Ivanti Endpoint Security, powered by Heat

エンドポイントをコントロールする

急速に変化する IT ネットワークはかつてないほど分散され仮想化しています。多くのデータがノートパソコンやスマートフォンなどのリモートのエンドポイントに保存され、クラウドベースの共有アプリ経由でのアクセスが増加しています。さらに、標的型攻撃の増加に伴い、多層防御型のセキュリティ体制がかつてないほど重要になっています。持続的なこれらの攻撃を防止する多層かつポイントベースの技術の必要性と、予算とリソースの制限のバランスを取るため企業は常に頭を抱えています。

規模や業界を問わずあらゆる企業が標的型攻撃の影響を受けています。

- 企業の 40%が、自社のエンドポイントがターゲット型攻撃（APT）の侵入経路となっていると回答しています。[1]
- 標的となっている企業の平均規模は社員 2,500 人ですが、社員 250 人以下の企業への攻撃が最も急速に増加しています。[2]

複数のポイントベースのエンドポイント管理およびセキュリティ技術に依存することにより、IT 環境が複雑化し、コストが追加されています。事実、エージェントの平均数はここ数年で 1 つのエンドポイントあたり 7 以上に増加しています。同様に基本的なエンドポイントセキュリティと運用機能を管理するために使用されるコンソールの平均数は 1 組織あたり約 7 台に増加しています。[3]

Ivanti Endpoint Security がもたらすメリット：

- 標的型攻撃に対する多層防御型の保護：運用およびセキュリティ機能を組み合わせることで、標的型の攻撃の進行を防止する予防技術の層を重ねつつ、攻撃対象領域を効果的に削減できます。
- エンドツーエンドのアプローチを使用する強化された可視化とコントロール：エンドツーエンドのアプローチには、エンドポイントの運用、セキュリティ、コンプライアンス、IT リスク管理のニーズを満たす機能が含まれます。
- 完全に統合された単一エージェント、単一コンソールのアーキテクチャによる複雑性の軽減と TCO（総所有コスト）の削減：ワークフローの能率化を図りつつ、エージェントの肥大化とエンドポイントのパフォーマンスの損失を排除します。

Ivanti Endpoint Security は、複雑性を削減しコストを削減する統合化されたプラットフォームを実現しつつ、運用およびセキュリティ両方の観点から、エンドポイント保護の問題に対応します。
エンドポイントにある既知の攻撃対象となる領域を軽減し、信頼できるアプリケーション環境を定義し、既知および不明なマルウェアを阻止し、データを保護することで、Ivanti はエンドポイントのリスクの様々な側面に対して多層防御を提供します。複雑性は、考え抜かれたセキュリティに対するアプローチを失敗させる原因となります。このため、Ivanti はモジュラー式のエージェントを使って単一のサーバー、データベース、コンソールアーキテクチャを通して運用できる Ivanti Endpoint Security を開発しました。これにより、場所を問わず、何千ものエンドポイントを簡単に管理できるようになります。

エンドポイントの運用

パッチ管理：すべてのエンドポイントとサーバーでオペレーティングシステムとアプリケーションの脆弱性を排除することで、企業のリスクを軽減し、IT 部門の業務を最適化します。様々な OS バージョン（例：Windows、Linux、UNIX、OSX）とサードパーティー社製アプリケーション（例：Adobe Acrobat Flash、Adobe Reader、Google Chrome、Mozilla Firefox、Oracle Java）をサポートします。

コンテンツウィザード：ソフトウェアの展開や削除、設定の修正、システム管理タスクの実行、お客様へのパッチの提供を実行するため、ウィザードベースのツールを通してカスタマイズされた拡張性を実現します。

レポートサービス：企業のニーズに合わせてカスタマイズできる統合された事前設定済みの集約化されたビジネスインテリジェンスを提供します。

企業の 40%が、自社のエンドポイントがターゲット型攻撃（APT）の侵入経路となっていると回答しています。

エンドポイントのセキュリティ

アプリケーションの管理：明確に権限が付与された、もしくは信頼できるアプリケーションのみの実行を保証するため、ホワイトリストのポリシーを通して信頼できるアプリケーションの使用法を設定し施行します。メモリ領域への高度なインジェクション攻撃を防ぐ高度なメモリ保護が含まれます。

ウイルス対策：ブラックリスト保護およびウイルス、ワーム、スパイウェア、トロイの木馬、アドウェアなどすべてのマルウェアの除去を実現します。

デバイスコントロール：データ損失や盗難を防止するためリムーバルメディア向けのデータの暗号化を実現しつつ、デバイスとポートに対して使用ポリシーを適用します。

主な特徴

- 単一の回復力のあるエージェントを使用するモジュラー式の拡張可能なアーキテクチャ：エージェントの肥大化を軽減するため、単一のエージェントを使用する拡張可能なプラットフォーム。
- 役割ベースのアクセス管理：機密情報を効率的に保護し、不正アクセスによるユーザーのエラーを防止するため、グループやドメインの詳細な管理を実現します。
- アクティブディレクトリの統合＆同期：Active Directory でドメイン、ユーザーグループ、個別のユーザーの設定をサポートし、設定と保守の負担を軽減するため、アクティブディレクトリと同期することを保証します。
- 強化された資産検出＆エージェントの展開：管理されているシステムと管理されていないシステムの可視化を保証するためエンドポイントをスキャンし、自動またはスケジュールに従って管理されていないシステムにエージェントを展開します。
- 速やかなポリシーの更新＆処理：プッシュ技術に頼らず、ほぼリアルタイムのポリシーとイベントの更新を実現します。
- 仮想インフラストラクチャ対応：環境上のすべての仮想システムを特定し、単一のソリューションで物理システムと仮想システム両方の管理を可能にします。
- レポート：企業にクリティカルなフィードバックを提供するあらゆる種類の運用および管理に関するレポートでエンドポイントの環境全体を把握できます。
- 強化された Wake-on-LAN：クリティカルなパッチの適用とソフトウェアアップデートが実行されるようにオフラインのマシンを起動させます。また、電力ポリシーを使用している場合に、コンテンツウィザード経由で、最大のエネルギー効率を保証します。

1 Ponemon Institute, 2014 State of Endpoint Risk
2 Symantec, Internet Security Threat Report vol. 17
3 Ponemon Institute, 2015 State of Endpoint Risk

03-5226-5960
www.ivanti.co.jp
Contact-Japan@ivanti.com