



Elastic 隐私数据表

Observability

客户有责任对本文件中的信息进行独立评估。本文件：（a）仅供参考，（b）代表当前 Elastic 的产品、服务和惯例，可能随时变更，恕不另行通知，（c）不构成 Elastic 及其关联公司、供应商或许可方的任何承诺或保证。Elastic 对其客户的责任和义务受 Elastic 协议的约束，本文档不构成 Elastic 与其客户之间任何协议的一部分，也不构成对协议内容的修改。

产品摘要：Elastic Observability

Elastic Observability 可针对在您的环境中运行的应用程序的行为提供细致的见解和上下文，从而快速检测和解决根本原因事件。它提供单一堆栈来统一您的日志、基础设施指标、应用程序跟踪、用户体验数据、合成和通用性能分析。数据直接摄入到 Elasticsearch 中，在此经过处理与增强后，即可在 Kibana 中进行可视化展示及告警设置。Observability 旨在通过开放、灵活和统一的可观测性解决方案，并辅以先进的机器学习和分析技术，加速解决问题。

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

在 Elastic Observability 中处理的数据

Elastic Observability 处理客户摄入的运营遥测数据，以监测他们的系统和应用程序。处理的具体个人数据类型取决于客户摄入的数据和配置。Elastic 提供管理这些数据的平台和工具，这些数据可能包括个人数据，具体取决于日志、指标、应用程序跟踪或用户体验数据的性质。

访问和使用 Elastic Observability 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、安全访问和可审计使用是必要的。

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：

- 来自日志、指标和跟踪的个人标识符和系统 / 网络活动数据：
 - 示例：用户 ID、IP 地址、主机名、机器名、进程 ID、文件名、目录路径、URL、电子邮件地址（如果存在于日志或错误消息中）、移动设备标识符，以及和来自用户体验监测的位置数据。
- 应用程序性能数据：
 - 示例：交易详情、范围、错误、指标和从应用程序收集的元数据，如果客户未进行净化，可能包含用户特定数据。
- 用户体验数据：
 - 示例：与真实用户感知的 Web 应用程序性能相关的数据，可能包括浏览器类型、操作系统以及概略位置数据。

处理输入到 Elastic Observability 中的客户数据的典型目的：

在具体部署中，客户可自行决定其选择提供给产品的任何数据的实际处理用途。一般来说，Elastic Observability 是为以下用例而设计的：

- 提供有关应用程序行为的细致见解和上下文。
- 统一并关联日志、基础架构指标、应用程序跟踪、用户体验数据、合成和通用性能分析，以加快根本原因检测。
- 分析来自主机、服务、Kubernetes 和 Apache 等各种来源的日志数据。
- 通过应用程序性能监测 (APM) 对代码进行检测，并在运行时收集性能数据和错误。
- 监测服务器、Docker、Kubernetes 及其他服务和应用的系统和服务指标。
- 通过真实用户监测 (RUM) 量化和分析 Web 应用程序的感知性能。
- 通过合成监测，在受控环境中以预定间隔模拟用户在网站上的操作和请求，生成一致和可重复的数据，用于趋势分析和告警。
- 构建栈跟踪，在不需更改应用源代码或进行插桩的情况下，获得系统性能的可视化，帮助识别高开销代码行、提高 CPU 效率，并排查性能回退问题（通用性能分析）。
- 通过预测分析和机器学习，检测时间序列数据中的异常和峰值，并研究日志率或指标分布异常变化的原因。
- 基于定义的规则和阈值，警示环境中的潜在问题，并与日志监测和 APM 集成。
- 为服务性能设定明确、可衡量的目标，并实时监测服务级别目标 (SLO)。
- 通过创建案例、实现团队协作以及与 ServiceNow、Jira 等第三方系统集成，收集和共享有关可观测性问题的信息。

产品使用数据

Elastic Observability 会自动收集与产品使用情况相关的某些信息。此类产品使用数据按照 [Elastic 产品隐私声明](#) 中的说明进行处理。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 Elastic Observability 的数据保留完全控制权。他们可以通过 Kibana UI 访问和分析其可观测数据，该界面提供搜索、筛选、可视化和分析日志、跟踪和指标数据的功能。客户可以使用 Elasticsearch 的 REST API 或通过各种 Elasticsearch 客户端直接检索数据。Kibana 内置基于角色的访问控制功能，用于管理用户对特定内容和功能的访问，确保遵守最小权限原则。
- **Elastic 的访问：**对于 Elastic Cloud 产品与服务，仅有极少数 Elastic 员工被授予生产环境的特权访问权限，且严格用于必要的平台管理、维护及支持活动目的。此类访问权限基于最小权限和按需知情原则进行配置，并且定期接受审查和调整。Elastic 在未连接到云的自我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

Elastic Cloud 部署的 Observability 解决方案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 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 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 Elastic Observability 数据的可移植性。您可以通过 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，使客户能够有效地管理其数据保留和删除策略。

- 客户可以定义并强制执行在 Elastic 环境中收集和处理的个人数据的保留策略。
- 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，这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

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。

- **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程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 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。