Forcepoint

Datasheet

Cloud Access Security Broker

CASB multimodo con proxy inverso sin agente, proxy forward y modos API.

Beneficios clave:

- 99.99% de tiempo de actividad verificado desde 2015
- El escalamiento automático y más de 300 puntos de presencia en AWS minimiza la latencia y maximiza el rendimiento
- DLP de clase empresarial en todos los canales clave - CASB, SWG, correo electrónico y endpoints, con gestión, configuración de políticas e informes unificados
- El agente de sincronización de Active Directory acelera la integración de usuarios
- El análisis de los datos en movimiento bloquea el malware y la exfiltración de datos entre usuarios en cualquier dispositivo y cualquier aplicación de SaaS administrada.
- La lógica de SASE programable en el campo puede bloquear métodos de solicitud de HTTP/S específicos que resultan en un control granular de cualquier elemento en una página web de SaaS administrada
- El escaneo de datos en reposo de SaaS e IaaS seleccionados identifica malware y datos confidenciales independientemente del escaneo de datos en movimiento
- El encriptado a nivel de archivo de aplicaciones SaaS administradas garantiza la privacidad de los datos y la soberanía de los datos sin bloquear completamente el acceso a los datos
- Los informes de Shadow IT ayudan a identificar el riesgo de aplicaciones no autorizadas
- La administración de derechos digitales (DRM) proporciona más flexibilidad con nuevas formas de proteger los datos confidenciales.

Forcepoint Cloud Access Security Broker (CASB) proporciona la visibilidad y el control más amplios sobre el uso de aplicaciones SaaS corporativas autorizadas, incluyendo IA generativa. Protege los datos confidenciales con Data Loss Prevention (DLP) líder de la industria, a la vez que proporciona control de acceso granular y protección contra malware para defenderse contra las amenazas modernas.

Modo de proxy inverso sin agente

El modo de proxy inverso sin agente aplica acceso granular con DLP y escaneo de malware integrado de Forcepoint CASB desde cualquier dispositivo con un navegador moderno. Es ideal para monitorear y controlar el acceso desde dispositivos BYOD y de contratistas. Aprovecha la integración patentada de Forcepoint con cualquier IdP compatible con SAML 2.0 para redirigir a los usuarios a un proxy inverso de Forcepoint, donde se establece una sesión complementaria con la aplicación SaaS.



Figura 1: Forcepoint CASB proxy inverso sin agente con AJAX/VM.

Combinado con la tecnología única de AJAX/VM de Forcepoint, que se ejecuta dentro del navegador del usuario, el modo de proxy inverso sin agente de Forcepoint CASB garantiza la reescritura adecuada de URL y cookies, lo que resulta en compatibilidad con cualquier aplicación SaaS. Las características clave que te permiten controlar y monitorear el uso de aplicaciones en modo de proxy inverso son políticas de proxy, encriptación a nivel de campo, informes de Shadow IT e informes de proxy inverso.

Políticas de proxy

Las opciones de control de acceso y las opciones de DLP y de escaneo de malware asociadas para datos en movimiento hacia y desde aplicaciones SaaS administradas se establecen en políticas de proxy. Esto te permite configurar el acceso a la aplicación SaaS administrada como acceso directo a la aplicación, denegar o proteger el acceso a la aplicación (todo el tráfico pasa por el proxy inverso con la opción de aplicar DLP y escaneo de malware). Los criterios para la implementación de políticas incluyen el grupo de usuarios, el método de acceso (navegador, aplicación cliente que no sea un navegador o cualquiera), el sistema operativo del dispositivo, el perfil del dispositivo y la ubicación.

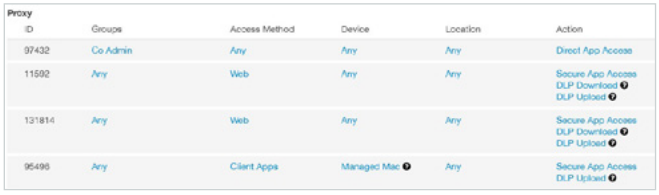


Figura 2: Lista de políticas de proxy para una aplicación de SaaS administrada

Una sola aplicación puede tener una lista de múltiples políticas de proxy que se evalúan secuencialmente hasta que se encuentra una política en la que todos los criterios de coincidencia en la política coinciden con la solicitud de conexión. Luego se aplica la acción de cumplimiento apropiada.

Cuando se especifica el acceso seguro a la aplicación, una única política de proxy puede incluir una lista de políticas de DLP y de escaneo de malware para cargar a la aplicación SaaS, y otra lista para descargar desde la aplicación SaaS. Además, si una aplicación de SaaS administrada tiene el encriptado a nivel de campo habilitado, la política de proxy te permite especificar si un campo se muestra sin encriptar según el nivel de seguridad de campo o si la ubicación del usuario coincide con la ubicación de creación de los datos. Esto respalda la privacidad de los datos y la soberanía de los datos

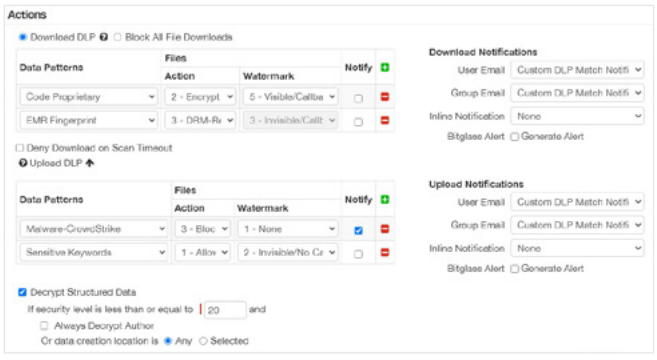


Figura 3: Detalles de la política de proxy para una conexión segura de acceso a aplicaciones

Dentro de una sola política de proxy, las políticas de DLP de descarga te permiten controlar la descarga de datos confidenciales y malware, mientras que las políticas de DLP de carga te permiten controlar la carga de datos confidenciales y malware. Simplemente utiliza los menús desplegables para especificar un patrón de datos para igualar, una acción de archivo y un control de marca de agua/seguimiento, y haz clic en la casilla de verificación si quieres que las personas sean notificadas sobre la coincidencia.

Forcepoint CASB incluye más de 190 patrones de datos predefinidos que te ayudan a aplicar estándares regionales e industriales con respecto a PII, PHI y datos financieros personales. También hay patrones de datos reservados para invocar escaneo de malware impulsado por múltiples motores antimalware de terceros. También puedes crear patrones de datos personalizados que utilizan expresiones regulares simples hasta expresiones booleanas complejas, y patrones de datos especiales para identificar registros. Los patrones de coincidencia especiales incluyen coincidencia de bases de datos (mediante coincidencia exacta), similitud con una forma estándar (mediante fingerprinting de archivos) y cualquier método de solicitud HTTP/S (mediante Field Programmable SASE Logic – FPSL).

Para las políticas de proxy de descarga, las acciones de archivos se cifran, bloquean (reemplaza el contenido con el mensaje de bloqueo), niegan (no transfieren), aplican DRM, y marca de agua y rastrea. Para las políticas de proxy de carga, las acciones de archivos se cifran (para Office 365, Google Workspace y Salesforce), se bloquean (reemplaza el contenido con el mensaje de bloqueo), se niega (no transfiere), se enmascaran datos (Salesforce Chatter, O365 Teams y Slack), se marca de agua y se rastrea.

Encriptación de nivel de campo

El modo de proxy inverso sin agente te permite cifrar datos estructurados en muchas aplicaciones de SaaS populares con soporte para encriptación o tokenización AES de 256 bits, un keystore integrado o tu propio keystore de Key Management Interoperability Protocol (KMIP), y encriptación y tokenización sin bóveda. También puedes especificar niveles de seguridad para cada campo que se controlan cuando el campo se descifra para el usuario.

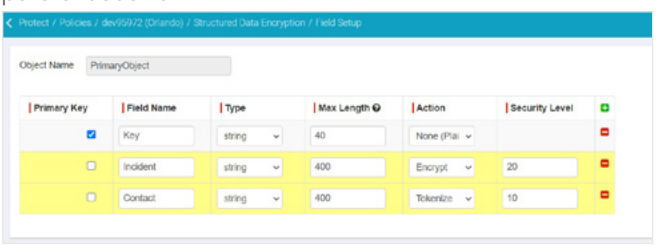


Figura 4: Configuración de encriptación a nivel de campo

Informes de Shadow IT

El modo de proxy inverso sin agente admite la generación de informes de Shadow IT. El uso de Shadow IT se recopila de los datos de registro de firewalls corporativos y servidores proxy, ya sea mediante importación manual o a través de un colector de syslog de Forcepoint. Los informes muestran la distribución de las aplicaciones por calificación de confianza, según lo calculado por Forcepoint, y las aplicaciones a las que se accede con detalle hasta aplicaciones individuales y direcciones IP de origen individuales, lo que te ayuda a comprender la postura de riesgo de tus organizaciones en relación con el tráfico web. Forcepoint CASB también puede permitirte controlar el tráfico de Shadow IT en modo de proxy forward (ver abajo).



Figura 5: Informe de Shadow IT Discovery.

El modo de proxy inverso ofrece informes para brindarte una amplia información sobre el tráfico de SaaS administrado que pasa por el proxy inverso: las secciones de 'Datos en Movimiento' de los paneles de Data Security y de Amenazas, y el informe de registros de proxy. El dashboard de Data Security muestra detalles sobre los datos confidenciales identificados por Forcepoint, incluyendo el movimiento de datos confidenciales dentro y fuera de aplicaciones protegidas por Forcepoint, y también muestra cargas confidenciales a aplicaciones no autorizadas, descargas confidenciales a dispositivos no administrados, grupos y usuarios principales que mueven datos confidenciales, y más.

El dashboard de amenazas incluye los mismos tipos de métricas que el dashboard de Data Security, pero específicamente para malware y amenazas cibernéticas.

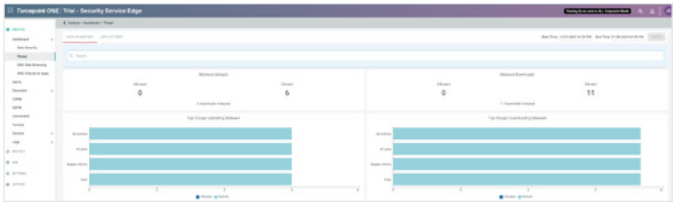


Figura 6: Dashboard de Proxy

El informe de los registros de proxy traza la actividad de las aplicaciones y marca de agua, actividad de DLP y DRM a lo largo del tiempo, y enumera los eventos recientes agrupados por categorías de resumen, auditoría y fuga de datos.

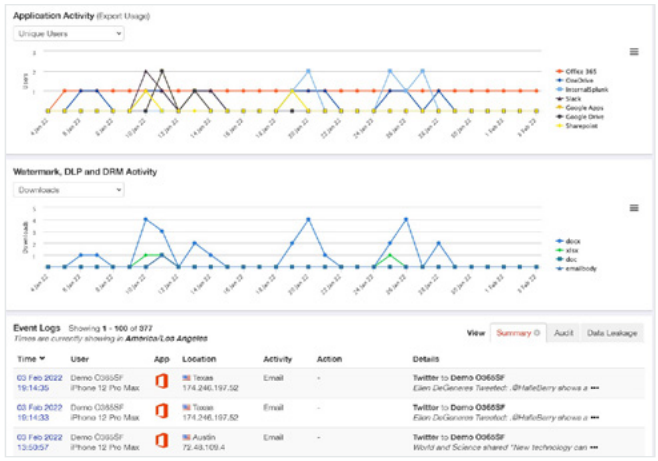


Figure 7: Proxy Logs Report Figura 7: Informe de registros de proxy

Modo de proxy direccional

El modo de proxy de envío utiliza el agente unificado de Forcepoint para Windows o MacOS. Todo el tráfico de SaaS administrado sigue pasando por el proxy inverso de Forcepoint pero sin la necesidad de reescribir URL para conectarse con el dispositivo del usuario. El modo de proxy directo admite todas las características del modo de proxy inverso sin agente, incluida la aplicación de escaneo de DLP y malware a través de políticas de proxy, pero también admite el uso de clientes que no son de navegador, como el cliente de Microsoft Outlook y el cliente de Slack. Además, el modo de proxy directo admite el control de Shadow IT.

Control de Shadow IT

El control de Shadow IT te permite controlar el acceso a cualquier aplicación de Shadow IT mediante políticas de proxy que se evalúan en secuencia como políticas de proxy de SaaS administradas. Sin embargo, las políticas de proxy para aplicaciones de Shadow IT no aplican DLP y escaneo de malware para la carga y descarga. En cambio, se limitan a las siguientes opciones de control de conexión: renderiza la aplicación en modo de solo lectura, entrena (muestra una recomendación para una aplicación alternativa autorizada por la compañía y permite o niega el acceso a la aplicación Shadow IT original), o niega el acceso sin un mensaje de coaching.



Figura 8: Detalles de la política de proxy de Shadow IT que muestran las opciones de coach

Si necesitas respaldar políticas de DLP y de escaneo de malware para shadow aplicaciones de TI, utiliza políticas de contenido de SWG.

Modo API

En modo API, el CASB utiliza llamadas API a tu inquilino de SaaS o IaaS para escanear datos en reposo en busca de datos confidenciales o malware y realizar acciones de remediación automáticas, como restringir el intercambio, poner en cuarentena, copiar, agregar metadatos de clasificación o notificar al propietario del archivo. Soporta el escaneo histórico de archivos y puede aplicar OCR a archivos de imagen y archivos PDF de imagen solo antes de escanear en busca de datos confidenciales. El modo API es compatible con muchos SaaS e IaaS populares, incluyendo Google Workspace, Office 365, Salesforce, ServiceNow, Box, Dropbox, Atlassian Confluence, Github, Webex Teams, Slack, AWS, GCP y Azure.

El modo API garantiza que incluso si archivos nuevos o actualizaciones de archivos antiguos omiten el proxy inverso, puedan ser escaneados en busca de datos confidenciales.

Políticas de API

Las políticas de API controlan el escaneo de datos que reposan en IaaS y SaaS. Al igual que las políticas de proxy, se pueden aplicar varias políticas de API a una sola aplicación SaaS y se evalúan secuencialmente.



Figura 9: Lista de políticas API.

Dentro de una política, puedes especificar criterios de coincidencia según el grupo de usuarios, patrón de datos de DLP, ruta de archivo, nombre de archivo, estado de intercambio (externo, interno, público o cualquier), tamaño de archivo, propietario, compartido con el nombre de usuario, fecha de creación y fecha de modificación. Los patrones de coincidencia de datos utilizados en una política de API pueden ser cualquiera de los patrones de coincidencia personalizados o predefinidos compartidos en las políticas de proxy, lo que te permite tener un control unificado de los datos confidenciales y el malware.

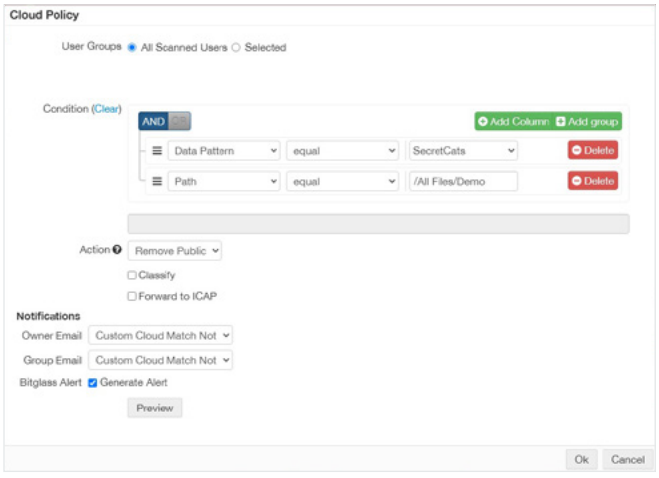


Figura 10: Detalles de la política de API

Cuando se produce una coincidencia de condiciones para un archivo escaneado, las acciones posibles de políticas API incluyen modificar el intercambio (eliminar público, eliminar público y externo, eliminar todo), permitir, poner en cuarentena, crear copia y encriptar.

Integraciones de terceros con CASB

Forcepoint CASB además se puede configurar para integrarse con varios otros sistemas de seguridad de datos como se describe a continuación.

- **Seguridad de la Información y Gestión de Eventos (SIEM).** Forcepoint CASB se integra con cualquier sistema que admita syslog. Esto permite que aplicaciones de terceros carguen registros desde Forcepoint para la visualización y el análisis
- **Sistemas de DLP on-premises.** Forcepoint CASB se integra completamente con Forcepoint DLP, también funciona con cualquier sistema de DLP on-premises que admita el Protocolo de Adaptación de Contenidos de Internet (ICAP). Esto proporciona a los clientes la capacidad de enviar archivos en reposo en almacenamiento en la nube de SaaS o IaaS administrados, que son marcados por Forcepoint como con datos confidenciales, al sistema de DLP on-premises mediante encriptación TLS. Los archivos se enriquecen con datos como el IP de origen y destino y la dirección de correo electrónico del propietario del archivo.
- **Security Orchestration and Response (SOAR).** Forcepoint CASB admite la integración de dos vías entre CASB y las plataformas de SOAR seleccionadas. En estos casos, la plataforma SOAR se utiliza para automatizar actividades dentro de Forcepoint CASB y otra herramienta.
- **Data Classification.** Forcepoint CASB puede utilizar metadatos de clasificación de cualquier clasificador de datos en un patrón de coincidencia de DLP.
- **Administración de endpoint.** Como parte del proceso de inicio de sesión con SAML, Forcepoint CASB puede validar un certificado de cliente almacenado en un dispositivo Windows, Mac, Android o IOS para confirmar que está administrado por un sistema de administración de endpoint. Este conocimiento permite al administrador aplicar diferentes políticas de acceso para los usuarios que inician sesión a través de dispositivos administrados y no administrados.

Diferencia de Forcepoint CASB

- **La más amplia visibilidad de SaaS:** La base de datos más grande conocida de más de 800.000 aplicaciones de SaaS, junto con su calificación de riesgo a través de la evaluación de más de 40 atributos.
- **Seguridad de datos líder en la industria:** Extiende las políticas de Forcepoint DLP a cada canal importante, ya sea tu endpoint, red, nube, web o correo electrónico, para que sus datos estén protegidos, donde sea que residan. La implementación de políticas unificada a través de una única consola, junto con más de 1700 plantillas, políticas y clasificadores predefinidos, ayuda a cumplir con las demandas regulatorias de 90 países y más de 150 regiones.
- **Acceso sin agente para aplicaciones SaaS:** Acceso sin fricción y con Zero Trust a cualquier aplicación desde cualquier dispositivo no administrado a través de la implementación de proxy inverso sin agentes, que protege el acceso desde dispositivos no administrados, incluidos BYOD y dispositivos de socios o contratistas de terceros.
- **Cualquier control de aplicaciones:** Controla cualquier aplicación basada en la web, incluidas aplicaciones inusuales y personalizadas, con controles extensibles mediante Field Programmable SASE Logic (FPSL). Esto desbloquea un número ilimitado de casos de uso que no estarán disponibles desde el principio, desde controles de inicio de sesión simples que distinguen entre cuentas corporativas y cuentas personales, hasta controles más refinados y específicos por servicio en la nube, como evitar que los usuarios compartan archivos externamente.

* La integración con Forcepoint DLP requiere un SKU de complemento separado

Características y Beneficios de Forcepoint CASB

CARACTERÍSTICA	BENEFICIO
Arquitectura distribuida y de auto-escalamiento en AWS con más de 300 POPs en todo el mundo.	→ 99.99% de tiempo de actividad → Latencia mínima: a menudo incluso más rápido que el acceso directo a las aplicaciones.
Integración con cualquier IdP compatible con SAML en modo de relay SAML o proxy ACS. IdP integrado opcional con Microsoft ADFS.	→ Implementación flexible. → Negación de servicio cuando se utiliza el modo de relay de SAML.
Active Directory Sync Agent. Sincroniza tus usuarios y grupos actuales de AD con usuarios y grupos de Forcepoint CASB.	→ Aprovecha tu instancia existente de Microsoft AD para incorporar rápidamente usuarios y mantener los grupos a los que están asignados.
Control de acceso contextual basado en el grupo de usuarios, el tipo de dispositivo, la ubicación o la hora del día, con escalamiento a la autenticación multifactorial basada en un "viaje imposible", una ubicación no autorizada o un dispositivo desconocido. Nivel adicional de control de acceso para sitios web o aplicaciones individuales según el grupo de usuarios, el tipo de dispositivo o la ubicación.	→ Detecta y bloquea intentos de inicio de sesión sospechosos. → Reduce los riesgos asociados con las contraseñas robadas. → Segmenta a los usuarios según el riesgo y la necesidad de acceso.
Un solo agente unificado para CASB forward proxy y ZTNA para aplicaciones que no son web. Incluye soporte para la implementación a través de sistemas de MDM y utiliza certificados autogenerados y auto-rotados.	→ Simplifica la implementación de agentes. → Mejora la seguridad. → Reduce el costo general de TI.
Integración con Forcepoint DLP para aplicar políticas de protección de datos unificadas en todos los canales: la nube, la red, los endpoints, la web y el correo electrónico.*	→ Reduces complexity and time to value. → Aumenta la visibilidad y el control de los datos. → Elimina productos de seguridad redundantes y fragmentados.
DLP y malware escaneo de datos en movimiento. Escanea los archivos adjuntos descargados o cargados en cualquier aplicación o sitio web basado en la web en busca de malware o datos confidenciales y los registra y bloquea la transferencia según corresponda.	→ Detiene la fuga de datos y la propagación de malware en tránsito entre los usuarios y cualquier aplicación SaaS corporativa.
Lógica de SASE programable en campo. Monitorea, registra y opcionalmente bloquea cualquier método de solicitud HTTP/S basado en cualquier parte del método de solicitud	→ Control más preciso del uso de las aplicaciones. → Capacidad para bloquear la carga de datos confidenciales como publicaciones de mensajes..
Escaneo de DLP y malware para datos en reposo en almacenamiento de IaaS y SaaS seleccionado. Soporta escaneo histórico y OCR de archivos de imágenes y archivos PDF de solo imágenes.	→ Detiene la fuga de datos y la propagación de malware en SaaS e IaaS seleccionados. → Garantiza que incluso si archivos nuevos o actualizaciones de archivos antiguos eluden el proxy inverso, puedan ser escaneados en busca de datos confidenciales.
Encriptación a nivel de archivo de SaaS administrado.	→ Garantiza la privacidad de los datos y la soberanía de los datos sin bloquear completamente el acceso a los datos.
Informes de Shadow IT sin agente mediante registros de firewalls y proxies corporativos.	→ Detecta el uso no autorizado de aplicaciones desde dispositivos on-prem sin un agente.
Control de Shadow IT mediante el agente unificado en modo de proxy forward.	→ Evita que los usuarios accedan a ciertas aplicaciones no administradas mientras recomiendas el uso de alternativas con aprobación corporativa.
Informes detallados del tráfico de SaaS administrado.	→ Visibilidad completa del acceso a aplicaciones de SaaS administradas, incluidas las a las que se accede desde dispositivos no administrados.

* La integración con Forcepoint DLP y Risk-Adaptive Protection requiere un SKU adicional separado

© 2025 Forcepoint. Forcepoint y el logotipo de FORCEPOINT son marcas comerciales de Forcepoint. Todas las demas marcas comerciales utilizadas en este documento son propiedad de sus respectivos duenos. [FP-CASB-Datasheet-ES] 05Aug2025