ivanti

ソリューションシート

簡単に適切なエンドポイントのセキュリティを確保

セキュリティと IT の専門スタッフは、近年の巧妙な攻撃から企業を守るためにどのような手段を講じているのでしょうか？

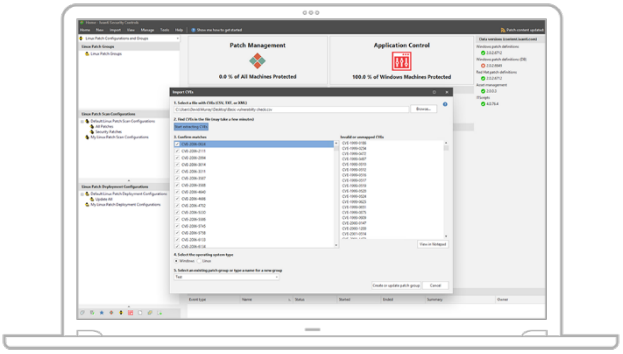
的を絞ったセキュリティ戦略がなければ、デバイスの無秩序な増殖には多大なコストがかかり、管理不能な状態に陥ります。IT チームは、これらのデバイスの管理に膨大な時間を費やしています。これに加え、サイバーセキュリティの知識を持つ労働力が不足しているため、企業はセキュリティ担当者を最適化せざるを得ない状況になっています。つまり、総合的かつ簡易化された管理技術を活用する集中的な戦略を実施し、実際の攻撃に対する最高のバリアを作るセキュリティの基本に集中することで、他のソリューションに勝る強力なメリットが得られることは明らかです。

まずはパッチ適用から

多くの脆弱性が悪用できる状態のまま放置されている背景には、長年利用できる状態にあるセキュリティパッチが一度も適用されていないという現実があります。

IT に大きな損害を及ぼすことなく、また新たな悩みの種を生じさせることなく、すべての脆弱性を追跡し、修正し続けるにはどうすればよいのでしょうか？企業に必要なのは、簡単に社内ネットワーク全体を調査、評価、テストし、パッチを適用する方法です。また、脆弱性の大半がサードパーティー製のアプリケーションに影響を及ぼすため、OS へのパッチ適用や更新だけでは不十分です。

時間やお金をかけず、主力事業の取り組みをサポートすることに集中しましょう。Ivanti のツールは、わずか数分で起動し、お客様が定義したポリシーに基づいて、社内ネットワーク上の Windows、MacOS、Linux、UNIX システムすべてを自動的に特定、評価、修正します。当社のツールは物理システムと仮想システムの両方へのパッチ適用を簡単な操作に変えます。オンラインとオフラインのワークステーションとサーバーを検出し、不足しているパッチをスキャンし、展開します。その後、OS やアプリから仮想マシン（VM）、仮想テンプレートまで、あらゆるシステムにパッチを適用します。さらに、VMware との統合により、ESXi ハイパーバイザーにもパッチを適用します。



また Ivanti は、SCCM コンソールを通してサードパーティー製アプリケーションのパッチを検出、展開するプロセスを自動化する Microsoft System Center Configuration Manager へのプラグインも提供します。

当社のパッチソリューション向けの高度な API スタックは、セキュリティソリューション、脆弱性スキャナ、構成管理ツール、そして報告ツールに統合できます。この統合は、セキュリティ部門、IT 部門、DevOps 間のギャップを埋めることにも役立ちます。例えば、テストを実施するために次のパッチのバッチに最新の脆弱性評価を自動インポートすることができるため、相当な時間を節約できるだけでなく、IT 部門をこれまで以上に効率的な企業保護のパートナーに変えることができます。DevOps の役割は、継続的に改善と自動化を進めることです。また、DevOps にパッチ管理を統合した場合、より回復力があり、一貫性のあるインフラストラクチャやシステムを実現できます。また、Splunk、Reporting Services、Archer、Crystal Reports などのソリューションに重要なデータを入れ、クリティカルなセキュリティインシデントを速やかに分析し、必要な対応をし、解決できます。

パッチが適用できないなら阻止

言うまでもなく、パッチでは、ゼロデイ攻撃に対する保護はできません。また、例えばレガシーシステムを実行している、もしくはパッチを適用することで使用している環境に何らかの支障がでることを懸念していて、パッチが適用できない場合はどうすればいいのでし

ようか？アプリケーションのホワイトリストなどのツールを使用してパッチを適用できないアプリを安全に保護する必要があります。

また、生産性を向上するために必要なアプリのみをユーザーに提供し、不正アプリを導入させないようにすることが極めて重要となります。不正アプリはデスクトップの安定性を軽減し、セキュリティに影響を及ぼし、ライセンスのコンプライアンスの違反となり、ユーザーのダウンタイムにつながり、デスクトップ管理コストを引き上げる原因となることがあります。

一方で、デスクトップをロックダウンすればリスクを軽減できるものの、ユーザーエクスペリエンスの質も大幅に低下してしまいます。パフォーマンスが低下するためユーザーの生産性は下がり、結果としてヘルプデスクに多くの問い合わせの電話がかかることになります。また、シャドーIT（個人用のデバイスを許可なく使用すること）で問題を対処する可能性があるため、新たなリスクにつながる場合があります。

Ivanti は、IT 部門に膨大なリストを手作業で管理させることなく、また、ユーザーの生産性に障害をもたらすことなく、不正コードの実行防止に役立つ革新的なソリューションを提供します。Trusted Ownership™は、既知のコードであっても、信頼できない所有者（例えば一般的なユーザーアカウントなど）が導入したすべてのコードの実行を自動的に防止します。簡単な操作でユーザー権限やポリシーを詳細に管理できるだけでなく、例外が発生した場合に自己昇格機能を使用できます。さらに、担当業務を遂行するために必要な権限のみをユーザーに付与することで、プロセスをシンプルにします。

安全な構成を最優先

オペレーティングシステムとアプリケーションのデフォルト設定は通常、セキュリティではなく展開しやすさと使いやすさを念頭に置いた設定です。結局、ユーザーが求めているのは、最低限の構成基準を維持することなのです。

SamSam ランサムウェアなどの攻撃を未然に防ぐサポートを提供するため、当社は、不要な場合にリモートデスクトッププロトコル（RDP）をオフに設定するセキュリティスイートを提供しています。同様に、WannaCry 攻撃が実行されて以来、IT 部門にはサーバメッセージブロック（SMB）バージョン 1 サービスを無効に設定することが推奨されるようになりました。当社はデフォルトで SMB バージョン 1 を無効に設定しています。

パスワード類推攻撃を制限するロックアウトのポリシーを設定することもできます。さらに当社は、このスイートまたはスタンドアロンのソリューション経由でデバイスコントロール（リムーバルデバイスの使用の管理、リムーバルデバイスおよびハードドライブ上での暗号化の施行）も提供できます。

Ivanti が実現できる安全の構成管理の例をいくつかご紹介します。

セキュリティスイートを活用したレベルアップ

Ivanti は、業界をリードする自動化された Windows と Red Hat Linux のパッチ管理、動的なホワイトリスティング、詳細な権限管理をひとつのソリューションに集約しています。CVE とパッチのリスト作成に対応しているだけでなく、Ivanti は他の製品との統合、共有プロセスの自動化、リモートアクセスとコンソールのコントロールを実現するため、Patch REST API も提供しています。2019 年、Ivanti Security Controls のパッチ適用範囲は、MacOS、CentOS などに拡大される予定で、デバイスコントロールの提供も予定されています。

さらに、お客様が単一のコンソールからデバイスを管理し、安全に保護できるようにするため、当社の統合エンドポイント管理プラットフォームにセキュリティスイートを内蔵します。Ivanti Endpoint Security for Endpoint Manager は、パッチ管理とアプリケーションコントロールに高度なアンチウイルス機能とアンチマルウェア機能を追加します。また、前述の通り、デバイスコントロールとファイルレス攻撃に対する高度な保護（インターネットからダウンロードされたスクリプトの無効化、アプリの挙動の検出、信頼できるアプリのスクリプト実行のみを許可、メモリ内攻撃に対する保護など）も提供できます。さらに、許可されたネットワークや IP アドレスにアクセス権を制限することや、個別のシステムやシステムグループに対してファイアウォールの設定（最新の Windows ファイアウォールを含む）をカスタマイズすることもできます。マルウェアをブラックリストして効果的に攻撃を阻止するため、ローカルマシンのファイルを暗号化しようとする試みを検出し、暗号化プロセスを阻止し、ネットワーク上の他のすべてのコンピューターにインシデントを通知できます。また、高性能リモートコントロール機能が装備されているため、ネットワーク上のエンドポイントを隔離し、調査して、クリーンアップできます。

リアルタイムダッシュボードのレポート

実環境の実態を把握していなければ適切な防御はできているとは言えません。そこで Ivanti Xtraction は、レポートをチェックボックスに変えます。さらに、ご要望に応じて、当社のソリューションに関するデータや、簡単に新しいダッシュボードやレポートを作成できる機能を提要します。経営陣や取締役、事業部門（LOB）やアプリケーション所有者に適切なデータを提供し、速やかに賢明な判断を下せるようサポートしましょう。

お問い合せはこちら　www.ivanti.co.jp　03-5226-5960　Contact-Japan@ivanti.com