

セキュリティ戦略を再評価する 5つの理由

エンドポイントのセキュリティ保護は日々複雑になってきており、組織にとって非常に大きな課題となっています。情報資産や知的財産の価値が増したため、データの盗難は、高度に組織化された犯罪組織の資金源と化しています。その結果、攻撃手法は多様化し、オペレーティングシステムやアプリケーションに対する最先端のセキュリティも新手の攻撃の脅威にさらされています。このように進化し続ける、情報インフラストラクチャに対するさまざまな脅威に対抗するため、組織ではさまざまなセキュリティソリューションを導入しています。その結果、コスト増、コンフリクト、管理の複雑化などの問題に加え、必要なレベルの保護が実現しないという問題も発生しています。

情報インフラストラクチャを適切にセキュリティで保護するには、次の 5 つの要素を念頭において組織の全体的なセキュリティを再評価する必要があります。

1. マルウェアの急速な進化
2. 非管理のモバイルやリモート ユーザによるリスクの拡大
3. データ盗難の手法の多様化
4. 多層的な防御を必要とする、攻撃手法の多様化
5. 管理とセキュリティの統合ソリューションによる、インフラストラクチャの管理性とセキュリティの向上

1 マルウェアの急速な進化

競合相手のブランド失墜、知的財産の破壊または盗難による競争力低下、または顧客の機密情報盗難による金銭的利益の獲得など、これらはいずれもプロの攻撃者による日常的な攻撃の動機となります。攻撃者は常に革新的な方法を生み出して、組織の一般的なセキュリティ対策や攻撃防御策に打ち勝とうとしています。この種のマルウェアは急速に進化し続けており、既知の脆弱性に対するパッチのリリースから、そのパッチの脆弱性を突く新たな攻撃の出現までの期間が短くなってきています。

たとえば、2008 年 10 月 23 日に Microsoft は世界中の企業コンピュータに影響する既知の脆弱性を解決するパッチをリリースしました。ところが、その翌日にはパッチの脆弱性を利用する攻撃が表面化しました。

これらの攻撃は、元の Conficker ウイルスの第 3 世代の亜種である Conficker.C ウイルス（“Kido” ウイルス）を含んでいました。

亜種ウイルス Kido は進化の途中で検出と除去を避けるための手段を身に付け、感染方法も新しくなっていました。Kido は、ファイアウォールやパッチ配布などのセキュリティ製品のスキャンと検疫プロセスやアンチウイルスソフトウェアを無効化してしまいます。F-Secure によると、2009 年 1 月中旬現在、33 % のコンピュータシステムにはまだ Kido ウイルスの防御パッチを適用されていません。¹

このようなパッチ配布の遅れにはさまざまな理由があります。たとえば、自動パッチ管理プロセスの欠如もその 1 つです。しかし、ほとんどの組織では、パッチを全社的に配布する前に非運用環境で準備およびテストする最初の段階で遅れが生じます。自動パッチ管理プロセスを導入済みでもそれだけでは、進化が早く適応性が高いマルウェアの出現に打ち勝つことはできません。これはゼロデイ攻撃の出現からも明らかです。

これらの課題を解決するため、Avocent の LANDesk® ソリューションは複数の側面からマルウェアに打ち勝ちます。LANDesk は、堅牢な自動パッチ管理システムに加えて、ホスト侵入防御システム（HIPS）と従来型のシグネチャベースのウイルス対策およびスパイウェア対策を組み合わせ、頻繁な更新が可能な一元管理のマルウェア対策を提供します。

LANDesk® Security Suite は脆弱性の高度な検出機能によって、スパイウェア、アドウェア、トロイ、キーロガーおよびその他のマルウェアを自動的に検出して対処します。また、LANDesk Security Suite のウイルス対策およびスパイウェア対策機能を補完する、LANDesk® Host Intrusion Prevention System（HIPS）もご利用いただけます。多様化する非シグネチャベースの悪意のあるコードを防御してゼロデイ攻撃対策を強化します。

LANDesk HIPS では、実証された経験則に基づく挙動認識技術で、悪意のあるコードの典型的なパターンおよび動作を識別します。LANDesk HIPS は、カーネルレベルにおけるルールベースのファイルシステムおよびレジストリの保護、システム起動の管理、ステルス型ルートキットからの多層的な防御、カーネルレベルのネットワークフィルタリングなどの機能を備えています。LANDesk HIPS は、進化し続けるマルウェアに対抗するための強力なツールです。システム上で実行可能にするコードやアプリケーションに許可する動作を管理者が指定できます。

2 非管理のモバイルや リモート ユーザによる リスクの拡大

組織におけるリスク レベルはモバイル作業員やリモート作業員の増加に伴い上昇し、セキュリティの脆弱性も拡大してきました。リスク上昇の主な原因は、これらのユーザのネットワーク接続はほとんどが不定期で発生するということです。VPN クライアントの起動が面倒になりがちであり、これらのモバイル ユーザやリモート ユーザの多くが、実際のオフィスにはあまり立ち寄りません。企業ネットワークへの接続が不定期なため、これらのエンドポイントのシステム セキュリティを定期的に一貫して管理することは難しく、最新のパッチやマルウェア対策シグネチャの更新を適切なタイミングで行うことも難しくなっています。

LANDesk® Management Gateway アプライアンスを使用すると、専用線や VPN を使用せずにモバイル エンドポイントやリモート エンドポイントを管理できます。Gateway アプライアンスでは証明書ベースの認証と SSL 暗号化を使用して、企業ネットワークとモバイル エンドポイントおよびリモート エンドポイント間の転送をセキュリティで保護します。以前は管理不能だったエンドポイントのセキュリティを、インターネットに接続しているときにいつでも管理することができます。

3 データ盗難の手法の 多様化

プロのハッカーが重要情報を盗む手段を多数考案するようになるにつれ、データ損失の脅威も増してきています。データ盗難の手法が多様化する中、USB ストレージ デバイスやマルチメディア プレーヤーを利用する手法が最も一般的になり、次いで CD/DVD およびその他のリムーバブル メディア ドライブを介した盗難が増えています。特にコンパクトで持ち運び自由な USB デバイスはあらゆる場所で使用されるようになりました。フラッシュドライブ、ポータブル ディスク ドライブ、iPod およびその他のポータブル メディア プレーヤーが何十億台も販売され、業務で使用されています。ところが、容量が右肩上がりが増えており小型で隠しやすいこともあって、データの盗難にもよく利用されるようになりました。これらのポータブル デバイスを使用したサムサッキング (thumb-sucking) やポッド スラッピング (pod slurping) などのデータ盗難では、



わずか数分足らずで PC 内のすべてのドキュメントが持ち去られてしまいます。

USB デバイスの普及は、エンドポイントのセキュリティ保護にさまざまな課題をもたらしました。便利なものであることは間違いなく、組織内での使用を禁止することは現実的には不可能です。したがって、悪意のある操作を禁止しながら効果的に使用されるように管理する必要があります。LANDesk Security Suite はこのニーズに対応するために、大容量ストレージ デバイスおよびメディア デバイスへのユーザ アクセスの詳細な管理手段を IT 管理者に提供します。

LANDesk Security Suite では、すべての USB デバイスとリムーバブル ディスク ドライブに対して読み取り / 書き込みレベルのアクセス制御を設定できます。USB インタフェースからのデータの書き込みは許可したまま、特定のグループのエンドポイントやすべてのエンドポイントに対してなど、USB デバイスの使用を柔軟に禁止することができます。正しいパスワードで承認を受けた場合にのみ USB デバイスに書き込みできるような設定も可能です。USB を暗号化して、USB デバイスに書き込まれたすべてのデータをパスワードで保護することもできます。エンドポイントがネットワークに接続されているかどうかにかかわらず、LANDesk クライアント エージェントは組織のアクセス制御ポリシーを一括適用します。これは、モバイル作業員がいる組織には欠かせない要件です。

その他の場所からのデータ漏えいも防御するため、LANDesk Security Suite には無線チャンネルのアクセス制御とクライアントベースのアクセス ポイント検出機能も備わっており、Bluetooth、802.11 および広域ブロードバンドなどさまざまなクライアント無線インタフェースに対してエンドポイントの通信をアクセス制御することができます。さらに、クライアント システムの無線アダプタを使用して、接続範囲内のすべてのアクセス ポイントを検出およびレポートすることもできます。ネットワーク管理者はレポートされたデバイスを分類して、環境内や傍受領域にある不正なアクセス ポイントを迅速に特定することができます。エンドポイント レポートの信号強度の分析では、物理的な場所をおおまかに三角測量で絞り込むことができます。

4 多層的な防御を必要とする、 攻撃手法の多様化

変化と多様化を繰り返す最新の脅威から組織のインフラストラクチャやエンドポイントを防御するには、ファイアウォール、侵入検知、およびアンチウイルスの専用ソリューションの組み合わせだけに頼ることはできません。これらの対策も必要ですが、変化し続ける脅威と攻撃手法に対抗するには不十分です。最新の過酷な脅威から組織の資産を防御するには、単一の管理コンソールから一元的に管理しながらあらゆるレベルとエントリポイントで攻撃を阻止する、自動化されたコアテクノロジーと付加テクノロジーから構成される多層防御のインフラストラクチャが必要です。

LANDesk は緊密に統合され自動化されたソリューションファミリによって、シンプルでコストパフォーマンスに優れた、エンドポイントの多層的なセキュリティ保護の段階的な実現パスを提供します。これらのソリューションがシームレスに連携し、単一の管理コンソールから一元的に管理可能なバランスのよいセキュリティ保護と管理機能を実現します。単一のクライアントソフトウェアエージェントから操作できるため、効率的で信頼性に優れています。

コア機能と付加機能の組み合わせ

変化を繰り返し多様化する脅威から防御するには、以下の機能を備えた、コアテクノロジーと段階的に強化可能な付加機能から構成される多層防御のセキュリティソリューションが必要です。

資産の検出およびインベントリ

組織がネットワークやエンドポイントを適切にセキュリティで保護するには、自社のネットワークに接続されているエンドポイントやエンドポイントで実行されているソフトウェアの把握が不可欠です。多層的なセキュリティ保護の基本機能として、資産の検出機能や接続されているハードウェアおよびソフトウェアすべてを検出する機能が必要です。これは、特定のデバイスが管理されていたりファイアウォールがローカルに運用されているかどうかなどの状況は問いません。

LANDesk® Management Suite は、接続されているエンドポイントをサブネットレベルで透過的にリアルタイムで自動的に検出し、資産をインベントリで管理します。また、構成の評価と状況の管理を行い、ローカルで有効化されているファイアウォールがあるかどうかを判別します。リモートに分散しているサイトのシステムに、VPN を使用せずにインターネット経由でアクセスできます。

LANDesk Security Suite には無線アクセスポイントの検出機能があり、ノート PC の無線ネットワークアダプタを使用して、企業環境内にあるまたは近隣にあるすべてのアクセスポイントを探して分類します。管理者は未承認のアクセスポイントからのアクセスをブロックすることができます。

パッチの自動管理

OS とセキュリティパッチを最新の状態に保つことは、IT 部門にとって最も煩雑で負担が大きい作業です。多くの組織では効果的なパッチ管理戦略を導入していないため、必要以上にコストをかけ、本来は回避可能なリスクに IT 資産をさらしています。手順を追った管理手法および処理方法を持たないために、拡大するリスクに自らをさらしている組織もあれば、単一障害点となる可能性をはらむ手動での対応に終始している組織もあります。

スキャン、脆弱性評価、ダウンロードおよび準備、配布および保守機能が自動化されている堅牢なパッチ管理ソリューションは、多層防御のセキュリティソリューションに欠かせないコンポーネントです。パッチの保守では、Microsoft Windows および Office アプリケーションから他のベンダのソフトウェアソリューションに拡張して適用します。

LANDesk Security Suite の一部である LANDesk® Patch Manager は、異種混在の IT 環境全体に対する脆弱性評価とパッチ管理を自動化します。脆弱性評価、パッチの調査、ダウンロード、準備および配布機能が統合されており、組織におけるセキュリティの基盤として、さまざまなアプリケーションおよびオペレーティングシステムのパフォーマンスの向上と安定化を実現します。

LANDesk Patch Manager は業界標準の情報を基に管理対象のコンピュータをアクティブにスキャンして、アプリケーションやオペレーティングシステムの脆弱性を特定します。ポリシーを作成して特定のオペレーティングシステム用の各パッチを自動的にインストールすることができます。検出された脆弱性に対する修正作業は個別に選択可能で、新しいパッチがリリースされたら自動的にダウンロードおよびインストールして脆弱性を自動で修正することもできます。パッチの配布を監視、追跡、および報告する機能もあり、ターゲットエンドポイントごとに適切に設定して正しく修正することができます。

マルウェアの防御

最新型の悪意のあるコードに多くみられるマルチポイント攻撃を防御するには、マルウェア対策ソリューションに複数の要素が必要となります。たとえば、更新が頻繁で一元的管理可能な従来型のシグネチャベースのウイルス対策およびスパイウェア対策機能や、認識済みのマルウェアのシグネチャが存在しなくてもアプリケーションの不審な



挙動を検出して未承認のコード実行をブロックする HIPS 機能などが連携して動作することが求められます。前述のとおり、LANDesk の多層防御型セキュリティ ソリューションはこれらをすべてカバーしています。

脆弱性の検出と修正

組織ではユーザの生産性確保とエンドポイント セキュリティの要件のバランスを調整することが必要とされます。企業全体のセキュリティ リスクを抑制しつつ、ユーザが生産性を高められるようにエンドポイントを構成しなければなりません。これが、ビジネス ルールおよびユーザの役割に基づいたセキュリティ構成の標準化が求められる理由です。

このニーズに応えるため、LANDesk ソリューションでは、個人、グループまたは職務単位ですべてのエンドポイントを一元的に管理する構成管理ポリシーを利用できます。さらに、自動的にスキャンしてポリシーに準拠していないマシンにリモートで対処します。LANDesk ソリューションは、組織の詳細なカスタム レベルに基づいて標準的な脆弱性スキャンを頻繁に実施します。これによって、構成変更、パッチ適用およびソフトウェア更新の必要性や、脆弱性へのその他の対応の必要性を迅速かつ具体的に特定できます。

データ損失の防止

データ損失を防ぐには、特に USB デバイスやその他のリムーバブル メディアを利用したデータの移動全般に対して、ポリシーベースの制御を適用する必要があります。LANDesk ソリューションでは、ポリシーを利用してすべての USB デバイスとリムーバブル ディスクドライブに対して読み取り / 書き込みレベルのアクセス制御を設定できます。また、無線チャンネル アクセス制御も、同様にすべてのエンドポイントに対して実行できます。

プロアクティブなモバイル管理

モバイル作業員やリモート作業員によってもたらされるリスク全般を最小化するには企業のファイアウォールを越えて拡張された、スキャンおよび修正機能が必要です。LANDesk Management Gateway アプライアンスは VPN や専用線を使用せずに、このニーズに安全に応えます。

セキュリティの状態の追跡とレポート

適切な保護が行われていると信じていても、実際のセキュリティ保護の効果をエンドポイントごとに測定できなければ、組織は大きなリスクにさらされます。企業全体におけるセキュリティ ポリシーの適用およびコンプライアンスの徹底状況をレポートし文書化する機能が必要です。

LANDesk Security Suite には、セキュリティ戦略の ROI を追跡および実証するための多彩なレポート作成オプションが用意されています。セキュリティ ポリシーの実施に関する詳細な履歴レポートはわかりやすいグラフィック表示で、セキュリティ ポリシーの運用状況を一目で把握できます。IT 管理者やセキュリティ管理者は、セキュリティ ポリシーの構成要素および属性を管理することができ、企業全体にわたって、スパイウェアが存在する可能性のあるインターネット サイトを閲覧するユーザを簡単に特定できます。また、セキュリティの傾向やパフォーマンスを分析することもできます。LANDesk エクゼクティブ ダッシュボードは単一のグラフィックビューで、セキュリティの懸案事項を企業レベルで掌握することができます。

さらに、エンドポイントの更新の必要性、パッチ レベル、パッチ適用の成否、修復されたパッチの履歴要求などもレポートで確認できます。脆弱性のカスタム パラメータもレポート可能で、タイプ、重要度およびその他の条件に基づいてアラートを生成する脆弱性の種類を指定可能で、悪意あるコードやセキュリティ侵害のアウトブレイクをリアルタイムで警告します。

包括的で柔軟な階層型セキュリティ ツール セット

LANDesk は、階層的なセキュリティ保護のための業界随一の包括的で柔軟なツールセットとして、多層防御のエンドポイント セキュリティを実装するための、以下のようなコア機能とコア機能と付加機能の基本的な組み合わせを提供しています。

- LANDesk Security Suite** 統合されたパッチ管理により、アクティブなセキュリティ管理をすべてのエンドポイントに拡張します。アクティブな脅威分析と修正、スパイウェアの検出と除去、ネットワーク アクセス制御、構成セキュリティ ツール、および USB 暗号化やリムーバブル ストレージ管理などの革新的な接続制御管理機能を備えています。LANDesk Host Intrusion Prevention が付属しており、ホストに対する悪意のあるアプリケーション攻撃を防御する挙動ベースの実行ブロックにより、ゼロデイ攻撃を防御します。

- **LANDesk Antivirus** ベスト オブ プリードのエンタープライズ用ウイルス防御、ルートキット検出、検疫機能、および一元管理機能を業界標準のソリューションよりも低コストで提供します。
- **LANDesk Management Gateway アプライアンス** 証明書ベースの認証と SSL 暗号化を使用し、時間や場所を問わずモバイル エンドポイントやリモート エンドポイントをインターネット経由で管理できます。パッチ管理、エンドポイントのセキュリティ ポリシー更新、ウイルス対策 / スパイウェア対策の実施と管理、アプリケーションのブロック、セキュリティ攻撃防御の管理などの機能を備えています。
- **LANDesk Management Suite** 組織環境内のさまざまなコンピュータ プラットフォームをアクティブに管理します。Windows、Mac OS、UNIX、Linux およびその他のハンドヘルド デバイスや組み込みデバイス用オペレーティング システムをサポートします。セキュリティ規約や設定標準へのコンプライアンス徹底を明確にすることができます。インベントリ管理機能によって、ネットワーク上のコンピュータ デバイスのインベントリおよび構成管理を実現します。

5 管理とセキュリティの統合ソリューションによる、インフラストラクチャの管理性とセキュリティの向上

多くの企業は、エンドポイント管理とエンドポイントのセキュリティ保護は個別の取り組みであると考えています。このような考えは、セキュリティ上のリスクを高めるだけでなく、管理上のオーバーヘッドを増やしインフラストラクチャのコストを増加させ、管理をより一層複雑なものにしてしまいます。

前述したように、管理されていないエンドポイントをセキュリティで保護することは不可能であり、また、セキュリティで保護されていないエンドポイントを適切に管理することも不可能です。これが、エンドポイント管理とセキュリティの統合ソリューションが求められる理由です。ただし、理由はこれだけではありません。他にも重要な理由があります。

複数のスイート製品や専用製品で構成される管理およびセキュリティ ソフトウェア アプリケーションを使用すると、エンドポイントでコンフリクトの原因となり、場合によっては、

あるエージェントが別のエージェントを無効化することもあります。たとえば、アンチウイルス エージェントが原因でパッチ エージェントが無効になり、セキュリティ パッチが適用されないことがあります。このようなコンフリクトは、ダウンタイムが発生したりエンドポイントが不必要なリスクにさらされる原因になりかねません。個々のセキュリティおよび管理製品が統合されていないと、各レベルでエンドポイントを適切にセキュリティ保護し、あらゆる攻撃手法から防御するための組織の取り組みが無駄になる可能性があります。

さらに、個別の管理用ソリューションとセキュリティ ソリューションを展開すると、エンドポイント上でソリューション別のエージェントを複数実行することになり、エンドポイントのセキュリティ保護と管理を行う単一のエージェントを実行する場合よりも、メモリや電力の消費が増えてしまいます。

トレーニングおよび IT スキルの問題としては、個別のセキュリティ ソリューションと管理用ソリューションを使用すると追加のトレーニングが必要となり、IT 担当者がスキルを身に付けるまでの時間が増えてしまいます。一方、エンドポイント管理とセキュリティの統合ソリューションで単一のユーザー インタフェースと管理コンソールを使用できれば、IT 担当者のトレーニングに要する時間とコストを低減することができます。クロストレーニングを行うこともできます。

また、エンドポイントのセキュリティ保護と管理の統合アプローチを導入すると、その他のコストや複雑性も大幅に改善されます。たとえば、複数の専用ソリューションや未統合の管理用ソリューションおよびセキュリティ スイートを追加しながら展開していくと、一般的にコストがかさむだけでなく、インフラストラクチャが散乱して管理や保守がより難しくなります。また、ソリューションごとのコストが重複する可能性もあります。

LANDesk は単一のエージェントに依存する、システムのライフサイクル管理とエンドポイントのセキュリティ管理機能を、使いやすい単一の共通コンソールで提供しており、企業に展開しているシステム全体を検出、管理、更新、保護することができます。エンドポイントのセキュリティ保護および管理用の統合プラットフォームは、組織の要件の拡大に伴い、特定のソリューションやソリューション群を段階的に導入することができます。

LANDesk は、組織が今日の複雑かつ変化を繰り返す脅威に対抗するために必要なセキュリティおよび管理機能を提供します。組織は環境内のエンドポイントのセキュリティ保護を強化できるだけでなく、管理を合理化しコストを削減して、ビジネスを成長させることができます。

参考文献

1. “Kido Worm Keeps On Truckin’ via USB Thumb Drives”, Chris Maxcer, *TechNews World*, January 16, 2009

詳細は www.landesk.co.jp をご覧ください。

本情報はアボセント社LANDesk製品に関連して提供しているものです。明示されているか否かに関わらず、また禁反言によらずにかかわらず、いかなる知的財産権のライセンスも、本資料によって許諾するものではありません。アボセントは本資料の内容に誤りがないことを保証するものではなく、またLANDeskはいつでも、予告なしに、本資料の内容または関連製品の仕様、製品に関する記述を変更することがあります。最新の製品情報はwww.landesk.co.jpをご参照ください。

Copyright © 2009, Avocent Corporation. All rights reserved. Avocent, LANDeskおよびAvocentのロゴは、米国および/または他国におけるAvocent Corporationまたは子会社または関連会社の登録商標または商標です。その他のブランド名や名称は各社の所有物です。個々のお客様の結果はそれぞれの実態と環境により異なる場合があります。 LSI-0832UK 06/09 KB/BB/NH

