



誇大宣伝だけじゃない クラウドベースのウェブセキュリティ: 効果的なツール、登場

2010年6月

はじめに

ウェブの危険性が日に日に増していることは、特にニュースでもないだろう。ネット犯罪者達には有り余るほどの経済的動機、そしてユーザのデータを捕らえ不正使用するための簡単に使えるツールがいくらかでもあるからだ。

ニュースになる価値があるのはクラウドベースで、レピュテーションドリブン防衛の革新的で効果的なウェブセキュリティが、企業の価値ある資産をウェブベース攻撃から守れるようになったことだ。

上昇傾向にあるウェブ脅威

ウェブは驚くべき成長を遂げているが、それに伴い、これまでにない数の新種のマルウェアがウェブ・ブラウザやアプリケーション、Web 2.0インフラストラクチャなどを標的にしている。ネット犯罪では攻撃を仕掛けてユーザの個人情報やデータを盗み多大な利益を上げることができるため、組織的犯罪集団は、マルウェアの拡大や、ウェブユーザの個人データを獲得するための新たな手段に掛かる資金を絶え間なく出している。攻撃者はパッキング変更や暗号化技術、難読な方法などで、同じ脅威から何千種類もの亜種を比較的容易に作成することができるようになった。しかし、それにもかかわらず、大方の組織は収益や効率性を上げるため、カスタマーや利害関係者と新しい方法でインタラクションを取ることが可能なWeb 2.0の技術など、新しいウェブベース・アプリケーションを利用し続けているというのが現状だ。

組織は悪質な攻撃を受けることを過小評価しているケースが多く、2009年だけでも、新たに発見された新しい悪質なウェブリンク数は345%も上昇したなど¹、その統計には驚かされる。

¹ IBM X-Force 2009 Trend and Risk Report

そうしたリンクにはMSNBCやZDNet、さらには国連やホンダなどによって運営されているものも入っており、知名度の高いサイトまでがその対象になっているのである。

IDCによると、500名もしくはそれ以上の社員数を持つ企業の30%がネットサーフィンで感染したことがあるという。³つまり、ウェブユーザのインタラクションがあればマルウェアはどこにでもあるともいえる。スパイウェアやウイルス、クライムウェアやその他の悪質なコードなど、新たな形式のマルウェアを回避する方法は、組織がウェブセキュリティのインフラストラクチャをより保護することである。先を見越すことができ、脅威ランドスケープの変化に順応できるように、反応型そして固定化したセキュリティ・インフラストラクチャを変える必要がある。

正当なウェブサイトが感染してしまう方法はいくつもある。ネット犯罪の世界で最近人気上昇中のインバウンド脅威は、SQLインジェクションだ。ハッカーはSQLインジェクションを使ってデータベース・ドリブンのウェブサイト・アクセスを獲得し、そのサイトを訪れるユーザに使う悪質なコードを仕掛ける。Web 2.0ベースのソーシャル・エンジニアリング攻撃と組み合わせれば、ユーザに正当なコンテンツを閲覧しているものと思込ませることができる。侵入されたサイトは、ドライブ・バイ・ダウンロードをホストしている可能性もあり、そうした場合マルウェアは、ユーザのシステムにある脆弱性を悪用し、ユーザのインタラクションなしにマルウェアをダウンロードできるようになる。Apple QuickTime®やAdobe PDF®など、一般的に使われているアプリケーションが悪用される場合もあるため、組織内で使用しているアプリケーションの脆弱性やウェブサイトのコード欠陥は、その組織のネットワークに侵入しようとするネット犯罪に向けてドアを開いてしまうことになる。

セキュリティとパフォーマンスにはバランスが必要

ITセキュリティ・プロフェッショナルであれば、ウェブセキュリティにおける管理面とネットワークユーザからの要求の間で頭を悩ませることはよくあるだろう。常にスピードの必要性を求められ、それを提供しながら、より拡大させたダイナミックな脅威環境でセキュリティを強化させるのは難しいことだ。そうした目標を達成させる場合に、よくつまづく点として次のようなものがある：

- ・ ネットワークセキュリティ強化に必要なIT追加予算の欠如
- ・ クラウドコンピューティングにまつわるセキュリティ問題と、それに対立するネットワーク制約
- ・ 追加ホストサービスによるネットワーク全体でのパフォーマンスの悪化

しかし、こうしたチャレンジを乗り越え、先を見越すことができるマルチレイヤのセキュリティにするためのオプションは、魅力のないものか不適當なものしかない。例えば、広範囲に渡り急増しているマルウェアに対抗する方法として、ウイルス対策をインストールしてゲートウェイでスキャンをし、ネットワークに入り込む前にマルウェアを捕らえる方法がある。しかし、そのURLのページやオブジェクトをすべてスキャンすると、ウェブページを閲覧するまでの時間が掛かり、デバイスのスループットやブラウザ側のユーザ・エクスペリエンスにも影響が出る。そうしたパフォーマンスへの影響から、ゲートウェイ・ウイルス対策を使うのは気が進まないというネットワーク管理者もいるだろう。

また、デスクトップやブラウザベースのスキャン・ソリューションは、ネットワークに入り込んだ脅威しかキャッチすることができない。つまり、それがユーザに警告する頃には、現在のレベルのマルウェアであれば、すでに多大な被害を組織のコンピューティング・インフラストラクチャに及ぼしているか、組織内の機密データに手をつけていることだろう。

充分とは言えないURLフィルタリング

1990年頃から、レピュテーションサービスは不必要なトラフィックや悪質なトラフィックを遮断し、ネットワークに脅威が入り込まないように支援している。境界線で脅威を識別したり遮断することで、レピュテーションサービスは攻撃を防いだり、トラフィックをスキャンするために必要なオンプレミスのITフットプリントを削減したり、バンド幅関連のコストやハードウェア、その他の脅威を阻止するために掛かる必要なリソースのコストを軽減できる。ウェブ技術やウェブ自体がより高度なものになっていくに連れ、脅威を識別し阻止する面において初期のレピュテーションサービス効果は低下している。しかし、その有効性の欠如をしっかりと把握するには、こうしたサービスがいかに進化したのかを理解する必要があるだろう。

² Gartner IT Security Conference 2009, *Securing the Web Gateway*, Peter Firstbrook

³ Journal Of Emerging Technologies In Web Intelligence, Vol. 2, No. 2, May 2010, *Protecting Data from the Cyber Theft – A Virulent Disease*

ダイナミックウェブにおいて、サイトは常に新しいコンテンツをもって更新され、URLは頻りに売られたり変更されたりしているため、今現在、URLフィルターでスキャンされ、正当なサイトとして分類されたサイトでも、後にマルウェアの拠点地となってしまうこともある。有害で危険なウェブサイトを適切にフィルターするには、変化のないデータベースだけに頼っては行けない。IDCのレポートによるとWeb 2.0テクノロジーは、これまでのURLフィルタリング以上の新世代ウェブセキュリティ・ツールを必要としている⁴という。ツールはウェブのようにダイナミックであり、リアルタイムで脅威保護を提供できなければならない。さらに、著しい成長を遂げているインターネットのスケールにも対応する必要がある。

効果的なセキュリティは先を見越すマルチレイヤ

ウェブのダイナミックな脅威に対抗するためのもっとも効果的な方法は、先を見越せること、そしてマルチレイヤの方法をウェブセキュリティに取り入れることである。

先を読めるようになるには、まずセキュリティ・ソリューションがインターネット・クラウドにリーチし、最新の脅威データをマルチ脅威監視の情報源から獲得、そして、そうした脅威がネットワークにやってきた場合のために、ネットワークの境界線の準備をしておくことだ。このため、ネットワークに侵入しようとするコンテンツによって脅威をスキャンできる追加対策を取り入れるマルチレイヤは、効果的な防衛手段といえるだろう。

WatchGuard® Reputation Enabled Defenseは、効果的で瞬時的そして掘り下げたセキュリティをリアルタイムで提供することができる。クラウドセキュリティからのWatchGuard Reputation Authority®をベースにしたReputation Enabled Defenseは、何百万ものグローバル・ソースやユーザのクラウドベースのインテリジェンスを利用し、URLやドメインに関連する脅威情報をリアルタイムでシェアし、新たな脅威が組織のネットワークに侵入する前に自動的に遮断することができる。

WatchGuard Reputation Enabled Defenseは、ウェブトラフィックのリアルタイム監視を含んでおりネットワークで許可される前に、各ウェブページのリスクレベルを決められるURLスキャン機能もある。このソリューションは、各脅威とネットワーク・トラフィックのタイプを査定する。接続レベルで悪質なコンテンツをスキャンしたり、悪質なURLをネットワークから遮断することで、Reputation Enabled DefenseはシンプルなURLフィルタリングだけでは手の届かないウェブセキュリティのギャップを埋め、より安全なネットサーフィンと、さらに速度を上げたウェブ・パフォーマンスを提供することができる。

ウェブセキュリティ・ナンバー

ウェブセキュリティにおいて、常に変化している脅威タイプを管理するにはITセキュリティプロが先を見通せる方法が必要であることは、最近の数字を見ればわかる。

- ・ 2008年から2009年において、毎週40,000のウェブサイトが障害を受けた。
- ・ Gumbler ウィルスだけでも60,000のウェブサイトに障害を与えた。⁶
- ・ 2009年には23,500の新しいウェブページが毎日感染された。⁷
- ・ グーグル検索結果の0.7%がマルウェアに感染したサイトを表示している。⁸
- ・ Mal/Bredoマルウェアには2010年第一四半期の間だけで838の亜種があった。⁹

⁴ IDC, Worldwide Web Security 2009-1013 Forecast and 2008 Marketshares: It's All About Web 2.0 You TwitFace, August 2009

⁵ Google Online Security Blog, *Malware Statistics Update*, August 25, 2009

⁶ Google Online Security Blog, *Top 10 Malware Sites*, June 3, 2009

⁷ Sophos, *Sophos Security Threat Report*, July 2009

⁸ Google Online Security Blog, *Malware Statistics Update*, August 25, 2009

⁹ Commtouch, *Well-known Web Names Misused to Give Spam Deceptive Legitimacy, According to New Report by Commtouch*, April 14, 2010

レピュテーションサービスに求めるもの

レピュテーションサービスは、パフォーマンスの改善や保護レイヤを追加することでゲートウェイ・ウィルス対策や、従来のデスクトップ・ソリューションを補足し合うことができる。通常、毎時間または毎日ベースでシグネチャをアップデートするゲートウェイ・ウィルス対策ソリューションとは異なり、レピュテーションサービスは、マルウェア・インテリジェンスのアップデートをリアルタイムと同等でアップデートすることができる。より幅広く改善されたURLレピュテーション・データは、ウェブ脅威に対する保護力を高め、これまで以上に成果の高いネットサーフィンを可能にすることができる。しかし、レピュテーションサービスすべてが同じように機能するのではないため、ITセキュリティプロが見込みのあるソリューションを評価する際には注意が必要である。

レピュテーションサービスの多くは、マルウェアやフィッシング詐欺で知られたウェブサイトにはユーザが行かないようにするプラグインとして実施されている。それに比べ、WatchGuardはレピュテーションサービスに貢献制を取り入れることで、次世代レピュテーションサービスの提供を可能にしている。WatchGuardのレピュテーションや接続管理の方法は、進化する脅威に対し、本当に効果的に、そして先を見越してそれらを阻止できるようにする。現在市場に出回っている大方のレピュテーションサービスのように、固定したデータベースの単なる監視システムとして機能するだけではなく、真のゼロアワー、そして防衛の最前線でなければならないという信念を反映させているのがWatchGuardのレピュテーションサービスだ。先を見通す適応同定のためにWatchGuardはウェブ脅威を接続レベルで管理し、掘り下げた分析をゲートウェイ・レイヤでも行っている。そして、ゲートウェイで収集した情報をリアルタイムでレピュテーションサービスに提供し、何百万ものグローバルユーザやソースのインテリジェンスを役立て、悪質なURLやウェブ脅威に対し、より強力でインテリジェントな保護力を使えるようにしている。

WatchGuard Reputation Enabled Defenseのユーザは、その時点で評価の高いウィルス対策やURLスキャン機能を迂回するように選択することもできるため、時間を節約しパフォーマンス・レベルを維持することができる。

WatchGuard Reputation Enabled Defense

WatchGuard Reputation Enabled Defenseは、WatchGuardのマルチ機能ファイアウォール製品シリーズ、統合脅威管理(XTM)およびXCSエクステンシブル・コンテンツ・セキュリティ製品にウェブセキュリティ・サブスクリプションを追加することで利用できる。クラウドベースのレピュテーション・ルックアップを提供し、安全または悪質なURLを識別することができ、世界中の何百万人というユーザからのスロットインテリジェンスを利用することでReputation Enabled Defenseは、ウェブ脅威に対し強力な防御の最前線の役割を担う追加保護レイヤを提供できる。脅威がネットワークに入り込む前に先手を打って阻止することで、Reputation Enabled Defenseはゲートウェイでの費用の掛かるオンボックス・スキャンや、ウィルス対策スキャンによるコンピューティング・オーバーヘッドの負担の削減にも役立つ。許可したコンテンツを送り出すスピードにおいても効果を出せる。要するに、WatchGuardはウェブセキュリティをボックスやネットワーク以上のレベルに引き上げ、できる限りクラウド内で管理しているのである。

Reputation Enabled Defense の機能

クラウド支援ベースのサービス、Reputation Enabled Defenseは、絶え間なくアップデートされる瞬時的なセキュリティを提供することができる。積極的にセキュリティを改善できるほかに、組織はクラウドでホストされているサーバから、よりよいコンピューティングやプロセッサパワーの利点も得られる。ITはローカル・アプライアンスの貴重なプロセッサ資源を節約できるため、より多くのユーザが高度なスループットで、そしてコストを削減しながら利用することが可能になるのである。

図1はReputation Enabled Defenseがどのようにウェブセキュリティを強化しているのかを示している。サービスの中心は業界のもっとも広範なデータベース、そしてオンアプライアンス・クエリ・システムであるクラウドベースのレピュテーション・スコアリング・データベースだ。

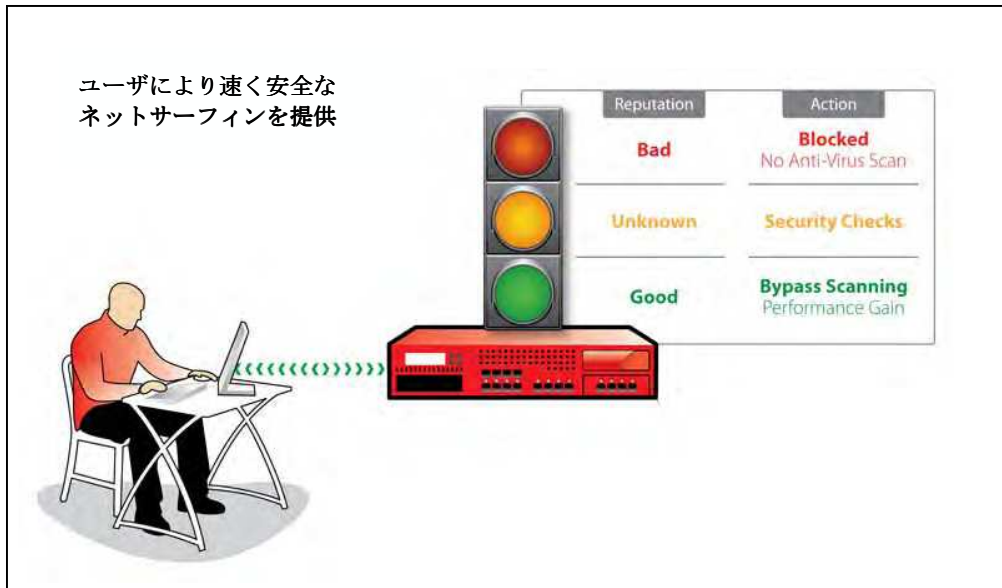


図 1: Reputation Enabled Defenseはパワフルなクラウドベース・データベースを使い、悪性トラフィックを除外しながら安全なトラフィックを許可する。AVスキャンの対象となるのは不明なトラフィックのみであるため、ウェブの処理時間においては相当な利益となる。

ウェブユーザーがURLに行くと、WatchGuardのアプライアンスはそのURLのレピュテーション・スコアのローカルキャッシュをチェックする。ローカルキャッシュで見つからない場合は、そのレピュテーション・スコア情報を得るため、クラウドベースのReputation Authorityサーバにクエリを出す。評価が高ければ、アプライアンスはそのURLを承認し、ローカル・ウィルス対策スキャンを迂回して、ページが早くレンダリングしコンテンツを表示できるようにする。

URLの評価が低かった場合は(例えば悪質なウェブ脅威を含んでいるなど)、WatchGuardアプライアンスはURLを即座に阻止し、至急、悪質なコンテンツからユーザーを保護してローカル・ウィルス対策スキャンも迂回させる。URLのスコアの良し悪しが明確でない場合やスコアがない場合、アプライアンスは「routine defense-in-depth」セキュリティチェックを行い、そのチェックにもとづいてURLを承認または阻止するようになっている。

どの組織においても、そのウェブの利用方法は異なることを理解しているからこそ、WatchGuardはReputation Enabled Defenseの設定をユーザーができるようにしている。最近の脅威は、前回のスキャンから何秒もしないうちに安全なウェブサイトが侵入される可能性をもたらすため、評価の高いURLのスキャンを迂回する機能を使わないように選択できるオプションも用意している。

節約効果がある真のサービス

WatchGuardはReputation Enabled Defenseが可能な限り強力で、資源使用を最小限に抑えたセキュリティをユーザーに届けることを保証している。そして、いくつものフィードや集合データを通じてURLレピュテーション・データベースの拡大を管理し、今後もそのプロセスを絶え間なく行いユーザーが自己環境で導入したものよりも遥かにレベルの高いインテリジェンスとセキュリティによる利益をユーザーに提供する。

Reputation Enabled Defenseは、通常30%から50%のURLがウイルス対策スキャンを迂回することを許可し、ネットサーフィンの速度やマルチ機能ファイアウォールでのスループットを向上させることができる。URL評価が常に高く、レピュテーション・データベースに常に入っているURLは、ウイルス対策スキャンを迂回した場合でもリスクは低い。このため、そのようなサイトをユーザが訪れる場合、セキュリティを犠牲にせずにパフォーマンスを最大限に伸ばすことができるのである。

レピュテーション対策の利点

WatchGuard Reputation Enabled Defenseは、クラウドで先を見越すことができるセキュリティ対策から幅広いセキュリティとパフォーマンスの利点を提供することができる。以下は、ITやネットワーク管理者にとってもっとも特徴的な利点だ。

セキュリティ

- URLベースのマルウェアを効果的にキャッチする確率を高めることで、**組織が貴重なデータを保護できる。**
- 危険なURLがネットワーク・アクセスを得る前にマルチレベルの自動保護機能を通過しなければならぬということを知っていることで、**管理者は安心を感じることができる。**
- クラウドベース・セキュリティを通じ、ネットワークのセキュリティスタンスには**WatchGuardの幅広いユーザコミュニティのフルパワーと知識がある。**
- 管理者はスキャンの結果を監視したりシステム設定を変更することで、**セキュリティとパフォーマンスの理想的なバランスをとることができる。**

パフォーマンス

- 管理者はURLスキャンを最小限に抑え、ゲートウェイでのスループットを高めることにより、**高度なパフォーマンスをビジネスにもたらし、ユーザの満足度を高めることができる。**
- 有害なウェブサイトを接続レベルで拒否することにより、管理者は**バンド幅の使用や処理サイクルを減少させることができる。**
- WatchGuardのテクノロジーは、どのURLが人気か知ることができるので、**頻繁に現れるURLはReputation Authorityデータベースで定期的にアップデートされるようになっている。**

先を見越してマルウェアに対抗する

マルウェアはウェブで蔓延し続けている。拡大する脅威の量や、新しい脅威そして変化し続ける脅威の亜種は、ある組織のITスタッフが監視し保護対策をするだけでは足りない状態になっている。そうした理由から、WatchGuardは先を見越せるクラウドベース・セキュリティの方法を改善したり、セキュリティとパフォーマンスのバランスを維持しなければならない点を考慮するなどして、より高いレベルを常に求めている。

WatchGuard Reputation Enabled Defenseは、ユーザ・エクスペリエンスやネットワーク・パフォーマンスを犠牲にすることなく組織が積極的にマルウェア脅威に対抗できるようにする。現に、ゲートウェイでURLレピュテーションソリューションを提供しているUTM/マルチ機能ファイアウォールのベンダはWatchGuardのみである。

Reputation Enabled Defense を使ってネットワークを保護しているWatchGuardのカスタマーは、素晴らしいマルウェア対策技術の利点をいくつも得ることができるため、マルウェア対策の情報源だけに頼っているシステムよりも遥かに充実したサービスを受けることができる。クラウドベース・サービスは、新にリアルタイムで発見された脅威からダイナミックにユーザを保護することができるので、Reputation Enabled Defenseの利点は利用者全員に向けられたものとなる。

ユーザはこのサービスに投資することで、飛躍のレベルの保護を楽しむことができる。ネット犯罪は今現在も活発に動いている。先手を打つには今こそがよいチャンスだろう。

詳細情報

Reputation Enabled DefenseやWatchGuard XTMセキュリティソリューションに関する詳細については、ご利用のWatchGuard認定リセラーにお問い合わせください。また、弊社ウェブサイトwww.watchguard.com/redまたは直接お電話からも受け付けております。+1.800.734.9905（北米）または +1.206.613.0895（インターナショナル）。

ご注意: Reputation Enabled DefenseはWatchGuard XTM 2, 5, 8, 10シリーズの統合脅威管理アプライアンスの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。

WatchGuard XCSアプライアンスにおいて、URL reputation enabled defenseはXCS Web Securityサブスクリプションをお買い上げいただき有効にされた場合にご利用可能となっております。WatchGuard XCSアプライアンスには、すべてIP reputation-enabled defense for enterprise-class email securityのReputation Authorityが含まれています。

住所:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

北米営業部:

+1.800.734.9905

インターナショナル:

+1.206.613.0895

WATCHGUARDについて

ウォッチガード・テクノロジー社は、1996年から信頼性が高く、管理しやすいセキュリティソリューションを世界中の何百、何千もの企業に提供しています。WatchGuardの受賞経験のあるエクステンシブル・スロット・マネージメント(XTM)ネットワーク・セキュリティソリューションは、ファイアウォールやVPN、セキュリティ・サービスを組み合わせたものです。エクステンシブル・コンテンツ・セキュリティ(XCS)アプライアンスは、メールやウェブ、データ紛失防止においてもコンテンツ・セキュリティを提供します。WatchGuardを代理しているパートナーは120か国に渡り15,000社以上あります。WatchGuard本社は米国ワシントン州、シアトルに所在し、北米、南米、ヨーロッパ、アジアパシフィックにもオフィスを構えています。詳細につきましてはwww.watchguard.comをご覧ください。

同資料における表現に保証はありません。全仕様書は変更される可能性があり、今後の製品や機能などの利用状況については弊社の意向にもとづき提供します。©2010 WatchGuard Technologies, Inc. 無断複写・転載を禁じます。WatchGuard、WatchGuardロゴ、WatchGuard Reputation Authorityはいずれも米国およびその他の国々においてWatchGuard Technologies, Inc.の登録商標あるいは商標です。その他すべての登録商標および商標は各所有者に権利があります。

Part.No. WGCE66705_06

