

Symantec Brightmail™ Gateway

数々の賞に輝く、インバウンド保護とアウトバウンド制御のためのメッセージセキュリティ



概要

Symantec Brightmail Gateway は、効果的で正確なスパム対策とウイルス対策の保護、高度なコンテンツフィルタ、情報漏えい対策技術によって、電子メールとインスタントメッセージ(IM)に対してインバウンドとアウトバウンドのメッセージセキュリティを提供します。Brightmail Gateway は管理が簡単で、99% を超えるスパムメールを捕捉し、誤検知率は 100 万分の 1 未満です。Brightmail Gateway を使用すると、企業は新しいメッセージの脅威に有効に対処でき、ネットワークの停止時間を最小限に抑え、従業員の生産性を維持し、企業のレピュテーションを保護することができます。Brightmail Gateway は、Symantec Global Intelligence Network からのスパム対策とウイルス対策の継続的な自動更新、グローバル IP レピュテーションと自己学習型のローカル IP レピュテーションを使用したオンボックスの接続スロットル、包括的なレポート機能を利用します。

Brightmail Gateway は、物理アプライアンス上、および VMware 環境上で稼働する仮想アプライアンスとしても利用でき、スパム量が増え続け、予測不能な状況でも、企業はスパム対策機能を簡単に設定してメッセージが滞りなく流れるようにすることができます。Brightmail Gateway は Symantec Multi-tier Protection の一部としても提供されております。Multi-tier Protection は、デスクトップからゲートウェイに至るまでを複雑なデータ紛失、マルウェア、スパムの脅威から保護するエンドポイントセキュリティとメッセージセキュリティのスイートで、コストを抑えリスクを管理することができます。

稼働時間と生産性の確保に役立つインバウンドのスパム対策とウイルス対策

Brightmail Antispam™ エンジン、スパム対策における 10 年以上の実績をもとに開発されました。Brightmail は、他の多くのエンジンとは異なり、20 種類を超えるスパム対策技術を採用しています。Brightmail Gateway は、検知率が 99% を超え、致命的な誤検知率が 100 万分の 1 未満であり、業界で最も精度の高いソリューションの 1 つとなっています¹。

Brightmail Gateway は、Symantec Global Intelligence Network を活用して、スパム対策情報を継続的に自動更新することで新しい攻撃からのリアルタイムの保護を提供します。Global Intelligence Network には、次のものが含まれています。

- 1 億 2 千万以上のウイルス対策センサー
- 4 万以上のファイアウォールと侵入検知センサー
- 70 カ国におけるマネージドセキュリティ配備
- シマンテック社が特許権を有する 250 万以上のデコイ(おとり)アカウントから成るプローブネットワーク

シマンテック社では、8 億以上のメールボックスをウイルスやスパムから保護します。Brightmail レピュテーション適管理は、オンボックスの接続スロットルを配信し、グローバル IP レピュテーションと自己学習型のローカル IP レピュテーションの分析をインテリジェンスリソース割り当てと組み合わせて、悪質な送信者をネットワークレベルで遮断することでスパムフィルタを改善します。Brightmail Gateway は、スパム量を減らし、電子メールを保護することにより、メッセージインフラストラクチャを保護し、業務の稼働時間とユーザーの生産性を確保するのに役立ちます。

¹ InfoWorld 誌による Technology of the Year Award の Best Anti-Spam/Mail Security Solution 部門賞を 2005 年から 2008 年まで受賞しました。

Brightmail Gateway は、1999 年 11 月以来、40 回以上連続で VB100 有効性評価を獲得するという業界唯一の記録からも明らかのように、ほかに例を見ないウイルス対策保護を提供します。Brightmail Gateway には、ゼロデイウイルス対策保護が組み込まれており、定義が利用可能になる前に疑わしいメッセージを先取的に検出し、検疫することで停止時間のリスクを軽減します。

Brightmail Gateway はウイルスやスパム(IM ベースのスパム)からの IM 保護機能を統合します。これには、IM を通じてウイルスやワームに対する業界初のゼロデイ脅威からの保護も含まれます。

規制への対応と企業レピュテーションの保護に役立つ機密データフローのアウトバウンド制御

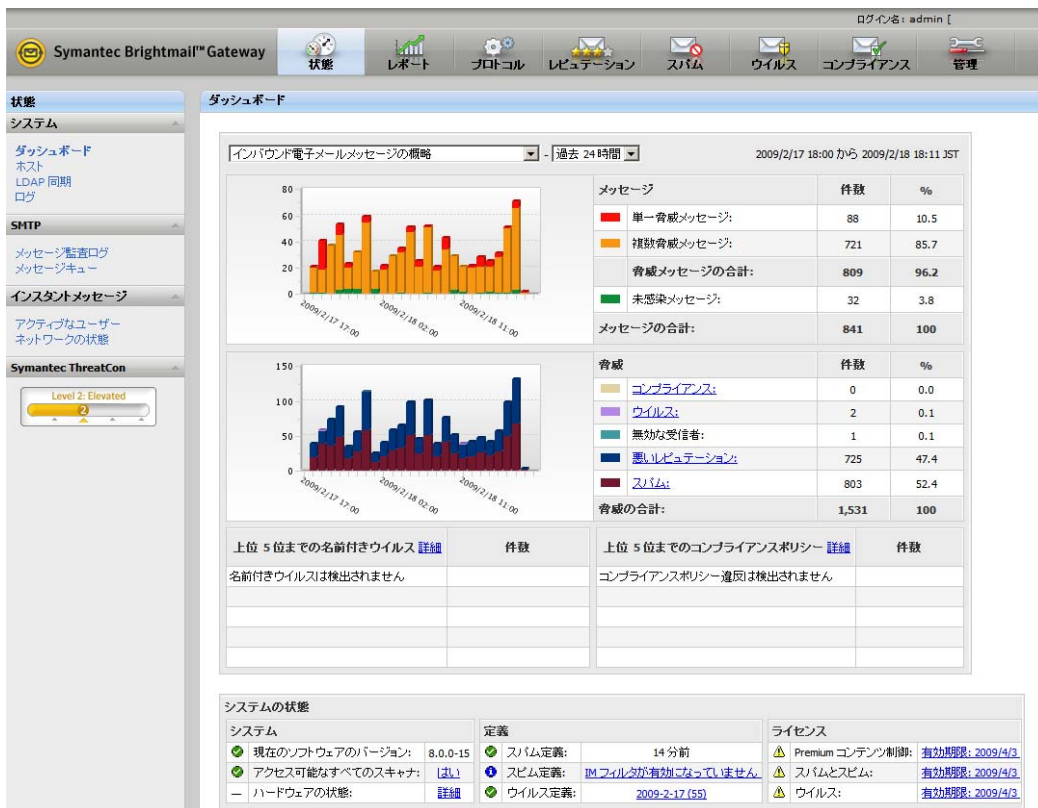
Brightmail Gateway は、機密データの保護と制御を容易にする高度なコンテンツフィルタと情報漏えい対策技術を特徴としています。管理者は、規制コンプライアンスを実施し、情報漏えいを防ぐ効果的で柔軟なポリシーを簡単に作成できます。ドメイン単位とポリシー単位の TLS (Transport Layer Security) 暗号化、インシデント管理、メッセージや添付ファイル内をスキャンするキーワードと正規表現、実際のファイルの類別は、管理者がメッセージコンテンツを管理し、規制に従うのに役立ちます。お客様は、事前設定済みのテンプレートと辞書を使用して、情報漏えい、内部ガバナンス、特定の法令順守に関連するリスクを管理するポリシーを簡単に配備できます。

Brightmail Gateway アプライアンスでは、Symantec Data Loss Prevention (情報漏えい対策製品) の高度な構造化データ照合技術との統合を利用して、アウトバウンドにおける最適な情報漏えい対策環境を構築できます。

データシート: メッセージセキュリティ
Symantec Brightmail™ Gateway

管理者は、疑いのあるメッセージの配信を許可する前にそれらに「レビュー保留」のマークを付けるポリシーを作成し、必要に応じてコンプライアンスまたは法務担当者が管理上の介入を行う機会を提供できます。このような設定しやすく統合されたワークフローツールを使用すると、業務を中断することなく、データを制御し、ポリシー違反に対処するためのポリシーを作成できます。

Brightmail Gateway は、IM トラフィックとコンテンツの管理を統合して、すべての IM トラフィックに対して ID 管理を実施し、ユーザーに Active Directory® または他のディレクトリサービス ID への登録を要求することで、IM トラフィックの認証と制御を行います。管理者は、アクセスを許可する IM ネットワークを選択したり、特定の機能(グループごとのファイル転送など)を無効にすることができます。これらの制御を行うことで、IM インフラストラクチャの管理容易性が向上し、かつ、ユーザーの利用意識が強化されます。



統一された管理と運用によるコストと複雑さの削減

Brightmail Gateway には、企業のメッセージインフラストラクチャの統一された管理と運用のための強力なコントロールセンターがあります。

管理者は、1 台の Web ベースのコンソールから、複数の Brightmail Gateway アプライアンスを管理して、傾向、攻撃の統計、非標準のインシデントを簡単に表示できます。複数のコンソール、多様なポリシー、互換性のないログ記録とレポートの手順などによる複雑さをなくすことで、Brightmail Gateway では、メッセージセキュリティインフラストラクチャの総所有コスト(TCO)を大幅に削減します。

Brightmail Gateway は、システムの有効性と影響を容易に把握するダッシュボードやエグゼクティブサマリーなど、すべてのレポートオプションをサポートします。管理者は、レポート機能を使用して、情報漏えいの傾向を確認したり、コンプライアンスを立証したりできます。管理コンソールには、50 種類以上の事前設定したレポートが用意されており、コンテンツまたは時間でのカスタマイズ、レポートの自動生成用のスケジュールの設定、およびエクスポートすることができます。GUI のメッセージ監視インターフェースを介してメッセージの追跡が簡単に行えるので、管理者はメッセージの処置を迅速に決めることができます。

Brightmail Gateway は設定の必要がほとんどなく、箱から取り出してすぐに使えるため、初期配備を簡単かつ迅速に進めることができます。スパムシグネチャとウイルス定義は強力な Symantec Global Intelligence Network を利用して自動的に更新されるため、管理が簡略化され、企業全体にわたって最新の脅威を検出できるというメリットを確実に得られます。

重要なメリット

Symantec Brightmail Gateway は、実質的で重要なメリットを企業に提供します。

- スパムやマルウェアがサーバーに届く前にそれらを電子メールや IM から削除して、メッセージインフラストラクチャを最適化する
- ゼロデイウイルス対策保護を使って、定義が利用可能になっていなくても、疑いのあるメッセージや添付ファイルを先取的に検出し、検疫することで停止時間のリスクを軽減する
- 数々の賞に輝いたスパム対策の効果(99% を超えるスパムメールを捕捉)と精度(誤検知率 100 万分の 1 未満の精度)のバランスを保つ
- 規制要件やガバナンス要件を順守するためにインバウンドとアウトバウンドのメッセージトラフィックをスキャンする
- 企業がポリシーを実装し、違反を分析、管理できるようにするインシデント管理とレポート機能を提供する
- ルールの自動更新を配信して、新しい脅威に対するリアルタイムの効果的な防御を確実に行えるようにする
- ほかに例を見ないウイルス対策保護を提供する(1999 年 11 月以来、連続して VB100 有効性評価を獲得するという業界唯一の記録により証明済み)

システムの必要条件

サポートされるプラットフォーム

Symantec Brightmail Gateway は、小企業から大企業に至るすべての規模の企業で調整可能な Brightmail/Mail Security 8300 シリーズのハードウェアアプライアンス上に配備できます。また、仮想アプライアンスとして使用可能な VMware® 環境上で稼働する Brightmail Gateway Virtual Edition も提供しております。アプライアンスは、専用のコントロールセンター、スキャナ、またはコントロールセンターとスキャナの組み合わせとして配備できます。

アプライアンスモデル	8340	8360	8380
プロセッサ	Intel® Core™ 2 Duo E4500 × 1	Intel® Xeon® E5520 × 2	Intel® Xeon® E5540 × 2
メモリ	4GB	8GB	8GB
ハードディスク	160GB × 2 (Serial ATA)	146GB × 2 (Serial Attach SCSI)	300GB × 6 (Serial Attach SCSI)
冗長構成	ハードディスク (RAID 1)	ハードディスク (RAID 1) 電源/電源ファン	ハードディスク (RAID 1+0) 電源/電源ファン
シャーシサイズ	1U (19 インチラック)	1U (19 インチラック)	2U (19 インチラック)
外形寸法	44.7 W × 4.3 H × 54.6 D (cm)	48.3 W × 4.3 H × 77.2 D (cm)	44.31 W × 8.6 H × 68.07 D (cm)
重量	11.8kg	17.7kg	26.1kg

※その他、規格に関しては製品マニュアルに記載されています。また、Symantec Brightmail 8340/8360/8380 アプライアンスは RoHS 指令に適合しています。

サポートされるインターネットブラウザ

- Microsoft® Internet Explorer® 6.0、7.0
- Firefox 2.0、3.0

サポートされる仮想プラットフォーム

- VMware ESX Server 3.x、4.0 (vSphere)
- VMware ESXi 3.x



製品に関する最新の情報

シマンテックの Web サイトをご覧ください。

<http://www.symantec.com/jp/business/>

株式会社シマンテック

〒107-0052 東京都港区赤坂 1-11-44 赤坂インターシティ
www.symantec.com/jp

お問い合わせ