《速融云安全白皮书》

2020 年 12 月

速融云技术团队

前言

速融云是一款无代码应用搭建平台，源自创始团队十多年的数字化办公实践，基于自主研发无代码引擎，可以快速搭建专属的 OA、销售、运营、售后、项目管理等个性化办公系统。通过云计算、面向对象存储、虚拟私有网络、微服务、数据分库等前沿互联网技术，来支撑整个平台的高效运行。

1. 安全战略

速融云是企业级别的 Paas 服务提供商，从团队写下第一行代码开始就以提供安全可高的服务为第一原则。因此速融云团队不仅在安全工作上投入了大量的资源，而且也组建了专职专业的安全专家团队，致力于提升平台的安全表现，完成了诸如安全加固、升级、改造工作，保障并推广团队安全政策及措施的普及与落地等。

由于速融云从开始设计就以云原生为设计基础，搭建在阿里云上，用到了许多阿里系的专业服务和能力，因此速融云的可靠性和安全性的起点都特别高。

2.安全组织及保障

1. 安全专员团队

速融云特别设立了平台技术安全保证组，设立了安全专家团队以及安全管理委员会。通过对网络传输安全、数据存储安全、业务安全等分工。各司其职。安全团队还会关注平台设计、研发、运维等整个生命周期的安全问题，及时发现隐患，防患未然。同时，安全团队还致力于通过建立安全平台、代码走查、安全培训等措施。

2. 安全保障团队

速融云购买了高达 500Gbps 的 DDos 硬件防火能力，阿里云 WAF 、阿里云盾、vpc（虚拟私有网络)等安全组件以及服务。整个运行环境依托于阿里云云技术团队，享受国际顶尖的云环境安全保证服务。

3. 安全日常职责

速融云安全团队日常完成如下（不限于）职责：

1） 及时响应阿里云外部安全平台提交的漏洞、入侵检测等，承诺 24 小时内解决上线。

2） 关注 速融云产品技术团队在需求分析、设计、研发、运维过程中存在的安全隐患并予

以解决。
3） 在测试、集成、生产环境中引入漏洞检测与扫描工具，及时发现安全漏洞并予以解决。
4） 依据数据类别及安全等级，设计访问控制策略,通过技术手段制定隔离措施和访问控制管理流程。
5） 依据业务系统访问逻辑，审核访问请求，自动化监控可疑活动（例如：数据 的非授权访问及操作）并实时审计，定期复查其执行情况。
6） 遵循信息安全事件管理标准,依据数据安全性的危害程度定义安全事件类别和 响应流程,提供全天候人工和系统的监控识别、分析和处理信息安全事件的能力。
7） 进行定期的安全演练，验证安全策略的有效性、可靠性和适用性。
8） 定期为团队成员提供安全意识培训,包括个人准则、信息保护、数据安全认证和安全开发等内容。
9） 积极参与安全论坛与会议，吸取业界前沿的安全技术并保持与外部安全专家的交流沟通。

4. 信息资产分类分级管理及安全事件分级管理机制

速融云 团队根据法律要求、价值、关键性对信息安全资产进行了细致的划分，共计 7 大类，每项安全资产均设定了责任人、使用人、CIA 级别（保密性、完整性、可用性）及重要等级，做到专人专项管理及负责。

此外，团队还对信息安全事件进行了分级和定义，根据安全事件的影响程度和范围，制定了不同的管理机制、应对策略、处理及报告流程、总结汇报等。

3 .生产过程安全

1. 保密要求

速融云 团队将严格遵守《中华人民共和国网络安全法》、《网络安全保护法》、《个人信息安全规范》、《中华人民共和国计算机信息系统安全保护条例》、《信息安全等级保护管理办法》、《中华人民共和国电子商务法》、《速融云服务协议》等法律法规和规范性文件及服务协议确保用户敏感信息及业务数据不被泄露。这里定义的用户敏感信息包括但用户个人信息、企业相关敏感信息等，业务数据指 速融云 平台上所保存的诸如看板、文档、需求、缺陷等由用户生成及维护的数据。
此外，依据员工的工作角色进行额外信息安全培训，确保员工管理的用户数据必须按照安全策略执行。

2. 平台研发过程及运维安全

在 速融云 平台的设计、研发、运维、发布等环节中，不会使用生产环境的数据，从而造成用户信息及数据的泄露。

4.系统安全

1. 系统服务及配置安全

速融云 生产环境运行于阿里云 Ubuntu /centos 版本的操作系统上，服务的安装、升级、迁移均由权限受限的运维人员完成，并从指定的可信任安装源下载。系统级服务如 nginx、mysql、redis、mongoDB、RMQ 等的配置文件则由代码库统一管理，通过部署、发布、作业平台进行统一维护和下发。同时也会禁止使用系统级服务的高危接口和函数。
建立补丁管理机制，安全团队会及时跟进并处理业界发布的服务漏洞，并在对改造成本及影响范围进行评估后，及时进行修复或升级。
速融云 平台所有服务器、服务均采用阿里云提供的服务，阿里云服务及相关机房目前已取得网络安全保护等级三级、ISO27000 族等多项认证。

2. 系统访问权限

于生产环境的运维操作，速融云 为后台运维人员提供运维平台进行维护操作，运维平台会维护运维人员的操作权限，并提供操作日志进行审计。
运维人员只能在必要情况下通过堡垒机登录服务器进行操作，并需要在 速融云 运维平台申请临时运维账号及权限，在通过审批后方可操作，相应权限会在运维完成后被及时回收。相关的权限审批、操作日志等均会被审计。
对于数据库、服务器 root 等账号密码，则严格要求定期强制变更，确保账号密码的时效性。
对于日志数据及运营数据的采集，速融云则提供了独立的运维及运营服务器，这些服务器采用更为严格的安全级别，包括外部网络隔离、动态因子校验、IP 访问验证、防火墙单向访问策略等，确保数据的安全性。
速融云的所有服务都运行在 Docker 容器之中，彼此服务之间隔离。实现更高的安全性。

3. 安全开发&运维流程

基于 ISO27001 框架标准建立安全开发及运维框架，为团队制定严格的安全开发流程，定期对全体人员进行安全方面的培训，巩固及完善安全意识。开发、测试和生产环境严格隔离。

5.网络传输安全

1. 传输协议

为了防止中间人攻击，速融云 全站采用 https/SSL 加密数据传输，采用 RSA 算法进行秘钥加密，签名算法则采用安全散列算法较高位数的 SHA-256，来保障密钥的不可破解性。企业级 SSL 证书颁发方为 TrustAisa。

2. 安全域划分

速融云 在阿里云云上的部署采用了 VPC (Virtual Private Cloud, 虚拟私有网络), 将用户数据、公共数据、redis/job 等基础服务进行网络隔离, 将各服务区块限制在各自的安全域中, 保障数据不被泄露。开发、测试、生产环境网络严格隔离。

3. 网络访问控制

在生产环境中, 各子网间通过防火墙、安全策略组等机制, 保证网络访问控制被限制在一定权限内。包括外部的上行出口, 也进行统一化管理。

4. DDos 安全防御

速融云采用购买了电信、联通 核心骨干网的防护资源, 最高可拦截 不低于 500Gbps 的 DDos 攻击服务, 能够有效地防止各类 DDos 攻击。同时通过告警机制, 及时发现攻击行为。

5. 流量监控

对于文件、静态资源等, 速融云依托于国内最大静态资源提供商七牛, 通过独立域名服务, 并对请求的上下行流量进行监控, 在确保不影响用户体验的前提下, 能够及时发现异常请求, 并结合强制下线、封号、客服沟通等措施, 确保及时得到响应和处理。

6.数据安全

1. 按企业分库分级存储

速融云的 业务数据均存储于独立的数据实例, 拥有各自的数据库账号密码, 确保了数据的互相隔离, 防止被拖库的危险。同时, 数据库帐号专号专用, 权限进行了控制, 避免越权漏洞导致数据被破坏。

2. 数据脱敏

所有数据库敏感信息, 包括用户敏感信息、数据库账号密码等均采用 MD5 加盐处理, 加密因子定期更换。

3. 文件存储

使用七牛提供的 对象存储，来存储所有附件、文档、公共资源等文件，具有扩容方便、安全及可靠性高等优点。。权限方面，则按企业进行权限控制，并通过旁路系统进行权限校验。

4. 生产环境数据权限

除非得到用户授权,否则 速融云团队任何成员被禁止生产环境数据,包括运维人员， 接触的形式包括但不仅限于数据库访问、文字、截图、视频等，更不会私自篡改数据， 避免给用户造成信息泄露。

定期对数据库操作日志进行审计。

5. 数据销毁管理

对于长期无访问记录企业（非付费）对应的数据，速融云 承诺会在 3 个月内予以保存，但逾期的， 数据会有被清理的风险。

速融云平台提供直接注销企业的操作，对于此类操作，一经用户确认，则被销毁的数据将无法恢复。

所有存储数据的存储介质(如硬盘等)，如若需要维修必需先进行卸载；需要报废或移出数据中心的网络设备及存储设备,依据相关安全标准进行清除数据、磁盘消磁以及物理销毁。

6. 数据备份安全

确保数据备份、运营统计等环节的数据安全。数据备份文件在存储、传输过程中， 严格控制权限，确保不被泄露。平台运营统计所涉及到的数据经脱敏、二次加工处理， 防止信息泄露。

7.应用及业务安全

1. 账号及密码安全

速融云 账号体系支持 手机、 飞书、微信、企业微信登录，并实现了 飞书 账号、企业微信账号同步。 平台会记录用户每次登录行为，生成常用 IP，若在非常用登录地点上登录，则会及时同时用户。

此外，平台也会监控账号的异常操作，如多次恶意尝试登录、多次越权操作等，均会有实时告警及下线、封号、封 IP 等相应措施。

2.业务权限

速融云平台采用自研的访问控制组件。被授权用户只能访问指定项目数据；在项目内部，速融云平台则提供基于权限组的权限控制，可对业务对象、操作类型、工作流流转等多维度进行访问权限控制。

3.接入安全

速融云平台引入了阿里云的 WAF，可在接入层阻断恶意请求，有效防止注入类及 XSS/CSRF 攻击请求。

4.业务逻辑安全

速融云安全团队会通过在代码框架层面引入参数过滤、数据二次校验等机制，防止在业务逻辑层出现漏洞，同时也会推动研发团队对此类安全机制严格落地。此外，团队还会定期排查系统中可能存在的业务逻辑隐患。

5. 消息通知

速融云平台提供了种类繁多的消息通知机制，包括微信消息、企业微信、站内信、短信、企业 QQ、第三方接入等等，为了确保功能及接口不被恶意利用，平台会对消息通知的频率、关键词、发送者等作过滤和限制，保证平台在消息通知方面的安全性。

6. 数据接口安全

速融云平台提供 API 服务，该子系统通过独立域名提供服务，通过 OAuth 接入，与主平台通过数据库读写分离、微服务等方式进行了解耦，传输过程全程加密。同时，API 系统也在 IP、帐号、数据操作权限等方面进行了严格限制，确保不发生数据泄漏、篡改的情况。此外，在访问频率上，API 系统也有非常严格的规定。

8. 操作日志监控及审计

1. 操作日志获取

速融云平台通过点击流、feed、访问 log 三种日志形式，从性能、详细操作记录等不同角度进行采集，但所有实际业务数据并不落地，仅对操作类型进行记录。此外，所有记录都有时效性，平台将只保留一年的详细日志，超过一年的将作归档处理，因此会进一步丢失细节。

2. 日志审计

速融云将部分日志提供给企业管理员、运维人员进行审计，但仍会有严格的权限限制和相关的审批流程。

3. 日志监控及告警

对于敏感的操作行为，如项目创建、文件下载、人员信息获取等，有越权或者超出频率的，平台则会进行告警，时效性视具体操作不同而不同。

9. 高可用解决方案

1. 速融云高可用及灾备

速融云高可用建设内容：

1） 数据分库：速融云将各企业的数据独立存储，在物理上进行隔离，当有企业的数据发生损坏时，不会影响到其他企业的正常使用。

2） 数据备份/恢复：在速融云数据备份的基础上，速融云 还提供按业务对不同级别的数据进行备份的服务，并且能快速进行恢复。

3） 健康检查：速融云云会对关键业务页面/模块、服务器资源使用情况等进行实时检查，及时发现高负载、高延迟、页面响应慢等情况，提前发现系统问题， 并进行告警。

阿里云高可用及灾备

1） 由于 速融云部署在阿里云上，因此本身便具备了阿里云的高可用能力，此外， 在此基础上，速融云云还作了适配和改良。

2） 云服务器虚拟技术：阿里云服务器采用了高性能高稳定性的虚拟技术，提供高可靠的 web 服务器、数据/文件存储等服务。而 速融云云购买部署的，则是阿里云上高规格的服务器。

3） 负载均衡：将来自前端的请求，分发到后端云服务器上，并能自动检测后端主机健康度，动态调整分发权重，甚至不分发，以此保障服务的高性能及高可用。

4） 服务器镜像：可将标准化的服务器进行镜像备份，当发生服务器物理损坏时， 能通过虚拟技术及镜像文件，快速部署生成新的同质服务。

5） 数据库高可用：实施双机热备，提供高性能分布式数据服务。

6） 异地容灾：服务器异地部署，降低因不可抗力导致的机房物理损坏等灾难给系统带来的影响。

2. 灾演及应急预案

建立应急响应团队及完善的业务连续性管理，针对不同级别的故障，速融云制定了相应的应对预案，并定期进行演练。此外，服务器、数据库等在异地均有全量备份，最坏情况下，在所有硬件遭遇完全灾难性损毁时，承诺 24 小时内完全恢复服务。

10. 安全认证及其他

速融云正在申请 ISO27001:2013 国际安全认证以及公安等级三保认证，在信息安全认证方面均有可靠保证。