Hoja de datos de privacidad de Elastic

Observability

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: Elastic Observability

Elastic Observability proporciona información detallada y contexto sobre el comportamiento de las aplicaciones que se ejecutan en tus entornos, lo que permite una rápida detección y resolución de eventos de causa raíz. Ofrece un único stack para unificar tus registros, métricas de infraestructura, trazas de aplicaciones, datos de experiencia de usuario, Synthetics y Universal Profiling. Los datos se ingieren directamente en Elasticsearch, donde se pueden procesar y mejorar antes de la visualización y las alertas en Kibana. La solución Observability está diseñada para acelerar la resolución de problemas con una observabilidad abierta, flexible y unificada impulsada por machine learning y analítica avanzada.

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

Datos procesados en Elastic Observability

Elastic Observability procesa los datos operativos de telemetría que los clientes ingieren para monitorear sus sistemas y aplicaciones. Los tipos específicos de datos personales procesados dependen de los datos ingeridos por el cliente y de su configuración. Elastic ofrece la plataforma y las herramientas para gestionar estos datos, que pueden incluir datos personales dependiendo de la naturaleza de los registros, las métricas, los rastros de aplicaciones o los datos de experiencia del usuario.

Categorías de datos personales necesarios para acceder y utilizar Elastic Observability:

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

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

- Identificadores individuales y datos de actividad del sistema o la red a partir de registros, métricas y rastros:
    - Ejemplos: ID de usuario, direcciones IP, nombres de host, nombres de máquinas, ID de proceso, nombres de archivo, rutas de directorio, URL, direcciones de correo electrónico (si están presentes en registros o mensajes de error), identificadores de dispositivos móviles y datos de ubicación del monitoreo de la experiencia del usuario.
- Datos sobre el rendimiento de la aplicación:
    - Ejemplos: detalles de transacciones, intervalos, errores, métricas y metadatos recogidos de aplicaciones, que podrían contener datos específicos del usuario si no son desinfectados por el cliente.
- Datos de experiencia de usuario:
    - Ejemplos: datos relacionados con el rendimiento percibido de aplicaciones de sitios web por usuarios reales, que pueden incluir tipos de navegadores, sistemas operativos y datos de ubicación generalizados.

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

Finalidades típicas del procesamiento de datos de clientes que se envían a Elastic Observability:

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, Elastic Observability está diseñada y destinada a casos de uso como:

- Proporcionar información detallada y contexto sobre el comportamiento de las aplicaciones.
- Unificar y correlacionar registros, métricas de infraestructura, trazas de aplicaciones, datos de experiencia del usuario, Synthetics y Universal Profiling para una detección más rápida de la causa raíz.
- Analizar datos de logs de diversas fuentes, como hosts, servicios, Kubernetes y Apache.
- Instrumentar el código y recopilar datos de rendimiento y errores en tiempo de ejecución mediante el monitoreo de rendimiento de aplicaciones (APM).
- Monitorear las métricas del sistema y de los servicios, como servidores, Docker, Kubernetes y otras aplicaciones.
- Cuantificar y analizar el rendimiento percibido de las aplicaciones web a través del monitoreo real de usuarios (RUM).
- Simular las acciones y solicitudes de los usuarios en un sitio web en intervalos predefinidos, en entornos controlados, mediante el monitoreo sintético, y generar datos coherentes y repetibles para analizar tendencias y generar alertas.
- Crear trazas de stack y obtener visibilidad del rendimiento del sistema sin requerir cambios en el código fuente de la aplicación ni instrumentación, lo que ayuda a identificar líneas de código costosas, aumentar la eficiencia de la CPU y depurar regresiones de rendimiento (Universal Profiling).
- Detectar anomalías y picos en datos temporales, e investigar las causas de cambios inusuales en las tasas de logs o distribuciones de métricas al aprovechar los análisis predictivos y el machine learning.
- Para alertar sobre posibles problemas en entornos basados en reglas y umbrales definidos, integrándose con monitoreo de registros y APM.
- Establecer objetivos claros y medibles para el rendimiento del servicio y monitorear los objetivos de nivel de servicio (SLO) en tiempo real.
- Recopilar y compartir información sobre problemas de observabilidad mediante la creación de casos, lo que facilita la colaboración entre equipos y la integración con sistemas de terceros como ServiceNow y Jira.

Datos de uso del producto

Elastic Observability recopila automáticamente cierta información relacionada con el uso del producto. Esos datos de uso del producto se tratan tal y como se describe en la Declaración de privacidad de los 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 los ajustes de configuración del producto (consulta la Documentación del producto correspondiente). 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 de los clientes

- **Acceso por parte de los clientes:** los clientes mantienen el control total sobre los datos que ingieren en la Elastic Observability. Pueden acceder y analizar sus datos de observabilidad a través de la interfaz de usuario de Kibana, que ofrece capacidades para buscar, filtrar, visualizar y analizar registros, trazas y datos métricos. Los clientes pueden obtener datos directamente usando la API REST de Elasticsearch o a través

de varios clientes de Elasticsearch. Los controles de acceso basados en roles están disponibles en Kibana para gestionar el acceso de usuario a contenido y características específicas, asegurando la adherencia a 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, estrictamente para actividades esenciales de gestión, mantenimiento y soporte de la plataforma. Este acceso se basa en los principios de menor privilegio y necesidad de saber, y está sujeto a revisiones y ajustes regulares. Elastic no tiene acceso a datos dentro de despliegues autogestionados que no estén conectados al cloud, y solo accederá al contenido del cliente en despliegues en el cloud bajo las instrucciones del cliente (por ejemplo, cuando presta 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 nuestra solución Observability 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 hospedar sus despliegues.

Subprocesamiento: Elastic emplea cierta infraestructura y subprocesadores 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 obligados contractualmente 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 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.

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

- **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 Elastic Observability. Puedes 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 personales que recopilan y procesan en el entorno de Elastic.
- Elastic puede ayudar a identificar datos no utilizados y orientar 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.

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

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.

- **Cifrado:** los datos del cliente se cifran en reposo usando 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:** las instancias de Elasticsearch se actualizan y despliegan regularmente según los kernels del sistema operativo más recientes. Se aplican los parches correspondientes de forma oportuna cada vez que se identifica una vulnerabilidad o exposición común (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 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.