Forcepoint

Resumo da Solução

Cloud Access Security Broker

Proteja os dados em qualquer aplicativo de nuvem, acessado de 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
- Detecção de shadow IT

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

Os novos modelos de força de trabalho atuais exigem que os usuários em qualquer lugar tenham acesso rápido, porém controlado, aos dados de negócios em todos os lugares. Isso significa que as pessoas precisam de acesso a dados em aplicativos de nuvem, como o Microsoft 365, Google Workspace, Slack, Jira e Salesforce a partir de qualquer tipo de dispositivo ou local. Com mais de 250 aplicativos de SaaS para a empresa média, a visibilidade e o controle podem facilmentetornar-se incontroláveis.

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 os funcionários e prestadores de serviços se conectam à Internet. O gerenciamento do acesso a esses aplicativos a partir de dispositivos móveis facilita a adoção e a produtividade, enquanto a existência de políticas diferentes com base na identificação e no local fornece controles Zero Trust granulares. A verificação inline para dados confidenciais e malware mantém a segurança dos dados em todos os aplicativos de SaaS. Você ganha mais certeza sobre como os dados confidenciais são compartilhados em aplicativos da empresa e com Data Loss Prevention (DLP) integrado, você não precisa de produtos pontuais para impedir as violações de dados.

Bloqueie malwares ocultos em arquivos de dados de negócios

O Forcepoint ONE CASB pode detectar e bloquear malware em dados movimentados entre os usuários e o aplicativo SaaS usando mecanismos anti-malware da Bitdefender e CrowdStrike. Também pode detectar malware em arquivos em armazenamentos populares de SaaS e IaaS e colocar esses arquivos em quarentena.

Detecção de shadow IT

O Forcepoint ONE CASB conta com o shadow IT e gera uma pontuação de risco para aplicativos não sancionados ao analisar vários atributos. Isso permite que as equipes de TI tenham um entendimento mais profundo do uso de SaaS em sua organização e apliquem os controles de segurança necessários. O CASB detecta aplicativos de SaaS não gerenciados em uso, empregando logs de rede ou com telemetria do gateway de web segura do Forcepoint ONE para permitir que políticas de segurança consistentes sejam aplicadas a aplicativos de SaaS sancionados e não sancionados. Assim, dados de empresas permanecem seguros, onde quer que sejam usados.

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 hyperscaler com mais de 300 pontos de presença (PoPs), acessibilidade global e tempo de atividade comprovado de 99,99% para proteger aplicativos de 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 mais próximos dos usuários e dos aplicativos que estão acessando. 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.

Simplificando a segurança de nuvem 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 dados para usuários de dispositivos gerenciados e não gerenciados (como BYOD e computadores de prestadores de serviços 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 gerenciado, sua localização e sua postura de segurança. Com base em políticas de segurança predefinidas, o CASB confirma a identidade de João por meio 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 João e do aplicativo passa pelo CASB (usando um proxy reverso ou de encaminhamento).
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 não gerenciados, o download será permitido, pois João está usando um notebook da empresa.
O João tenta transferir dados confidenciais ou um arquivo contaminado com malware por meio do Slack.	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 verificação de provedores de nuvem quanto a configurações de risco Cloud Security Posture Management (CSPM) e SaaS Security Posture Management (SSPM), 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.

forcepoint.com/contact