Forcepoint

Datasheet

Cloud Access Security Broker

CASB multimodal com modos de reverse proxy sem agentes, forward proxy e API.

Principais benefícios:

- Tempo de atividade verificado de 99,99% desde 2015
- O escalonamento automático e mais de 300 pontos de presença na AWS minimizam a latência e maximizam o throughput
- DLP de classe empresarial em todos os principais canais — CASB, SWG, e-mail e endpoints, com gerenciamento, configuração e relatórios unificados.
- O agente de sincronização do Active Directory acelera a integração de usuários
- O exame de dados em trânsito bloqueia malwares e exfiltração de dados entre usuários em qualquer dispositivo e qualquer aplicativo SaaS administrado.
- A lógica SASE programável em campo pode bloquear métodos de solicitação HTTP/S específicos, resultando em controle granular de qualquer elemento em uma página da web gerenciada pelo SaaS
- A varredura de dados em repouso de SaaS e IaaS selecionados identifica malware e dados sensíveis, independentemente da varredura de dados em movimento
- A Criptografia em nível de arquivos de aplicativos SaaS gerenciados garante a privacidade e a soberania dos dados sem bloquear completamente o acesso aos dados
- Os relatórios de shadow IT ajudam a identificar o risco de aplicativos não autorizados
- O Digital Rights Management (DRM) fornece mais flexibilidade com novas formas de proteger dados confidenciais.

O Forcepoint Cloud Access Security Broker (CASB) oferece a mais ampla visibilidade e controle sobre o uso de aplicativos SaaS sancionados por corporações, incluindo IA Generativa. Protege dados confidenciais com o Data Loss Prevention (DLP) líder do setor, fornecendo controle de acesso granular e proteção contra malware para defender contra as ameaças modernas.

Modo de Reverse Proxy sem agentes

O modo de proxy reverso sem agentes aplica o acesso granular com o DLP integrado e varredura de malware do Forcepoint CASB a partir de qualquer dispositivo que use um navegador moderno. É ideal para monitorar e controlar o acesso de dispositivos BYOD e de prestadores de serviços. Ele aproveita a integração patenteada da Forcepoint com qualquer IdP compatível com SAML 2.0 para redirecionar os usuários para um reverse proxy da Forcepoint, onde uma sessão complementar com o aplicativo SaaS é estabelecida.

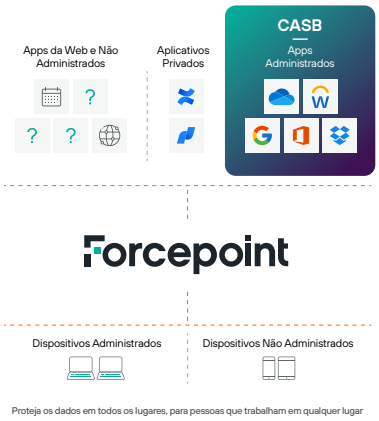

Figura 1: Reverse proxy sem agentes do Forcepoint CASB com AJAX/VM.

Combinado com a tecnologia exclusiva AJAX/VM da Forcepoint, executada no navegador do usuário, o modo de proxy reverso sem agentes do Forcepoint CASB garante a reescrita adequada de URLs e cookies, resultando em compatibilidade com qualquer aplicativo SaaS. Os principais recursos que permitem controlar e monitorar o uso de aplicativos no modo de proxy reverso são políticas de proxy, criptografia em nível de campo, relatórios de shadow IT e relatórios de reverse proxy.

Políticas de proxy

As opções de controle de acesso e as opções de verificação de DLP e malware associadas para dados em movimento de e para aplicativos SaaS gerenciados são definidas em políticas de proxy. Isso permite que os administradores definam o acesso ao aplicativo SaaS gerenciado como acesso direto ao aplicativo, neguem ou protejam o acesso ao aplicativo (todo o tráfego passa pelo proxy reverso com a opção de aplicar o DLP e a varredura por malware). Os critérios para aplicação de políticas incluem grupo de usuários, método de acesso (navegador, aplicativo cliente não navegador ou qualquer outro), SO do dispositivo, perfil do dispositivo e localização.

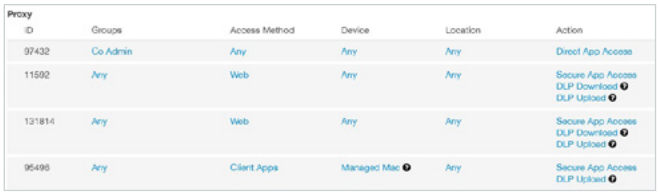

Figura 2: Lista de políticas de proxy para um aplicativo SaaS gerenciado

Um único aplicativo pode ter uma lista de várias políticas de proxy que são avaliadas sequencialmente até que uma política seja encontrada em que todos os critérios de correspondência da política correspondam à solicitação de conexão. Em seguida, a ação de execução apropriada é aplicada.

Quando o acesso seguro ao aplicativo é especificado, uma única política de proxy pode incluir uma lista de políticas de DLP e varredura de malware para upload no aplicativo SaaS e outra lista para download no aplicativo SaaS. Além disso, se um aplicativo SaaS gerenciado tiver criptografia em nível de campo ativada, a política de proxy permite que você especifique se um campo é exibido sem criptografia com base no nível de segurança do campo ou se o local do usuário corresponde ao local de criação dos dados. Isso suporta a privacidade e a soberania dos dados

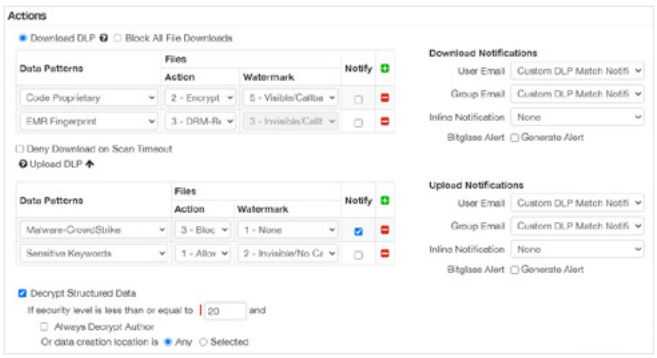

Figura 3: Detalhes da Política de Proxy para uma conexão segura de acesso ao aplicativo

Dentro de uma única política de proxy, as políticas DLP de download permitem que você controle o download de dados confidenciais e malware, enquanto as políticas DLP de upload permitem que você controle o upload de dados confidenciais e malware. Basta usar menus suspensos para especificar um padrão de dados para corresponder, uma ação de arquivo e controle de marca d'água/rastreamento, e clicar na caixa de seleção se quiser que as pessoas sejam notificadas sobre a correspondência.

O Forcepoint CASB inclui mais de 190 padrões de dados predefinidos que ajudam você a aplicar padrões regionais e do setor sobre PII, PHI e dados financeiros pessoais. Também há padrões de dados reservados para invocar a varredura de malware alimentada por vários mecanismos anti-malware de terceiros. Você também pode criar padrões de dados personalizados que usam expressões regulares simples até expressões booleanas complexas e padrões de dados especiais para identificar registros. Os padrões de correspondência especiais incluem correspondência de bancos de dados (usando correspondência exata), semelhança com um formulário padrão (usando impressão digital de arquivos) e qualquer método de solicitação HTTP/S (usando a lógica SASE programável do Campo – FPSL).

Para políticas de proxy de download, as ações de arquivos são criptografadas, bloqueadas (substituindo o conteúdo por mensagem de bloqueio), negadas (não transferidas), aplicadas DRM, marca d'água e rastreadas. Para políticas de proxy de upload, as ações de arquivos são criptografadas (para Office 365, Google Workspace e Salesforce), bloqueio (substitua o conteúdo por mensagem de bloqueio), negação (não transferência), mascaramento de dados (Salesforce Chatter, O365 Teams e Slack), marca d'água e rastreamento.

Criptografia em nível de campo

O modo de proxy reverso sem agentes permite que você criptografe dados estruturados em muitos aplicativos SaaS populares com suporte para criptografia ou tokenização completa do AES de 256 bits, um keystore integrado ou seu próprio keystore do Key Management Interoperability Protocol (KMIP) e criptografia e tokenização sem vault. Você também pode especificar níveis de segurança para cada campo para controlar quando o campo é descriptografado para o usuário.

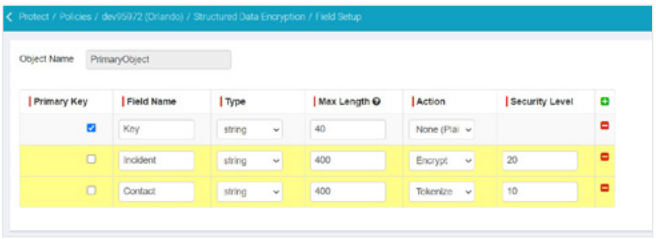

Figura 4: Configurações de Criptografia em nível de campo

Relatórios de shadow IT

O modo de proxy reverso sem agentes suporta os relatórios de shadow IT. O uso de shadow IT é coletado a partir dos dados de log de firewalls corporativos e servidores proxy, por importação manual ou por meio de um coletor de syslog da Forcepoint. Os relatórios mostram a distribuição de aplicativos por índice de confiança, calculado pela Forcepoint, e os aplicativos mais acessados com detalhamento de aplicativos individuais e endereços IP de origem individuais, ajudando você a entender suas organizações e a postura de riscos em relação ao tráfego da web. O Forcepoint CASB também pode permitir que você controle o tráfego de shadow IT no modo de forward proxy (veja abaixo).

Figura 5: Relatório do Shadow IT Discovery.

O modo de proxy reverso oferece relatórios para fornecer informações abrangentes sobre o tráfego SaaS gerenciado que passa pelo proxy reverso: as seções 'Data in Motion' dos painéis de Data Security e Threat e o relatório de logs do proxy. O dashboard do Data Security exibe detalhes sobre dados confidenciais identificados pela Forcepoint, incluindo o movimento de dados confidenciais para dentro e para fora de aplicativos protegidos pela Forcepoint, além de mostrar uploads confidenciais para aplicativos não autorizados, downloads confidenciais para dispositivos não gerenciados, os principais grupos e usuários movendo dados confidenciais e muito mais.

O dashboard de Ameaças inclui os mesmos tipos de métricas do dashboard de Data Security, mas especificamente para malware e ameaças cibernéticas.

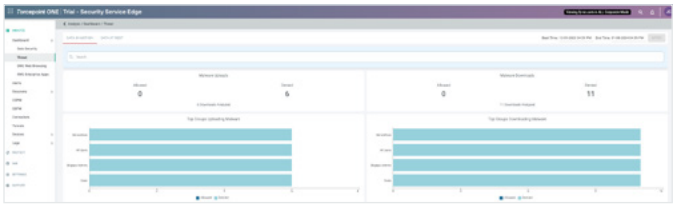

Figura 6: Dashboard do Proxy

O relatório de logs de proxy plota a atividade de aplicativos e marca d'água, DLP e DRM ao longo do tempo e lista eventos recentes agrupados por categorias de resumo, auditoria e vazamento de dados.

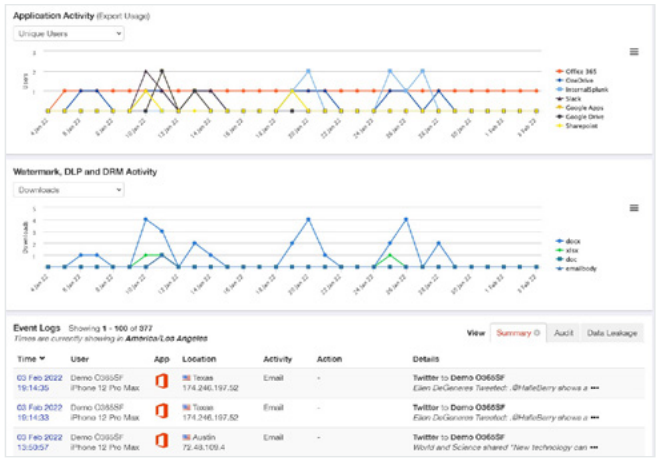

Figura 7: Relatório de logs do proxy

Modo de Proxy Avançado

O modo de proxy de encaminhamento usa o agente unificado da Forcepoint para Windows ou MacOS. Todo o tráfego SaaS gerenciado ainda passa pelo reverse proxy da Forcepoint, mas sem a necessidade de reescrever a URL para se conectar com o dispositivo do usuário. O modo de proxy direto suporta todos os recursos do modo de proxy reverso sem agentes, incluindo a aplicação de DLP e varredura de malware por meio de políticas de proxy, mas também suporta o uso de clientes que não são navegadores, como o cliente Microsoft Outlook e o cliente Slack. Além disso, o modo de proxy de encaminhamento suporta o controle do shadow IT.

Controle do shadow IT

O controle de Shadow IT permite que você controle o acesso a qualquer aplicativo de shadow IT usando políticas de proxy que são avaliadas em sequência, como políticas de proxy gerenciadas do SaaS. No entanto, as políticas de proxy para aplicativos de shadow IT não aplicam a varredura de DLP e malware para upload e download. Em vez disso, eles são limitados às seguintes opções de controle de conexão: renderizar o aplicativo em modo somente leitura, treinar (exibir uma recomendação para um aplicativo alternativo sancionado pela empresa e permitir ou negar o acesso ao aplicativo original de shadow IT) ou negar o acesso sem uma mensagem de coaching.

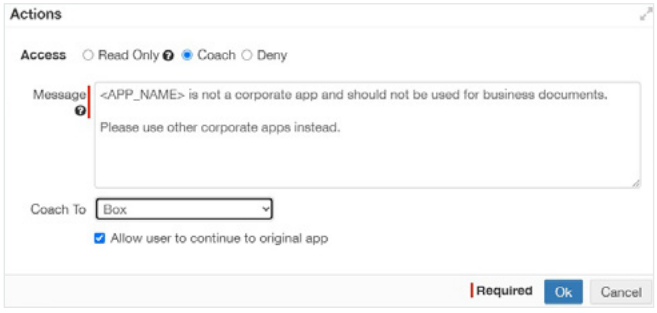

Figura 8: Detalhes da política de proxy do shadow IT mostrando as opções do coach

Se você precisa suportar políticas de DLP e varredura de malware para aplicativos de shadow IT, use as políticas de conteúdo do SWG.

Modo API

No modo API, o CASB usa chamadas de API para seu inquilino SaaS ou IaaS para verificar dados em repouso em busca de dados confidenciais ou malware e executar ações de remediação automáticas, como restringir o compartilhamento, colocar em quarentena, copiar, adicionar metadados de classificação ou notificar o proprietário do arquivo. Within a policy, you can specify match criteria based on user group, DLP data pattern, file path, file name, sharing status (external, internal, public, or any), file size, owner, shared with username, create date, and modified date. The data match patterns used in an API policy can be any of the custom or predefined match patterns shared across the proxy policies, letting you have unified control of sensitive data and malware.

Políticas da API

As políticas da API controlam os dados de varredura em IaaS e SaaS. Como as políticas de proxy, várias políticas de API podem ser aplicadas a um único aplicativo SaaS e são avaliadas sequencialmente.

Figura 9: Lista de políticas da API.

Dentro de uma política, você pode especificar critérios de correspondência com base em grupo de usuários, padrão de dados do DLP, caminho do arquivo, nome do arquivo, status do compartilhamento (externo, interno, público ou qualquer outro), tamanho do arquivo, proprietário, compartilhado com o nome de usuário, data de criação e data de modificação. Os padrões de correspondência de dados usados em uma política de API podem ser qualquer um dos padrões de correspondência personalizados ou predefinidos compartilhados nas políticas de proxy, permitindo que você tenha controle unificado de dados confidenciais e malware.

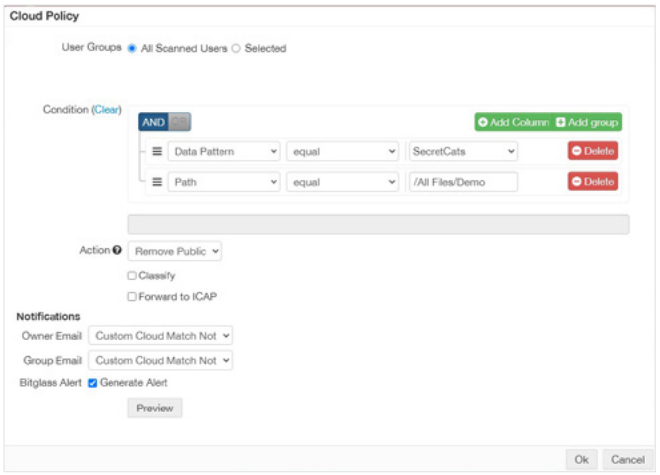

Figura 10: Detalhes da política da API

Quando uma correspondência de condições para um arquivo verificado ocorre, as possíveis ações da política da API incluem o compartilhamento de modificar (remover público, remover público e externo, remover tudo), permitir, colocar em quarentena, criar cópia e criptografar.

CASB Integrações com terceiros

O Forcepoint CASB também pode ser configurado para se integrar com vários outros sistemas de segurança de dados, conforme descrito abaixo.

- → **Segurança das Informações e Gerenciamento de Eventos (SIEM).** O Forcepoint CASB se integra a qualquer sistema que suporte syslog. Isso permite que aplicativos de terceiros façam upload de logs da Forcepoint para visualização e análise
- → **Sistemas DLP on-premises.** Embora o Forcepoint CASB seja totalmente integrado ao Forcepoint DLP, ele também funciona com qualquer sistema DLP on-premises que suporte o Internet Content Adaptation Protocol (ICAP). Isso fornece aos clientes a capacidade de enviar arquivos em repouso em armazenamento gerenciado na nuvem SaaS ou IaaS, que são sinalizados pela Forcepoint como tendo dados confidenciais, para o sistema DLP on-premise usando Criptografia TLS. Os arquivos são enriquecidos com dados como IP de origem e destino e o endereço de e-mail do proprietário do arquivo.
- → **Security Orchestration and Response (SOAR).** O Forcepoint CASB suporta a integração bidirecional entre o CASB e as plataformas SOAR selecionadas. Nesses casos, a plataforma SOAR é usada para automatizar atividades dentro do Forcepoint CASB e de outra ferramenta.
- → **Classificação de dados.** O Forcepoint CASB pode usar metadados de classificação de qualquer classificador de dados em um padrão de correspondência do DLP.
- → **Gerenciamento do endpoint.** Como parte do processo de login por SAML, o Forcepoint CASB pode validar um certificado de cliente armazenado em um dispositivo Windows, Mac, Android ou IOS para confirmar que ele é gerenciado por um sistema de gerenciamento de endpoint. Esse conhecimento permite que o administrador aplique diferentes políticas de acesso para usuários que fazem login por meio de dispositivos gerenciados e não gerenciados.

Diferença do Forcepoint CASB

- → **Maior visibilidade do SaaS:** o maior banco de dados conhecido com mais de 800.000 aplicativos SaaS, juntamente com sua classificação de riscos por meio da avaliação de mais de 40 atributos.
- → **Segurança de dados líder do setor:** Estenda as políticas do Forcepoint DLP para todos os principais canais, como endpoint, rede, nuvem, web ou e-mail, para que seus dados estejam protegidos, onde quer que residam. A aplicação de políticas unificada por meio de um único console, juntamente com mais de 1700 modelos, políticas e classificadores predefinidos, ajuda a atender às demandas regulatórias de 90 países e mais de 150 regiões.
- → **Acesso sem agentes para aplicativos SaaS:** Acesso sem atrito e Zero Trust a qualquer aplicativo a partir de qualquer dispositivo não gerenciado por meio de implementação de reverse-proxy sem agentes, protegendo o acesso a partir de dispositivos não gerenciados, incluindo BYOD e dispositivos de parceiros ou contratados terceirizados.
- → **Controle de qualquer aplicativo:** Controle qualquer aplicativo baseado na web, incluindo aplicativos incomuns e personalizados, com controles extensíveis usando a lógica SASE Programável (FPSL). Isso desbloqueia um número ilimitado de casos de uso que não estarão disponíveis out-of-the-box — como controles de login simples que distinguem entre contas corporativas e pessoais — e controles mais refinados e específicos por serviço de nuvem, como impedir que os usuários compartilhem arquivos externamente.

* A integração com o Forcepoint DLP requer um SKU adicional separado

Recursos e Benefícios do Forcepoint CASB

FUNCIONALIDADE	BENEFÍCIO
Arquitetura distribuída e de dimensionamento automático na AWS com mais de 300 POPs em todo o mundo.	→ 99,99% de tempo de atividade → Latência mínima: muitas vezes ainda mais rápido do que o acesso direto a aplicativos.
Integração com qualquer IdP compatível com SAML em relay SAML ou modo proxy ACS. IdP integrado opcional usando o Microsoft ADFS.	→ Implantação flexível. → Proteção contra negação de serviço ao usar o modo de retransmissão de SAML.
Agente de sincronização do Active Directory. Sincroniza seus usuários e grupos atuais do AD com usuários e grupos do Forcepoint CASB.	→ Aproveita sua instância existente do Microsoft AD para integrar rapidamente os usuários e manter os grupos aos quais eles são atribuídos.
Controle de acesso contextual com base em grupo de usuários, tipo de dispositivo, localização ou hora do dia, com escalonamento para autenticação multifatores com base em "viagem impossível", localização não autorizada ou dispositivo desconhecido. Camada adicional de controle de acesso para sites ou aplicativos individuais com base no grupo de usuários, tipo de dispositivo ou local.	→ Detecta e bloqueia tentativas de login suspeitas. → Reduz os riscos associados a senhas roubadas. → Segmenta os usuários com base no risco e na necessidade de acesso.
Agente único e unificado para proxy de encaminhamento CASB e ZTNA para aplicativos não web. Inclui suporte para implementação por meio de sistemas MDM e usa certificados autogerados e autogerados com rotação automática.	→ Simplifica a implementação de agentes. → Melhora a segurança. → Reduz a sobrecarga de TI.
Integração com o Forcepoint DLP para aplicar políticas de proteção de dados unificadas em todos os canais — nuvem, rede, endpoints, web e e-mail.*	→ Reduz a complexidade e o tempo para valorizar. → Aumenta a visibilidade e o controle dos dados. → Elimina produtos de segurança redundantes e fragmentados.
DLP e exame de malwares para dados em trânsito. Examina anexos de arquivos baixados ou carregados em qualquer app baseado na web ou site de Internet para identificar malwares ou dados confidenciais, e registra e bloqueia a transferência, conforme apropriado.	→ Impede o vazamento de dados e a propagação de malware em trânsito entre usuários e qualquer aplicativo SaaS corporativo.
Lógica de SASE programável no campo. Monitora, registra e opcionalmente bloqueia qualquer método de solicitação HTTP/S com base em qualquer parte do método de solicitação	→ Controle mais detalhado do uso de aplicativos. → Capacidade de bloquear o upload de dados confidenciais como postagens de mensagens.
Varredura de DLP e malware em busca de dados em repouso em armazenamentos selecionados de IaaS e SaaS. Suporta varredura histórica e OCR de arquivos de imagens e arquivos PDF apenas com imagens.	→ Impede o vazamento de dados e a disseminação de malware em SaaS e IaaS selecionados. → Garante que, mesmo que novos arquivos ou atualizações de arquivos antigos ignorem o proxy reverso, eles possam ser verificados em busca de dados confidenciais.
Criptografia em nível de arquivos de SaaS gerenciado.	→ Garanta a privacidade e a soberania dos dados sem bloquear completamente o acesso aos dados.
Relatórios de shadow IT sem agentes usando logs de firewalls e proxies corporativos.	→ Detecte o uso não autorizado de aplicativos em dispositivos on-prem sem um agente.
Controle do shadow IT usando o agente unificado em modo de proxy forwardado..	→ Impeça que os usuários acessem determinados aplicativos não gerenciados, recomendando o uso de alternativas sancionadas por corporações.
Relatórios detalhados do tráfego SaaS gerenciado.	→ Visibilidade completa do acesso a aplicativos SaaS gerenciados, incluindo aqueles acessados a partir de dispositivos não gerenciados.

* A integração com o Forcepoint DLP e o Risk-Adaptive Protection requer um SKU adicional separado

© 2025 Forcepoint. Forcepoint e o logotipo da FORCEPOINT são marcas comerciais da Forcepoint. Todas as outras marcas registradas usadas neste documento pertencem às respectivas empresas. [FP-CASB-Datasheet-PT] 05Aug2025