Intelligent Security. Everywhere.

評価ガイド

AI 駆動型セキュリティソリューションを評価するための 5 つのヒント

自社製品の AI 機能を宣伝する
セキュリティベンダーに何を尋ねるべきか

AI（人工知能）はセキュリティ業界で話題となっており、宣伝文句としてほとんど意味をなさなくなるほど広く採用されています。すべての製品で AI 機能が宣伝されているため、セキュリティの意思決定者は、今日のサイバーセキュリティを形成する最も魅力的なイノベーションさえも高く評価しないことがあります。

AI ベースのテクノロジーを評価する場合には、サイバーセキュリティに関して AI と機械学習の違いを理解することが重要です。

- **AI** とは、インテリジェントとみなされる方法でタスクを実行できるマシンを示す幅広い概念です。
- **機械学習**とは、もっと具体的に AI を応用することです。これは、マシンがデータセットへのアクセスを付与され、自ら学習できる場合に、割り当てられたタスクをインテリジェントに実行できるという原則に基づいています。このプロセスは、一般に「トレーニング」と呼ばれます。

以下に、製品の AI 機能を勧められたときに、セキュリティベンダーに尋ねるべき 5 つのカテゴリの質問を示します。

各ベンダーの実装によって自社の全体的なセキュリティがどのように改善するかを把握することにより、AI を搭載した真の動機を明らかにすることが重要です。

1. 貴社のセキュリティ製品にはなぜ AI 機能が搭載されているのですか？

一般にベンダーは、システムの保護を改善する方法を発見した場合や、市場の需要を満たすプレッシャーに対応する場合に、ソリューションに機能を追加します。AI の搭載についても例外ではないため、AI を自社のテクノロジーに組み込んだベンダーの動機を把握することが重要です。

- なぜこの製品は AI を利用しているのですか？
- AI は貴社のセキュリティ製品のコアコンポーネントですか、それとも既存の製品に追加された機能ですか？
- AI によって、どのような新しい機能が実行されますか？
- AI の搭載によって、AI を搭載していない類似の製品よりも貴社製品の性能はどのように高まりますか？

2. 貴社の AI はどのようなメリットを当社にもたらしますか？

顧客のメリットよりも、マーケティング上の目的のために製品に機能を追加するベンダーも存在します。各ベンダーの実装によって自社の全体的なセキュリティがどのように改善するかを把握することにより、AI を搭載した真の動機を明らかにすることが重要です。

- 貴社製品の AI は具体的にどのようなメリットを当社にもたらしますか？
- 貴社の AI は、生産性を低下させることなく従業員を保護しますか？
- 貴社の AI によって、モバイルデバイス、OEM デバイス、IoT デバイスは保護されますか？
- AI の搭載は、貴社の製品のパフォーマンスと、企業やエンドポイントのリソースの利用にどのような影響を及ぼしますか？

3. 貴社の AI はどの程度スマートですか？

シンプルな AI もあれば、複雑な AI もあります。シンプルな AI は、チェス盤の現在の状態に基づいて駒の動きを選択するような、既知の情報に基づいて意思決定を下すことが得意です。このような AI は、既存のデータに重みを付けて最適な結果を決定し、何度もこの処理を繰り返すことができます。しかし、これは過去の記憶や未来を予測する優れた機能を備えていません。

複雑な AI は、大量のトレーニングデータセット、ニューラルネットワークアーキテクチャ、適切にトレーニングするための相当な時間を必要とします。このような AI は、パターンマッチングと予測タスクに優れています。複雑な AI は定量的な回答（たとえば、X に対するチェスの駒の移動）を返す代わりに、定性的な回答（たとえば、このオブジェクトが他のオブジェクトと同じである確率は 89%）を返します。

どの程度の結果が期待できるかを正しく判断するために、セキュリティベンダーが利用している AI のタイプを把握することが重要です。同様に、AI の効果は、トレーニングの期間と深さによって改善されます。したがって、大規模なデータセットで 10 年間トレーニングした AI は、同じデータセットで短期間トレーニングした比較的新しい AI よりも効果的になります。

- 貴社のソリューションはシンプルな AI を利用していますか、それとも複雑な AI を利用していますか？
- 貴社の AI はどのようにトレーニングされていますか？
- 貴社の AI モデルは、テスト環境と実際の環境の両方で、どの程度トレーニングされていますか？
- 貴社の AI は、ゼロトラストアーキテクチャ内で動作しますか、または MITRE ATT&CK フレームワークの脅威に対処できますか？
- 貴社の AI は環境とユーザー行動の変化を検知し、それに応じてアクセスと権限を調整できますか？

複雑な AI は、大量のトレーニングデータセット、ニューラルネットワークアーキテクチャ、適切にトレーニングするための相当な時間を必要とします。このような AI は、パターンマッチングと予測タスクに優れています。

4. どのように AI がメンテナンスされていますか？

AI を十分にトレーニングし、妥当性を保つために必要なメンテナンスは、AI の利用方法によって異なります。たとえば、ベンダーが新たな脅威に対するシグネチャの生成を自動化するために AI を利用している場合、一般に AI はベンダーによってメンテナンスされます。これにより、エンドポイントに対する更新が増加するため、実際上、組織にメリットをもたらさない可能性があります。その代わりに、AI がクラウドでトレーニングされてからエンドポイントに展開される場合、組織は最小限のメンテナンスで一貫した防御のメリットを受けることができます。

- 貴社の AI はどこに配置されていますか？AI はクラウドで実行されますか、それともエンドポイントでローカルに実行されますか？
- 具体的に、AI はどのように利用されますか？AI は、シグネチャの生成を自動化するために利用されますか？AI は、脅威に対してリアルタイムの意思決定を下すために利用されますか？
- 貴社の AI ソリューションでは、従業員のトレーニングと意識的な注意を含め、どの程度のメンテナンスが必要ですか？
- AI は、どの程度の頻度で再トレーニングされますか？

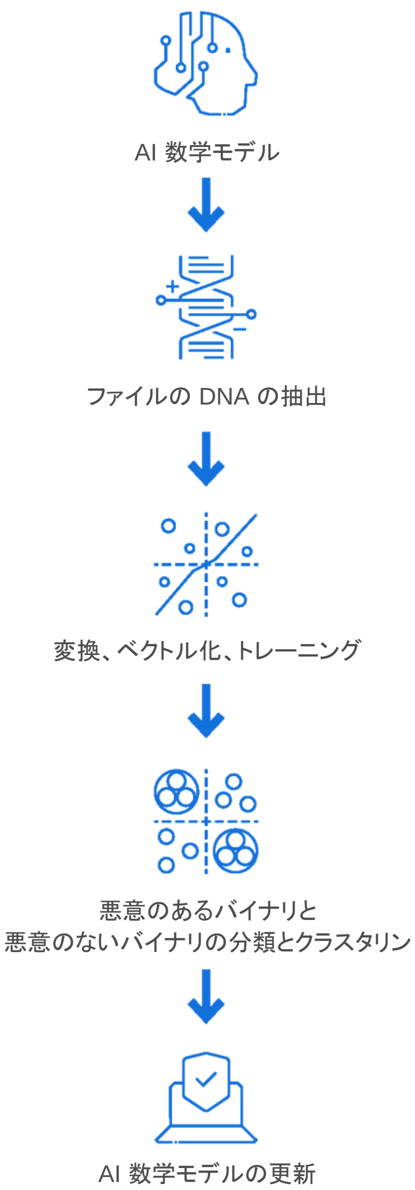
5. 当社の環境でデモを実行できますか？

セキュリティソリューションを正しくテストするには、自らの組織でどの程度機能するかを検証する必要があります。セキュリティ製品を販売している企業は、顧客のインフラストラクチャ内でそのパフォーマンスのデモを進んで引き受けるはずです。社内テストの結果のみを示して、性能について大胆に断言する企業には注意してください。テスト環境で使用される保護レベルは、実際の企業のニーズとは大きく異なり、エンドユーザーによる調整が必要になることがあります。つまり、エンドポイント保護に関して社内テストの結果しか示さない場合は、トレーニングの不十分な数学モデルが利用されている可能性があります。

- AI は複数の保護レベルを提供しますか？
- AI を効果的にするためにどの程度クラウドに依存していますか？AI はオンラインの場合と同程度にオフラインで効果的ですか？
- AI は、クラウドに接続せずに、エンドポイントでゼロデイマルウェアを防御できますか？
- AI は、トレーニングセットに含まれていなかったマルウェアを防御できますか？
- AI は、AI モデルのトレーニング時に存在していなかったマルウェアを検知/防御する機能を確認するために、サードパーティによるテストを受けましたか？

すべてのエンドポイントにわたる AI 対応セキュリティの詳細については、BlackBerry®Spark Suites アクセスしてください。

AI/ML モデルのトレーニング



BlackBerry について

BlackBerry (NYSE: BB; TSX: BB) は、インテリジェントなセキュリティソフトウェアおよびサービスを世界中のエンタープライズと政府機関に提供しています。現在セキュリティで保護しているエンドポイントの数は 5 億台を上回り、そのうちの 1 億 7,500 万台は道路を走行する車両です。BlackBerry はカナダのオンタリオ州ウォータールーに本拠を置き、AI と機械学習を活用してサイバーセキュリティ、安全、データプライバシーソリューションの分野に革新的なソリューションを提供しています。また、エンドポイントセキュリティ管理、暗号化、組み込みシステムの分野におけるトップクラスの企業です。BlackBerry のビジョンは明確です。つながる未来に信頼性あるセキュリティを確保することです。

詳細については、BlackBerry.com にアクセスし、@BlackBerryJPsec をフォローしてください。

BlackBerry
Intelligent Security. Everywhere.