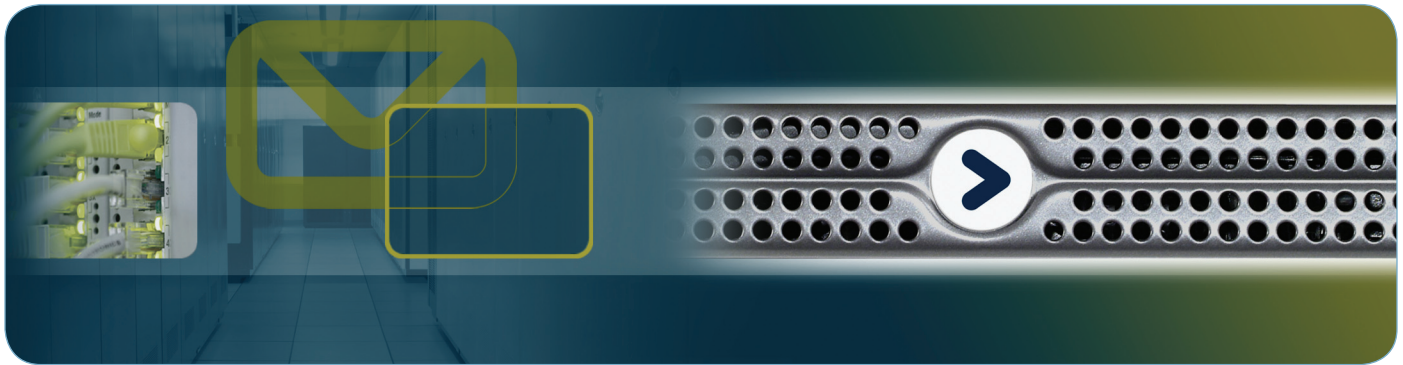


Proofpoint Messaging Security Gateway アプライアンス



Proofpoint on Demand ホストサービスと Proofpoint Protection Server ソフトウェア



Proofpoint Messaging Security Gateway™ アプライアンス、Proofpoint on Demand™ サービス、そして Proofpoint Protection Server® ソフトウェアは、インバウンドメッセージに伴う脅威からの防御、機密情報の漏洩防止、メッセージの暗号化、メッセージングインフラの分析を行います。これらの統合型アーキテクチャ、モジュール式防御、ポリシー管理インターフェイスは、まさにエンタープライズゲートウェイにおけるあらゆる種類のメッセージングリスクから組織を守ります。

防御、防止、暗号化、分析

なぜまた別のポイント・ソリューションを導入するのですか？ Proofpoint の統合型電子メールセキュリティ/データ損失防止プラットフォームは、インバウンド脅威とアウトバウンドコンテンツセキュリティリスクの両方に対して総合的な防止効果を発揮します。そして Proofpoint のモジュール式アーキテクチャでは、必要に応じて新たな防御機能を簡単に導入することができます。

スパム対策、ウィルス対策、マルチプロトコルコンテンツセキュリティ、ポリシーベースの暗号化およびレポーティングといった機能を含めて Proofpoint の全機能は、単一の管理 GUI から集中的に管理され、統合型アプライアンスアーキテクチャ上に導入されます。各機能は組織の固有要件に応じるために、ほぼあらゆるコンフィギュレーションにおいて導入することができます。

導入に伴う Proofpoint サーバが 1 台であるかそれ以上であるかを問わず、グローバルに分散されたアプライアンスやすべてのポリシー管理タスクは Proofpoint の集中型ウェブベース管理コンソールを介して制御されます。

自由度の高い導入オプション

Proofpoint の電子メールセキュリティ/データ損失防止ソリューションは、最大限の導入自由度を確保するためにさまざまなフォームファクターで提供されています。

- **ハードウェアアプライアンス**：Proofpoint Messaging Security Gateway は数分でインストールできる安全で導入簡単な強化されたアプライアンスです。あらゆる規模のエンタープライズをサポートするためにさまざまなアプライアンスモデルが用意されています。
- **バーチャルアプライアンス**：Proofpoint Messaging Security Gateway - Virtual Edition は Proofpoint のハードウェアアプライアンスと同じクラスで最高のプロテクト効果を発揮するだけでなく、コスト削減、迅速な導入とプロビジョニング、簡易化された変更管理、簡単なバックアップと障害復旧など、多くの仮想化メリットもあります。仮想アプライアンスは VMware Server または VMware インフラを用いた標準 x86 デスクトップまたはサーバで動作します。
- **ソフトウェア**：Proofpoint Protection Server は Sun Solaris または Red Hat Enterprise Linux オペレーティングシステム用のソフトウェアとして Proofpoint のメッセージングセキュリティプラットフォームを提供しています。
- **ホストサービス**：Proofpoint on Demand は、構内のハードウェアやソフトウェアを必要としない経済的で、高度なカスタマイズ化が可能なオンデマンドサービスで Proofpoint の電子メールセキュリティやデータ損失防止の機能を提供します。

安全、効果的、簡単導入

Proofpoint の統合型電子メールセキュリティ/データ損失防止プラットフォームを説明する上で、これらの言葉はその特徴のごく一部を表しているにすぎません。これは業界でもっとも強力なソリューションがエンタープライズ対応アプライアンス、仮想アプライアンス、またはソフトウェアとしてパッケージングされたもので、次のような特徴を備えています。

- 他社の追従を許さないスパム検出とコネクシオンマネージメント
- ワールドクラスのウィルス対策
- 総合的なマルチプロトコルデータ損失防止およびコンテンツセキュリティ
- ポリシーベースの電子メール暗号化
- 先進的なレポーティングおよび分析
- 統合型ポリシー管理
- エンタープライズグレードのパフォーマンス
- 迅速な導入とプロビジョニング
- 最適なスケラビリティアーキテクチャ

“Pacific Sunwear 社では、非常に多数のスパム対策やウィルス対策、コンテンツキャッシング製品を評価してきましたが、当社が持つ電子メールとメッセージングに関するすべての課題を、導入と管理が容易な 1 つのソリューションで解決できるプラットフォームを提供している企業は Proofpoint が初めてでした。Messaging SecurityGateway アプライアンスは、当社の電子メールチャネルがメッセージングの威を素通りさせる回転ドアとしてではなく、ビジネス通信のための戦略的なルートとしてみごとに設計されていました”
パシフィック・サンウェア
(Pacific Sunwear)
インフォメーション・システムズ担当
バイスプレジデント (VP of Information Systems)
ロン・エアーズ氏 (Ron Ehlers)

完全な対策

Proofpoint MLX テクノロジー 先進的マシンラーニング

Proofpoint のエンタープライズメッセージングセキュリティソリューション – Proofpoint MLX – の背後には、Proofpoint Attack Response Center の科学者たちが開発した特許出願済中の先進的マシンラーニングシステムが力強くバックアップしています。ロジスティック回帰や情報獲得分析などの先進的統計技法に基づいて、Proofpoint MLX は電子メールやその他のドキュメントで見られるような非組織化コンテンツの正確な分類や識別を可能にします。

比類ない精度

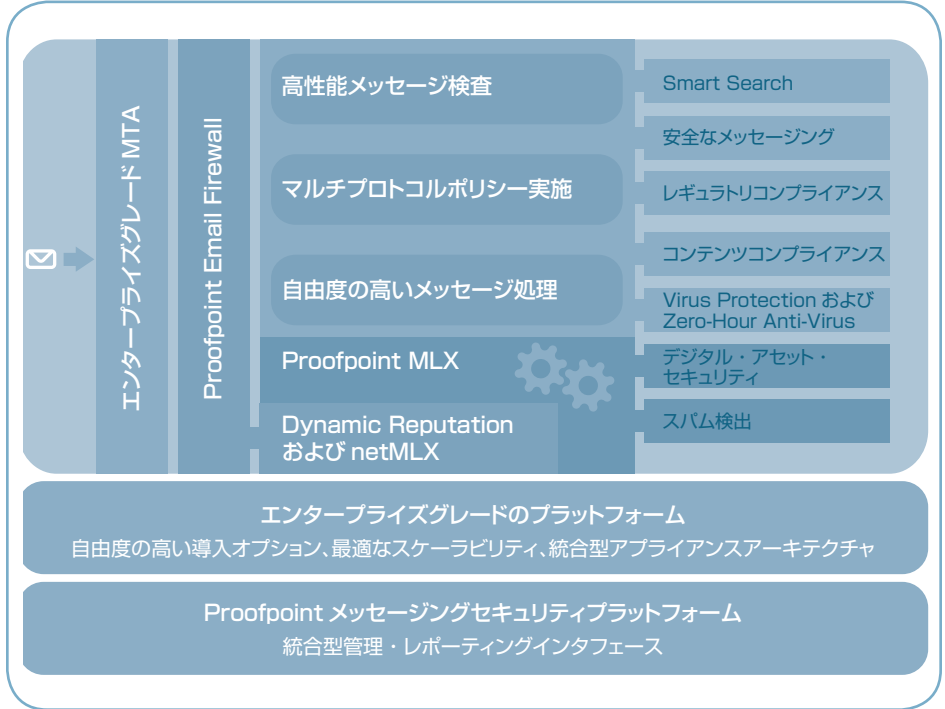
Proofpoint MLX は Proofpoint Spam Detection モジュールによってもたらされる無類のスパム対策精度の基礎となるものです。MLX を使用して、Proofpoint はスパムと有効なメッセージを正確に区別するために何十万という構造上、画像上、コンテンツ上、レピュテーション上の属性を分析します。従来のスパム対策ソリューションは限定数の属性だけを評価し、スパムを決定的に分類することができず、検知率の低下や偽陽性率の上昇という結果になりました。

将来に対して万全なインテリジェンス

Proofpoint のインテリジェントスパム対策技術は継続的に自己更新を行って、新しい形態のスパムに対して防衛を実施します。Proofpoint の科学者たちが開発した現行の自己トレーニングや新技術のおかげで、MLX は新しい形態のスパムを予想することができ、そういったスパムが現れてもそれらに適応することができます。MLX の更新は 1 日に数回すべての顧客に自動的に配信されます。結果として、もっとも困難な形態の画像ベースのスパム、後方散乱 (backscatter)、日本語スパムに対しても、Proofpoint MLX は 99.8% を超える検知率を実現します。

他のウィルス対策ソリューションと違って、スパム攻撃を防御する Proofpoint の能力は時の経過とともに低下せず、MLX スパム対策エンジンに対する更新は自動的にユーザーのエンタープライズに定期的に届けられます。Proofpoint MLX は浮上する脅威に対抗してたえず進化しており、ユーザーのメッセージングインフラが今日のスパマーだけでなく明日のスパマーに対しても安全であることを確実にします。

Proofpoint MLX は Proofpoint Digital Asset Security モジュールの先進的コンテンツセキュリティ機能や、Proofpoint Email Firewall および Dynamic Reputation サービスのインテリジェント周辺セキュリティ機能も支えています。Proofpoint はこういった強力なマシンラーニングテクニックを電子メールセキュリティおよびデータ損失防止に応用している唯一のベンダーです。



インバウンド脅威に対する防衛

Proofpoint MLX[™] に支えられた先進的スパム検出

特許出願中の Proofpoint MLX マシンラーニングテクノロジーによって支えられた Proofpoint Spam Detection[™] モジュールは、メッセージエンベロープヘッダおよび構成、画像プロパティ、差出人レピュテーションデータ、そしてメッセージの本文における非構造化コンテンツなど、あらゆる電子メールにおける何十万の属性を調べ、新しい攻撃が出現するたびにそれらに自動的に適応しながら、ほとんどのスパム、画像ベースのスパム、フィッシング攻撃を阻止します。そして、Proofpoint Dynamic Update Service[™] はユーザのスパム対策を自動的に最新の状態に維持し、いつでも最大の検知率を保証します。スパムスコアやアダルトコンテンツスコアは個別に管理できるので、ボロノグラフィスパムに対してゼロトレランスポリシーを適用することができます。フィッシング対策機能は従業員から個人情報を盗むことからフィッシングやその他の ID 盗用攻撃が広がることを阻止します。また Bounce Address Tag Validation (BATV) を採用したバウンスマネージメントによって、Non-Delivery Report (NDR) メッセージを利用したスパム攻撃「後方散乱 (backscatter : バックスキャッター)」を 100% 防ぐことが可能です。

Proofpoint Spam Detection は多言語対応であり、日本語や中国語などの分析が難しい全角言語を含めていかなる言語によるスパムに対しても抜群の精度を誇ります。

スパム対策ポリシーは LDAP または Active Directory へ完全統合した状態でグローバルレベル、グループレベル、そしてエンドユーザレベルでカスタマイズして、現行の管理を合理化することができます。

統合型電子メールファイアウォール対策

Proofpoint Email Firewall[™] は、DNS、MX レコード確認、SPF、宛先確認、Proofpoint Dynamic Reputation 情報、および任意の netMLX データなど、数多くのコネクションレベルデータポイントを評価することにより、スパムや悪意のあるコネクションからステートフルな最前線の防御を行います。

革新的なコネクションマネージメント

Proofpoint netMLX[™] を備えた Proofpoint Dynamic Reputation[™] は、業界でもっとも強力なコネクションマネージメント機能を貴社の導入済 Proofpoint に提供します。これは強力なマシンラーニングアルゴリズムによって分析されたローカルな予測行動データとグローバルに観察したレピュ

インバウンド脅威に対する防御（続き）

テーションの組み合わせを用いて、悪意のある IP アドレスからのコネクションを阻止する唯一の電子メールレピュテーションサービスです。

Proofpoint アプライアンスおよびソフトウェアをすべて導入すると、ローカル IP トラフィックの内蔵型予測行動分析が実施されますが、これはリアルタイムで反応し、ターゲット攻撃によって引き起こされる電子メールトラックスパイクを除去したり、ボットネットからの悪意のあるコネクションを阻止または抑制したりします。電子メールの量が多いお客様は Proofpoint net-MLX の強化対策を自社の導入に追加して、合計 80% 以上インバウンドコネクション量を減少することができます。Proofpoint netMLX は、インターネット全体にわたって電子メールを配信するすべての IP アドレスに対する業界でもっとも正確かつ最新のレピュテーションデータベースを作成します。すべての IP アドレスに対する何千ものデータポイントは、分単位で先進的マシンラーニングアルゴリズムにより解析され、差出人のレピュテーションを表すスコアを生成します。Proofpoint Dynamic Reputation はローカル行動データと組み合わせられたこれらのスコアを用いて、電子メールコネクションを受け入れるか、抑制するか、あるいは拒否するかについてインテリジェントな決定を行います。

Virus Protection および Zero-Hour Anti-Virus 防御

Proofpoint Virus Protection™ は、主要なウィルス対策ベンダとの戦略的パートナーシップを通じて、完全なウィルススキャン機能を提供します。ウィルスエンジンは Proofpoint のプラットフォームに深く統合されており、スパムポリシーやコンテンツポリシーを管理するのに用いるのと同じインタフェースから、ウィルス対策ポリシーに対する便利な集中的管理を行います。メッセージは、スパムやメッセージコンテンツと平行してウィルスがないか効率的にスキャンされ、ウィルス、ワーム、その他悪意のあるコードからユーザを守ります。さらに、Proofpoint Zero-Hour Anti-Virus™ モジュールはそれらの拡散のもっとも早い段階における発現ウィルスへの対策を実施し、競合するソリューションが反応を始める何時間も前にそれらを阻止します。

複数プロトコルにわたる情報漏れを防止

Proofpoint の先進的データ損失防止機能は、アウトバウンド電子メールだけでなく、ウェブベースの電子メールや、ブログ投稿、メッセージボード投稿、その他の HTTP または FTP ベースのアクティビティを含む追加的なメッセージストリームを守ることができます。

コンテンツコンプライアンス：受け入れ可能な使用ポリシーを簡単に実施

Proofpoint Content Compliance™ によって、メッセージコンテンツや添付物に対する企業が受け入れ可能な使用ポリシーを定義し、実施することが簡単になります。便利なポイントアンドクリックインタフェースは、ファイルタイプ、メッセージサイズ、メッセージコンテンツに関連する複雑なルールを定義するプロセスを簡易化してくれます。これらの機能を使用すれば、攻撃的な言葉、ハラスメント、ファイル共有、外部規則の違反を含めて、非常に多種多様なインバウンドおよびアウトバウンドポリシー違反を特定し、防止することができます。

Regulatory Compliance：個人データを安全に保持

これまで以上に、エンタープライズはお客様や従業員のデータのプライバシーならびにセキュリティを守る必要があります。Proofpoint Regulatory Compliance™ モジュールは、個人データを保護し、かつプライバシーおよびデータセキュリティ規定 (HIPAA、GLBA、PCI、SEC ルールなど) に関連する責任から組織を守るためのベストプラクティスを実施します。カスタマイズ可能なルール、管理された辞書、そして「スマート識別子」を使用して、非公開情報、たとえば、保護された健康情報や個人的な財務情報がないか自動的にスキャンし、メッセージの拒否や暗号化を適宜行います。

Proofpoint のスマート識別子は単純な正規表現よりも洗練されています。これらの識別子は正しい桁数や文字数を探しますが、複雑なアルゴリズムによって、偽陽性をできるだけ少なくしながら、高い検出精度を確実にします。

Digital Asset Security：機密ドキュメントを保護

電子メール、ウェブメール、およびその他のメッセージングシステムは、もっとも重要なコミュニケーションツールになるにつれて、同時に機微な情報や機密情報が漏出するルートになってきました。Proofpoint Digital Asset Security™ モジュールは、貴重な法人資産や機密データが電子メールやその他のメッセージングプロトコルを介して自社組織外に漏れ出さないようにします。強力

集中的管理

ウェブベースのポリシー管理、管理、およびエンドユーザコントロール

Proofpoint Messaging Security Console™ は、Proofpoint の統合型ポリシー管理フレームワークに対する集中的な 100% ウェブベースの統括インタフェースを提供し、法人メッセージングポリシーの一貫した適用を確実にします。この Console によって、メッセージングインフラのモニタ・制御やメッセージングポリシーの定義が簡単になります。異なるエンドユーザグループに対して別々のポリシーを定義し、実施することさえできます。ユーザの導入に別の Proofpoint モジュールが追加されるにつれて、同じ便利なインタフェースがポリシー管理のために使用されません。

Ajax ベースのインタフェースでは、レポート、ステータス情報、RSS フィード、およびその他の表示コンポーネントの「ドラッグアンドドロップ」カスタマイズが可能です。外部ソースから情報の「マッシュアップ (複合コンテンツ)」の生成さえ行います。

Proofpoint の卓越した簡単使用はエンドユーザにもおよびます。わかりやすいレポートやコントロール、たとえば、Proofpoint のエンドユーザダイジェスト、ウェブベースの検疫、個別のセーフ/受信拒否リストなどによって、ユーザは自分自身のスパム選好を完全に支配できます。

堅固なレポーティング

Proofpoint Messaging Security Console は、50 を超えるリアルタイムのグラフィカルレポートおよびアラートへのアクセスも行い、これらによってユーザのエンタープライズメッセージングシステムの状態を完全に見ることができます。レポートは HTML/XML として簡単に電子メールで送ったり、ポストインクしたりすることができます。Proofpoint の「アクティブ」レポートは重要な情報を配信しますが、同時に管理者は即時処置を講じることができます (たとえば、リンクをクリックするだけで、不正な差出人を阻止します)。

ゼロアドミニストレーション

つねに最新の対策、最大限に簡単な管理

最新コンポーネントの自動インストールおよび通知によって、現行の管理は簡単になります。Proofpoint Dynamic Update Service は、ユーザのネットワークがメッセージ媒介脅威に対して最高レベルの対策をつねに実施することを確実にします。Proofpoint Dynamic Update Service は、ユーザの Proofpoint ソフトウェアまたはアプライアンス導入のあらゆるコンポーネントに対して継続的な更新を行います。これらのコンポーネントには強化されたオペレーティングシステムおよび MTA、スパムおよびウィルスエンジン、レキシコン (Proofpoint Regulatory Compliance モジュールによって使用される辞書など)、アプリケーションコンポーネント、カスタマイズされたホットフィックスが含まれます。

Proofpoint Messaging Security Gateway および Proofpoint Protection Server

機微な情報を暗号化

な MLX マシンラーニングテクノロジーは機密ドキュメントを分析・分類してから、アウトバウンドメッセージストリームにそのような情報（またはその一部）がないかモニタし、コンテンツセキュリティ違反を発生前に阻止します。

Proofpoint Secure Messaging™ は、強力なコンテンツ認識暗号化機能を貴社の導入済 Proofpoint に提供し、ユーザの組織のポリシーに基づいてメッセージを自動的に暗号化します。Proofpoint Secure Messaging はユーザの暗号化ポリシーを自動的に一貫して適用し、エンドユーザに特別な処置を講じることを必要としません。Voltage IBE (ID ベースの暗号化) テクノロジーは他のソリューションに伴うキーや証明書の管理の手間がかからない強力かつ使用簡単な暗号化を提供してくれます。Proofpoint のハードウェアおよび仮想アプライアンスはデジタル証明書もサポートしており、Transport Layer Security (TLS) を用いた電子メールのゲートウェイ間セキュア転送および受信を可能にします。

メッセージングインフラを分析

Proofpoint Smart Search™ は、メッセージトレッシング、フォレンジック、ログ分析といった先進的機能により Proofpoint の内蔵ロギング/レポート機能を強化し、ユーザのメッセージングインフラ全体にわたるメッセージフローに簡単なリアルタイムな視認性を提供します。グローバルに分散した導入済 Proofpoint 全体にわたってさえ、便利で簡単に使用できる単一の GUI からユーザのメッセージログを検索・分析します。

高性能、簡単導入、最適スケーラビリティ

Proofpoint Messaging Security Gateway および Proofpoint Protection Server は、大規模エンタープライズ、ISP、大学および政府機関の独自のニーズに応じるよう設計されました。どちらも大規模導入に必要な性能、フレキシビリティ、スケーラビリティ、カスタマイズ、エンドユーザコントロールといった機能をすべて備えています。

Proofpoint システムのコンポーネントはいずれもエンタープライズ性能に関する厳格な要求に応じるよう設計されています。Proofpoint アプライアンスで用いられる強固でメッセージング処理用に最適化された OS から、すべてのメッセージスキャン機能をメモリ内で行うことができる Proofpoint の独特なキューレスアーキテクチャにいたるまで、Proofpoint はどんなに高度な導入であっても必要な高性能を提供します。

Proofpoint アプライアンスおよびソフトウェアは、1 日あたり何百万というメッセージをサポートするよう無制限に規模の変化に対応します。これらは複数アプライアンスのマスタ/エージェントコンフィギュレーションで簡単に導入することができ、複雑な、または地理的に分散したデータセンタをサポートし、それによって単一の管理インタフェースの利便性と組み合わせられた 100% 冗長化されたセキュリティを提供します。Proofpoint はハードウェアと仮想アプライアンスの両方が協調したハイブリッド導入さえサポートしています。

Proofpoint の最適スケーラビリティアーキテクチャでは、単一のマスタコンソールからすべてのエージェントサーバを管理することができます。自動的なコンフィギュレーション伝播、集中的なメッセージ検疫、そして集中的なレポートングによって、保守が簡易化され、TCO が削減されます。

Proofpoint はどのように分散しようともあらゆる IT インフラと簡単に統合することにより、TCO をさらに削減します。GUI ベースの LDAP コマンドコンソールおよび Microsoft Active Directory® のサポートによって、ディレクトリサーバ統合は簡単になっています。Proofpoint は Microsoft Exchange® や Lotus Notes® といった過大な負荷のかかる電子メールサーバソリューションとも適合性があり、それらに対する負荷をできるだけ少なくします。

無料トライアル版—すぐにご試用を！

Proofpoint のパワーをご自分で体験してみてください。www.proofpoint.com/trial にて、Proofpoint のインバウンド電子メールセキュリティモジュールを備えた Proofpoint Messaging Security Gateway - Virtual Edition の完全動作 45 日試用版をダウンロードしてください。Proofpoint の仮想アプライアンスは数分で導入することができ、即座にあらゆる種類の電子メール媒介脅威から貴社の電子メールユーザを守ります。

アプライアンスバージョン

Proofpoint Messaging Security Gateway アプライアンスは、あらゆる規模の導入をサポートするためにさまざまなハードウェアコンフィギュレーションで用意されています。Proofpoint アプライアンスモデルに関する最新の情報については、以下をご参照ください。
www.proofpoint.com/products/msg.php

ソフトウェアシステム要件

Proofpoint Protection Server ソフトウェアはあらゆる下流電子メールサーバとも適合性があり、Linux のハードウェアプラットフォーム上で使用可能です。

Linux プラットフォーム

Red Hat Enterprise Linux ES 3.0 または 4.0
Red Hat Enterprise Linux AS 4.0

Virtual Edition 要件

Proofpoint Messaging Security Gateway - Virtual Edition は、事前インストールおよび事前コンフィギュレーションが完全に実施済みのエンタープライズメッセージングセキュリティアプリケーションとメッセージ転送エージェント (MTA)、そして VMware 仮想化製品を使用するあらゆる標準 x86 デスクトップまたはサーバで動作するセキュアな動作環境です。

製造、レピュテーション、または実験導入のためには、VMware Server または VMware Infrastructure (VMware ESX 3.0 以上) が必要です。

サポートされているブラウザ

すべてのコンフィギュレーションおよび管理タスクは、ハードウェアアプライアンス、仮想アプライアンス、ソフトウェアバージョンのいずれについても、Proofpoint の 100% ブラウザベースのインタフェースを通じて取り扱われます。サポートされているブラウザには以下が含まれます。

Microsoft® Internet Explorer 6.0 以上

Mozilla Firefox 2.0 以上

©2008 Proofpoint, Inc. Proofpoint Protection Server は米国およびその他の国々における Proofpoint, Inc の登録商標です。Proofpoint, Proofpoint Messaging Security Gateway, Proofpoint Email Firewall, Proofpoint Spam Detection, Proofpoint Virus Protection, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint Dynamic Update Service, Proofpoint MLX, Proofpoint Dynamic Reputation, Proofpoint netMLX, Proofpoint Smart Search, Proofpoint Messaging Security Console, Proofpoint on Demand は米国およびその他の国々における Proofpoint, Inc. の商標です。ここに含まれる他のすべての商標はそれぞれの所有者の所有物です。09/08