

テクノロジー ベスト プラクティス エンドポイント セキュリティ

はじめに

高速ネットワーク、スイッチング、エンドツーエンドの暗号化などのテクノロジーが広く普及するにつれて、ネットワークレベルでのセキュリティが大きな課題になりつつあります。セキュリティ強化を最も必要とする箇所は、データが存在し、被害を受ける可能性の高いエンドポイントです。現在、企業は、エンドポイントのセキュリティ問題に部分的に対処する個別の製品を複数利用しています。これらの製品には、ネットワーク経由の脅威に対する分散型ファイアウォール、ファイル単位の脅威を検出するアンチウィルススキャナ、悪意のある設定を検出する監査または整合性製品などがあります。これらのテクノロジーでは、既存のプロトコルを利用した新しいアプリケーション攻撃や、バンダーがシグニチャなどの対応策をリリースする前にシステムを攻撃する新しいコンテンツベース攻撃には対処できません。

この文書では、企業においてエンドポイントセキュリティ製品を選択する際の判断材料を提供するために、エンドポイントセキュリティソリューションのテクノロジー ベスト プラクティスについて概説します。

ベスト プラクティス

エンドポイントセキュリティテクノロジーを利用して企業を保護する場合、企業のセキュリティ要件に対応可能な製品を評価する際には、複数の要素を考慮に入れる必要があります。社内のセキュリ

ティ、管理性、柔軟性の要件を満たすソリューションを選択しないと、ソリューションの効果が不完全になったり、セキュリティ上の利点以上に管理上の作業負荷が発生することになります。

ベスト プラクティスには、次のポイントが含まれている必要があります。

1. リアルタイム防止判定

セキュリティ水準を高めつつホスト上のセキュリティポリシーのバイパスを低減するには、アプリケーションの呼び出しをカーネル上で代行受信して、ポリシーに適合しているかどうかを確認する必要があります。共有ライブラリの置き換えまたはシステム監査ログの分析によって実装されるソリューションは、簡単にバイパスされる傾向があります。効果的なエンドポイントセキュリティ戦略には、攻撃またはシステム変更を発生後に認識する機能ではなく、ポリシー違反のリアルタイム防止機能があります。

2. 攻撃からの徹底的な保護

企業のセキュリティポリシーを完全に遵守させるには、アプリケーションとその基盤となるシステムの間の手元の主要通信点をエンドポイントセキュリティテクノロジーによって代行受信する必要があります。ネットワークコントロールでは、クライアント/サーバ間の通信をポートまたはプロトコル単位で制限するほか、ホストでの利用を許可する通信を制限する必要があります。



ファイルシステムコントロールでは、フォルダおよびファイルに対する読み取りまたは書き込みアクセスを、個人またはグループ単位で許可または拒否する必要があります。レジストリコントロールでは、システムおよびその他のアプリケーションの動作を制御する重要なレジストリキーの上書きを禁止する必要があります。また、COMコントロールでは、プロセス間通信において許可されるアクセスを制限する必要があります。

攻撃には、ネットワークおよびアプリケーションの脆弱性の不正利用、増殖および感染拡大、不正なシステム変更といった複数のフェーズがあります。完全なエンドポイントセキュリティ戦略では、新種の攻撃が現れた場合に早い段階で阻止できるように、これらのすべての攻撃からシステムを保護する必要があります。

3. エージェントおよび企業のレベルでのリアルタイム関連付け

エンドポイントセキュリティテクノロジーでは、関連付けが不可欠です。エージェントレベルの関連付けを展開すると、シグニチャ照合アプローチには備わっていない一定の防止判定機能が実現されます。アプリケーションの動作に関するイベント発生順序を関連付けると、False Positiveの可能性がなくなります。また、企業レベルでの関連付けでは、セキュリティの適応性が高まります。分散されたエージェント上のイベントと関連付けることで、エンドポイントのセキュリティポリシーが動的にアップデートされて、悪意のあるコードの感染が阻止されます。このため、数多くのリソースへの被害の拡大が防止されます。

4. 動作に基づくアプローチ

エンドポイントのセキュリティアプローチでは、システムおよびアプリケーションを正常に動作させて、対処的ではなく予防的なセキュリティを実装する必要があります。シグニチャに依存したソリューションでは、シグニチャアップデートの最新リリース時点までのセキュリティしか提供されません。

5. 独自の企業ニーズに対応できる柔軟性

システムおよび社内アプリケーションの設定方法および管理方法の詳細は、企業ごとに異なります。エンドポイントセキュリティソリューションは、この独自性に対応可能な柔軟性を備えている必要があります。そのためには、固有のアプリケーションおよび実装に対応できるように、既存のポリシーをカスタマイズする機能や、新しいポリシーを作成する機能が必要になります。また、ポリシーの手動作成による管理上の作業負担を軽減するには、ポリシーの自動作成をサポートしているソリューションを選択する必要があります。

6. 展開のしやすさ

エンドポイントセキュリティ戦略では、エージェントの展開に必要な人員数を最小限に抑える必要があります。そのためには、適切なセキュリティポリシーを簡単かつ迅速に展開できる機能を備えたソリューションを選択し、ホストレベルでの操作なしで新しいポリシーおよびカスタムポリシーを必要に応じて展開できるようにする必要があります。また、Webベースの展開をサポートし、標準的な企業内ソフトウェア配信メカニズムと容易に統合できるソリューションを選択する必要があります。

7. イベントの集中管理

エージェントから出力されるすべてのイベントが、アラートおよびレポートを出力する中央のリポジトリに集約される必要があります。SNMP、ページング、電子メール、フラットファイルなどの標準的なアラームインターフェイスをサポートし、社内システムと容易に統合可能なカスタムインターフェイスをアラートシステムに利用できるソリューションを検討する必要があります。

8. デスクトップおよびサーバのサポートを含めたプラットフォーム対応

保護対象となる重要なオペレーティングシステムに対応したソリューションを検討する必要があります。複数のホストを標的にするウイルスやワームなどの最近の攻撃を考慮すると、デスクトップシステムとサーバベースシステムの管理および実施手法を統一する必要があります。

9. 管理

ポリシー管理の負荷を軽減するには、ポリシーの一元的な定義と一定間隔でのエージェントへの自動配信が可能なソリューションが必要になります。また、複製および保管の目的で、ポリシーをエクスポートできるソリューションも必要になります。複数の管理者を配置している企業では、環境の管理を容易にするために、「どんな場所からでも管理できる」機能が重要です。エンドポイントセキュリティソリューションは、標準的な Web ブラウザ経由でどんな場所からでも管理可能である必要があります。これにより、各管理者のデスクトップにカスタムソフトウェアや安全性が低く保守の困難なリモート管理ソフトウェアをインストールする必要がなくなり、IT 担当者の学習曲線が緩やかになります。

数千台のシステムの保護を必要としている大企業では、1 人の責任者が数千のエージェントをサポートでき、組織または地域を越えてポリシーを複製できるソリューションを検討する必要があります。

まとめ

制約の多いソリューションまたは管理不可能なソリューションを避けるには、ここで説明されているセキュリティ、管理性、および柔軟性の要件をエンドポイントセキュリティソリューションが満たしているかどうかを確認する必要があります。

©2003 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

問合せ URL: <http://www.cisco.com/jp/service/contactcenter/>

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL.03-6670-2992

電話でのお問合せは、以下の時間帯で受け付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先