Tableau Online 的云安全性

tableau

目录

简介

数据的安全和隐私是组织成功的基石，因此 Tableau 将数据保护视为重中之重。本白皮书概述了 Tableau 通过怎样的措施，确保客户数据在 Tableau Online 中的安全性和可用性。

发布到 Tableau Online 的数据受到企业级安全功能的保护，包括：

- 物理安全性
- 操作安全性
- 数据安全和隐私
- 帐户安全性
- 传输数据安全性
- 应用程序安全性

而这一切的基础，是一种对可用性、性能、容量和安全性进行持续监控的架构。通过这种监控得到的信息可用于实现经常性改进，有助于确保数据的机密性、完整性和可用性。

Tableau 采用了一种多层安全性模型，该模型可以针对众多已知威胁和"零天"威胁提供有效防护。根据 Tableau 的事件响应协议，任何安全违规事件都将通过 Trust 网站 (https://trust.tableausoftware.com) 报告，或者直接向受影响的客户报告。事件报告包括范围、严重性和解决情况。

为了持续提供安全的世界级托管服务，让您对数据的安全性充满信心，Tableau 一直在不懈努力。

操作安全性

SOC 2 和 ISAE 3402

Tableau 每年都会和有执业资格的会计师事务所合作，对 Tableau Online 的控制目标和活动进行深度审计。Tableau 自豪地宣布，Tableau Online 服务的控制规程已经在一份 SOC 2 二类报告中通过验证。该报告根据《鉴证业务准则公告第 16 号》(SSAE 16) 及《鉴证业务国际准则》(ISAE) 第 3402 号的条款编制。我们可以为索求者提供上述 Tableau Online SOC 2 二类报告。

数据中心

Tableau Online 服务托管在独立审计的企业级数据中心；这些中心为所有关键服务提供内部冗余。数据中心内配备有灭火系统和其他监控系统，此类监控系统可以检测环境问题，并在这些问题引发故障之前对其做出响应。此外，托管服务提供商已与供应商签订合同，确保可以在长时间停电时保持运行。

在签署保密协定的前提下，Tableau 可向索求者提供其数据中心提供商的审计报告。如需了解更多信息，请联系您的 Tableau 客户代表。

系统维护

负责维护 Tableau Online 架构的团队执行定期维护工作，确保系统保持出色的稳定性、安全性和性能。我们会提前至少两天在 Tableau Trust 站点公布计划维护窗口期。此外，站点管理员会收到关于即将实施的工作的电子邮件通知，用户在登录到 Tableau Online 站点后也可以看到相关通知。

数据安全和隐私

隐私之盾

在与欧洲经济区 (EEA) 居民相关的个人数据方面，Tableau 是隐私之盾框架下获得认证的 积极参与者，并且受美国联邦贸易委员会的调查和强制执行权的制约。

备份和恢复

所有关键组件都有备份。备份介质经过加密，始终保存在安全的设施内。基于磁盘的备份存储在安全的数据中心设施内。由外部备份服务提供商管理的备份会以加密方式进行传输和存储。只有获得许可的系统管理员才能访问备份。

根据 Tableau Online 备份政策，每日备份的保留期为 31 天。

凭借这些备份，Tableau 可以恢复整个 Tableau Online 系统。这些备份当前不允许恢复单个客户站点，也就是说，如果单个客户的工作簿或数据因为系统故障以外的原因而丢失，Tableau 无法对其进行恢复。

灾难恢复

对于 Tableau Online 服务的每个实例，Tableau 都在不同的地理位置维护主数据中心和备份数据中心。如果主数据中心失去可用性，系统将转到备份站点运行，备份站点会重新配置，以便处理生产流量。数据随即从最近一次备份恢复。

由于 Tableau Online 是一种只读应用程序，并且数据一般来自于客户管理的数据源，因此也许可以直接从数据源拉取信息来重新发布可视化，而无需从备份进行恢复。这样可以显著降低恢复点目标。

数据管控

您的数据属于您自己，即便它们存储在 Tableau Online 中。只有获得您授权的个人才能访问您站点中的数据和工作簿 – Tableau 员工和其他客户均无法访问您的数据。唯一的例外是严格受控的少数几个受信任的 Tableau 管理员，他们负责管理运行服务的系统。涉及该级别访问权限的用户授权必须根据记录在案的流程进行，并且我们每个季度都会对所有管理级别访问权限进行审批。

应该记住，您的大部分数据仍然安全地存储在您自己的数据源中。Tableau Online 中存储的仅仅是工作簿、数据提取和缓存数据。

Tableau 的确能够访问并且可以监控涉及系统利用率、帐户状态和性能的指标。此类指标包括：

- 帐户和用户使用的存储总量
- 帐户和用户使用的带宽总量
- 帐户和用户的工作簿和视图总数
- 用户访问日期和时间（登录）
- 帐户和用户的数据源数量和类型（例如 SQL Server、Salesforce.com）
- 帐户和用户刷新数据的日期和时间
- 站点性能指标

要让数据进入 Tableau Online，有以下四种方式：

1. 发布工作簿并将数据嵌入其中。
2. 将数据从本地数据源"推送"至 Tableau 数据提取。这种方法总是生成数据提取，而不是实时连接。因此，无需创建虚拟专用网络 (VPN) 或安全通道来接入您的公司环境。对于 Tableau Online 无法直接访问的数据源，您可以发布数据提取并使用 Tableau Online 同步客户端来制定自动刷新计划。
3. 通过应用程序编程接口 (API) 连接到 Web 服务。对于大多数云端数据源（例如 Salesforce.com 和 Google Analytics）而言，这种 API 连接用于生成可以按计划定期更新的数据提取。
4. 直接连接到云平台上托管的数据。对于这些数据源，Tableau Online 可以创建实时连接或基于数据提取的连接。

用户和数据源筛选器

您可以通过添加用户和数据源筛选器，在自己的工作簿和数据源中进行额外的安全性定义。用户筛选是一种特殊的筛选。您可以用它来限制任何特定人员可以在发布的视图中看到的数据。例如，在一份与多位地区经理共享的销售报告中，您可能希望西部地区经理只能看到西部销售额，东部地区经理只能看到东部销售额，以此类推。您不必为每名经理创建一个单独的视图，只需定义一个用户筛选器即可让每名经理看到特定地区的数据。

用户筛选器针对单个字段定义。用户或组有权查看该字段中的一部分成员。在以上销售报告示例中，用户筛选器针对"地区"字段定义，每名经理获得查看相应地区的权限。

数据源筛选器的运行方式与用户筛选器类似，您可以针对已发布数据源设置应用于全局的筛选器。数据源筛选器可用于在发布工作簿或数据源时限制用户可以看到的数据。您将数据源发布到 Tableau Online 时，数据源及所有关联文件或提取将整体传输到服务器。发布数据源时，您可以定义数据源的下载或修改访问权限，还可以选择能够通过 Tableau Online 针对该数据源远程提交查询的用户和组。如果用户获得查询权限而没有下载权限，则可以共享包含计算字段、别名、群组、集等项目的丰富数据模型，但这些项目仅能用于查询。

此外，查询该数据源的用户绝无可能看到或修改最初发布的数据源上的任何数据源筛选器，但用户的所有查询都将经过这些数据源筛选器的处理。这种方法可以很好地提供对受限制的数据子集的访问权限。

用户安全性

访问和身份验证

只有您明确添加到自己站点的用户才能访问您的内容和工作簿。您指定的管理员负责所有帐户管理工作，包括添加和移除用户以及分配权限。帐户管理完全在您的控制之下。如果用户在您站点中的权限失效，只需将其移除，该用户就无法再访问 Tableau Online 中存储的内容。

Tableau Online 提供了两种身份验证方法，而您可以灵活配置自己的站点，选择使用其中一种或同时使用这两种方法。

1. Tableau 帐户

Tableau 帐户是默认的方法，这些帐户安全地存储在由 Tableau 维护的身份存储区中。借助这种身份验证方法，站点管理员能够快速配置用户，而无需与另外的身份提供程序集成。帐户由客户管理，可以实现安全的 Tableau Online 身份验证。此类帐户还可用于访问其他 Tableau 服务和资源，例如 Tableau 网站、Tableau 客户/合作伙伴门户以及 Tableau 论坛。

进行身份验证时，用户使用自己的电子邮件地址作为用户名，并提供自己选择的密码。管理员将用户添加到自己的站点时，该用户将收到一封电子邮件，其中包含关于如何设置密码的说明。管理员不会设置用户密码，也无法检索存储的密码。我们使用强大的哈希算法对密码进行"加盐"和哈希处理。

十次登录尝试失败后，帐户将被锁定 10 分钟，并且锁定时间会在发生后续锁定时逐次加倍。用户的并发会话数量不能超过五个，并且会话会在 8 小时后超时。

密码长度不应少于 8 个字符，且必须包含字母和数字。

2. SAML

借助 SAML，管理员可以使用自己的支持 SAML 2.0 的身份提供程序 (IdP) 为其站点配置单点登录。如需了解更多信息，请访问在线产品指南的"站点身份验证"部分。

注意：SAML 和单点登录相关功能当前仅为提出请求的客户提供。要提出功能请求，请联系 Tableau 支持。

Tableau Online 会在非活动状态持续两小时后强制会话超时。

角色和权限

Tableau Online 中的访问可以通过站点角色和权限来进行控制。添加到 Tableau Online 的每个用户都必须具有关联的站点角色。站点角色由管理员分配，决定用户的权限级别，包括用户能否将内容发布到 Tableau Online 并与内容交互，或者用户是否只能查看已发布的内容。关于站点角色的更多详细信息，请参考此内容。权限针对内容（项目、工作簿、视图和数据源）进行分配，并可以分配给单个用户或群组。指定权限时，需要通过规则指定谁可以使用相关内容。

权限可用于赋予创建、查看、修改和删除等权限。针对项目分配的权限控制发布至相应项目的所有工作簿和视图的默认访问级别。管理员可以创建群组（如"财务用户"），使权限管理更加简单。

权限窗口

可以使用 20 多个参数化自定义项来帮助管理对象安全。如需了解更多信息，请参阅在线文档的管理权限部分。

传输（网络）安全性

加密

客户端（Tableau Desktop 或支持的浏览器）与 Tableau Online 之间的所有通信均使用 TLS 加密，为传输中的数据提供保护。

与数据源的连接是否会进行加密取决于数据源的加密功能。客户应该了解自己要使用的数据源所具有的加密选项。

此外，Tableau 产品还有许多内置安全机制，有助于防止欺骗、劫持和 SQL 注入攻击。Tableau 还积极对其产品进行漏洞测试，同时通过定期的更新来应对新出现的威胁。

请注意，使用电子邮件的功能（例如订阅电子邮件）通过 SMTP 来发送电子邮件，而标准的 SMTP 不会进行加密。

应用程序安全性

应用程序安全性需要通过一系列安全设计做法来实现，包括定义安全性要求、威胁建模、代码审查以及安全测试。开发流程包括自动和手动的漏洞测试；在发布主要版本前，Tableau 会邀请第三方安全公司对应用程序进行渗透测试。Tableau 坚持不懈地与第三方安全专家合作，共同进行测试、探索、验证并解决安全问题。

此外，Tableau 还实施了第三方漏洞扫描服务，该服务对本公司面向 Internet 的资源和服务（包括 Tableau Online）持续进行漏洞扫描。一旦发现漏洞，就会生成警报；该服务随后对警报进行分级，以便评估其严重性和影响，再据此为可能需要的任何补救措施确定优先级。

多租户架构

Tableau Online 是一种多租户解决方案，不会为每个客户提供专用环境。该应用程序按站点对用户、数据和元数据进行逻辑分区，从而实现客户之间的隔离。上传或链接到该服务的所有数据均以编程方式连接到拥有该数据的客户。这些控制措施可以确保客户之间无法访问彼此的数据。

管理仪表板

Tableau Online 发布了一组默认仪表板，它们可以提供有关您站点的使用情况统计数据。其中的一些详细信息包括用户活动、视图计数以及数据源使用情况。管理员可以通过这些默认仪表板来了解自己站点的使用情况。

如需详细了解如何使用这些仪表板，请参阅在线产品指南的管理视图部分。

结语

Tableau Online 以可靠的安全性模型作为构建和运行基础，该模型借鉴了行业最佳做法，并通过了第三方安全专家的验证。Tableau 理解数据的重要性，对保护数据的责任一丝不苟。

关于 Tableau

Tableau 帮助人们将数据转化为可以付诸行动、发挥重大作用的见解。轻松连接到以任何形式存储在任意地点的数据。快速执行临时分析，发现隐藏的机会。通过拖放操作，通过高级可视化分析创建交互式仪表板。然后在整个组织共享，让其他团队成员能够从自己的数据视角进行探索。从全球性企业到早期初创企业和小企业，使用 Tableau 的分析平台来查看和理解数据的人无处不在。

资源

下载免费试用版

为何要在云端实现业务分析？

创建有效活动仪表板的 5 个最佳做法（英文）

查看所有白皮书