Elastic 隐私数据表

Elasticsearch

产品摘要：Elasticsearch

Elasticsearch 使组织能够利用 Elastic 的统一平台，为网站、应用程序和企业数据构建强大的搜索体验。它支持由 AI 和机器学习驱动的搜索应用程序。Elasticsearch 利用 Elasticsearch 的向量数据库、AI 工具包和高级检索功能来支持搜索和检索增强生成 (RAG) 应用。它针对生产规模级的工作负载进行了速度与相关性的优化，允许用户近乎实时地对各种形式和规模的数据进行搜索、索引、存储和分析。

- **产品类型：**软件
- **部署模式：**
    - 本地部署（自管理）
    - 云 (SaaS) (Elastic Cloud Hosted, Elastic Cloud Serverless)
    - 混合

在 Elasticsearch 中处理的数据

Elasticsearch 处理客户为各种搜索应用所摄入的数据。由于 Elastic 主要提供的是数据处理平台，因此所处理的个人数据的具体类型完全取决于客户的数据及配置。

访问和使用 Elasticsearch 所需的个人数据类别：

- 管理员和用户标识符、凭据、权限、会话 cookie 和活动日志。处理此类数据对于产品部署、配置、治理、管理、安全访问和确保使用过程可供审计至关重要。

所处理的其他个人数据类别可能包括但不限于包含在以下内容中的数据：

- 客户向产品提供的任何数据（根据客户的用例，可能包括个人数据）。
    - 示例：用户查询、网站内容、产品目录、知识库、工作场所文档、客户支持互动，以及用于训练 AI 模型或 RAG 应用的数据。
- 与搜索活动有关的在线标识符和使用数据：
    - 示例：IP 地址（如果是系统日志的一部分）、用户活动跟踪数据（用于优化搜索相关性）。

处理输入到产品中的客户数据的典型目的：

在具体部署中，客户可以自行决定其选择提供给产品的任何数据的实际处理目的。一般来说，Elasticsearch 是为以下使用场景而设计的：

- 为应用程序、网站和企业数据打造强大且无缝的搜索体验。
- 为客户和员工启用 AI 和机器学习驱动的搜索应用程序。
- 允许近乎实时地高效存储、索引、搜索和分析各种数据类型（结构化、非结构化、文本、数字和地理空间）。
- 通过执行最近邻搜索并将其与文本相结合，从而支持向量搜索和混合搜索能力，以获取相关结果。
- 通过分析并可视化网站及用户行为数据，识别用户查询趋势，从而提升搜索结果的相关性，进而优化客户与用户的搜索体验。
- 为聊天机器人和检索增强生成 (RAG) 等应用实现自然语言对话、提供上下文并维护知识。

产品使用数据

对于 Elastic Cloud 和自管理部署的 Elasticsearch，Elastic 均会自动收集与产品使用情况相关的某些信息。此类产品使用数据将按照 Elastic 产品隐私声明中所述的方式进行处理。在本地部署和某些混合部署模式中，客户可以在产品的配置设置中限制或禁用产品使用数据处理（请参阅适用的产品文档）。但是，在云 (SaaS) 部署模式中，此类产品使用数据的收集和处理对于产品的正常运行是必不可少的。

访问客户数据

- **客户访问：**客户对摄入到 Elasticsearch 的数据保留完全控制权。他们可以通过 Kibana 图形用户界面访问和管理他们的数据，该界面用于可视化和分析数据。客户可以利用 Elastic 强大的查询 DSL 来查询、探索和可视化数据集。通过 Elasticsearch 的 REST API 或适用于常见编程语言的 Elasticsearch 客户端也可以直接访问数据。基于角色的访问控制已集成到 Kibana 中，允许管理员定义角色，以限制用户对特定索引、仪表板或操作的访问，从而遵循最小权限原则。

- **Elastic 的访问：**对于 Elastic Cloud 产品与服务，仅有极少数 Elastic 员工拥有对生产环境的特权访问权限，且仅用于平台管理、维护及支持目的。此类访问权限严格遵循最小权限原则和按需知晓原则，并定期接受审查，且根据需要进行调整。Elastic 在自管理部署中无法访问数据，只有在客户指示下（例如应客户要求提供支持服务时）才会访问云部署中的客户内容。
    - Elastic 已实施集中式日志记录，包括代理日志、访问日志、Elasticsearch 日志和 Auditbeat 日志，以记录对客户数据及其所在系统的所有访问。Elastic 的内部团队积极开发和实施针对可疑内部账户活动和未经授权访问的检测，包括文件完整性监控和账户接管指标。

    - Elastic 的原则规定，只有在法律严格强制的情况下，其才会披露客户数据或提供对客户数据的访问权限，这些原则还包括挑战此类请求以及在法律允许的情况下通知相关方的既定规程。

处理地点

Elastic Cloud 部署的 Elasticsearch 托管在由行业领先的 IaaS 提供商管理的经认证云平台上，这些提供商包括 Amazon Web Services (AWS)、Google Cloud Platform (GCP) 和 Microsoft Azure。客户可以选择地理区域来托管其部署。

子处理：Elastic 利用特定的基础架构和客户支持子处理方来提供服务。具体涉及的子处理方取决于客户选择的数据中心位置、服务和功能。这些子处理方受合同约束，必须提供至少等同于 Elastic 信息安全附录中所述水平的数据保护。Elastic 对其子处理方保持完全透明（参见内部和外部列表），并为其行为和疏忽承担责任，其责任范围与 Elastic 自行提供服务时相同。

遵守隐私法规

Elastic 根据适用的客户数据处理附录和本隐私数据表中概述的承诺收集、处理、存储和保护客户个人数据。我们的信任中心是一个综合性资源平台，提供关于我们隐私实践与合规工作的各类信息。

- **数据所有权：**客户数据仍归客户所有。Elastic 仅为客户协议中指定的目的处理这些数据，并且绝不会将客户数据出售给第三方。
- **GDPR 合规性：**Elastic Cloud 功能在设计时即致力于支持遵守《通用数据保护条例》及其他全球数据保护和隐私法律。这包括通过有效的技术和组织措施优先保障个人数据安全，提供符合 GDPR 要求的数据处理附录。在 Elastic，我们拥有专门的隐私团队来监督 GDPR 的合规工作。
- **数据隐私框架 (DPF)：**Elasticsearch, Inc. 已通过由美国商务部制定的《欧盟-美国数据隐私框架》、《欧盟-美国数据隐私框架英国扩展版本》以及《瑞士-美国数据隐私框架》认证。
- ∉ **跨境数据传输：**Elastic 依据现行的标准合同条款及参与数据隐私框架（针对向美国的传输以及从美国发出的后续传输），在开展业务的各司法管辖区之间合法进行个人数据传输。此外，我们还实施强有力的补充措施以保护传输过程中的数据，如传输中加密和静态加密、对公共机构索要数据的请求提出挑战的程序，并为客户提供选择区域服务器的选项以托管数据。

数据可移植性

客户可以轻松管理其 Elasticsearch 数据的可移植性。他们可以通过 REST API 以及各种常用编程语言的 Elasticsearch 客户端检索存储在 Elasticsearch 中的数据。该功能可帮助客户履行数据主体访问请求的义务。此外，Elastic 还提供将 Kibana 仪表板和可视化内容导出为 PDF、PNG 或 CSV 文件等格式的选项。

保留和删除

Elastic 提供了工具和功能，使客户能够有效管理其数据保留和删除策略。

- 客户可以为其在 Elastic 环境中收集和处理的数据定义和执行保留策略。
- Elastic 允许客户将数据分类到存储层并查看访问日志，从而帮助识别未使用的数据并为数据保留实践提供信息。
- Logstash 作为 Elastic 组件，可用于执行数据转换，包括匿名化和假名化，有助于实现数据最小化目标，并降低数据安全风险。
- Elastic 的平台使组织能够更深入地分析其保留个人数据的实际使用情况，从而能够更有效地调整数据保留期限和政策。
- 针对数据主体的删除请求，Elastic 提供了相应的功能：既可对数据进行标记以作为例外情况予以保留，也可利用匿名化等合规的删除与去标识化技术对数据进行永久删除，从而协助客户在短响应时限内保持合规。

安全性

您的 Elastic Cloud 数据安全还依赖于保持稳妥配置 Elasticsearch 集群并维护 Elastic Cloud 登录凭证的机密性（详情请参阅我们的安全常见问题解答）。Elastic 支持一套全面的纵深防御安全模型，旨在于整个生命周期中保护客户数据，无论其处于传输中、静止中还是内存，并辅以稳健的密钥管理程序。

- **加密：**客户数据在静态下使用 AES-256 加密，在传输中通过 TLS 1.2 进行加密。Elastic 实施严格的加密密钥管理程序。
- **访问控制：**Elastic 实施技术、逻辑和管理控制措施，使数据访问权限限制在授权用户范围内。这些控制措施包括多因素身份验证、严格的密码强度标准以及使用虚拟专用网络 (VPN) 进行管理访问等。此外，基于角色的访问控制 (RBAC) 已集成到 Elastic 部署和 Elastic Cloud 管理平台中，允许对用户权限进行精细控制。
- **日志记录和监控：**Elastic 已实施集中式日志记录，包括代理日志、访问日志、Elasticsearch 日志和 Auditbeat 日志，以记录对客户数据及其所在系统的访问。Elastic 的威胁检测和响应团队利用自动化工作流来检测和调查可疑的内部账户活动和未经授权的访问，包括文件完整性监测和账户接管指标。
- **系统更新和补丁：**Elasticsearch 实例会定期根据最新的操作系统内核进行更新和部署。每当在任何组件软件中识别出常见漏洞与披露 (CVE) 时，我们都会及时应用相应的补丁。
- **事件检测与响应：**Elastic 已实施并持续更新针对可疑活动和未经授权访问的检测规则。这些检测是自动化工作流的一部分，可以向威胁检测与响应团队发出警报，并触发分析调查。Elastic 在内部使用 Elastic Security，该解决方案包括终端检测和响应功能，并集成了威胁情报源以支持入侵检测。它通过与第三方 SOAR 平台集成支持自动响应，从而降低了数据泄露的可能性并缩短了响应时间。
- **安全软件开发框架 (SSDF)：**Elastic 维护着一套基于 NIST 800-218 标准的安全软件开发框架。该框架指导着所有 Elastic 软件的安全设计、开发、部署、跟踪和维护过程，确保落实“设计即安全”和“默认安全”的原则。

- **第三方供应商审核：**Elastic 与主要 IaaS 提供商（AWS、GCP、Azure）开展合作，并按第三方风险管理计划对他们的安全与合规标准进行严格审核，包括审核其 SOC 2 审计报告和 ISO 27001 认证情况。
- **渗透测试：**Elastic Cloud 至少每年由独立的第三方机构进行应用程序和网络渗透测试。Elastic 还设有公开的漏洞赏金计划，供研究人员进行持续测试。
- **员工培训：**所有 Elastic 员工在入职时及之后至少每年都必须完成全面的信息安全和数据保护/隐私培训。