



McAfee Web Gateway Cloud Service

Segurança na Web fornecida pela nuvem, proporcionando proteção abrangente

Principais benefícios

- A maneira mais econômica de distribuir segurança na Web — sem a necessidade de hardware ou software no local
- Vá além da proteção básica — a emulação de comportamento evita o malware de dia zero em questão de milissegundos, conforme o tráfego é processado
- Estenda a proteção aos usuários fora da rede — a entrega via nuvem dilui o tradicional perímetro de rede
- Eficiência de gerenciamento incomparável com a plataforma McAfee® ePolicy Orchestrator® (McAfee ePO™) Cloud como console de gerenciamento unificado para todos os serviços da Intel Security na nuvem
- Arquitetura comprovada: O McAfee® Web Gateway Cloud Service foi concebido como uma versão multilocalização do McAfee Web Gateway, o confiável appliance local utilizado por empresas do mundo todo

A defesa contra ameaças sofisticadas da Web exige tecnologia avançada, mas não precisa aumentar o custo e a complexidade. O fornecimento de segurança na Web a partir da nuvem permite que as equipes de segurança obtenham as mesmas vantagens da proteção contra ameaças avançadas com appliances no local, mas sem o custo do hardware e dos recursos utilizados para sua manutenção. Conforme mais acessos à Web ocorrem fora do perímetro da rede, a nuvem torna-se o ponto de contato consistente para dispositivos e usuários em trânsito. Em vez de construir uma segurança para o tráfego que flui para um único local, é mais eficaz construir a segurança do endpoint para fora. Conectar endpoints (e até mesmo localidades inteiras) à nuvem proporciona uma proteção abrangente, sem sair do novo perímetro que transcende os limites da rede.

Proteção abrangente e econômica

O gerenciamento de appliances locais de segurança na Web é caro e consome ciclos das equipes de segurança, já tão sobrecarregadas. A distribuição de segurança na Web como um serviço na nuvem pode reduzir o custo total de propriedade. Não há mais appliances de hardware para comprar, ter e manter. Todos os recursos antes utilizados para manter appliances, realizando tarefas como atualizações e correções de software, podem ser realocados para iniciativas mais estratégicas dentro da organização de TI ou de segurança de TI.

Appliances e o serviço na nuvem podem ser utilizados juntos em uma distribuição híbrida. A maioria das organizações escolhe esse modelo para preservar a posse e o controle de appliances na rede e estender a proteção proporcionada via nuvem a pequenos escritórios remotos e usuários em roaming.

As equipes de TI que desviam o tráfego de Web de escritórios remotos para circuitos de comutação de rótulos multiprotocolo MPLS (Multiprotocol Label Switching) para filtragem por um appliance gateway de Web na rede são imediatamente beneficiadas pela segurança na Web oferecida via nuvem. O desvio de tráfego é caro e agrega complexidade à rede. Em vez disso, escritórios remotos podem ser diretamente roteados para a nuvem para proteção, eliminando circuitos MPLS e simplificando a arquitetura de rede.

Finalmente, o acesso à Web pelos funcionários não fica mais limitado ao perímetro da rede, o que deixaria desprotegidos e invisíveis para a TI os usuários e dispositivos fora da rede. Deslocar a segurança na Web para a nuvem inverte esse perímetro. O tráfego de Web dos usuários e dispositivos fora da rede pode ser automaticamente roteado do endpoint para a nuvem, mantendo uma conexão segura para

quem trabalha em casa, em aeroportos, em cafeterias ou em qualquer lugar fora da rede. O foco da rede não se restringe mais ao tráfego dentro de paredes físicas. Em vez disso, ele se estende até onde um endpoint esteja.

Arquitetura global e de alto desempenho

O McAfee Web Gateway Cloud Service foi desenvolvido para corporações e muitas organizações terão um nível mais alto de desempenho do que o atualmente conseguido no local. Por exemplo, no local, quando há necessidade de aumentar a capacidade, o departamento de TI precisa adquirir e distribuir um novo appliance, o que pode levar dias ou semanas. Em nossa nuvem, aumentos de capacidade levam aproximadamente 15 minutos devido ao conceito elástico de nuvem incorporado no serviço.

Quando um appliance no local falha e precisa de reparo, ele pode cortar o acesso à Internet ou prejudicar a postura de segurança se permitir o trânsito direto de dados com a Web. Em caso de falha em um de nossos centros de dados, nosso serviço na nuvem redireciona automaticamente todo o tráfego da Web para o centro de dados mais próximo e mais rápido, assegurando continuidade imediata.

Nossa arquitetura de serviços na nuvem também foi projetada para operar conjuntamente com o backbone da Internet nos maiores pontos de intercâmbio de Internet (IXPs) do mundo. Isso elimina saltos de roteamento de provedores de serviços de Internet intermediários que simplesmente tornam a conexão mais lenta. Com menos saltos para provedores de conteúdo populares, como Microsoft Office 365 e Google, os usuários frequentemente obtêm uma conexão mais rápida através de nosso serviço na nuvem do que quando se conectam diretamente à Internet aberta.

O McAfee Web Gateway Cloud Service é global. Para conhecer as localizações atuais e o status dos centros de dados nos quais o tráfego da Web é processado, visite <https://trust.mcafee.com>. O conteúdo da Web pode ser entregue no idioma local da região para que, independentemente de onde o usuário se conecte, ele veja, por exemplo, resultados locais de pesquisas no Google.



Figura 1. Distribuição do McAfee Web Gateway Cloud Service.

Defenda-se contra ameaças sofisticadas

As equipes de segurança frequentemente não estão à altura do malware sofisticado e dos ataques direcionados que burlam defesas tradicionais, e isso consome muitos recursos e torna o trabalho de correção dos endpoints um constante “apagar de incêndios”. Diferentemente das abordagens tradicionais para prevenção de ameaças da Web com base em assinaturas e filtragem de URLs, o McAfee Web Gateway Cloud Service protege os endpoints contra malware sem arquivo e de dia zero através da emulação em linha de arquivos JavaScript e HTML. Isso viabiliza a prevenção de malware de dia zero antes que este atinja o usuário, além de melhorar as taxas de bloqueio em aproximadamente 20% em relação às soluções com base em assinaturas e filtragem de URLs. As operações de segurança beneficiam-se dos custos mais baixos e da maior flexibilidade de recursos ao reduzir o número total de incidentes de malware.

As ameaças da Web são frequentemente entregues por meio de tráfego criptografado para se ocultarem das defesas de segurança na Web. Praticamente todos os aplicativos na nuvem ou mídias sociais, utilizam tráfego criptografado por padrão. O McAfee Web Gateway Cloud Service pode descriptografar e inspecionar completamente o tráfego criptografado com HTTPS, possibilitando a prevenção de malware e a visibilidade de aplicativos na nuvem dentro de canais criptografados.

Em que lugares do mundo se encontra o McAfee Web Gateway Cloud Service?

Visite <https://trust.mcafee.com> para ter

visibilidade e atualizações ao vivo das localizações de nossos centros de dados, status de disponibilidade e mais.

Para a maioria das equipes de TI, é um desafio controlar a proliferação de aplicativos na nuvem, particularmente os de "TI invisível", e o risco associado a serviços escolhidos pelos usuários. Com total visibilidade sobre todo o tráfego na Web, incluindo HTTPS, relatório predefinidos podem mostrar os sites acessados, os aplicativos na nuvem utilizados e os pontos de dados correspondentes para se determinar o risco. A TI invisível é facilmente revelada comparando-se o que está realmente em uso com o que a TI aprovou. Aplicativos na nuvem, especialmente os de armazenamento na nuvem, são cada vez mais utilizados como mecanismo de entrega de malware. A identificação de quais aplicativos entregaram malware pode ajudar na tomada de decisões quanto a políticas. Com todo o escopo de quais serviços na nuvem estão sendo acessados, mais de 1.600 controles de aplicativos na nuvem podem ser implementados para minimizar o risco, como prevenção de uploads e mensagens instantâneas ou o bloqueio imediato de aplicativos.

Gerenciamento eficiente da segurança

O gerenciamento da segurança em vários consoles e políticas é trabalhoso, especialmente quando a segurança de Web com base na nuvem e no local é gerenciada separadamente. Em um ambiente híbrido, há um único console de gerenciamento para ambas as distribuições no local e na nuvem, um único conjunto de políticas e uma única interface de relatórios.

Quando distribuído isoladamente sem hardware ou software no local, o McAfee Web Gateway Cloud Service é gerenciado pelo McAfee ePO Cloud, o console de gerenciamento unificado para todos os serviços de segurança com base na nuvem da Intel Security, juntamente com segurança de endpoint, proporcionando uma eficiência incomparável no gerenciamento da segurança.

A distribuição de segurança na Web para dispositivos endpoints é desafiadora, especialmente o roteamento e a autenticação. O McAfee Client Proxy, um cliente endpoint opcional, automatiza o roteamento e a autenticação para nosso serviço na nuvem, assegurando uma conexão pervasiva com a nuvem, com imposição consistente de políticas. O McAfee Client Proxy funciona perfeitamente em uma distribuição híbrida com appliances no local, roteando de maneira inteligente o tráfego para o appliance quando está na rede e para o serviço na nuvem quando está fora da rede. Opções adicionais de roteamento e autenticação estão disponíveis e podem ser escolhidas com base em requisitos organizacionais.

Saiba mais

Para obter mais informações, visite mcafee.com/br/products/web-protection.aspx.

