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
- Detecte e controle shadow IT

Solução

- Segurança de aplicativos SaaS 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 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 SaaS, como Microsoft 365, Google Workspace, Slack, Jira e Salesforce, de qualquer tipo de dispositivo ou local. Com mais de 250 aplicativos SaaS para a empresa média, a visibilidade e o controle podem facilmente se tornar impossíveis de gerenciar.

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

A Forcepoint simplifica a Cloud Security. O serviço de segurança CASB do Forcepoint ONE implementa o acesso Zero Trust que permite que aplicativos SaaS críticos para os negócios sejam usados com segurança a partir de dispositivos pessoais de funcionários (BYOD) e dispositivos não gerenciados 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 em movimento entre os usuários e o aplicativo SaaS usando mecanismos de malware de vários mecanismos antimalware de terceiros. Também pode detectar malware em arquivos em armazenamentos populares de SaaS e IaaS e colocar esses arquivos em quarentena.

Detecte e controle shadow IT

O Forcepoint ONE CASB dá visibilidade à shadow IT e gera uma pontuação de risco para aplicativos não aprovados ao analisar vários atributos. Isso permite que as equipes de TI tenham um entendimento mais profundo sobre o uso de SaaS em sua organização e apliquem os controles de segurança necessários. O CASB detecta aplicativos SaaS não gerenciados em uso empregando logs de rede de firewalls e proxies corporativos para permitir que políticas de segurança consistentes sejam empregadas em aplicativos SaaS aprovados e não aprovados, de modo que os dados de negócios permaneçam seguros onde quer que sejam usados.

Solução de segurança SaaS que maximiza o tempo de atividade, a disponibilidade e a produtividade

Nosso CASB é desenvolvido sobre uma arquitetura nativa da nuvem e baseado em hyperscaler, com mais de 300 pontos de presença (PoPs), acessibilidade global e tempo de atividade comprovado de 99,99% para proteger aplicativos SaaS de forma transparente e preservar a produtividade do usuário. Outras soluções desviam o tráfego de rede de e para aplicativos SaaS para data centers privados, em vez de para locais mais próximos dos usuários e dos aplicativos que eles 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 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 os arquivos que estão sendo carregados em aplicativos SaaS. O CASB pode bloquear automaticamente o upload. Pode até bloquear o upload de arquivos em aplicativos não aprovados usando o agente unificado no dispositivo.

Parte da abordagem Data Security Everywhere da Forcepoint

A missão do Data Security Everywhere da Forcepoint permite que as organizações protejam dados em SaaS, web, e-mail, rede e endpoints, para que as pessoas possam trabalhar com segurança em qualquer lugar com dados em todos os lugares.

Estendendo os recursos de DLP líderes do setor para aplicativos SaaS

Com a Forcepoint, as organizações podem utilizar suas políticas do Forcepoint DLP existentes para proteger dados em aplicativos SaaS, estendendo a mesma segurança de dados líder do setor para a nuvem com apenas alguns cliques. Políticas de DLP unificadas aplicadas a partir de um único console ajudam a oferecer segurança de dados consistente e de classe empresarial para aplicativos SaaS, simplificando o gerenciamento de segurança de dados, minimizando violações e simplificando a conformidade. Os clientes podem obter os seguintes benefícios por meio dessa integração:

- → Segurança de dados na nuvem simplificada com políticas e console unificados.
- → 1.700 classificadores e modelos de políticas out-of-the-box para cobertura abrangente e suporte à conformidade para mais de 150 regiões.
- → Configuração e tempo de retorno do investimento em minutos, melhorando a produtividade das equipes de TI/segurança.
- → Eliminando produtos de segurança redundantes e fragmentados para alcançar uma economia de custos significativa.

Leia o folheto do Forcepoint DLP para obter mais detalhes.

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

Vamos começar com uma demonstração.

forcepoint.com/contact