Forcepoint

Datasheet

Forcepoint ONE Data Security

DLP de nivel empresarial, unificado en todos los canales clave y administrado de froma sencilla desde la nube.

Hoy en día, la seguridad de los datos es un aspecto comercial crítico. Pero justo cuando su organización siente que ha resuelto el tema de la seguridad de los datos, llega el más reciente desafío de seguridad: el uso seguro de las aplicaciones de inteligencia artificial generativa (GenAI). Con datos esparcidos en dispositivos y entornos de nube, y ahora con el aumento de las aplicaciones de GenAI, proteger datos confidenciales en un mundo de inteligencia artificial (IA) puede parecer una tarea imposible.

Forcepoint ONE Data Security es una solución de prevención de pérdida de datos (DLP) nativa de la nube diseñada para la empresa moderna. Esta solución de software como servicio (SaaS) de DLP protege la información confidencial, evita violaciones de datos y facilita el cumplimiento de las normativas de privacidad a nivel mundial. Al proporcionar un despliegue rápido y administración de políticas, optimiza la protección de los datos y ofrece una administración unificada en aplicaciones de GenAI y en la nube, web, correo electrónico y endpoints. Además, con Forcepoint Risk-Adaptive Protection, ofrece información sobre el riesgo del usuario en tiempo real. Experimente costos y riesgos reducidos, así como una mayor productividad con Forcepoint ONE Data Security.

Identificación de datos de DLP empresarial poderosa en todos los canales

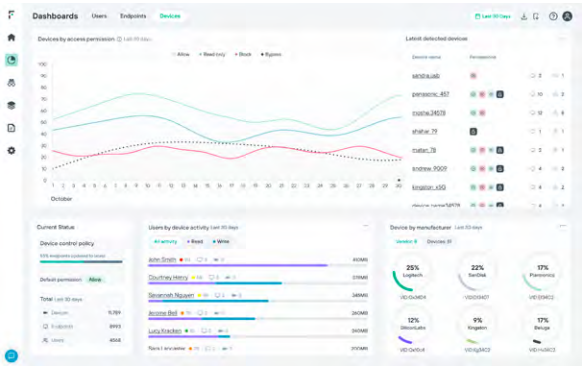
- → Más de 1700 clasificadores, plantillas y políticas predefinidos listos para implementar.
- → Procesamiento del lenguaje natural (NLP)
- → Detección avanzada de tipo de archivo verdadero que cubre más de 900 tipos de archivos.

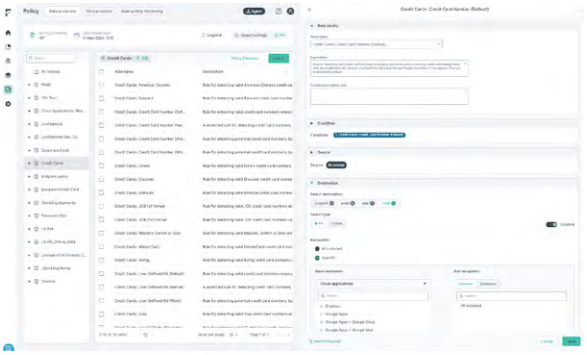
Use aplicaciones de GenAI de forma segura

Comience su viaje de transformación de la IA hoy mismo con Forcepoint. Propulse la productividad y la eficiencia con el uso seguro de aplicaciones de GenAI, como ChatGPT, Copilot, Gemini y muchas otras. Con Forcepoint ONE Data Security, puede capacitar a los usuarios sobre cómo usar las aplicaciones de GenAI correctamente, inspeccionar y bloquear información confidencial en cargas y pegado de información de manera automática, y registrar los intentos de uso indebido de datos confidenciales.

Administración unificada: “Una política para regirlos a todos”

Puede administrar todos los servicios de Forcepoint ONE a la perfección desde la interfaz de Forcepoint ONE Data Security. Ejerza el control sobre todos los canales (CASB, SWG, correo electrónico y endpoint) a través de una única política, lo que garantiza la uniformidad en todos los puntos de salida clave. Con un solo clic, implemente una nueva política o aplique una política existente en todos los canales clave. Monitorice a su conveniencia los incidentes de DLP desde un dashboard unificado para obtener una visión integral de la seguridad de datos en toda su organización.





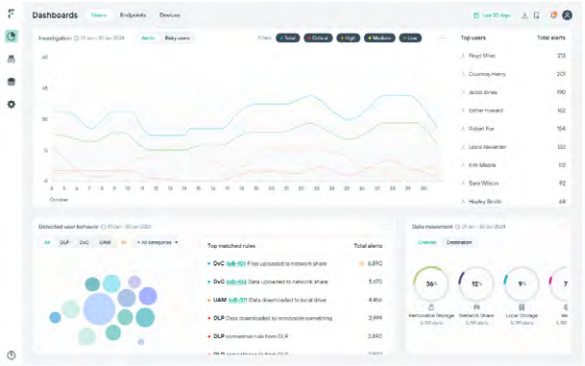
Configuración simple de políticas

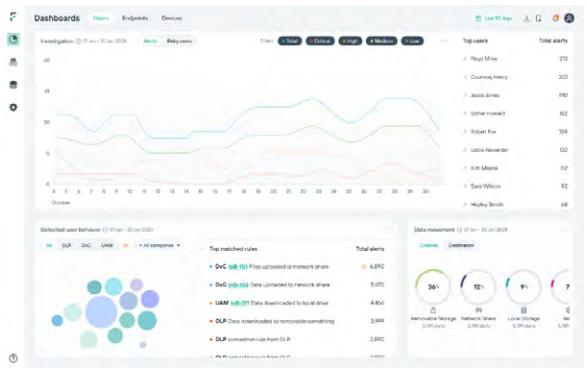
- → Optimice la administración mediante el uso de actualizaciones OTA de las políticas, clasificadores y plantillas predefinidas más recientes.
- → Cree políticas con solo unos clics e impleméntelas en minutos en lugar de horas.
- → Obtenga políticas de cumplimiento listas para implementar para más de 150 regiones y 90 países para garantizar el cumplimiento de la regulación de la privacidad en cada región global importante.

Administración fácil de incidentes y alertas

Obtenga una visión completa de todos los incidentes y alertas en tiempo casi real a través del dashboard de informes. Con la elaboración de informes integrados, los administradores obtienen una vista holística de las aplicaciones en la nube, el tráfico web, el correo electrónico y los endpoints. El control nativo de dispositivos mejora la seguridad de datos y el control de acceso para medios extraíbles, como las unidades USB. Forcepoint ONE Data Security se integra a la perfección con Risk-Adaptive Protection, lo que ofrece contexto en tiempo real y comprensión de la intención del usuario al centrarse en el comportamiento y la interacción de datos. Las capacidades de análisis forense permiten una visión más profunda del movimiento de datos, lo que permite una investigación eficaz de incidentes de seguridad para mejorar la implementación de políticas y optimizar el cumplimiento. Todo esto se administra a través de un único agente e IU.

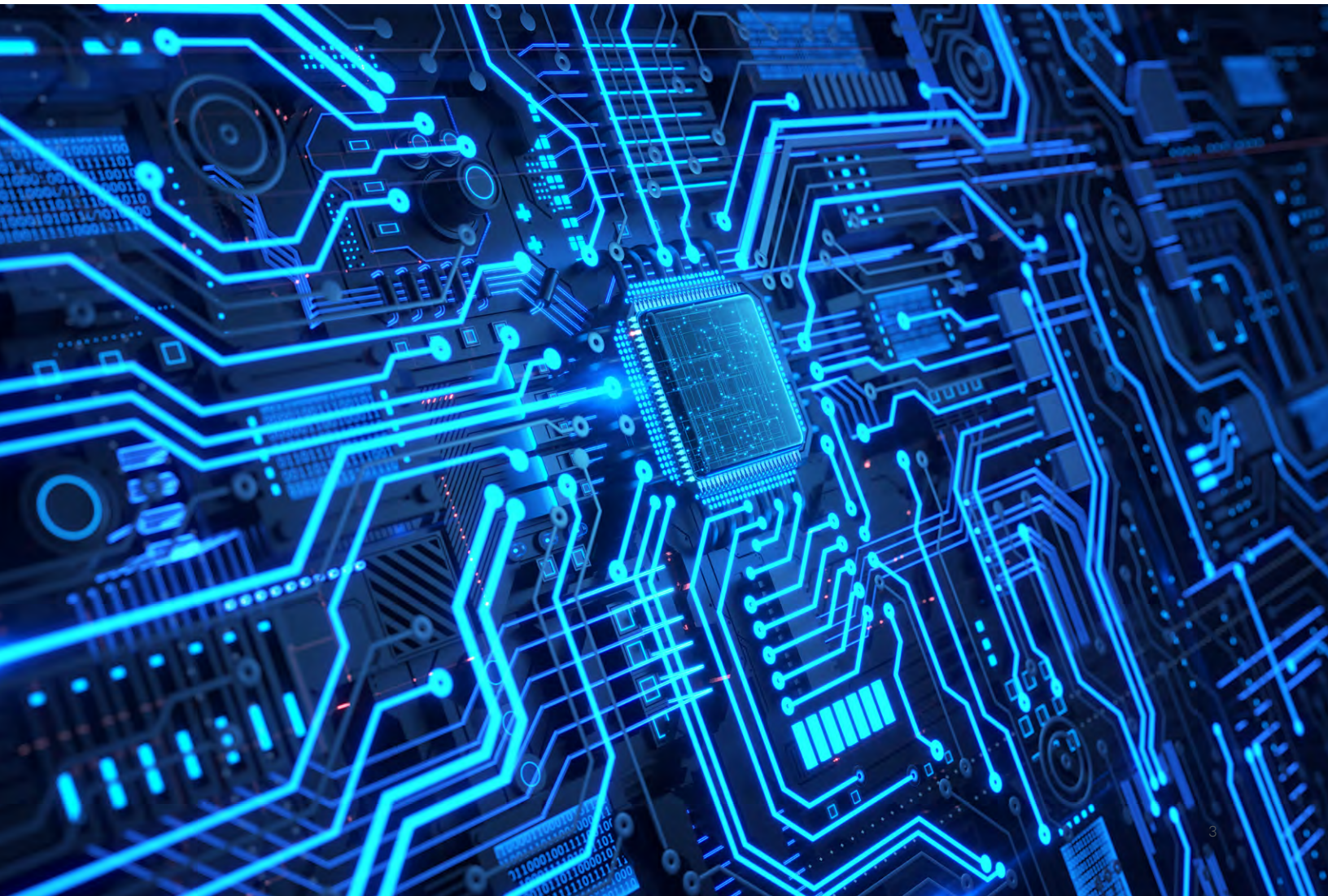
*La integración con Risk-Adaptive Protection (endpoint necesario para informar la puntuación de riesgo) requiere una SKU separada (complemento de Forcepoint ONE Data Security).





Solución de SaaS nativa en la nube

- → Reduzca los costos generales.
- → Sin costos de configuración de hardware y software on-premises.
- → La solución nativa en la nube ofrece una escalabilidad mayor y más eficiente.
- → Administración simple de la seguridad de datos con actualizaciones continuas con nuevas características, corrección de errores y parches de seguridad.
- → Actualizaciones automáticas OTA para el endpoint.
- → Implementado en AWS a nivel mundial con un tiempo de actividad del 99,99 % sin tiempo de inactividad programado.
- → Creado en AWS IoT para escalar fácilmente a cientos de miles de endpoints.



Forcepoint ONE Data security proporciona una solución integral para administrar políticas globales en todos los canales, incluidas aplicaciones de GenAI y en la nube, web, correo electrónico y endpoints. Con una amplia gama de plantillas, políticas y clasificadores predefinidos, simplificamos su carga de trabajo, lo que permite una administración de incidentes optimizada y priorizar las tareas críticas.

CARACTERÍSTICAS	BENEFICIOS
Más de 1700 clasificadores, plantillas y políticas predefinidos listos para implementar	Optimice la implementación inicial de DLP y la administración continua de políticas con políticas, plantillas o clasificadores predefinidos
Procesamiento del lenguaje natural (NLP)	Precisión sin precedentes que reconoce los tipos de datos comunes (PII, PHI, PCI) en función del contenido descrito mediante el uso de más de 300 scripts de lenguaje natural predefinidos
Detección avanzada de tipo de archivo verdadero	Identifique más de 900 tipos de archivos, independientemente de si han cambiado de nombre para evitar la detección, incluidos OCR y texto en las imágenes
Control unificado de políticas en CASB, SWG, correo electrónico y endpoints	Administre todos los canales desde dentro de una única política. Escriba una vez e implemente en todos los canales de salida
Informes unificados en CASB, SWG, correo electrónico y endpoints	Informes unificados en CASB, SWG, correo electrónico y endpoints
Políticas de cumplimiento para más de 150 regiones de todo el mundo listas para usar, 90 países	Políticas disponibles listas para usar para permitir el cumplimiento de la regulación de la privacidad en cada región importante a nivel mundial
Actualizaciones automatizadas	Simplifique la administración de la seguridad de datos con actualizaciones automatizadas de las políticas, clasificadores y plantillas predefinidas más actualizadas
Acceso rápido a alertas en el dashboard de informes (portal en la nube)	Vea todos los incidentes y alertas en tiempo casi real desde un dashboard eficiente y organizado
Informes integrados	Vea todos los informes en DLP, Control de dispositivos y Risk-Adaptive Protection en una interfaz de usuario integrada
Priorización de incidentes	Vea las diez acciones principales que requieren atención inmediata en la interfaz del incidente. Combinado con la calificación de Risk-Adaptive Protection, puede incluir el número de incidentes y la gravedad del riesgo de los usuarios para priorizar el flujo de trabajo
Análisis forense	Proporciona visibilidad al movimiento de datos para investigar incidentes de seguridad, comprender la causa de las fugas de datos, realizar investigaciones detalladas de incidentes, mejorar la efectividad de las políticas y respaldar las necesidades legales/de cumplimiento.
Visibilidad de administración de agentes	Obtenga visibilidad del estado de implementación de su endpoint y encuentre rápidamente problemas con los agentes
No se requiere conexión de red para la implementación de endpoint	No es necesario estar conectado a la red para que los endpoints tengan visibilidad de las violaciones de seguridad. Los datos siempre están protegidos independientemente de la conectividad de red
Integración con el control de dispositivos	Amplía la seguridad de datos y el control de acceso para medios extraíbles en un único agente e IU
Integración con Risk-Adaptive Protection	La implementación de políticas automatizada y sensible al contexto en tiempo real, así como la administración de incidentes desde un único agente/IU requiere una SKU separada para Risk-Adaptive Protection (complemento de Forcepoint ONE Data Security)
Tiempo de actividad del 99,99 % sin tiempo de inactividad programado	Implementado en AWS a nivel mundial con un tiempo de actividad del 99,99 %