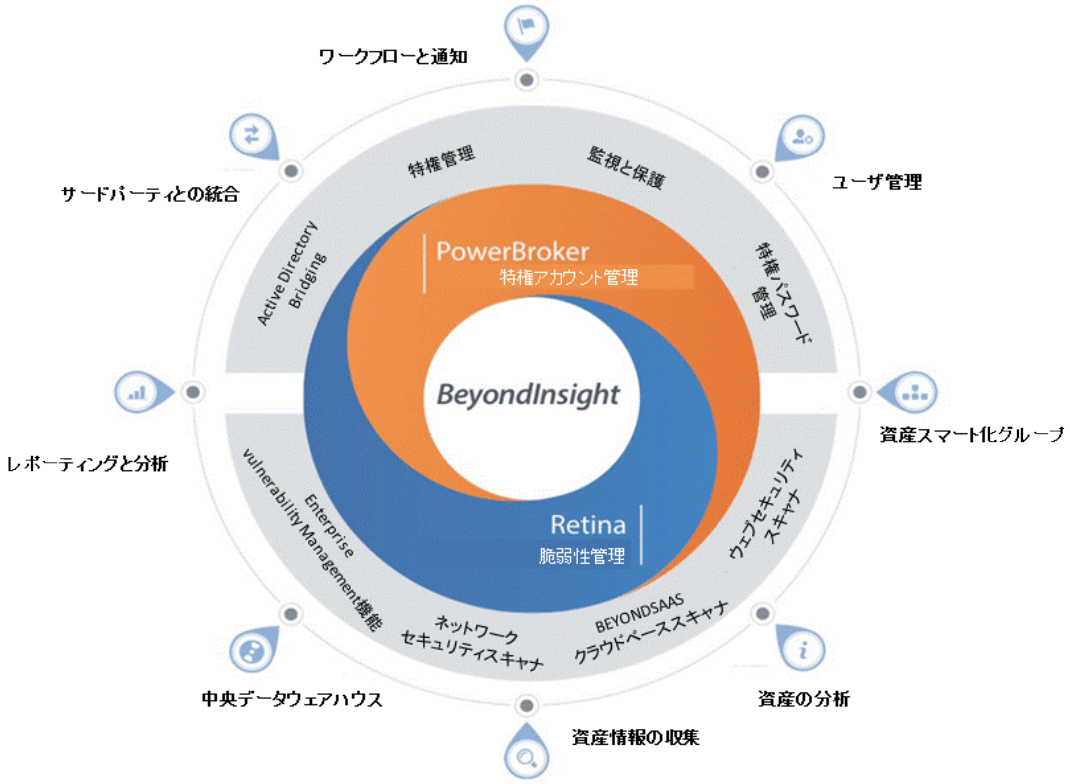
アプリケーション制御： PowerBroker for Windows Difference

2014 年 10 月 22 日

beyondtrust®
Beyond Traditional Security

目　次



はじめに

アプリケーション制御ソリューションは、ホワイトリスト化やブラックリスト化、そして最近では「グレイリスト化」という手法を使って、許可されていないアプリケーションの実行を防ぐように設計されています。これを使って、企業のサーバやワークステーション、ラップトップ、固定機能デバイスなどを保護することができます。また、ポリシの強制や動的信頼モデリングを使って、APT(高度な標的型攻撃)を防ぐこともできます。さらに、通常は手間のかかるシグネチャの更新やグレイリスト用アプリケーションのためのリスト管理を必要としません。

アプリケーション制御ソリューションには、以下のようなセキュリティ上およびコスト上の利点がいくつかあります。

- **望まないアプリケーションからの保護**：実行可能なファイルや Java アプリケーション、ActiveX 制御、スクリプト、専用アプリケーションを通じて、望ましくないコードが実行されないようにする
- **ヘルプデスクのコストを削減**：アプリケーションのインストールやシステム構成などに対する制御を維持することによって、不適切なソフトウェアを識別し、削除するための費用を削減することができる
- **パッチの柔軟性**：信頼されたアプリケーションのみを実行するように設定することで、定期的なパッチ適用の周期に合わせ、遅れてパッチを当てることができる
- **中央一元管理**：管理下にあるすべてのシステムがアプリケーションの使用状況、ソフトウェアの使用状況測定、偽ソフトウェアや悪意あるソフトウェアについてソリューションに報告できる

ただし、企業にアプリケーション制御ソリューションを導入するには、コストがかかります。

アプリケーション制御の「デフォルト拒否設定」方法

大手のアプリケーション制御ベンダーは、「デフォルト拒否設定」のモデルに力を入れています。ここでは、信頼されたアプリケーションをホワイトリストに入れて実行しなければなりません。こうしたソリューションでは、管理を簡単にするために、何百万という信頼されたアプリケーションのハッシュを一覧表にして提供し、一方で、新しいソリューションへの入力を更新するように常にガイダンスを行っています。ガイダンスの例は、次のようなものです。

- このアプリケーションは、信頼できる発行元として登録されます
- このアプリケーションは、信頼できるソフトウェア配信システムからインストールしなければなりません*
- このアプリケーションは、信頼できるディレクトリのどれかから実行開始またはインストールしなければなりません*
- 信頼できる更新元から、新しいバージョンのインストールを行わなければなりません*

注)* こうした機能は、通常は管理者特権を有するユーザーが実行しなければならず、標準ユーザが実行することは禁じられています

上記のような基準があるため、通常アプリケーション制御のベンダーは、アプリケーションの信頼性のための閾値を定義する非常に正確なモデルを作成します。その結果、「ファイル評価」が決定し、グレイリスト用のパラメータが指定されます。
エンドユーザーへの影響を最小限に抑えるため、アプリケーション制御製品のベンダーは、他のセキュリティソリューションに倣って、異なるレベルの「信頼性」を設定しました。この実装のしかたはベンダーによって様々ですが、共通の型が 1 つあります。

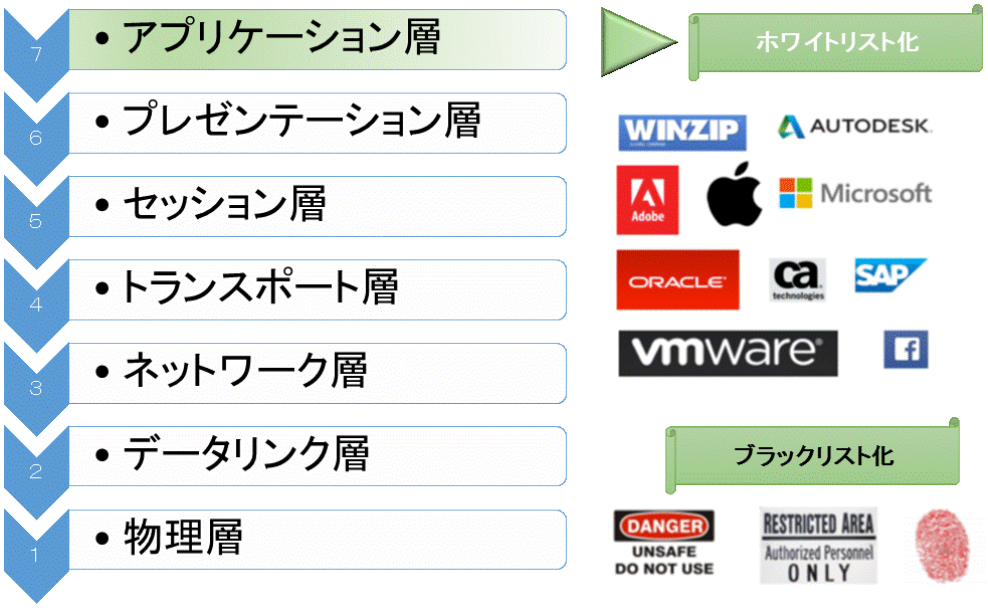
- **低リスク**:エンドユーザーは、制限されずにソフトウェアを実行することができ、イベントは中央のコンソールに報告されて、詳細な調査とルール作成が行われる
- **中リスク**:ソフトウェアの評価とグレイリストが、脅威とみなされる可能性がある閾値に達したため、エンドユーザーは、ソフトウェアの実行を確認するよう指示される
- **高リスク**:アプリケーションが実際に脅威であると認識され、実行を拒否される。「デフォルト拒否設定」のモデルでは、これは信頼性基準に合致しないすべてのアプリケーションに適用される。カスタムアプリケーションやベンダー特製のパッチ、署名のないアプリケーションは一般的に、パラメータ無効により遮断される

高リスクアプリケーションを実行するには、この後ホワイトリスト化しなければなりません。

アプリケーション制御のホワイトリストへの依存

初めてホワイトリストを導入したのは、StormWatch ソリューションを使った Okena でした。同社はのちに Cisco に合併され、StormWatch は、Cisco Security Agent（CSA)と改名されました。この技術は、アプリケーションとシステムのファイアウォール規則を使って、ネットワークトラフィックをホワイトリスト化したものです。これには、予測される動作をエージェントが「学習」し、許容できるネットワークの動作に関して、膨大な量の規則を作成することが必要です。初期のころは、StormWatch はネットワークへの猛攻撃とサービスベースのワームを防ぐように設計されていました。未知のプロセスやアプリケーションはすべて、ネットワークへのアクセスを拒否され、改ざんされたプログラムはすべて自動的に修正されました。

この手法は、ISO のモデルをアプリケーションレイヤに拡張したもので、技術のしかるべき進化を反映しています。アプリケーション制御ソリューションの第一世代は、業務上すべての信頼できるソフトウェアを特定する必要があり、そのために名称が「ホワイトリスト」というのです。ソリューションの維持には、かなりの人員を投入しなければなりませんでした。そこで、もっと人手をかけないプロセスが求められていたのです。



労働集約型のホワイトリスト化における必要性から生まれた努力によって、以下のようなアプリケーション制御ソリューションの開発に拍車がかかりました。

- 既知の、信頼できるアプリケーションを何百万も掲載したホワイトリストライブラリの事前設定
- マルウェアや疑わしいアプリケーションを何百万も掲載したブラックリストと評価のライブラリ
- 未知のアプリケーションを分類するためのグレイリストの基準
- 規則のカスタマイゼーションに対応したり、業務に特化したアプリケーションを取り込んだりするための管理ツール

また、多くの場合、特定の信頼できるベンダーからのアプリケーションがすべて、全従業員に適しているとは限らないことも覚えておくべきことです。これを踏まえると、ホワイトリストの手法はそもそも複雑で欠点が多く、代替ソリューションを考える必要があるのです。

アプリケーションのセキュリティリスクを少なくするためのよりよい方法

BeyondTrust の PowerBroker® for Windows は、アプリケーション制御を超えた、次の論理ステップを実現しました。従来のアプリケーション制御と同様、Power Broker for Windows もソフトウェアの使用状況、やインストール、オペレーティングシステムの構成変更に関して強制的に制限をかけます。しかし、このソリューションは、サードパーティのエージェントにデフォルト拒否設定モードを強制実行されなくても、システムの安全性を保つことができるのです。

代わりに PowerBroker for Windows は、すべてのユーザーを標準ユーザー権限にしておき、規則とポリシを利用して、アプリケーションを管理者権限に上げて、正しく機能するようにします。PowerBroker for Windows は、オペレーティングシステム標準のセキュリティモデル（Windows XP 以降）を使用することによって、アプリケーションやタスクのパーミッションを上げながら、基本的には不適切なユーザーの動作を「デフォルト拒否設定」することができます。こうして PowerBroker for Windows は生産性を損なうことなく、最小権限のベストプラクティスの導入を実現することができるのです。

複雑なホワイトリストを何千というアプリケーション署名と共に管理するのに比べ、PowerBroker for Windows のユーザーは、通常ほんの数十個の規則しか必要としません。この規則は、アクティブディレクトリのグループポリシーまたは BeyondTrust の BeyondInsight® Web サービスのいずれかで動作し、Publish、Path、URL、Active X Control、MSI、その他多種多様な基準を基にすることができます。PowerBroker for Windows は、最も一般的なプログラム用にルールライブラリをつけて出荷し、迅速な導入を図ることもできます。

脆弱性をベースにしたアプリケーション管理を通じたグレイリスト化

では、グレイリストとは何でしょうか？ 上で述べたように、アプリケーション制御ソリューションは閾値を使ってアプリケーションを評価するので、必ずしも絶対的な規則を必要としません。PowerBroker for Windows は同様の手法を用いながら、ガイダンス用に業界標準を使っています。

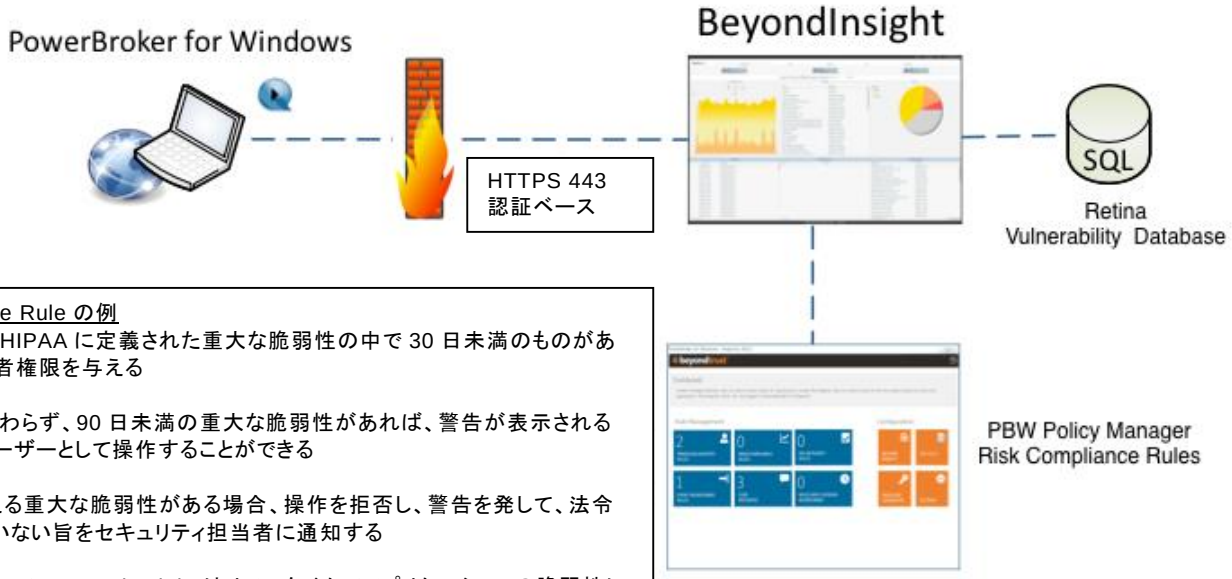
PowerBroker for Windows には、脆弱性に基づいたアプリケーション管理に関する特許技術が使われています。BeyondTrust の Retina Vulnerability Database を基盤にすれば、あるアプリケーションの公開済みの脆弱性に基づいて、そして以下の事項によってフィルタリングをかけて、グレイリストの規則を作成することができます。

- PCI、HIPAA、HiTrust、NIST、ISO、SOX、GLBA、ITIL などの標準に照らした法令違反
- PCI と CVSS による脆弱性の深刻度
- 脆弱性が公開されてからの期間

こうした規則は、あるアプリケーションをブラックリスト化したり、さらにはその権限を変更したりするのにも使えます。したがって、アプリケーションは、業界標準や法令ごとに、既知の脆弱性や、巧妙な標的型の脅威に基づいて制御されます。

使用例：Acrobat Reader のリスク軽減

わかりやすい例として、Adobe の Acrobat Reader 10 の最初のリリースについて考えてみましょう。従来のアプリケーション制御の環境では、この製品は信頼できるものです。既知のベンダーから出されたものだし、電子署名がしてあるし、他のソフトウェアパッケージの一部として簡単にインストールすることができます。これをインストールしたという事実だけで、管理者権限を有していることを示します。さて、このプログラムを実行すると、これは信頼されて現在のユーザーの許可を得ます。従来のアプリケーション制御ソリューションは、上述の通り、通常はユーザーが管理者である、または管理者の証明書を有しているホスト上で実行されます。このバージョンの Reader は非常に脆弱で、誰でも利用できるエクスプロイトがあり、しかもマルウェアのツールキットで簡単に手に入るマルウェアに感染しやすくなっています。さあ、一体なぜこれを信頼できるというのでしょうか？ 管理者権限を与えることは言うに及ばず、です。これは非常に大きな不必要なリスクです。下図は、現実世界でこれが如何に簡単にできるかを示しています。



Risk Compliance Rule の例

1. PCI または HIPAA に定義された重大な脆弱性の中で 30 日未満のものがあれば、管理者権限を与える
2. 法令にかかわらず、90 日未満の重大な脆弱性があれば、警告が表示されるが、標準ユーザーとして操作することができる
3. 90 日を超える重大な脆弱性がある場合、操作を拒否し、警告を発して、法令を遵守していない旨をセキュリティ担当者に通知する

全ての場合において、BeyondInsight はリアルタイムでアプリケーションの脆弱性に関して警告を発します。

PowerBroker for Windows を使った場合、単純な Risk Compliance ルールでは、脆弱性のあるバージョンにフラグを立て、これを実行できないように拒否することもあれば、ただ特権を剥奪して攻撃にさらされないようにするだけのこともあります。これに加えて、BeyondInsight 管理コンソールは、既知のリスクを持つアプリケーションがその環境で実行されたという通知をリアルタイムで受けます。こうすることで、デスクトップとサーバのパッチ管理ポリシが、ほぼすべてのアプリケーションとオペレーティングシステムの機能に関してきちんと守られていることを確認するのに役立ちます。

アプリケーションリスク管理を超えて

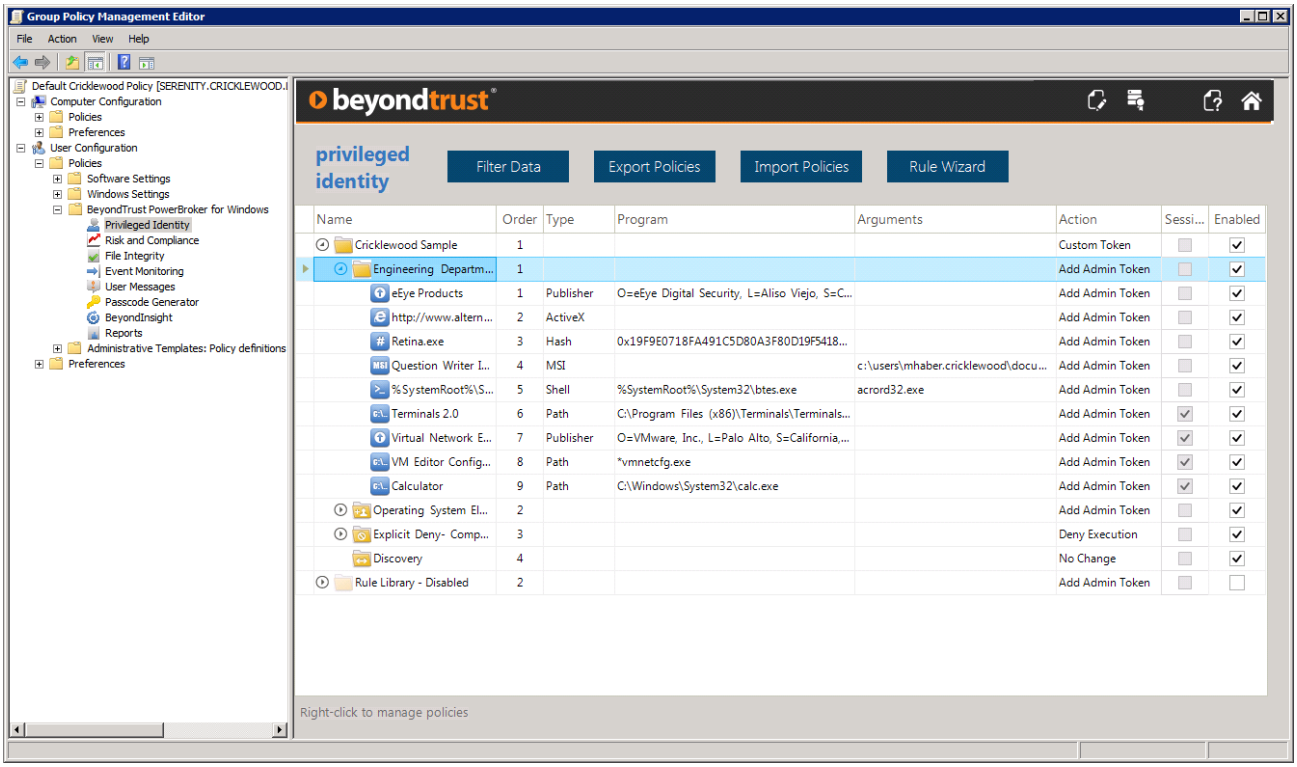
PowerBroker for Windows が行うのは、単なるアプリケーションリスクの管理だけではありません。これは、オペレーティングシステムのコア構成要素をアプリケーション制御に利用する最小権限ソリューションです。また、BeyondInsight 管理コンソールを使って、デスクトップやサーバでの特権を与えられた動作やアプリケーションの動作をすべて文書化することもできます。これによって、以下のことが可能になります。

- UAC イベント、アプリケーション規則、要求された権利の格上げ、拒否されたアプリケーションなどを監視する
- Windows のイベントログで、特権を与えられた動作や疑わしい動作に関するイベントを監視し、それについて報告する
- ファイルシステムで、ユーザーまたはグループに基づいて行われた許可されていない変更を監視し、場合によっては許可されていない変更を拒否する
- ユーザーの画面（マルチモニタ認識）を記録し、キー操作の完全な記録や検索の再生を可能にする
- ロールベースのアクセス機能やマルチテナントの機能と統合されたデータウェアハウスを使って、ユーザーや規則の動作について報告する

アプリケーション制御は、企業にとって維持できないほど管理の難しいプロジェクトである必要はありません。Microsoft の Windows オペレーティングシステムも、ユーザーを締め出す点では素晴らしい仕事をするのですが、残念なことに、生産性を高めるよう手綱を緩めるためのツールが備わっていないのです。

PowerBroker for Windows は、必要なパーミッションを使ってアプリケーションを実行できるようにする一方で、オペレーティングシステムに本来備わったセキュリティのレベルを維持することができます。その結果、設計され

たとおりにアプリケーションを実行することができ、セキュリティと運用のチームは、構成全体の完全な制御、許可されたソフトウェア、Active X の制御さえも実現できるのです。



特許技術である最小権限の技術を持つ PowerBroker for Windows は、次世代のアプリケーションセキュリティソリューションです。Microsoft の Windows オペレーティングシステムに本来備わっているセキュリティモデルと組み合わせると、PowerBroker は、ほんのわずかな規則を使って、アプリケーションや権限に対して詳細な制御を維持することが容易にできるようになります。

BeyondTrust について

BeyondTrust は、IT セキュリティリスクを軽減し、コンプライアンス報告を単純化するのに必要な可視性を実現するコンテクストアウェア（状況認識型）の特権アカウント管理と脆弱性管理のためのソフトウェアソリューションを提供しています。

当社は、企業がシステムやデバイスの特権を誤用したことによっておこるユーザー側のリスクを軽減するだけでなく、サイバー攻撃の標的にされた資産の脆弱性を識別し、改善することができるようにします。その結果、当社のお客様は、内部からの脅威と外部からの脅威の両方に対処でき、物理デバイスや仮想デバイス、モバイルやクラウドなど、あらゆるデバイスをできる限り安全に保つことができます。

BeyondTrust のソリューションは、BeyondInsight の Risk Management プラットフォームの下に統合されており、これによって、IT やセキュリティのチームは、1 つの状況認識型のレンズを通してユーザーや資産のリスクを見ることができます。このようなわかりやすく統合されたリスク分析によって、共同での決定を積極的に下すことができ、しかもリスクの軽減という共通の目的に向かって日常業務を進めることが確実に行えるようになるのです。

本社：米国アリゾナ州 Phoenix 市、詳細情報は、www.beyondtrust.com をご参照ください。

beyondtrust
Beyond Traditional Security