惡意軟體。 MetaDefender ICAP Server 提供 ICAP 頂部的介面 OPSWAT的高階威脅防禦解決方案，MetaDefender Core.

柏林勃蘭登堡機場現在可以掃描和處理通過 MetaDefender ICAP 在它進入他們的網路並到達最終使用者之前進行介面。

在柏林勃蘭登堡機場的案例中，掃描入站檔案對於確保它們不包含任何類型的惡意負載以及保護其基礎設施中的關鍵元素不被破壞至關重要。 MetaDefender ICAP 只是柏林勃蘭登堡機場大型安檢系統中的一個組成部分。

OPSWAT 多重掃描 技術可以利用 30+ 領先的反惡意軟體引擎，並使用簽名、啟發式和機器學習主動檢測超過 99% 的惡意軟體。這顯著改進了已知和未知威脅檢測，並提供了針對惡意軟體爆發的最早保護。

通過部署 OPSWAT的解決方案是，在進入網路之前，使用多重掃描技術和八個防病毒引擎對檔案進行掃描，在潛在威脅造成問題之前識別它們。

移至 MetaDefender ICAP 還為柏林勃蘭登堡機場提供了速度、上傳能力和可擴充性，以促進未來的增長。

“以前的獨立防病毒解決方案已被棄用，”Querfurth 解釋道，“所以我們決定切換。我們試圖預先評估的是，我們是否可以輕鬆部署它，輕鬆地自己維護它，並且它的性能至少與我們之前的解決方案一樣好。[OPSWAT]做得好，做得更好！

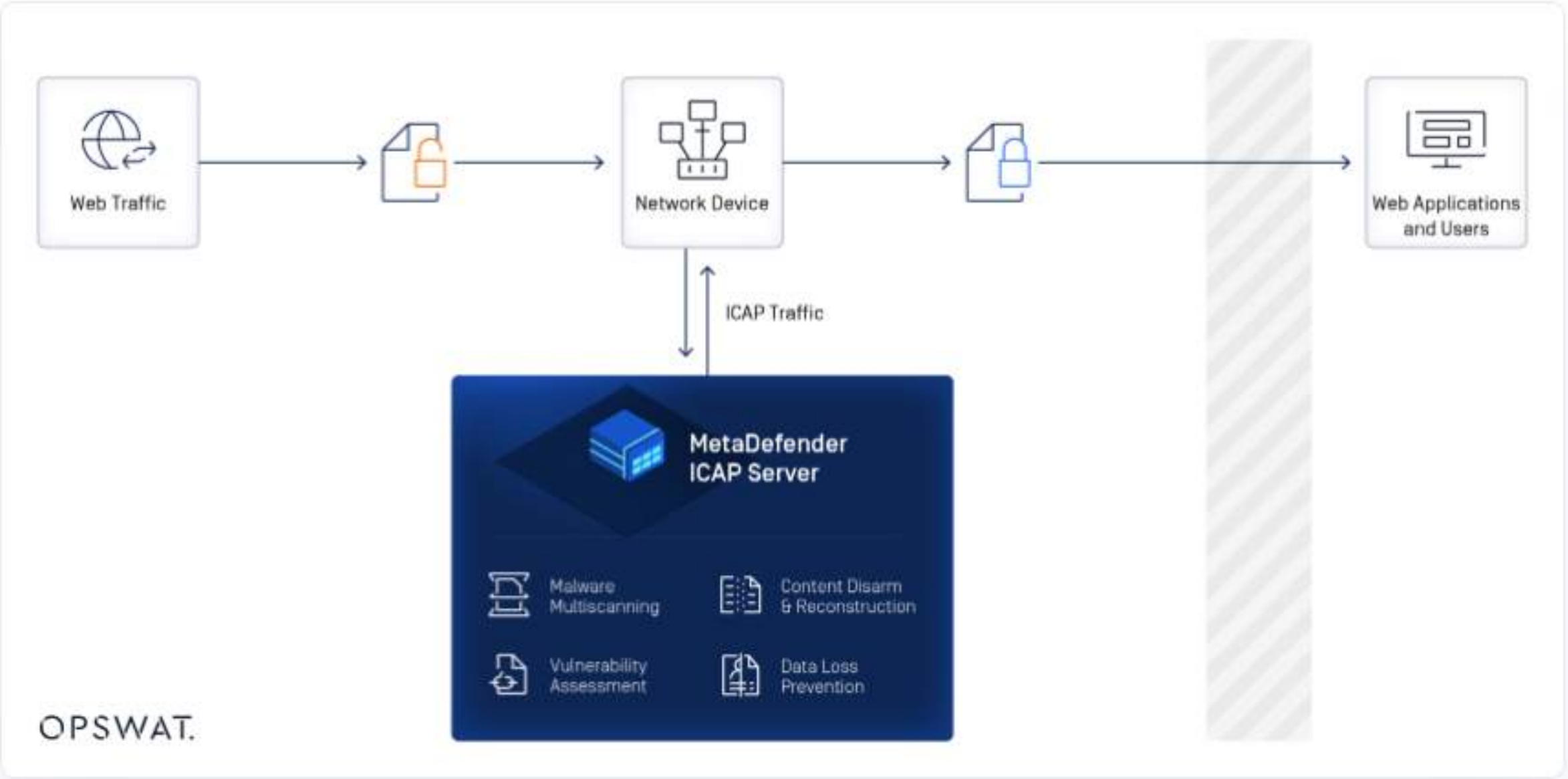
MetaDefender ICAP 還滿足了 Querfurth 團隊的一些額外要求，包括自動更新、監控以及能夠使用他們的代理基礎設施。

系統如何工作

MetaDefender ICAP是一種隨插即用的解決方案，可防止惡意軟體進入網路，它位於柏林勃蘭登堡機場工作流程的中間，並在傳入檔進入系統之前將其拉到一邊進行掃描。

“當有人想嘗試通過我們的數據交換平臺上傳檔時，”Querfurth 解釋說，“他們會觸發上傳過程。例如，一個檔案來自 Internet，並命中位於 DMZ 外側的 Gateway 節點到 Internet。這些網關節點將連接引導到我們 DMZ 中的傳輸節點。

“在非軍事區的另一邊，在我們的保護網路的邊界上，是Transfer節點所在的地方。在檔案進入 Transfer 節點之前，Transfer 節點會將其重定向到 MetaDefender ICAP Server，掃描檔。如果它 [MetaDefender ICAP Server] 認為它是一個無害的檔，它再次將檔重定向到數據交換系統的傳輸節點，該節點獲取檔並將其存儲在我們的數據空間中。



> 有 [MetaDefender ICAP]增加了我們的保護。通過八個防病毒引擎，增加了對惡意檔或惡意軟體的檢測範圍。
>
> **羅尼·奎爾福特**
> IT解決方案和平台顧問，
> 柏林勃蘭登堡機場

最大限度地發揮使用的優勢 MetaDefender ICAP

部署 MetaDefender ICAP 自安裝之日起，柏林勃蘭登堡機場就獲得了許多重要的優勢：

每個檔 在到達柏林勃蘭登堡機場的伺服器之前都會被掃描。
→

OPSWAT 多重掃描通過發現更多潛在威脅來 **提供更好的保護** 。
→

與之前的單掃描儀解決方案相比，**掃描時間縮短，精度提高**。
→

重新掃描的檔更少， **節省了時間和金錢**。
→

MetaDefender ICAP 使機場的系統更快、可擴展、更高效，從而減少了所有相關人員 **的工作量** 。
→

柏林勃蘭登堡機場大大擴展 **了檔案掃描量**， 而不會出現中斷或停機。
→

防護 Supply Chain 攻擊

去年夏天，總部位於馬薩諸塞州 的Progress Software 公司發生了一起重大違規行為，這證明瞭這一點。 IT 公司可能會被犯罪分子貶低。在這種情況下，Progress 的MOVEit Transfer檔管理程式遭到破壞，該程式被全球數千家組織用於通過Internet傳輸通常包含敏感材料的檔。

據 路透社報導，全球有600多個組織受到影響，包括石油和天然氣巨頭殼牌、一些金融機構、眾多醫療機構以及包括一些機場在內的許多其他組織，使其成為今年迄今為止最大的駭客攻擊。

機場仍然是有吸引力的目標，正如 最近的攻擊 所表明的那樣，採用 零信任 和漏洞掃描等網路安全最佳實踐可以幫助潛在目標保護自己免受 DDoS 攻擊和影響英國航空公司等知名公司的 MOVEit SQL 注入。文章還建議機場採用以程 threat intelligence 監控，因為目標通常在攻擊之前宣佈。

未來會怎樣?

在Querfurth看來，未來將是柏林勃蘭登堡機場的本地系統和外部雲服務之間的互連。柏林勃蘭登堡機場今天正在採取措施，確保這些連接的安全。

正如 Querfurth 所解釋的那樣，“你不能只是說，'安全性將在未來某個地方得到改善。 **您必須立即採取行動，找到解決方案，找到**挑戰，在安全層上檢查整個過程，保護您的網路，保護您的客戶數據，並保護您的系統。

瞭解如何操作 OPSWAT的 MetaDefender ICAP Server配置為隨插即用解決方案，可以增強您的惡意軟體防護，請立即聯繫我們的專家。

諮詢專家

標籤： MetaDefender ICAP Server，多重掃描技術