

WHITE PAPER

エンタープライズセキュリティ：難しい方法ではなく賢い方法を

Sponsored by: Trend Micro

Charles J. Kolodgy

Andrew Hanson

February 2009

IDC の見解

「時は金なり」「知は力なり」は決まり文句だが、コンテンツセキュリティの専門家にとってはリアルな意味を持っている。コンテンツセキュリティの脅威は拡大を続け、攻撃者はさらに洗練された、絶えず変化する攻撃形態を手に入れている。これらの脅威が到達する速度は、以前にもましてセキュリティ専門家に大きな圧力を与えている。

従来型のセキュリティアプローチは、洗練された攻撃者に対して優位を保つには力不足になってきている。主にパターンファイルに依存するソリューションは、企業のクライアントとサーバー全体に展開しなければならないため、保護に遅れが生じる。また、変種の数の増加に伴ってパターンファイルが大きくなりすぎ、リソース量を過剰に消費する。これは脅威の数が増え続けるに従ってさらに深刻な問題になる。

多くの企業は、コンテンツセキュリティを確保するため幅広いポイント製品に投資している。しかし、セキュリティ上の問題の解決につながるどころか、ポイント製品の「スプロール現象」は単純に、継続的な展開とアップグレード、監視と管理、24 時間態勢のサポート要求などといった、新たな、さらに費用のかかるタスクを上乗せする。この場合、「時は金なり」の言葉どおり企業は数十億ドルを消費して堅固な防衛線を築こうとしたにもかかわらず、複雑さに対応するため、解決しようとしていた問題よりも大きな問題を発生させている。

問題に対して常に優位に立つには、複雑さを抑えつつ即時保護を行う、新しい革新的なアプローチが必要となっている。

コンテンツセキュリティの分野では、知識は脅威をすばやく特定して阻止するアプローチとソリューションを模索するための確固たる基盤を築くのに不可欠な「力」であるといえる。Trend Micro は、タイムリーであることと、すべての攻撃手段を知ることの必要性を理解している。この概念に従って、同社はソリューションの基礎に「クラウドクライアント」アーキテクチャを採用した新しいアプローチを開発し、セキュリティ専門家の側に再びアドバンテージを取り戻している。

調査方法

IDC では、セキュリティソリューションにおける顧客と市場の傾向を特定するため、複数の業界に属する企業の経営陣に対して聞き取り調査を行った。さらに IDC では、顧客のセキュリティ上の課題に対応する新しいアプローチを評価するため、Trend Micro の経営陣にもヒアリングした。本調査レポートではこれらの調査上の観点すべてを使用して、企業が今日直面するコンテンツセキュリティ上の課題と、Trend Micro の新しいアプローチがそれらを解決する方法について、現実的に即して展望する。

概況

混迷を深める IT セキュリティの世界

脅威

IDC の調査によると、ウイルス、トロイの木馬、ワーム、スパイウェアなどのマルウェアは最も深刻な脅威であり続け、企業に最も重大な影響を与えている。毎日、数千もの新しいマルウェアの変種がリリースされ、IT スタッフメンバーは深刻な損害が発生する前にそれぞれの新しい攻撃に対応しようと苦心している。ウイルスの感染速度は、数週間や数日ではなく、数時間や数分といった単位で測定されるようになってきている。マルウェアの最も危険な形態の 1 つはスパイウェアである。IDC は、企業のコンピュータの 4 分の 3 近くが何らかのスパイウェアに感染していると考えている。

毎日、数千もの新しいマルウェアの変種がリリースされ、IT スタッフメンバーは新しい攻撃に対応しようと苦心している。IDC は、企業のコンピュータの 4 分の 3 近くが何らかのスパイウェアに感染していると考えている。

さらに、スパムもいまだに企業を悩ませている。スパムは、危険な添付ファイルや、悪意のあるダウンロード、フィッシング、その他の脅威を含むウェブサイトへのリンクなど、他の脅威の配信メカニズムとしても使われている。

IDC が 2008 年に行ったセキュリティ調査の結果、攻撃の複雑化と、それに伴うセキュリティアーキテクチャの複雑化が、IT 専門家が直面する課題の上位に来ることが判明した。

攻撃者は絶えず、既存のセキュリティ防衛手段を回避して企業ネットワークに侵入する革新的な技術を開発している。IDC は、「複合型脅威」が近い将来さらに顕著になり、統合型コンテンツセキュリティへのニーズが高まると予測している。多様な脅威のプロファイルを組み合わせ、それぞれのマルウェアアルゴリズムについて変種の数を指数関数的に増大させることで、攻撃者は従来型のコンテンツセキュリティソリューションを回避する方法を見つけ出している。対策の効果を最大限に高めるためには、IT 専門家はゼロデイ攻撃、ウイルス、トロイの木馬、ワーム、スパイウェア、botnet 攻撃、rootkit、アドウェア、スパム、フィッシング、ソーシャルエンジニアリング、その他多くのコンテンツセキュリティ攻撃の組み合わせに対して、企業のインフラストラクチャを保護できるよう備えなければならない。前述したように「知は力」であり、企業はこれらすべてのセキュリティ上の脅威を理解し、防御できるベンダーのソリューションを必要としている。

IDC は、「複合型脅威」が近い将来さらに顕著になり、統合型コンテンツセキュリティへのニーズが高まると予測している。

攻撃対象領域の拡大

情報技術の進歩はビジネスにとってかつてないほどの重要性を占めているが、企業が常に新しい脅威の一步先に行くことはますます難しくなっている。企業活動とビジネスアプリケーションをサポートするためにはネットワークに依存しなければならないため、ビジネスの内部、外部、および枠内に潜む脅威にさらされる攻撃対象領域は拡大し続けている。

インターネットを介した攻撃対象領域は拡大し続けている...企業が「防弾」保護を確立することは、途方もない複雑さと困難さに達している。

分散オフィスによる支社、ノートパソコンを携えるモバイル従業員、ポータブルデバイスや携帯電話、インスタントメッセージング、VoIP、電子メール、ウェブサイト、ウェブベースアプリケーションのアクセス、Web 2.0、そしてあらゆる形態のクラウドコンピューティングによって、たやすい金もうけの方法を模索する犯罪者が仕掛ける攻撃に対して企業が「防弾」保護を確立することは、途方もない複雑さと困難さに達している。

中心的なビジネスアプリケーションである電子メールはこれまでも特に影響を受けやすかったが、主な脅威の媒介源は現在、ウェブに移行している。マルウェアはウェブページを開くだけでダウンロードされる可能性がある。ユーザーは電子メールのリンクをクリックしたり、壊れた検索結果をたどったり、ハイジャックされた信頼済みサイトにアクセスしたりするだけで被害者になりうる。感染方法がこのように容易であるため、脅威がネットワークに侵入すらできないうちに、電子メールのソース、電子メールのリンク、ファイル、ウェブページなど、攻撃のすべての段階でブロックする防御手段を実装することが企業にとって非常に重要となっている。

IDC では、Web 2.0 および Business 2.0 のアプリケーションやコミュニティが、マルウェア配布、なりすまし、プライバシー侵害、企業データ消失の主な原因になると予測している。これらの新しい技術に対してポリシーやセキュリティ保護の効果的な手段を確立しなかった企業は、巨大で高コストなリスクに直面する可能性がある。

コンテンツセキュリティへの包括的なアプローチとして、企業には、脅威がネットワークに入った時点でブロックする、メッセージング、ウェブ、およびエンドポイントセキュリティが必要となる。コンテンツセキュリティは、ユーザーがネットワーク上にいるときもいないときも、電子メールやその他の通信手段（インスタントメッセージング[IM]、モバイルデバイス、コラボレーション環境）、ウェブサイト、およびクライアントコンピュータ上の脅威から保護するために必要である。ネットワーク全体にわたって即時保護を提供し、かつソリューションの取得、展開、管理の労力が最小限で済むコンテンツセキュリティソリューションが企業に求められている。「時は金なり」の言葉どおり、企業はセキュリティ管理にかかる時間を削減し、その時間でビジネスを成長させるためのコアイニシアチブをサポートしなければならないからである。

これらの新しい技術に対してポリシーやセキュリティ保護の効果的な手段を確立しなかった企業は、巨大で高コストなリスクに直面する可能性がある。

ネットワーク全体にわたって即時保護を提供し、かつソリューションの取得、展開、管理の労力が最小限で済むコンテンツセキュリティソリューションが企業に求められている。

応急セキュリティ

従来のセキュリティソリューションはシグネチャスキャンに依存し、企業ネットワークへの侵入を試みる既知の脅威をブロックしていた。このアプローチは脅威の阻止とウイルスの封じ込めには大いに有効だが、従来型の脅威対策の展開手段は遅く、脅威の発見と脅威からの保護の間に致命的なギャップが生じる。

シグネチャとパターンファイルを配布するという従来型のアプローチは、かなりの時間がかかることがある。このアプローチでは、保護シグネチャを作成できるように、脅威を発見して分析する必要がある。特定のシグネチャが利用可能になると、企業のコンテンツセキュリティ製品のアップデートに使用するパターンファイルに追加される。その後、このプロセスでは以下が必要になる。

- ☑ すべてのクライアントおよびサーバーへのパターンファイルのダウンロード。これには数時間かそれ以上かかることがあり、脅威がリリースされてから企業が完全に保護されるまでの間に、長い脆弱性の窓（無防備な時間帯）が生じる。
- ☑ 脅威シグネチャのアップデートの定期的ダウンロード。
- ☑ 一部のソリューションは、電子メールとウェブトラフィックを含むネットワーク上のすべてのコンテンツをスキャンして脅威を検索するため、ネットワークリソースに負荷がかかる。

感染性のウイルスが企業にもたらす脅威に加えて、量そのものが純粋に脅威になっている。脅威の量が増加するに伴って、シグネチャの数も増加し、パターンファイルのサイズも大きくなる。パターンファイルは扱いにくくなり、ネットワークリソースが過剰に消費され、保護が行き届くのがさらに遅くなる。また、脅威はあまりに爆発的に増加し、ネットワークのダウンを誘発

従来型の脅威対策の展開手段は遅く、脅威の発見と脅威からの保護の間に致命的なギャップが生じる。パターンファイルは扱いにくくなり、ネットワークリソースが過剰に消費され、保護が行き届くのがさらに遅くなる。

している。脅威を大元からブロックせずにネットワーク上でスキャンする製品は、帯域幅やストレージなど、高価なネットワークリソースを過剰に使用している。

問題をさらに悪化させること

多くの場合、企業が採用するソリューションアプローチは問題を悪化させている。多くの企業は複数のベンダーの製品を重ねて使用して、トータルで今日の脅威に対して十分に高速で幅広い保護を実現しようとする。実際には、このアプローチは必ずしも効率アップにはつながらず、それどころかソリューションの副作用として誤検知が増加する。

さらに、ポイント製品や単機能セキュリティソリューションのスプロール現象は、企業セキュリティにとってかえって有害となりうるレベルに達している。IT 管理者は急速に追い込まれつつある。脅威の数だけではなく、さまざまなテクノロジー、プラットフォーム、ベンダーの技術を組み合わせる構築されたネットワークを管理、統合しなければならない負担も原因となっている。無数のコンソールとの絶え間ないインタラクションは、管理者にとっての「バベルの塔」になる。

...ポイント製品や単機能セキュリティソリューションのスプロール現象は、企業セキュリティにとってかえって有害となりうるレベルに達している。無数のコンソールとの絶え間ないインタラクションは、管理者にとっての「バベルの塔」になる。

より賢い行動

即時保護

ますます洗練される脅威と、また本質的に利益目的で行われる攻撃が組み合わさると、どのように小さく、あるいは短命のセキュリティ違反でも、侵害にあったすべての企業にとって巨額の出費に結びつくことがある。IT 管理者は、すばやく簡単に配布でき、また最も重要な点として新しい脅威をできるだけ迅速に特定して対処できるセキュリティソリューションを模索している。ここで再び「時は金なり」である。この場合は、脅威に迅速に対応する能力によって、企業は膨大な修復コストを節約できる。そして、「知は力なり」であるため、新世代のセキュリティソリューションでは、企業は互換性のないスタンドアロン製品から、脅威についての知識がビジネスアプリケーションのすべての境界にあまねく行き渡る、即効性のある総合的なソリューションに移行できるようになる必要がある。

IDC が「ハイブリッドセキュリティモデル」と呼ぶ、インザクラウド型のテクノロジーとオンサイトソリューションを組み合わせるモデルは、脅威が企業ネットワークに届かないうちに迅速なセキュリティレスポンスを実現することができる。

IDC が「ハイブリッドセキュリティモデル」と呼ぶ、インザクラウド型のテクノロジーとオンサイトソリューションを組み合わせるモデルは、ネットワークから負荷を大幅に取り除き、脅威が企業ネットワークに届かないうちに迅速なセキュリティレスポンスを実現して、IT スタッフメンバーがセキュリティ関連の問題について保守、アップデート、障害対応に追われる時間を確実に削減する。

レピュテーションサービス

クラウドベースのレピュテーション(評判)サービスは、適応性と効果が高く賢いセキュリティソリューションで、その実効性のため急速に広がりつつある。このアプローチでは、洗練されたナレッジデータベースを使用して「評判の悪い」電子メール送信者、ウェブサイト、ファイルをカタログ化し、トラフィックとファイルをブロックおよび廃棄する。レピュテーションサービスは、脅威を「大元で」インテリジェントに阻止し、レーダーに保護された企業システムを攻撃しようとする複合型脅威を検出することができる。このアプローチは脅威がネットワークに入る前に阻止することができるため、貴重なリソースを節約する。

クラウドベースのレピュテーション(評判)サービスは、適応性と効果が高く賢いセキュリティソリューションで、その実効性のため急速に広がりつつある。

クラウド上に展開されたオンサイトソリューションは、オンサイトクライアントを使用して脅威対策をすばやくクエリできるため、クライアントとサーバーにダウンロードする必要のある情報量を節減できる。このアプローチはネットワーク上の負荷を減らすほか、ベンダーがデータベースをアップデートするとすぐに企業が最新の保護にアクセスできるようになるため、パターンファイルやシグネチャのダウンロードを待つ必要がなくなる。高度なレピュテーションサービスはウェブ、電子メール、およびエンドポイントファイルの脅威に対して挙動分析を適用して、悪意ある攻撃を発見することができる。

複雑性の軽減

特にネットワーク全体が常にアップグレード、拡張、リストラクチャリングを続けている大企業にとって、企業インフラストラクチャ管理のダイナミクスは複雑である。インフラストラクチャの個々のコンポーネントが使用するテクノロジーは、数世代にわたる場合がある。多くの場合、企業セキュリティソリューションはベンダー製ポイント製品の組み合わせで構成されている。

ハイブリッドな「インザクラウド型」セキュリティアプローチでは、セキュリティアプリケーションは密接に統合され、脅威に関する知識をよりよく共有できるようになる。これによって IT 部門は、単一の管理ポータルを経由して、セキュリティポリシーの管理と、イベントや脅威ステータスの監視とレポートが行えるようになる。この種のソリューションは、集中化された場所から、限られた数の IT スタッフメンバーによって制御できる。これらすべてによって、セキュリティを向上しつつ時間と資金を節約することができる。

ネットワークセキュリティに対するハイブリッドなインザクラウド型アプローチは、ビジネスプロセスを改善し、IT プロフェッショナルの労働時間をずっと効率的なものにする。正しく構成されたセキュリティアーキテクチャは、企業内で透過的に動作し日々のパフォーマンスを実際に向上させることで、ユーザーの生産性アップとセキュリティに必要な IT リソースの削減につながる。

TREND MICRO エンタープライズセキュリティ

革新的なアプローチ

Trend Micro Smart Protection Network は、Trend Micro の製品とサービスの基盤となる、高い効果と統合性を誇るクラウドクライアント型セキュリティアーキテクチャによって、ハイブリッドなインザクラウド型アプローチを実現する。この革新的なアプローチは、即時保護を提供し、安全なネットワークインフラストラクチャを設定、管理、監視、維持する複雑さを大幅に軽減する。

Trend Micro は、20 年前の創業以来コンテンツセキュリティ専門にフォーカスしてきた、世界最大のセキュリティベンダーである。Trend Micro は、シンプルさとスピードを包括的なセキュリティ機能と融合させる必要性を常に強調してきた。同社はその技術革新の長い伝統にならって、クラウドクライアントセキュリティ製品の先頭に立とうとしている。Trend Micro Enterprise Security は Trend Micro Smart Protection Network によって駆動され、顧客に即時保護を提供し、複雑さを軽減して、ビジネス上のリスクとコストを抑える。

Trend Micro は急展開を遂げるセキュリティの状況を理解しており、Trend Micro Smart Protection Network に基づいてそのソリューション戦略を構築してきた。Trend Micro Smart Protection Network は、インザクラウドテクノロジーと軽量なクライアントアーキテクチャが結びついた革新的なクラウドクライアントインフラストラクチャである。

Trend Micro Smart Protection Network

Trend Micro は急展開を遂げるセキュリティの状況を理解しており、Trend Micro Smart Protection Network に基づいてそのソリューション戦略を構築してきた。Trend Micro Smart Protection Network は、インザクラウドテクノロジーと軽量なクライアントアーキテクチャが結びついた革新的なクラウドクライアントインフラストラクチャである。Smart Protection Network は、コンスタントに更新され、相互に強化する仕組みを持ったウェブ、電子メール、ファイルのレピュテーションデータベースを格納している。これによってインザクラウド型の脅威対策が実現し、最新の保護が可能になると同時に、従来型の施設ベースのセキュリティソリューションで必要とされるパターンファイル展開に関する遅延やオーバーヘッドが防止される。

Smart Protection Network では、Trend Micro のグローバル研究サービス機関 TrendLab やサポートセンターに勤務する、熱意ある献身的な 1,000 人を超えるセキュリティ専門家によって脅威情報が分析される。Trend Micro は脅威情報を、同社のグローバル顧客ベースを含む多くのソースから収集する。組み込みのフィードバックループによって Trend Micro の製品と同社の脅威研究センターや脅威研究テクノロジーの間に継続的なコミュニケーションが行われ、包括的な脅威対策が形成される。

Smart Protection Network では、ウェブ、電子メール、ファイルの各レピュテーションデータベース間の脅威対策を相互に関連させる。ある要素が悪いレピュテーションを示すと、その要素はすべての脅威送信方法について自動的にブロックされる。レピュテーションの判断には挙動分析が適用される。1 つの攻撃コンポーネント(単一の電子メールまたはファイル)は無害に見えることがあるが、Trend Micro Smart Protection Network では挙動分析を使用して、実際に脅威が存在するかどうか判断するための全体的なビューを作成する。この高度な相互関係スキャン機能により、潜在的に有害な電子メール、ウェブページ、ファイルは、企業ネットワークの周囲にすら到達しないうちに除外される。レピュテーションデータベースを使用して脅威をその大元で阻止することで、即時保護が実現し、複雑さが軽減され、ネットワークリソースの負荷が取り除かれる。

ポイント製品による単純なセキュリティを越えるため、Trend Micro では、有効範囲の狭いセキュリティ製品のパッチを当てる負担をなくし、従来型と新型の両方のテクノロジーから保護する統合コンテンツセキュリティソリューションをネットワーク全体に展開する。こうすることでウェブ、メッセージング、およびエンドポイント全体で統一された防御が形作られ、攻撃場所にかかわらず脅威が阻止される。

Smart Protection Network では、Trend Micro のグローバル研究サービス機関

TrendLab やサポートセンターに勤務する、熱意ある献身的な 1,000 人を超えるセキュリティ専門家によって脅威情報が分析される。組み込みのフィードバックループによって Trend Micro の製品と同社の脅威研究センターや脅威研究テクノロジーの間に継続的なコミュニケーションが行われ、包括的な脅威対策が形成される。

Trend Micro の Smart Protection Network に
より、顧客ははコンテンツセキュリティへの脅威の拡大と巧妙化に対応するよう設計された新しいセキュリティパラダイムを展開できる Smart Protection Network は最新の脅威に対応するスマートなセキュリティを提供する。

Trend Micro の有効性

知は力なり：結果をすぐにもたらす効率的なセキュリティ

ことわざにあるとおり、結果はそれ自身が雄弁に語るものだ。業務遂行上電子メールとウェブに大きく依存し、これまでにスパムやあらゆる形態のマルウェアの発生に圧倒されていた Trend Micro の顧客は、Trend Micro Smart Protection Network で駆動するソリューションからすぐに成果と利益を得ている。Trend Micro の顧客の 1 社は「スパマーとの分刻みの戦争」が存在すると信じているが、クラウドコンピューティングテクノロジーが機能するまでの早さを称賛した。

別の Trend Micro 顧客は、電子メールとインスタントメッセージングは同社のビジネスにとってクリティカルな部分だと話した。同社のメッセージング要件は 24 時間年中無休の運用で、その中で大量のオンライン注文を生成する。この機能が侵され、通信不能な状態が数時間続くと、ビジネスに致命的な影響を与えるという。Smart Protection Network によって駆動される Trend Micro の電子メール/インスタントメッセージングセキュリティにより、顧客は「設定するだけ」の保守状態に近づいている。ほとんどの脅威がすぐ止まったことから、良好な保護を受けられることを顧客は確信している。

時は金なり：複雑さを軽減したコンテンツセキュリティ

IT 組織は常に、システムの管理と保守のためにスタッフが消費する時間の量を削減するためのオプションを評価している。以前に説明したように、時間はたしかにお金に換算できるが、日常業務に消費する時間もまた、機会費用と機会損失を意味する。Trend Micro のサーバー型メッセージングセキュリティを使用する IT マネージャの 1 人はこう話す。「弊社のメッセージングシステムのサポートにはパートタイマー 4 人しか割り当てられないため、Trend Micro Smart Protection Network を導入した最大のメリットは手動のパッチ適用とアップグレードがなくなったことでした。製品の日常保守が削減できたため、以前に比べてプロアクティブになっています。」

別の聞き取り調査では、Trend Micro ウェブセキュリティを使用する IT マネージャは、このソリューションを導入する前にはスパイウェアとマルウェアに関するたくさん問題があったと語る。「私たちはウイルス保守に時間を使いすぎていました。Trend Micro のソリューションを使い始めてから、ウイルスは一度も発生していません。以前に経験していたダウンタイムでは、セキュリティ違反に対抗するために大幅な残業時間が発生していました。状況は大幅に改善され、残業の必要もなくなりました。」

強力な管理コンソールがもたらす時間と資金の節約能力は、Trend Micro 顧客の間のテーマとなっている。Trend Micro Control Manager (Trend Micro Product Descriptions セクションで説明) では、管理者はグローバルポリシーを設定し、世界中に適用することができる。管理者はコントロールパネルを使用して、集中管理ビューから「ネットワークで起こっていることの概観」を確認することができる。また、Trend Micro Control Manager は、セキュリティとユーザー生産性の面で Trend Micro 製品が実現している ROI についての情報を経営陣に示すツールともなっている。

確実な利益をもたらす親密な関係

Trend Micro 顧客への聞き取り調査から浮かび上がってくるのは、顧客の成功に心から関心を抱く企業の鮮明な像である。ある顧客はこう話す。「Trend Micro とはこれまでのどのベンダーよりも良い関係を維持しています。Trend Micro はこのように顧客へのフォローアップを行い、製品の効果と存在しうるギャップについて、実際に即したフィードバックを収集しています。」

米国とヨーロッパに支社がある国際的な顧客は次のように指摘する。「Trend Micro は世界中の顧客にサポートを提供しています。すばらしいサポートです。」

Trend Micro の顧客は「設定するだけ」の保守状態に近づいている。ほとんどの脅威がすぐ止まったことから、良好な保護を受けられることを顧客は確信している。

「私たちはウイルス保守に時間を使いすぎていました。Trend Micro のソリューションを使い始めてから、ウイルスは一度も発生していません。」

「Trend Micro とはこれまでのどのベンダーよりも良い関係を維持しています。Trend Micro はフォローアップをしてくれます。」

また別の顧客は、Trend Micro が顧客の成功にいかにか意欲的であるかを語る。「Trend Micro のセールスおよびエンジニアリングチームからの支援には非常に感動しています。弊社は売りっぱなしのソフトウェアベンダーに慣れていましたが、Trend Micro はこちらの成功を明確に意欲を持って後押ししてくれました。ネットワーク全体への展開がスムーズに問題なく進行し、弊社におけるすべての要件が確実に満たされるよう、必要なすべての情報を揃えてくれたのです。」

「Trend Micro は、ネットワーク全体への展開がスムーズに問題なく進行し、弊社におけるすべての要件が確実に満たされるよう、必要なすべての情報を揃えてくれたのです。」

Trend Micro 製品の説明

エンタープライズ向け Trend Micro 製品

Trend Micro は、安全なコンテンツ/脅威マネジメントソリューションの強力なラインナップを揃えている。同社はさまざまな統合ソリューションを提案しているが、個々に購入可能なポイント製品の提供も続けている。単一の Trend Micro 製品と完全なセキュリティソリューションのどちらを選んでも、Smart Protection Network 内の相互関連型脅威対策のため、よりよい保護を受けることができる。

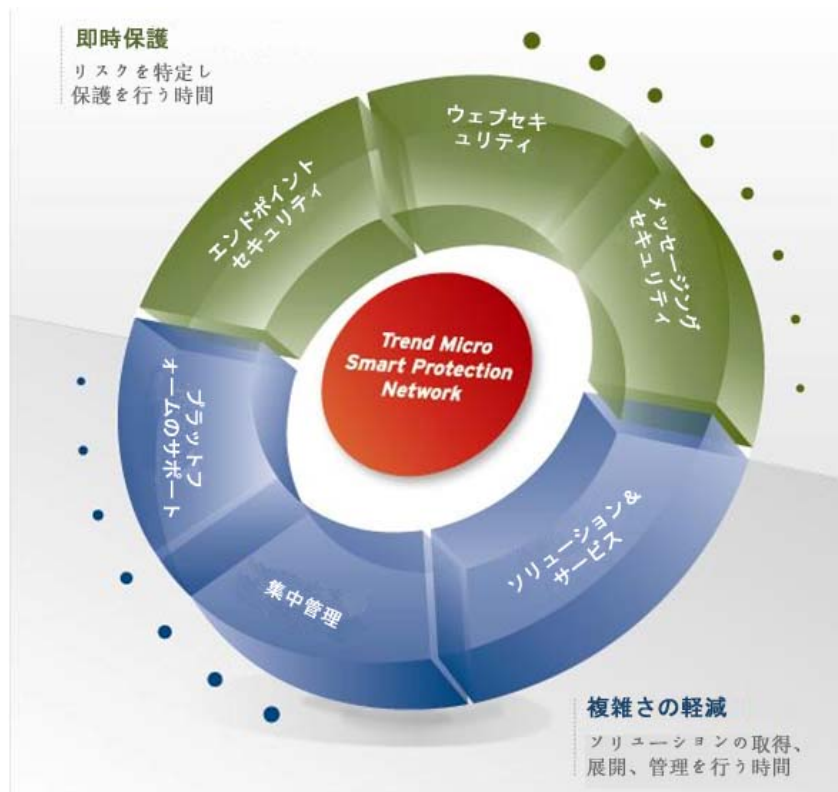
Trend Micro Smart Protection Network は、Trend Micro の製品とサービスの基盤となる、ハイブリッドなインザクラウド型アプローチを実現する。

Trend Micro 製品およびソリューション

Figure 1 に示すように、Trend Micro のコンテンツセキュリティ製品は主に 3 つのカテゴリに分かれる。ウェブセキュリティ、メッセージングセキュリティ、エンドポイントセキュリティである。

FIGURE 1

Trend Micro コンテンツセキュリティ製品のカテゴリ



Source: Trend Micro, 2008

Trend Micro Web Security は、脅威がネットワークに到達する前にブロックし、マルウェア攻撃、不適切なコンテンツ、その他のネットワーク外の脅威からネットワークから保護する。また **Smart Protection Network** の使用によって、統合されたリアルタイムアプローチを脅威管理に導入することで、TCO を削減する。さらに、**Web Application Security** により、企業のウェブサイトの保護を支援する。このソリューションは一定間隔またはオンデマンドの脆弱性アセスメントスキャンを行い、幅広いエキスパートレポートを自動的に生成する。

Trend Micro Messaging Security は、スパム、マルウェア、混合されたウェブの脅威、ゼロデイアタック、データ損失など、メッセージングに関する脅威から組織を保護する。このソリューションは **Trend Micro Smart Protection Network** を活用して、サーバー側、ソフトウェア、および IM/コラボレーション環境でのバーチャルアプライアンスソリューション、メールセキュリティ、および保護を備えた周辺部電子メールセキュリティについて、複雑さを軽減した即時保護を行う。また、電子メール暗号化とデータリーク保護ソリューションによって、さらにセキュリティが強化される。

Trend Micro Endpoint Security は高度な検索テクノロジーとクリーニングテクノロジーの業界独自の組み合わせを使用し、また **Smart Protection Network** のリアルタイム脅威対策を活用して、今日の複雑なマルウェアの脅威からノートパソコン、デスクトップ、サーバーを保護する。インザクラウド型のウェブレピュテーションは、悪意あるサイトからの、およびサイトへのアクセスをブロックして、ネットワークに接続されたクライアントと接続されていないクライアントをともに保護する。

総合スイート は、コンテンツセキュリティ脅威をブロックする、より包括的なアプローチを提供する。一部の **Trend Micro** スイートはデスクトップからゲートウェイまでの保護を目的とし、別のスイートは特定のプラットフォームやビジネス上の痛点をターゲットにしている。

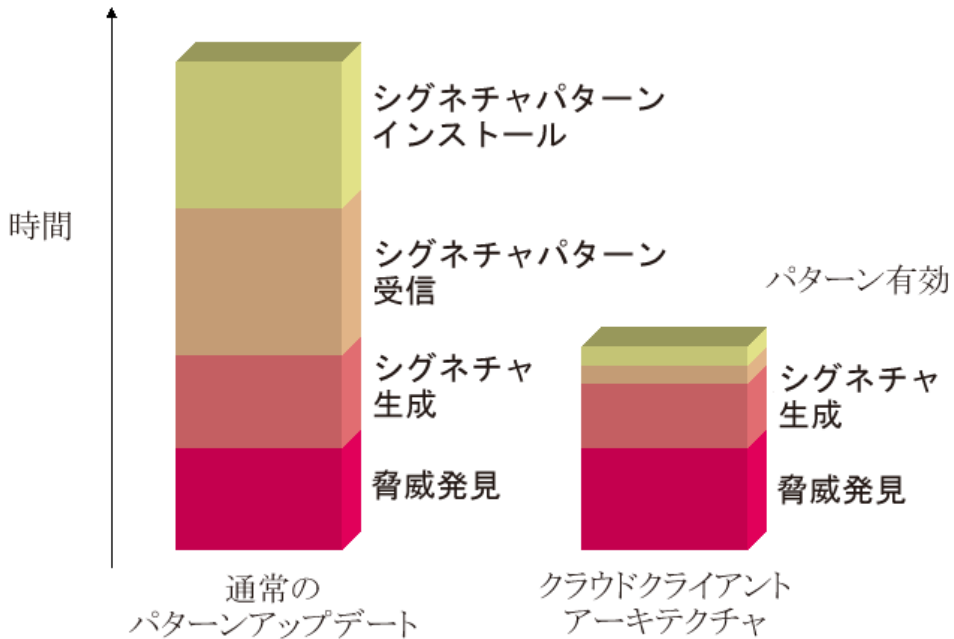
Trend Micro Control Manager は、ウェブベースのコンソールを備えた、集中管理型のセキュリティマネジメントを提供する。**Control Manager** は、追加のクライアントベースソフトウェアを必要とせずに、個々のクライアントの詳細な情報を表示する。また、統合化されたアップデート、グローバルアラート、カスタマイズ可能な脅威レポートも提供する。さらに、**Control Manager** は **Trend Micro Outbreak Prevention Services (OPS)** とセットで動作し、プロアクティブな脅威固有ポリシーのダウンロードと展開を可能にしている。

脅威の 1 歩先を走り続けるという挑戦

レガシー型のセキュリティシステムを保守する IT スタッフメンバーは、増え続ける今日の複雑な脅威の 1 歩先を走り続けるという挑戦に不必要に縛られている。レガシー型のソリューションは増加する脅威の量に対抗できず、ネットワークリソースのダウンを誘発し、保護の遅れによるセキュリティのギャップに企業をさらしている (Figure 2 参照)。

FIGURE 2

保護までの時間



Source: Trend Micro, 2008

また、個々に保守管理するポイントソリューションに基づいたセキュリティシステムで自衛するビジネスは、スタッフに負担をかけるだけでなく、システムをダウンさせる可能性を秘めたウイルスを逃してしまうリスクを負っている。今日のビジネスは、ネットワーク侵入が成功した際のダウンタイムや、機密情報が盗まれた際の被害に耐えられない。IT 部門はこれらが発生しないように警戒する重大な責任を負っている。

従来のコンテンツセキュリティはパターンファイルの更新に頼っていた。これはリアクティブで、展開までに数時間から数日かかることがある。しかし、攻撃があらゆる方向から迫り驚きの速さで侵入する、めまぐるしい変化にさらされた脅威の環境では、従来型の手法は適切ではなくなっている。Trend Micro のクラウドクライアントアーキテクチャは、脅威対策がネットワーク外のクラウドに常駐するためより迅速である。この方法なら、静的パターンファイルの周期的ダウンロードを待つことなく、Trend Micro はレピュテーションデータベースをよりすばやく更新でき、ビジネスは必要に応じてこの情報にすばやくアクセスできる。

結論

コンテンツセキュリティ環境の管理と保護は、日を迫うごとにますます難しくなっている。スパム、スパイウェア、データ盗難用マルウェア、ウイルス、内部の機密漏洩、ポータブルデバイス、その他の襲撃は、ネットワークの保護側が防衛するより急激なペースで成長を続けている。

攻撃者やスパム送信者との戦争では、企業は脅威に対抗する知識(ナレッジ)を持つことで優位に立つことができる。ここでいう知識とは、脅威を理解し、これらの脅威、特に最新の脆弱性を阻止できる防衛手段を展開することである。従来型のソリューションには、脅威の発見から、シグネチャファイルまたはパターンファイルをロールアウトするまでの期間に起因する遅延が存在する。クラウド内で脅威を取り除くことにより、脅威が企業の防衛線に到達する前に保護の準備ができるため、脅威を迅速にブロックできる。Trend Micro はコンテンツセキュリティ上の脅威に対抗する知識と防衛手段を、同社の Smart Protection Network のクラウドクライアントアーキテクチャに利用している。

Trend Micro の密に統合されたウェブ、メッセージング、およびエンドポイントソリューション/サービスは、管理を容易にし、企業がコンテンツセキュリティを購入、展開、管理する時間を節約できるようにする。機能強化されたコンテンツセキュリティを導入することで、企業は優先度の高いその他のイニシアチブにフォーカスし、生産性と売り上げのアップにつなげることができる。

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2009 IDC. Reproduction without written permission is completely forbidden.