

Forcepoint ONE Web Security

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
- › Arquitetura distribuída elimina pontos de obstrução em plataforma de alto tempo de atividade
- › Inclui o Remote Browser Isolation (RBI) para navegação segura e downloads de sites não categorizados e recém-registrados

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
- › Reduz os custos simplificando operações de segurança

A web é ao mesmo tempo uma bênção e uma maldição. A maioria das pessoas depende dela para obter informações e realizar seu trabalho, mas a web também cria riscos de exfiltração de dados, violações de políticas de RH, perda de produtividade e infecção por malware. O GenAI só aumentou o risco - enquanto promete aumentos de produtividade substanciais, ele também expõe sua organização a muito mais riscos. No entanto, com os protetores adequados, você pode aproveitar os aumentos de produtividade que a IA pode oferecer, mantendo os dados confidenciais seguros e garantindo o uso aceitável. No momento em que as consequências de não manter os dados e as pessoas seguros estão crescendo a cada dia, a proteção de interações na web é um requisito estratégico para as organizações modernas.

Forneça aos funcionários acesso rápido e seguro à Internet

A maioria das soluções de segurança da Web modernas forçam todo o tráfego da Web a desviar por um centro de dados centralizado, seja on-premises ou na nuvem, adicionando latência que pode interferir significativamente em aplicativos da web modernos. E, embora as arquiteturas de nuvem sejam projetadas especificamente para dimensionar a escala de acordo com a demanda, muitos fornecedores de SWG não têm uma presença de nuvem tão altamente distribuída. Em contraste, o Forcepoint ONE possui uma arquitetura distribuída que não só fornece uma arquitetura de nuvem altamente resiliente, 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 pontos de bloqueio e pode fornecer até o dobro da taxa de transferência para conteúdo da Web sensível ao desempenho e aplicativos como gateways da Web seguros 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.

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

A web pode ser um lugar de distração que nem sempre é usado para negócios da empresa. Os controles da Web no Forcepoint ONE permitem que você bloqueie, use uma página de confirmação, use o tempo de cota, solicite autenticação de vários fatores, permita ou até use o RBI para isolar o tráfego. Você pode gerenciar o acesso com base no grupo de usuários, postura do dispositivo, localização. Isso pode permitir que uma organização imponha controles para bloquear o uso de shadow IT de sites GenAI, por exemplo, para gerar código com uma página de bloqueio para direcioná-los para recursos corporativos sancionados, e a granularidade para distinguir entre outros tipos de sites de IA, digamos, para permitir o acesso a site de IA de conversa ou geração de multimídia, enquanto também impõem proteções em torno de quais dados podem ser postados nesses sites.

Bloqueie o upload de dados confidenciais para sites não aprovados

Com nosso mecanismo de segurança, é possível evitar que dados regulamentados ou propriedade intelectual sejam enviados para armazenamento de arquivos pessoais, mídias sociais, contas de e-mail pessoais ou sites GenAI. Você pode digitalizar e bloquear uploads de arquivos e postagens de texto para dados confidenciais com controles fáceis de usar. Opcionalmente, os clientes podem herdar políticas de DLP avançadas do Forcepoint ONE Data Security para aumentar com a solução avançada de segurança de dados líder do setor.

Impeça que malwares invadam dispositivos de usuários sem comprometer a usabilidade

O Forcepoint ONE Web Security fornece várias formas de proteção contra malware transmitido pela web, incluindo o bloqueio de categorias de sites, digitalização em linha de arquivos baixados e proteção avançada contra ameaças baseada em Zero Trust, como isolamento de navegador remoto. Com o Forcepoint RBI mesmo os sites ou arquivos baixados que estejam contaminados podem ser usados com segurança e eficiência.

Detecte e controle o shadow IT

O Web Security trabalha para identificar sites que estão sendo usados no lugar dos aplicativos preferidos da empresa. Esses sites de "shadow IT" são coletados automaticamente e exibidos no painel do Cloud Apps.

Evite a exposição corporativa aos dados privados dos usuários

Para proteger a privacidade dos funcionários, as organizações podem impedir a descryptografia 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.

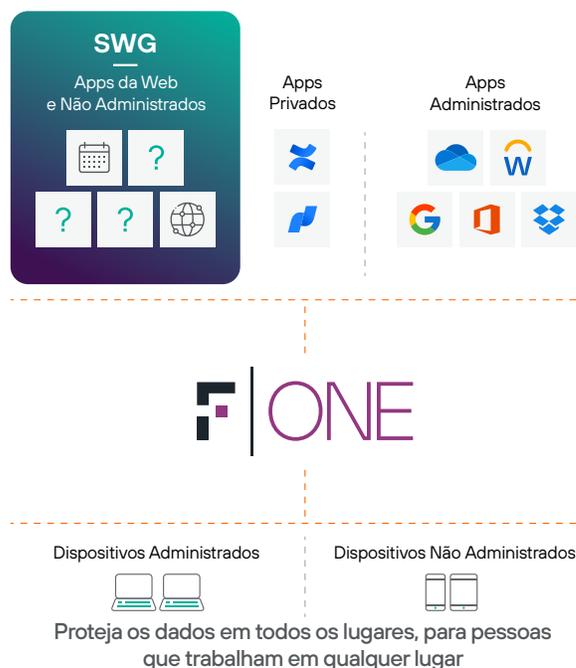
O Forcepoint ONE Web Security maximiza o tempo de atividade, produtividade e desempenho

O serviço de Web Security é parte do Forcepoint ONE, nossa plataforma de nuvem avançada com 300 pontos de presença (PoPs), acessibilidade global e tempo de atividade comprovado de 99,999% para proteger o acesso à Web e preservar a produtividade do usuário. O Forcepoint ONE integra CASB, SWG e ZTNA para acesso seguro a aplicativos corporativos de 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.

A partir de uma console, os administradores podem gerenciar o acesso e controlar os downloads e uploads de arquivos com qualquer site em tempo real, incluindo a aplicação do Zero Trust Web Access usando o Forcepoint RBI.





Vejamos como o serviço de segurança da Web simplifica as coisas quando Carlos, um analista de negócios trabalhando de casa, inicia o 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 integrada para aplicativos da Web, da nuvem e privados

Além da segurança da Web, a plataforma de segurança da nuvem do Forcepoint ONE protege o acesso a informações de negócios em quaisquer aplicativos de locatário SaaS corporativos e privados:

- **Nuvem (SaaS e IaaS):** o CASB aplica controle de acesso contextual, prevenção contra perda de dados (DLP) e proteção contra malware para qualquer aplicativo da Web voltado para o público que suporte à integração do SAML 2 com provedores de identidade (IdPs) terceirizados, de qualquer navegador moderno em qualquer dispositivo conectado à Internet. Dados em repouso em IaaS e SaaS populares também podem ser digitalizados para dados confidenciais e malware e corrigidos. Integra-se ao Forcepoint ONE Data Security para impor políticas de DLP avançadas em canais SSE.
- **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:** expandir o nível essencial de RBI com CDR para uso além de sites desconhecidos ou recém-registrados para a forma mais avançada de proteção contra ameaças da Web, ou adicionar Advanced Malware Detection and Protection para sandboxing de malware e analytics de classe empresarial.

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