Forcepoint

Resumo da Solução

Cloud Access Security Broker

Proteja os dados de forma simples em qualquer app de nuvem, acessado em qualquer dispositivo

Desafio

- Proteja e controle o acesso a apps administrados em dispositivos BYOD
- Controle o upload e o download de dados sensíveis em qualquer app SaaS administrado
- Bloqueie malwares ocultos em arquivos de dados de negócios
- Detecte e controle TI sombra

Solução

- Segurança para apps de nuvem com DLP integrado e proteção contra ameaças avançadas
- Acesso Zero Trust granular e controles de dados com base em usuário, dispositivo ou local
- A plataforma AWS com hiperescala maximiza o tempo de atividade e minimiza a latência
- Aplicação de DLP em dispositivos administrados e não administrados

Resultado

- Aumente a produtividade, habilitando as pessoas a usar as informações 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 único local para definir políticas
- Simplifique a conformidade com processos demonstráveis para controlar informações

Acessar aplicativos e dados em nuvem usando dispositivos móveis é comum para a força de trabalho híbrida de hoje. A empresa média implementa mais de 280 aplicativos SaaS, incluindo ferramentas de colaboração como Microsoft 365, Google Workplace, Slack ou Jira, indispensáveis para funcionários e prestadores de serviços remotos. Usar esses serviços sem uma forma de administrar o acesso a partir de dispositivos móveis ou estabelecer confiança nos dispositivos (postura do dispositivo) adiciona complexidade e risco.

Proteja o acesso a aplicativos de negócios a partir de dispositivos BYOD e não administrados

A Forcepoint simplifica a segurança na nuvem. O serviço de segurança CASB do Forcepoint ONE implementa acesso Zero Trust que habilita apps de nuvem críticos para os negócios, para que sejam usados com segurança nos dispositivos pessoais dos funcionários (BYOD) e em dispositivos não administrados de parceiros e prestadores de serviços.

Controle o upload e o download de dados sensíveis em qualquer app SaaS administrado

Nós disponibilizamos um conjunto de políticas de segurança para controlar dados confidenciais, com desempenho líder do setor, independentemente de onde e como funcionários e prestadores de serviços se conectam à Internet. Administrar o acesso a esses aplicativos a partir de dispositivos móveis facilita a adoção e a produtividade, enquanto ter políticas diferentes com base na postura e localização do dispositivo fornece controle granular Zero Trust que mantém os dados seguros. Você obtém mais certeza sobre como os dados confidenciais são compartilhados nos aplicativos da empresa em qualquer dispositivo, mesmo os pessoais. A prevenção contra perda de dados (DLP) é integrada; portanto, você não precisa de produtos pontuais para impedir violações de dados.

Bloqueie malwares ocultos em arquivos de dados de negócios

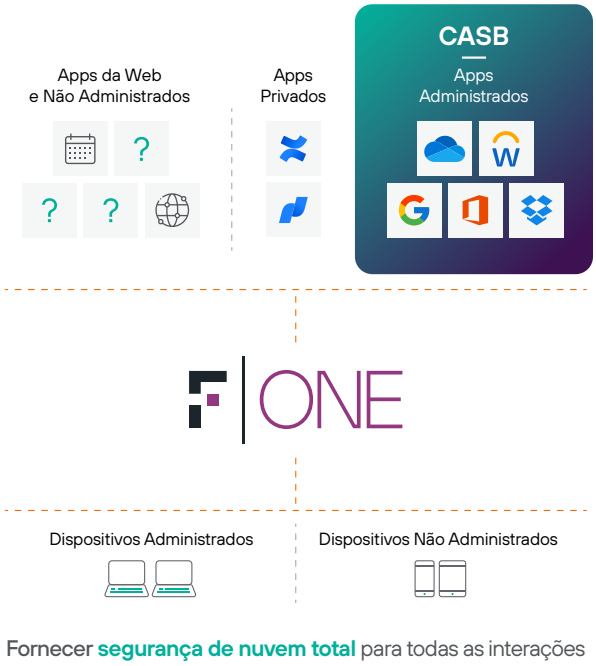
Nosso CASB pode detectar e bloquear malware em dados em trânsito entre usuários e o aplicativo SaaS usando mecanismos de malware Bitdefender e CrowdStrike. Também pode detectar malware em arquivos em armazenamentos SaaS e IaaS populares e colocar esses arquivos em quarentena.

Detecte e controle TI sombra

O CASB não apenas revela a TI sombra: também fornece controle e orientação sobre o uso seguro e melhores alternativas. O CASB detecta e lista aplicativos SaaS não administrados em uso, permitindo que os administradores criem políticas para dispositivos da empresa que possam bloquear o acesso ou exibir uma mensagem de encaminhamento do usuário para aplicativos SaaS aprovados.

O CASB no Forcepoint ONE maximiza o tempo de atividade, a disponibilidade e a produtividade

Nosso CASB 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 aplicativos em nuvem de forma transparente e preservar a produtividade do usuário. Outras soluções desviam o tráfego de rede de/para aplicativos em nuvem para data centers privados em vez de locais próximos aos usuários. Isso leva a desempenho ruim, fazendo com que aplicativos sensíveis à latência, como o Slack, falhem e os funcionários busquem soluções alternativas de alto risco.



Fornecer **segurança de nuvem total** para todas as interações

Simplificando a segurança de nuvem 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 para usuários de dispositivos administrados e não administrados (como BYOD e computadores de fornecedores ou parceiros).

Vamos ver como o CASB simplifica a segurança na nuvem quando Carlos, uma analista de negócios que trabalha em casa, inicia seu dia de trabalho.

Carlos faz login na conta do Salesforce usando o notebook corporativo.	O CASB no Forcepoint ONE gerencia conexões com aplicativos de negócios, permitindo que os usuários façam logon de forma transparente e segura.
Carlos acessa o salesforce.com diretamente ou por intermédio de um portal de aplicativos da empresa.	O Salesforce redireciona a sessão para o CASB (por meio de SAML), que analisa se o dispositivo é administrado, sua localização e sua postura de segurança. Com base em políticas de segurança predefinidas, o CASB confirma a identidade de Carlos por meio de aplicativos de autenticação multifatores.
Carlos recebe acesso ao aplicativo administrado.	As políticas de administração também controlam se haverá acesso direto ao aplicativo, acesso controlado ou nenhum acesso. Isso acontece em milissegundos sem afetar a produtividade dos funcionários. Todo o tráfego do dispositivo de Carlos e do aplicativo passa pelo CASB (usando um proxy reverso).
Carlos decide fazer download de uma previsão de receita do Salesforce.	O CASB verifica qualquer arquivo baixado do aplicativo em busca de malware e dados confidenciais. Dependendo do resultado e da política, pode bloquear arquivos de malware, e bloquear, rastrear ou criptografar dados confidenciais. Se uma política restringir o download de dados confidenciais para dispositivos administrados, o download será permitido, pois Carlos está usando um notebook da empresa.
Carlos tenta transferir dados confidenciais ou um arquivo contaminado com malware via Slack ou carrega os dados em seu armazenamento pessoal do Dropbox.	O CASB também pode verificar arquivos que estão sendo carregados em aplicativos em nuvem. O CASB pode bloquear automaticamente o upload. Pode até bloquear o upload de arquivos em aplicativos não autorizados usando o agente unificado no dispositivo.

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

Além do CASB, a plataforma all-in-one Forcepoint ONE protege o acesso a informações comerciais em qualquer site de Internet e aplicativo privado:

- **Internet:** O SWG monitora e controla as interações com qualquer site de Internet com base no risco e na categoria, bloqueando o download de malware ou uploads de dados confidenciais para compartilhamento de arquivos pessoais e contas de e-mail. Nosso SWG no dispositivo impõe políticas de uso aceitável em dispositivos administrados em qualquer lugar.
- **Apps privados:** A ZTNA protege e simplifica o acesso a aplicativos privados sem a complicação ou risco associados às VPNs.
- **Recursos adicionais,** como RBI ou varredura de provedores de nuvem para configurações arriscadas (CSPM), conforme necessário.

Leia o resumo da solução Forcepoint ONE para mais detalhes.

Pronto para proteger dados em aplicativos na nuvem a partir de qualquer dispositivo?

Vamos começar com uma demonstração.