Forcepoint Data Loss Prevention

Protección de datos en un mundo sin perímetros

Forcepoint

Folleto

forcepoint.com/es

Forcepoint Data Loss Protection (DLP)

Seguridad de datos donde quiera que su personal trabaje y sus datos residan

En la actualidad, la seguridad de datos es un problema importante para las organizaciones de todos los tipos y tamaños. Por un lado, se requiere que las organizaciones de TI estén al día con las regulaciones y protejan la información de identificación personal (PII), la información de salud protegida (PHI) y otros tipos de información regulada de ataques maliciosos dirigidos, así como de la pérdida de datos accidental. Y por el otro, deben adaptarse a los movimientos de TI macro, como la adopción de aplicaciones en la nube, los entornos en la nube híbridos y las tendencias de "traiga su propio dispositivo" (BYOD). Todo esto multiplica las maneras en que los datos salen de su organización.

Esta superficie de ataque en expansión supone el desafío más significativo para proteger datos críticos. Los equipos de seguridad de datos deben tener en cuenta la explosión del movimiento de datos desde "dentro" de la organización a todos los lugares y canales donde los datos ahora residen y se trasladan. Se debe ganar visibilidad de todos los datos en la nube y en las instalaciones. Los equipos de seguridad de datos también deben contar con visibilidad y control de todos los canales (endpoints, tráfico web, redes, correo electrónico, aplicaciones en la nube y aplicaciones privadas) con un único punto de administración.

Forcepoint DLP es la solución en la que más confía la industria, brindándole las herramientas que necesita para administrar fácilmente políticas globales en todos los canales importantes, ya sea que se trate de endpoints, redes, la nube, la web, aplicaciones privadas o correo electrónico. Podemos simplificar su trabajo con los clasificadores, las políticas y plantillas más predefinidos que cualquier otro proveedor de DLP de la industria. Esto puede agilizar dramáticamente su gestión de incidentes de modo que pueda enfocarse en lo que más importa: eliminar el riesgo para que su personal pueda ser cada vez más productivo. Forcepoint DLP aborda el riesgo brindándole visibilidad y control donde quiera que su personal trabaje y sus datos residan.

La protección de datos debe:

- **Proteger los datos regulados** mediante un unico punto de control para todas las aplicaciones que su personal utiliza para crear, almacenar y mover datos.
- **Proteja los datos confidenciales** con DLP avanzado que analiza la manera en la que las personas usan los datos, asesora a su personal para que tomen buenas decisiones respecto de la información y prioriza los incidentes según el riesgo.

Visibilidad y control donde quiera que su personal trabaje y sus datos residan

- **Aplicaciones personalizadas**
- **Cloud Applications**
- **Aplicaciones privadas**
- **Endpoint**
- **Network**
- **Discovery**
- **Web**
- **Email**

Acelere el cumplimiento

Empodere a su personal para que proteja los datos

Detección y control avanzados

Responda y corrija riesgos

Acelere el cumplimiento

El entorno de TI moderno presenta un gran desafio a las empresas que apuntan a cumplir con decenas de regulaciones de seguridad de datos a nivel mundial, en especial mientras migran a aplicaciones en la nube y fuerzas de trabajo moviles. Muchas soluciones de seguridad ofrecen alguna forma de DLP integrado, como el que se encuentra dentro de aplicaciones en la nube.

Sin embargo, los equipos de seguridad enfrentan una complejidad no deseada y costos adicionales al implementar y administrar políticas individuales e incongruentes entre distintos endpoints, aplicaciones en la nube y redes. Forcepoint DLP acelera sus esfuerzos de compliance brindándoles más de 1600 clasificadores, políticas y plantillas predefinidos. Esto agiliza el despliegue inicial de DLP y simplifica la administración continua de DLP. Forcepoint DLP protege de manera eficiente la información confidencial de los clientes y datos regulados para que puedan probar su cumplimiento constante con confianza.

- → **Regule la cobertura** para alcanzar y mantener fácilmente el cumplimiento de más de 1600 clasificadores, políticas y plantillas predefinidos aplicables a las exigencias regulatorias de 83 países en más de 150 regiones.
- → **Localice y corrija** datos regulados con detección en sus redes, la nube y los dispositivos finales.
- → **Control centralizado** y politicas uniformes en todo el entorno de TI.

Empodere a su personal para que proteja los datos

DEI DLP solo con controles preventivos frustra a los usuarios que los eludiran con la unica intencion de completar una tarea. Eludir la seguridad conduce a riesgos innecesarios y a la exposicion de datos involuntaria.

Forcepoint DLP reconoce a su personal como la linea de defensa ante las amenazas ciberneticas en la actualidad.

- → **Detección y control de dato** en donde sea que residan, ya sea en la nube o en la red, se envien por correo electronico o se encuentren en un dispositivo final.
- → **Asesore a sus empleados** para que tomen decisiones inteligentes, mediante mensajes que guien las acciones de los usuarios; eduque a los empleados sobre las politicas y valide las intenciones de los usuarios cuando interactuan con datos criticos.
- → **Colabore de manera segura** con socios confiables utilizando autoencriptacion basada en politicas que proteja los datos cuando salen de su organizacion.
- → **Automatice el etiquetado y la clasificación de datos** mediante la integración en Forcepoint Data Classification y Microsoft Purview Information Protection.

Detección y controles avanzados que monitorean a los datos

Las fugas de datos accidentales y maliciosas son incidentes complejos, no eventos aislados. Forrester, Gartner, Radicati Group y Frost & Sullivan reconocen a Forcepoint DLP como líder en la industria en soluciones de DLP. Una de las características clave es la capacidad de Forcepoint DLP de identificar los datos en reposo, en movimiento y en uso. La identificación de datos clave incluye lo siguiente:

- → **Reconocimiento Óptico de Caracteres (OCR)** que identifica datos integrados en imagenes cuando estan en movimiento o inactivos.
- → **Identificación robusta** de informacion de identificacion personal (PII) que ofrece verificaciones de validacion de datos, deteccion de nombres reales, analisis de proximidad e identificadores de contexto.
- → **Identificación de encriptación personalizada** que expone datos ocultos para evitar su deteccion y los controles aplicables.
- → **Análisis acumulativo** para deteccion de DLP por goteo (es decir,datos que se fugan lentamente a lo largo del tiempo).
- → **Integración en Forcepoint Data Classification,** sacando provecho de modelos de IA/AA altamente entrenados a fin de ofrecer una clasificación muy precisa para los datos en uso.

- → **Aprendizaje automatizado** que permite a los usuarios entrenar al sistema para identificar datos relevantes, nunca antes vistos. Los usuarios brindan al motor ejemplos positivos y negativos para senalar documentos comerciales, codigo fuente, etc. similares.
- → **ocalización (fingerprinting)** de datos estructurados (como bases de datos) y no estructurados (como documentos) que permite a los propietarios de los datos definir tipos de datos e identificar coincidencias parciales y totales entre documentos comerciales, planes de diseno y bases de datos, y luego aplicar la politica o el control adecuado para esos datos.
- → **Análisis** para identificar cambios en el comportamiento de los usuarios en lo que respecta a la interaccion con los datos, como un aumento en el uso del correo electronico personal. Con la proteccion de datos dinamicos (DDP), Forcepoint DLP se vuelve todavia mas efectivo al sacar provecho del analisis conductual del riesgo de los usuarios, que luego se utiliza para implementar politicas adaptables al riesgo. Esto le permite a los equipos de seguridad implementar politicas dinamicas e individualizadas en lugar de estaticas y globales.

Identifique, administre y corrija el riesgo de la protección de datos

Los enfoques tradicionales respecto de la DLP sobrecargan a los usuarios con falsos positivos a la vez que pasan por alto datos en riesgo.

Ademas de reducir la eficacia de los equipos de seguridad, esto hace que los empleados o usuarios finales se frustren y vean a las soluciones de seguridad como un impedimento para su productividad laboral. Al utilizar el analisis, Forcepoint DLP reduce los falsos positivos, lo que optimiza las operaciones de seguridad. Para aumentar la concientizacion sobre la seguridad en los empleados, DLP permite el asesoramiento de empleados y la integracion con soluciones de clasificacion de datos.

- → **Enfoque a los equipos de respuesta** en el riesgo mas grande con incidentes priorizados que destacan a las personas responsables del riesgo, los datos criticos en riesgo, y los patrones de comportamiento comunes a distintos usuarios.
- → **Aumento de la concientización de los empleados** respecto del manejo de datos confidenciales y propiedad intelectual con asesoramiento para para Windows y macOS, además de ofrecerles integración de soluciones de clasificación como Forcepoint Data Classification y Microsoft Purview Information Protection.
- → **Implemente capacidades de identificación de datos con DLP de avanzada**, como localizacion (fingerprinting), en dispositivos finales de trabajo remoto y en aplicaciones en la nube empresariales.
- → **Brinde a los propietarios de datos y gerentes empresariales** un flujo de trabajo de incidentes distribuido por correo electronico para su revision y respuesta ante incidentes de DLP.
- → **Resguarde la privacidad de los usuarios** con opciones de anonimidad y controles de acceso.
- → **Agregue el contexto de los datos** en analisis de usuarios mas exhaustivos mediante integraciones profundas con Forcepoint Insider Threat y el analisis conductual de Forcepoint Behavioral Analytics.

Visibilidad en donde sea que trabaje su personal; control en donde sea que residan sus datos

Las empresas de hoy se enfrentan a entornos complejos, en los que los datos están en todas partes, y requieren protección de datos en ubicaciones que no son administradas por la empresa ni pertenecen a ella. Forcepoint ONE CASB, SWG y ZTNA amplían el análisis y las políticas de DLP a aplicaciones en la nube críticas, tráfico web y aplicaciones privadas basadas en la nube de modo que los datos estén protegidos, sin importar en dónde residan. Las REST API como API de seguridad de datos de Forcepoint DLP aportan visibilidad y aplicación de DLP a aplicaciones internas desarrolladas a medida.

- → **Oriente a los equipos de respuesta para identificar y proteger** datos en aplicaciones en la nube, almacenamiento de datos de su red, bases de datos y endpoints administrados y no administrados.
- → **Identifique y prevenga automáticamente** cuando se comparten datos confidenciales con usuarios externos o usuarios internos no autorizados.
- → **Proteja los datos** en tiempo real para cargas y descargas de datos de aplicaciones criticas en la nube, como Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack y muchas mas.
- → **Unifique la aplicación de políticas** a traves de una unica consola para definir y aplicar datos en movimiento y politicas de deteccion de datos en todos los canales: la nube, la red y los dispositivos finales.
- → **Implemente una solución alojada por Forcepoint** que amplie las funciones de la politica de DLP, incluso la localizacion (fingerprinting) y el aprendizaje automatizado, a aplicaciones en la nube, al mismo tiempo que cuenta con la opcion de mantener los datos forenses y de incidentes dentro de su central de datos.
- → **Vea incidentes y administre en herramientas de terceros** a través de REST API expuestas. Automatice los flujos de trabajo de administración de incidentes y apoye los procesos empresariales que dependen de incidentes de DLP mediante herramientas de automatización y servicio como ServiceNow, Nagios y Tableau, así como soluciones SIEM y SOAR, como Splunk y XSOAR.Forcepoint DLP incluye plantillas de politicas regulatorias y analisis avanzado desde un unico punto de control con cada implementacion.

Las empresas eligen las opciones de implementacion adecuadas para su entorno de TI.

Apéndice A: Descripción general de los componentes de la solución de DLP

Forcepoint DLP Endpoint	Forcepoint DLP – Endpoint protege sus datos confidenciales en dispositivos finales Windows y Mac dentro y fuera de la red corporativa. Incluye control y proteccion avanzada de datos inactivos (deteccion), en movimiento y en uso. Se integra con Microsoft Azure Information Protection para analizar datos encriptados y aplicar los controles de DLP correspondientes. Permite la autocorreccion del riesgo de datos por parte de empleados basandose en mensajes de asesoramiento de DLP. La solucion monitorea las cargas en la web, incluidos los HTTPS, asi como las cargas en servicios en la nube como Office 365 y Box Enterprise. Integracion total con Outlook, Notes y clientes de correo electronico.
Forcepoint ONE CASB	Impulsado por Forcepoint ONE CASB, amplíe el control único y análisis avanzado de Forcepoint DLP a aplicaciones sancionadas en la nube, como Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack y muchas más. Obtenga el control continuo de datos esenciales para la empresa, sin importar dónde estén o qué dispositivos utilicen los usuarios.
Forcepoint ONE SWG	Forcepoint ONE SWG le permite acceder de manera segura a cualquier sitio web y descargar cualquier documento mientras obtiene el rendimiento web de alta velocidad con el que su equipo cuenta. Integración de aislamiento remoto del navegador (RBI) para una representación de contenedor seguro de sitios riesgosos, y desarme y reconstrucción de contenido (CDR) de Zero Trust para la limpieza completa de todos los documentos descargables.
Forcepoint ONE ZTNA (disponible la segunda mitad de 2023)	Forcepoint ONE ZTNA lleva el acceso remoto de Zero Trust simple, seguro y escalable a aplicaciones en la nube privadas e internas sin la necesidad de contar con VPN en dispositivos administrados y no administrados.
Forcepoint DLP —Discover	Forcepoint DLP – Discovery identifica y protege datos confidenciales de distintos servidores de datos, SharePoint (en las instalaciones y en la nube), Exchange (en las instalaciones y en la nube), y brinda capacidades de deteccion dentro de bases de datos como SQL Server y Oracle. La tecnologia de localizacion (fingerprinting) identifica los datos regulados y la propiedad intelectual inactivos, y protege esos datos al aplicar la encriptacion y los controles correspondientes. Discovery tambien incluye reconocimiento de caracteres opticos (OCR) que brinda visibilidad a datos en imagenes.
Forcepoint DLP —Network	Forcepoint DLP – Network proporciona el punto de aplicacion critico para detener el robo de datos en movimiento que se produce a traves del correo electronico y la web. La solucion ayuda a identificar y prevenir la exfiltracion de datos y la perdida accidental de datos causada por ataques externos o producida como resultado de la amenaza interna. El reconocimiento de caracteres opticos (OCR) reconoce datos dentro de imagenes. El analisis identifica la DLP para detener el robo de datos con un registro por vez y otros comportamientos de usuarios de alto riesgo.
Forcepoint DLP for Cloud Email	Forcepoint DLP for Cloud Email detiene las exfiltraciones no deseadas de sus datos e IP a través de correo electrónico saliente. Puede combinarlo con otras soluciones de canales de Forcepoint DLP como Endpoint, Network, Cloud y Web a fin de simplificar su administración de DLP, escribiendo una política y desplegándola en múltiples canales. A diferencia de las soluciones no diseñadas para la nube, Forcepoint DLP for Cloud Email posibilita un potencial de escalabilidad enorme desde explosiones imprevistas de tráfico de correo electrónico. También permite que el tráfico de correo electrónico saliente crezca a la par de su empresa sin tener que configurar y administrar recursos de hardware adicionales.
API Forcepoint DLP App Data Security	La API de Forcepoint DLP App Data Security facilita que las organizaciones protejan los datos en sus aplicaciones y servicios personalizados internos. Permite el análisis del tráfico de archivos y datos, y aplica acciones de DLP como permitir, bloquear y solicitar confirmación con una ventana emergente personalizada, cifrar, dejar de compartir y poner en cuarentena. Es una REST API que es fácil de entender y simple de usar sin haber llevado una capacitación extensa o tener conocimiento de protocolos complejos. También es independiente del lenguaje, lo que permite el desarrollo y el consumo en cualquier lenguaje o plataforma de programación.

Apéndice B: Descripción general de los componentes de la solución de DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP— DISCOVER	FORCEPOINT DLP— NETWORK	FORCEPOINT DLP FOR CLOUD	FORCEPOINT ONE SWG	FORCEPOINT ONE ZTNA: API FORCEPOINT DLP APP DATA SECURITY	FORCEPOINT ONE ZTNA (PRÓXIMAMENTE, SEGUNDO SEMESTRE DE 2023)
¿Cuál es la función principal?	Detección de datos y aplicación de políticas de protección de datos en los endpoints de los usuarios a través de canales de medios extraíbles, impresiones, la web, aplicaciones, entre otros.	Detectar datos y aplicar politicas en la nube o mediante aplicaciones en la nube	Detectar, escanear y corregir datos inactivos dentro de centrales de datos y otros entornos en las instalaciones	Brindar visibilidad y control a datos en movimiento a través de la web o el correo electrónico web dentro de la red	Brindar visibilidad y control a datos en movimiento a través de la web o el correo electrónico web dentro de la red	Brindar visibilidad y control a datos en movimiento a través del correo electrónico saliente	Visibilidad y control de los datos en aplicaciones y servicios personalizados internos	Brindar visibilidad y aplicación de políticas de protección de datos para los datos en movimiento (cargas y descargas) dentro de una aplicación privada corporativa
¿Dónde están los datos inactivos detectados/ protegidos?	Puntos finales de Windows, MacOS	OneDrive, Sharepoint Online, Exchange Online, Google Drive, Box, DropBox, Salesforce, ServiceNow	En las instalaciones en servidores de archivos y almacenamiento de redes, servidor Sharepoint, servidor Exchange, bases de datos como Microsoft SQL Server, Oracle e IBM DB2					
¿Dónde están los datos en movimiento protegidos?	Correo electronico, web: HTTP(S), impresoras, medios extraibles, servidores de archivos/NAS	Cargas, descargas e intercambio de archivos para Office 365, Google Apps, Salesforce.com, Box, Dropbox y ServiceNow vía API y TODAS las aplicaciones principales vía proxy		Correo electrónico, impresoras, web: HTTP(S) vía ICAP	Correo electrónico	HTTP(S)	Aplicaciones personalizadas internas y servicios personalizados	Cargas y descargas vía ZTNA Connector a aplicaciones privadas
¿Dónde están los datos en uso protegidos?	Zoom, Webex, Google Hangouts, IM, archivos compartidos mediante VOIP, intercambio de M365 Teams, aplicaciones (clientes de almacenamiento en la nube), portapapeles del OS	Durante actividades de colaboracion donde se usen aplicaciones en la nube					Aplicaciones personalizadas internas y servicios personalizados	

Apéndice B: Comparación de funciones de los componentes de las soluciones de DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP—NETWORK	FORCEPOINT DLP FOR CLOUD	FORCEPOINT ONE SWG	FORCEPOINT ONE ZTNA: API FORCEPOINT DLP APP DATA SECURITY	FORCEPOINT ONE ZTNA (PRÓXIMAMENTE, SEGUNDO SEMESTRE DE 2023)
Risk-Adaptive Protection	Complemento		Complemento	Complemento	Complemento	Complemento; actualmente admitido con túneles GRE/IPSec con Forcepoint ONE SWG		
Reconocimiento óptico de caracteres			Incluido	Incluido	Incluido			Soporte de OCR para DLP mejorado (segunda mitad de 2023)
Clasificación de datos e integración de etiquetado	Forcepoint Data Classification y Microsoft Purview Information Protection.							
¿Qué datos pueden localizarse (fingerprinting)?*	Estructurados (bases de datos), no estructurados (documentos), binarios (archivos no textuales)							Disponible la segunda mitad de 2023
Administración de políticas unificada	Configuración y aplicación de políticas a través de una única consola desde endpoints a aplicaciones en la nube							Disponible la segunda mitad de 2023
Biblioteca de políticas robusta	Detección y aplicación desde la biblioteca de políticas de cumplimiento más grande de la industria							

Forcepoint

forcepoint.com/contact

Acerca de Forcepoint

Forcepoint simplifica la seguridad para las empresas y los gobiernos de todo el mundo. La plataforma todo en uno y realmente nativa en la nube de Forcepoint facilita la adopción de un enfoque de Zero Trust y evita el robo o la pérdida de datos confidenciales y propiedad intelectual sin importar desde donde trabajen las personas. Con sede en Austin, Texas, crea entornos seguros y confiables para los clientes y sus empleados en más de 150 países. Conéctese con Forcepoint a través de www.forcepoint.com, Twitter y LinkedIn.

[FP-DLP-Brochure-ES] 18Aug2023