McAfee Email Protection

Proteção avançada para caixas de correio, em qualquer lugar e a qualquer hora

As empresas precisam de proteção avançada de e-mail, agora, mais do que nunca. Segundo o SANS Institute, 95% dos ataques de rede são resultado direto de spear phishing bem-sucedido.[1] Os usuários continuam sendo vítimas de técnicas de engenharia social e os cibercriminosos expandiram seu repertório, incluindo outras táticas inteligentes que pegam desprevenidas até as organizações mais ciosas em relação à segurança. Malware avançado e perda de propriedade intelectual corporativa são problemas crescentes que podem ter um impacto negativo considerável sobre qualquer organização. As empresas estão começando a migrar seu e-mail para caixas de correio hospedadas, o que pode aumentar o nível de risco. Enfim, a falta de flexibilidade nas soluções de proteção de e-mail tradicionais pode obrigar as empresas a buscar uma alternativa melhor. O McAfee® Email Protection é a resposta. Essa solução poderosa oferece uma proteção de nível corporativo completa contra ameaças de phishing direcionado, com tecnologia de prevenção de perda de dados (DLP) e continuidade de e-mail. Com opções de distribuição flexíveis — como uma solução com base na nuvem, no local ou híbrida integrada — você pode implementar a segurança de e-mail da maneira que quiser e quando quiser.

Principais vantagens

Proteção contra ataques direcionados de phishing

- Detecte ameaças de URLs maliciosos em tempo real com o ClickProtect
- Integração com o McAfee Advanced Threat Defense para defesa contra malware furtivo
- Tecnologia de prevenção de perda de dados incorporada

Segurança para caixas de correio hospedadas

- Proteção contra ataques direcionados, não importando para onde o e-mail vá
- Controles de usuário final de graymail
- Continuidade de e-mail
- Capacidades granulares de criptografia e proteção contra perda de dados

Opções de distribuição flexíveis

- Distribuição da forma que você quiser, quando quiser
- Opção de distribuição híbrida com um console único para gerenciamento e geração de relatórios

Além da engenharia social: novas táticas de spear phishing

No que se refere a ataques de phishing, o usuário é o elo mais fraco. *The Verizon Data Breach Investigation Report, 2014*[2] (Relatório de investigações de violações de dados de 2014 da Verizon) revela que quase um em cada cinco usuários clica em links dentro de e-mails de phishing. Os cibercriminosos continuam a se aproveitar da vulnerabilidade dos usuários utilizando técnicas de engenharia social, mas foram além disso ao empregar outras táticas sofisticadas que tornam as ameaças de e-mail difíceis de rastrear. Veja a seguir alguns exemplos:

- **URLs não reutilizáveis:** os cibercriminosos estão cancelando URLs maliciosos após os usuários serem vitimados por fraudes de phishing e infectados. Isso torna as detecções e perícias difíceis ou mesmo impossíveis.
- **Infecção retardada:** em alguns casos, os atacantes *aguardam* até que um e-mail seja examinado, aprovado e entregue em caixas de entrada corporativas, para somente então inserir a carga viral no site de destino. Os funcionários tendem a confiar nos e-mails que recebem no trabalho e acabam clicando em um link nocivo.

intel Security

- **Malware com detecção de sandbox:** esse tipo de código malicioso evita detecções ao permanecer latente, deixando para causar problemas futuramente.

Defesas avançadas em camadas

Proteção no momento do clique

O McAfee Email Protection oferece múltiplas camadas de proteção para ajudar você a debelar ataques sofisticados de spear phishing e o malware furtivo a eles associado. Aproveitando o McAfee Gateway Anti-Malware Engine do McAfee Web Gateway, solução número um em antimalware[3], o McAfee Email Protection inclui uma proteção de URL no momento da varredura e no momento do clique conhecida como ClickProtect, que funciona a partir de qualquer dispositivo e em qualquer lugar, frustrando tentativas de spear phishing. O ClickProtect detecta e elimina ameaças em URLs incorporados em mensagens de e-mail. Ele verifica se há mudanças nas intenções do URL ocorridas entre o momento em que a mensagem é examinada — independentemente do quão inócua ela tenha parecido — e o momento em que o usuário clica nela.

Examinemos um cenário de malware retardado no qual um atacante cria um e-mail com um URL aparentemente não malicioso que visa o controlador financeiro dentro da sua organização. A sua solução de segurança de e-mail recebe o e-mail, interroga-o, descobre que ele é seguro e o entrega na caixa de entrada de destino. Porém, agora que o e-mail se encontra na caixa de entrada do controlador financeiro, o atacante insere malware na página Web de destino. Se o controlador clicar no link, a sua rede será infectada.

Com o ClickProtect, no momento em que um URL de um e-mail é clicado, ele faz a seguinte pergunta: "O URL ainda é seguro?" Todos os URLs entregues são reescritos e inspecionados pelo McAfee Gateway Anti-Malware Engine utilizando emulação comportamental para detectar conteúdo malicioso da Web sem depender de assinaturas.

Uma visualização segura permite que os usuários vejam os sites maliciosos com segurança e aprendam as melhores práticas, acrescentando mais uma camada de segurança e reduzindo o risco total. As mensagens podem ser encaminhadas com segurança e, mesmo que os destinatários não tenham o ClickProtect, a proteção acompanha o e-mail onde quer que este vá.

Detecção e bloqueio de malware furtivo

Graças à integração com o McAfee Advanced Threat Defense, o McAfee Email Protection pode detectar e bloquear malware furtivo de dia zero em arquivos anexados suspeitos antes que estes cheguem à sua caixa de entrada. Essa abordagem inovadora e em camadas combina análise detalhada de código estático e análise dinâmica (em área restrita ou sandbox) para analisar o real comportamento do malware. A análise completa de código estático proporciona informações detalhadas de classificação de malware, amplia a proteção contra ameaças evasivas e altamente camufladas e permite identificar a reutilização de código por malware associado. Caminhos de execução atrasada ou contingente, que geralmente não são executados em um ambiente dinâmico de área restrita (sandbox), podem ser detectados com a descompactação e análise completa do código estático.

Prevenção de perda de dados incorporada

Os ataques direcionados de spear phishing têm um único objetivo: a apropriação de dados confidenciais e valiosos. O McAfee Email Protection incorpora uma tecnologia líder do setor, oriunda de nossas soluções DLP. Estão incluídos dicionários de conteúdo para PCI DSS, assistência médica, informações financeiras, regulamentos regionais de privacidade e muito mais, para ajudá-lo a desenvolver políticas de conformidade para identificação, armazenamento e transmissão de dados confidenciais.

Ao criar e armazenar impressões digitais de documentos selecionados, o McAfee Email Protection aprende qual tipo de conteúdo precisa ser controlado e protegido por políticas. A ferramenta de expressões regulares, os dicionários personalizáveis, os contadores de limites, a varredura profunda de conteúdo em mais de trezentos tipos de documentos e as listas brancas permitem criar e cumprir políticas de anexos e de conteúdo para diferentes grupos de usuários dentro da sua organização.

McAfee Email Gateway

Requisitos de sistema e ambientes de applicance virtual

- VMware vSphere 4.x ou superior
- VMware vSphere Hypervisor (ESXi) 4.x ou superior
- Processador: dois processadores virtuais
- Memória virtual disponível: 2 GB
- Espaço livre em disco: 80 GB

Appliance de hardware

- Disponível em dois modelos e vendido separadamente
- Também disponível no formato de servidor blade

Pelo terceiro ano consecutivo, o McAfee Email Protection obteve uma **classificação de cinco estrelas pela SC Magazine.**

O McAfee Email Protection inclui criptografia de e-mail própria via push, pull, TLS, S/MIME ou PGP para distribuição como servidor blade, appliance de hardware ou appliance virtual, sem custo adicional.

Continuidade de e-mail para continuidade dos negócios

Os negócios não param quando sua rede de e-mails sofre uma interrupção. Caso a rede esteja inacessível devido a desastres naturais, cortes de energia ou mesmo manutenção rotineira, o McAfee Email Protection oferece opções para manter funcionários, clientes, parceiros e fornecedores conectados 24 horas por dia, sete dias por semana. O recurso de continuidade de e-mail retém todas as mensagens enviadas ou recebidas durante interrupções, sincronizando com inteligência um registro preciso de toda a atividade de mensagens no período da interrupção quando seus servidores de e-mail voltarem a operar on-line.

Inteligência e reputação de ameaças

O McAfee Email Protection tem mais uma ferramenta poderosa em seu arsenal — o McAfee Global Threat Intelligence (McAfee GTI), serviço de inteligência sobre ameaças mais abrangente do setor, que coleta e redistribui dados em tempo real de mais de 100 milhões de sensores nos vetores de aquivo, Web, e-mail e rede. A análise de reputação do McAfee GTI minimiza o risco ao bloquear e-mails oriundos de fontes suspeitas, com links para sites suspeitos ou que contêm arquivos maliciosos anexados.

Ao reduzir significativamente a probabilidade de infiltração por malware, ataques de phishing e ataques de ameaças persistentes avançadas na sua rede, a sua organização permanece mais segura e a necessidade de correções onerosas é reduzida.

Desafios de segurança do e-mail hospedado

Um número cada vez maior de endereços de e-mail corporativo está sendo provisionado por serviços de e-mail hospedado, como Microsoft Office 365, Google Apps for Work e outros. Muitas soluções de e-mail hospedado podem oferecer segurança como parte de seus serviços. Mas ela é suficiente? Provavelmente não, pois as tentativas de phishing, spam e graymail continuam a surgir e os recursos de segurança existentes não estão preparados para evitar o vazamento de dados. Além disso, interrupções de e-mail associadas ao Office 365, por exemplo, podem afetar a produtividade. O McAfee Email Protection oferece uma proteção de nível corporativo para defesa contra ataques direcionados de phishing e malware avançado durante as fases de teste, migração e pós-migração. Não importa quando ou onde suas caixas de correio sejam distribuídas, o McAfee Email Protection oferece total cobertura e continuidade de e-mail.

Opções de distribuição flexíveis para agora e para o futuro

O McAfee Email Protection oferece flexibilidade para distribuir segurança de e-mail da sua maneira preferida. Escolha uma solução Software-as-a-Service (SaaS) com base na nuvem, uma solução no local (appliance virtual, appliance de hardware ou servidor blade) ou uma combinação híbrida de ambas. Com o McAfee Email Protection, você pode distribuir a sua segurança de e-mail da maneira mais adequada às suas necessidades atuais, podendo redimensioná-la e mudar seu direcionamento no futuro.

Seja qual for sua opção de distribuição, o McAfee Email Protection oferece um console único de gerenciamento centralizado para relatórios consolidados que permitem avaliar facilmente a eficácia de seus programas de segurança de e-mail. As políticas são aplicadas aos componentes da solução, sejam estes com base na nuvem ou no local.

Para obter informações ou começar uma avaliação do McAfee Email Protection, entre em contato com um representante da McAfee ou visite **www.mcafee.com/br/products/email-and-web-security/email-security.aspx**.

1. **http://blogs.mcafee.com/business/security-connected/is-there-something-phishy-in-your-inbox**
2. **https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf**
3. AV-TEST: *McAfee Web Gateway Security Appliance Test* (Teste do appliance do McAfee Web Gateway Security)

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com

61523ds_email-protection-o365_0115