FORCEPOINT
POWERED BY Raytheon

Datasheet

Forcepoint CASB

El agente de seguridad de acceso a la nube (*Cloud Access Security Broker*, CASB) Forcepoint CASB detecta automáticamente el uso de aplicaciones en la nube, analiza los riesgos y aplica los controles apropiados para aplicaciones de producción y de Seguridad como Servicio (SaaS). Con Forcepoint CASB, los usuarios obtienen las aplicaciones que desean y el personal de TI obtiene el control que necesita.

VISIBILIDAD Y CONTROL DEL USO DE APLICACIONES EN LA NUBE

Las aplicaciones en la nube les permiten a las organizaciones reducir costos y asignar recursos con elasticidad, pero también presentan riesgos para la postura de seguridad y cumplimiento. La aceleración de la adopción de aplicaciones en la nube en el lugar de trabajo, junto con la proliferación de la política "Trae tu propio dispositivo" (*Bring Your Own Device*, BYOD), ha creado la necesidad de brindar protección a aplicaciones sancionadas basadas en la nube como Office 365, Dropbox y Salesforce. La prevención contra la pérdida de datos y la aplicación de controles granulares de acceso son justificadamente una prioridad para TI.

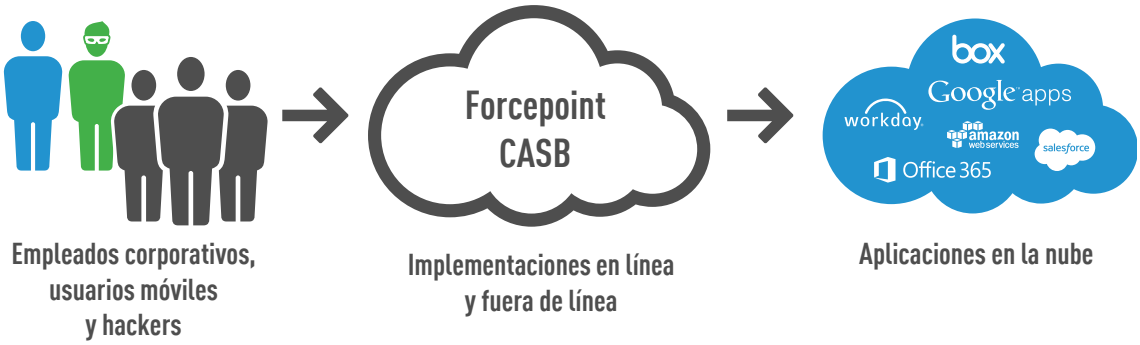
Los empleados pueden ser una fuente importante de riesgo a la seguridad, ya que los empleados con malas intenciones buscan aprovecharse del acceso sin restricción a las aplicaciones en la nube de una organización para exfiltrar información.

Forcepoint garantiza el uso seguro y productivo de las aplicaciones en la nube entre todos los usuarios y dispositivos finales.

Para tener visibilidad y control se necesita un agente de seguridad de acceso a la nube que proporcione detección de aplicaciones, gobierno de riesgos, control del acceso y protección de datos para aplicaciones sancionadas y también no sancionadas.

MITIGACIÓN DE RIESGOS EN LAS APLICACIONES EN LA NUBE

Típicamente, las organizaciones requieren visibilidad del acceso a la nube antes de aplicar políticas para eliminar o limitar el riesgo. Por eso es importante disponer de un conjunto de funciones fuera de línea que puedan ayudarlo a identificar y evaluar su postura en materia de riesgos. Una vez que haya investigado el panorama de amenazas y creado las políticas requeridas para atender los riesgos a la seguridad, puede desactivar estas funciones fuera de línea y transformarlas en funciones en línea para aplicar esas políticas. Gartner recomienda soluciones que ofrecen "lo mejor de ambos mundos" (esto es, una combinación de proxys y API) para cubrir todos los casos de uso de seguridad en la nube para las organizaciones modernas.



El agente de seguridad de acceso a la nube de Forcepoint proporciona visibilidad y control de aplicaciones en la nube sancionadas y no sancionadas.

CARACTERÍSTICAS Y BENEFICIOS

- Parte de la familia de productos de seguridad para la nube de Forcepoint se pueden implementar ambientes tanto en las instalaciones como en la nube.
- Funciones integrales de detección de aplicaciones, gestión, análisis y protección en una solución integrada.
- Opciones de implementación fuera de línea (modo API) y/o en línea (modo proxy).
- Las políticas granulares para dispositivos móviles y dispositivos finales permiten el control del acceso y la protección de los datos para teléfonos móviles, tabletas y computadoras portátiles administrados y no administrados.
- Integración incorporada con directorios empresariales, SIEM y MDM.
- Soporte para Office 365, AWS, Salesforce, Google Apps, Box, Dropbox, NetSuite, Workday, Microsoft Azure y más.
- Interoperabilidad certificada con socios de Identidad-como-Servicio: Centrify, Ping, Okta, OneLogin, SecureAuth y Microsoft.
- Extiende a las aplicaciones en la nube las funcionalidades de detección de anomalías y amenazas de una organización.
- Los datos de reputación de IP permiten la creación y la aplicación de políticas más precisas de mitigación de riesgos.

DETECCIÓN Y GESTIÓN EN LA NUBE

Forcepoint CASB extiende la información tradicional de detección de aplicaciones en la nube al brindar detalles de factores de riesgo que son únicos y específicos de su organización. Por ejemplo, Forcepoint CASB proporciona visibilidad de cuentas latentes (esto es, inactivas), cuentas huérfanas (p. ej., exempleados) y cuentas externas (p. ej., contratistas) que presentan diversos riesgos a la seguridad.

Además, Forcepoint compara las configuraciones de seguridad para aplicaciones en la nube de su organización con las mejores prácticas y requisitos reguladores de la industria, para que usted pueda detectar con más facilidad sus brechas de seguridad y cumplimiento y tome medidas para remediarlas.

Todas las funciones de detección y gestión en la nube se realizan a través de las API de proveedores de aplicaciones en la nube, un proceso fuera de línea que no es intrusivo y no requiere el envío de ningún agente, cambio de aplicaciones o registro fuera de su organización a Forcepoint.

AUDITORÍA Y PROTECCIÓN EN LA NUBE

La función de auditoría y protección en la nube de Forcepoint CASB le proporciona la inteligencia operativa y las herramientas que necesita para proteger los datos en la nube y aplicar controles integrales de acceso de los usuarios. Forcepoint proporciona información esencial e inteligencia sobre:

- **Prevención contra la pérdida de datos para aquellos datos que están en reposo y datos en tránsito:** Controles para datos sensibles y regulados en la nube.
- **Monitoreo de usuarios:** Monitoreo y elaboración de informes en tiempo real sobre la actividad de usuarios finales y administradores.
- **Prevención contra las amenazas cibernéticas:** Aplicación de políticas para alertas, bloqueo o solicitud de verificación de identidad para cualquier actividad sospechosa.

Forcepoint CASB monitorea y controla cargas, descargas e intercambio de datos sensibles basado en diversos criterios, como destino, usuario o aplicación en la nube. Además, escanea sus datos corporativos almacenados en servicios de sincronización de archivos como OneDrive y Box, y destaca los archivos que son sensibles o están regulados para que usted pueda aplicar la política apropiada (p. ej., enviar un alerta) para mitigar el riesgo.

Forcepoint CASB inspecciona archivos y contenido en tiempo real para garantizar que su información de identificación personal (PII), PCI, HIPAA y otra información sensible se mantenga protegida. Los administradores pueden elegir poner archivos en cuarentena, eliminar los archivos sensibles del repositorio en la nube y notificar a usuarios finales. También se puede agregar una copia del archivo a una carpeta confiable para una posterior revisión. Forcepoint CASB ofrece prevención contra la pérdida de datos (DLP) incorporada o integración estándar basada en ICAP con soluciones de DLP líderes para que usted pueda aprovechar las políticas de protección de datos existentes.

Forcepoint CASB detecta y bloquea en forma automática las amenazas a las aplicaciones en la nube y aplica políticas de mitigación de riesgo. A través de técnicas de impresión digital únicas, Forcepoint CASB establece rápidamente perfiles de comportamiento detallados basados en patrones de uso normal para cada usuario, departamento y dispositivo. Todo acceso que no pase la prueba de impresión digital puede ser configurado para que de inmediato se emita un alerta, se realice un bloqueo o se solicite autenticación de dos factores en tiempo real. También se pueden crear rápidamente políticas personalizadas y emplearlas en aplicaciones seleccionadas en la nube.

Forcepoint CASB le permite bloquear o restringir el acceso a aplicaciones en la nube desde dispositivos finales no administrados (p. ej., dispositivos BYOD o dispositivos de propiedad personal), lo que presenta una alternativa rentable al enrutamiento de todos los accesos remotos a través de una red privada virtual (VPN). Además, Forcepoint CASB posee adaptadores incorporados que facilitan la integración con directorios empresariales y soluciones SIEM líderes del mercado.

FORCEPOINT CASB: COMPARACIÓN DE CARACTERÍSTICAS DE PRODUCTOS

		PRODUCTOS FORCEPOINT		
GRUPO DE CARACTERÍSTICAS	**DESCRIPCIÓN DE LA CARACTERÍSTICA**	**GESTIÓN EN LA NUBE**	**AUDITORÍA Y PROTECCIÓN EN LA NUBE**	**PAQUETE DE SEGURIDAD PARA LA NUBE**
Visibilidad de aplicaciones y evaluación de riesgos (disponible en implementaciones fuera de línea/API)	DETECCIÓN DE APLICACIONES EN LA NUBE: Aprovecha los archivos de registro existentes para automatizar la detección y categorización de las aplicaciones utilizadas en la nube.	●		●
	CLASIFICACIÓN DE RIESGOS DE APLICACIONES EN LA NUBE: Califica el riesgo general para cada aplicación en la nube basado en certificaciones y mejores prácticas reguladoras y de la industria.	●		●
	RESUMEN DE USO DE APLICACIONES EN LA NUBE: Incluye la cantidad de usuarios, actividades, volumen de tráfico y horario de uso típico de cada aplicación en la nube.	●		●
	INDICADORES DE RIESGO AVANZADOS: Indicadores detallados de la postura en materia de riesgos de las aplicaciones en la nube e información de cada aplicación.	●		●
	INDICADORES DE RIESGO PERSONALIZADOS: Indicadores detallados de la postura en materia de riesgos de las aplicaciones en la nube con ponderaciones personalizadas.	●		●
	DETECCIÓN CONTINUA: Programa el escaneo automático de archivos de registro y la generación de informes de detección en forma periódica.	●		●
	PANEL DE DETECCIÓN CENTRALIZADO: Resultados de detección, uso actual comparado con actividad anterior y tendencias de uso, todo integrado.	●		●
	INTEGRACIÓN CON SIEM: Genera datos de detección en formato de evento común para la integración con entornos SIEM existentes.	●		●
	ACTUALIZACIONES DE RIESGOS Y CATÁLOGO DE APLICACIONES: Actualizaciones automáticas del catálogo de aplicaciones en la nube y cambios en las propiedades de riesgos a medida que están disponibles.	●		●
	RECOPILACIÓN DE REGISTROS DE ACTIVIDADES: Recopila registros de actividades básicas de usuarios y usuarios con privilegios a través de API de aplicaciones en la nube.	●		●
Gestión de cuentas y datos (disponible en implementaciones fuera de línea/API)	CLASIFICACIÓN DE DATOS: Categoriza e identifica datos sensibles o regulados, incluidos permisos de intercambio para cada archivo, almacenados en servicios de sincronización de archivos para garantizar el cumplimiento de regulaciones tales como PCI, SOX e HIPAA.	●		●
	GESTIÓN DE USUARIOS: Identifica cuentas latentes (esto es, inactivas), cuentas huérfanas (p. ej., exempleados) y usuarios externos (p. ej., contratistas) para reducir los costos operativos y minimizar las amenazas a la seguridad asociadas.	●		●
	GESTIÓN DE APLICACIONES: Compara sus configuraciones de seguridad para las aplicaciones en la nube con un conjunto de mejores prácticas y requisitos reguladores de la industria (p. ej., PCI DSS, NIST, HIPAA, CJIS, MAS, ISO) para identificar brechas de seguridad y cumplimiento.	●		●
	FLUJO DE TRABAJO DE RECUPERACIÓN INTEGRADO: Aprovecha un flujo de trabajo organizacional incorporado para asignar y realizar tareas de mitigación de riesgo a través de Forcepoint CASB o de la integración con sistemas de emisión de tickets de terceros.	●		●
Monitoreo y análisis de actividades en tiempo real (disponible en implementaciones en línea/proxy)	MONITOREO Y ANÁLISIS DE ACTIVIDADES: Monitoreo y análisis de actividades en tiempo real por usuario, grupo, ubicación, dispositivo, acción en la aplicación y más.		●	●
	MONITOREO DE USUARIOS CON PRIVILEGIOS: Monitoreo y elaboración de informes en tiempo real de las actividades de usuarios con privilegios y administradores.		●	●
	INTEGRACIÓN CON SIEM EMPRESARIAL: Adaptadores que proveen registros de actividad directamente a las principales soluciones SIEM, que incluyen ArcSight, Splunk y Q1 Labs.		●	●
	INTEGRACIÓN CON DIRECTORIOS EMPRESARIALES: Utiliza la infraestructura existente de directorios AD o LDAP para elaboración de informes y políticas para la organización, usuarios y grupos.		●	●
	ADMINISTRACIÓN BASADA EN ROLES: Define los permisos de administrador para editar recursos, políticas y configuraciones del sistema.		●	●
	ELABORACIÓN DE INFORMES EMPRESARIALES: Opciones flexibles de elaboración de informes, que incluyen informes predefinidos con capacidad para editar y guardar informes personalizados.		●	●

PRODUCTOS FORCEPOINT

GRUPO DE CARACTERÍSTICAS	DESCRIPCIÓN DE LA CARACTERÍSTICA	GESTIÓN EN LA NUBE	AUDITORÍA Y PROTECCIÓN EN LA NUBE	PAQUETE DE SEGURIDAD PARA LA NUBE
Gestión de cuentas y datos (disponible en implementaciones fuera de línea/API)	DETECCIÓN AUTOMÁTICA DE ANOMALÍAS: Monitorea continuamente las conductas y detecta actividades anómalas, que incluyen empleados de alto riesgo y ataques externos.		●	●
	PREVENCIÓN CONTRA AMENAZAS EN TIEMPO REAL: Correlaciona anomalías en actividades con direcciones IP riesgosas.[1] Aplica políticas para alertar, bloquear, poner en cuarentena o solicitar verificación de identidad para cualquier aplicación o acción específica dentro de una aplicación.		●	●
	PREVENCIÓN CONTRA LA FUGA DE DATOS: Clasificación de datos en reposo e inspección de contenido en tiempo real para más de 100 tipos de archivos y cientos de tipos de datos predefinidos que reúnen los requisitos de diversas regulaciones (p. ej., PCI, PII, PHI, HIPAA, SOX).		●	●
	AUTENTICACIÓN DE MÚLTIPLES FACTORES: Verificación de identidad basada en riesgos (p. ej., contraseña única enviada al dispositivo móvil de un usuario) cuando se detectan actividades anómalas o de alto riesgo.		●	●
	IDENTIFICACIÓN ÚNICA: Aprovecha la identificación única (SSO) incorporada o una solución de terceros para acceder a aplicaciones basadas en SAML.		●	●
	ALERTAS DINÁMICAS: Reciba notificaciones en tiempo real sobre violaciones de políticas o límites de actividad a través de un mensaje SMS/de correo electrónico.		●	●
	CONTROL DEL ACCESO DESDE DISPOSITIVOS MÓVILES Y DISPOSITIVOS FINALES: Permite políticas únicas para dispositivos administrados y no administrados, ya sea que se origen en navegadores o en aplicaciones móviles.		●	●
	CONTROLES DE ACCESO BASADOS EN LA UBICACIÓN: Restringe el acceso según la ubicación del usuario o la ubicación del servicio en la nube.		●	●
	INTEGRACIÓN CON MDM: Aprovecha la implementación MDM existente para administrar la inscripción de dispositivos finales y el acceso a la nube.		●	●
	POLÍTICAS PERSONALIZADAS: El editor visual de políticas permite la fácil configuración de políticas personalizadas basadas en diversos atributos.		●	●
Arquitectura avanzada en la nube	OPTIMIZACIÓN DEL DESEMPEÑO: Acelera el acceso a aplicaciones en la nube a través de funciones de almacenamiento en caché y optimización de contenido de una red de entrega de contenido de clase mundial con más de 30 centros de datos en todo el mundo.		●	●
	INTELIGENCIA CENTRALIZADA SOBRE AMENAZAS: Visión unificada de anomalías y amenazas de tablas de bases de datos de empresas, archivos almacenados en intercambios de archivos y datos almacenados en aplicaciones en la nube.		●	●

[1] Complemento opcional de la licencia de Forcepoint CASB; se adquiere por separado.

CONTACTO

www.forcepoint.com/contact

ACERCA DE FORCEPOINT

[DATASHEET_FORCEPOINT_CASB_ES]-100055.022217.