Forcepoint

Solution Brief

Secure Web Gateway

Impeça a perda de dados e os ataques de malware, não a produtividade

Casos de Uso

- Forneça aos funcionários acesso rápido e seguro à Internet
- Exija o cumprimento da política de uso aceitável
- Bloqueie o upload de dados confidenciais para sites não aprovados
- Impeça que malwares invadam dispositivos de usuários sem comprometer a usabilidade
- Detecte e controle o shadow IT
- Evite a exposição corporativa aos dados privados dos usuários

Solução

- Segurança para Internet rápida com DLP integrado e proteção contra ameaças avançadas
- Acesso granular Zero Trust e controles de dados com base em grupo de usuários, tipo de dispositivo, localização do usuário, categoria do site, pontuação de risco do site e muito mais
- A arquitetura distribuída elimina gargalos em uma plataforma AWS com hiperescala e alto tempo de atividade
- Remote Browser Isolation (RBI) opcional para navegação e downloads seguros

Resultados

- Aumente a produtividade, habilitando as pessoas a navegar na Internet em qualquer lugar, de forma transparente e segura
- Reduza o risco por meio do controle de dados confidenciais na nuvem e do bloqueio de malware
- Reduza os custos, simplificando as operações de segurança com um

A Internet é uma bênção e também uma maldição. A maioria das pessoas dependem dela para obter informações para fazer seu trabalho, mas a Internet também cria riscos de exfiltração de dados, violações de políticas de RH, perda de produtividade e infecção por malware. Quando as consequências de não manter os dados e as pessoas seguras aumentam a cada dia, proteger as interações na Internet é um requisito estratégico para as organizações modernas.

Forneça aos funcionários acesso rápido e seguro à Internet

A maioria dos SWGs forçam todo o tráfego da Internet a passar por um data center centralizado (seja no local ou na nuvem), adicionando latência que pode interferir significativamente nos aplicativos de Internet modernos. E, embora as arquiteturas de nuvem hiperescaláveis sejam projetadas especificamente para se ampliar e expandir sob demanda, muitos fornecedores de SWG carecem de uma presença de nuvem altamente distribuída e, em vez disso, administram uma infraestrutura desatualizada que contém gargalos de rede internos. Em contraste, o SWG no Forcepoint ONE tem uma arquitetura distribuída que não apenas fornece uma arquitetura de nuvem hiperescalável com mais de 300 pontos de presença em todo o mundo, mas vai ainda mais longe com uma opção alternativa para oferecer aos clientes ainda mais flexibilidade - um agente no dispositivo que elimina gargalos e pode fornecer até o dobro da taxa de transferência para conteúdos de Internet e aplicativos sensíveis ao desempenho, em comparação com os SWGs concorrentes. Esta opção aplica políticas de segurança localmente no dispositivo do usuário para que o tráfego possa ser trocado diretamente entre o usuário e o site.

Aplique controles de política de uso aceitável (AUP) em sites arriscados

A Internet ser um local distrativo, que nem sempre é usado para os negócios da empresa. O SWG no Forcepoint ONE permite bloquear ou permitir visitantes de sites não produtivos ou inapropriados com controle total do caminho; por exemplo, você pode bloquear alguns subreddits do Reddit e permitir outros. Você pode administrar o acesso com base em grupo de usuários, postura do dispositivo, localização, categoria de URL (pré definida ou personalizada), pontuação de reputação e pontuação de risco do aplicativo corporativo. As categorias de URL personalizadas podem incluir entradas de caminho de diretório de URLs completo, permitindo que os administradores apliquem políticas diferentes para diretórios diferentes.

Bloqueie o upload de dados confidenciais para sites não aprovados

Com o nosso SWG, você pode impedir que dados regulamentados ou propriedade intelectual sejam enviados para armazenamentos de arquivos pessoais, redes sociais ou contas de e-mail pessoais. Você pode verificar e bloquear uploads de arquivos e métodos HTTPS Post para dados confidenciais com os mesmos padrões de DLP predefinidos e personalizados usados pelos serviços CASB e ZTNA no Forcepoint ONE.

Impeça que malwares invadam dispositivos de usuários sem comprometer a usabilidade

Nosso SWG fornece várias formas de proteção contra malwares da web, incluindo bloqueio de categorias de websites, scan online de arquivos baixados e proteção contra ameaças avançadas com base em Zero Trust, como Remote Browser Isolation. Com o nosso RBI, até mesmo sites ou arquivos baixados que estão contaminados podem ser usados com segurança e eficiência.

Detecte e controle o shadow IT

O serviço SWG funciona em conjunto com o nosso CASB para identificar sites que estão sendo usados no lugar dos aplicativos preferenciais da empresa. Esses sites de "shadow IT" são reunidos e exibidos automaticamente na console.

Evite a exposição corporativa aos dados privados dos usuários

Para proteger a privacidade dos funcionários, as organizações podem impedir a descriptografia e a inspeção do tráfego de/para de categorias específicas de sites que normalmente são usados com informações de identificação pessoal (PII), como dados bancários, de saúde e de seguros.

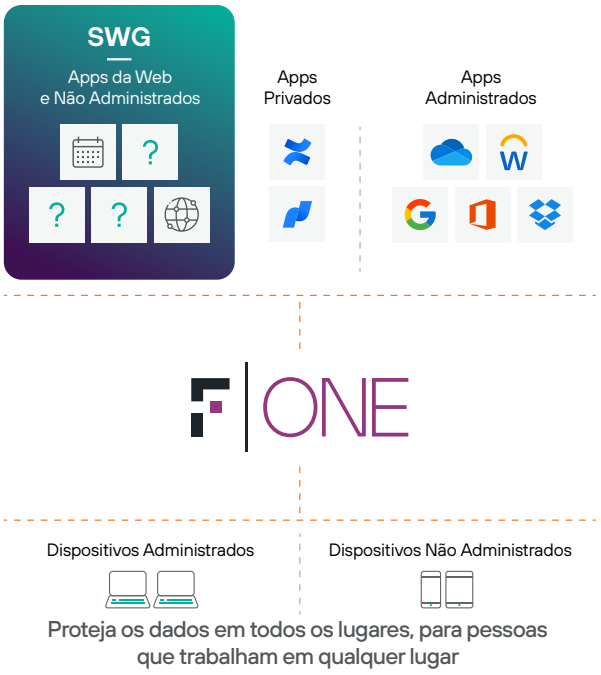
O SWG no Forcepoint ONE maximiza o tempo de atividade, a produtividade e o desempenho

O SWG faz parte do Forcepoint ONE, nossa plataforma de nuvem baseada em hiperescalador com 300 pontos de presença (PoPs), acessibilidade global e tempo de atividade comprovado de 99,99% para proteger o acesso à Internet e preservar a produtividade do usuário. O Forcepoint ONE unifica CASB, SWG e ZTNA para proteger o acesso a aplicativos corporativos SaaS, da web e privados, simplificando a segurança.

Simplificando a segurança da web no mundo real

A plataforma em nuvem Forcepoint ONE fornece um "botão fácil" para implementar a segurança na nuvem.

Em uma console, os administradores podem gerenciar o acesso e controlar downloads e uploads de arquivos entre qualquer site de Internet e qualquer local ou dispositivo gerenciado, incluindo a aplicação de Zero Trust Web Access usando o Forcepoint RBI.



Vamos ver como o SWG simplifica a segurança na Internet quando Carlos, um analista de negócios que trabalha em casa, inicia seu dia de trabalho.

Carlos acessa o reddit.com para pesquisas relacionadas à empresa.	Carlos acessa reddit.com/r/technology para ler publicações recentes sobre malware. As políticas de conteúdo SWG permitem granularidade em nível do diretório; esse subreddit é considerado relacionado ao trabalho, então Carlos pode acessá-lo.
Dentro do subreddit r/technology, Carlos acidentalmente clica em um link para uma página inapropriada.	O administrador do Forcepoint ONE de Carlos criou políticas de conteúdo SWG que permitem o acesso a diretórios como r/technology, mas bloqueiam o acesso a subreddits e páginas inapropriadas. O SWG impede o erro de Carlos e bloqueia a nova página.
Carlos inicia uma planilha confidencial no notebook da empresa que inclui PII do cliente e quer continuar trabalhando no notebook pessoal. Tenta fazer upload do arquivo para um armazenamento em nuvem pessoal e baixar no notebook pessoal.	Para evitar perda de dados empresariais, o administrador do Forcepoint ONE da empresa criou uma política de conteúdo SWG que bloqueia o upload de informações confidenciais de clientes (PII) para qualquer site de compartilhamento de arquivos pessoais. Quando Carlos tenta enviar, o upload é bloqueado e uma mensagem aparece explicando por quê.

Parte de uma solução de segurança unificada para apps de web, nuvem e privados

Além do SWG, a plataforma all-in-one Forcepoint ONE protege o acesso a informações empresariais em qualquer tenant SaaS corporativo e aplicativo privado:

- **Nuvem (SaaS e IaaS):** O CASB aplica controle de acesso contextual, prevenção contra perda de dados (DLP) e proteção contra malware a qualquer aplicativo de Internet voltado para o público com suporte para integração SAML 2 com provedores de identidade de terceiros (IdPs), em qualquer navegador moderno e qualquer dispositivo conectado à Internet. Os dados armazenados em IaaS e SaaS populares também podem ser examinados para identificação de dados sensíveis e malware, e corrigidos. Usa os mesmos padrões de correspondência DLP disponíveis para SWG e ZTNA para aplicativos privados da Web privados.
- **Apps privados:** O ZTNA protege e simplifica o acesso a aplicativos privados sem a complicação ou risco associados às VPNs. Como outras soluções Forcepoint ONE, o ZTNA também aplica controle de acesso contextual, DLP e proteção contra malware a qualquer aplicativo da web.
- **Recursos adicionais:** como o RBI para a forma mais avançada de proteção contra ameaças na web ou o Cloud Security Posture Management (CSPM) para rastrear os provedores de nuvem em busca de configurações de risco.
- **Firewall de nuvem:** complemento do SWG para proteger todo o tráfego de internet e proteger contra ataques projetados para explorar sites de filiais vulneráveis.

Leia o solution brief Forcepoint ONE para mais detalhes.

Que tal proteger dados em aplicativos na nuvem a partir de qualquer dispositivo?

Vamos começar com uma demo.

forcepoint.com/contact