Forcepoint

Datasheet

Forcepoint DLP

Prevención contra la pérdida de datos líder en la industria con administración unificada en todos los canales

La seguridad de datos es crítica, pero no tiene por qué ser complicada. La fuerza de trabajo híbrida de hoy requiere acceso a la información confidencial desde cualquier dispositivo, en cualquier ubicación. Forcepoint Data Loss Prevention (DLP) simplifica la protección de datos para la empresa moderna, ofreciendo una prevención contra la pérdida de datos integral on-premises sin sacrificar el rendimiento o la productividad.

Con una visibilidad profunda del movimiento de datos en endpoints, redes y almacenamiento, Forcepoint DLP protege sus activos críticos y garantiza el cumplimiento de normativas. Ofrece la capacidad única de extender las políticas desde Forcepoint Security Manager (FSM) a canales adicionales, lo que permite una protección de datos perfecta en las aplicaciones de SaaS en la nube y la web, al tiempo que garantiza una implementación de políticas consistente y unificada. Benefíciese de los análisis forenses avanzados, la integración perfecta, la escalabilidad y una solución que evoluciona con las necesidades de su negocio.

Optimice el cumplimiento de datos

- → **Regule la cobertura** para alcanzar y mantener fácilmente el cumplimiento de más de 1700 plantillas, políticas y clasificadores predefinidos aplicables a las exigencias regulatorias de más de 90 países en más de 160 regiones.
- → **Localice y corrija** los datos regulados con la detección en sus redes, la nube y los endpoints.
- → **Control central** y políticas consistentes en todos los canales, incluidos la nube, endpoints, red, web y correo electrónico.

Proporcione una protección de datos integral

- → **Detecte y controle los datos** en donde sea que residan, ya sea en la nube o en la red, se envíen por correo electrónico o se encuentren en el endpoint.
- → **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 mediante la encriptación automática basada en políticas que proteja los datos cuando salen de su organización.
- → **Automatice el etiquetado y la clasificación de datos** a través de la integración con Forcepoint Data Classification, así como con Microsoft Purview Information Protection.

Utilice funciones y controles avanzados

- → **El reconocimiento óptico de caracteres (OCR)** identifica los datos integrados en imágenes mientras están en reposo o en movimiento.
- → **La identificación robusta** de información de Identificación Personal (PII) ofrece verificaciones de validación de datos, detección de nombres reales, análisis de proximidad e identificadores de contexto.
- → **La identificación de encriptación personalizada** expone los datos para evitar su detección y a los controles aplicables.
- → **El análisis acumulativo** para la detección de DLP por goteo (es decir, datos que se fugan lentamente a lo largo del tiempo).
- → **El escaneo avanzado de archivos** detecta la exfiltración de datos parciales al examinar secciones aleatorias de archivos grandes, evitando que los exfiltradores oculten información confidencial.
- → **La integración con Forcepoint Data Classification**, que aprovecha modelos de IA/LLM altamente capacitados para proporcionar una clasificación de alta precisión para datos en uso y datos en reposo con Forcepoint Data Security Posture Management (DSPM).
- → **La IA generativa avanzada** permite a los usuarios entrenar el sistema y construir un modelo de IA de autoaprendizaje, encontrando, categorizando y clasificando automáticamente todos sus datos para ahorrar tiempo y aumentar drásticamente la precisión.
- → **La localización (fingerprinting)** de datos estructurados (por ejemplo, bases de datos) y no estructurados (por ejemplo, documentos) permite a los propietarios de datos definir tipos de datos e identificar coincidencias completas y parciales entre documentos comerciales, planes de diseño y bases de datos, y luego aplicar el control o la política adecuados para esos datos.
- → Con **Risk-Adaptive Protection**, Forcepoint DLP se vuelve aún más eficaz, ya que aprovecha la analítica del comportamiento para comprender el riesgo del usuario, que luego se utiliza para implementar la aplicación de políticas automatizadas en función del nivel de riesgo del usuario.

Encuentre y mitigue el riesgo de protección de datos

- → **Oriente a los equipos de respuesta** en el mayor riesgo con priorización de incidentes que destacan a las personas responsables del riesgo, los datos críticos en riesgo y los patrones de comportamiento comunes entre los usuarios.
- → **Utilice la herramienta de ayuda de Smart Search impulsada por IA** integrada directamente en la solución para encontrar rápidamente información de soporte específica sin salir de la consola de administración.
- → **Aumente la concienciación de los empleados** respecto del manejo de datos confidenciales y propiedad intelectual con capacitación de empleados en Windows y macOS, además de brindarles a los empleados la integración de soluciones de clasificación, como Forcepoint Data Classification y Microsoft Purview Information Protection.
- → **Implemente capacidades avanzadas de identificación de datos de DLP**, como la localización (fingerprinting), en endpoints de trabajo remoto y en aplicaciones en la nube empresarial.
- → **Brinde a los propietarios de datos y a los 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** a un análisis de usuarios más amplio a través de integraciones profundas con Forcepoint Risk-Adaptive Protection.

Logre visibilidad sobre sus datos en todas partes

- **Capacite a los administradores** para identificar y proteger los datos en aplicaciones en la nube, almacenamiento de datos de su red, bases de datos y endpoints administrados y no administrados.
- **Identifique y evite automáticamente que se compartan** datos confidenciales con usuarios externos o usuarios internos no autorizados.
- **Proteja los datos en tiempo real** para cargas y descargas desde aplicaciones críticas en la nube, incluidos Office 365, Teams, SharePoint, OneDrive, Salesforce, Box, Dropbox, Google Apps, AWS, ServiceNow, Zoom, Slack y muchos más.
- **Unifique la implementación de políticas** a través de una única consola para definir y aplicar políticas de datos en movimiento y de detección de datos en todos los canales: nube, red, endpoints, web y correo electrónico.
- **Mantenga la propiedad de los datos** con una solución de DLP on-prem y opciones híbridas para extender las funciones avanzadas, como la localización (fingerprinting), el aprendizaje automatizado y la implementación de políticas, a las aplicaciones en la nube y los canales web. Ideal para industrias altamente reguladas, garantiza la soberanía de los datos al mantener de forma segura los datos de incidentes y análisis forenses dentro de su data center, lo que admite los requisitos de cumplimiento.
- **Vea y administre incidentes mediante herramientas de terceros** a través de REST APIs 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.

Para obtener más información sobre nuestras soluciones DLP enterprise , solicite una demo.

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

Forcepoint DLP Endpoint	Forcepoint DLP Endpoint protege sus datos críticos en endpoints de Windows y Mac dentro y fuera de la red corporativa. Incluye protección y control avanzados para datos en reposo (detección), en movimiento y en uso. Se integra con Microsoft Azure Information Protection para analizar datos encriptados y aplicar controles de DLP adecuados. Permite a los empleados la autocorrección del riesgo de datos en función de los mensajes de asesoramiento de DLP. La solución monitorea las subidas web, incluyendo HTTPS, así como las subidas a servicios en la nube, como Office 365 y Box Enterprise. Integración total con Outlook, Notes y clientes de correo electrónico.
Forcepoint ONE CASB	Impulsado por Forcepoint ONE CASB, amplíe el control único y análisis avanzado de Forcepoint DLP a las aplicaciones en la nube autorizadas, incluidas 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 o 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 Zero Trust CDR para la limpieza completa de todos los documentos descargables.
Forcepoint DLP Discover	Forcepoint DLP Discovery identifica y protege los datos confidenciales en servidores de archivos, SharePoint (on-premises y en la nube), Exchange (on-premises y en la nube), y la detección dentro de bases de datos, como SQL Server y Oracle. La tecnología avanzada de localización (fingerprinting) identifica los datos regulados y la propiedad intelectual en reposo, y protege esos datos mediante la encriptación y controles adecuados. Discovery también incluye reconocimiento de caracteres ópticos (OCR) que brinda visibilidad a datos en imágenes.
Forcepoint DLP Network	Forcepoint DLP Network ofrece el punto de aplicación crítico para detener el robo de datos en movimiento a través de correo electrónico, canales web y FTP. La solución ayuda a identificar y prevenir la exfiltración de datos y la pérdida de datos accidental ante ataques externos o amenazas internas. El reconocimiento óptico de caracteres (OCR) reconoce datos dentro de una imagen. Analytics proporciona DLP por goteo para detener el robo de datos de a un registro a la vez, así como otros comportamientos de usuario de alto riesgo.
Forcepoint DLP for Cloud Email	Forcepoint DLP for Cloud Email detiene la exfiltración no deseada de sus datos e IP a través del correo electrónico saliente. Puede combinarlo con otras soluciones de canal de Forcepoint DLP, como endpoint, red, nube y web, para simplificar su administración de DLP, escribir una política e implementar esa política en múltiples canales. A diferencia de las soluciones que no están en la nube, Forcepoint DLP for Cloud Email permite un enorme potencial de escalabilidad ante ráfagas imprevistas de tráfico de correo electrónico. También permite que el tráfico de correo electrónico saliente crezca junto a su empresa sin tener que configurar y administrar recursos de hardware adicionales.
Forcepoint DLP App Data Security API	La Forcepoint DLP App Data Security API 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 realizado 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 ONE SWG	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
¿Cuál es la función principal?	Detección de datos e implementación 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.	Detección de datos e implementación de políticas en la nube o con aplicaciones entregadas en la nube	Visibilidad y control a datos en movimiento a través del correo electrónico saliente	Detección, escaneo y corrección de datos en reposo dentro de centrales de datos y otros entornos on-prem	Visibilidad y control a datos en movimiento a través de la web o el correo electrónico web dentro de la red	Visibilidad y control a datos en movimiento a través de la web o el correo electrónico web dentro de la red	Visibilidad y control de los datos en aplicaciones y servicios personalizados internos
¿Dónde están los datos en reposo detectados/ protegidos?	Endpoints de Windows Endpoints de macOS	OneDrive, Sharepoint Online, Exchange Online, Google Drive, Box, DropBox, Salesforce, ServiceNow	En servidores de archivos y almacenamiento de redes on-premises, 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 uso compartido para Office 365, Google Apps, Salesforce.com, Box, Dropbox y ServiceNow a través de API y TODAS las otras aplicaciones principales a través de proxy	HTTP(S)		Correo electrónico, impresoras, FTP, Web: Http(S), ICAP	Correo electrónico	Aplicaciones personalizadas internas y servicios personalizados
¿Dónde están los datos en uso protegidos?	Zoom, Webex, Google Hangouts, mensajería instantánea, uso compartido de archivos de VOIP, uso compartido de M365 Teams, aplicaciones (clientes de almacenamiento en la nube), portapapeles de OS	Durante las actividades de creación, modificación y colaboración que utilizan aplicaciones en la nube					Aplicaciones personalizadas internas y servicios personalizados

Apéndice B: Comparación de características de componentes de soluciones de DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT ONE SWG	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
Risk-Adaptive Protection	Complemento		Complemento; actualmente admitido con túneles GRE/ IPSec con Forcepoint ONE SWG	Complemento	Complemento	Complemento	
Optical character recognition				Incluido	Incluido	Incluido	
Integraciones de clasificación y etiquetado de datos	Forcepoint Data Classification y Microsoft Purview Information Protection.						
¿Qué datos pueden localizarse (fingerprinting)?	Estructurados (bases de datos), no estructurados (documentos), binarios (archivos no textuales)						
Administración de políticas unificada	Configuración e implementación de políticas a través de una única consola desde endpoints a aplicaciones en la nube						
Biblioteca de políticas robusta	Detección y aplicación desde la biblioteca de políticas de cumplimiento más grande de la industria						

© 2025 Forcepoint. Forcepoint y el logotipo de FORCEPOINT son marcas registradas de Forcepoint. Todas las demás marcas registradas que se utilizan en este documento son propiedad de sus respectivos propietarios. [FP-DLP-Datasheet-ES] 06Jan2025