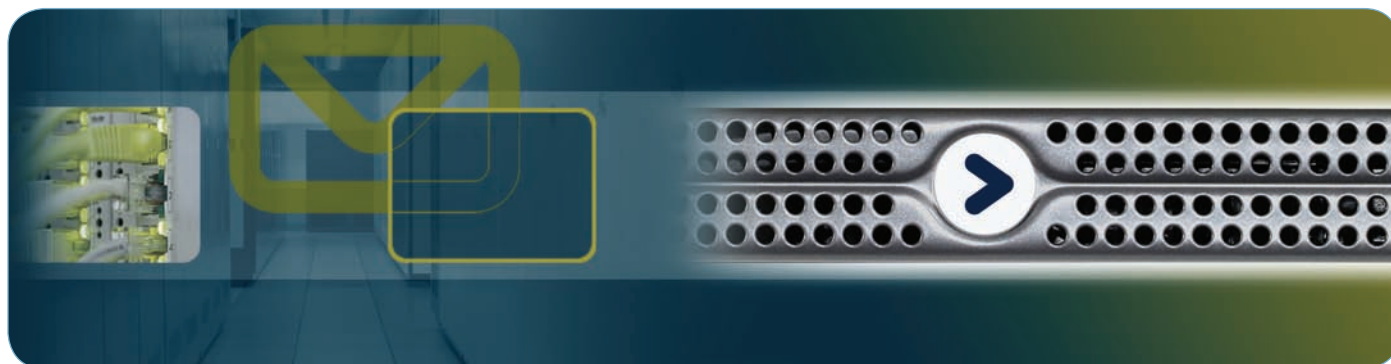


Dispositivos Proofpoint Messaging Security Gateway

Serviço Hospedado Proofpoint on Demand e Software Proofpoint Protection Server



Os dispositivos Proofpoint Messaging Security Gateway™, o serviço Proofpoint on Demand™ e o software Proofpoint Protection Server® defendem contra ameaças de mensagens de entrada, evitam vazamentos de informações confidenciais, criptografam mensagens e analisam sua infra-estrutura de mensagens. Suas defesas de arquitetura unificada, modular e interface de gerenciamento de políticas protegem as organizações contra todo tipo de riscos associados a mensagens—diretamente no gateway da empresa.

defender, prevenir, criptografar, analisar

Por que adquirir outra solução de ponta? A plataforma unificada do Proofpoint para prevenção de perda de dados e segurança de e-mail fornece proteção abrangente contra ameaças de entrada e riscos de segurança de conteúdo de saída—e a arquitetura modular do Proofpoint ajusta-se facilmente sempre que as necessidades mudam.

Todos os recursos Proofpoint incluindo anti-spam, anti-vírus, segurança de conteúdo multi-protocolo, criptografia baseada na política da empresa e recursos de emissão de relatórios—são gerenciados centralmente em uma única Interface Gráfica de Usuário (GUI) administrativa baseada na web e desenvolvida em uma arquitetura unificada de dispositivos. Os recursos podem ser implantados em praticamente qualquer configuração para atender aos requisitos exclusivos de sua organização.

Tenha sua implantação em um único servidor Proofpoint ou múltiplos servidores, dispositivos globalmente distribuídos, todas as tarefas de administração e gerenciamento de políticas são controladas por meio de um console de administração centralizada baseada na web.

opções flexíveis de implantação

As soluções de segurança de e-mail e prevenção de perda de dados do Proofpoint são oferecidas em vários fatores de forma para uma implantação com flexibilidade máxima:

- **Serviço hospedado:** O Proofpoint on Demand fornece recursos de segurança de e-mail e prevenção de perda de dados do Proofpoint em um serviço on-demand altamente personalizável e econômico que não requer hardware ou software instalados no local.
- **Dispositivo de hardware:** O Proofpoint Messaging Security Gateway é um dispositivo rígido, seguro, e fácil de implantar, que pode ser instalado em alguns minutos. Há vários modelos de dispositivos disponíveis capazes de oferecer suporte a empresas de qualquer tamanho.
- **Dispositivo virtual:** O Proofpoint Messaging Security Gateway—Edição Virtual fornece a mesma proteção de alto nível oferecida pelos dispositivos de hardware do Proofpoint, além dos inúmeros benefícios de virtualização—including redução de custos, rapidez na implantação e provisionamento, simplificação na gestão de mudanças, facilidade de backup e recuperação de desastres. O Dispositivo virtual pode ser operado em qualquer computador x86 ou servidor por meio da infra-estrutura do VMware Server ou do VMware.
- **Software:** O Proofpoint Protection Server fornece uma plataforma de segurança de mensagens do Proofpoint como um software do sistema operacional Red Hat Enterprise Linux.

Seguro. Eficaz. Fácil de Implantar.

Essas são apenas algumas das maneiras de descrever a plataforma de segurança de e-mails e prevenção de perda de dados do Proofpoint. É a solução mais poderosa do setor—apresentada como um dispositivo enterprise-ready (pronto para empresas), dispositivo ou software virtual que oferece:

- Detecção de spam e gerenciamento de conexões inigualáveis
- Proteção de nível internacional contra vírus e epidemias
- Segurança de conteúdo e prevenção de perda de dados multi-protocolo e abrangente
- Criptografia de e-mails baseada na política
- Análise e elaboração de relatórios avançados
- Gerenciamento unificado de políticas
- Desempenho de nível empresarial
- Rapidez na implantação e provisionamento
- Arquitetura com ótima escalabilidade

“A Pacific Sunwear avaliou vários produtos anti-spam, anti-vírus e de digitalização de conteúdo, e a Proofpoint foi a primeira empresa a fornecer uma plataforma que resolve todos os nossos desafios de e-mail e mensagens em uma implantação única e fácil, além de oferecer soluções simples. O dispositivo Messaging Security Gateway restaurou nosso canal de e-mails, transformando-o novamente em uma fonte estratégica de comunicações empresariais, em vez de uma porta giratória de ameaças propagadas por mensagens.”
Ron Ehlers
VP da Information Systems
Pacific Sunwear

Proofpoint Messaging Security Gateway e Proofpoint Protection Server

proteção completa

Tecnologia MLX Proofpoint

Aprendizagem de máquina avançada

O poder por trás das soluções de segurança de mensagens empresariais—a tecnologia Proofpoint MLX—é um sistema de aprendizagem de máquina com patente pendente desenvolvido por cientistas do Centro de Respostas a Ataques da Proofpoint. Com base em técnicas estatísticas avançadas que incluem regressão logística e análise de ganho de informações, o Proofpoint MLX possibilita a classificação e a identificação precisa de conteúdos não estruturados, como os de mensagens de e-mail e de outros documentos.

Precisão inigualável

O Proofpoint MLX é a base para a precisão anti-spam incomparável fornecida pelo módulo de detecção de spam da Proofpoint. Ao usar a tecnologia MLX, o Proofpoint analisa milhares de atributos estruturais, de imagem, conteúdo e reputação para diferenciar com precisão entre mensagens válidas e mensagens de spam. As soluções anti-spam tradicionais avaliam somente um número limitado de atributos e são incapazes de classificar decisivamente um spam, resultando em pouca eficácia e uma alta taxa de falsos positivos.

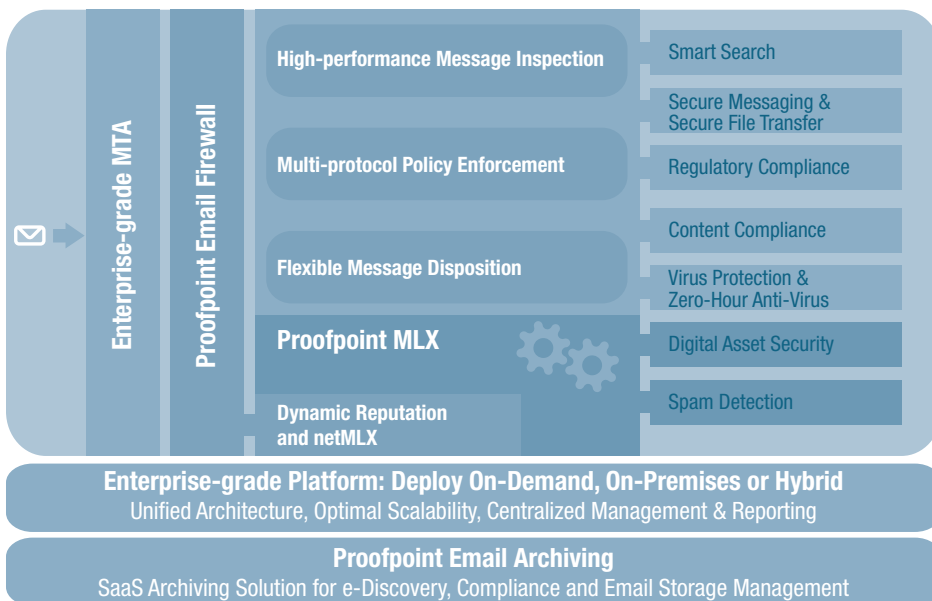
Inteligência à prova de obsolescência

A tecnologia anti-spam da Proofpoint é constantemente atualizada para continuar protegendo contra novas formas de spam. Um treinamento contínuo e novas técnicas desenvolvidas pelos cientistas da Proofpoint permitem que o MLX preveja e se adapte a novas formas de spam à medida que forem criadas. As atualizações do MLX são automaticamente fornecidas para todos os clientes, várias vezes ao dia.

Como resultado, o Proofpoint MLX oferece eficácia 99,8% ou superior, mesmo contra formas difíceis de spam, inclusive spams de imagem, PDF, anexo, “backscatter” (notificações ilegítimas de mensagens rejeitadas) e em idiomas estrangeiros.

Diferentemente de outras soluções anti-spam, a capacidade do Proofpoint de defender contra ataques de spam não diminui com o tempo—e as atualizações do mecanismo MLX anti-spam são fornecidas a sua empresa de modo automático e regular. O Proofpoint MLX está sempre se desenvolvendo para enfrentar novas ameaças, garantindo a proteção de sua infra-estrutura de mensagens contra os spammers no futuro, assim como os spammers de hoje.

Proofpoint MLX também aciona seus recursos avançados de segurança de conteúdo do módulo de Segurança de Ativos Digitais da Proofpoint (Digital Asset Security module) e os recursos inteligentes de segurança do perímetro dos serviços Proofpoint Email Firewall e Dynamic Reputation. A Proofpoint é o único fornecedor que aplica essas técnicas poderosas de aprendizagem de máquina para a prevenção de perda de dados e a segurança dos e-mails.



defenda-se contra ameaças de entrada

Detecção avançada de spams, desenvolvida pela tecnologia Proofpoint MLX™

Desenvolvido pela tecnologia Proofpoint MLX de aprendizagem de máquina de patente pendente, o módulo **Proofpoint Spam Detection™** examina milhares de atributos de cada e-mail—including a estrutura e os cabeçalhos, a imagem, a reputação do remetente da mensagem, assim como o conteúdo não estruturado do corpo da mensagem—para bloquear spams, spams baseados em imagens e ataques phishing, enquanto se adapta automaticamente à medida que surgem novos ataques.

O **Proofpoint Dynamic Update Service™** mantém sua proteção contra spam automaticamente atualizada, garantindo sempre o máximo de eficácia. Os índices de conteúdo adulto e spam individualmente controláveis permitem que você aplique políticas de tolerância zero contra o spam pornográfico.

Os recursos anti-phishing interrompem a disseminação de phishing e impedem o roubo de informações pessoais dos funcionários. Os recursos de gerenciamento de mensagens de retorno, incluindo a especificação Bounce Address Tag Validation (BATV), bloqueiam 100% de spam “backscatter” (mensagens NDR, com notificações falsas de falha de entrega).

O Proofpoint Spam Detection é multilíngüe e oferece precisão inigualável contra spams em qualquer idioma—including aqueles de difícil análise e caracteres multibytes, como os idiomas japonês e chinês. As políticas anti-spam podem ser personalizadas em níveis gerais, ou conforme os grupos e os usuários finais, com integração total aos sistemas LDAP ou Active Directory para agilizar uma administração contínua.

Proteção integrada de firewall de e-mails

Proofpoint Email Firewall™ fornece um sistema de defesa de primeira linha contra spam e conexões maliciosas, testando vários pontos de dados em nível de conexão incluindo DNS, verificação de registro MX, SPF, verificação de destinatário, informações da tecnologia Dynamic Reputation da Proofpoint e dados opcionais netMLX.

Gerenciamento de conexões inovador

Proofpoint Dynamic Reputation™—desenvolvido pela **Proofpoint netMLX™**—adiciona os mais poderosos recursos de gerenciamento de conexões do setor à sua implantação Proofpoint. É o único serviço de reputação de e-mails que usa uma combinação de dados locais de comportamentos previsíveis e reputação globalmente observada—analisada por poderosos algoritmos de aprendizagem de máquina—para bloquear conexões de entrada de endereços de IP maliciosos

Proofpoint Messaging Security Gateway e Proofpoint Protection Server

defenda-se contra ameaças de entrada (continuação)

Todas as implantações de software e dispositivos Proofpoint fornecem análise comportamental previsível integrada de tráfego IP local que responde em tempo real para eliminar picos de tráfego de e-mails causados por ataques direcionados e para bloquear ou reprimir conexões maliciosas de botnets.

Os clientes com altos volumes de e-mail podem adicionar a proteção ampliada do Proofpoint net-MLX em suas implantações para reduzir os volumes de conexão de entrada até 80% ou mais. O Proofpoint netMLX cria o banco de dados de reputação mais preciso e atualizado do setor para endereços de IP enviando e-mails pela Internet. A cada minuto, centenas de pontos de dados de todos os endereços de IP são analisados sintaticamente com avançados algoritmos de aprendizagem de máquina para gerar um índice que representa a reputação do remetente. Em seguida, o Proofpoint Dynamic Reputation usa esses índices, combinados com dados comportamentais locais, para tomar decisões inteligentes que envolvem a aceitação, a repressão ou rejeição de conexões de e-mail de entrada.

Proteção contra vírus e Defesas de Anti-vírus Zero-Hour

Por meio de parcerias estratégicas com os principais fornecedores de anti-vírus, o **Proofpoint Virus Protection™** fornece uma funcionalidade completa de digitalização de vírus. Os mecanismos de anti-vírus são totalmente integrados à plataforma Proofpoint, fornecendo uma administração centralizada e conveniente de políticas de anti-vírus por meio da mesma interface usada para gerenciar políticas de conteúdo e spams. As mensagens são digitalizadas eficientemente em busca de vírus juntamente com o spam e o conteúdo de mensagens para proteger os usuários contra vírus, worms e outras formas de códigos maliciosos. Além disso, o módulo **Proofpoint Zero-Hour Anti-Virus™** protege contra vírus emergentes nos estágios iniciais de sua proliferação —bloqueando-os horas antes de as soluções dos concorrentes começarem a reagir.

evite vazamento de informações através de múltiplos protocolos

Os recursos avançados de prevenção de perda de dados do Proofpoint podem proteger e-mails de entrada, assim como outros fluxos de mensagens, incluindo webmail, postagens para blog e fóruns de discussão e outras atividades baseadas em HTTP ou FTP.

Conformidade de conteúdo: Fácil aplicação de políticas de uso aceitáveis

Proofpoint Content Compliance™ permite definir e reforçar políticas de uso aceitável para conteúdos e anexos de mensagens em toda sua empresa. Uma interface conveniente apontar-e-clique simplifica o processo de definição de regras complexas relacionadas aos tipos de arquivos, e ao tamanho e conteúdo das mensagens. Esses recursos podem ser usados para identificar e prevenir uma ampla variedade de violações de políticas de entrada e saída—incluindo linguagem ofensiva, assédio, compartilhamento de arquivos e violações de normas externas.

Conformidade normativa: Proteja a privacidade e a segurança dos dados

Mais do que nunca, as empresas precisam proteger a privacidade e a segurança dos dados de clientes e funcionários. O módulo **Proofpoint Regulatory Compliance™** aplica as melhores práticas para garantir a privacidade dos dados e protege sua organização das responsabilidades associadas às normas de segurança de dados e de privacidade (como as normas HIPAA, GLBA, PCI, SEC e outras).

Normas personalizáveis, dicionários gerenciados e “identificadores inteligentes” são usados para digitalizar automaticamente informações não-públicas—como informações protegidas sobre saúde e finanças pessoais—e rejeitar ou criptografar mensagens quando apropriado. Os identificadores inteligentes do Proofpoint são mais sofisticados do que simples expressões regulares. Eles procuram pelo número correto de dígitos ou caracteres, mas também realizam um processamento complexo de algoritmos para garantir uma detecção de alta precisão enquanto minimizam os falsos positivos.

Segurança de ativos digitais: Proteger documentos confidenciais

Quando o e-mail, o webmail e outros sistemas de mensagens se tornaram os canais de comunicação mais importantes, também se tornaram uma fonte de exposição de informações privadas ou confidenciais. O módulo **Proofpoint Digital Asset Security™** impede que os ativos valiosos e as informações confidenciais de sua empresa vazem para fora da organização via e-mail e outros protocolos de mensagem. A poderosa tecnologia de aprendizagem de máquina MLX analisa e classifica seus documentos confidenciais e depois monitora essas informações (ou parte delas) no fluxo de mensagens de saída—impedindo falhas na segurança de conteúdo antes de que ocorram.

Gerenciamento centralizado

Gerenciamento e administração de políticas baseadas na web, com controle do usuário final

O Proofpoint Messaging Security Console™ fornece uma interface de administração centralizada, 100% baseada na web para a estrutura de gestão unificada de políticas do Proofpoint, garantindo consistência na aplicação das políticas de mensagens corporativas. O Console facilita o monitoramento e o controle da infra-estrutura de mensagens, além da definição de políticas de mensagens. Você pode até mesmo definir e aplicar políticas distintas para diferentes grupos de usuários finais. Como outros módulos Proofpoint são adicionados à sua implantação, a mesma interface conveniente é usada para o gerenciamento de políticas. A interface baseada em Ajax oferece uma personalização “arrastar e soltar” dos relatórios, informação sobre status, fontes RSS (RSS feeds) e outros componentes exibidos. Até mesmo cria “mashups” de informações de fontes externas. A incrível facilidade de uso do Proofpoint se estende também aos usuários finais. Relatórios e controles de fácil compreensão, como o sumário para usuário final e listas personalizadas de remetentes autorizados e proibidos, permitem que o usuário tenha controle total sobre suas preferências de spam.

Elaboração de relatórios robusta

O Console também fornece acesso a mais de 60 relatórios na forma de gráficos e alertas, que propiciam uma visão clara e em tempo real do estado do sistema de mensagens de sua empresa. Os relatórios podem ser facilmente enviados por e-mail ou exportados como HTML/ XML. Os relatórios “ativos” do Proofpoint fornecem informações estratégicas, mas também permitem que os administradores ajam imediatamente (por exemplo, um simples clique em um link pode bloquear um remetente hostil).

Administração zero

Proteção sempre atualizada, com administração facilitada

A instalação e notificação automática de componentes atualizados facilita a administração contínua. O Proofpoint Dynamic Update Service garante sempre à sua rede o mais alto nível de proteção contra ameaças propagadas por e-mails. Fornece atualizações contínuas a todos os componentes para a implantação de seu software ou dispositivo Proofpoint, incluindo seu robusto sistema operacional e mecanismos MTA, anti-spam e anti-vírus, lexicons (como dicionários usados pelo módulo Proofpoint Regulatory Compliance), componentes de aplicação e hotfixes customizados.

Proofpoint Messaging Security Gateway e Proofpoint Protection Server

criptografe informações confidenciais

Proofpoint Secure Messaging™ adiciona poderosas capacidades de criptografia content-aware (conteúdo consciente) à implantação de seu Proofpoint, criptografando automaticamente as mensagens com base nas políticas da organização. Ele aplica automática e consistentemente suas políticas de criptografia, sem solicitar aos usuários que tomem qualquer tipo de medida especial. A tecnologia Voltage IBE (identidade baseada em criptografia) fornece uma criptografia poderosa e fácil de usar sem as complicações que envolvem o gerenciamento de certificados de outras soluções. O hardware e os dispositivos virtuais da Proofpoint também suportam certificados digitais e permitem a transferência segura entre gateways e o recebimento de e-mails por meio do Transport Layer Security (TLS).

otimize sua infra-estrutura de mensagens

Amplie a implantação de seu Proofpoint com uma variedade de otimizações que melhoram a usabilidade e a eficiência de gerenciamento de sua infra-estrutura de mensagens. O **Proofpoint Smart Search™** otimiza os recursos integrados de elaboração de relatórios e registro de logs com rastreamento avançado de mensagens, capacidades de perícia e análise de logs—oferecendo visibilidade fácil e em tempo real dos fluxos de mensagens em toda sua infra-estrutura de mensagens. Pesquise, analise e exporte logs de mensagens de uma Interface gráfica de usuário conveniente e fácil de usar—até mesmo através de implantações de Proofpoint globalmente distribuídas. O **Proofpoint Secure File Transfer™** adiciona capacidades seguras de transferência de arquivos grandes para sua implantação de Proofpoint. Ele permite que os usuários enviem arquivos grandes (ou arquivos que necessitam de maior segurança) de forma mais rápida e fácil, ao mesmo tempo que reduz o impacto de anexos pesados sobre sua infra-estrutura de e-mails. A solução on-demand **Proofpoint Email Archiving™** trata do gerenciamento de armazenamento de e-mails, descobertas jurídicas e conformidade normativa sem precisar se preocupar em gerenciar um arquivo de e-mails internamente.

alto desempenho, fácil implantação, ótima escalabilidade

Proofpoint foi criado para atender às necessidades exclusivas de grandes empresas, ISPs (Provedores de acesso à internet), universidades e organizações governamentais. Oferece todos os recursos de desempenho, eficiência, personalização e controle de usuário final necessários em implantações de larga escala.

Todos os componentes do sistema Proofpoint foram elaborados para atender aos rigorosos requisitos de desempenho das empresas. Desde um sistema operacional rígido e otimizado para mensagens usado nos dispositivos Proofpoint até a exclusiva arquitetura queue-less (menos enfileiramento) que permite que todas as funções de digitalização de mensagens sejam executadas na memória, o Proofpoint fornece o alto desempenho exigido até mesmo nas implantações mais sofisticadas. Os dispositivos do Proofpoint ajustam-se indefinidamente para suportar milhões de mensagens por dia. Eles podem ser facilmente implantados em configurações mestre/escravo para suportar centros de dados complexos ou distribuídos geograficamente—oferecendo a segurança de redundância 100% combinada com a conveniência de uma única interface administrativa. O Proofpoint suporta inclusive implantações híbridas com hardware e dispositivos virtuais trabalhando juntos.

A perfeita escalabilidade de sua arquitetura permite que todos os servidores escravos sejam gerenciados por meio de um único console mestre. A propagação automática de configurações, a quarentena de mensagens e relatórios centralizados simplificam a manutenção e reduzem o custo total de propriedade.

O Proofpoint também reduz o custo total de propriedade integrando-se facilmente com qualquer infra-estrutura de TI, independentemente da forma como é distribuída. O console de comando LDAP baseado na GUI e o suporte Microsoft Active Directory® facilitam a integração dos servidores de diretórios. O Proofpoint também é compatível com —e minimiza a carga de—soluções de servidores de e-mail sobrecarregados como o Microsoft Exchange® e o Lotus Notes.

versão de teste gratuita — experimente hoje!

Teste a potência do Proofpoint. Visite o site www.proofpoint.com/trial e cadastre-se para fazer o download de uma versão de teste de 45 dias totalmente operacional do Proofpoint Messaging Security Gateway—Edição Virtual que pode ser implantada em minutos. Ou cadastre-se no site www.proofpoint.com/trypod e faça um teste gratuito da solução de segurança de e-mails Proofpoint on Demand SaaS.

Proofpoint fala o seu idioma

Além de oferecer um excelente desempenho anti-spam em qualquer idioma, os mecanismos de digitalização de conteúdo e política do Proofpoint detectam e “compreendem” textos em qualquer idioma, inclusive idiomas com caracteres multibytes. As políticas de prevenção de perda de dados reconhecem palavras-chave e termos de dicionários escritos em conjuntos de caracteres internacionais em outros idiomas diferentes do inglês, incluindo o japonês, o chinês e o cirílico. Os administradores podem criar políticas acionadas com base no idioma detectado no conteúdo de um e-mail. Por exemplo, anexar termos de isenção de responsabilidade em um idioma específico a uma mensagem de saída dependendo do idioma em que a mensagem foi escrita. Há interfaces de usuário final para sumário de mensagens e quarentena baseadas na web disponíveis em chinês, holandês, inglês, alemão, finlandês, francês, italiano, japonês, português, russo, espanhol e sueco.

A Interface Gráfica de Usuário administrativa, a documentação do produto e a ajuda on-line do Proofpoint estão disponíveis atualmente tanto nas versões em inglês quanto japonês.

Assim como é feito com as interfaces de usuário final do Proofpoint, os administradores podem definir suas preferências de idioma conforme sua necessidade individual.

Versões de dispositivos

O dispositivo Proofpoint Messaging Security Gateway dispõe de várias configurações de hardware para suportar implantações de qualquer tamanho. Para obter informações atualizadas sobre os modelos de dispositivos Proofpoint, visite: www.proofpoint.com/products/msg.php.

Navegadores compatíveis

Todas as tarefas de configuração e administração—das versões do dispositivo de hardware, dispositivo virtual ou software—são realizadas pela interface 100% baseada em navegadores da Proofpoint. Navegadores compatíveis:

Microsoft® Internet Explorer 6.0 ou superior

Mozilla Firefox 2.0 ou superior

©2008 Proofpoint, Inc. Proofpoint Protection Server é uma marca comercial registrada da Proofpoint, Inc. nos Estados Unidos e em outros países. 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 e Proofpoint on Demand são marcas comerciais da Proofpoint, Inc. nos Estados Unidos e em outros países. Todas as outras marcas comerciais contidas neste documento pertencem a seus respectivos proprietários. 09/08