Elastic 隐私数据表

支持服务

服务摘要：Elastic 支持服务

Elastic 支持服务为客户提供一套全面的系统，使客户能够就 Elastic 产品（包括 Elastic Cloud 和自托管部署）及相关特性与功能向 Elastic 寻求帮助。支持服务旨在快速处理技术咨询并解决问题，借助全球支持工程师团队的专业经验以及 AI 驱动的工具（如支持助手）提供全面支持。

- **产品类型：**支持服务
- **部署模式：**
    - 托管/管理

在 Elastic 支持服务中处理的数据

Elastic 支持服务在交付服务时处理个人数据。具体处理的个人数据类型取决于客户在支持互动过程中提供的信息和技术问题的性质。

访问和使用支持服务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。处理此类数据对于管理支持系统的安全访问和确保使用过程可供审计至关重要。
- 客户根据其订阅级别提供的支持联系方式。
- 当客户联系 Elastic 支持时收集的业务联系数据，例如姓名、电子邮件地址和电话号码。

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：

- 包含在支持工单和评论中的客户个人数据。
    - 示例：与技术咨询、问题以及与 Elastic 支持团队交流的相关信息。
- 诊断文件（运行时信息和集群元数据）：支持诊断工具会收集节点的健康状况信息及其他集群元数据。这包括来自各种 Elasticsearch API 和系统调用的输出内容。根据客户的部署和基础设施情况，此类诊断数据可能包含可直接或间接识别客户最终用户的信息。但是 Elastic 不会监测或过滤此类内容：
    - 支持诊断工具**不会**收集存储在集群中的实际源事件或文档数据。
    - 客户可以选择在与 Elastic 共享之前，通过清除敏感元数据（如 IP、主机名和索引名称）来进一步清理诊断文件。
- 来自上传文件用于故障排除的内容，例如堆转储文件（经客户明确授权）。
- 大型语言模型 (LLM) 提示和响应（如果在支持场景下使用支持助手）。
- 源自或产生于使用生成式及智能体 AI 功能的数据，此类数据对于运行、优化、改进及监控相关技术的性能和/或满足监管与法律要求而言是必要或重要的。

处理与支持部门共享的客户数据的典型目的：

一般而言，Elastic 的支持服务是为以下使用场景而设计的：

- 促进客户与 Elastic 支持之间的沟通和互动，以解决问题和回答疑问。
- 利用由 GenAI 驱动的支持助手为技术问题提供自助解答。
- 协助摄取数据、扩展部署和获取有意义的见解，从而实现业务影响。
- 支持工单管理，包括创建、审查和更新支持工单。
- 支持进行协作式问题解决的安全信息交换，包括使用 Markdown 的代码片段或大文件。
- 通过分析集群性能、配置、字段映射和使用诊断文件的一般集群状态来诊断和排除技术问题。
- 管理客户订阅和许可证。
- 通过经验丰富的支持工程师，为 Elastic 软件提供专业建议和指导。
- 监测我们系统与用户互动的效率和准确性。

产品使用数据

作为 Elastic 生态系统的一部分，Elastic 支持服务会自动收集与服务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。

访问客户数据

- **客户访问：**Elastic 支持中心与 Elastic Cloud 完全集成。现有订阅用户可通过 Elastic Cloud 账户访问该中心，并可以创建和审核支持工单、获取更新、下载许可证以及查看订阅信息。所有先前的支持数据（包括工单、评论、订阅和许可证）仍然可以在门户中访问。所有 Elastic Cloud 账户都可以访问支持中心，无论是否有任何正在运行的云部署。基于角色的访问控制 (RBAC) 已集成到 Elastic 部署中，允许客户管理员定义角色，以限制用户对特定信息的访问，从而遵循最小权限原则。

- **Elastic 的访问：**Elastic 支持在排除故障时通常处理的是“元数据”（间接和非身份识别数据），如日志文件、配置文件和产品诊断，而不是实际的客户内容、客户个人数据、直接数据库或终端用户身份识别数据。

    - 在几乎所有支持或运营场景中，Elastic 的工程师不会访问存储在数据索引中的客户数据内容，也不会直接访问客户文档或文件系统。Elastic 只有在客户指示下才会访问云部署中的客户内容，例如在客户要求下提供支持服务时。如果特殊问题需要访问客户内容（例如堆转储），则必须获得客户的书面授权。这些流程受到严格控制，完全可审计，并遵守 SOC 2 和 ISO 27001 等合规标准。

    - Elastic 支持团队使用支持诊断工具来了解客户集群的健康状况，但该工具不会收集存储在客户集群中的实际源事件或文档数据；它仅收集运行时信息和集群元数据。在与 Elastic 共享之前，可以通过清除 IP 地址、主机名或索引名称等敏感元数据，对诊断输出进行进一步处理。

- 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，包括文件完整性监测和账户接管指标。

- 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

支持服务通过特定的支持子处理方提供。这些子处理方受合同约束，须提供与 Elastic 水平相当的数据保护。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 Elastic 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 支持服务在设计时即致力于遵守《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 还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），合法传输源自欧洲经济区、瑞士或英国的个人数据。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，并为客户提供在欧盟服务器上托管数据的选项。

保留和删除

上传到 Elastic 支持中心的文件将在上传 30 天后自动清除，以保护敏感信息。支持服务使用的工单系统会在工单关闭 15 天后移除所有工单附件。

安全性

在 Elastic Cloud 中，您数据的安全性取决于您是否对部署进行了安全配置，并妥善保管了您的 Elastic Cloud 登录凭据（如需了解更多信息，请参阅我们的安全性常见问题解答）。此外，Elastic 支持全面的深度防御安全模型，致力于在整个生命周期内保护客户数据：在传输中、静态存储中和内存中，并辅以强大的密钥管理程序。我们也使用 Elastic Security 进行内部信息安全运营。

- **加密：**客户数据在静态时使用 AES-256 加密，在传输时通过 TLS 1.2 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。
- **系统更新与补丁：**Elastic 系统会定期根据最新的操作系统内核进行更新和部署。每当在任何软件组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 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。