Hoja de datos de privacidad de Elastic

Seguridad

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 Security

Elastic Security combina análisis de detección de amenazas, seguridad nativa del cloud y capacidades de protección de endpoints en una única solución unificada. Permite a las organizaciones detectar, investigar y responder rápidamente a amenazas cibernéticas y vulnerabilidades en todo su entorno mediante análisis de seguridad impulsados por AI. Aprovechando la Search AI Platform, Elastic Security ayuda a los clientes a abordar numerosas amenazas a escala, lo que reduce eficazmente la fatiga por alertas y permite investigaciones rápidas sobre la relevancia de los hallazgos de seguridad.

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

Datos procesados en Elastic Security

Elastic Security procesa datos de eventos de seguridad y otra información relacionada que los clientes ingieren para la detección, investigación y respuesta ante amenazas. Los tipos específicos de datos que se procesan dependen del entorno del cliente y de las configuraciones de logging. Los clientes pueden ingerir datos de diversas fuentes, incluidos logs, datos de entrenamiento y salidas de modelos de machine learning, para su análisis de seguridad.

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

- 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.

- Cualquier dato personal contenido incidentalmente en indicadores de ciberamenazas (por ejemplo, identificadores de red no confiables, muestras, hashes y rutas de ejecutables sospechosos y otros archivos) que Elastic Security deba procesar para ofrecer determinadas funcionalidades de seguridad. Ten en cuenta que algunas de estas características solo pueden funcionar si se comunican con los servidores de fondo de Elastic (p. ej., la consulta de reputación y las bases de datos de inteligencia sobre amenazas). Los clientes que, a su entera discreción, decidan deshabilitar dichas funcionalidades o bloquear esas comunicaciones entre implementaciones autogestionadas o híbridas del producto y los servidores de backend de Elastic deben comprender y reconocer que esto dará lugar a una funcionalidad reducida del producto y a un menor rendimiento en materia de seguridad.

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

- Identificadores individuales y datos de actividad de red/sistema a partir de los registros de eventos de seguridad:

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

    - Ejemplos: ID de usuario, nombres de usuario, direcciones de correo electrónico, direcciones IP, direcciones MAC, nombres de host, rutas de directorio, nombres de archivos, URL.

- Datos de inteligencia sobre amenazas:
    - Ejemplos: información relacionada con amenazas conocidas, que puede incluir identificadores si está vinculada a entidades o campañas maliciosas específicas.

- Cualquier dato ingerido para análisis forense, generación de informes de cumplimiento o análisis de seguridad impulsado por AI:
    - Ejemplos: documentación técnica, detalles de los datos de entrenamiento, registros operativos, prompts y respuestas de modelos de lenguaje de gran tamaño (LLM) (si se utilizan AI Assistant o Attack Discovery) y datos de todo el flujo de decisiones (desde los datos de entrada hasta los resultados finales de seguridad).

- Metadatos de entornos en el cloud y endpoints para la gestión de la postura de seguridad:
    - Ejemplos: detalles de configuración para activos en el cloud de AWS, GCP y Azure, recursos de Kubernetes y máquinas virtuales que pueden contener información identificable.

Finalidades típicas del tratamiento de los datos de los clientes que se envían a Elastic Security:

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 Security está diseñado y pensado para casos de uso como:

- Detectar, investigar y responder a amenazas cibernéticas y vulnerabilidades en todo el entorno de TI.
- Identificar una amplia gama de amenazas utilizando un sofisticado motor de detección.
- Proporcionar un espacio de trabajo centralizado para la priorización de eventos, investigación y gestión de casos.
- Ofrecer herramientas interactivas de visualización de datos para obtener información detallada sobre la seguridad.
- Habilitar integraciones que permitan recopilar datos de seguridad de diversas fuentes, incluidos endpoints, servidores y servicios en el cloud.
- Para proporcionar capacidades de seguridad nativas de la nube, como Cloud Security Posture Management (CSPM), Kubernetes Security Posture Management (KSPM), Cloud Native Vulnerability Management (CNVM) y protección de cargas de trabajo en la nube.
- Habilitar capacidades de protección de endpoints, lo que incluye la recopilación de eventos y la prevención de actividades maliciosas, a través de Elastic Defend.
- Identificar comportamientos maliciosos al aprovechar las herramientas integradas de machine learning y las detecciones avanzadas de comportamiento.
- Generar análisis de riesgo integrales para usuarios y hospedajes a través de analíticas avanzadas de entidades y puntuación de riesgo de entidades.
- Ayudar a los analistas de seguridad con un asistente de AI para resolver dudas sobre Elastic Security, entender las alertas y generar consultas ES|QL.

- Facilitar Attack Discovery, que utiliza modelos de lenguaje de gran tamaño (LLM) para analizar múltiples alertas e identificar posibles ataques, detallando los usuarios y hosts involucrados y realizando el mapeo al marco MITRE ATT&CK.
- Habilitar el monitoreo proactivo del entorno a través de reglas y alertas de detección prediseñadas y personalizadas.
- Evaluar la composición e identificar posibles sesgos o lagunas en los datos de entrenamiento que puedan afectar al rendimiento y la equidad de los sistemas de AI, y comparar los resultados entre diferentes grupos demográficos para prevenir la discriminación algorítmica.

Datos de uso del producto

Elastic Security recopila automáticamente cierta información relacionada con el uso del producto. Esos datos de uso del producto, que son distintos y no guardan relación con los indicadores de amenazas cibernéticas mencionados anteriormente, se tratan tal y como se describe en la Declaración de privacidad del producto 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 Elastic Security. Pueden acceder y analizar datos de seguridad a través de la UI de Elastic Security en Kibana, ya sea en Elastic Cloud o en despliegues autogestionados. Kibana ofrece varios dashboards (p. ej., visión general, detección y respuesta, postura de seguridad en el cloud) para visualizar, ordenar y filtrar datos y alertas. Los clientes pueden usar una poderosa consulta DSL para explorar sets de datos para la detección de sesgos y filtrar datos para comparar resultados entre grupos demográficos. Attack Discovery proporciona información sintetizada sobre posibles ataques, que detalla los usuarios y hosts involucrados. Los clientes pueden crear casos para hacer un seguimiento de las investigaciones, añadir alertas y colaborar con los equipos, además de aprovechar el asistente de AI para hacer preguntas sobre los hallazgos y las medidas correctivas. Los RBAC están integrados en Elastic Security y Kibana, lo que permite a los administradores definir roles que limiten el acceso de usuario a índices, dashboards o acciones específicas, 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 actividades esenciales de gestión, mantenimiento y soporte de 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 los clusters ni al contenido del cliente en los despliegues autogestionados, y solo accederá al contenido del cliente en los despliegues de Elastic Cloud luego de obtener la autorización por escrito del cliente (por ejemplo, cuando sea necesario para proporcionar 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 Security se alojan en plataformas cloud certificadas gestionadas por proveedores líderes en IaaS del sector, como 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. 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 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 Security y descargar alertas y reportes generados por Elastic Security. Esto es compatible con las necesidades del cliente para las solicitudes de acceso de los interesados y la exportación de datos para su posterior análisis o integración.

Retención y eliminación

Elastic proporciona herramientas y capacidades que permiten a los clientes administrar sus políticas de retención y eliminación de datos de manera efectiva para registros y datos de seguridad.

- Los clientes tienen la capacidad de definir y hacer cumplir políticas de retención para los datos que recopilan y procesan dentro del entorno de Elastic.
- Elastic ofrece soporte para la retención de logs a largo plazo y proporciona opciones de almacenamiento rentables utilizando su estructura de niveles de datos, lo que garantiza que todos los datos permanezcan inmediatamente accesibles para el análisis.
- 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 de los datos personales

La seguridad y la privacidad de tus datos en Elastic Cloud también dependen de que mantengas tus despliegues configurados de forma segura y de que protejas la confidencialidad de tus credenciales de inicio de sesión en 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. También empleamos Elastic Security para nuestras propias operaciones internas de InfoSec.

- **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 para el acceso administrativo. Además, los controles de acceso basados en roles 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. Elastic Security se destaca por su capacidad para agregar, almacenar y analizar registros a gran escala, lo que permite realizar análisis y visualizaciones en tiempo real. También admite capacidades sólidas de alerta y detección de anomalías.
- **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 en cualquier componente de software.
- **Detección y respuesta de incidentes:** Elastic implementó y actualiza continuamente las reglas de detección para actividades sospechosas y accesos no autorizados, incluyendo el monitoreo de integridad de archivos e indicadores de apropiación de cuenta. 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”.
- **Evaluación de proveedores terceros:** 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 contra 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 momento de ser contratados y al menos una vez al año después.