2020 年 3 月 26 日
フォーティネットジャパン株式会社

米国時間 2020 年 2 月 24 日に発表されたプレスリリースの抄訳です。

フォーティネット、高速に脅威を検知する自己学習型の人工知能アプライアンスを発表

ディープニューラルネットワークを活用して脅威の検知と修復を自動化する FortiAI が、フォーティネットの AI ドリブン セキュリティのさらなる強化に貢献

幅広い適用領域で（Broad）システム連携し（Integrated）自動化された（Automated）サイバーセキュリティソリューションの世界的リーダーであるフォーティネット（Fortinet®、NASDAQ: FTNT）は本日、自己学習型のディープニューラルネットワーク（DNN）を活用して脅威の修復を高速化し、時間のかかるセキュリティアナリストの手作業のタスクを処理する初のオンプレミスアプライアンス、FortiAI を発表しました。FortiAI の Virtual Security Analyst™ は、フォーティネットの FortiGuard Labs が開発した業界最高レベルの成熟度を誇るサイバーセキュリティ用の人工知能を組織のネットワークに直接組み込むことで、高度な脅威を非常に高速に検知します。

困難な戦いに直面する今日の組織

セキュリティアーキテクトは、脅威の検知と修復において次のような多くの課題に直面しています。

- **ますます高度化するサイバー犯罪者の手口：**従来からのサイバー脅威が継続する一方で、脅威の高度化も進んでおり、その多くに人工知能や機械学習、オープンソースコミュニティが関与しています。その結果、脅威の進化に後れを取らないことが組織とその防御対策の課題になっています。

- **拡大を続ける攻撃対象領域**：何百万もの新しいアプリケーションの登場、そしてクラウドの採用や接続デバイスの増加によって、数十億規模のエッジが生まれています。セキュリティチームにはその適切な保護と管理が求められており、組織は数多くの潜在的な侵入ポイントに起因する脅威の増加への対応という課題に直面しています。

- **サイバーセキュリティのスキル不足に苦しむセキュリティチーム**：サイバーセキュリティ業界におけるスキルギャップが組織にとって最大のリスクになっています。増加し続ける潜在的あるいは実際の脅威のトリアージ、調査、レスポンスを適切に処理できるスキルを持つプロフェッショナルの不足が原因で、サイバー犯罪者は従来型のセキュリティプロセスやツールを簡単に突破するようになっています。

組織の脅威保護に適応する自己学習型 AI

セキュリティのプロフェッショナルが直面している前述の課題を解決するため、フォーティネットは脅威の修復を高速化する FortiAI Virtual Security Analyst™ を発表しました。時間を要する手作業による多くのタスクを FortiAI が担うことで、セキュリティプロフェッショナルはより価値の高いセキュリティに集中できるようになります。FortiAI は、その自己学習能力によって組織のネットワークへの導入後も進化を続けます。

FortiAI は、人間の脳のニューロン（神経細胞）を模倣するディープニューラルネットワークと呼ばれるディープラーニング機能を活用し、導入された組織に固有の脅威に対する科学的分析に基づいて複雑な判断を行います。FortiAI の人工知能の成熟度が継続的に向上するに伴って、FortiAI の Virtual Security Analyst™も効果的に変容し、脅威保護の改善によるメリットがもたらされます。

高度化する脅威に対抗する FortiAI

フォーティネットの DNN（ディープニューラルネットワーク）のアプローチにより、FortiAI は脅威保護に次のような革新的進歩をもたらします。

- **時間の要する手作業の調査を自動化し、リアルタイムの脅威の特定と分類を実現：**限られた人数のセキュリティ担当者が従来型のセキュリティプロセスを担当している組織では、すべての脅威アラートを手作業で調査することは困難です。結果としてレスポンスが遅れることになり、データ侵害やセキュリティインシデントをはじめとするさらなるリスクが発生します。このような課題を解決するため、FortiAI は DNN を活用して調査を自動化し、脅威のあらゆる動きを特定して最初の感染デバイスとそれに続くすべての感染を素早く見つけ出します。

- **攻撃を直ちに検知して修復を可能にするセキュリティプロセスの転換：**FortiAI の Virtual Security Analyst™は、脅威の特性を科学的に分析して精度の高い判定を実行することで脅威への迅速なレスポンスを実現し、組織が脅威にさらされる時間を大幅に短縮します。

- **脅威インテリジェンスのカスタマイズによって誤検知を大幅に低減：**誤検知の原因調査はセキュリティアナリストにとって大きな負担であり、脅威かどうかの判断にも時間を要します。FortiAI は、個別にカスタマイズされた脅威インテリジェンスを活用してマルウェアの新たな機能を学習し、新たな攻撃にも即座に適用して誤検知を低減します。

エアギャップで隔離されたネットワークをオンプレミスで保護

FortiAI のもう 1 つの重要な差別化要素として、エアギャップで隔離されたネットワークが存在する組織に最適なオンプレミスの AI が提供されている点が挙げられます。OT 環境、政府機関、そして一部の大規模エンタープライズは、ネットワークへのインターネット接続を制限する厳格な法規制やセキュリティポリシーを遵守しなければなりません。自己学習型 AI モデルを採用する FortiAI は、学習や成熟度の向上にあたってインターネット接続を必要としないため、閉じられた環境や厳格なセキュリティポリシーが要求される組織であっても常に最新の脅威に対応できるようになります。

フォーティネットの AI ドリブンテクノロジーで脅威保護を自動化

フォーティネットは、長年にわたって人工知能を活用し、お客様のセキュリティ態勢の強化を支援してきました。フォーティネットが提供している次の既存製品やサービスは、最小二乗法による最適化やベイズ確率メトリクスなどのさまざまな形の AI を活用する新しい FortiAI によって補完されることになります。

- **FortiGuard Labs の脅威インテリジェンス：**FortiGuard Labs は、実績ある高度な AI と機械学習を活用して 1,000 億以上のセキュリティイベントを日々収集し、分析しています。FortiGuard Labs によって生成されるこの脅威インテリジェンスは、フォーティネットを代表する FortiGate NGFW をはじめとする多くのフォーティネット製品で、サブスクリプションサービスとしてご利用いただけます。このサービスにより、お客様はグローバル規模で FortiGuard Labs に配備された人工知能を活用して迅速に脅威を防止できます。

- **FortiSandbox：**フォーティネットは、サンドボックスに AI を採用して侵害からの保護を自動化した初のセキュリティベンダーです。FortiSandbox は、2 つの機械学習モデルをゼロデイ脅威の静的 / 動的両方の分析に採用し、ランサムウェアやクリプトジャッキングなどの常に進化するマルウェアの検知機能を強化しています。さらに FortiSandbox は、ユニバーサルなセキュリティ言語を使用してマルウェアを分類し、ネットワークチームとセキュリティチームの議論を相互に関連付けてセキュリティオペレーションの統合と改善を促進します。

- **FortiEDR：**フォーティネットの FortiEDR は、機械学習を活用してオーケストレーションによるリアルタイムのインシデントレスポンスを実現し、高度な脅威に対するエンドポイント保護を自動化します。お客様は、自社の環境内でネットワーク、ユーザー、ホストのアクティビティの詳細な制御が可能になるというメリットを享受することも可能です。

- **FortiInsight：**FortiInsight は、機械学習に基づく分析を活用してエンドポイント、データの移動、ユーザーの行動を監視し、異常や悪意のある振る舞い、内部リスクに起因するポリシー違反などを検知します。

- **FortiWeb：**Web アプリケーションや API の保護を強化するため、FortiWeb は機械学習を活用して個々のアプリケーションに最適な防御を提供します。結果として、FortiWeb は脅威を迅速にブロックし、エンドユーザーエクスペリエンスの低下につながる恐れがある誤検知を最小限に抑制することができます。

- **FortiSIEM**：FortiSIEM は、機械学習を活用して場所や時刻、使用デバイス、アクセスした特定のサーバーなど、一般的なユーザーの振る舞いにおけるパターンを認識します。異なる場所からの同時ログインをはじめとする異常なアクティビティが発生した場合は、FortiSIEM がセキュリティオペレーションチームに自動的に通知できます。

サイバー犯罪者が攻撃を高度化し、拡大するデジタル攻撃対象領域を悪用しようとする状況においては、フォーティネット セキュリティ ファブリックの幅広く綿密な AI ドリブンテクノロジーによって、自動化された瞬時の比類ない脅威の防止、検知、そしてレスポンスが実現します。

お客様の声

「フォーティネット セキュリティ ファブリックのプラットフォーム活用により、FortiSandbox の導入からゼロデイ脅威に対する保護の実現に至るまで、すべてがシームレスに進行しました。FortiSandbox は、当社の境界、クライアント、メールサーバーを保護するとともに、究極的には高度な未知の脅威から当社の資産を保護してくれます。FortiSandbox の AI ドリブンの優れた能力を活用することで、AI ドリブンの脅威への対応が可能になっただけでなく、セキュリティの構成と管理も容易になりました」

- Ente Autonomo Volturno 社、システム / ネットワーク管理者、Dario Palermo 氏

フォーティネット プロダクト担当エグゼクティブバイスプレジデント兼 CMO、John Maddison（ジョン・マディソン）は次のように述べています。

「フォーティネットは、FortiGuard Labs が提供するクラウドベースの AI ドリブンの脅威インテリジェンスに対して多大な投資を続け、脅威の検知数増加、迅速化、そして精度向上を実現してきました。FortiAI は、FortiGuard Labs から人工知能に関する知見を取得し、オンプレミス環境への配備に最適なパッケージとして提供されます。お客様は自社環境に最適な FortiGuard Labs のインテリジェンスを活用でき、高度な脅威であっても自己学習型の AI が非常に高速に特定し、分類、調査を行うことが可能になります」

関連リンク

FortiAI

フォーティネットについて (www.fortinet.com)

フォーティネット（NASDAQ: FTNT）は、世界中の大手企業、サービスプロバイダ、そして政府機関を守っています。フォーティネットは、拡大するアタックサーフェス（攻撃対象領域）に対するシームレスな保護とインテリジェンスを提供し、外部との明確な境界が消滅したネットワークでの、増え続けるパフォーマンスの条件に応じるパワーで、現在もまた将来も、お客様に貢献します。ネットワーク上でも、アプリケーションやクラウド、またはモバイル環境であっても、妥協することなく、極めて重大なセキュリティ上の問題に対応するセキュリティを提供できるのはフォーティネットのセキュリティ ファブリックのアーキテクチャだけです。フォーティネットは世界で最も多くのセキュリティアプライアンスを出荷し、世界 440,000 以上のお客様がビジネスを守るためにフォーティネット に信頼を寄せています。フォーティネットのネットワークセキュリティエキスパート(NSE)インスティチュートは、テクノロジーカンパニーとしても、ラーニングカンパニーとしても業界で最も大きく広範なサイバーセキュリティのトレーニングプログラムを有しています。フォーティネットジャパンについては、www.fortinet.com/jp をご覧ください。

合があります。フォーティネットは、本プレスリリース内の第三者に帰する声明、認可またはテストについては、検証を行っておらず、また、このような第三者に帰する声明を承認するものではありません。本プレスリリースは、保証または債務保証、または契約として一切拘束を受けるものではなく、記載された製品仕様または製品性能は、ある特定の環境や条件のもとで計測されていることがあります。また、本プレスリリースには、将来の見通しに関して不確実性および仮説を伴う記述が含まれている場合がありますが、本不確実性が現実になったり、あるいは本仮説が正しくないことが判明したりする場合、明文的あるいは暗黙的に記述された内容と異なる結果が生じることがあります。これには、サイバー犯罪活動の動向予測に関する記述などが含まれますが、これに限定されるものではありません。このような動向は予測することが困難であり、また、このような動向に関する公開予測や期待事項は結果として正しくないことがあります。フォーティネットは、このような将来見通しを改正する義務を一切負うものではなく、また改正を発行することもありません。