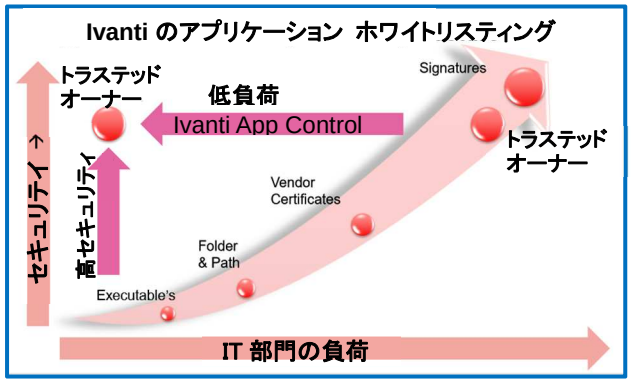
ivanti Application Control

低運用負荷で高度なセキュリテイ:アプリケーションホワイトリスティングと権限管理/ワークステーション、サーバー対応

ICT システムのセキュリティのための TOP4 の対策の実装により Windows の脅威の 85%を防ぐことが出来ると指摘されています[*1]。Ivanti は、この 4 つの対策、オペレーティングシステムのパッチ、アプリケーションのパッチ、アプリケーションのホワイトリスティング、権限管理を実装するセキュリティ製品を提供しています。Ivanti Application Control は、アプリケーションのホワイトリスティングと権限管理の機能を提供します。従来のホワイトリスティングは、OS やアプリケーションのアップデートに伴うホワイトリストのメンテナンスが課題となっていましたが、Ivanti Application Control は、ユニークなアプローチで、ホワイトリストのメンテナンスに必要とされてきた IT 部門の継続的な負荷を解消し、運用負荷とセキュリティのバランスのとれたアプリケーション実行制御を実現します。
また、ファイルのデジタル署名による実行許可も合わせて適用することで、改ざんやなりすましアプリケーションの実行を防ぐことができます。
ビジネスを安全に保ちながら、運用負荷を最小限に抑えることで、IT 部門がコアビジネス目標に集中することを可能にする非常に強力で使いやすいソリューションです。

○メンテナンスフリーのランサムウェア、マルウェア対策

ランサムウェアをはじめ、マルウェアに対して唯一有効な方法はシステム上で動作させないことです。Ivanti Application Control は、アプリケーションのファイルの所有者を確認し、信頼されたリストと一致した場合にのみ実行を可能とし、それ以外のファイルの実行をブロックすることで、追加設定なしに、ランサムウェアをはじめとするマルウェアに対する強力なセキュリティを実現します。また、ファイルの所有者に加え、ファイル属性によるリスト登録、ファイルシグネチャによるリスト登録及びファイルベンダーのデジタル署名を併用することで、運用負荷とセキュリティ効果のバランスをとりつつ、きめの細かい制御を行なうことができます。



○Windows 権限管理によるセキュリティ

システム運用においては、最低限必要な利用者のみ必要最小限のアクセスを許可することが重要です。ユーザーに完全な管理者権限を付与することにより、エンドポイントが脆弱になり、特権アカウントの乱用による内部不正・情報漏洩、操作ミスによるシステム障害、不正使用による情報漏洩やシステム改ざん等のリスクが増大します。Ivanti Application Control の Windows 権限管理は、ユーザーから完全な管理者権限を除去した運用環境で、ユーザーが必要とするアプリケーションやタスクにのみアクセスできる昇格権限を付与することでエンドポイントの安全性を確保しつつ円滑な運用を可能にし、IT 部門の負荷を低減します。

○アプリケーション N/W アクセスコントロール

Ivanti Application Control のアプリケーション N/W アクセスコントロールは、ルーター、スイッチ等によることなく、N/W リソースへのアクセスを制御します。IP アドレス、UNC パスのファイル/フォルダ、URL や FTP ロケーション 等の N/W リソースへのアクセスを、グループやエンドポイントに対するポリシー定義により許可/禁止し、きめ細かい設定で、セキュリティを強化します。

株式会社アイユート

AIUTO!

ivanti Application Control

○特長

○実行許可- トラステッドオーナー

•アプリケーションが管理者、TrustedInstaller 等、信頼された所有者により導入された場合、実行許可
•アプリケーションや OS 更新に伴うホワイトリスト維持・管理の IT 部門の継続的負担を解消

○実行許可- トラステッドベンダー

•トラステッドオーナーで不許可のアプリケーションのファイルベンダーのデジタル署名が TrustedVendors のリストとマッチングする場合、実行許可

○実行許可- パス、ファイル属性

•ファイルのパス、属性により、許可ファイル指定
•トラステッドオーナーと併せて指定
•パス、ファイル属性のみによる実行許可も可
•実行可能な曜日、時間帯の指定可

○実行許可- ファイルシグネチャ

•ファイルシグネチャにより、許可ファイルを指定
•改ざん、なりすましアプリケーションをブロック
•実行可能な曜日、時間帯の指定可

○ブラックリスト

•アプリケーションの使用管理の徹底
•サーバ OS コンポーネントのアクセス管理でリソースの不用意な変更を防止し、サーバ保護を強化
•パス、属性によりファイル指定

○Windows 権限管理

•ユーザーから完全な管理者権限を除去した運用環境で、必要なアプリケーションやタスクにのみアクセスできる昇格権限を付与
•エンドポイントの安全性確保、IT 部門の負荷低減

○アプリケーション N/W アクセス管理

• N/W リソースへのアクセスを、グループやエンドポイントに対するポリシー定義により許可/禁止

○コマンドラインのマッチング

•実行中のアプリケーションや、それに関連するコマンドライン引数にセキュリティを適用
•サーバー環境での管理者アクセスを制限的に運用

○コンディション管理

•広範な条件設定により、ログオンユーザーの状況に基づくサーバーリソースへのアクセスを管理
•コンディションに応じて、リソース/アプリケーションにアクセスを許可

○その他

•特定の Web ページへのアクセスを指定 URL にリダイレクト
•オンデマンドの変更リクエストにより、緊急の権限昇格や未承認のアプリケーション使用をリクエスト
•ブロックされたファイルを自動コピーし、保存
•ライセンス管理

***1: Top four mitigation strategies to protect your ICT system --- Australian Signals Directorate**
“2011 年に ASD が対応したイントルージョンの少なくとも 85%は、上位 4 つの対策をパッケージとして実装することで緩和されていたであろう攻撃によるものであった。それらの対策とは:アプリケーションのホワイトリスティング。アプリケーションと OS にパッチを適用し最新バージョンを使用すること。管理者の権限を最小限に抑えること。”

AIUTO!

ivanti
総発売元　株式会社アイユート
〒180-0006 東京都武蔵野市中町 1-22-5
TEL : 0422-56-1917 ／ FAX : 0422-26-8717
お問い合わせ先 TEL : 0422-56-1917
E-mail : info@t-aiuto.jp
URL http://www.endpointsecurity.jp/