Forcepoint Data Loss Prevention (DLP)

Protección de datos en un mundo sin perímetros

Forcepoint

Folleto

forcepoint.com

Forcepoint DLP

Seguridad impulsada por el factor humano

La seguridad de datos es un desafío que nunca acaba. Por un lado, las organizaciones de TI deben cumplir con las regulaciones y proteger la propiedad intelectual de ataques dirigidos y exposición 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 adoptan el enfoque aparentemente lógico de perseguir los datos: encontrarlos, catalogarlos y controlarlos. Sin embargo, este enfoque tradicional respecto de la prevención contra la pérdida de datos ya no resulta eficaz dado que no toma en cuenta la variable más importante en la seguridad de datos: su personal.

En lugar de enfocarse exclusivamente en los datos, la seguridad debe comenzar y terminar con las personas. La clave reside en ganar visibilidad respecto de las interacciones de los usuarios con los datos y las aplicaciones. Una vez que se logra eso, es posible aplicar un nivel de control basado en el riesgo específico de los usuarios y la confidencialidad o el valor de los datos.

El programa de protección de datos de una organización debe considerar el factor humano: la intersección entre usuarios, datos y redes. Además, se debe monitorear la transferencia de los datos y poner énfasis en las personas que crean, tocan y mueven datos a través de la empresa.

Forcepoint DLP aborda el riesgo centrado en las personas con visibilidad y control donde quiera que su personal trabaje y sus datos residan. Los equipos de seguridad aplican la calificación de riesgo de los usuarios para enfocarse en los eventos que más importan y acelerar el cumplimiento con las regulaciones de datos globales.

La protección de datos debe:

- **Proteger los datos regulados** mediante un único punto de control para todas las aplicaciones que su personal utiliza para crear, almacenar y mover datos.
- **Proteger la propiedad intelectual** con DLP avanzado que analiza la manera en que las personas utilizan 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

- **Cloud Applications**
- **Endpoint**
- **Network**
- **Discovery**

Acelere el cumplimiento

El entorno de TI moderno presenta un gran desafío 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 móviles. 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 dispositivos finales, aplicaciones en la nube y redes. Forcepoint DLP acelera sus esfuerzos de cumplimiento al combinar paquetes de cobertura de regulaciones globales con control centralizado de todo el entorno de TI. Forcepoint DLP protege de manera eficiente la información confidencial de los clientes y datos regulados para que puedan probar su cumplimiento constante con confianza.

- → **Cobertura regulatoria** para lograr rápidamente y mantener el cumplimiento con más de 370 políticas aplicables a las exigencias regulatorias de 83 países.
- → **Localice y corrija** datos regulados con detección en sus redes, la nube y los puntos finales.
- → **Control centralizado** y políticas uniformes en todo el entorno de TI.

Empodere a su personal para que proteja los datos

El DLP solo con controles preventivos frustra a los usuarios que los eludirán con la única intención de completar una tarea. Eludir la seguridad conduce a riesgos innecesarios y a la exposición de datos involuntaria.

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

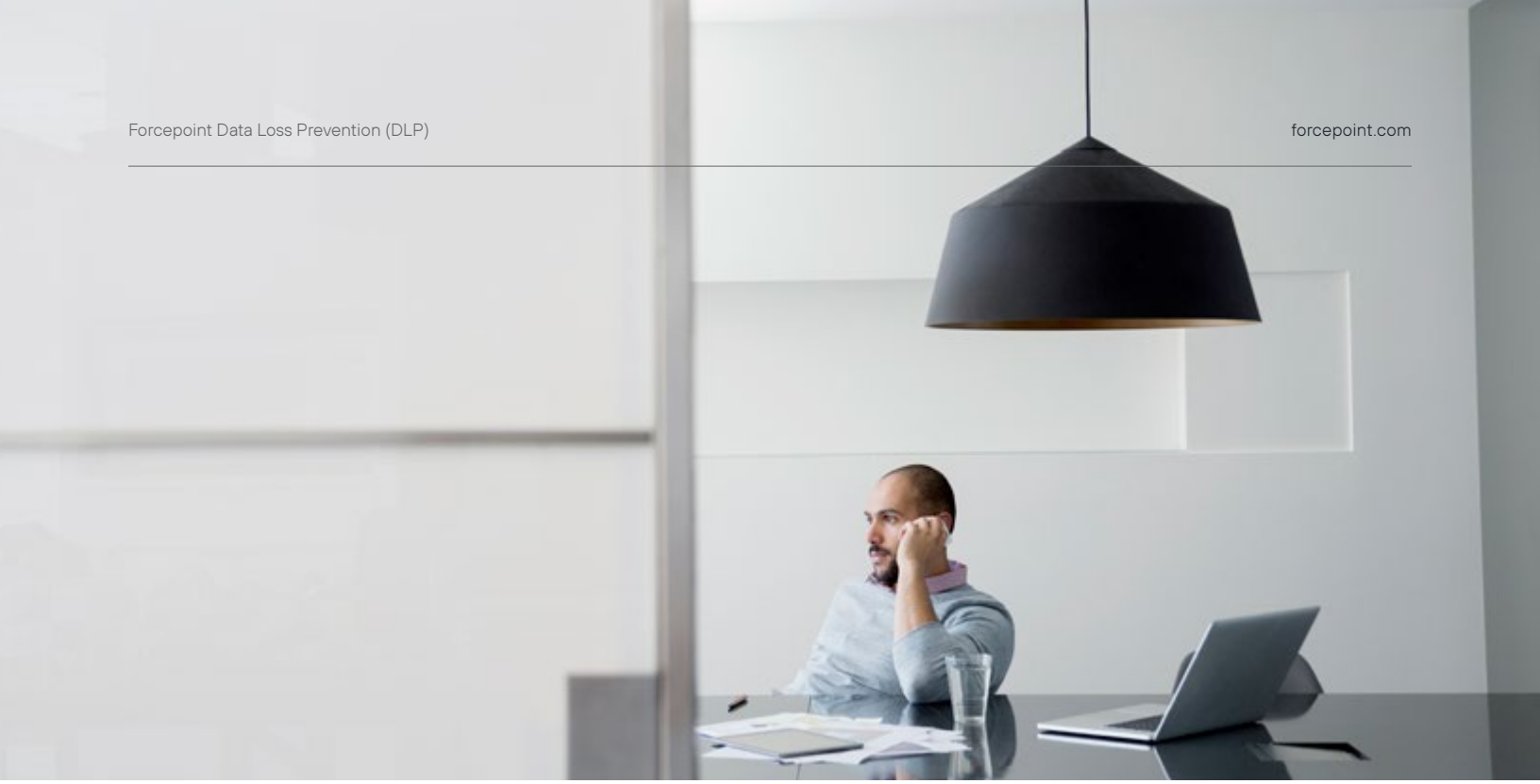
- → **Detección y control de datos** en donde sea que residan, ya sea en la nube o en la red, se envíen por correo electrónico o se encuentren en un dispositivo final.
- → **Asesore a sus empleados** para que tomen decisiones inteligentes, mediante mensajes que guíen las acciones de los usuarios; eduque a los empleados sobre las políticas y valide las intenciones de los usuarios cuando interactúan con datos críticos.
- → **Colabore de manera segura** con socios confiables utilizando autoencriptación basada en políticas que proteja los datos cuando salen de su organización.
- → **Automatice el etiquetado y la clasificación de datos** al integrarse con soluciones de clasificación de datos de terceros líderes (por ej., Microsoft Azure Information Protection, Titus, Boldon James).

Detección y controles avanzados que monitorean a los datos

Las fugas de datos accidentales y maliciosas son incidentes complejos, no eventos aislados. Forcepoint DLP es una solución comprobada que firmas de analistas como Gartner, Radicati y otras reconocen como líder dentro de la industria. Las soluciones DLP de Forcepoint están disponibles en dos versiones: DLP para Cumplimiento y DLP para Protección de Propiedad Intelectual (IP).

Las soluciones DLP de Forcepoint para Cumplimiento y Protección de IP brindan capacidades críticas que abordan el cumplimiento con funciones como:

- → **Reconocimiento Óptico de Caracteres (OCR)** que identifica datos integrados en imágenes cuando están en movimiento o inactivos.
- → **Identificación robusta** de información de identificación personal (PII) que ofrece verificaciones de validación de datos, detección de nombres reales, análisis de proximidad e identificadores de contexto.
- → **Identificación de encriptación personalizada** que expone datos ocultos para evitar su detección y los controles aplicables.
- → **Análisis acumulativo** para detección de DLP por goteo (es decir, datos que se fugan lentamente a lo largo del tiempo).
- → **Integración con Microsoft Azure Information Protection** que analiza archivos encriptados y aplica los controles de DLP correspondientes a los datos.



Forcepoint DLP para la protección de la IP incluye las capacidades detalladas más arriba y además, aplica la detección y el control de la pérdida de datos potencial más avanzados con funciones como:

- → **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 señalar documentos comerciales, código fuente, etc. similares.
- → **Localización (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 diseño y bases de datos, y luego aplicar la política o el control adecuado para esos datos.
- → **Análisis** para identificar cambios en el comportamiento de los usuarios en lo que respecta a la interacción con los datos, como un aumento en el uso del correo electrónico personal. Con la protección de datos dinámicos (DDP), Forcepoint DLP se vuelve todavía más efectivo al sacar provecho del análisis conductual del riesgo de los usuarios, que luego se utiliza para implementar políticas adaptables al riesgo. Esto le permite a los equipos de seguridad implementar políticas dinámicas e individualizadas en lugar de estáticas 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. Además 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 análisis, Forcepoint DLP reduce los falsos positivos, lo que optimiza las operaciones de seguridad. Para aumentar la concientización sobre la seguridad en los empleados, DLP permite el asesoramiento de empleados y la integración con soluciones de clasificación de datos.

- → **Enfoque a los equipos de respuesta** en el riesgo más grande con incidentes priorizados que destacan a las personas responsables del riesgo, los datos críticos en riesgo, y los patrones de comportamiento comunes a distintos usuarios.
- → **Aumente la concientización de los empleados** respecto del manejo de datos confidenciales y propiedad intelectual con asesoramiento para Windows y macOS, además de brindarles a los empleados integración con soluciones de clasificación como Boldon James y Microsoft Azure Information Protection.
- → **Implemente capacidades de identificación de datos con DLP de avanzada**, como localización (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 electrónico para su revisión 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 análisis de usuarios más exhaustivos mediante integraciones profundas con Forcepoint Insider Threat y el análisis 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 DLP for Cloud Applications amplía el análisis y las políticas de DLP a aplicaciones críticas en la nube para así proteger sus datos, donde sea que se encuentren.

- → **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 dispositivos finales 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 críticas en la nube, como Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack y muchas más.
- → **Unifique la aplicación de políticas** a través de una única consola para definir y aplicar datos en movimiento y políticas de detección de datos en todos los canales: la nube, la red y los dispositivos finales.
- → **Implemente una solución alojada por Forcepoint** que amplíe las funciones de la política de DLP, incluso la localización (fingerprinting) y el aprendizaje automatizado, a aplicaciones en la nube, al mismo tiempo que cuenta con la opción de mantener los datos forenses y de incidentes dentro de su central de datos.

Forcepoint DLP incluye plantillas de políticas regulatorias y análisis avanzado desde un único punto de control con cada implementación. Las empresas eligen las opciones de implementación 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 protección avanzada de datos inactivos (detección), 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 autocorrección del riesgo de datos por parte de empleados basándose en mensajes de asesoramiento de DLP. La solución monitorea las cargas en la web, incluidos los HTTPS, así como las cargas en servicios en la nube como Office 365 y Box Enterprise. Integración total con Outlook, Notes y clientes de correo electrónico.
Forcepoint DLP – Cloud Applications	Impulsado por Forcepoint CASB, DLP – Cloud Applications amplía 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.
Forcepoint DLP – Discovery	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 detección dentro de bases de datos como SQL Server y Oracle. La tecnología de localización (fingerprinting) identifica los datos regulados y la propiedad intelectual inactivos, y protege esos datos al aplicar la encriptación y los controles correspondientes. Discovery también incluye reconocimiento de caracteres ópticos (OCR) que brinda visibilidad a datos en imágenes.
Forcepoint DLP – Network	Forcepoint DLP – Network proporciona el punto de aplicación crítico para detener el robo de datos en movimiento que se produce a través del correo electrónico y la web. La solución ayuda a identificar y prevenir la exfiltración de datos y la pérdida accidental de datos causada por ataques externos o producida como resultado de la amenaza interna. El reconocimiento de caracteres ópticos (OCR) reconoce datos dentro de imágenes. El análisis identifica la DLP para detener el robo de datos con un registro por vez y otros comportamientos de usuarios de alto riesgo.

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

	FORCEPOINT DLP – ENDPOINT	FORCEPOINT DLP – CLOUD APPLICATIONS	FORCEPOINT DLP – DISCOVER	FORCEPOINT DLP – NETWORK
¿Cómo se implementa?	Forcepoint en un dispositivo final	Forcepoint en la nube	Servidor de detección administrado por TI	Dispositivo de red o nube pública
¿Cuál es la función principal?	Recopilar información del dispositivo final del usuario	Detectar datos y aplicar políticas en la nube o mediante aplicaciones en la nube	Detectar, escanear y corregir datos inactivos dentro de centrales de datos	Brindar visibilidad y control a datos en movimiento a través de la web o el correo electrónico
¿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 electrónico, web: HTTP(S), impresoras, medios extraíbles, servidores de archivos/NAS	Cargas, descargas y datos compartidos de Office 365, Google Apps, Salesforce.com, Box, Dropbox y ServiceNow vía API, y todas las aplicaciones principales vía proxy		Correo electrónico, proxy ActiveSync, web: HTTP(S) vía ICAP
¿Dónde están los datos en uso protegidos?	Zoom, Webex, Google Hangouts, mensajería instantánea, archivos compartidos mediante VOIP, aplicaciones (clientes de almacenamiento en la nube), portapapeles del OS	Durante actividades de colaboración donde se usen aplicaciones en la nube		
Protección de datos dinámicos*	Complemento			Complemento
Reconocimiento óptico de caracteres			Incluido	Incluido
Clasificación de datos e integración de etiquetado	Microsoft Azure Information Protection, Boldon James, Titus			
¿Qué datos pueden localizarse (fingerprinting)?*	Estructurados (bases de datos), no estructurados (documentos), binarios (archivos no textuales)			
Administración de políticas unificada	Configuración y aplicación de políticas a través de una única consola desde dispositivos finales a aplicaciones en la nube. Entre centrales de datos y la nube pública			
Biblioteca de políticas robusta	Detección y aplicación desde una amplia biblioteca de políticas de cumplimiento			

Los humanos son el nuevo perímetro

Forcepoint

forcepoint.com/contact

Acerca de Forcepoint

Forcepoint es la compañía líder en seguridad cibernética de protección de datos y usuarios, encargada de proteger a organizaciones a la vez que impulsa la transformación digital y el crecimiento. Las soluciones de Forcepoint se adaptan en tiempo real a la manera en que las personas interactúan con los datos, y proporcionan un acceso seguro a la vez que permiten que los empleados generen valor. Con sede en Austin, Texas, Forcepoint crea entornos seguros y fiables para miles de clientes en todo el mundo.

[DLP-BROCHURE-ES] 3Nov2020