ウォッチガード、拡大するセキュリティの盲点を払拭し、フィッシング攻撃の防御を行うDNSWatchGOを発表

調査ではリモートユーザの64%がサイバー攻撃の被害経験があり、新サービスではこうしたネットワーク境界外のセキュリティギャップを解消

2019年11月1日（金）
ー企業向け統合型セキュリティプラットフォーム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、「DNSWatchGO」のリリースを発表しました。DNSWatchGOはクラウドベースの新セキュリティサービスであり、ネットワーク境界の内と外の両方のユーザに対するフィッシング攻撃、C&C（コマンド＆コントロール）コールバック、および情報漏えいを検知・防御します。DNSWatchGOは、スタンドアローンあるいはウォッチガードの新たなユーザ向けセキュリティサービスバンドルである「Passport」を通じて利用可能となっており、DNSレベルのプロテクション（DNSファイアウォール）とコンテンツ（URL）フィルタリングを提供し、場所を問わずオフネットワーク環境でもユーザを保護します。また、自動化されたエンドユーザセキュリティアウェアネスと教育機能も提供しており、働き方改革を実現するための1つのソリューションとして、将来にわたるセキュリティインシデントの防止を支援するために設計されています。DNSWatchGOは、これら全ての機能をコストパフォーマンスの高い、容易な実装と管理が可能なシンプルなソリューションとして提供します。

最近CITE
Researchにより実施されたITアドミニストレータ、およびIT責任者を対象とした調査によると、現在リモートワークは急激に普及しており、回答者の92%が組織においてリモートワークを許可しているとの結果が出ています。しかしながら、オフネットワーク（ネットワークの外）で業務を行っている従業員が増加するにつれて、組織のセキュリティリスクは高まる一方となっています。事実、組織の90%が現在エンドポイントの脅威検知／レスポンスソリューションを導入しており、85%がオフネットワークの従業員の活動の監視に注力しているにもかかわらず、回答者の3分の2近くが、リモートワーカーがサイバー攻撃を受けたことがあると認めています。

ウォッチガードのプロダクトマネジメント担当シニアバイスプレジデントAndrew
Young（アンドリュー・ヤング）は、次のように述べています。「社外で業務を行う従業員が増えるにつれて、コアネットワークの外で仕掛けられる攻撃も増加しており、企業は新たな保護対策が必要になってきています。オフネットワークのトラフィックの監視、不正および好ましくないコンテンツへのアクセスフィルタリング、そしてユーザがVPNを使用していない状況での保護・対策が求められています。DNSWatchGOはこうした対策機能を提供するために構築されており、私たちの業界最先端の多層防御機能を、ネットワーク境界を越えてリモートワーカーを守るために活用し、同時にユーザに対するセキュリティのベストプラクティスに関する教育とトレーニングをプロセスの中に組込んでいます。」

DNSWatchGOのサービスは、中小／中堅組織およびこれらの組織をサポートするITソリューションプロバイダに対して、オフネットワークのセキュリティをシンプル化するために特化して設計されています。以下に主な機能と特長を紹介します。

場所を問わないプロテクション –
本ソリューションでは、ウォッチガードの既存のDNSWatchサービスにより提供されているDNSレベルのプロテクションとコンテンツフィルタリング機能を拡張しており、オフネットワークのユーザによるアウトバウンドDNSリクエストを不正ドメインの集約リストを元に監視・相関分析を実行します。エンドポイントの既知の不正インフラへの全ての接続の試みは防御され、ユーザはリダイレクトされ、トラフィックはDNSWatchサーバに転送されて詳細な調査およびマルウェアの除去が行われます。これらの機能により、オフネットワークのフィッシング攻撃、C&Cコールバック、情報漏えいを容易に防御することが可能になります。DNSWatchGOではまた、ロケーションを問わず、設定、調整、実行が容易なポリシーを用いて、ユーザが不適切なデスティネーションにアクセスすることも自動的に防止します。さらにMSPはサービスポートフォリオを拡張し、オフネットワークのエンドポイントに新たなセキュリティレイヤを提供することにより、顧客に付加価値を提供することができます。

迅速なセキュリティ教育
DNSWatchGOでは、ウォッチガード初となる自動化されたフィッシングプロテクションおよびエンドユーザへのリアルタイムでの教育を実現しており、組織のセキュリティ体制を劇的に改善することができます。プラットフォームによりフィッシングとして特定されたメールまたはリンクを従業員がクリックした場合、従業員はフィッシング攻撃に関する教育並びに防止対策のベストプラクティスを提供するコンテンツにすぐさまリダイレクトされます。さらに、防御された攻撃に関する明確な分析結果を提供し、ITアドミニストレータやMSPに送信され、コンテキストとして活用したり内部アクションに役立てたりすることができます。

CITE
Researchによると、従業員の49%は年間僅か2回もしくはそれ以下のセキュリティアウェアネストレーニングしか受けておらず、迅速な教育とトレーニングを受けることで、組織は将来的なオフネットワークで発生するセキュリティインシデントを最小限に止めることが可能になります。MSPにとってビルトインの分析機能および教育プロセスは、顧客にさらなる付加価値を提供し、アピールすることができます。

オフプレミスの可視化
DNSWatchGOは、ネットワーク内外の全てのデバイスを網羅する集約された可視化と高度なプロテクション機能により、一般的にリモートユーザがもたらすオフネットワークのセキュリティの盲点を払拭することができます。また、ITアドミニストレータやITソリューションプロバイダ向けに、ログデータを調べることなく、エンドポイントのロケーション、防御された攻撃のタイプ、および各攻撃の最終目的など豊富な実用情報を提供します。このようなレベルの可視化は特にMSPにとって貴重であり、プロテクションの証拠やオフネットワークのセキュリティインシデント、攻撃者、およびその手法に関する詳細レポートを提供できるようになります。

クラウドベースの管理
DNSWatchGOは100%クラウドベースのソリューションであり、実装と管理プロセスを合理化することで、企業やITソリューションプロバイダの時間とコストを節約することができます。ハードウェアや手動によるソフトウェアアップデートは不要であり、一元的なインターフェースを通じてネットワーク内外のユーザ向けにポリシーを管理・調整することができます。高価なハードウェアコンポーネントや時間を要する実装プロセスを排除することにより、特にMSPにとって大きな収

益の機会をもたらし、新規顧客への実装に際してすぐさま付加価値を提供することが可能になります。

DNSWatchGOは、ウォッチガードのユーザ向けの新セキュリティバンドル「Passport」を通じて利用することができます。ウォッチガードの多要素認証ソリューションAuthPointとDNSWatchGOサービスを組合せることにより、お求めやすい単一のバンドルライセンスでネットワーク境界の内外のユーザ向けに持続性を備えた常時稼動のプロテクション機能を提供します。
詳細はこちら（英語）
https://www.watchguard.com/wgrd-products/watchguard-passport

Verus Corporation社のプレジデント兼CEOのKevin Willette氏は次のようにコメントしています。「著名なITソリューションプロバイダとして、長年にわたり多くのベンダーと協業してきた中、製品のイノベーションは数多く見てきましたがチャネルのイノベーションはほとんど経験していません。チャネルは単にディスカウントやトレーニングプログラムを提供するだけでなく、製品やサービスをベンダーから調達し、クライアントに再販してライフタイムを通じて管理サービスを提供することにあります。ウォッチガードは、テクノロジーのイノベーションと同様に自社のエクスペリエンスの向上ももたらしてくれています。DNSWatchGOは、ユーザベースのセキュリティスタックにオフネットワークのコンテンツフィルタリングをもたらし、Passportは単一のSKUでウォッチガードのその他全てのユーザベースのセキュリティサービスをシンプルな方法で提供してくれます。」

CITE Researchのオフネットワークセキュリティレポートの完全版はこちらからダウンロードできます。
https://www.watchguard.com/wgrd-resource-center/ebook/state-prem-security-en（英語）

【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 https://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

WatchGuardは、WatchGuard Technologies, Inc.の登録商標です。その他の商標は各社に帰属します。

【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
Tel： 03-5797-7205 Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： https://www.watchguard.co.jp

Generated by ぷれりりプレスリリース
https://www.prerele.com