ウォッチガード、AIを活用したアンチウイルスサービス「IntelligentAV」を発表

2018年8月
８日（水）ー企業向けネットワークセキュリティソリューションのグローバルリーダであるWatchGuard（R）Technologiesの日本法人、ウォッチガード・テクノロジー・ジャパン株式会社（本社：東京都港区、代表執行役員社長 谷口 忠彦、以下ウォッチガード）は、同社のUnified Security
Platform（TM）アプライアンスFirebox（R）に搭載されているオペレーティングシステムの最新バージョン
Fireware（R）12.2を発表しました。今回のアップデートでは、新たなアンチウイルススキャンサービス、IntelligentAV（TM）が追加されました。IntelligentAVは、AI（人工知能）によるスキャンエンジンにより、常に進化するゼロデイマルウェアを予測、検知、そして防御を実現します。同機能は、既にFireboxプラットフォームで利用可能なThreat Detection and Response（TDR：相関分析、優先順位付け、レスポンス）、Gateway AntiVirus（ゲートウェイアンチウイルス）、APT Blocker（標的型攻撃対策）などの先進技術に加わり、多層防御機能をさらに強化します。

ウォッチガードのプロダクトマネジメント担当VPであるBrendan Patterson（ブレンダン・パターソン）は、次のように説明しています。「当社が四半期ごとに発行しているインターネット脅威レポートでは、ウォッチガードの顧客を標的にしているマルウェアの半数近くがゼロデイ攻撃によるものであることが判明しています。従来のシグニチャベースのアンチウイルス機能は、現在でも重要なセキュリティ機能の1つであることに変わりありませんが、最新の巧妙化したマルウェアに対しては十分な防御機能を提供できておらず、検知が回避されているのが現状です。ウォッチガードでは、企業が情報資産や顧客情報を保護する上で、高度なセキュリティサービスによる多層防御が最善策であると確信しています。今回、ユーザにハイパフォーマンスな多層防御を提供するために、ベストインクラスのテクノロジを提供する当社の方針の一環としてIntelligentAVを導入することに決定しました。」

IntelligentAVは、Cylance社の機械学習技術を活用したマルウェア検知エンジンを使用しており、最新の脅威インテリジェンスやシグニチャデータベースを必要とせずに、今後出現し得るマルウェアサンプルを正確に予測し、検知することが可能です。例えば、独立系調査会社であるSE Labsが実施したテストでは、2015年バージョンのAI検知エンジンを使用して、公に拡散する33ヵ月前の主要な脅威を正確に特定し、防御しています。結果として、IntelligentAVはシグニチャに依存せずにマルウェアを継続的に検知し、防御することが可能であることが証明されました。

「この度、Cylanceの先進的なセキュリティ技術がIntelligentAVとしてウォッチガードのFireware OSの重要な多層防御の1つに採用されたことは大変喜ばしく、今後、ウォッチガードのTotal Security
Suiteのさらなる付加価値の向上に貢献できることを期待しています。CylanceのAI技術は予測お

よび防御の精度を高めることができるため、ウォッチガード製品の脅威に対する保護をより強固にするものです。」（Cylance Japan株式会社 取締役社長 金城 盛弘）

Advanced Network Systems, Inc.のエンジニアリング担当バイスプレジデントであるTony Petrella（トニー・ペトレラ）氏は、次のようにコメントしています。「ゼロデイマルウェアの脅威は、私たちのクライアントにとって大きな問題であり、IntelligentAVは、強力な『多層防御』戦略の一環として重要な位置付けにあると言えます。AIコンポーネントにより、レガシーのAVが見逃してしまうような新たなマルウェアやランサムウェアに対して、さらに堅牢かつプロアクティブな防御体制を敷くことが可能になります。」

Fireware バージョン12.2では、IntelligentAVの他にも様々な機能強化が提供されています。以下に主要な機能を紹介します：

Firebox Cloud管理のアップグレード：WatchGuard System Manager で、Amazon Web ServicesまたはMicrosoft Azureでホスティングされている複数のFirebox Cloudインスタンスの管理が行えるようになりました。

地域別防御設定ポリシー：特定の国における送受信トラフィックに制限を設けるきめ細かいポリシーを設定することが可能になりました。

TLSプロキシプロトコル：POP3SおよびSMTPS（またはTLS上のPOP3およびSMTP）のメール検索プロトコルで、プロキシおよびマルウェアのインスペクションが可能になりました。

WebBlockerのアップデート：カテゴリ別（例：武器、攻撃性、精神衛生上の問題）にアラートを生成する機能が追加されました。

複数サーバの認証：単一のFireboxの背後で、それぞれのプロキシ認証により、複数の異なるサーバやアプリケーションのホスティングが可能になりました。

USB型データ端末に対応：Firebox内蔵USBポートでUSB型データ端末に対応し、WAN回線に3GやLTE通信（４G）を利用することが可能になりました。工事現場やイベント会場など有線回線を引くことができない環境、バックアップ回線としてのLTE通信、およびIoT向けのセキュリティ対策など多方面で活用できます。なお、富士ソフト社製 FS040U、ネクス社製 UX302NC、UX302NCRが既に、対応USB型データ端末（USBモデム）として各通信キャリア、MVNOへの対応が可能です。

IntelligentAVは、WatchGuard Total Security Suiteライセンスで利用可能となっており、本日発表したFirebox M270以上の上位機種並びにクラウドおよび仮想アプライアンスをご利用になられているお客様は、追加費用なしに、すぐにIntelligentAV機能が利用可能です。

IntelligentAVに関する詳細は以下のページをご覧下さい。
https://www.watchguard.co.jp/products/security-services/intelligentav

【WatchGuard Technologiesについて】
WatchGuard (R) Technologiesは、ネットワークセキュリティ、セキュアWi-Fi、多要素認証、そしてネットワークインテリジェントを提供するグローバルリーダとして、全

世界で約10,000社の販売パートナーとサービスプロバイダより80,000社以上の企業にエンタープライズクラスのセキュリティ製品とサービスを提供しています。ウォッチガードのミッションは、中堅・中小企業や分散型企業を含むすべての企業がエンタープライズレベルのセキュリティをシンプルに利用できるようにすることです。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジア太平洋地区、中南米に支社を展開しています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、数多くのパートナーを通じて、国内で拡大する多様なセキュリティニーズへのソリューションを提供しています。詳細は http://www.watchguard.co.jp をご覧下さい。

さらなる詳細情報、プロモーション活動、最新動向はTwitter（@WatchGuardJapan）、Facebook（@WatchGuard.jp）、をフォローして下さい。また、最新の脅威に関するリアルタイム情報やその対策法はSecplicityJPまでアクセスして下さい。
SecplicityJP： https://www.watchguard.co.jp/security-news

【本プレスリリースに関するお問合せ】
ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041
東京都港区麻布台1-11-9 BPRプレイス神谷町5階
マーケティング担当：角田・堀江
Tel： 03-5797-7205
Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： https://www.watchguard.co.jp
