Elastic Privacy Datasheet

Security

Product Summary: Elastic Security

Elastic Security combines threat detection analytics, cloud native security, and endpoint protection capabilities into a single, unified solution. It empowers organizations to quickly detect, investigate, and respond to cyber threats and vulnerabilities across their entire environment through AI-driven security analytics. Leveraging the Elasticsearch AI Platform, Elastic Security helps customers address numerous threats at scale, effectively reducing alert fatigue and enabling rapid investigation into the relevance of security findings.

- **Product type:** Software
- **Deployment model(s):**
    - On-premises (self-managed)
    - Cloud (SaaS) (Elastic Cloud Hosted, Elastic Cloud Serverless)
    - Hybrid

Data Processed in Elastic Security

Elastic Security processes security event data and other related information that customers ingest for threat detection, investigation, and response. The specific types of data processed depend on the customer's environment and logging configurations. Customers may ingest data from diverse sources, including logs, training data, and outputs from machine learning models, for security analysis.

Categories of personal data necessary to access and use the Elastic Security:

- Admin and user identifiers, credentials, permissions, session cookies and activity logs. The processing of such data is necessary for the purposes of product deployment, configuration, administration, management, secure access, and auditable use.

- Any personal data incidentally contained in cyberthreat indicators (e.g., untrusted network identifiers, samples, hashes and paths of suspicious executables and other files) which Elastic Security must process in order to deliver certain security features. Note that some of these features can only operate if they communicate with Elastic back-end servers (e.g., reputation lookup and threat intelligence databases). Customers who, at their sole discretion, choose to disable such features or to block such communications between self-managed or hybrid deployments of the product and the Elastic back-end servers must understand and acknowledge that this will result in diminished product functionality and lesser security performance.

Additional categories of personal data processed may include, but are not limited to, data contained within:

- Individual identifiers and network/system activity data from security event logs:
    - Examples**:** User IDs, usernames, email addresses, IP addresses, MAC addresses, hostnames, directory paths, filenames, URLs.

- Threat intelligence data:

    - Examples**:** Information related to known threats, which may contain identifiers if linked to specific malicious entities or campaigns.

- Any data ingested for forensic analysis, compliance reporting, or AI-driven security analysis:
    - Examples**:** Technical documentation, details from training data, operational logs, Large Language Model (LLM) prompts and responses (if AI Assistant or Attack Discovery are used), and data from the full decision pipeline (from input data to final security outcomes).

- Metadata from cloud environments and endpoints for security posture management:
    - Examples**:** Configuration details for AWS, GCP, and Azure cloud assets, Kubernetes resources, and virtual machines that may contain identifiable information.

Typical Purpose(s) of Processing Customer Data Fed to Elastic Security:

In their specific deployments, customers have sole discretion to determine the actual purpose(s) of processing of any data they choose to feed to the product. In general, Elastic Security is designed and intended for use cases such as:

- To detect, investigate, and respond to cyber threats and vulnerabilities across the IT environment.
- To identify a wide range of threats using a sophisticated detection engine.
- To provide a centralized workspace for event triage, investigation, and case management.
- To offer interactive data visualization tools for comprehensive security insights.
- To enable integrations for collecting security data from various sources, including endpoints, servers, and cloud services.
- To provide cloud native security capabilities, such as Cloud Security Posture Management (CSPM), Kubernetes Security Posture Management (KSPM), Cloud Native Vulnerability Management (CNVM), and cloud workload protection.
- To enable endpoint protection capabilities, including event collection and malicious activity prevention, through Elastic Defend.
- To identify malicious behavior by leveraging built-in machine learning tools and advanced behavioral detections.
- To generate comprehensive risk analytics for hosts and users through advanced entity analytics and entity risk scoring.
- To support security analysts with an AI Assistant for inquiries about Elastic Security, understanding alerts, and generating ES|QL queries.
- To facilitate Attack Discovery, which uses LLMs to analyze multiple alerts and identify potential attacks, detailing involved users and hosts, and mapping to the MITRE ATT&CK framework.
- To enable proactive monitoring of the environment through prebuilt and custom detection rules and alerts.

- To assess the composition and identify potential biases or gaps in training data that could affect AI system performance and fairness, and to compare outcomes across different demographic groups to prevent algorithmic discrimination.

Product Usage Data

Elastic Security automatically collects certain information related to the use of the product. Such Product Usage Data – which is different from and unrelated to the cyberthreat indicators referenced earlier – is processed as described in the Elastic Product Privacy Statement. In on-premises and certain hybrid deployment models, customers may restrict or disable Product Usage Data processing in the product's configuration settings (please refer to the applicable product Documentation). However, such Product Usage Data collection and processing is indispensable to the proper functioning of the product in Cloud (SaaS) deployment models.

Access to Customer Data

- **Access by Customers:** Customers retain full control over the data they ingest into Elastic Security. They can access and analyze security data through the Elastic Security UI in Kibana in either Elastic Cloud or self-managed deployments. Kibana offers various dashboards (e.g., Overview, Detection & Response, Cloud Security Posture) for visualizing, sorting, and filtering data and alerts. Customers can use a powerful query DSL to explore datasets for bias detection and filter data to compare outcomes across demographic groups. Attack Discovery provides synthesized insights into potential attacks, detailing involved users and hosts. Customers can create cases to track investigations, add alerts, and collaborate with teams, also leveraging the AI Assistant to ask questions about discoveries and remediation. Role-based access controls are built into Elastic Security and Kibana, allowing administrators to define roles that limit user access to specific indices, dashboards, or actions, thereby enforcing least-privilege principles.

- **Access by Elastic:** For Elastic Cloud offerings, a limited number of Elastic employees are granted privileged access to the production environment solely for essential platform management, maintenance, and support activities. This access is provisioned based on the principles of least-privilege and need-to-know and is subject to regular review and adjustment. Elastic does not have access to clusters or to the Customer Content within self-managed deployments, and will only access Customer Content in Elastic Cloud deployments after obtaining written authorization from the customer (e.g. when necessary to provide Support Services at the customer's request).

    - Elastic has implemented centralized logging, encompassing proxy logs, access logs, Elasticsearch logs, and Auditbeat logs to record all access to customer data and the systems on which it resides. Elastic's internal teams actively develop and implement detections for suspicious internal account activity and unauthorized access, including file integrity monitoring and account takeover indicators.

- Elastic's principles dictate that it will only disclose or provide access to customer data when strictly compelled by law, and it includes established protocols for challenging such requests and notifying relevant parties where legally permissible.

Processing Locations

Elastic Cloud deployments of our Security solution are hosted on certified cloud platforms managed by industry-leading IaaS providers that include Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. Customers can select the geographic region where they want to host their deployments.

Sub-Processing: Elastic utilizes certain infrastructure and customer support sub-processors to deliver its services. The specific sub-processors involved depend on the data center location, services, and functionalities chosen by the customer. These sub-processors are contractually bound to provide a level of data protection at least equivalent to that described in the Elastic Information Security Addendum. Elastic maintains full transparency regarding its sub-processors (see internal and external lists) and is liable for their actions and omissions to the same extent as if Elastic performed the services itself.

Compliance with Privacy Regulations

Elastic captures, processes, stores, and protects Customer Personal Data in accordance with the applicable customer Data Processing Addendum. Our Trust Center serves as a comprehensive resource for information on its privacy practices and compliance efforts.

- **Data Ownership:** Customer data remains the property of the customer. Elastic only processes this data for the purposes specified in the customer's agreement, and never sells customer data to third parties.
- **GDPR Compliance:** Elastic Cloud features are designed to support compliance with the General Data Protection Regulation and other global data protection and privacy laws. This includes prioritizing the security of personal data through effective technical and organizational measures, offering a GDPR-compliant Data Processing Addendum. Our dedicated privacy team at Elastic oversees GDPR compliance.
- **Data Privacy Framework (DPF):** Elasticsearch, Inc. is certified under the EU-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework as set forth by the U.S. Department of Commerce.
- **Cross-Border Data Transfer:** Elastic legalizes transfers of personal data across the jurisdictions where we operate by relying on current Standard Contractual Clauses, and on our participation in the Data Privacy Framework for transfers to the U.S. and from there onwards. Additionally, we implement robust supplementary measures to protect data during transfers, such as encryption in transit and at rest, protocols for challenging public authority requests, and providing customers with the option to select regional servers for hosting.

Data Portability

Customers can easily manage the portability of their data from Elastic Security and can download alerts and reports generated by Elastic Security. This supports customer needs for data subject access requests and exporting data for further analysis or integration.

Retention and Deletion

Elastic provides tools and capabilities that enable customers to manage their data retention and deletion policies effectively for security logs and data.

- Customers have the ability to define and enforce retention policies for the data they collect and process within the Elastic environment.
- Elastic supports long-term log retention and provides cost-effective storage options using its data tiering structure, ensuring all data remains immediately accessible for analysis.
- Logstash, an Elastic component, can be used to perform data transformation, including anonymization and pseudonymization, which helps achieve data minimization goals and reduces data security risks.
- Elastic's platform enables organizations to more closely analyze their actual use of retained personal data, allowing them to tailor data retention periods and policies more effectively.
- For data subject deletion requests, Elastic provides capabilities to tag data for retention under an exception, or to permanently delete data using permissible deletion and de-identification techniques such as anonymization, to help customers remain compliant within short response timeframes.

Security of Personal Data

The security and privacy of your Elastic Cloud data also relies on you keeping your deployments configured securely and maintaining the confidentiality of your Elastic Cloud login credentials (please see our Security FAQ for more information). Elastic supports a comprehensive defense-in-depth security model designed to protect customer data throughout its entire lifecycle: in transit, at rest, and in memory, as well as through robust key management procedures. We also use Elastic Security for our own internal InfoSec operations.

- **Encryption:** Customer data is encrypted at rest using AES-256 and in transit via TLS 1.2. Elastic implements strict encryption key management procedures.
- **Access Controls:** Elastic maintains technical, logical, and administrative controls to restrict data access solely to authorized users. These controls include measures such as multi-factor authentication, strong password strength standards, and the use of Virtual Private Networks for administrative access. Additionally, Role-based Access Controls are integrated into Elastic deployments and the Elastic Cloud management platform, allowing granular control over user permissions.
- **Logging and Monitoring:** Elastic has implemented centralized logging, encompassing proxy logs, access logs, Elasticsearch logs, and Auditbeat logs to record all access to customer data and the systems on

which it resides. Elastic Security excels in aggregating, storing, and analyzing logs at scale for real-time analysis and visualization. It also supports robust alerting and anomaly detection capabilities.

- **System Updates and Patches:** Elasticsearch instances are regularly updated and deployed based on the latest operating system kernels. Appropriate patches are applied promptly whenever a Common Vulnerability and Exposure is identified in any component software.
- **Incident Detection and Response:** Elastic has implemented and continuously updates detection rules for suspicious activity and unauthorized access, including file integrity monitoring and account takeover indicators. These detections are part of automated workflows that alert the Threat Detection and Response team, triggering analyst investigations. Elastic uses Elastic Security internally which includes Endpoint Detection and Response capabilities and integrates threat intelligence feeds to support intrusion detection. It supports automated responses through integrations with third-party SOAR platforms, reducing the likelihood of a breach and speeding response times.
- **Secure Software Development Framework (SSDF):** Elastic maintains a secure software development framework based on NIST 800-218. This framework guides the process to securely design, develop, deploy, track, and maintain all Elastic software, ensuring a "secure by design" and "secure by default" approach.
- **Third-Party Vendor Review:** Elastic partners with major IaaS providers (AWS, GCP, Azure) and conducts rigorous reviews of their security and compliance standards, including SOC 2 audits and ISO 27001 certifications, as part of its third-party risk management program.
- **Penetration Testing:** Independent third parties conduct annual application and network penetration tests against Elastic Cloud. Elastic also hosts a public Bug Bounty Program for continuous researcher testing.
- **Employee Training:** All Elastic employees are required to complete comprehensive information security and data protection/privacy training upon hire and at least annually thereafter.