機能紹介：CylancePROTECT

固定機能デバイス向けのアプリケーション制御

CYLANCE

アプリケーション制御を通じて固定機能デバイスの状態を維持

CylancePROTECT® アプリケーション制御は、固定機能デバイスが継続的に正常な状態に保たれるようにする機能を提供します。デバイスが長期間管理されていない状態にあると正常な状態から外れてしまうことがありますが、そのような事態を防止できます。

アプリケーション制御は、CylancePROTECT の AI（人工知能）駆動型マルウェア防御機能をさらに高め、固定機能デバイスを簡単に保護する手段を提供します。

- セキュリティ侵害のない状態を継続的に維持する。
- 特定の機能に関して週7日24時間の可用性を維持する。
- 攻撃による混乱状態から影響を受けないようにする。

ATM やキオスクなどの固定機能デバイス上で承認されていないアプリケーションが実行されると、セキュリティ侵害のリスクが大きく上昇します。

攻撃者がデバイスへのアクセス手段を得て悪意のあるアプリケーションをインストールしてしまうリスクに対処するには、デバイスが意図した目的にのみ使用されるようにする簡単な手段が必要になります。CylancePROTECT に含まれるアプリケーション制御機能は、アプリケーション使用に関する規則適用とポリシー管理のための合理的なアプローチを提供します。

固定機能デバイスのセキュリティ強化

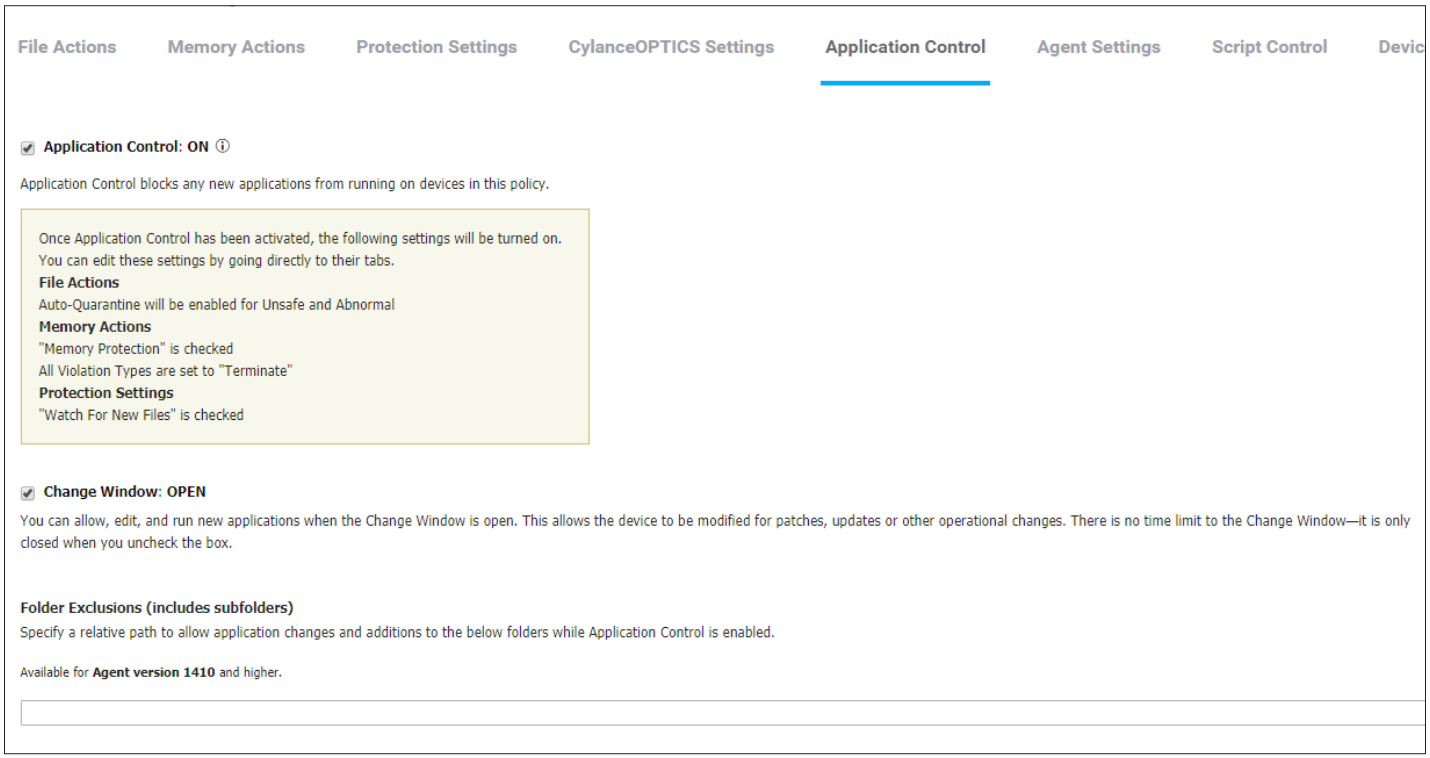
従来、デバイスのアプリケーションスタックの管理にはブラックリスト方式が使用されてきました。これは、悪意のあるアプリケーションであると具体的に知られているか、またはアプリケーションが既知の有害な動作を示さない限り、すべてのアプリケーションの実行を許可するというものです。この方法には、デバイスの管理者が既知の有害なアプリケーションをすべて明示的に特定する役割を負わなければならないという問題があり、これは非現実的な話です。

CylancePROTECT アプリケーション制御は、特定の機能を持つデバイスのセキュリティに関して異なるアプローチを採用しています。管理者が悪意のあるアプリケーションのエキスパートになって常に更新プログラムを提供するよう強いられることはありません。管理者はアプリケーション制御を利用することによって、デバイスの「ゴールデンイメージ」を作成し、それを目的のデバイスに展開して、デバイスが変更されないようグローバルなロックダウンを適用することができます。このデバイスロックダウン機能と、デバイスをアクティブに保護する CylancePROTECT の他の防御機能によって、管理者はデバイスのセキュリティが保たれていると確信を持つことができます。

CylancePROTECT アプリケーション制御：機能の詳細

アプリケーション制御は、指定したシステムをロックダウンし、その後のデバイスの変更を制限できる、オプションの設定です。ロックダウン前にデバイスに存在しているアプリケーションのみが、そのデバイスでの実行を許可されます。新しいアプリケーションだけでなく、既存のアプリケーションの実行可能ファイルへの変更も拒否されます。アプリケーション制御が有効になっている場合は、Cylance®Agent Updater も無効になります。

アプリケーション制御を有効にすると、以下の推奨設定が実施されます（以下の図を参照）。アプリケーション制御が有効になっている場合、これらのポリシー設定は、直接そのタスクに進むと編集できます。



変更ウィンドウ
「変更ウィンドウ」オプションを使用すると、アプリケーション制御を一時的に無効にして、新しいアプリケーションの許可、編集、実行や、更新を行うことができます。これには、エージェントの更新も含まれます。

フォルダ除外（サブフォルダを含む）
絶対パスを指定し、アプリケーション制御が有効な場合でも、アプリケーションの変更や追加が指定したフォルダに適用されるようにすることができます。

主な利点

すべての領域にわたる脅威防御
ただ1つのエンドポイントエージェントによって、継続的なマルウェア防御、デバイスとスクリプトの制御、アプリケーション制御、メモリエクスプロイト保護が行われます。シグネチャの使用や頻繁な製品の更新は不要であるため、アナリストの負担が軽減され、他のビジネスニーズに取り組むことができるようになります。

単一のエージェント／単一のコンソール
管理者は単一の Web ベースのコンソールからすべてのエンドポイントを管理できます。動的（ラップトップ PC、デスクトップ PC）、固定機能（POS システム、ICS、ATM）のいずれのエンドポイントにも対応でき、管理コンソールが複数存在することによって生じる複雑さを解消できます。

エアギャップネットワークの完全なサポート
CylancePROTECT はエアギャップネットワーク（他の部分から切断されたネットワーク）をサポートしています。ICS などの機密性の高いシステムは、インターネットなどの外部ネットワークに直接接続できませんが、CylancePROTECT はそうしたシステム向けの最良のソリューションです。

サイランスについて

サイランスは人工知能を活用することによって、防御ファーストで予測的なセキュリティ製品と特別なセキュリティサービスを提供しています。これらの製品やサービスは、エンドポイントセキュリティに対するアプローチを変革します。

サイランスのセキュリティソリューションは、企業のすべての領域に対して予測的な脅威防御と可視性をもたらし、マルウェア、ランサムウェア、ファイルレスマルウェア、悪意のあるスクリプト、武器化したドキュメント、その他の攻撃ベクトルの脅威に対処します。

AI（人工知能）に基づくマルウェア防御、アプリケーションとスクリプトの制御、メモリ保護、デバイスポリシー適用、根本原因分析、脅威ハンティング、自動化された脅威検出と対処に、エキスパートセキュリティサービスを組み合わせることによって、サイランスはスタッフの作業負荷やコストを増加させることなくエンドポイントを保護します。

Cylance Japan 株式会社
〒100-6510
東京都千代田区丸の内 1-5-1　新丸の内ビルディング 10F
www.cylance.co.jp
03-6386-0061 (代表)

CYLANCE

201806-FF004