AUTODESK

Autodesk® Fusion 360
安全白皮书

2022 年 10 月

目录

1. 简介

Autodesk® Fusion 360™ 是首款三维 CAD、CAM 和 CAE 工具。它在可在 Mac 和 PC 上运行的基于单一云的平台中连接您的产品开发流程。Fusion 360 工具支持您使用安全且集成的概念到制造工具集快速轻松地探索设计理念，该工具集可扩展至包含 Web 浏览器和移动设备。

1.1 文档用途和范围

本文档旨在介绍 Autodesk 的操作、软件开发流程以及在环境中实施的安全措施。在本文档中，Autodesk Fusion 360 指的是 Fusion 360 客户端软件和 Fusion 360 浏览器访问软件。

Autodesk 的安全框架基于行业标准来保护客户信息的机密性、完整性和可用性。

Fusion 360 经过精心设计，可实现高可用性和可扩展性，为客户提供快速且具有弹性的云服务。Autodesk 的云托管提供商是 Amazon Web Services (AWS)，它是云基础架构领域的佼佼者。Autodesk 依赖 AWS 托管提供商共担责任模式，其中包括由运行 AWS 云服务的硬件、软件、网络和设施组成的基础架构。（有关详细信息，请参考：https://aws.amazon.com/cn/compliance/shared-responsibility-model/）。

2. Autodesk 安全

Autodesk 安全框架基于行业标准来确保实施一致的安全实践，使我们能够安全构建、安全运行和保障安全。

- **安全构建** - 从一开始便将安全性嵌入到产品中，这是保护客户在 Autodesk 产品和服务上的投资的关键部分。我们将安全性集成到软件开发的所有阶段。
- **运行安全** - 我们将安全性直接内置于我们的基础架构中。我们的整体方法包括端点保护工具展开、标准化的修补和强化要求、身份和访问管理控制以及攻击性安全活动。
- **保障安全** - Autodesk 的安全性关注三个核心目标，即保护信息的机密性、完整性和可用性 (CIA)：

- 机密性：仅获得授权的人员可访问信息
- 完整性：信息完整且准确
- 可用性：数据可供客户访问和使用

首席安全官 (CSO) 负责制定、实施和监管安全战略与计划，并确保在所有 Autodesk 产品和环境中应用安全策略和标准。CSO 和安全团队得到 Autodesk 高管和董事会的支持。

3. Fusion 360 工程

Fusion 360 工程团队负责设计、实施和测试 Fusion 360 客户端软件和云服务应用程序。

Fusion 360 的设计、编码、测试和维护基于敏捷的软件开发流程。在设计冲刺期间，架构师会制作和审阅详细的设计文档，以评估设计的功能性和可扩展性。在实施冲刺期间，软件工程师和架构师会执行同行代码评审，以检测与 Fusion 360 应用程序开发实践的偏差。在该过程中生成的所有代码都包括功能单元测试，直到质保人员确认接受和“完成定义”标准，用户案例才算完成。Fusion 360 的性能测试也集成到了开发生命周期中。Fusion 360 团队在整个开发冲刺过程中执行负载测试，以便在流程中尽早发现对性能产生负面影响的更改。

3.1 员工培训

作为新员工入职培训的一部分，所有 Autodesk 员工必须认同信息安全的重要性。员工需要阅读、理解并参加有关公司行为准则的培训课程。该准则要求每位员工在开展业务时均应遵守法律、道德规范、诚信，并尊重彼此以及公司的用户、合作伙伴和竞争对手。

Autodesk 员工必须遵守公司有关机密性、商业道德、适当使用和专业标准的指导原则。新员工必须签署保密协议。新员工入职培训强调客户数据的机密性和隐私性。

为了实施安全最佳实践，Autodesk 为工程和云基础架构职能部门中的每个人引入了年度软件安全认证计划 (SSCP)。

4. Fusion 360 产品安全

Autodesk Fusion 360 具有内置的安全功能，从与云服务进行通信到用户可以控制的产品级安全和协作功能，丰富而全面。

4.1 通信安全

Autodesk Fusion 360 和云服务之间的所有通信都需要安全的 HTTPS 连接。

4.2 加密和密码

Fusion 360 与后端服务之间的通信以及后端服务内部的通信都通过加密通道进行。

4.3 身份验证

访问 Autodesk Fusion 360 需要包含 Autodesk ID、用户 ID 和密码的凭据。凭据在网络传输期间受到保护，并仅存储为加盐哈希。

Fusion 360 为最终用户提供了登录时使用多重身份验证的选项。选择启用此功能的用户可以使用授权的安全个人设备（例如手机）来接收要与其密码一起使用的代码。

4.4 数据安全

所有 Fusion 360 设计都保存在云中的加密存储上。该存储解决方案使用 256 位高级加密标准 (AES-256) 来加密数据。

在本地，缓存的设计依赖操作系统用户级权限来进行访问控制。

4.5 设计版本控制

对于每个设计，Autodesk Fusion 360 都会维护一个版本历史记录。版本控制允许用户回滚到早期版本并提供包含每个文件相关修改信息的可审核列表，从而保护数据的完整性。

4.6 基于中心和组的协作安全

项目为授予或限制一组协作者访问 Autodesk Fusion 360 设计提供了简单的基础。项目邀请由项目的所有者或负责人批准，以确保对授予新用户访问权限的成员进行严格控制。

公司可以选择使用团队中心，这样他们可以对成员创建的所有项目行使所有权和访问控制。项目隐私设置（例如开放、封闭和机密项目）允许进行受控制的协作。使用团队中心，成员可以选择将访问权限仅限于已受邀参与项目的协作者。团队中心还允许客户管理员停用前员工的帐户，并将项目所有权转移给团队中的其他成员。

4.7 公共共享

通过公共共享，用户可以与没有 Autodesk ID 或 Fusion 360 授权的外部利益相关方进行协作。Fusion 360 用户可创建一个链接，提供对设计的只读访问。用户还可以选择启用下载/导出功能。用户可以随时撤消此链接提供的公共共享。

5. 云基础架构

云基础架构团队负责定义和执行应用程序版本管理、硬件和操作系统升级、系统运行状况监控的相关过程以及维护 Fusion 360 所需的其他活动。

5.1 高可用性

Autodesk Fusion 360 旨在通过在其支持基础架构中采用冗余系统并在可扩展的实例机群之间分配负载，实现高可用性级别。

5.2 数据复制和冗余

在 Amazon Web Services (AWS) 可用性分区 (AZ) 之间执行客户数据复制。如果需要故障切换到备份数据中心，复制可限制数据丢失或服务恢复延迟的可能性。

5.3 电源系统冗余

AWS 数据中心包含冗余电源系统，以便全天候维持运营。不间断电源 (UPS) 在发生故障时会自动为主电气系统提供备份。每个数据中心的发电机在发生断电时都可提供长期备用电源。

5.4 Internet 连接冗余

冗余多供应商系统用于保持与每个数据中心的 Internet 连接。

Autodesk Fusion 360 客户端软件还具有脱机模式，允许用户在未连接到 Internet 时继续访问和处理其设计的本地副本。

5.5 物理基础架构安全

Autodesk Fusion 360 应用程序在 AWS 安全数据中心上运行，这些数据中心受到一系列安全控制措施的保护，可抵御未经授权的物理访问和环境危害。下面汇总了一些物理和环境控制措施。有关 AWS 安全流程的完整概述，请单击此处。

5.6 设施访问控制

AWS 数据中心由专业的物理安保人员全天候守卫。每个数据中心的周边以及放有计算和支持设备的房间都受视频监控保护。视频监控保存在数字媒体上，允许用户按需查看最近的活动。数据中心入口处设有捕人陷阱，每次仅允许一人进入。所有访客和承包商必须出示身份才能进入，并始终由授权人员护送。只有具有合法业务需求的员工才可获得数据中心访问权限，并且所有访问都以电子方式记录。

5.7 防火

在每个数据中心都装有火灾检测和灭火系统（如烟雾警报器和热激活湿管），以保护放有计算设备和支持系统的房间。在天花板中和高架地板下面装有火灾检测传感器。

5.8 气候控制

如果违反严格的环境范围，数据中心气候控制可保护受故障影响的服务器、路由器和其他设备。系统和人员均可实施监控来防止过热等危险情况的发生。控制系统会自动做出调整，使温度和其他环境测量保持在可接受的范围内。

6. 运营事件管理

Autodesk 实施一项事件管理策略，该策略定义了推动事件解决的最佳实践。Autodesk 事件管理策略强调记录补救步骤并使用根本原因分析来建立可操作步骤的知识库。Autodesk 事件管理策略的目标不仅是要快速、有效地关闭事件，而且要收集和分发事件信息，以便不断改进流程并通过积累的知识来推动未来的响应。

7. 修补程序管理

云基础架构团队实施修补程序管理策略，可帮助确保有效的修补程序展开。如果可能，还会实施自动化以检查新修补程序并准备可由授权的云基础架构人员批准的展开列表。修补程序策略还定义了用于确定修补程序对系统稳定性的影响的标准。如果某个修补程序被标识为可能产生较大的影响，则在展开该修补程序之前先完成回归测试。变更管理可跟踪修补程序在生产系统上的展开。

8. 变更管理

云基础架构团队实施变更管理策略，其中包括以下活动：

- **变更请求 (RFC) 表单。**必须提交 RFC 表单才能进行所有更改。该表单包含变更发起者的姓名、变更优先级、变更的业务理由以及请求的变更实施日期。
- **回退计划。**云基础架构团队会在展开之前创建详细的回退计划，以便在变更导致服务中断时恢复系统状态。回退计划包括脚本中定义的可执行说明，这些脚本可以通过最少的手动步骤恢复系统状态。
- **定义的维护时间。**云基础架构团队会指定计划的时间、应急时间和延长的维护时间。他们会将计划的维护安排在非高峰时段。
- **测试计划。**云基础架构团队会定义一组测试，以验证在展开更改后功能是否可供访问。
- **测试执行。**展开完成后，云基础架构和 Autodesk Fusion 360 QA 团队会执行测试以检查标识为存在风险的功能是否仍然可用。

9. 容量管理

由于客户通过自助服务模式按需配置对云服务的访问，因此流量模式具有很大的变化性，并且会受到使用高峰的限制。当出现峰值时，如果为服务提供支持的计算资源池耗尽，则服务的可用性可能会受到不利影响。为了保持高可用性，云基础架构团队会实施容量管理策略。这些实践包括：

- **频繁记录资源使用情况。**我们会在一系列基础架构组件中频繁收集 Autodesk Fusion 360 资源的使用情况，包括虚拟实例、虚拟存储卷和虚拟网络设备。使用情况统计信息存储在容量管理存储库中。

- **容量规划。**云基础架构团队使用容量管理生成详细的容量计划，以记录当前的使用水平，并根据统计分析和即将发布的业务增强功能的影响对未来使用水平进行建模。容量计划将根据需要进行更新，或者在检测到使用模式发生重大更改时更新。

- **资源分配。**计算资源会根据客户的需求进行分配。预热的计算资源始终可用。如果出现活动高峰，将实例化新资源。例如，Autodesk Fusion 浏览器资源的可用性通常在 10 分钟内就可实现。

- **活动监控。**活动面板和警报在后端服务中定义，工程师可以使用它们观察系统活动并执行事件后的检查和分析。

10. 警报和监控

为了尽可能缩短平均修补时间，Autodesk 使用自动化系统来监控 Fusion 360，以验证服务的运行状况。从数据库到服务的每个组件都单独进行监控。

如果某个事件影响服务，将生成警报，并通过上报流程通知云基础架构团队。

服务运行状况还描述了 Autodesk 服务之间的相互关系。Autodesk Fusion 360 等服务对 ACM 服务（访问控制）非常敏感。每项服务在相关服务出现问题时都必须具有弹性，而当该服务无法再运行时，都应该“优雅地退场”，而不会给客户带来任何数据损失。

Fusion 360 服务的状态由 Autodesk 的运行状况面板服务公开显示：https://health.autodesk.com。

11. 展开期间停机时间为零

将修补程序应用于生产环境时，对于 Autodesk Fusion 浏览器及其他 Fusion 360 服务，我们将采用蓝绿色展开方法。这有助于确保客户不会经历任何服务停机的情况。

12. Autodesk Fusion 360 操作控制

Autodesk Fusion 360 提供对敏感客户数据的保护，防止未经授权的访问。

- **对数据中心实施物理限制。**对数据中心实施物理限制可防止未经授权的各方访问 Autodesk Fusion 360 使用的硬件和支持系统。
- **背景调查。**对于可亲身接触到 Autodesk Fusion 360 使用的计算资源和支持系统的员工，需要执行背景调查。
- **数据复制。**数据复制可跨冗余数据中心复制客户数据，以便在设施之间发生故障切换时可以保持业务连续性。
- **冗余技术**。负载平衡器和群集数据库等冗余技术可限制单点故障。

13. Autodesk 安全

Autodesk 安全团队由一组专业的信息安全专家组成，致力于在 Autodesk 云环境中确定和实施安全实践。Autodesk 安全团队的职责包括：

- 查看 Autodesk 云基础架构设计和实施的安全状况。
- 定义并确保实施安全策略，包括身份和访问管理、密码管理和漏洞管理。
- 通过执行内部审查和审计来推动遵守已确立的安全程序。
- 确定并实施保护客户信息安全的技术
- 邀请第三方安全专家执行信息安全评估
- 监控云服务以发现可能的安全问题并根据需要对事件做出响应
- 对 Autodesk 安全策略执行年度审查。

13.1 漏洞扫描和渗透测试

Fusion 360 服务会进行年度渗透测试和定期扫描以发现安全威胁和漏洞。应用程序还会执行静态分析和第三方库扫描。安全扫描和渗透测试涵盖由开放式 Web 应用程序安全项目 (OWASP) 和 SANS Top 25 定义的广泛漏洞。

13.2 网络安全

我们通过使用物理和逻辑控制（包括加密、防火墙和系统强化过程）组合来强制实施网络安全。此外，AWS 还提供网络安全控制来保护其物理数据中心。有关详细信息，请参见安全性、身份和合规性最佳实践。

13.3 加密

在通过 Internet 将所有网络流量传输到 Autodesk 云环境的周界时，所有网络流量均会经过加密。凭据、应用程序会话信息、访问令牌和用户配置文件等敏感信息将进行静态加密。

13.4 隐私

Autodesk 在收集和使用客户个人数据的方式上保持透明。有关详细信息，请阅读 Autodesk 隐私声明。

14. 资源

以下资源提供了有关 Autodesk 的常规信息以及本文档主部分中引用的其他主题。

- **Autodesk** - 若要查看有关 Autodesk 的信息，请访问 https://www.autodesk.com.cn。
- **Autodesk 信任中心** - 若要查看有关 Autodesk 信任中心的信息，请访问 https://www.autodesk.com.cn/trust/overview。
- **Autodesk Fusion 360** - 若要查看有关 Fusion 360 的信息，请访问 https://www.autodesk.com.cn/products/fusion-360/overview。