インテリジェントなホワイトリスティング

さらに効果的で効率的なエンドポイントセキュリティのご紹介

マルウェアは件数が急増しているだけでなく、その技術も高度化しているため、従来のアンチウイルス対策では対応が難しくなっています。これまで、マルウェアの件数増加と高度化に対応するためのアプローチは、基本的な管理モデルを変更することなく、エンドポイント環境での変更を入念に検査するためのさらに優れたアンチウイルス対策を講じることでした。結果的に、保護は効果的でなく、性能がお粗末な過剰なアンチマルウェア技術につながっています。これにより、IT リソースへの負担が増加するためエンドポイントの総所有コストが増え、エンドユーザーの生産性が低下し、すでに少ないもしくは削減された IT 予算にさらなる圧力がかかります。

エンドポイントを保護する方法について考え直す時期を迎えています。

一般的にセキュリティの専門家は、エンドポイントの管理を白か黒かの選択肢として考える傾向にあります。ここで白とは、ユーザーの生産性を妨げる傾向にある第 1 世代のホワイトリストテクノロジー、黒とは、現代の脅威の対応に苦戦しているシグネチャベースのアンチウイルステクノロジーを意味します。もう一度考え直してみてください。

アプリケーションのホワイトリスティングに対する新しい「インテリジェント」なアプローチは、この両方の方法を活用し、さらにその間にあるグレーリストに該当するものを信頼しネットワークへのインストールが許可されるべきかの判断を自動化する方法を追加します。

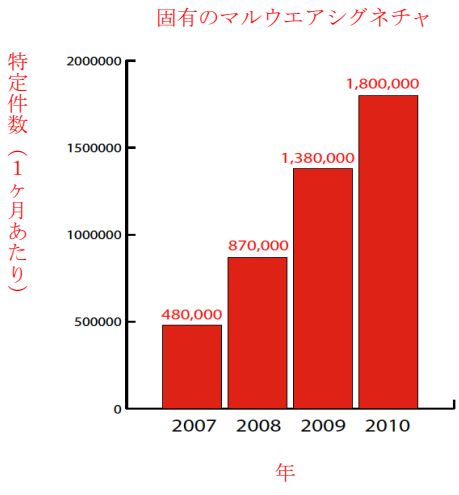
インテリジェントなホワイトリスティングは、シグネチャベースの行動分析とホワイトリスト機能の効果を統合し、さらに許可する変更を管理する「信頼のエンジン」を追加する一元化されたワークフローを提供します。これにより、信頼されたアプリケーションをホワイトリストに追加するプロセスが円滑化かつ自動化されます。インテリジェントなホワイトリスティングは、パッチ管理など他のエンドポイントセキュリティからのデータを使用して「提供元を把握していますか？」や「他の人はこれを使用していますか？」など、アプリケーションに対する重要な質問を自動化し、希望の管理レベルとセキュリティレベルに調整します。インテリジェントなホワイトリスティングは、生産性に影響を与えることなくマルウェアの感染率を劇的に軽減するだけでなく、エンドポイントを維持するための TCO（総所有コスト）の削減も可能にします。

新しいアプローチの必要性

会社の財政を管理している経営陣は、セキュリティの効果が落ちている一方でエンドポイントの TCO（総所有コスト）が増加しているという悲しい事実を認識しています。マルウェアの蔓延は加速していますが、経営幹部は IT 部門にセキュリティにかかるコストを抑えることを要求しています。IT の専門家に「一度立ち止まって自社のエンドポイントを保護するための戦略について考え直そう」と思わせる明確な理由が現時点で 3 つあります。

I. マルウェアの件数の急増＆マルウェアの技術の高度化

2007 年から 2010 年に間に、セキュリティの研究者が新しいアンチウイルスシグネチャが必要だと判断した脅威の件数は 1 ヶ月あたり約 480,000 件から 1 ヶ月あたり約 1,800,000 件に増加しました（以下のグラフを参照）。また、件数が急増しているだけでなく、攻撃の技術も高度化しています。現代のマルウェアの多くが金銭目当ての犯罪組織によって設計されています。このような犯罪組織は、アンチウイルス防御を潜り抜け、特定の企業を標的とする悪意のあるコードを開発しています。



II.従来のアプローチの限界

新しいマルウェア発見時の、アンチウイルスソフトウェアによる新しいマルウェアの検出率は平均わずか 19%で、発見から 30 日後の検出率もたった%です(2)。 従来のアンチウイルスは、現代とはまったく異なる時代、すなわちマルウェアの種類が制限されていた時代に十分に発達してしまったのです。シグネチャベースのアンチウイルスのベンダーは、マルウェアの急増について行けず、無駄になっています。膨大なシグネチャがエンドポイントのパフォーマンスを低下させているだけでなく、従来のアンチウイルスのベンダーも新しい高度なマルウェアの新種の急増について行くことが出来なくなっているのです。このため、多くのマルウェアが見過ごされてしまっているのです。

III.予算の縛り &エンドポイントの TCO の増加

CIO や CFO は、直近の IT への支出を控えています。ガートナーは、2011 年まで企業が自社の IT の総予算の 3%～6%までセキュリティへの支出を削減すると予測しています(3)。これは現状のエンドポイントセキュリティから抜け出せずにいる企業にとっては厄介な事態です。現行のアンチウイルスモデルにより、エンドポイントを感染のない状態に維持することは IT 部門にとってますますコストのかかる業務になっています。事実、一般的な企業からは、生産性に影響を及ぼすマルウェアインシデントの件数は 1 ヶ月あたり 50 件を超えると報告されており(4)、これは IT のヘルプデスク、インシデント対応、修復費用の増加につながっています。

アプリケーションホワイトリスティングとアプリケーション管理：この 2 つの違いとは？

アプリケーションホワイトリスティングとアプリケーション管理の違いについて少し混乱しているとしても心配はありません。この 2 つの言葉を別々の言葉として扱うほどこの 2 つの間に大した違いはないのが事実です。両方とも同じプロセスを指しています。ただし、アプリケーションのファイアウォールのベンダーがホワイトリストとは異なる自社の製品基盤を「アプリケーション管理」という言葉を使用していることもあるため、他の意味にも解釈できるため、当社は「アプリケーションホワイトリスティング」という言葉を一貫して使用しています。

インテリジェントなホワイトリスティングへの移行

純粋に、アプリケーションホワイトリスティングは従来のアンチウイルス対策を覆しています。ソフトウェアの疑わしい部分を突いて、考えられるあらゆる点において問題がないかを見極める代わりに、アプリケーションのホワイトリストは基本的な質問—このコードを信頼する理由はありますか—を問いかけます。基本的にホワイトリスティングソリューションは、アプリケーションがソフトウェアの有効なピースであることを確認することを目的としています。確認できるまで、アプリケーションをエンドポイントで実行することはできません。ホワイトリストが誕生した当初、最も単純な展開では、アプリケーションとコードの実行がすべて「確認済みの既知の問題のないコードのリスト」に制限されていました。これは、ミッションクリティカルなサーバーにマルウェアを近付けない極めて確実な方法でした。これが進化し、POS 端末を使うリテール環境やコールセンター環境など「ロックダウンされた」エンドポイントのセキュリティレイヤーになりました。

ところが、現在企業はこれよりもはるかに複雑で動的な環境で運営されています。オープンソースツールや Web アプリケーション、自社製のコード、市販されているプログラムなど、多くのアプリケーションがダウンロードされ、業務を履行するために使用されて。また、これらのアプリケーションにより、すべてエンドポイいますントの設定がそのエンドポイントの社員向けに変更されています。さらに、リモートワーカーやモバイルワーカーが存在し、アプリケーションをクラウドに拡張することを望む声が高まっています。IT 部門とエンドユーザーの両方にとってさらに柔軟なホワイトリストのポリシーが求められているのは明白です。この種の環境を円滑化するため、ホワイトリストは社員が生産性を向上する新しいツールを安全に活用することを可能にする十分な順応性のあるポリシー施行を実現できなければなりません。

幸いなことに、先見の明のあるベンダーはこれらの問題を考慮し、さらに強化されたセキュリティを提供し、動的な環境に対して十分な柔軟性を持つスマートなホワイトリスティングソリューションを開発しています。変更が許可される前に集約化されたホワイトリストを常に管理するのではなく、インテリジェントなホワイトリスティングのユーザーは、リスク選好と管理許容差に合わせて微調整される自動化された信頼のルールを定義します。これは、ソフトウェアパブリッシャーの評判やソフトウェアの更新プログラムや新しいコンテンツをインストールするツールの評判など、共通の指標を使用して既知の問題のないソフトウェアの確認を自動化することで、常に IT 部門が介入する必要性をなくします。

信頼の管理

信頼。それは極めて単純な概念に思えます。何かをエンドポイントで実行することを信頼するか、しないか。ただそれだけのことのように思えますが、現実はそんなに単純ではなく、はるかに複雑であることは周知の事実です。例えば、自社環境で実行中の P2P アプリケーションを見つけたと仮定します。このファイルは破損しておらず、広く使用されているプログラムですが、自社のネットワークで使用し続けたいアプリケーションでしょうか？極めて機密な情報を扱っている企業であれば、P2P アプリケーションはおそらく適切なアプリケーションではないでしょう。一方、定期的に zip ファイルを添付したメールのやりとりを行う広告会社であれば、おそらく P2P アプリケーションはさして問題視するほどのものではないでしょう。結局のところ、自社のセキュリティのニーズを見極める責任は企業自体にあるべきなのです。企業が責任を持つことにより、技術で制限される代わりに企業は自社で判断を下すことができます。

確実にエンドポイントの保護を強化するため、当社のインテリジェントなアプリケーションホワイトリスティングソリューションには以下の機能が装備されています。

信頼のエンジン

企業のホワイトリスティングソリューションは、自社で設定した信頼のルールに基づいてエンドポイントの変更を確認し、状況に応じてホワイトリストを自動更新できなければなりません。これらの信頼のルールには以下の項目に基づく確認を可能にする柔軟性が必要となります。

- ソフトウェアのパブリッシャー（デジタル証明やその他のメタデータを使用しての確認）
- 新しいまたは更新されたソフトウェアをインストールする更新プログラム
- パスまたは集約化された場所（頻繁に変更される社内で開発された、もしくは無署名の実行可能ファイルがブロックされていないことを確認するため）
- 予期せぬ変更が必要になる機会の多い特定の信頼できるユーザーのローカル権限

スナップショット

スナップショット機能により、すべての実行可能ファイルのローカルホワイトリストを作成できます。ローカルホワイトリストを作成することにより、エンドポイント環境へのさらなる望ましくない変更を防止でき、企業全体を押し込む全社規模の「完璧な」ゴールデンイメージの必要性を排除できます。さらにスナップショット機能は、ホワイトリストの展開にかかる時間を大幅に短縮し、一ヶ所で可視性、グループ化、ポリシー評価を実現するため、全社規模で独自のホワイトリストを展開することを可能にします。

「ローカル管理者」ユーザーの管理

多くの企業において、各自が自分の仕事を履行するためアプリケーションの更新プログラムをインストールして実行する柔軟性を確保することを目的に、エンドユーザーには管理者権限が付与されています。エンドユーザー管理に対するこのアプローチは混乱を招き、エンドポイントの設定がまったく管理されていない状態につながっています。これによりシステムは攻撃にかなり脆弱な状態になります。

一方、インテリジェントなホワイトリスティングは、ユーザーにローカル管理者の役割を付与したまま、ユーザーが実行できる変更の種類や、設定の変更に影響するローカルシステムコンソールへのアクセス権の範囲を制限することを可能にします。結果、エンドポイントのセキュリティ設定と状況について把握、管理しつつ、エンドユーザーの生産性を向上できます。

エンドポイント管理の全体的なワークフローへの適合性

アプリケーションのホワイトリスティングは、他のエンドポイントセキュリティや管理ツールなど全体的なフレームワークの中に難なく組み込むことができる場合のみインテリジェントなツールとなります。これまで異なるツールにサイロ化されていた情報を統合し、情報源や普及率に目を向けることで、エンドポイントの保護を大幅に強化できます。アンチウイルスツール単独での効果は失われていますが、ツール内で生成、保存されている情報がアプリケーションホワイトリスティングと連動していれば、アンチウイルスツールはこれまで通り価値のあるツールとして機能します。同様に、ホワイトリスティングツール内に保存されている情報をパッチ管理や信頼されている変更ポリシーとスムーズに統合できれば、企業のセキュリティ体制を強化できるだけでなく、エンドポイントの TCO（総所有コスト）も削減できます。

信頼に基づくポリシーの作成：

インテリジェントなホワイトリスティングソリューションは、次の質問に回答する上で役立ちます。

- これは既知の問題のあるファイルか？
- これは既知の問題のないファイルか？
- これは望ましくないファイルか？
- これは許可されているファイルか？
- これは適切にライセンスが付与されているファイルか？
- ベンダーを信頼しているか？
- インストールするプログラムを信頼しているか？
- 提供元を信頼しているか？
- インストールするこのユーザーを信頼しているか？

問題は白黒はっきりさせることではない

アプリケーションをホワイトリスティングするかどうかは、もはや「いずれか」を選択することではなくなっています。選択肢はアンチウイルスか、それともホワイトリストかではなくなっています。Bloor Research のアナリスト、ナイジェル・スタンリーはこの状況を次のように表現しています。「個人的にホワイトリストとブラックリストの問題は、一見白黒はっきりし過ぎていることだと思います！もちろん、簡単に問題があると判断し、ブラックリスト化できるコードはたくさんあります。同様に、例えば大手ソフトウェアサプライヤーからダウンロードしたファイルなど、簡単にホワイトリスティングできるコードもあります。そしてその一方で、私は信頼できるベンダーからダウンロードした「グッドウェア」に見えるけれど、アプリケーションの互換性の問題で瞬く間に IT 資産を台無しにしてしまうコードも知っています。ホワイトリストとブラックリストの間には、一部のヒューリスティックな分析の対象となるグレーリストに分類されるコードがあるため、ホワイトリストとブラックリストの融合は、おそらく避けられないでしょう」[5]

同様に、企業は環境がどの程度静的か動的かに基づいてホワイトリストを使用するかどうかを決める必要がなくなっています。その代わりとして企業に求められているのは、柔軟性とセキュリティのバランスをとるためにどんなポリシーを使用するかを判断することです。極めて安全で静的な環境では、

純粋なホワイトリストポリシーを使用してください。動的なエンドポイント環境では、ユーザーを信頼できるかもしれませんが、提案された変更が信頼でき許可されていることを確認する必要があります。企業のネットワークでは、おそらくホワイトリストで特定できない新しいコードがシステム管理ツールによって取り込まれる場合があります。

いずれにしても、賢明な企業は、マルウェアのクリーンアップと自動化されたパッチ管理に加え、アプリケーションの展開を管理する多層防御のアプローチに向けて取り組む必要があります。これにより、マシンが安全に設定されていることに加え、ホワイトリストが適切かつ継続的に更新されることが保証されます。この融合型の信頼を中心にしたアプローチは、エンドポイントを保護するための現行のアプローチよりも柔軟かつ安全です。このインテリジェントなホワイトリスティングのアプローチによって、得られるメリットは以下の通りです。

- セキュリティの強化
- コストの削減
- エンドポイント管理の強化
- 生産性の向上

エンドポイントを保護するためのこの信頼できる変更のアプローチにより、使いやすさとセキュリティのバランスを取ることができ、IT 管理者への負担を増やすことなくエンドユーザーの生産性を向上できます。そして現代の IT 環境において、それは望ましいことです。

http://www.ivanti.co.jp/

03-5226-5960

Contact-Japan@ivanti.com

1.Extrapolated from: McAfee Labs, McAfee Threats-Report: Third Quarter 2010, November 2010

2.Cyveillance, Malware Detection Rates for Leading AV Solutions, August 2010

3.Gartner, Vic Wheatman, Research Director, June 2010

4.Ponemon Institute, State of Endpoint Risk 2011, November 2010

5 Nigel Stanley in Lumension blog, Winning the Malware Battle: The Move Towards Whitelisting, December 2009