BlackBerry
Intelligent Security. Everywhere.

評估指南

評估 AI 驅動型安全解決方案的 5 個技巧

當安全供應商推廣其產品的 AI 功能時，要詢問他們哪些問題

人工智能 (AI) 已經成為安全行業的一個熱門詞彙，但由於這種說法隨處可見，幾乎失去了本身的意義。當每個產品都宣傳其 AI 功能時，安全決策者可能會變得對此不屑一顧。甚至影響當今網絡安全態勢的重大創新也激不起其興趣。

在評估基於 AI 的技術時，理解 AI 和機器學習在網絡安全方面的區別非常重要：

- AI 是一個廣義的概念，指機器能夠以人類認為的智能方式執行任務。
- 機器學習是 AI 的具體應用。它所依據的原理是，如果機器能夠訪問數據集並得到自學許可，機器就能夠智能地執行指定任務。這個過程通常被稱為“訓練”。

當安全供應商推廣其產品的 AI 功能時，您應當詢問以下五類問題。

發現增加 AI 的真正動機非常重要，這就需要向每位供應商瞭解新增的 AI 功能將如何提高您的整體安全。

1. 您的安全產品為何增加 AI 功能？

當供應商發現有更好的方法來保護系統，或者在應對市場需求的壓力時，他們通常會為其解決方案增加新功能。增加 AI 也不例外，所以瞭解供應商在其技術中增加 AI 的動機很重要。

- 您的產品為什麼要使用 AI?
- AI 是您的安全產品的核心組成部分，還是現有產品的特色功能?
- AI 將帶來哪些新功能?
- 與類似的非 AI 產品相比，AI 為您的產品增加了哪些優勢?

2. AI 對我的組織有什麼益處？

供應商為了營銷而不是客戶利益在產品中增加新功能，這種情況並不少見。發現增加 AI 的真正動機非常重要，這就需要向每位供應商瞭解新增的 AI 功能將如何提高您的整體安全。

- 您產品的 AI 功能將如何具體惠及我的組織?
- 您的 AI 能否在不影響員工工作效率的情況下保護員工網絡?
- 您的 AI 是否能保護移動、OEM 和 IoT 設備?
- AI 的融入將如何影響您的產品性能以及其對企業和終端資源的使用?

3. 您的 AI 有多智能？

AI 可以簡單也可以複雜。簡單的 AI 擅長基於已知信息做出決策，比如根據棋盤的當前局勢移動某個棋子。它會衡量現有數據以確定最佳結果，並可以通過多次迭代重復此行為。它沒有關於過去的記憶，也沒有預測未來的強大能力。複雜的 AI 需要大量的訓練數據集、神經網絡體系結構和長期、適當的訓練。它擅長模式匹配和預測任務。複雜的 AI 不返回定量答案（例如，將某個棋子移動 X 步），而是返回定性答案（例如，該對象與其他對象相同的概率為 89%）。

瞭解安全供應商使用的是哪種類型的 AI 非常重要，這樣您才能對結果有正確的預期。同樣，AI 的有效性也可以通過其訓練的持續時間和深度得到提高。這意味著一項在大型數據集上訓練了十年的 AI 比在同一數據集上訓練了較短時間的新 AI 更為有效。

- 您的解決方案使用的是簡單還是複雜的 AI?
- 您的 AI 是如何訓練的?
- 您的 AI 模型在測試和真實環境中的表現如何?
- 您的 AI 是否能夠在零信任架構中運行，或者在 MITRE ATT&CK 框架中解決威脅?
- 您的 AI 能否檢測環境和用戶行為的變化，並相應地調整訪問和權限?

甲、

> 複雜的 AI 需要大量的訓練數據集、神經網絡體系結構和長期、適當的訓練。它擅長模式匹配和預測任務。

4. 您的 AI 是如何維護的？

保持 AI 訓練有素和相關性所需的維護取決於 AI 的使用方式。例如，如果供應商使用 AI 來自動創建針對新威脅的簽名，這時 AI 通常由供應商維護。這實際上可能不會讓組織受益，因為這可能會導致更多的供應商更新終端。或者，如果 AI 在雲端經過訓練後再部署到終端，這時組織可以受益於一致的防護，且維護成本最低。

甲、 您的 AI 在哪裡? AI 是在您的雲端運行還是在終端本地運行?

乙、 您的 AI 具體是如何使用的? 您的 AI 是否用於自動創建簽名? 您的 AI 是否用於對威脅做出實時決策?

丙、 您的 AI 解決方案需要多少維護成本，包括員工培訓和主動的關注?

丁、 AI 多久接受一次再訓練?

5. 您能在我們的環境中演示一下嗎？

對任何安全解決方案的真正測試標準應基於它在您組織中的表現好壞。任何銷售安全產品的公司都應該樂於在您的基礎設施中展示其產品性能。警惕那些只提供內部測試結果和一味地向您作出保證的公司。測試環境中使用的攻擊性級別可能與企業的實際需求有巨大差別，終端用戶需要進行調整。這意味著終端保護的內部測試結果可能代表未完成訓練的數學模型。

甲、 AI 提供攻擊性級別了嗎?

乙、 AI 需要多大程度地依賴雲端才能發揮作用? AI 在線下能否像在線上一樣有效?

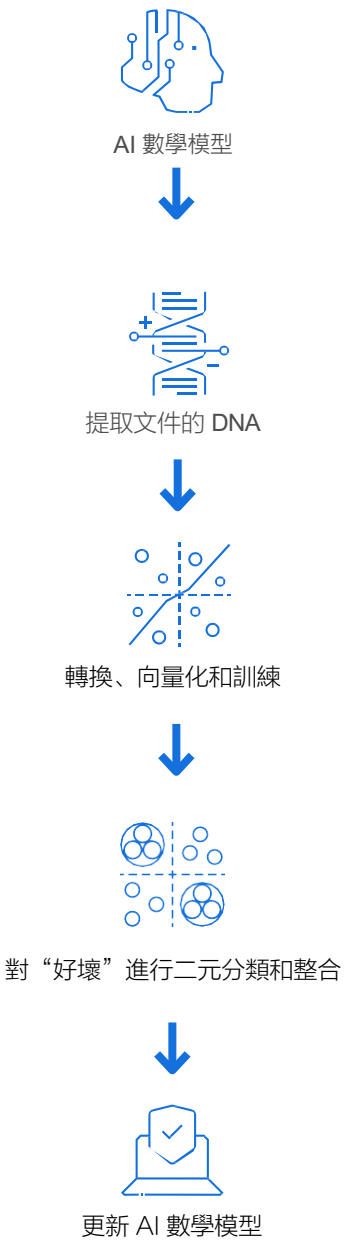
丙、 在沒有連接到雲端的情況下，AI 能否阻止終端上的零日惡意軟件?

丁、 AI 能阻止其訓練集從未遇到過的惡意軟件嗎?

戊、 AI 是否經過第三方測試，以確認其是否能檢測和/或防止 AI 模型訓練時不存在的惡意軟件?

訪問 BlackBerry®Spark Suites，進一步瞭解所有終端上 AI 驅動的安全性。

訓練 AI/ML 模型



關於BlackBerry

BlackBerry 公司（NYSE：BB；TSX：BB）致力於為世界各地的企業和政府機構提供智能安全軟件和服務。今天，公司為超過 5 億台終端提供安全保障，包括 1.75 億輛上路行駛的汽車。公司總部位於安大略省滑鐵盧，運用人工智能（AI）和機器學習，在網絡安全、安全和數據隱私領域提供創新解決方案，並且也是終端安全管理、加密和嵌入式系統領域的領軍企業。BlackBerry 的願景明確清晰，就是要打造值得信任的、安全的互聯未來。

如需了解更多信息，请造訪 *BlackBerry.com* 並關注 *@BlackBerry*。

BlackBerry
Intelligent Security. Everywhere.

MKTG20-0696 | 211027