クラウド-クライアント型
エンタープライズセキュリティの効果

低コストで優れた保護を

Osterman Research 社 ホワイトペーパー

2009 年 1 月発行

提供：トレンドマイクロ株式会社

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Phone: +1 253 630 5839 • Fax: +1 866 842 3274 • info@ostermanresearch.com • www.ostermanresearch.com

セキュリティの管理コストを 40％削減

不正ファイル、迷惑メールなどの Web からの脅威は、組織の規模や業界を問わず、現在も猛威をふるっています。組織が感染した不正ファイルの影響度は計り知れず、若干の迷惑程度のものからデータ破壊に至るまで広範囲の問題を引き起こしています。ひどい場合には、キーロガーのようなデータ盗用型不正ファイルのように、ネットワークに侵入し、機密性が高い極秘の情報を搾取して、それを許可されていない第三者に送信するものもあります。さらに、改ざんされた Web ページを開くだけで、情報が盗まれることもあります。Web は、不正ファイルを配信する主要な手段となっており、迷惑メールによる危険なリンクへの誘導、悪意のある検索結果への誘導、改ざんされた正式なサイトの閲覧によってユーザーは感染します。不正ファイルに対する防御で、安全に業務を遂行することが困難になる場合があります。

問題がさらに深刻化しているのは、不正ファイルの悪意の度合いが高まり、より秘密裏に侵入し、検出されにくくなってきているためです。悪いことに、多くの不正ファイルの亜種のライフサイクルが、今や時間や日単位ではなく分単位になっており、多数の亜種が出現しては損害を与え、新たなパターンファイルやシグネチャが、サーバやネットワーク上のクライアントに実装や展開されるかなり以前に、それらは消滅してしまいます。

ただし、組織が新たな不正ファイルや迷惑メールがネットワークに到達する前に、それらをブロックするようなクラウド型レピュテーションデータベースを使用して、脅威情報取得に必要な時間の長さを劇的に短縮できるならば、エンドポイントの感染割合の低減、セキュリティ管理コストや損失した生産性コストの低減、セキュリティ侵害の可能性の低減が実現できるでしょう。さらに、組織がこれらのアクティビティをまとめ、コンテンツセキュリティインフラを集約して 1 社のベンダーに任せることを選択するならば、その優位性とコスト削減の効果はさらに大きくなるでしょう。

既存のセキュリティソリューションを使用した場合、5,000 人の企業では毎年

2/3 のエンドポイントが感染し

2000 万円の経費がエンドポイントのクリーニングにかかり

1600 万円の損失が従業員の生産性において起こります

従来のアプローチではなくクラウド-クライアント型アーキテクチャの包括的なコンテンツセキュリティソリューションを使用すれば、年間 3000 万円の削減が可能です

このホワイトペーパーでは、コンテンツセキュリティインフラを 1 社のベンダーに任せて集約する企業の利点に加えて、即効果のあるクラウド-クライアント型アーキテクチャを使用した、脅威情報への迅速なアクセスの多くの利点について解説しています。これらの利点を重ね合わせることで、生産性損失の低減、セキュリティ侵害の頻度の低下、その他具体的なコストの低下によるコスト削減は言うまでもなく、企業のセキュリティ管理コスト全体の 40%以上が削減できます。本ドキュメントでは、トレンドマイクロが提供する組織のコンテンツセキュリティインフラを著しく改善するソリューションに加えて、このホワイトペーパー用として Osterman Research 社が作成したコストモデルを紹介しています。

調査の方法と背景

このホワイトペーパーの作成作業の一環として、Osterman Research 社はクラウド-クライアント型アーキテクチャのインパクトと、コンテンツセキュリティにおけるベンダーの集約について理解を深めるため、組織ごとのエンドポイント数（クライアントとサーバ）、IT 業務に費やす時間、不正ファイルのパターンファイルとシグネチャの更新頻度、およびその他の様々な問題について 2008 年 12 月に調査を実施し、100 人以上から回答を得ました。調査対象の組織は、北米および欧州を拠点とし、従業員数の中央値が 4,500 人でした。このホワイトペーパーでは、5,000 人の従業員に基づいた例を使用します。

安心できない現状

増加するエンドポイント数

不正ファイルが組織のネットワークに侵入できるエンドポイント数は増えています。サーバ、デスクトップやノートパソコンの従来からのメールクライアント、企業や個人の Web メール、Web ブラウザ、共同作業環境、企業や個人のモバイルデバイス、インスタントメッセージングクライアント、家庭のパソコン、USB ストレージデバイスなどがあります。

ウイルス、ワーム、トロイの木馬やその他の種類の不正ファイルにとって、あらゆるエンドポイントが企業ネットワーク侵入の足掛かりとなる潜在的なエントリーポイントとなります。今日では、不正ファイルはサイバー犯罪活動の一部となっており、サイバー犯罪者はデータとリソースの盗用に多数のエンドポイントを対象として複雑な配信メカニズムを使用しています。つまりビジネスツールの利用が普及すればするほど、サイバー犯罪者に狙われるようになります。

刻々と悪化する不正ファイル

迷惑メール、ウイルス、ワームの単一の亜種が作成され、インターネットを介してゆっくりと増殖し、数週間をかけて広まっていくというのはかつての話です。むしろ、今日の不正ファイルは数百や数千の亜種に変形して、数分で増殖し、非常に短い時間で膨大な数のエンドポイントに感染します。

毎年エンドポイントのおよそ2/3が感染

エンドポイント数が増加した状況と、より悪意があり能力の高い不正ファイルの登場が相まって、エンドポイントの感染が増えています。今回の調査を実施した結果から、一般的な 1 ヵ月において、調査した組織内のエンドポイントの平均 5.4%（中央値 2.0%）が感染していたことがわかりました。これを 5,000 人の組織に換算すると、毎月平均して 270 のエンドポイントが感染、つまり毎年 3,250 弱のエンドポイントが感染していることになります。これを統計的に見れば、あなたの組織が一般的な組織であるとすれば、特定の 1 年間において組織内のエンドポイントのおよそ 2/3 が感染する恐れがあるということになります。

IT部門は時間を浪費し、生産性は低下

エンドポイントが感染した場合に起こりえるデータ損失や機密情報の搾取という最も深刻な結果は別として、IT 部門はコンピュータが使用不能となっている従業員の生産性が低下している間にも、エンドポイントをクリーニングしなければなりません。例えば、調査結果からは IT 部門が 1 台のエンドポイントのクリーニングに平均して 95 分（中央値 60 分）かかっていることがわかりました。つまり、IT 部門の貴重な時間が大きな割合で感染したエンドポイントのクリーニングに費やされ、一方で自分のコンピュータがクリーニングされるのを待つ間、生産性が低下している従業員がいることになります。

一般的な 1 ヵ月で見ると、IT 部門は感染したエンドポイントのクリーニングだけのために、平均して 428 人時費やすことになります。仮に専任の IT スタッフとしての給料を 800 万円だと想定

すると、エンドポイントから不正ファイルをクリーニングするという IT 業務だけのために、5,000 人の従業員あたり毎月約 160 万円を費やしていることになります。

ただし、従業員は自分のシステムがクリーニングされている間に作業できない場合もあるため、感染の結果として従業員の生産性も影響を受けることになります。仮に不正ファイルに感染した一般的な従業員の給料が 650 万円だと想定すると、感染したエンドポイントの生産性損失は 5,000 人の従業員あたり毎月約 130 万円となります。

結論として、組織は様々な種類の不正ファイルの感染からエンドポイントをクリーニングするだけのために、膨大な時間と費用を要していることがわかります。IT 部門と非 IT 部門を合わせたコストの合計は、5,000 人の従業員あたり毎年約 3500 万円です。

別の脅威としてのセキュリティ侵害

調査結果から、組織の半数強が過去 12 ヵ月にスパイウェア感染、ボットネット感染などセキュリティ侵害の被害を受けていることがわかりました。被害による影響は以下のように様々です。

- 従業員の生産性が損失した（回答者のうちの 78%）
- ネットワークがダウンした（24%）
- 顧客記録が漏えいした（10%）
- 顧客記録が使用不能になった（10%）
- 顧客との関係が悪くなった（8%）
- ネットワークが損害を受けた（6%）
- データの機密保持規定が侵害された（6%）
- 企業の信用度が落ちた（6%）
- 顧客にデータ侵害の件を伝えるべきであった（6%）
- 若干の財務上の損失があった（6%）

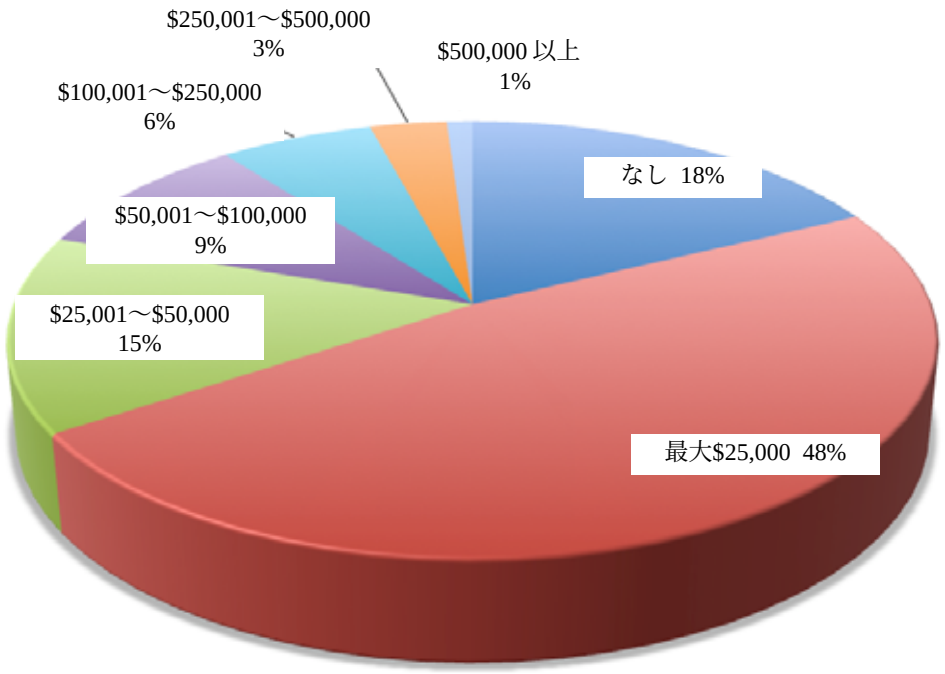
過去 12 ヵ月にセキュリティ侵害の被害を受けた組織のうち、悪影響が発生していないのは 4% のみでした。さらに、セキュリティ侵害が発生したときには、平均して 74 分間（中央値 18 分間）ネットワークがダウンしたと回答されています。

データ侵害の被害額は高額

また、セキュリティ侵害の潜在的な被害コストについても尋ねました。次の図にある通り、回答者のおよそ半数が、一般的な単一のセキュリティ侵害で最大 250 万円のコスト的被害を受け、10%がセキュリティ侵害によるコスト被害を 1000 万円以上だと回答しています。

Osterman Research 社は、以下の図で示されたデータの平均を基にして、セキュリティ侵害の平均的被害コストを約 480 万円と見積もっています。この額は、以下で示されているそれぞれのコスト範囲（「$500,000（約 5000 万円）以上」の範囲ではコストを$800,000（約 8000 万円）と見積もりました）の中間点を抽出して、それぞれのコストの可能性を掛けて算出しました。

1度のセキュリティ侵害の
推定総被害コスト



また、今後 12 ヵ月間におけるセキュリティ侵害発生の可能性についても尋ねました。セキュリティ侵害はほぼ起こりえないという回答者はいませんでしたが、5%が実際に確実に発生すると回答し、平均は 45%以下でした。つまり、組織は今後 12 ヵ月の間にネットワーク上でセキュリティ侵害が発生する確率は 45%であると考えていることになります。

従来の定量的経営分析手法を用いると、セキュリティ侵害の平均的被害コストにその発生の可能性を掛けると、組織が今後 12 ヵ月間に被ると考えられるセキュリティ侵害の平均被害コストは約 220 万円 ($48,698×44.8%) となります。ただし、これは潜在的なセキュリティ侵害の被害コストを一番低く見積もった場合のものです。例えば、個人が特定できる情報が侵害された場合、侵害発生について説明する手紙を被害者ごとに送信する必要性や、信用報告書などを作成するコストも発生します。わずか 1 つの侵害でも、組織の信用度に多大なマイナス影響を及ぼすだけでなく、その被害コストは数億円に達することもありえます。

コンテンツセキュリティ管理も同様に高額

このホワイトペーパー用に実施した調査で、IT 業務のコストが高いことがわかりました。例えば、コンテンツセキュリティに関わる問題において、次のようなコストが IT 業務で発生します。

- 1 人の IT スタッフが平均 216 人の従業員をサポートしています。この人数は、小さな組織ではかなり小さな人数となり、大企業の場合ははるかに大きな人数となるため、非常に幅があります。仮に専任の IT スタッフの年収が 800 万円と想定すると、従業員 1 人あたりの IT 業務コストは年間 3 万 7000 円となり、月間で見ると従業員 1 人あたり 3100 円弱となります。

- 一般的な週において、5,000 人の従業員のいる組織では IT スタッフは様々な業務に次のような時間を費やしています。

- パターンファイル、シグネチャ、およびその他の重要なエンドポイントの問題の管理に 62 人時。
- セキュリティインフラで発生した誤検出や関連する問題の管理に 51 人時。

- さらに、5,000 人の従業員のいる組織の IT スタッフは、帯域幅、ストレージ、新しいサーバやアプライアンスなどの追加を行い、リソース容量をアップグレードするのに年間 1,674 人時費やしており、これは正規社員のまさに 0.8 人分以上の業務に相当します。

上記の 800 万円の給料で考えると、これら 3 つの作業にかかるコストの総額は年間でおよそ約 2900 万円になり、これは正規社員の IT スタッフ 3.6 人分に相当します。このコストに、感染のクリーニングに要するコストを加えると、5,000 人の従業員のいる組織では、コンテンツセキュリティ管理に少なくと約 4800 万円費やしていることになります。

コストに関するまとめ

これまでの分析を基にすると、5,000 人の従業員規模の組織が年間に費やすコストは次の通りとなります。

- エンドポイントの感染に対処する際の IT 業務コスト：5,000 人の従業員で年間約 1900 万円
- 従業員の生産性損失：5,000 人の従業員で約 1600 万円
- セキュリティ侵害の被害コスト：セキュリティ侵害 1 件あたり約 4 万 9000 円
- パターンファイル、シグネチャ、およびその他の重要なエンドポイントの問題の管理に関わる IT 業務コストは、年間約 1200 万円
- セキュリティインフラで発生した誤検出や関連する問題の管理に関わる IT 業務コストは、年間約 1000 万円
- セキュリティ用にリソース容量をアップグレードする IT 業務コストは、年間約 640 万円

コンテンツセキュリティ管理のコストは高く、そのコストの大半は不正ファイル対策に向けられた業務やリソースに関連するものです。膨大な迷惑メールや不正ファイルの亜種から保護するために、エンドポイントにダウンロードするパターンファイルやシグネチャのサイズが巨大化することをサポートする必要があることから、さらに広帯域なネットワーク、ストレージ、新たなサーバやアライアンス、およびその他のネットワーク機器をアップグレードすることに加え、パターンファイルの管理や誤検出の処理にかかる業務コストなど、組織は不正ファイルに対する防御に相当なコストを費やしています。このような取り組みをしていても、従来のコンテンツセキュリティ管理手法を使用している組織は、毎年エンドポイントの 2/3 が感染し、これらエンドポイントのクリーニングにさらにコストがかかります。また、これらのコストには、生産性が高まり、さらに売上に貢献するようなより優先度の高いイニシアティブに IT スタッフを登用すれば、企業はさらに利点が享受できるという点も考慮されていません。

すぐに保護効果が得られるとしたらどうでしょうか？

頻繁には行われていないセキュリティの更新

現状の根本的な問題の 1 つが、多くの組織が使用しているセキュリティシステムが稀にしか更新されていないという点です。例えば、24%の組織がパターンファイルとシグネチャの更新が 1 日に 1 回以下で、37%の組織が 1 日に 1 回パターンファイルとシグネチャを更新していることが調査結果からわかりました。わずか 25%の組織のみが、1 日に 2 回以上ファイルを更新しているようです。

これは不正ファイルのライフサイクルが分単位になっている一方で、業務ではセキュリティを 1 日に 1〜2 回程度しか更新しないというのは問題です。更新頻度が少なければ、不正ファイルが出現してきた時と、クライアントやサーバに保護措置が講じられた時との間に、セキュリティにギャップが生じます。結果的に、新たな不正ファイルの亜種が出現して損害を与え、それに対抗するために最初のパターンファイルやシグネチャが実装される前に、新たな亜種に取って代わられる、ということになります。サイバー犯罪者が、さらに巧妙に不正ファイルを作成するようになったため、この問題はよりひどい状態となるでしょう。

不正ファイルのライフサイクルは場合によっては分単位になっていますが調査結果から組織は 1 日にわずか 1〜2 回程度しかパターンファイルを更新しない傾向にある

24%の組織が
1 日に 1 回以下の更新

37%の組織が
1 日に 1 回のみの更新

25%の組織が
1 日に 2 回以上の更新

迅速なアクセスが優れた保護に

パターンファイルとシグネチャの更新が、頻繁には行われないことで引き起こされるこの問題の対処法は明確です。それは、迅速に脅威情報にアクセスすることですが、できる限りリアルタイムにというのが理想的です。脅威の数が増えれば、同様にパターンファイルのサイズも大きくなります。パターンファイルとシグネチャの配信という従来の方法だけに頼るアプローチでは、展開が遅過ぎるためセキュリティを維持することが大変です。一方、クラウド-クライアント型アーキテクチャでは、脅威情報はクラウド内で維持され、クライアントから問い合わせする形態です。企業は社内のコンピュータにパターンファイルを配信して保護されるのを待つ必要がなくなり、リソースの削減や迅速に対応できるセキュリティが実現できます。このアプローチを使用すれば、セキュリティシステムは新たに発見した脅威の検出や修正がよりすばやく行えるようになるため、感染するエンドポイント数やセキュリティ侵害数は減少します。これでユーザーと組織にとっては、コスト削減とマイナスの影響の低減が実現できるようになります。

調査回答者には次のような質問をしました。「あなたの組織のサーバとエンドポイントが、新たな脅威が検出された後に、新しいパターンファイルとシグネチャを 10 倍早く(例えば、シグネチャの更新を 8 時間から 15 分に)更新できたと想像してください」。注目すべきなのは、調査でクラウド-クライアント型アーキテクチャについて説明するのではなく、パターンファイルとシグネチャの更新といった脅威情報への迅速なアクセスが重要であるということがわかったという点です。ただし、この調査の回答でキーとなるのは、組織は 15 分以内に脅威情報にアクセスする手段を持っているということです。

迅速な保護による重要なアドバンテージの 1 つが、セキュリティ侵害の可能性を低減できることです。例えば、先述の通り今後 12 ヵ月間にデータ侵害が発生する可能性はおよそ 45%ありますが、回答者は保護処理をさらに迅速にすれば、その侵害の可能性は 36%になるだろうと回答しています。

迅速なアクセスがコスト削減に

脅威情報に迅速にアクセスすることで、データ損失のリスクやエンドポイントの感染修復に費やされる IT 業務のコストを削減できるだけでなく、セキュリティ管理全体のコストも削減できるようになります。

Osterman Research 社は、このホワイトペーパー用として、組織が脅威情報に迅速にアクセスすることで得られるコスト優位性を見積もったコストモデルを作成しました。例えば、5,000 人の従業員のいる組織においては、次のように見積もっています。

- エンドポイントの感染率が 5.4%から 2.0%に低減します。
- パターンファイル、シグネチャおよびその他の重要なエンドポイントの問題の管理に要する IT スタッフへの投資が 25%削減されます。
- 広帯域ネットワーク、ストレージ、サーバやアプライアンスなどを追加するリソース容量のアップグレードに要する IT スタッフへの投資が 10%削減されます。
- 誤検出や関連する問題の管理に要する IT スタッフへの投資が 2%削減されます。

この想定に基づき、Osterman Research 社ではクラウド-クライアント型のコンテンツセキュリティソリューションを使用した迅速な保護を行うことで、実現できる組織のセキュリティ管理のコスト削減総額が、コンテンツセキュリティ管理の総コストの 34%に相当すると見積もっています。この値に、損失生産コストの削減分とセキュリティ侵害の回避分のコストを加えると、5,000 人の従業員のいる組織では、およそ約 2700 万円相当となります。

コンテンツセキュリティベンダーを1社に絞ったらどうでしょうか？

多くの組織は、コンテンツセキュリティのインフラに複数のベンダーを利用しており、調査からコンテンツセキュリティに平均 4 社(中央値 3 社)のベンダーを利用していることがわかりました。ただし、多くの組織はボリュームディスカウントを求めたり、複数ベンダーの製品を管理する IT 業務への投資を削減したり、パッチ管理を簡素化するなどして、コスト削減のためにベンダー数を減らそうとしています。

複数のコンテンツセキュリティベンダーを利用している組織に次のように尋ねてみました。「あなたの組織のサーバとエンドポイントのすべてのセキュリティの要求を満たす「ベストオブブリード」のベンダーが 1 社あるとすれば、IT スタッフがコンテンツセキュリティの管理に費やしている時間の割合は、一般的な週でどの程度削減できると思いますか？」の質問では、14%の回答者がベンダーの集約では削減が見込めないと回答する一方で、22%が IT 業務コストは最大 5%削減できると回答し、さらに 41%が 6%～10%の業務コストが削減、そして 23%が 10%以上のコスト削減ができるであろうと回答しています。平均の削減率は 9.5%でした。これは、特に大規模な組織では大変なコスト削減をもたらす可能性があります。

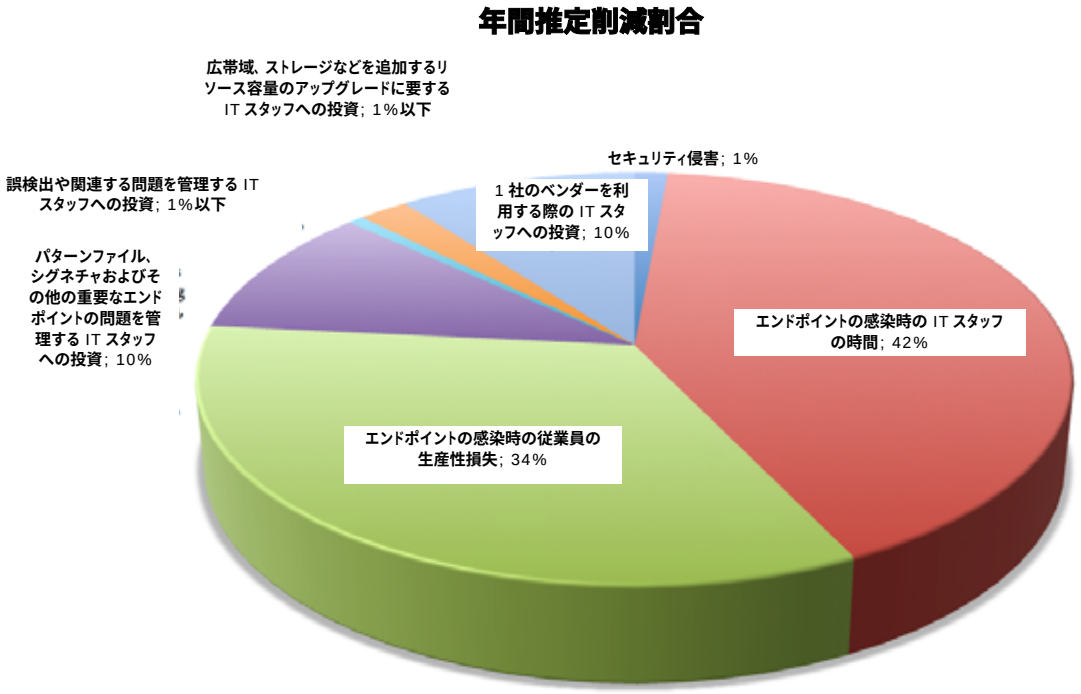
セキュリティの集約で実現できるコスト削減

コンテンツセキュリティに
平均 4 社のベンダーを現在利用

5,000 人の従業員規模の企業は
1 社の「ベストオブブリード」の
ベンダーを利用すればコンテンツ
セキュリティ管理コストを
9.5%削減可能

まとめ

脅威情報の迅速なアクセスを、1 社のコンテンツセキュリティベンダーの利用と併用すれば、大幅なコスト削減につながることになります。これまで 5,000 人の従業員のいる組織で見てきたように、コンテンツセキュリティ管理の総コストは約 4800 万と推定できます。迅速なセキュリティ適用によるコスト削減の総額はおよそ 34%、つまり約 1600 万円となります。これらのコスト削減に加え、1 社のベンダーを利用した場合のセキュリティ管理コストの削減を考えると、さらに 9.5%、つまり約 300 万円の利点が生まれることになります。これに生産性損失の削減とセキュリティ侵害の低減によるコスト削減を加え、5,000 人の従業員のいる組織で 1 社のベンダーによるクラウド-クライアント型ソリューションを利用すると、およそ約 3000 万の削減になると考えられます。これらの削減の内訳は次に挙げる通りですが、1 回のセキュリティ侵害を回避するための膨大な潜在的コスト削減額は、表示されているその他のコストすべてを上回っている点に注意してください。



Trend Micro Smart Proction Networkでコスト削減

トレンドマイクロのクラウド-クライアント型アーキテクチャは、パターンファイルの更新だけに頼る従来のアプローチに比べ、迅速な保護を可能にします。また、トレンドマイクロは包括的なソリューションを提供するため、企業はコンテンツセキュリティに 1 社のベンダーを利用すればよいようになります。このホワイトペーパーの前半に解説した利点をもたらすこの組み合わせによって、従業員の生産性向上やセキュリティ侵害の低減に加え、企業はセキュリティ管理コスト全体の 40%以上を削減できるソリューションを手に入れることができます。

以下には、複数のベンダーを利用した従来型と言えるコンテンツセキュリティに対して、Trend Micro Smart Protection Network を使用した場合に企業がさらに削減できるコストについてまとめています。

従業員数	迅速な保護によるコンテンツセキュリティ管理の推定削減コスト	1 社のベンダーを利用した場合の削減コスト	コンテンツセキュリティ管理の総コストの割合	コンテンツセキュリティに関するその他の削減コスト	トレンドマイクロを利用した場合の従業員あたりの年間削減コスト
1,000	330 万	60 万	40%	240 万	**6337 円**
5,000	1600 万	300 万	40%	1050 万	**5994 円**
10,000	3300 万	610 万	40%	2060 万	**5951 円**

Smart Protection Network によってサポートされる Trend Micro Enterprise Security は、複雑さを軽減し、企業におけるビジネス上のリスクとコストを削減する迅速な保護を提供します。

最後に

不正ファイルの状況はさらに悪化しています。不正ファイルの亜種は、より膨大になり、より悪質となり、検出はさらに困難になり、そしてそのライフサイクルは劇的に短くなっています。パターンファイルとシグネチャを毎日 1～2 回更新するだけの従来のコンテンツセキュリティインフラを展開している組織は、不正ファイルの亜種がネットワークに侵入して損害を与え、企業がそれに対抗する最新のパターンファイルやシグネチャを実装する前に消滅してしまうため、まったく不利な状態にあります。

一方、クラウド-クライアント型アーキテクチャを使用して最新の脅威情報にアクセスできる統合型コンテンツセキュリティインフラを導入している組織は、最新の迷惑メールや不正ファイルの脅威に対して迅速に保護を行うことができます。このためセキュリティ侵害の機会が低減し、感染するエンドポイント数が削減し、セキュリティ管理に向けられる IT 業務コストが削減できるようになります。コンテンツセキュリティベンダーを 1 社にすることも平行して行えば、その削減による効果は非常に大きいでしょう。

トレンドマイクロは、Trend Micro Smart Protection Network によってサポートされる Trend Micro Enterprise Security を使用したソリューションなどを提供しています。このアプローチは、Web、メッセージング、エンドポイントセキュリティを兼ね備えた統合型ソリューションで迅速に保護を提供します。この包括的なコンテンツセキュリティは、将来脅威が進化を遂げても、継続的に維持可能なアーキテクチャを提供しながら今日のコスト削減を実現しています。

このドキュメントでは、1ドル＝100 円として、ドル表記の英語ドキュメントを翻訳しました。