Segurança do e-mail:

Guia para compradores

Segurança do e-mail: Guia para compradores

Introdução

Com a quantidade crescente de dados comerciais confidenciais e informações de identificação pessoal enviadas por e-mail, o potencial de vazamento e comprometimento de dados nunca foi tão grande. O cenário de ameaças de e-mail contém cada vez mais ameaças combinadas sofisticadas e ataques direcionados. Esses ataques têm o objetivo de distribuir malware que se infiltra nos data centers onde dados comerciais confidenciais de alto valor são armazenados. As defesas tradicionais, incluindo firewalls e soluções de antivírus de endpoint, não conseguem bloquear esses tipos de ataques.

Para enfrentar esses desafios, as organizações de hoje precisam de uma solução que forneça segurança em camadas para o e-mail. Este documento examina os requisitos que as empresas devem considerar ao comprar uma solução de segurança do e-mail para se defender contra spam e vírus, ameaças combinadas e perda de dados. Além disso, mostra como as soluções de segurança de e-mail da Cisco® podem ajudar.

Critérios do comprador para a segurança do e-mail

Ao considerar soluções de segurança do e-mail, as empresas precisam avaliar os critérios a seguir para ajudar a garantir que receberão a proteção em camadas profundas necessária para proteger seus negócios contra as ameaças de e-mail de entrada e de saída de hoje. Uma solução de segurança do e-mail deve oferecer:

- Análise de big data e inteligência de segurança global coletiva
- Proteção contra spam e vírus
- Proteção contra ameaças e correção de problemas de segurança
- Prevenção contra perda de dados e criptografia
- Opções de implantação flexíveis

*O e-mail é o principal vetor de ameaças para ataques cibernéticos, de acordo com o Relatório de Segurança Anual da Cisco de 2015.**

Requisito 1: análise de big data e inteligência de segurança global coletiva

O aumento no big data que atravessa os gateways de e-mail e da Web ganhou a atenção dos hackers. Para proteger os clientes do volume crescente de malwares conhecidos, os provedores de segurança de endpoint tradicionais introduziram o antivírus assistido pela nuvem, essencialmente movendo as assinaturas para a nuvem no intuito de proteger sua base de clientes inteira usando a imunidade coletiva. No entanto, essa solução sozinha não protege contra o malware avançado projetado para driblar a detecção tradicional baseada em assinatura.

A proteção holística só pode ser alcançada pela análise contínua e pelo monitoramento do comportamento de um arquivo, mesmo depois que ele foi admitido no seu ambiente. Se a disposição de um arquivo for alterada, o monitoramento constante permite detectar, conter e corrigir a ameaça enquanto rastreia a infecção em sua origem.

A abordagem da Cisco

- Suporte de milhões de amostras de malware conhecido e a imunidade coletiva da comunidade de clientes da Cisco
- Análise do Cisco Talos Security Intelligence and Research Group (Talos)
- Identificação de malware com base no que ele faz, e não em como ele se parece, permitindo a detecção até mesmo dos ataques de dia zero mais recentes
- Cisco Advanced Malware Protection (AMP) para proporcionar mais visibilidade, controle e retrospecção

**Relatório Anual de Segurança da Cisco de 2015*, Cisco, janeiro de 2015.

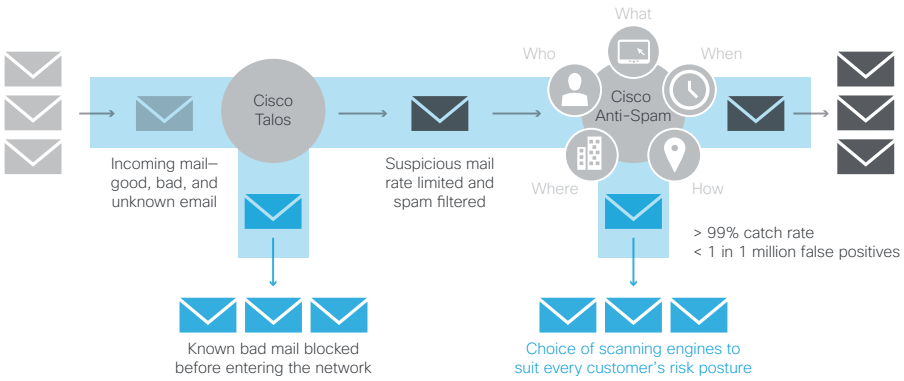
Requisito 2: proteção contra spam e vírus

O spam é um problema complexo que exige uma solução sofisticada, em várias camadas. De acordo com o *Relatório Anual de Segurança da Cisco de 2015*, os mais recentes métodos de ataque em uso são desenvolvidos para driblar os filtros de spam de e-mail tradicionais, por meio do envio de spam *"snowshoe"*. Esse método de ataque consiste no envio de pequenos volumes de spam de muitos servidores, bem como na rápida mudança do conteúdo da mensagem, a fim de fugir da detecção. Essa tática é um excelente exemplo da necessidade de uma segurança em várias camadas para o e-mail, fornecendo vários mecanismos que trabalhem em conjunto não apenas para aumentar os índices de proteção, mas para reduzir os falsos positivos, servindo como um sistema de freios e contrapesos entre si.

A abordagem da Cisco

- Mecanismo antispam em várias camadas
- Combinação de filtragem de camada exterior e interior que considera a reputação do remetente para impedir que o spam chegue às caixas de entrada (ver Figura 1)
- Cisco Context Adaptive Scanning Engine (CASE), que fornece taxas de captura de spam superiores a 99% e uma baixa taxa de falsos positivos para o setor: menos de um em um milhão
- Verificação do contexto e do conteúdo da mensagem para fornecer uma filtragem mais precisa
- Defesa antivírus abrangente em camadas com mecanismos antivírus Sophos ou McAfee (ver Figura 2)

Figura 1. Defesa antispam aprofundada da Cisco



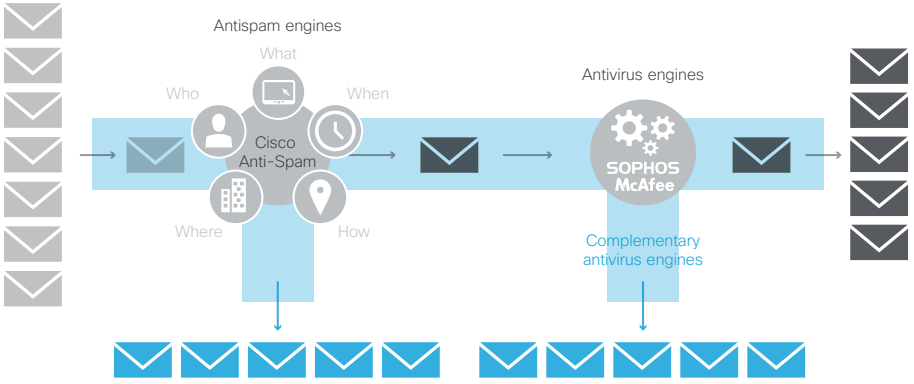
Requisito 3: proteção contra ameaças e correção

Mesmo com uma abordagem em camadas para a segurança do e-mail, alguns ataques sofisticados conseguirão passar pelas primeiras camadas. A análise contínua e a segurança retrospectiva são necessárias para identificar arquivos mal-intencionados que driblam a detecção inicial e ajudar os defensores a determinar o escopo do ataque, a fim de que possam rapidamente conter e corrigir a ameaça.

A abordagem da Cisco

- Camada adicional de segurança com o Cisco AMP
- Usa uma combinação de reputação do arquivo, inclusão no sandbox e análise retrospectiva do arquivo; identifica e bloqueia ameaças durante todo o ciclo do ataque (ver Figura 3)
- Filtros de detecção avançados que utilizam o Cisco Threat Operations Center (TOC) e a inteligência de ameaças do Cisco Talos para identificar, colocar em quarentena e modificar regras, conforme vão aprendendo mais sobre um ataque
- Reescrita de URL automática ou manual para redirecionar os destinatários por meio de proxy de segurança, "neutralização" de URLs ou substituição de URLs com uma notificação ao usuário de que parte do conteúdo do e-mail foi bloqueada

Figura 2. Defesa antivírus aprofundada da Cisco



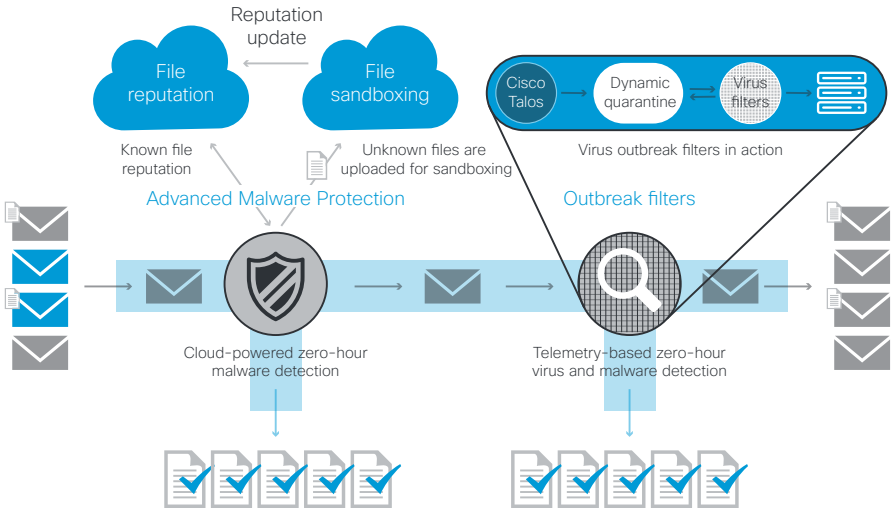
Requisito 4: prevenção contra perda de dados e criptografia

As soluções modernas de segurança do e-mail com capacidade de detectar, bloquear e gerenciar riscos em e-mails de saída podem ajudar a reduzir as chances de dados importantes saírem da rede acidental ou propositalmente. As soluções de DLP (data loss prevention, prevenção contra perda de dados) com reconhecimento de conteúdo e baseadas em políticas, além dos recursos de criptografia, podem oferecer essa proteção. A verificação antispam e antivírus de saída, juntamente com a limitação na taxa de saída, ajuda as empresas a evitar o vazamento de dados, a permanecer em conformidade e a impedir que máquinas ou contas comprometidas acabem sendo incluídas em soluções de listas negras de e-mails.

A abordagem da Cisco

- Parceria com a líder em DLP RSA Security para fornecer mais de 100 políticas predefinidas
- Revogação de chave de criptografia por mensagem e por destinatário pelo remetente ou administrador
- Serviço de envelope registrado da Cisco (CRES) – oferece autenticação de registro do usuário como um serviço gerenciado altamente disponível

Figura 3. Proteção da Cisco contra vírus e malware desde a primeira hora



Requisito 5: opções de implantação flexíveis

Não existem duas empresas com redes e infraestruturas concebidas da mesma forma. Para atender às suas necessidades operacionais e de segurança, seu provedor de segurança do e-mail deve ter opções de implantação flexíveis que lhe permitam gerenciar a solução de uma forma que seja mais adequada para sua empresa – seja um modelo local, baseado em nuvem ou híbrido.

Solução Cisco Email Security

A Cisco oferece um conjunto flexível de opções de implantação para o Cisco Email Security Appliance (ESA) (ver Figura 4). Ela oferece essas opções com suporte em vários dispositivos – incluindo desktops, telefones celulares, notebooks e tablets – e para Android, iOS, Mac, PC e Linux.

No local – O Cisco ESA pode ser implantado no local com um dispositivo ou um grupo de dispositivos em cluster, físicos ou virtuais. Vários clusters podem ser usados, se necessário.

Nuvem ou híbrida – Por meio dessas abordagens de implantação, as empresas podem lidar com toda a segurança de entrada e saída na nuvem, se não desejarem manter o dispositivo no local ou se preferirem que terceiros a administrem.

Figura 4. Opções de implantação do Cisco Email Security

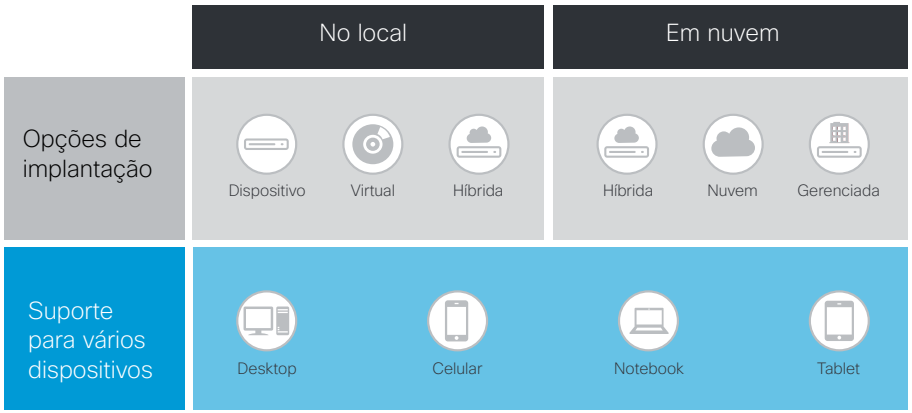


Tabela 1. Produtos Cisco Email Security

Cisco ESA	Mantém os dados confidenciais no local, com um sólido desempenho e fácil gerenciamento
Cisco Email Security Virtual Appliance (ESAv)	Fornece implantação mais rápida, escalabilidade sob demanda e a eficiência operacional obtida com os investimentos existentes
Cisco Cloud Email Security	Fornece um modelo de implantação flexível para segurança do e-mail a qualquer hora e em qualquer lugar
Cisco Hybrid Email Security	Fornece controle avançado de mensagens no local, aproveitando, ao mesmo tempo, a conveniência econômica da segurança na nuvem
Cisco Managed Email Security	Oferece o desempenho e a segurança de um ESA no local com a confiança do gerenciamento Cisco TOC

Conclusão

Para proteger dados, redes e usuários, as empresas de hoje precisam de um modelo de segurança do e-mail com foco nas ameaças. Elas devem ser capazes de enfrentar todos os vetores de ataques e responder a ameaças de forma contínua a qualquer momento – antes, durante ou após um ataque. Soluções de segurança do e-mail eficientes como as da Cisco são um componente essencial de uma estratégia moderna de segurança, pois contam com inteligência em tempo real, oferecem controle de acesso preciso e apresentam reconhecimento de conteúdo, contexto e ameaças.

Com a segurança do e-mail da Cisco, é possível monitorar e controlar o fluxo de dados que entra e sai da empresa. A defesa avançada contra ameaças da Cisco começa com o trabalho do Talos. Composto pelos principais pesquisadores de ameaças, o Talos é a equipe principal que fornece informações de ameaças para o ecossistema Cisco Collective Security Intelligence (CSI), que inclui Threat Response, Intelligence, and Development (TRIAD); Cisco Managed Threat Defense e Cisco Security Intelligence Operations (SIO). O Cisco CSI é compartilhado entre várias soluções de segurança e fornece eficácia e proteção líderes do setor.

A segurança do e-mail da Cisco fornece:

- **Foco na ameaça** – A solução oferece proteção de e-mail de alta disponibilidade contra o bombardeio constante de ameaças cada vez mais sofisticadas e dinâmicas, enfrentado por todas as empresas modernas.
- **Alto desempenho** – O Cisco ESA apresenta uma defesa em camadas, em um único dispositivo. Ele rapidamente bloqueia novas ameaças enviadas por e-mail e spam, e barra ou criptografa e-mails de saída confidenciais.
- **Inovação contínua** – A segurança do e-mail da Cisco oferece as opções de implantação mais amplas do setor. A solução reduz os custos com menos dispositivos, integração mais rápida e treinamento simplificado.

Para obter mais informações sobre o portfólio de segurança do e-mail da Cisco, acesse www.cisco.com/go/emailsecurity. Um representante de vendas, parceiro ou engenheiro de sistemas da Cisco pode ajudá-lo a avaliar como as soluções de segurança do e-mail da Cisco atenderão às necessidades exclusivas da sua empresa.