Hoja de datos de privacidad de Elastic

Servicios de soporte

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 servicio: Servicios de soporte de Elastic

Los servicios de soporte de Elastic proporcionan un sistema integral para que los clientes se comuniquen con Elastic y obtengan asistencia con sus productos Elastic, lo que incluye Elastic Cloud y despliegues autogestionados, así como sus características y funciones relacionadas. Los servicios de soporte se utilizan para abordar rápidamente las consultas técnicas y resolver problemas, aprovechando tanto la experiencia humana de un equipo global de ingenieros de soporte como las herramientas impulsadas por AI, como el asistente de soporte.

- **Tipo de producto:** servicios de soporte
- **Modelo(s) de despliegue:**
    - Hospedado/Administrado

Datos que se procesan en los servicios de soporte de Elastic

Los servicios de soporte de Elastic procesan datos personales como parte de la prestación del servicio. Los tipos específicos de datos personales procesados dependen de la información proporcionada por el cliente durante las interacciones de soporte y de la naturaleza del problema técnico.

Categorías de datos personales necesarios para acceder y usar los Servicios de soporte:

- Identificadores de administrador y usuario, credenciales, permisos, cookies de sesión y registros de actividad. El procesamiento de estos datos es esencial para gestionar el acceso seguro y el uso auditable del sistema de soporte.
- Contactos de soporte proporcionados por el cliente según su nivel de suscripción.
- Datos de contacto comercial recopilados cuando el cliente se comunica con el soporte de Elastic, como nombre, dirección de correo electrónico y número de teléfono.

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

- Datos personales del cliente contenidos en casos de soporte y comentarios.
    - Ejemplos: información relacionada con consultas técnicas, problemas y comunicaciones intercambiadas con el soporte de Elastic.
- Archivos de diagnóstico (información de tiempo de ejecución y metadatos del cluster): la herramienta de diagnóstico de soporte recopila datos sobre la condición de los nodos y otros metadatos del cluster. Esto incluye las salidas de varias API de Elasticsearch y llamadas al sistema. Dependiendo de los despliegues y la infraestructura del cliente, esos datos de diagnóstico pueden contener información que permita identificar, directa o indirectamente, a los usuarios finales del cliente. Sin embargo, Elastic no monitorea ni filtra este tipo de contenido:
    - La herramienta de diagnóstico de soporte **no** recopila los datos reales del evento de origen o del documento almacenados en tu cluster.
    - Los clientes tienen la opción de realizar una depuración adicional de los archivos de diagnóstico, eliminando metadatos sensibles como direcciones IP, nombres de host y nombres de índices antes de compartirlos con Elastic.
- Contenido de los archivos subidos para la resolución de problemas, como volcados de memoria, siempre que el cliente lo autorice expresamente.
- Prompts y respuestas de modelos de lenguaje de grande (LLM) cuando se utiliza el Asistente de soporte dentro del contexto de soporte.

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

- Datos derivados del uso o generados a partir del uso de funcionalidades de AI generativa y agéntica, necesarios o relevantes para operar, optimizar, mejorar y supervisar el rendimiento de estas tecnologías y/o para cumplir con requisitos regulatorios y legales.

Finalidades típicas del procesamiento de los datos de los clientes compartidos con el servicio de asistencia:

En general, los servicios de soporte de Elastic están diseñados y destinados a casos de uso como:

- Facilitar la comunicación y la interacción entre los clientes y el equipo de soporte de Elastic para resolver problemas y responder preguntas.
- Proporcionar respuestas de autoservicio a consultas técnicas con el asistente de soporte impulsado por GenAI.
- Colaborar en la ingesta de datos, el escalado del despliegue y el acceso a información para generar un impacto empresarial.
- Permitir la gestión de casos, que incluye la creación, revisión y actualización de casos de soporte.
- Facilitar la resolución colaborativa de problemas y el intercambio seguro de información, lo que incluye fragmentos de código en Markdown o archivos de gran tamaño.
- Diagnosticar y solucionar problemas técnicos analizando el rendimiento del cluster, la configuración, el mapping de campos y el estado general del cluster utilizando archivos de diagnóstico.
- Gestionar tus suscripciones y licencias de clientes.
- Brindar asesoramiento y orientación especializados sobre el software de Elastic a través de ingenieros de soporte con amplia experiencia.
- Supervisar la eficacia y precisión de nuestros sistemas mediante las interacciones del usuario.

Datos de uso del producto

Los servicios de soporte de Elastic, como parte del ecosistema más amplio de Elastic, recopilan automáticamente cierta información relacionada con el uso del servicio. Dichos datos de uso del producto se procesan como se describe en la Declaración de privacidad del producto de Elastic.

Acceso a los datos de los clientes

- **Acceso por parte de los clientes:** el centro de soporte de Elastic está completamente integrado con Elastic Cloud. Los usuarios con una suscripción activa pueden acceder con su cuenta de Elastic Cloud y crear y revisar casos de soporte, recibir actualizaciones, descargar licencias y consultar la información de su suscripción. Todos los datos de soporte previos, incluidos casos, comentarios, suscripciones y licencias, siguen siendo accesibles en el portal. Todas las cuentas de Elastic Cloud pueden acceder al Centro de soporte, independientemente de si tienen algún despliegue en el cloud en ejecución. Los controles de acceso basados en roles (RBAC) están integrados en los despliegues de Elastic, lo que permite a los administradores de clientes definir roles que limitan el acceso del usuario a información específica, al aplicar los principios de privilegio mínimo.

- **Acceso por parte de Elastic:** el soporte de Elastic normalmente maneja “metadatos” (datos indirectos y no identificables) para solucionar problemas, como archivos de registro, archivos de configuración y diagnósticos de productos, en lugar de contenido real del cliente, datos personales del cliente, bases de datos directas o datos de identificación del usuario final.

    - En casi todos los casos de soporte técnico u operaciones, los ingenieros de Elastic no acceden al contenido de los datos de los clientes almacenados en los índices de datos, ni tienen acceso directo a los documentos o sistemas de archivos de los clientes. Elastic solo accederá al contenido del cliente en despliegues en el cloud siguiendo las instrucciones del cliente, por ejemplo, al proporcionar servicios de soporte a petición del cliente. Si surge algún problema excepcional que requiera acceder al contenido del cliente (por ejemplo, un volcado de memoria), es obligatorio contar con la autorización por escrito del cliente. Estos procesos están estrictamente controlados, son completamente auditables y cumplen con los estándares de cumplimiento como SOC 2 e ISO 27001.

    - La herramienta de diagnóstico de soporte es empleada por el soporte de Elastic para entender el estado del cluster del cliente, pero no recopila datos reales de eventos de origen ni documentos almacenados en el cluster del cliente; solo recopila información en tiempo de ejecución y metadatos del cluster. Esta salida de diagnóstico se puede depurar aún más eliminando metadatos confidenciales como direcciones IP, nombres de host o nombres de índices antes de compartirla con Elastic.

    - 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 servicios de soporte se aprovisionan a través de ciertos subprocesadores de soporte. Estos subprocesadores están contractualmente obligados a proporcionar un nivel equivalente de protección de datos al 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 sirve como un recurso integral para obtener información sobre sus prácticas de privacidad y esfuerzos de cumplimiento.

- **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 con el GDPR:** los Servicios de soporte de Elastic están diseñados para cumplir con el 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 dedicado equipo de privacidad en 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.
- **Transferencias transfronterizas de datos:** Elastic también autoriza las transferencias de datos personales procedentes del EEE, Suiza o el Reino Unido, basándose en las cláusulas contractuales estándar vigentes y en su participación en el Marco de privacidad de datos para las transferencias a Estados Unidos. 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 de la UE para el alojamiento.

Retención y eliminación

Los archivos cargados en el centro de soporte de Elastic se purgan automáticamente 30 días después de la carga para proteger la información confidencial. El sistema de tickets utilizado por el Servicio de soporte elimina todos los archivos adjuntos de los casos 15 días después del cierre del caso.

Seguridad

La seguridad de tus datos dentro de Elastic Cloud depende de que mantengas tus despliegues configurados de forma segura y la confidencialidad de tus credenciales de inicio de sesión de Elastic Cloud (consulta nuestras Preguntas frecuentes sobre seguridad para obtener más información). Además, Elastic soporta un modelo integral de seguridad 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. Elastic también emplea Elastic Security para sus propias operaciones internas de InfoSec.

- **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 ante amenazas de Elastic usa flujos de trabajo automatizados para detectar e investigar actividades sospechosas en cuentas internas y accesos no autorizados.

- **Actualizaciones y parches del sistema:** los sistemas de Elastic se actualizan y se despliegan regularmente con base en los kernels más recientes del sistema operativo. Los parches adecuados se aplican de inmediato cada vez que se identifica una Common Vulnerabilities and Exposures (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 auditorías SOC 2 y 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 para Elastic Cloud. 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.