Hoja de datos de privacidad de Elastic

Elasticsearch

Los clientes son responsables de realizar su propia evaluación independiente de la información en este documento. Este documento: (a) tiene fines meramente informativos, (b) representa las ofertas de productos, servicios y prácticas actuales de Elastic, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de Elastic y sus afiliadas, proveedores o licenciantes. Las responsabilidades y obligaciones de Elastic frente a sus clientes se rigen por los acuerdos de Elastic, y este documento no forma parte ni modifica ningún acuerdo entre Elastic y sus clientes.

 © 2025 Elasticsearch B.V. Todos los derechos reservados.

Resumen del producto: Elasticsearch

Elasticsearch permite a las organizaciones crear experiencias de búsqueda potentes para sitios web, aplicaciones y datos empresariales mediante la plataforma unificada de Elastic. Impulsa aplicaciones de búsqueda con AI y machine learning. Elasticsearch aprovecha la base de datos vectorial, el kit de herramientas de AI y las capacidades avanzadas de recuperación de Elasticsearch para dar soporte a aplicaciones de búsqueda y de generación aumentada por recuperación (RAG). Está optimizado para la velocidad y la relevancia en cargas de trabajo a escala de producción, lo que permite a los usuarios buscar, indexar, almacenar y analizar datos de todo tipo y tamaño en tiempo casi real.

- **Tipo de producto:** software
- **Modelo(s) de despliegue:**
    - Local (autogestionado)
    - Cloud (SaaS) (Elastic Cloud Hosted, Elastic Cloud Serverless)
    - Híbrido

Datos procesados en Elasticsearch

Elasticsearch procesa los datos que los clientes introducen para diversas aplicaciones de búsqueda. Los tipos específicos de datos personales que se procesan dependen totalmente de los datos y la configuración del cliente, ya que Elastic se limita principalmente a proporcionar la plataforma para el manejo de datos.

Categorías de datos personales necesarios para acceder y usar Elasticsearch:

- Identificadores de administrador y usuario, credenciales, permisos, cookies de sesión y registros de actividad. El tratamiento de estos datos es necesario para el despliegue, la configuración, la administración, la gestión, el acceso seguro y el uso auditable del producto.

Las categorías adicionales de datos personales que se pueden tratar incluyen, entre otras, los datos contenidos en:

- Cualquier dato que el cliente introduzca al producto (que puede incluir datos personales dependiendo del caso de uso del cliente).
    - Ejemplos: búsquedas de usuarios, contenido de sitios web, catálogos de productos, bases de conocimiento, documentos del lugar de trabajo, interacciones de atención al cliente y datos utilizados para entrenar modelos de AI o aplicaciones RAG.
- Identificadores en línea y datos de uso relacionados con las actividades de búsqueda:
    - Ejemplos: direcciones IP (si forman parte de los registros del sistema), datos de seguimiento de actividad del usuario (usados para optimizar la relevancia en la búsqueda).

Propósito(s) típico(s) de procesar los datos de clientes que se suministran al producto:

En sus despliegues específicos, los clientes tienen la exclusiva discreción de determinar el propósito real del procesamiento de cualquier dato que elijan alimentar al producto. En general, Elasticsearch está diseñado y pensado para casos de uso como:

© 2025 Elasticsearch B.V. Todos los derechos reservados.

- Para crear experiencias de búsqueda potentes y fluidas para aplicaciones, sitios web y datos empresariales.
- Habilitar aplicaciones de búsqueda impulsadas por AI y machine learning para clientes y empleados.
- Para permitir el almacenamiento, la indexación, la búsqueda y el análisis eficientes de diversos tipos de datos (estructurados, texto no estructurado, numéricos, geoespaciales) casi en tiempo real.
- Para admitir capacidades de búsqueda vectorial y búsqueda híbrida mediante la ejecución de una búsqueda de vecinos más cercanos y su combinación con texto para obtener resultados relevantes.
- Optimizar las experiencias de búsqueda para clientes y usuarios mediante el análisis y la visualización de datos sobre el comportamiento de los usuarios y del sitio web, e identificar las tendencias en las consultas de los usuarios para mejorar la relevancia de los resultados de búsqueda.
- Para habilitar conversaciones en lenguaje natural, proporcionar contexto y mantener el conocimiento para aplicaciones como chatbots y generación aumentada por recuperación (RAG).

Datos de uso del producto

Tanto para los despliegues de Elastic Cloud como para los despliegues autogestionados de Elasticsearch, Elastic recopila automáticamente cierta información relacionada con el uso del producto. Estos datos de uso del producto se procesan según lo descrito en la Declaración de privacidad de productos de Elastic. En los modelos de despliegue local y ciertos modelos de despliegue híbrido, los clientes pueden restringir o deshabilitar el procesamiento de datos de uso del producto en la configuración del producto (consulta la documentación del producto aplicable). Sin embargo, la recopilación y el procesamiento de estos datos de uso del producto son indispensables para el correcto funcionamiento del producto en modelos de despliegue en el cloud (SaaS).

Acceso a los datos del cliente

- **Acceso de los clientes:** los clientes mantienen el control total sobre los datos que ingieren en Elasticsearch. Pueden acceder a sus datos y administrarlos a través de la interfaz gráfica de usuario de Kibana, que se utiliza para visualizar y analizar datos. Los clientes pueden aprovechar el potente DSL de consultas de Elastic para consultar, explorar y visualizar sets de datos. También está disponible el acceso directo a los datos a través de la API REST de Elasticsearch o de los clientes de Elasticsearch para lenguajes de programación comunes. Los RBAC están integrados en Kibana, lo que permite a los administradores definir roles que limitan el acceso de usuario a índices, dashboards o acciones específicos, aplicando así los principios de privilegio mínimo.

- **Acceso por parte de Elastic:** en cuanto a las ofertas de Elastic Cloud, un número limitado de empleados de Elastic tiene acceso privilegiado al entorno de producción únicamente para la gestión, el mantenimiento y el soporte de la plataforma. Este acceso se ajusta estrictamente a los principios de menor privilegio y necesidad de saber, y se revisa y modifica de manera regular según sea necesario. Elastic no tiene acceso a los datos en los despliegues autogestionados, y solo accederá al contenido del cliente en los despliegues en el cloud cuando el cliente lo indique (por ejemplo, al prestar servicios de soporte a petición del cliente).
    - Elastic ha implementado un registro centralizado, que abarca logs de proxies, logs de acceso, logs de Elasticsearch y logs de Auditbeat para registrar todo el acceso a los datos del cliente y a los sistemas en los que residen. Los equipos internos de Elastic desarrollan e implementan activamente detecciones para actividades sospechosas en cuentas internas y acceso no autorizado, lo que incluye el monitoreo de integridad de archivos e indicadores de apropiación de cuenta.

- Los principios de Elastic dictan que solo divulgará o proporcionará acceso a los datos de los clientes cuando la ley lo imponga estrictamente, e incluye protocolos establecidos para impugnar tales solicitudes y notificar a las partes relevantes cuando sea legalmente permisible.

Ubicaciones de procesamiento

Los despliegues de Elastic Cloud de Elasticsearch se alojan en plataformas en el cloud certificadas gestionadas por proveedores líderes en IaaS que incluyen Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure. Los clientes pueden seleccionar la región geográfica donde desean alojar sus despliegues.

Subprocesamiento: Elastic emplea ciertos subprocesadores de infraestructura y de atención al cliente para ofrecer sus servicios. Los subprocesadores específicos involucrados dependen de la ubicación del centro de datos, los servicios y las funcionalidades elegidas por el cliente. Estos subprocesadores están contractualmente obligados a proporcionar un nivel de protección de datos al menos equivalente al descrito en el Anexo de Seguridad de la Información de Elastic. Elastic mantiene total transparencia respecto a sus subprocesadores (ver listas internas y externas) y es responsable de sus acciones y omisiones en la misma medida que si Elastic realizara los servicios por sí misma.

Cumplimiento de las regulaciones de privacidad

Elastic captura, procesa, almacena y protege los Datos personales del cliente de acuerdo con el Anexo de procesamiento de datos del cliente aplicable y los compromisos descritos en esta Hoja de datos de privacidad. Nuestro Centro de confianza es un recurso completo donde encontrarás información sobre nuestras prácticas de privacidad y nuestras iniciativas de cumplimiento normativo.

- **Propiedad de los datos:** los datos del cliente siguen siendo propiedad del cliente. Elastic solo procesa estos datos para los fines especificados en el contrato del cliente y nunca vende los datos de los clientes a terceros.
- **Cumplimiento de GDPR:** las características de Elastic Cloud están diseñadas para respaldar el cumplimiento del Reglamento General de Protección de Datos y otras leyes globales de protección de datos y privacidad. Esto incluye dar prioridad a la seguridad de los datos personales mediante medidas técnicas y organizativas eficaces, y ofrecer un Anexo de procesamiento de datos que cumpla con el GDPR. Nuestro equipo especializado en privacidad de Elastic supervisa el cumplimiento del GDPR.
- **Marco de privacidad de datos (DPF):** Elasticsearch, Inc. está certificado de conformidad con el marco de privacidad de datos UE-EE. UU., la extensión del Reino Unido al marco de privacidad de datos UE-EE. UU. y el marco de privacidad de datos Suiza-EE. UU., según lo establecido por el Departamento de Comercio de los Estados Unidos.
- ∉ **Transferencia transfronteriza de datos:** Elastic legitima las transferencias de datos personales entre las jurisdicciones en las que opera mediante el uso de las Cláusulas contractuales estándar vigentes, así como a través de su participación en el Marco de privacidad de datos para las transferencias hacia Estados Unidos y desde allí en adelante. Además, implementamos medidas complementarias sólidas para proteger los datos durante las transferencias, como el cifrado en tránsito y en reposo, protocolos para impugnar solicitudes de autoridades públicas y la opción para los clientes de seleccionar servidores regionales para el alojamiento.

Portabilidad de datos

Los clientes pueden gestionar fácilmente la portabilidad de sus datos desde Elasticsearch. Pueden recuperar datos almacenados en Elasticsearch con su API REST y a través de diferentes clientes de Elasticsearch para lenguajes de programación comunes. Esta capacidad ayuda a los clientes a cumplir con las solicitudes de acceso de los interesados. Además, Elastic ofrece opciones para exportar los dashboards y visualizaciones de Kibana a formatos como PDF, PNG o CSV.

Retención y eliminación

Elastic proporciona herramientas y capacidades que permiten a los clientes gestionar eficazmente sus políticas de retención y eliminación de datos.

- Los clientes pueden definir y aplicar políticas de retención para los datos que recopilan y procesan dentro del entorno de Elastic.
- Elastic facilita la identificación de datos no utilizados y ayuda a definir las prácticas de retención de datos, ya que permite a los clientes clasificar los datos en niveles de almacenamiento y revisar los registros de acceso.
- Logstash, un componente de Elastic, se puede utilizar para transformar datos, lo que incluye la anonimización y la seudonimización, y ayuda a cumplir los objetivos de minimización de datos y reduce los riesgos de seguridad de los datos.
- La plataforma de Elastic permite a las organizaciones analizar más de cerca su uso real de los datos personales retenidos, lo que les permite adaptar los períodos y las políticas de conservación de datos de forma más eficaz.
- Para las solicitudes de eliminación de datos de los sujetos, Elastic proporciona capacidades para etiquetar datos para su retención bajo una excepción, o para eliminar datos de forma permanente con técnicas de eliminación y desidentificación permisibles, como la anonimización, con el fin de ayudar a los clientes a mantenerse en cumplimiento dentro de plazos de respuesta breves.

Seguridad

La seguridad de tus datos de Elastic Cloud también depende de que mantengas tu cluster de Elasticsearch configurado de forma segura y de que mantengas la confidencialidad de tus credenciales de inicio de sesión de Elastic Cloud (consulta nuestras Preguntas frecuentes sobre seguridad para obtener más información). Elastic soporta un modelo de seguridad integral de defensa en profundidad diseñado para proteger los datos de los clientes durante todo su ciclo de vida: en tránsito, en reposo y en memoria, así como mediante procedimientos robustos de gestión de claves.

- **Cifrado:** los datos del cliente se cifran en reposo con AES-256 y en tránsito a través de TLS 1.2. Elastic implementa procedimientos estrictos de gestión de claves de cifrado.
- **Controles de acceso:** Elastic mantiene controles técnicos, lógicos y administrativos para limitar el acceso a los datos exclusivamente a los usuarios autorizados. Estos controles incluyen medidas como la autenticación multifactorial, normas estrictas sobre la seguridad de las contraseñas y el uso de redes privadas virtuales (VPN) para el acceso administrativo. Además, los controles de acceso basados en roles (RBAC) están integrados en los despliegues de Elastic y la plataforma de administración de Elastic Cloud, lo que permite un control granular sobre los permisos de los usuarios.

- **Logging y monitoreo:** Elastic implementó un sistema de logging centralizado, que incluye logs de proxies, logs de acceso, logs de Elasticsearch y logs de Auditbeat para registrar todo el acceso a los datos del cliente y a los sistemas en los que residen. El equipo de Detección y Respuesta a Amenazas de Elastic usa flujos de trabajo automatizados para detectar e investigar actividad sospechosa en cuentas internas y acceso no autorizado, lo que incluye el monitoreo de la integridad de archivos e indicadores de apropiación de cuenta.
- **Actualizaciones y parches del sistema:** las instancias de Elasticsearch se actualizan y despliegan regularmente según los kernels del sistema operativo más recientes. Los parches apropiados se aplican de inmediato cada vez que se identifica una Vulnerabilidad y Exposición Comunes (CVE) en cualquier componente de software.
- **Detección y respuesta a incidentes:** Elastic implementó y actualiza continuamente las reglas de detección para actividades sospechosas y accesos no autorizados. Estas detecciones forman parte de flujos de trabajo automatizados que alertan al equipo de Detección y Respuesta a Amenazas, y desencadenan investigaciones de analistas. Elastic usa Elastic Security a nivel interno, que incluye capacidades de detección y respuesta de endpoint e integra fuentes de inteligencia de amenazas para admitir la detección de intrusiones. Permite respuestas automatizadas mediante integraciones con plataformas SOAR de terceros, lo que reduce la probabilidad de una brecha y acelera los tiempos de respuesta.
- **Marco de desarrollo de software seguro (SSDF):** Elastic mantiene un marco de desarrollo de software seguro basado en NIST 800-218. Este marco guía el proceso para diseñar, desarrollar, implementar, supervisar y mantener de forma segura todo el software de Elastic, garantizando un enfoque de “seguridad desde el diseño” y “seguridad por defecto”.
- **Reseña de proveedores externos:** Elastic colabora con los principales proveedores de IaaS (AWS, GCP, Azure) y realiza revisiones rigurosas de sus estándares de seguridad y cumplimiento, incluidas las auditorías SOC 2 y las certificaciones ISO 27001, como parte de su programa de gestión de riesgos de terceros.
- **Pruebas de penetración:** terceros independientes realizan pruebas anuales de penetración de aplicaciones y redes contra Elastic Cloud, como mínimo. Elastic también cuenta con un programa público de recompensas por errores para pruebas continuas de investigadores.
- **Formación de empleados:** todos los empleados de Elastic deben completar una formación integral en seguridad de la información y protección/privacidad de datos al ser contratados y al menos una vez al año a partir de entonces.

© 2025 Elasticsearch B.V. Todos los derechos reservados.