Elastic Cloud
信息安全概述

2023 年 10 月

elastic.co/cn

目录

服务和范围

借助企业搜索、可观测性和安全性这三个方面的解决方案，我们可以协助用户更快地找到所需内容，确保任务关键型应用程序平稳运行，有效防范网络威胁。Elastic Cloud 旨在让您能够针对您的特定用例灵活地调整和管理部署，从而降低复杂性，管理底层平台，以便在速度、规模和相关性方面为您的搜索体验提供支持。

我们清楚，作为我们的客户，我们对您负有重要责任，您依赖我们提供领先的搜索体验，同时保护您的数据 — 我们努力工作正是为了赢得您的信任。从组织高层的董事会监督和行政监管，到我们如何录用并持续培训每一位 Elastic 员工，安全性对我们所做的一切都至关重要。Elastic 为 Elastic Cloud 服务和我们的信息安全管理系统 (ISMS) 获得了一系列广泛的行业领先的合规性报告和认证。这些报告和认证证明，有效的安全实践体现在我们的所有活动中，包括产品开发和部署、漏洞管理、事件管理和威胁处理流程。

本文档概述了我们现有的政策、程序和技术控制措施，让您放心使用 Elastic Cloud 为您的解决方案提供支持。Elastic Cloud 及其相关软件解决方案可以部署在本地、公有云或私有云中，也可以部署在混合环境中，以满足各种用户和客户需求。但是，对自管型部署的控制不在本文档的讨论范围内。

Elastic Cloud 概述

Elastic 提供了企业搜索、可观测性和安全方面的云原生解决方案，可改进客户和员工的搜索体验，确保任务关键型应用程序平稳运行，有效防范网络威胁。Elastic 产品可以从任何来源采集数据，并以任意格式存储数据，以供搜索、分析和可视化。

Elastic Cloud 是一系列软件即服务 (SaaS) 产品，其中包括 Elasticsearch Service (ESS)、企业搜索、可观测性和 Elastic Security。Elastic 在客户选择的基础架构上托管和管理 Elastic Stack 组件，包括 Elasticsearch 和 Kibana，这些基础架构来自多个公共云服务提供商，包括 Amazon Web Services (AWS)、Google Cloud Platform (GCP)、Microsoft Azure 和 IBM。Elastic Cloud 产品包括高级 Elastic Stack 功能，例如安全性、告警、监测、报告、Machine Learning 和可视化功能。

下面提供了有关 Elastic Cloud 组件的更多信息。

Elastic Cloud 组件	组件描述
Elasticsearch Service (ESS)	ESS 是一个分布式实时搜索及分析引擎和数据存储，适用于包括文本、数字、地理空间、结构化和非结构化数据等在内的所有数据类型。
企业搜索	Elastic 企业搜索提供了强大的工具，可以在无缝扩展的同时快速提供搜索体验： Workplace Search 是一种工具，可将组织的内容平台（Google 云端硬盘、Slack、Salesforce 等）统一成个性化的自然搜索体验。 App Search 是一个工具箱，可供开发人员利用 Elasticsearch 的强大功能，为移动和 SaaS 应用添加搜索体验，并配有网络爬虫、经过优化的 API、直观的仪表板和可调的相关性控件。 Site Search 可向网站添加强大的搜索功能，例如根据需要添加搜索框。
可观测性	Elastic 可观测性支持对日志、指标、应用程序性能和运行状态监测信息进行统一分析。使用 Elastic Agent 和预构建的集成连接器进行数据收集，组织可以通过 Machine Learning 和同时支持 DevOps 和 SecOps 团队的开箱即用型检测规则来发现离群值。
Security	Elastic Security 通过单个用户界面预防和检测威胁并做出响应： Elastic SIEM 具备传统的日志聚合和关联功能，支持威胁检测和响应，以及高级安全功能，例如利用 Machine Learning 进行风险评估、集成用例管理和 SOAR。 Elastic Agent 带来了无限的多功能性，占用空间小，几乎可以在任何地方使用，包括混合环境。它可以抵御威胁、转发数据并支持多种用例，在丰富安全信息的同时也增强了保护。 Limitless XDR 可实现安全运营现代化，从而整合 SIEM 和终端安全，支持对多年数据进行分析，自动执行检测和响应流程，并为每台主机提供原生终端保护。

云合规计划

Elastic Cloud 的设计以安全为核心。我们已经获得并持有行业领先的认证和证明报告，足以表明我们对安全性、合规性、隐私性和可靠性的承诺。

Elastic 的全球信息安全管理系统已通过 ISO 27001 认证，Elastic Cloud 商业服务已通过 ISO 27017、ISO 27018、SOC 2 Type 2、CSA 云合规矩阵 (CCM)、HIPAA 和 PCI-DSS 的审核或认证。我们还提供渗透测试执行摘要以及行业和特定地域认证（即 TISAX）。有关我们评估所依据的合规标准以及如何获取我们的报告和认证副本的更多信息，请参阅本文档的“合规性标准”部分。

此外，Elastic Cloud 在 AWS GovCloud 中获得了中等影响级别的 FedRAMP 授权。请访问我们的 FedRAMP 授权云产品/服务页面，查看认证详情。相关政府客户和潜在客户可以使用 FedRAMP 包访问请求表，通过 FedRAMP Marketplace 访问我们的 FedRAMP 安全包。

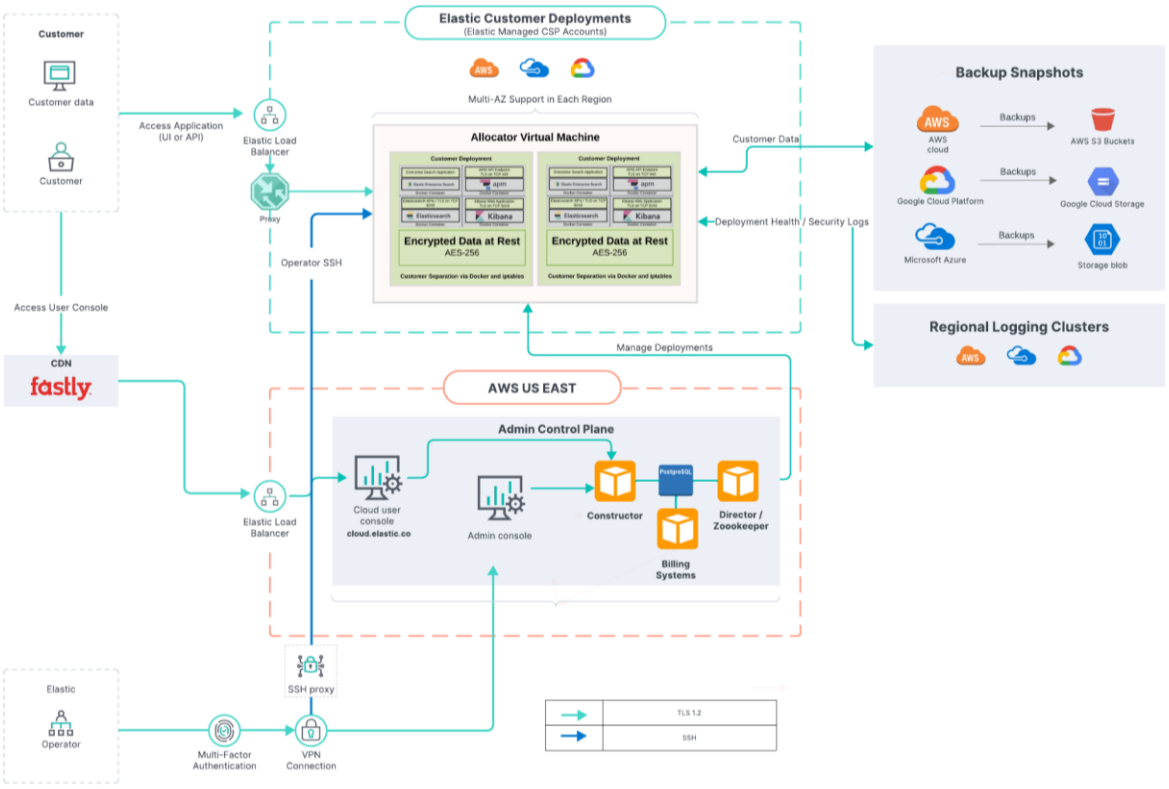
产品使用数据和客户内容

我们以最谨慎的态度对待我们客户的信息，本文档中所述的保护措施旨在保护客户内容。下面将进一步解释产品使用数据与客户内容之间的区别。

产品使用数据： Elastic 使用这些数据来加快产品交付、管理和监测基础架构、提供支持以及进行产品分析和改进。产品使用数据受到严格控制和保护，并接受内部和外部评估，以测试数据的安全性和完整性。然而，本文档的重点是如何部署纵深防御来保护客户内容。

客户内容： 这是客户采集、上传或以其他方式提交到 Elastic 产品和服务中的数据。Elastic 仅在提供产品或服务所需的情况下以及遵守法律可能需要的情况下处理这些数据。客户始终可以完全控制将哪些数据采集到 Elastic Cloud 中。

Elastic Cloud 服务示意图



Elastic Cloud 架构描述

控制平面

Elastic Cloud 的控制平面包括 **ZooKeeper**、**Director** 和 **Constructor** 管理服务，具体说明如下：

- **ZooKeeper** - ZooKeeper 是一个分布式数据存储，用于保存 Elastic Cloud 组件的基本信息：代理服务器路由表、分配器公布的内存容量、通过管理控制台提交的更改等。它充当各服务之间通信的消息总线。它还用于存储 Elastic Cloud 安装的状态以及 Elastic Cloud 中运行的所有部署的状态。

- **Director** - Director 负责管理 ZooKeeper 数据存储，并为想要与 ZooKeeper 通信的内部客户端签署证书签名请求 (CSR)。它还维护 ZooKeeper 用于通信的 STunnels，并在创建新的 ZooKeeper 节点时设置法定数量。

- **Constructor** - Constructor 的工作原理与监测来自管理控制台的请求的调度程序类似。它会确定需要更改的内容，并将更改写入由分配器监测的 ZooKeeper 节点。它还会将集群节点分配给分配器，并最大限度地利用底层分配器，以减少为新部署启动额外硬件的需要。Constructor 将集群节点和实例放置在不同的可用区中，以此来确保部署能够承受任何可用区故障。

这些放置偏好可根据数据主权要求进行自定义。

- **Cloud UI 和 API** - 这些功能为管理员提供了 Web 和 API 访问权限，以便管理和监测安装。

代理服务器

代理服务器可处理用户请求，从而将容器的请求 URL 中所传递的部署 ID 映射到实际的 Elasticsearch 集群节点和其他实例。部署 ID 与容器之间的关联存储在 ZooKeeper 中，由代理服务器缓存。在 ZooKeeper 中断的情况下，平台仍然可以使用缓存处理发往现有部署的请求。

如果您拥有高度可用的 Elasticsearch 集群，代理服务器还会跟踪可用区的状态和可用性。如果其中一个可用区出现故障，则代理服务器不会将请求路由到那里。此外，代理服务器还有助于实现无中断扩展和升级。在执行升级操作前，会先创建快照并将数据迁移到新节点。迁移完成后，代理服务器会将流量切换到新节点并断开与旧节点的连接。通常情况下，一个负载均衡器的后面会配置多个代理服务器，以确保系统一直可用。

分配器

分配器可在托管 Elasticsearch 节点和 Kibana 实例的所有机器上运行。它通过以下方式控制集群节点的生命周期：

- 根据请求创建新容器和启动 Elasticsearch 节点
- 如果节点没有响应，则重新启动节点
- 如果不再需要节点，则将其移除

它还会将底层主机的内存容量公布给 ZooKeeper，以便 Constructor 在选择部署位置时做出明智的决定。

风险管理

Elastic 采用基于风险的安全性和合规性方法，利用领先的定量风险评估和分析方法 FAIR，以便识别和评估业务风险，并确定风险缓解活动的优先级。

Elastic 的风险评估流程可识别和管理风险，而这些风险可能关系到我们能够为客户提供值得信赖的可靠服务。我们已经识别并重点控制的主要风险包括：

- 组织管理
- 人力资源安全
- 资产管理
- 访问控制
- 密码系统
- 安全通信
- 系统购置、开发和维护
- 供应商关系
- 信息安全事件管理
- 业务连续性管理

风险识别流程会考虑内部和外部因素及其对实现目标的影响。

已识别的风险会通过一个流程进行分析，该流程涉及分析与我们的业务目标相关的潜在威胁和漏洞，以及预估风险的潜在重要性。
风险评估流程会考虑如何管理风险，以及是接受、避免、减轻还是转移风险。我们会为已识别的风险确定缓解策略。这些策略可能包括设计、制定和实施控制措施，以及采用或修改政策和程序。

我们的风险登记册的信息来源于集体风险识别、分析和评估流程，登记册中的风险场景使用 FAIR 方法进行评估，并根据对 Elastic 的预估财务影响进行排名。风险登记册每半年重新评估一次，以充分考虑内外部风险因素、业务优先级的变化，以及不断发展的风险缓解策略。这一流程也促使信息安全团队向董事会审计委员会报告时采用基于风险的方法。

治理

信息安全管理系统 (ISMS) 和监督

Elastic 实施了信息安全管理系统，其中包括协同运作的策略、程序、运营结构和技术控制措施，以保护客户和公司数据。信息安全管理系统已通过 ISO 27001 认证，旨在全面解决所有安全性和合规性领域的问题，包括治理、信任、风险和漏洞管理、安全架构和工程、产品安全、威胁检测和事件响应。

Elastic 董事会（审计委员会）负责监督信息安全管理系统，并定期与首席信息安全官 (CISO) 举行会议，以确保信息安全计划的运作符合业务目标，采用行业最佳实践，并随着威胁态势的变化而演变。

Elastic 信息安全管理系统通过一个专门的业务完整性和隐私团队得到了加强，该团队与信息安全团队密切合作，共同制定组织解决方案，确保遵守全球数据法律和法规。

信息安全策略

Elastic 根据 NIST 和 ISO 27001 等行业标准制定了一套全面的策略来管理我们的信息安全实践，并在整个公司传达管理层的期望。策略所有者会每年审查一次，并由高级管理层批准所有信息安全策略。Elastic 的策略适用于以下领域：

- 信息安全计划
- 可接受的使用
- 风险管理
- 资产管理
- 数据分类
- 记录保留
- 访问控制
- 工作站和服务器安全

- 安全分析和日志记录
- 漏洞管理
- 变更管理
- 安全软件开发
- 事件响应
- 业务连续性和灾难恢复

所有 Elastic 员工都必须证明，他们在入职时以及此后每年都阅读并认可 Elastic 行为准则以及信息安全、隐私和可接受的使用政策。

我们不会对外分享我们的信息安全政策的全文。但是，我们会提供信息安全政策包，其中包括每个政策的目录和版本历史记录，以明确每个政策所涵盖的领域，以及证明定期阅读、更新和批准每个政策的证据。如需本文档的副本，请联系您的 Elastic 客户代表或 Elastic 支持。

除了正式的政策外，Elastic 还为具有更具体流程要求或不断改进的最佳实践（如云加密、证书和密钥管理以及第三方风险管理）的领域制定了行动手册、流程文档和计划。

人力资源管理

我们认识到，全面的安全计划始于高层的肯定，并与每位 Elastic 员工息息相关。我们的源代码、员工手册和行为准则包含明确的指导和道德标准，所有 Elastic 员工都应遵守。Elastic 对任何违反这些承诺的人采取零容忍政策，无论其职位高低、资历或任期长短。

Elastic 还制定了具有正式报告渠道的实体级安全最佳实践，有助于向相关人员传信息，并确保对员工行为和绩效进行适当的问责和监督。岗位和职责根据职能要求进行分离，并明确定义工作岗位。

所有的雇用和解雇均按照政策文件和程序进行，其中包括安全快速的正式员工和合同工入职和离职程序。

其他实体级安全实践包括在新员工和合同工入职前对其进行背景调查。此外，所有 Elastic 员工（包括高管和高级管理层）都必须在入职时和入职后每年完成一次安全意识培训，阅读并认可信息安全和隐私政策、行为准则和员工手册。

资产管理

资产管理标准规定了资产管理生命周期，包括资产清单、资产所有权、资产返还和处置以及审计追踪要求。机群管理和终端管理之间的资产管理流程有所不同。下面将解释每个独立的流程：

机群

我们的合作伙伴云服务提供商 (CSP)、AWS、GCP、Azure 和 IBM 负责管理为 Elastic Cloud 提供支持的基础架构。Elastic Cloud 客户可以灵活地针对每个部署为其数据选择底层 CSP 和地理区域。物理安全、媒体和硬件控制由 CSP 负责。在第三方重新认证（作为第三方风险管理计划的一部分）期间，Elastic 会审查合作伙伴云服务提供商的媒体和硬件生命周期管理控制措施的设计和运营有效性。

Elastic 集群利用 Elastic 可观测性来跟踪性能和运行时间指标。关键资产登记在我们的资产清单中，我们会定期审查资产清单的完整性和准确性。

员工终端

Elastic IT 会集中跟踪和管理员工终端。我们使用设备管理软件来强制执行安全设置，包括加密、密码管理、会话管理和屏幕锁定，这些设置都是默认启用的。这些设置不能在本地禁用或修改。终端受到 Elastic Security 的保护，后者提供 EDR 功能以及实时监测和告警。有关如何保护员工终端免受恶意软件攻击的更多信息，请参阅“恶意软件防护”部分。

Elastic 发放的所有设备都按照我们的设备管理生命周期进行处理。当 Elastic 员工离职时，其逻辑访问权限将被禁用，公司托管的终端将直接送到第三方处理商那里执行数据清除和销毁程序。我们的第三方合作伙伴会向 Elastic 提供销毁证书，并根据 Elastic 笔记本电脑使用标准重新发放或处置计算机。Elastic IT 负责维护 Elastic 托管的终端的审计追踪，以便跟踪每台设备在数据销毁生命周期中的状态。

根据政策，非托管或个人移动设备不能存储客户数据，也不能用于 Elastic Cloud 的开发或支持。

配置管理

Elastic 通过代码来管理配置，配置更改遵循标准的变更管理程序，包括授权、同行评审和批准以及自动化测试套件。Elastic 通过文件完整性监测和可疑活动检测来监测对生产配置文件的直接更改。

数据保护

数据分类和保留

Elastic 数据分类标准要求根据敏感度对数据进行分类，并为每个分类定义访问和共享限制。客户内容和产品使用数据被归类为受限数据（最敏感的分类），并受最严格的数据保护标准的约束，旨在保护数据的机密性、完整性和可用性。有关客户内容和产品使用数据的定义，请参阅本文档的“产品使用数据和客户内容”部分。

Elastic 记录保留标准要求根据数据类型以及运营、合同、法律和法规要求，按照定义的保留计划处置数据。客户可以随时向 Elastic 支持提交帐户删除请求，以删除其信息。有关如何提交数据访问请求的信息，请参阅本文档的“数据隐私”部分。

数据收集、处理和处置

数据收集

Elastic 仅收集提供、支持、维护、保护和改进我们的服务所需的信息。这些信息绝不会出售给第三方。有关我们向客户收集的信息的更多信息，请参阅我们的产品隐私声明。

数据采集

Elastic 不会控制或访问客户选择在其 Elastic 部署中存储、传输或处理的数据。客户的 Elastic 部署所采集的任何数据均由客户自行处理，并始终处于其控制之下。

数据销毁

Elastic 记录保留标准和资产管理标准规定了数据销毁要求。我们的云服务提供商合作伙伴负责管理托管基础架构的安全删除和数据销毁。客户保有对其存储在 Elastic 实例中的内容的完全控制权，并有权随时从其 Elastic 实例中移除或删除任何内容。

加密

传输中加密

默认情况下，Elastic Cloud 的传输中加密是通过传输层安全协议 (TLS) 来实现的。可接受的最低密码强度为 TLS 1.2。TLS (HTTPS) 连接会显示在 Elastic Cloud 服务示意图中。

用于支持 Elastic Cloud 的证书由 Digicert 提供，并使用 RSA 2048 位密钥进行公钥身份验证。Elastic 会为我们的云部署维护有效证书，这些证书被 Qualys SSL Labs 评为 A+。这些测试结果可以通过访问 SSL Labs 来重现。

静态加密

我们的云服务提供商合作伙伴提供静态加密，并在默认情况下处于启用状态。我们所有的云服务提供商都使用符合 NIST 准则（256 位）的最小密钥长度。

密钥管理

加密密钥永远不会离开生成它们的主机，并且被视为一次性密钥。创建或替换虚拟机主机时会自动生成加密密钥。这种密钥不会被备份、暴露或离开主机。底层 IaaS 服务中的加密密钥管理是使用提供商的密钥管理服务自动执行的。

Elastic 服务的密钥管理以基础架构即代码的形式并作为每个适用组件或服务的操作文档的一部分进行维护。

网络和设备安全管理

防火墙

我们的云服务提供商合作伙伴负责管理生产基础架构的硬件防火墙。Elastic 还维护软件防火墙，以过滤来自互联网的未经授权的入站流量，并拒绝未经明确授权（默认拒绝）的传入网络连接。环境中的逻辑区域之间进一步设置了网络分段和防火墙。防火墙规则集至少每半年审查一次。对防火墙规则的更改遵循标准变更管理流程，并受变更管理控制的约束。此外，对防火墙的所有访问都是使用 RBAC 实现的。

Elastic Cloud 客户可以利用流量过滤功能，或者配置 PrivateLink 以进一步限制通往其部署的流量。
IP 流量过滤器 | Elasticsearch Service 文档 | Elastic
AWS PrivateLink 流量过滤器 | Elasticsearch Service 文档 | Elastic

恶意软件防护

通过集中管理的 IT 配置在所有员工终端上启用了反恶意软件。本地管理员无法禁用或修改这些设置。Elastic Security 解决方案提供 EDR 功能以及一支处理信息安全审查和操作警报的全天候待命团队。

Elastic Security 用于保护 Elastic Cloud 生产环境。签名和行为模式会自动持续更新。可以针对新出现的威胁快速部署检测，并有一个专门的威胁情报、检测和响应团队管理针对潜在的恶意软件感染的检测、分析、响应和补救。

时间同步

时间同步是通过具有公共时间源（NIST 服务器）的 NTP 实现的。

逻辑访问

基于角色的访问控制

在向内部用户提供访问权限时，Elastic 遵循最低权限原则。仅向 Elastic 员工授予其工作岗位所需的访问级别。我们会定期审查访问权限，并在工作变动或其他不再需要用户访问权限的情况下修改权限。

Elastic 产品还具有基于角色的访问控制功能，使我们的客户能够在他们的 Elastic 部署和 Elastic Cloud 管理平台中为用户实施细粒度的访问管理。

入职和离职

根据我们的集中式身份和访问管理 (IAM) 系统中的预配置规则，会为新员工自动配置对企业云原生 SaaS 应用程序的访问权限。自动配置规则集利用 HR 记录系统中的职位属性（例如监管组织、职位类别、职位等级和管理结构）来授予单个用户所需的特定访问权限。超出此范围的任何访问都需要在工单中记录正式请求，并接受管理层的审查和批准。

如果员工被调到 Elastic 中的其他工作岗位或组织，则 HR 记录系统中其职位属性的更改将自动启动集中式 IAM 系统中的工作流，以重新为其账户配置适合其新角色的访问权限。他们先前岗位的访问权限将被取消配置，并根据其新角色的职位属性配置新访问权限。

员工离职后，其雇用状态在我们的 HR 管理系统中会发生变更，通过我们的集中式 IAM 系统授予的访问权限也会自动暂停。这种验证检查每天会进行多次。

生产访问

只有部分 Elastic 员工有权访问 Elastic Cloud 生产环境。Elastic 维护这种访问是为了进行平台管理、维护和支持。Elastic 数据处理政策明确禁止 Elastic 员工访问客户数据，即使在维护或故障排查场景中也是如此。对于客户自愿共享的用于支持或故障排查的任何数据，Elastic 员工必须获得客户的书面同意方可查看。

Elastic 不会主动查看上传到 Elastic Cloud 或采集到 Elastic Cloud 的客户数据。客户可以选择在与 Elastic 共享数据之前编辑或净化数据。

此外，我们的信息安全威胁检测和响应团队还开发并实施了对可疑内部帐户活动和未经授权访问的检测，包括文件完整性监测和帐户接管或数据渗漏迹象。这些检测是自动化工作流的一部分，这些工作流会提醒威胁检测和响应团队留意可疑活动，并触发分析师调查。

用户访问权限审查

Elastic 遵循最小权限原则，仅授予履行各个工作岗位所需的访问权限。在季度用户访问权限审查期间，系统所有者和管理层会审查并重新认证用户访问权限，包括特权访问权限。不再需要的访问权限将被取消配置。

变更管理

变更管理标准规定了变更管理流程，并制定了旨在以安全的托管方式控制软件的开发和部署以及生产环境基础架构变更的要求。

变更管理流程可确保以可控制的方式授权、同行评审、测试、实施和发布提议的变更，并记录和监测每个提议的变更的状态。如果需要进行紧急变更，仍需要书面批准和自动化测试。还需要对紧急变更进行人工审查，但可以在实施后进行。

供应链安全

将软件部署到生产环境是通过自动化的 CICD 管道进行管理的。变更存储在每个相应存储库中的指定分支中。开发分支用于主动开发，主分支包含生产就绪代码。变更受版本控制，在合并到主分支之前，会执行一系列包括安全检查在内的自动化测试。我们支持分支保护，这要求通过测试套件，然后才能授权更改合并到主分支。当变更获得完全授权（通过测试和安全检查，获得同行评审和批准，并通过集成检查）时，自动化部署软件会将变更推送到生产环境，而无需人工介入。

我们的源代码存储在访问受到控制和监测的版本控制系统中。用户活动会记录在审计日志中，并设置了检测，以便在出现意外或可疑的修改和构建过程时发出警报。能否修改每个存储库中的代码取决于具体的工作岗位。

安全开发

SDLC

我们的系统开发生命周期 (SDLC) 的安全要求在安全软件开发框架中进行维护。这个框架规定了安全设计、开发、部署、跟踪和维护所有 Elastic 软件的流程。它还包括保护我们的构建系统和降低构建链泄漏风险的要求。构建系统包括软件交付管道、包注册表、构件存储库、CI/CD 和源代码管理系统。安全软件开发框架禁止将生产数据用于测试和非生产系统。它还要求将生产环境和非生产环境分开。在第三方渗透测试期间，会对环境分割情况进行评估。

安全设计和架构

Elastic 软件开发遵循设计和架构方面的安全性最佳实践，以生产“设计即安全”和“默认安全”的软件。

安全软件开发框架概述了所有设计应遵循的数据保护要求和安全原则，包括：

- 机密性 - 数据在传输和存储时都受到保护，不会遭到未经授权的查看或披露。
- 完整性 - 保护数据免受未经授权的创建、更改或删除。
- 可用性 - 授权用户可以根据需要使用数据，并满足任何定义的可用性 SLA。
- 识别、身份验证、授权
- 不可否认性
- 审计和日志记录
- 访问控制和最小权限原则
- 安全通信和加密标准
- 安全默认值和故障安全/故障保护

威胁建模和安全架构审查也是软件开发过程的一部分，可确保设计考虑了所需的安全原则。

安全编码

作为 SaaS 提供商，我们认识到安全编码实践的重要性。OWASP Top 10 和 CWE Top 25 等常见编码漏洞可在安全软件开发培训中得到解决，该培训面向相关团队和个人，每年进行一次。在合并更改之前，源代码变更需要至少一名审查人员（而非变更的作者）进行审查和批准（通过合并请求）。变更会进行审查，以确定变更可能带来的潜在安全影响。此外，独立的渗透测试（包括安全代码审查）将重点放在常见的不安全编码实践上。威胁建模、安全审查或源代码审查期间发现的任何问题都将根据漏洞管理标准进行跟踪、评估并基于所评估的风险进行补救。

为了维护安全软件和保护客户免受漏洞影响，Elastic 还赞助了漏洞赏金计划。有关更多信息，请参阅“漏洞和补丁管理”部分中的“漏洞披露计划”。

开源和第三方软件审查

安全软件开发框架要求识别和跟踪开源和第三方库的代码依赖关系。依赖关系管理软件可以帮助识别、扫描和修复易受攻击的依赖关系。

漏洞和补丁管理

漏洞管理标准管理漏洞管理计划，并制定了扫描 Elastic 资源以及漏洞分类、分析、修复和披露的要求。Elastic 会执行漏洞扫描，并将补丁应用到为 Elastic Cloud 提供支持的基础架构以及 Elastic Cloud 组件本身。下面详细介绍了这些流程。

基础架构漏洞和补丁管理

Elastic 利用商业漏洞扫描软件持续扫描我们的资产。这些扫描覆盖所有生产资产。第三方软件供应商会持续更新规则集。漏洞的严重性取决于 CVSS 评级，修补时间表也与 CVSS 评级相对应。严重性为“严重”和“高”的漏洞会优先立即修补，或者在下一个计划版本中进行修补。

产品漏洞和补丁管理

我们通过第三方渗透测试、自动和手动代码扫描和审查、OSS 扫描、分段测试以及我们的漏洞披露计划，严格测试我们的产品是否存在安全漏洞。如果在 Elastic 产品中发现漏洞，Elastic 会根据漏洞管理标准对其进行评估，以确定严重性并制定修复计划。必要时，我们会发布 Elastic 安全通报 (ESA)。 这是 Elastic 向其用户发出的有关 Elastic 产品安全问题的通知。Elastic 会为每个通报分配 CVE 和 ESA 标识符，并提供摘要以及补救和缓解详细信息。所有新通报都在安全公告论坛中公布。

漏洞管理标准还规定了发布披露流程。披露流程包括发布新产品版本（如有必要），并在“通报”页面上发布公告。根据漏洞的性质，我们还会逐个联系客户、发布博客文章和/或将 CVE 提交给 MITRE。

客户可以通过 RSS 源跟踪 ESA。

漏洞披露计划

Elastic 很荣幸能够赞助一项公开的漏洞披露计划，通过该计划，安全研究人员可以负责任地提交漏洞以供内部审查。Elastic 产品安全团队会审查提交的内容，评估风险暴露，并根据评估的风险进行补救。请访问 HackerOne 上的 Elastic 漏洞赏金计划，了解我们的漏洞赏金政策或提交报告。

第三方风险管理

第三方入职

所有第三方（包括分处理商）均需经历一个全面的聘用和审查流程。每个供应商的风险状况都是根据他们提供的服务、他们将处理的数据类型、他们对内部系统的访问权限级别以及捕获供应商的关键性和风险状况的其他因素来评估的。

是否要执行审查工作流将视供应商的风险状况以及他们将向 Elastic 提供的服务类型而定。所有有权访问敏感信息、访问内部系统或提供关键技术服务的供应商都需要进行额外的审查，包括但不限于信息安全、法律和隐

私审查。这种额外的审查涉及审查第三方的安全实践、安全认证和合规性报告。我们会考虑对数据处理、存储和传输所在国家/地区的法律的遵守情况，并且在必要时，Elastic 可能会在第三方协议中添加额外的安全要求。

Elastic 还发布了供应商行为准则，其中记录了供应商和合作伙伴应遵守的道德要求。它包括但不限于道德与合规性、员工健康与安全、人权和劳工权利以及环境保护要求。

第三方重新认证

我们制定了持续的第三方信息风险管理流程，对现有供应商重新进行认证。我们会根据风险级别对第三方进行分类，Elastic 信息安全团队会根据每个风险级别的要求审查第三方的安全实践。

所有为 Elastic Cloud 提供基础架构服务的云服务提供商至少每年都要进行一次审查和重新认证。重新认证过程包括审查供应商的风险状况并检查供应商的安全性和合规性报告，以确保预期的安全性和合规性控制措施充分涵盖我们使用的服务，并确保控制措施的设计和运行切实有效。

威胁检测

监测和告警

我们使用 Elastic Security 作为我们的 SIEM 解决方案，以便快速开发和部署针对新出现的威胁和攻击模式的检测，以及可疑行为检测、文档完整性监测检测和常见恶意软件行为模式。通过自动检测实时监测我们的环境。预先配置的更改工作流可在出现可疑指标时通知相应的 Elastic 人员。我们的全天候待命威胁检测和响应团队负责调查和处理这些告警。

获得认证和持续培训的员工会根据我们的事件响应标准和事件响应计划处理安全事件。有关事件管理流程的更多详细信息，请参阅本文档的“事件响应”部分。

日志管理和保留

我们使用 Elasticsearch 作为日志管理解决方案。我们能够从各种来源（包括检测引擎、我们的 IaaS 提供商、漏洞管理工具、云管理控制台等）采集和集中日志，从而开发出强大的日志记录、审计和取证功能。我们日志的访问受到控制，目的是防止篡改，并且基于最小权限原则，编辑访问权限仅限于安全工程部门。此外，自动检测和告警（包括文件完整性监测）可保护我们的日志记录系统，并近乎实时地将可疑活动通知威胁检测和响应团队。

日志会根据我们的数据保留标准基于业务、法律和合同要求进行保留。客户如有兴趣提交数据访问请求，可以参考本文档的“数据隐私”部分。

事件响应

Elastic 信息安全部门拥有一支全天候威胁检测和响应团队，专门负责管理安全事件。事件响应标准管理事件响应职能，并规定了事件识别、事件处理、报告和培训要求。单独的事件响应计划详细说明了如何准备、检测、分析、遏制、根除、恢复和报告安全事件。训练有素的事件响应人员负责处理所有事件，他们会定期练习和测试事件响应计划。事件还需要书面的事后报告和经验教训练习。

如果我们检测到违规行为或发现未经授权访问系统或数据的情况，Elastic 法律和信息安全部门会立即按照法律要求或根据合同条款通知客户。

如果安全事件需要向外部监管机构或行业实体报告，Elastic 事件响应计划会根据当前的情况，详细说明我们的报告义务。该计划还指定了一个正式的计算机安全事件响应团队 (CSIRT)，该团队具有记录在案的角色和职责，以确保与相应个人进行适当的沟通。

可靠性

可用性和状态

高可用性架构可用，建议在具有增强 SLA 的 Elastic Cloud 上使用。如果您可能会从中受益，请与您的客户团队讨论此方案。Elastic 提供 Elastic Cloud 服务性能的实时和历史数据。

业务连续性和灾难恢复

除了业务连续性和灾难恢复标准外，Elastic 还制定了全面的业务连续性和灾难恢复计划，旨在为灾难做准备、应对灾难并从灾难中恢复。

Elastic 是一家全球分布的公司，自成立以来一直如此。员工装备齐全，可以远程办公，全球分布的团队在人员配备时考虑到了地理冗余。Elastic 的办公场所没有员工联系或向客户提供 Elastic 服务和支持所需的任何基础架构或 IT 系统。

Elastic 维护 Elastic Cloud 的灾难恢复计划，这些计划至少每年进行一次测试。每次测试都是独一无二的，每年都有一个明确的重点领域，以确定我们在技术恢复能力方面的知识缺口和弱点。每个测试都会跟踪和记录 RTO 和 RPO，以确保我们的恢复能够满足内部定义标准。灾难恢复测试会详细记录场景细节、事件时间轴和需要改进的操作项。

独立评估

渗透测试

Elastic 认识到纵深防御的优势和重要性，同时考虑到了人员安全、横向移动、权限提升和持续威胁。因此，Elastic 与多家独立的渗透测试服务提供商合作，执行网络和应用程序层渗透测试、分段测试和安全代码审查。

渗透测试至少每年进行一次。渗透测试的结果会根据重要性进行修正。渗透测试结果也会报告给高级管理层，以促进跨职能部门的协调和问责，从而补救调查结果，并在必要时实施额外的预防和检测控制措施。渗透测试摘要报告和修复状态报告可应客户的要求提供。

除了独立的渗透测试外，Elastic 还赞助并维护正式的漏洞披露（漏洞赏金）计划。我们鼓励安全研究人员通过漏洞披露计划报告漏洞。Elastic 产品安全团队会根据重要性对提交内容进行分类和补救。要了解有关漏洞赏金政策的更多信息或者提交报告，请访问我们在 HackerOne 上的漏洞赏金计划。

合规性标准

Elastic 致力于获得和维护安全性和合规性认证和证明，以便为我们的客户提供最大价值。我们认真对待客户对我们的信任，并满足他们在全球各地高度监管的行业和区域中的搜索、可观测性和安全需求。如需查看 Elastic Cloud 提供的认证和证明的完整列表，请访问 Elastic 安全性与合规性。

数据隐私

在 Elastic，数据隐私在赢得和维护客户信任方面发挥着至关重要的作用。我们致力于让客户透明地了解我们如何在 Elastic Cloud 中处理和保护数据。

数据托管

Elastic 使用云服务提供商（例如 Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP)）来提供 Elastic Cloud。我们通过我们的每个云服务提供商支持全球托管选项。客户可以选择他们想要托管 Elastic Cloud 部署的区域，以最好地满足其数据主权要求。备份还配置为将客户备份保留在其所选区域中。

合同承诺

Elastic 在整个公司建立了流程、组织结构和技术措施，以确保我们符合全球隐私原则。这些承诺基于我们在 Elastic Cloud 客户数据处理修订 (DPA) 文件中向您提供的合同隐私条款。

Elastic 会定期审查和更新我们的数据处理修订，以反映适用的数据隐私性要求，包括以下规定：

- 您的数据归您所有。我们对您的个人数据的处理仅在您的指示下进行。
- 我们处理的数据受到适用的法律数据保护要求的约束。
- 我们已经实施并在合同中承诺采取适当的技术和组织措施，其中包括根据欧盟委员会第 2021/914/EU 号决议制定的标准合同条款（简称“SCC”）（如适用）。
- 所有获得授权处理个人数据的人员都必须遵守严格的保密政策和程序。
- 客户会收到数据主体请求的通知。Elastic 只有在征得客户同意的情况下才会做出回应，并且会协助客户满足其对此类请求的响应要求。
- 根据标准合同条款的规定，Elastic 有义务在收到政府机构访问客户个人数据的请求时通知其客户。如果法律禁止 Elastic 进行此类披露，则根据标准合同条款的规定，Elastic 有义务对此类禁令提出质疑并寻求豁免。
- Elastic 利用保密协议和员工培训计划来确保参与处理个人数据的任何人员都能保密。这些协议的有效期长于员工在 Elastic 的任期。
- Elastic 的分处理商也应遵守同样严格的标准和组织要求。Elastic 对我们的分处理商的作为和不作为负责，就像我们自己提供服务一样。

分处理商

为了向您提供服务，Elastic 使用某些外部服务提供商和内部关联公司提供 Elastic Cloud，这可能需要（作为分处理商）严格处理提供服务所需的客户个人数据。

Elastic 目前聘用的外部分处理商在 https://www.elastic.co/cn/agreements/external_subprocessors 中列出，内部分处理商在 https://www.elastic.co/cn/agreements/internal_subprocessors 中列出。

国际数据传输和 Schrems II

Elastic 是一家全球性公司，可能会将来自欧洲经济区和英国的数据传输给 Elastic 在欧洲以外的第三国员工，以及我们提供服务所需的第三方组织。这些位置已在上面的分处理商部分中列出。在这种情况下，除了强大的补充措施，Elastic 还依赖于标准合同条款，包括客户的控制者-处理者模块以及分处理商的处理者-处理者模块。Elastic 审查了 EDPB 关于 Schrems II 后国际数据传输补充措施的指导方针。考虑到 Elastic 的实践经验，且政府不太可能会对 Elastic 个人数据流程感兴趣，以及 Elastic 为保护客户个人数据而采取的保护措施，Elastic 不认为其在欧洲以外处理客户个人数据会对个人权利构成风险，进而妨碍 Elastic 履行其作为标准合同条款中所述的“数据进口商”的义务。

- 内部分析和外部顾问审查得出的结论是，Elastic 数据传输不属于监督法律的典型关注重点。我们还主动提供补充措施来保护任何传输的数据。
- 就我们的服务和数据处理活动的性质而言，政府当局提出请求的可能性极小。Elastic 从未收到过根据《外国情报监视法案》、美国第 12333 号行政命令或《澄清境外合法使用数据法案》提出的相关请求。
- 标准合同条款用于保护适用的客户数据传输。如果来源于欧洲的个人数据 (i) 由其客户直接传输给 Elastic，(ii) 由 Elastic 在 Elastic 集团实体之间以集团内部方式传输，或 (iii) 由 Elastic 传输给外部分处理商，则 Elastic 将与相关方签订标准合同条款。
- 数据在传输和静态时都会加密。
- 客户可以选择为我们的服务应用程序选择欧盟服务器。
- Elastic 会持续评估和制定我们的合同、技术和组织保障措施，以保护数据传输。

政府当局访问请求

Elastic 制定了响应政府当局访问客户内容请求的政策和流程。这类政策和流程遵守适用的数据保护法律和您的客户协议。

Elastic 并不清楚是否有任何适用法律会影响其履行与政府当局访问请求和要求披露相关的承诺的能力。在任何情况下，Elastic 都不会以超出民主社会所需范围的大规模、不成比例或无差别的方式披露任何个人数据。

尽管有上述规定，Elastic 从未收到任何来自政府当局的访问客户内容的请求，包括根据 FISA 第 702 条。我们也不知道任何根据 EO 12333 直接访问客户内容的行为。Elastic 从未为我们的任何产品或服务设置后门或万能钥匙，也从未允许任何政府机构不受限制地或直接访问我们的服务器。

作为企业保护个人数据

隐私声明

有关 Elastic 如何在 Elastic Cloud 中收集、使用、披露、传输和存储个人信息的更多信息，请参阅我们的产品隐私声明。

全球隐私法规

Elastic 致力于遵守全球隐私法规，包括 GDPR 和 CCPA。要提交数据主体请求，请查看一般隐私声明中的“如何联系我们”部分。有关如何确保您的 Elastic 部署符合 GDPR 的更多信息，请访问 Elasticsearch GDPR 和 Elastic Stack GDPR 合规性。

