

セキュリティ成熟段階の実現

エンドポイント セキュリティを実現するためのレイヤ化されたアプローチ

適用される法により認められる最大の範囲において、LANDesk はいかなる責任も負いません。また、特定目的への適合性、市場性、特許、著作権あるいはその他の知的財産権（著作権で保護される権利に限定されない）を侵害しないことに関する責任または保証を含む LANDesk 製品の販売および使用に関する明示または黙示の保証を放棄します。

LANDesk は、本書および関連する製品の仕様および説明書をいつでも予告なしに変更する権利を保有します。LANDesk は、本書の使用に関する保証を行わず、本書に発生しうるいかなる間違いの責務を負わないことを前提とし、ここに記載されている情報を更新する責務を負いません。最新の製品情報については、www.landesk.com をご覧ください。

Copyright © 2011, LANDesk Software, Inc. and its affiliates. All rights reserved. LANDesk およびそのロゴ は、米国およびその他の国における LANDesk Software, Inc. またはその関連会社の登録商標または商標です。その他のブランドおよび名称は、それぞれの所有者に帰属します。

LSI-0909 03/11 BB/AZUU

内容

要旨	4
複雑化する IT セキュリティ環境において求められる成熟したセキュリティ管理	4
成熟度の高い体系的なセキュリティ管理アプローチ	5
レベル 1:強力な周辺防御環境の構築と資産インテリジェンスの開始	5
LANDesk のアプローチ:	6
レベル 2:インテリジェンスと体系的な修正能力の強化による積極的なセキュリティ機能の導入	7
LANDesk のアプローチ:	8
レベル 3:重要なデータの保護	9
LANDesk のアプローチ:	10
レベル 4:セキュリティ プロセスの最適化	11
LANDesk のアプローチ:	11
セキュリティ成熟度モデルの上位段階を目指す方法の簡素化	12

要旨

マルウェア犯罪は革新性を高め、その対応にはますます経費がかかるようになってきました。脅威は急速に進化し続けています。独自のマルウェアの数は増加の一途をたどっていますが、Web ベースのマルウェアが占める割合が拡大しています。IT 部門は防御機能の数を増やすことによってサイバー攻撃やデータ損失に対応しています。この理由としては、データ保護が複雑化しているということだけではなく、機密顧客データを紛失した場合にはその事実を公表しなければならないため企業の評価が低下する事態を避けたいという狙いがあります。

セキュリティ強化に向けた取り組みを行っている企業は敏感に反応し、安全性を高める製品ではなく、安全であると感じられる 1 つの機能しか提供しない製品を購入する可能性があります。このような企業は本質的に敏感に対応する傾向がありますが、多くの企業における現状がこれに当てはまります。問題は、高度な攻撃が蔓延する時代において、単に敏感に反応するだけではもはや不十分であるということです。成熟度の高いセキュリティ システムと対策を導入している企業は、セキュリティについてより積極的に対応できます。積極的な対応とは、複数レイヤから構成される積極的な統合型技術を導入し、ネットワーク違反を困難にすることです。次の表には、敏感に反応する企業の傾向と積極性と成熟度の高い

IT セキュリティを導入している企業の傾向について示します。:

消極的な対応の企業	積極的な対応の企業
<ul style="list-style-type: none"> 低レベルのセキュリティ 複数のポイントソリューション IT資源の非能率的な使用 手動での脅威の緩和 ITセキュリティが全セキュリティプロセスを管理 	<ul style="list-style-type: none"> 複数レイヤのセキュリティ 統合セキュリティソリューション 最低限のステップに減らされたプロセス 自動的な脅威の緩和 IT運用は既知のセキュリティプロセスを管理し、ITセキュリティは脅威の監視と調査を継続

レイヤ化されたセキュリティを実現する上で、LANDesk は各レイヤを簡素化するというアプローチを取っています。LANDesk のセキュリティの基盤は、LANDesk® Management Suite が備える包括的なハードウェアおよびソフトウェア管理機能です。これにより、企業は密接に統合されたセキュリティ機能を論理的かつ段階的な方法で追加し、同じクライアント側のソフトウェア エージェント、サーバインフラストラクチャおよび管理コンソールを活用できます。これらの機能には、マルウェア対策、デバイスとアプリケーション

の管理、データ保護、アプリケーションのホワイトリスト、ファイアウォール、ホスト侵入防止 (HIPS)、ネットワーク アクセス管理 (802.1x) および包括的なパッチ管理が含まれています。新しい防御機能強化コンポーネントはそれぞれ共通の管理プラットフォームに統合され、一元化された連携アプリケーションとして動作します。

このホワイトペーパーでは、セキュリティ管理を実施する上で成熟したレイヤ化アプローチが必要である理由と、LANDesk を導入してレイヤ化されたアプローチのニーズに対応する方法について説明します。

複雑化する IT セキュリティ環境において求められる成熟したセキュリティ管理

より回復力の高いエンドポイント セキュリティのニーズが高まっています。現在の IT に対する脅威の環境は、多数のデスクトップとモバイル ノートブック PC の安全の確保に努めている IT 部門に対してきわめて困難な課題を突き付けています。さらに、モバイル デバイスを使用して企業リソースにアクセスするモバイル従業員の数が増えているため、IT セキュリティにおいてユーザの場所とユーザがファイアウォールの内部にいるのか外部にいるのかを考慮することがますます重要になっています。重大なセキュリティ違反が発生した場合の財務的な影響は多大です。脆弱性と攻撃の方向性の展望は常に変化しさらには進化しています。現在の脅威環境はきわめてダイナミックであるため、1 つの機能のみを提供するソリューションでは効果的な保護機能を実現できません。

部門が日々直面する脅威の拡大を考えてみてください。:

- OS のセキュリティが強化されたため、攻撃の戦略はアプリケーションの脆弱性を利用するという方法に集中しています。たとえば、ブラウザ、オフィス生産性ツール、メディア プレイヤー、バックアップ ソフトウェア、スマートフォン、iPad などの脆弱性が狙われています。ときにはセキュリティ ソフトウェアさえもターゲットになる場合があります。通常、このような攻撃の目的はボットネットを探すことです。
- Web ベースの攻撃は劇的に増加しました。このような攻撃には、フィッシング詐欺だけではなく、欠陥のある信頼できるサイトから実行される攻撃も含まれます。通常、これらは独自のコードによりアクセス ユーザを攻撃し、署名ベースのセキュリティを回避します。
- 現在、情報窃盗は多国籍犯罪組織が中心となって行っています。多くの企業ネットワーク侵入は、個人情報と知的財産を盗むための攻撃であり、企業の内外から実行されます。通常、このような攻撃は侵入者が去ってからしばらくたった後に検出されます。

- データの紛失の範囲と量は拡大しています。ノートブック PC はもっとも一般的ですが、リムーバブル大容量記憶装置 (特に至るところに存在し容易に隠すことができる USB ドライブ) や一時的なワイヤレス ネットワーク ブリッジも急速に一般化しています。
- マルウェア革新は加速し続けています。

また、企業内の IT セキュリティ チームと IT 運用チームの間の協力と連携を強化する必要があります。多くの場合、企業内のこれらの 2 つの IT グループは衝突しています。IT セキュリティ チームはリスクと脅威、ポリシーの定義、環境の評価について懸念しています。一方、IT 運用チームはサーバ管理、ネットワーク管理、デスクトップ管理といった領域に集中し、可用性とパフォーマンス、環境の安定性の維持、変更管理、可用性とパフォーマンスの阻害要因の排除について懸念しています。

通常、IT セキュリティ チームは、攻撃や脅威に対してポリシーを適用し、新しい技術を推奨して迅速に導入します。場合によっては、管理やパフォーマンスの問題につながる可能性のある技術を環境に強制的に導入します。IT 運用チームはインターフェース、管理、レポート、ワークフローを統合し、可用性とパフォーマンスを外部から阻害しない技術を求めています。

ワシントン郊外で開かれた 2010 年 Gartner セキュリティ・リスク管理サミットの IT セキュリティと IT 運用統合ベスト プラクティス セッションで、副社長兼上級アナリストの Mark Nicolett 氏が次のように述べました。

「情報セキュリティ脅威と脅威を処理する技術は成熟期に達しているため、このような活動は IT 部門の運用側に任せるべきです。情報セキュリティ部門は出現する新しい脅威と技術に集中する必要があります。このためには、情報セキュリティ チームはより日常的で一般的な脅威保護技術を手放す必要があります。もっともわかりやすい例は、ウイルス (脅威) とウイルス対策 (保護) 技術です。これらは成熟した技術として認識されています。デスクトップ運用グループはウイルス対策ソフトウェアと署名更新に対応する必要があります。情報セキュリティ チームはポリシーを設定できますが、実行するのは運用チームです。もう 1 つの例として、パッチ管理があります。パッチ管理はソフトウェア配布と統合する必要があります。なぜ 2 つのグループと 2 つのプロセスがパッチ管理を別々に実行しているのでしょうか。このことは、情報セキュリティと運用が 1 つにまとまっていることを意味しているわけではありません。むしろ、それぞれのチームが得意としてい

ることに集中しています。運用チームは何も変更したくはありません。セキュリティ脅威が関連してくる場合、この対応は必ずしも正しい方法ではありません。

情報セキュリティ チームには得意としていることに集中させ、新しい脅威に効果的に対応させましょう。IT 運用チームには得意としていることに集中させ、成熟したシステムを効率的に運用させましょう。」¹

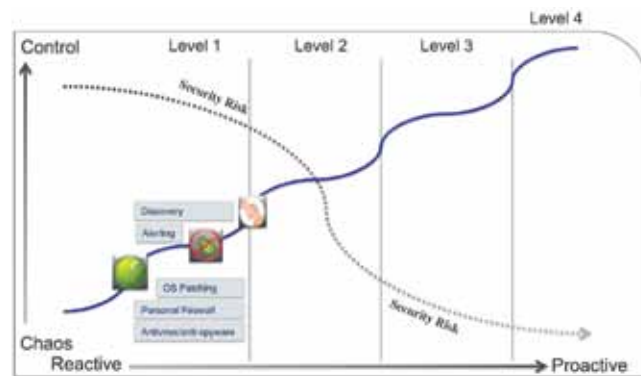
より成熟度の高いセキュリティ ソリューションを推進するために、IT セキュリティ チームには次の選択肢が与えられています。1 つの機能のみを提供するソリューションをいくつも導入し続け、このようなソリューションを個別に管理するか、IT 運用チームに管理させることができます。1 つの機能のみを提供するソリューションをいくつも導入し、より包括的なセキュリティ ソリューションが見つかったときに置き換えることができます。あるいは、IT 運用のエンドポイント デバイス管理ワークフローと連携するソリューションを見つけ、複数レイヤで統合セキュリティを活用できます。

成熟度の高い体系的なセキュリティ管理アプローチ

セキュリティの成熟段階に到達するまでには、さまざまなレイヤ化されたエンドポイント保護、管理、防御機能が必要です。そして、それぞれが統合され、完全に自動運用に対応していなければなりません。

レベル 1: 強力な周辺防御環境の構築と資産インテリジェンスの開始

次の図に示すように、セキュリティ構築の最初のステップは、環境内にあるソフトウェアとハードウェアを把握することです。マルウェア攻撃に対する最初の防御壁を構築し、すべての稼働中のシステムには常に最新のパッチを適用するとともに、選択した時点でのセキュリティ ステータスを示すレポートを作成します。



エンドポイントセキュリティ成熟度カーブ

¹ Mark Nicolett, "2010 Gartner Security & Risk Management Summit, National Harbor, MD, "Best Practices in IT Security and IT Operations Integration" session speaker notes, slide 4.

資産の検出とインベントリまた、接続しているデバイスとデバイスで実行されているソフトウェアを把握せずにネットワークのセキュリティを保証することはできないため、管理するデバイスだけではなく、ネットワークに接続するすべてのデバイスを確認することも重要です。このためには、資産が本社サイトにあるかリモート サイトにあるかに関係なく、企業ネットワーク全体で資産を検出し、インベントリをリアルタイムで管理する機能が必要です。

マルウェア保護

セキュリティのベースラインとして、ウィルス対策やスパイウェア対策などのマルウェア対策ソフトウェアを導入して、特定の脅威をブロックしたり、企業を脅威から保護したりする必要があります。これらのセキュリティ アプリケーションは、新しいマルウェア パターンによって継続的に更新されるため、既知の攻撃をブロックできます。ただし、膨大な数の新しい脅威が出現しているため、ブラックリストはそれほど効果的ではなくなっています。的を絞った脅威についてはほとんど役に立ちません。

結果として、多くの企業がアプリケーション管理やホワイトリストに基づく非署名ベースのソリューションを使用してセキュリティを強化することで、特定のアプリケーションを除くすべてをブロックしたり、未承認のアプリケーションの使用をブロックしたりできます。また、悪意のあるコードに対する防御機能には、積極的に更新され、一元的に管理される従来の署名ベースのウィルス対策やスパイウェア対策保護などのコンポーネントを含める必要があります。これはマルウェア署名が認識されない場合であっても、不正なコード実行のブロック、バッファオーバーフロー エクスプロイトの防止、異常なアプリケーション動作の検出が可能なホスト侵入防止ソリューション (HIPS) と組み合わせる必要があります。

パーソナル ファイアウォール

保護を強化するために、IT 管理者はパーソナル ファイアウォール採用し、特定の送受信接続をブロックする必要があります。最も効果的なファイアウォールは、コンピュータが信頼できるネットワークに接続しているか、信頼できないネットワークに接続しているかどうかによって、ブロック処理を動的に変化させ、ファイアウォール違反が発生した場合には、アラートの発行やログの出力を行うことができます。一部のファイアウォールはさらに充実しており、ネットワークにアクセス可能なアプリケーションとアクセス方法も制限します。

通常、エンド ユーザ向けのファイアウォールは保護されたネットワークと保護されていないネットワークの間に置かれます。ファイアウォールは資産を保護するゲートのように動作し、個人情報が送信されず、悪意のあるアクセスがないことを保証します。パーソナル ファイアウォールを設定することで、

送受信接続を許可または拒否し、違反が発生した場合には IT 部門にアラートを送信してその内容を記録できます。一部のファイアウォールは、ユーザが信頼できるサイトにいるか信頼できないサイトにいるかどうかによってポリシーを変えることができます。ファイアウォールはアプリケーションの制御やブロックを行い、企業にとってのリスクを最小限に抑えることもできます。

オペレーティング システム パッチ管理

OS の脆弱性に関連するセキュリティ リスクを低減するためには、Microsoft Windows などのオペレーティング システムに適用されるパッチ プログラムを管理することがきわめて重要です。ネットワーク上に存在するものを認識するために重要なのは、検出とインベントリです。次に、ポリシーを確立して、特定のオペレーティング システムに対してパッチを自動的にインストールできます。また、新しいパッチが提供された時点で自動的にダウンロードしてインストールすることで、作業時間とリスクを削減できます。

LANDesk のアプローチ:

資産の検出とインベントリについては、LANDesk Management Suite ユーザは、サブネット レベルのリアルタイム検出技術に慣れています。この技術はコンピュータ資産の特定、検索、一覧表の作成を行うとともに、資産の構成と管理ステータスを評価して、ローカル ファイアウォールが有効になっているかどうかを判断します。インターネット経由で VPN を使用せずに、分散したリモート サイトのシステムにもアクセスできます。LANDesk Security Suite はワイヤレス アクセス ポイント検出ソリューションによってこのような機能を拡張しています。ワイヤレス アクセス ポイント検出ソリューションはノートブック PC のワイヤレス NIC を使用して、企業環境内またはそれに隣接したすべてのアクセス ポイントの検出と分類を実行するため、管理者はアクセス ポイントへの不正な接続をブロックできます。

LANDesk のソリューションでは、2 つの方法でマルウェアに対する保護を簡素化できます。LANDesk マルウェア ソリューションを使用するか、1 つの LANDesk コンソールでサードパーティ製のウィルス対策およびスパイウェア対策単体製品を管理できます。世界最高レベルの LANDesk® Antivirus ソリューションを使用する場合、マルウェア保護機能は LANDesk Management Suite と LANDesk Security Suite に統合されます。処理は 1 つのエージェントにより簡素化され、すべてのセキュリティ アクティビティを 1 つのコンソールで確認できます。

LANDesk Antivirus は Kaspersky Labs エンジンと署名データベースに基づいて実行され、ウィルス、ワーム、トロイの木馬、スパイウェア、ルートキットなどの悪意のあるコード

に対する優れた保護を提供します。さらに、1 時間間隔で業界で最も完全な脅威署名データベースの更新が提供されます。Kaspersky Labs のスピードと増分パターン ファイル更新を特許取得済みの LANDesk 配布技術と組み合わせることで、クライアントを更新する際の手間が軽減されます。しかも、ネットワークへの悪影響はありません。

LANDesk はメール サーバ向けのウイルス対策ソリューションも提供します。LANDesk® Antivirus – Mail Server ソリューションはエンドポイント セキュリティの保護レイヤをさらに 1 段階追加し、外部の脅威から企業メール サーバを保護します。さらに、企業ネットワーク内におけるウイルスの発生を防止し、未承諾メールを除外します。このソリューションの主要な目的は、悪意のあるプログラムから Microsoft Exchange Server 上のメールボックス、公開フォルダ、中継された電子メールを保護することです。メールボックスと公開フォルダにある電子メールトラフィックとメッセージをスキャンし、最新バージョンの署名データベースにある情報を使用して感染しているオブジェクトを修復することで、この保護機能が実行されます。

管理コンソールのボタンを選択するだけで LANDesk Antivirus ソフトウェアを選択できます。以前にインストールしたウイルス対策アプリケーションの削除から、すべてのコンピュータへの LANDesk Antivirus のプッシュ配信まで、残りの処理はすべて LANDesk が実行します。

他社のウイルス対策単体製品を保持または新規で導入する場合は、LANDesk 統合管理コンソールから直接 LANDesk Security Suite が他社 (CA、ESET、Kaspersky Lab、McAfee、Sophos、Symantec、Trend Micro) のウイルス対策製品を管理します。ユーザー側で組織を保護する最適な方法を自由に決定できます。LANDesk はその計画をサポートします。

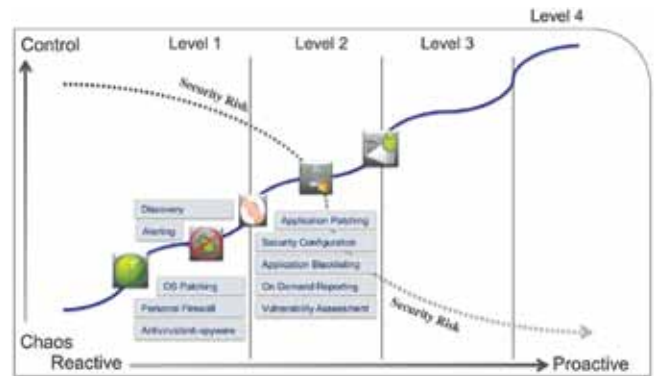
LANDesk エンドポイント パーソナル ファイアウォールは、許可されたネットワークまたは IP アドレスへのアクセスを制限することで、システム保護を強化し、効果的なシステム攻撃の可能性を大幅に抑えます。簡素化の観点から、複数のコンソールや複数のエージェントを導入する必要はなく、異なる単体製品をサポートする経費を削減できます。LANDesk Security Suite のファイアウォール技術では、一元化された方法で管理することで、アプリケーションの制御とファイアウォールの設定を実行できます。IT 管理者は送受信接続を許可または拒否し、ファイアウォール違反があった場合にはアラートを送信し、その内容をログに出力できます。LANDesk ロケーション認識ポリシーは、データ紛失と感染の可能性を低減できるように支援します。特定のコンピ

ュータが存在する環境に基づいて、アプリケーション制御、マルウェア対策設定、リムーバブル記憶装置の制約などセキュリティ設定を調整するダイナミックなポリシーを使用します。

管理者は LANDesk Security Suite を使用することで、管理コンソールから直接 Windows ファイアウォールも一元的に有効化したり設定したりできます。有線の場合もワイヤレスの場合も、保護されていないコンピュータを容易に特定できます。また、1 つの設定を使用して標準化したり、別のユーザーグループ用にカスタマイズしたりできます。

レベル 2:インテリジェンスと体系的な修正能力の強化による積極的なセキュリティ機能の導入

セキュリティ基盤が構築されると、IT 部門は脆弱性評価、アプリケーションのパッチ適用、ホワイトリストおよびアプリケーション制御によって、より積極的な方法を探ります。



エンドポイントセキュリティ成熟度カーブ

脆弱性評価

脆弱性はデバイスの全体的なセキュリティにおける弱点です。脅威はこのような弱点につけ込み、コンピュータや個人データに潜在的な被害を及ぼします。

企業の IT 部門は環境における脆弱性を評価し、企業資産を保護するための対策を決定する必要があります。IT 担当者が組織内におけるユーザー ロールと IT 環境に合わせたセキュリティ ポリシーを設定した時点で、潜在的なセキュリティ欠陥があるかどうかを評価し、違反が発生する前に欠陥を修正します。

アプリケーションのパッチ適用

アプリケーション セキュリティ パッチを使用して最新の状態を保つことは、IT 部門における最も複雑で時間がかかる作業の 1 つです。スキャン、脆弱性評価、修正、ダウンロードとステージング、メンテナンス機能が含まれている強力なパッチ管理ソリューションが欠かせません。メンテナンス機能は、Microsoft Windows や Office アプリケーションだけ

ではなく、ますます頻繁に使用される Microsoft 以外のブラウザやアプリケーション、メディア プレイヤー、バックアップソフトウェア、セキュリティソフトウェアにまで対応していなければなりません。

ホワイトリストとアプリケーション制御

セキュリティ エクスペリエンスに優れ成熟度が高い企業はブラックリストだけでは効果がないことを認識しています。このため、ブラックリスト、ファイアウォール、侵入検出システム (IDS)、ウイルス対策ソフトウェアを組み合わせるようになってきました。これらのすべての対策は必要ですが、脅威が進化し続けることや攻撃の対象がさまざまであることを考えるとこれだけでは不適切です。そのため、企業はホワイトリストを採用して、許可されているアプリケーションと接続を定義し、残りのものをブロックしなければなりません。ホワイトリストを正しく設定すると、ブラックリストやウイルス対策アプリケーションを使用する必要性が少なくなります。

Gartner は次のように報告しています。

「新しい脅威の数が圧倒的に増える中で、標準的なマルウェア対策署名エンジンは急速にその効果を失い、価値はほとんどありません。PC に不明な脅威に対する予防策を講じるには、非署名ベースのソリューション (ホストベースの侵入防止システム - HIPS など) と優れた運用方法 (資産検出、構成管理、脆弱性評価、ソフトウェア管理、ホワイトリストなど) が必要です。²

LANDesk Security Suite はホワイトリスト戦略の導入を容易にします。まず、ホワイトリストを設定して既存のアプリケーション動作から学習します。次に、既存のアプリケーションで許可されるものを規定し、環境に感染被害を及ぼすマルウェアを含む可能性がある他のアプリケーションをブロックするためのポリシーを設定します。LANDesk ロケーション認識機能を使用して信頼できるネットワークと信頼できないネットワークを定義して、企業全体のポリシーを設定できます。これらのポリシーはすべて IT 管理者のコンソール上に一元的に表示されます。ロケーション認識ポリシーの定義機能によって、企業内の制御を緩めたり、セキュリティ ポリシーを厳しくしたりできます。

多くの IT 部門はエンドポイント セキュリティの一部として、ホストベースの侵入防止 (HIPS) 技術を使用する利点を認識しています。HIPS 技術はファイアウォール、サンドボックス、さまざまなシステムレベル処理のアプリケーション制御を統合します。この技術は信頼できない環境 (ホテルの Wi-Fi ネットワークなど) でノートブック PC を保護する際に便利です。また、不正なアプリケーションが悪意のある処

理を実行できないように防止します。HIPS 機能が不審な動作を検出すると、その動作を防止するだけでなく、アラートを発行してその問題を IT 管理者に通知します。

バッファオーバーフロー保護は HIPS の重要なコンポーネントとなりました。この機能は、ユーザ入力を待機しているプログラムを利用するエクスプロイトから環境を保護します。バッファオーバーフロー保護はスタック割り当てまたはヒープ割り当て変数のバッファオーバーフローが発生したときにそれを検出し、重大なセキュリティ脆弱性にならないように防止することで、実行可能プログラムのセキュリティを強化します。

2009 年 9 月の SANS Institute の報告書によると、オペレーティング システムは多くの攻撃のターゲットとなっています。

依然としてオペレーティング システムには、大量のインターネット ワームにつながる、リモートで利用される脆弱性はほとんどありません。

報告期間中には、Conficker/Downadup 以外には、OS をターゲットとした新しい主要ワームはありませんでした。たとえそうであっても、5 月と 6 月の 2 ヶ月と 7 月から 8 月の 2 ヶ月を比較すると、Windows におけるバッファオーバーフロー脆弱性を利用した攻撃の数は 3 倍となり、Windows オペレーティング システムに対する攻撃に占める割合は 90% を超えていました。³

LANDesk のアプローチ:

LANDesk Security Suite は、セキュリティの成熟度をより積極的に高めようとする IT 部門の取り組みを簡素化します。このソリューションは高頻度で実行される標準脆弱性評価スキャン機能を備えているため、構成、バッチ適用、ソフトウェア更新要件を迅速かつ容易に特定できます。カスタム スキャンを設定することで、特定の条件セットを検索する際の詳細レベルを定義できます。ルールベースの管理ツールとポリシーベースの管理ツールを使用することで、安全な構成を簡単な方法で定義およびメンテナンスできます。

LANDesk は最も広範囲にわたり多数のアプリケーションの脆弱性評価を実行するため、潜在的なリスクを確認して、企業標準を満たしているかどうかを判断できます。企業が次のような基準に準拠することが求められている場合、この点は特に重要です。

- PCI – 決済カード業界基準
- FDCC – 連邦政府デスクトップ コンピュータ基準
- SCAP – セキュリティ設定共通化手順

² Peter Firstbrook, Arabella Hallawell, John Girard, Neil MacDonald. "Magic Quadrant for Endpoint Protection Platforms"; Gartner, Inc., May 4, 2009, p. 2

³ "The Top Cyber Security Risks", SANS Institute, September 2009; <http://www.sans.org/top-cyber-security-risks/>

- FISMA – 連邦情報セキュリティ マネジメント法
- HIPAA – 医療保険の相互運用性と説明責任に関する法律

LANDesk インテリジェント パッチ管理は LANDesk Security Suite の一部であり、異種混合 IT 環境におけるオペレーティング システムとアプリケーション向けの統合脆弱性評価、パッチ調査、ダウンロード、ステージング、配布機能を提供します。パッチ ソリューションは各種 Windows オペレーティング システム、Macintosh オペレーティング システム、Linux オペレーティング システムに対応します。

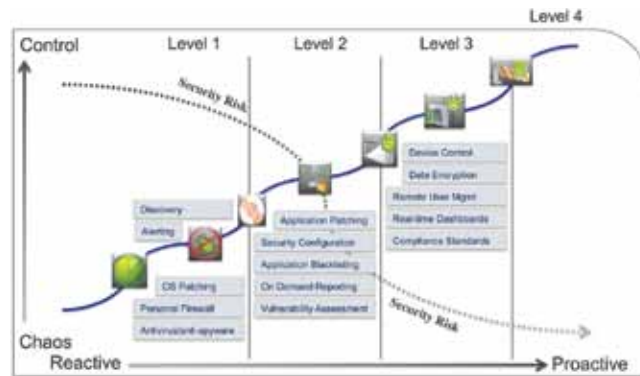
LANDesk® Targeted Multicast™ および LANDesk® Peer Download™ 技術は配置を加速化し、配布時の帯域幅要件を低減します。追加ハードウェアやルータの再構成は不要です。たとえば、ある大手多国籍企業がわずか 5 台のサーバを使用して、世界中で 77,000 を超えるノードに対してパッチを配置しています。この企業は 5 日以内で 95% を超える修正率を達成しています。別の企業は 2010 年 2 月だけでも 118,000 ノードに対して 846,000 を超えるパッチを送信し、95% の成功率を達成しています。

配置を自動化し、パッチを配布先のコンピュータのキャッシュに保存することで、その後の認証とインストールが可能で、また、LANDesk® Process Manager の自動パッチ配布機能が含まれているため、継続中の完全に自動化された更新処理に合わせて新しいパッチを設定し、修正可能なワークフロー、自動承認、パイロット グループを利用できます。

LANDesk Security Suite の機能である LANDesk® Host Intrusion Prevention (HIPS) は、さまざまな非署名ベースの悪意のあるコードを防止し、アプリケーションを管理するためのアプリケーション制御機能を提供します。ウィルス対策およびスパイウェア対策システムを補完するとともに、マルウェア パターンが利用できないゼロデイ エクスプロイトに対する保護を提供します。実証済みの動作認識技術により、悪意のある活動がブロックされます。LANDesk HIPS はシステムで実行されるアプリケーションを制御するための強力なツールであり、許可されたアプリケーションが実行できる動作を規定します。

レベル 3:重要なデータの保護

企業セキュリティ ポリシーと規制要件に準拠するためには、企業の機密情報と個人情報（従業員情報と顧客情報の両方）のセキュリティを確保するためにできる取り組みを実施しなければなりません。この第 3 段階のセキュリティ成熟レベルでは、データを暗号化し、エンド ユーザのポリシーを設定して適用することがきわめて重要です。



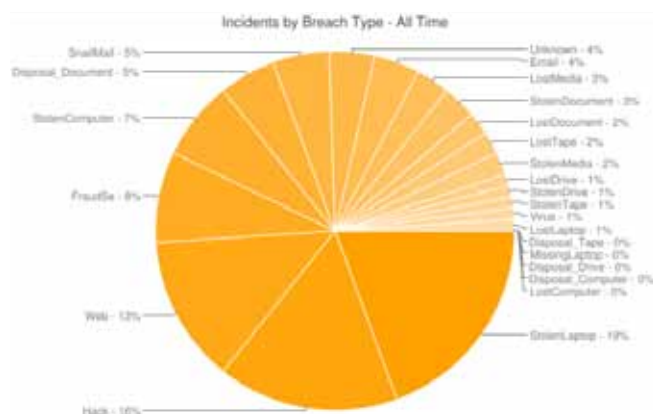
エンドポイントセキュリティ成熟度カーブ

デバイス管理とデータ損失防止

IT 部門は企業の機密情報ポリシーを設定し、ポリシー違反とデータ漏洩の可能性を容易に特定しなければなりません。IT 部門が高リスクのアクション（企業機密情報ファイルのコピーなど）をブロックし、ディスクドライブへのユーザー アクセスと通信チャンネルを制御してデータ窃盗を防止できるとさらに効果的です。

データの暗号化

リムーバブル大容量記憶装置とコンパクト メディアにより機密情報のコピー、移動、隠蔽が容易になりましたが、同時にこのようなデバイスはマルウェアを拡大させるための便利なツールとなりました。個人を特定できる情報の損失、窃盗あるいは公開に関するインシデント情報を収集している Open Security Foundation の DataLossDB によると、データ損失インシデントの約 3 分の 1 がコンピュータ、ノートブック PC、ドライブおよびメディアの紛失や盗難に起因しています。



出典: DataLossDB.org

データセキュリティを保証するためには、たとえ正式なアクセス権を持つユーザの場合であっても、データの移動時にはポリシーベースの制御を実施する必要があります。また、有線ネットワーク上のユーザが安全ではないネットワークに接続して、IT 環境の外部にデータを転送できないようにする必要があります。

暗号化については、個々のユーザのみが参照すべき情報（社会保障データなど）を保護するユーザ データ暗号化、USB や iPod などの外部記憶装置を暗号化する外部メディア暗号化、システム データ暗号化などさまざまな形式があります。

モバイル ユーザとリモート ユーザ

ユーザが本社にいるか、リモート オフィスにいるか、あるいは一時的に外出しているかに関係なく、IT 部門はハードウェアおよびソフトウェア インベントリの収集、脆弱性の評価、そしてリスク懸案事項の修正を行いたいと考えています。目標はユーザの生産性を維持しながらネットワークの安全性を確保することです。たとえば、外出後に企業ネットワークに再接続するユーザをロックすることなく、再接続時にアプリケーションとオペレーティング システムを更新するといった運用が必要です。安全な環境を維持する上で非常に重要なことは、企業ファイアウォール外部にいるユーザ向けにウィルス対策の適用、管理、アプリケーションのブロックを実行する能力を備えていることです。

継続的なデータ セキュリティ基準の準拠

一般的に、PCI（決済カード業界基準）、SCAP（セキュリティ設定共通化手順）、FDCC（連邦政府デスクトップ コンピュータ基準）などの規制準拠は企業にとって重荷であり、セキュリティ上の価値はほとんどないと考えられています。しかし実際には、このような基準に準拠することで企業のセキュリティ状態が改善されます。企業は最も一般的なベスト プラクティスに従い、基準がなければ見落とされていた可能性のある不一致点を修正することを要求されているためです。

たとえば、多くの規制基準は大文字、小文字、数字および記号を組み合わせ、ユーザの名前を含まない 8 文字以上の強力なパスワードを設定するように義務付けています。したがって、「steve」などのパスワードは容易に推測可能であるため拒否されます。逆に、「\$teVe136」というパスワードは許可され、セキュリティ違反を許す脆弱性の要因となる可能性が低くなります。このような強力なパスワードは Conficker/Kido ワームによるコンピュータの選択を防止します。

このような基準に準拠することは、企業のセキュリティ成熟度を示す指標です。また、セキュリティ領域のベスト プラクティスの指針や IT 環境の確認方法を理解できるようになります。ユーザと顧客データの保護が可能になります。

リアルタイムのダッシュボード (レイヤ ビュー)

受信する情報を管理できるダッシュボードを導入すると、問題を容易に認識できます。また、企業環境に合わせてダッシュボードをカスタマイズできると、セキュリティ管理が一層容易になり、管理者の信頼が高まります。

LANDesk のアプローチ:

LANDesk Security Suite のもう 1 つの技術であるデバイス管理マネージャを使用すると、デバイス管理とデータ損失防止ポリシーを設定できるため、ポリシー違反とデータ漏洩の可能性を容易に特定できます。デバイス管理マネージャはリムーバブル メディアにコピーされたファイルを記録し、シャドー コピーも保持します。コピー処理の内容とアクションをブロックしているデバイスを同じアクティビティ ウィンドウから確認できます。ディスク ドライブへのユーザ アクセス、通信方法、ポートおよびモデルを管理し、盗難や怠慢によるデータ損失を未然に防止します。新しい機能として、すべての許可されたデータの暗号化を実施して、USB スティックなどのポータブル デバイスにファイルを転送できます。

LANDesk が提供する CREDANT データ暗号化は、ファイル・フォルダベースの暗号化製品によってセキュリティ上の不一致を解決します。同時に、管理、データ回復、セキュリティおよびディスク全体の暗号化またはハード ディスク暗号化ソリューションに関連する生産性上の問題を回避します。LANDesk 管理ツールを使用すると、強力なデータ暗号化技術をすべてのエンドポイントに迅速に配布するとともに、ユーザ データ、アプリケーション データ、USB スティックなどの外部メディア、iPods、SD カードなどを暗号化できます。また、不正ユーザ アクセスからデータを保護し、他の暗号化レイヤによって保護されないデータも守ります。

LANDesk® Management Gateway Appliance を使用すると、LANDesk Security Suite の機能は企業ファイアウォール外部にも拡大できます。LANDesk® Management Gateway Appliance はプラグイン型のデバイスであり、既存のインターネット接続、証明書ベースの認証、SSL 暗号化を使用してモバイル ユーザを簡単に安全な方法で管理できます。このアプライアンスにより、モバイル ユーザが外出時にはパッチ、ウィルス対策署名およびその他の設定更新をシームレスに受信し、企業ネットワークに戻ったときに既にセキュリティ ポリシーに準拠していることを保証できます。このゲートウェイ技術により、VPN、

専用回線、ローカル管理サーバが不要になり、ユーザのスケジュールではなく自分のスケジュールに合わせてリモートコンピュータを一元的な方法で積極的に管理できます。LANDesk Management Gateway Appliance を使用すると、ファイアウォールに穴を開けずに、時間や場所に関係なくシステムを管理できます。また、自動冗長バックアップも含まれているため、設定およびログ情報をいつでも利用できます。

LANDesk Security Suite を導入することで、包括的な評価を実施し、PCI、FDCC、SCAP、SOX などの基準への準拠を保証できます。

また、トレンド グラフ、セキュリティ ポリシー レポート、スパイウェア レポートなどのさまざまな強力なレポート機能により、セキュリティ活動の追跡と文書化が容易になります。ポリシー実施とパッチ配置に関する詳細な履歴レポートがグラフィカルに表示され、ポリシー、パフォーマンス、問題領域、経時的なトレンドがわかりやすく示されます。特定の PCI、FDCC、SCAP、HIPAA、SOX 規制への準拠状況の監査においては、この種の準拠レポートが義務付けられます。

レベル 4:セキュリティ プロセスの最適化

最初の 3 つのレベルのセキュリティが実施されると、企業基準と規制基準に準拠し、新しい脆弱性と新しいモードのマルウェア攻撃を調査できるようになるため、IT 部門はより積極的になります。最後のステップには、確認された攻撃に基づくポリシーの改善、最小限の手順でセキュリティを維持するためのプロセスの自動化、ホワイトリストと HIPS の使用、ロケーションベースのポリシーと権限ロックなどの安全な設定を維持するための高度な方法の使用があります。



エンドポイントセキュリティ成熟度カーブ

ポリシーと設定の改善

企業ポリシーまたは規制への準拠を保証する最もよい方法の 1 つは、外部の攻撃であるか従業員によるアクションであるかに関係なく、セキュリティ イベントを監査するか、その

情報を収集して保持することです。イベント ログのレポートは実際に発生したイベントの概要を示すだけでなく、環境内で発生する脅威をリアルタイムで警告できます。

プロセス エンジンによるセキュリティの推進

セキュリティ プロセスの自動化は時間と工数の削減につながるだけではなく、人的ミスの可能性も抑えるためリスクの低下にもつながります。さらに、プロセスがモデル化され文書化されると、簡単に改善が可能です。たとえば、ホワイトリストを使用して環境を設定したとします。ユーザが新しいアプリケーションにアクセスする必要があるとしたらどうなるでしょうか。最初のステップは、ラボのアプリケーションをロードしてテストした後に、LANDesk Security Suite によって学習モードを適用し、アプリケーションのパターンを特定することです。ここで、新しいホワイトリストを設定して、新しいアプリケーションを含めます。そのアプリケーションをパッケージ化して、アプリケーションとライセンスをユーザにプッシュ配信します。

これらのステップをワークフローに統合すると、ほとんどのステップを自動的に完了できます。承認が必要な場合は、自動的に作成された電子メールが適切な担当者へ送信されます。システムをサイトにアクセスさせてファイル パターンをプル配信し、照合後のアプリケーションをユーザにプッシュ配信することで、この処理をさらに簡素化できます。プロセス自動化の可能性は事実上無限に存在します。

イベント相関関係

毎時ではないとしても、毎日、企業は環境に侵入しようとする新しいウィルスがウィルス対策ソフトウェアによって検出されていることを認識しています。理想的には、IT 部門はこれが発生する都度、HIPS システムが問題を確認したことを把握し、自動的にアクションを防止するか、アクセス権のためにエンド ユーザに通知したいと考えています。

また、HIPS 機能が問題を検知して IT 部門にアラートを送信するときにはイベント ログが出力されるため、IT 部門は発生した問題をウィルス対策 ソリューション ベンダに送信して対応を依頼できます。ベンダは問題を解決し、署名をアラートの発信元に送信します。IT 部門の介入は最小限に抑えられます。イベント相関関係を含めたプロセス エンジンによるプロセスの自動化は、作業工数を削減するだけではなく、問題を自動的に解決するため企業にとっての全体的なリスクも低減します。

LANDesk のアプローチ:

動的な LANDesk ロケーション認識ポリシーを使用したポリシーと設定の改善により、データ損失と感染の可能性が低減されます。動的なポリシーは選択したコンピュータが存

在する環境に応じてセキュリティ設定を調整できます。たとえば、アプリケーション制御、マルウェア対策設定、HIPS、ホワイトリスト、デバイス管理、LANDesk パーソナル ファイアウォール、リムーバブル記憶装置の制約などを調整できます。

LANDesk プロセスによってセキュリティを推進できます。

管理エンジンはシンプルなドラッグアンドドロップ式のユーザ インターフェースを提供し、プロセスの設計と文書化が可能になります。ここには実行中のワークフローが表示されます。セキュリティ管理とパッチ管理を統合したソリューションを採用することで、ビジネス プロセスを自動化できます。LANDesk Process Management は作成したポリシーが組織全体で実行されることを保証するとともに、プロセスを文書化します。また、基準への準拠が容易になり、準拠を達成するまでの時間も短縮されます。

LANDesk Security Suite には、ウィルス対策、ファイアウォール、HIPS、ホワイトリスト、デバイス管理といったすべてのセキュリティ アクティビティを 1 つの視点にまとめて表示するアクティビティ ビューがあり、最新のセキュリティ イベントに迅速にアクセスできます。また、イベント相関関係プロセスを構築して、イベントに関するアラートを送信することで、正確なイベントを自動的に検索して対応できます。

セキュリティ成熟度モデルの上位段階を目指す方法の簡素化

エンドポイント セキュリティの最終結果は、現在の脅威環境はきわめてダイナミックであるため、1 つの機能のみを提供するソリューションでは効果的な保護機能を実現できないということです。唯一の実践的で生き残り可能な防御戦略は、成熟段階の高いセキュリティ モデルに移行して、複数レイヤの保護技術を取り入れることです。

LANDesk 製品をご利用のお客様は世界最高レベルのレイヤ化されたエンドポイント セキュリティの利点を享受しています。LANDesk のエンドポイント セキュリティは市場において実証済みであるため、すぐに導入可能です。お客様は一元化されたコンソールを使用してすべてのセキュリティ リソースを管理できます。また、日常業務のプロセスを自動化することで、コストを削減し、管理負荷も軽減できます。さらに、最も重要な点は、ビジネスおよび技術要件に合わせて容易に拡張および適合可能なセキュリティ インフラストラクチャを導入できるということです。

最近行われた Forrester Research 独自の調査では次のような結果が報告されています。

「過去数年間、セキュリティ部門はますます複雑化する脅威と組織内で明確化する役割に対応しなければならなかったため、セキュリティ部門に対するビジネスの期待も大幅に高まりました。ビジネスはセキュリティ部門がこのような課題すべてに対応し、人員数をほとんど変えずに新しい責任を担うことを期待しています。結果として、セキュリティ部門が現実的にできることと、ビジネスが期待することの間の乖離が一般的になりました。現在、セキュリティ部門は機敏性と高パフォーマンスを実現し、多くの責任とニーズに同時に対応しなければなりません。」⁴

機敏で高パフォーマンスを発揮する IT 部門となるためには、とりわけ、単体のソリューションから脱却して、複数レイヤの保護技術を採用したより成熟度の高いセキュリティ モデルに移行しなければなりません。LANDesk 製品をご利用のお客様は世界最高レベルのレイヤ化されたエンドポイント セキュリティの利点を享受しています。LANDesk のエンドポイント セキュリティは市場において実証済みであるため、すぐに導入可能です。お客様は一元化されたコンソールを使用してすべてのセキュリティ リソースを管理できます。また、日常業務のプロセスを自動化することで、コストを削減し、管理負荷も軽減できます。さらに、最も重要な点は、ビジネスおよび技術要件に合わせて容易に拡張および適合可能なセキュリティ インフラストラクチャを導入できるということです。

LANDesk のレイヤ化されたエンドポイント セキュリティ ソリューションについては、www.landesk.co.jp をご覧ください。

⁴ Khalid Kark and Rachel A. Dines, "Security Organization 2.0: Building A Robust Security Organization", Forrester Research, Inc., May 10, 2010, p. 1