Forcepoint

Solution Brief

Forcepoint ONE: a plataforma de nuvem simplifica a segurança para a força de trabalho híbrida

Casos de Uso

- Obtenha visibilidade e controle das interações dos trabalhadores híbridos com dados na web, na nuvem e em aplicativos privados.
- Evite o uso indevido de dados confidenciais acessados de dispositivos gerenciados ou não gerenciados.
- Controle o acesso a conteúdo da Web de alto risco e diferentes tipos de sites de GenAI.
- Forneça acesso remoto, rápido e seguro a recursos de negócios e aplicativos privados sem a complexidade das VPNs.

Solução

- Uma só plataforma unificada permite o gerenciamento de políticas de segurança consistentes em todos os aplicativos de negócios.
- Serviço completo na nuvem que protege o acesso e os dados combinando o Secure Web Gateway (SWG) Cloud Access Broker (CASB) e o Zero Trust Network Access (ZTNA).
- Proteção avançada integrada contra ameaças e segurança de dados para manter os invasores do lado de fora e os dados confidenciais do lado de dentro.
- Recursos adicionais, como RBI com CDR para acesso Zero Trust à web, CSPM para verificar inquilinos de nuvem pública quanto a configurações de risco.
- Forcepoint Classification para marcação de dados.

Resultado

- Simplificada – reúne a segurança para aplicativos da Web, da nuvem e privados em uma plataforma unificada (com suporte sem agentes).
- Moderno — combina os princípios de Zero Trust com uma arquitetura SASE e segurança avançada, como o Remote Browser Isolation e a higienização de arquivos baixados.
- Em todos os lugares — está disponível globalmente, com mais de 300 pontos de presença (PoPs).
- Confiável — oferece tempo de atividade verificado de 99,99% desde 2015.
- Rápido — utiliza aplicação distribuída e dimensionamento automático para eliminar os pontos de estrangulamento.

Segurança Data-First

A segurança continua cada vez mais complexa, mas há uma maneira melhor. Os usuários agora estão trabalhando de qualquer lugar com dados que estão espalhados por todos os lugares — em sites, aplicativos de nuvem e aplicativos privados.

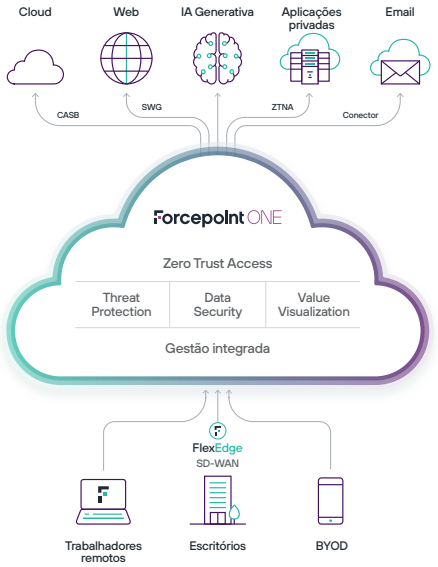
Para dar suporte às iniciativas de retorno ao escritório (RTO) e às forças de trabalho híbridas, as equipes de segurança precisam de uma plataforma de segurança convergente que coloque os dados no centro das atenções. Os controles de segurança precisam ser capazes de se estender pela web, nuvem e acesso a aplicativos privados com visibilidade e controle consistentes para que as organizações possam se antecipar para impedir a perda de dados antes que ela ocorra.

Com uma solução data-first, os dados de negócios podem ser protegidos em todos os lugares para pessoas que trabalham em qualquer lugar.

O Forcepoint ONE simplifica a segurança

O Forcepoint ONE é uma plataforma de nuvem integrada que torna a segurança simples. Você pode adotar rapidamente o Zero Trust e o Security Service Edge (SSE, o componente de segurança do SASE) porque reunimos serviços de segurança cruciais, incluindo SWG, CASB e ZTNA.

Libere a produtividade adotando com segurança novas tecnologias, como GenAI controlando o acesso a diferentes tipos de sites GenAI e, de forma consistente, impondo barreiras de proteção para salvaguardar dados confidenciais e prevenir a exposição ao malware.



Os recursos Zero Trust nativos da nuvem do Forcepoint ONE incluem:

- **Segurança de DLP sem agente para aplicativos de nuvem e privados.** Use com segurança aplicativos da web de negócios privados a partir de dispositivos pessoais, mantendo os dados confidenciais seguros.
- **Proteção avançada contra ameaças e segurança de dados integradas.** Evite a perda ou a exfiltração de dados e impeça os hackers de entrar com controles consistentes em todos os lugares.
- **Gateways unificados para acesso à nuvem, web e aplicativos privados.** Controle de acesso baseado em identidade para aplicativos de negócios gerenciados em um só lugar para SWG, CASB e ZTNA.
- **Escalabilidade dinâmica com acesso global.** 300 PoPs construídos na AWS fornecem conectividade rápida e de baixa latência e tempo de atividade de 99,99%, independentemente de onde as pessoas trabalham.

Segurança unificada para web, nuvem e aplicativos privados

- **Nuvem:** o CASB aplica acesso granular a aplicativos de SaaS corporativos e dados de qualquer dispositivo. O CASB bloqueia o download de dados confidenciais e bloqueia o upload de malware em tempo real. Ele verifica os dados em repouso em SaaS e IaaS populares para detectar malware e dados confidenciais e corrige conforme necessário. O CASB detecta aplicativos de shadow IT e controla o acesso a partir de qualquer dispositivo gerenciado.
- **Web:** o SWG monitora e controla as interações com qualquer site baseando-se em risco e categoria, bloqueando o download de malware ou uploads de dados confidenciais para compartilhamento de arquivos pessoais e contas de e-mail. Nossa segurança da web no dispositivo impõe políticas de uso aceitáveis em dispositivos gerenciados localizados em qualquer lugar.
- **Aplicativos privados:** a ZTNA protege e simplifica o acesso a aplicativos privados sem a complicação ou o risco associados às VPNs.

Segurança de dados e proteção contra ameaças generalizadas

- **Data Loss Prevention (DLP):** os arquivos e o texto são verificados após o upload e download quanto a dados confidenciais e bloqueados, rastreados, criptografados ou editados, conforme apropriado. Mais de 190 regras de DLP predefinidas ajudam a simplificar a conformidade regulatória e fornecem tempo para valor rápido. A integração fácil com o Forcepoint Enterprise DLP permite a segurança de dados em todos os lugares — no endpoint, na rede, na web e em serviços de nuvem.
- **Verificação de malware:** os arquivos são verificados após o upload e download quanto a malware e bloqueados quando detectado.

Visibilidade e controle integrados

- **Conjunto de gerenciamento integrado** para configuração, monitoramento e relatórios em canais de SSE.
- **Políticas de login** para controlar o acesso a aplicativos da Web, da nuvem ou privados com base na localização do usuário, tipo de dispositivo, postura do dispositivo, comportamento do usuário e grupo de usuários. Esses parâmetros ajudam a evitar aquisições de contas.
- **Políticas de DLP fáceis de usar** para controlar o download e upload de dados confidenciais e malware para aplicativos SaaS gerenciados, aplicativos privados e sites, bem como para dados armazenados em SaaS e IaaS gerenciados.
- **Agente no dispositivo** para Windows e MacOS para suporte a SWG, CASB ou ZTNA para aplicativos de cliente não navegadores e controle de TI sombreado.
- **Análises unificadas e visualização de valor** para insights rápidos sobre riscos de segurança, utilização geral e impacto da plataforma de segurança de nuvem tudo-em-um.

Capacidades adicionais disponíveis conforme necessário

- **Gerenciamento de postura de segurança na nuvem (CSPM):** verifica as configurações de inquilinos AWS, Azure e GCP quanto a configurações de risco e fornece correção manual e automatizada.
- **Gerenciamento de Postura de Segurança SaaS (SSPM):** verifica as configurações de inquilinos do Salesforce, ServiceNow e do Office 365 para configurações de risco e fornece correção manual e automatizada.
- **Remote Browser Isolation (RBI):** protege um usuário contra malware transmitido pela web em seu dispositivo local rodando um navegador em uma VM hospedada na nuvem. Usa o CDR para higienizar arquivos baixados durante uma sessão de RBI de qualquer malware ou elementos estrangeiros.
- **Forcepoint Classification:** tagueamento e classificação de dados com sugestões habilitadas por IA para aprimorar a precisão de marcação.
- **AMDP:** analisa o comportamento de arquivos em um sandbox de malware controlado para identificar conteúdo oculto e malicioso.

Assinaturas que desbloqueiam a simplicidade

Assinaturas anuais por usuário estão disponíveis:

- **Edição tudo-em-um** para web, nuvem e segurança de aplicativos privados.
- **A edição de segurança da Web** inclui o web gateway além de CASB em linha para aplicativos de nuvem ilimitados e princípios básicos de RBI para sites não categorizados e recém-registrados para adicionar suporte a API para aplicativos e suporte em nuvem para aplicativos privados mais tarde.
- **A edição ZTNA** protege um número ilimitado de aplicativos privados.
- **A edição CASB** protege um número ilimitado de aplicativos de nuvem inline e inclui APIs para 3 aplicativos com a capacidade de adicionar pacotes de aplicativos extras ou nós de pesquisa de API dedicados.
- **Todas as assinaturas** incluem gerenciamento de nuvem centralizado, políticas com prevenção de perda de dados acesso automatizado por meio de agente de endpoint, e relatórios abrangentes.

forcepoint.com/contact