

文档密级：公开

钉钉安全白皮书

版本（V3.0）



■ 声明

本文档任何文字叙述、插图、方法、过程等内容，版权均属钉钉所有，受到有关产权及版权法保护。

本文档仅供读者了解钉钉安全体系使用。任何个人、机构未经钉钉的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ 版本变更记录

时间	版本	说明
2016-04-15	V1.0	版本创建
2018-04-16	V2.0	版本修订
2021-11-25	V3.0	版本大幅修订

目 录

1 前言	1
2 安全合规.....	1
2.1 体系建设.....	1
2.2 拥抱监管.....	1
2.3 内控审计.....	2
2.4 廉正合规.....	3
3 安全文化.....	3
3.1 安全组织.....	3
3.2 人才理念.....	3
3.3 社会责任.....	4
4 安全责任共担.....	5
4.1 基础架构安全	6
4.2 钉钉应用安全	6
4.3 用户数据安全	7
4.4 业务安全运营	7
5 全链路安全防护	7
5.1 标准钉钉.....	8
5.1.1 客户端安全	8
5.1.2 传输安全.....	9
5.1.3 服务端安全	9
5.1.4 基础设施安全	11
5.1.5 安全运营.....	13
5.2 专有钉钉.....	15
5.2.1 专有钉钉安全设计	15
5.2.2 客户端安全	16
5.2.3 传输信道安全	18
5.2.4 接入控制安全	19
5.2.5 服务端安全	19
5.2.6 密码安全.....	20
6 产品安全	22
6.1 即时通讯.....	22

6.1.1 全链路数据加密.....	22
6.1.2 聊天记录.....	22
6.2 音视频.....	22
6.2.1 加密语音通话.....	23
6.2.2 安全视频会议.....	23
6.3 文档和钉盘.....	23
6.3.1 云端安全存储.....	23
6.3.2 权限管控.....	23
6.4 钉邮.....	24
6.4.1 账号安全.....	24
6.4.2 加密传输.....	24
6.4.3 日志查询.....	24
6.4.4 防欺诈.....	24
6.4.5 反垃圾和反病毒.....	25
6.5 通讯录.....	25
6.5.1 对内权限分级.....	25
6.5.2 对外保护隐私.....	25
6.6 专有钉钉安全中心.....	25
7 数据安全.....	27
7.1 数据生命周期安全.....	28
7.1.1 数据产生.....	28
7.1.2 数据传输.....	28
7.1.3 数据使用.....	28
7.1.4 数据存储.....	29
7.1.5 数据共享.....	29
7.1.6 数据销毁.....	29
7.1.7 数据安全审计.....	30
7.2 以数据为中心的安全.....	30
7.2.1 静止态数据（Data at rest）.....	30
7.2.2 传输态数据（Data in transit）.....	31
7.2.3 使用态数据（Data in use）.....	31
8 隐私保护.....	32
8.1 隐私采集保护.....	32
8.1.1 黑白盒扫描.....	33
8.1.2 隐私 API 监控.....	33
8.1.3 代码审计.....	33
8.2 隐私共享保护.....	34
8.3 隐私使用保护.....	34

9 生态安全	34
9.1 生态安全体系建设	34
9.2 安全责任共担	35
9.2.1 平台安全责任	35
9.2.2 开发商安全责任	36
9.2.3 企业安全责任	36
9.2.4 用户安全责任	37
9.3 基础安全	37
9.3.1 主机安全	37
9.3.2 网络安全	37
9.3.3 应用安全	38
9.4 内容安全	38
9.4.1 风险发现	38
9.4.2 反馈机制	38
9.4.3 监管对接	38
9.5 数据安全	39
9.6 应用生命周期安全管理	39
9.6.1 入驻签约	39
9.6.2 创建应用	39
9.6.3 开发应用	40
9.6.4 产品共创	40
9.6.5 产品验收	40
9.6.6 产品运营	40
9.6.7 退出市场	41
9.7 安全赋能	41
附录	42
术语/缩略语	42

1 前言

随着移动办公的日益普及，即时通讯软件的应用场景越来越多，技术创新为我们生活、工作带来便利的同时，也带来了敏感信息泄露、无用信息干扰、消息传递不及时等诸多问题和隐患。

钉钉自 2015 年面市以来，作为中国领先的智能移动办公平台，其以淘宝、天猫、支付宝等积累的多年安全经验为前提，经过三年的沉淀创新以及阿里巴巴集团 11 万多名员工的使用锤炼，目前已建立强大的移动办公生态保障体系，为 1900 万企业组织提供“简单、高效、安全”的服务。

为加强 1900 万企业组织对钉钉安全的认知，本文档重点从安全合规、安全文化、全链路安全防护、产品安全、数据安全、隐私保护、生态安全、专属安全八个维度，全面阐述了钉钉安全技术工作思路和实践方法，旨在向社会公众披露钉钉努力抵御互联网各类攻击，防范用户信息泄露，保护企业和公民个人合法权益的决心。

2 安全合规

2.1 体系建设

根据《中华人民共和国网络安全法》要求，参考 ISO27001、ISO27018、PCIDSS、SOC 2/3、GDPR、TrustE、GM/T 0054-2018 以及信息安全等级保护等国内外标准和最佳实践，结合阿里巴巴集团多年互联网安全工作经验，钉钉建立了覆盖安全策略方针、组织及人员安全、研发安全、运行安全、外包安全以及信息安全的业务连续性和合规审计等十四个控制域的安全体系。每个控制域建立了规范的四级文档架构和可配置的度量体系，所有安全流程基本实现线上化，过程数据指标化，运营度量平台化，全面覆盖钉钉各项安全控制措施，有效保障钉钉安全、稳定、合规。

2.2 拥抱监管

在阿里巴巴集团安全部“轻管控、重检测、快响应”的“九字方针”指导下，钉钉积极开展安全合规认证工作，截止目前，先后获得并通过如下认证审核：

信息安全等级保护：信息安全等级保护是由公安部监制，由属地公安机关认可并颁发的国家级信息系统等级认证。在 2016 年度，公安部组织多支国家队伍对钉钉信息系统进行等级测评、风险评估和渗透测试，评估结果在经过多位院士和行业安全专家评审后，确定钉钉信息系统安全等级为“三级”，钉钉安全控制措施符合国家要求。

ISO/IEC 27001：ISO27001:2013 信息安全管理体系是世界应用最广泛的信息安全管理标准。钉钉国内首家获得 ISO27001:2013 认证的移动协同办公平台服务商，通过该认证建立的钉钉信息安全管理体系（ISMS），覆盖了产品研发、业务运营、安全保障、营销推广等全生命周期，实现钉钉信息安全管理的第一位“责任人”按照明确的“规范”、遵守标准的“流程”并输出有效的过程“记录表单”，从而持续有效保障钉钉业务和数据的机密性、完整性和可用性。

ISO/IEC 27018：ISO/IEC27018:2014 是国际标准化协会制定的首个云端隐私保护标准，其重点关注数据收集、使用、存储等必须获得用户授权，且用户对其存储的数据具备完全的控制权和合理的透明度等。

SOC2 安全审计报告：SOC 报告即 Report on System and Organization Controls。报告的内容框架和格式由美国注册会计师协会（AICPA）制定，其重点关注企业安全性、过程完整性、可用性、保密性和隐私性相关的服务控制。

GM/T 0054-2018：GM/T 0054-2018 是国家出台的《信息系统密码应用基本要求》，用于商用密码应用安全性评估（简称“密评”）。钉钉专有版中商用密码的均符合密评规定的合规性、正确性和有效性。

钉钉先后通过了国家公安部监督认证的三级等保认证、ISO27001:2013 信息安全管理体系认证、ISO27018 公有云体系下的用户隐私认证以及全球知名会计事务所普华永道出具的 SOC2 类型二安全审计报告，标志着钉钉安全实践已达到国内领先、国际一流的安全标准要求，标明用户在使用钉钉的过程中，其数据的保密性、完整性、可用性和隐私性已经与国内外最佳实践进行对标，且得到独立的第三方安全鉴证和审计。

2.3 内控审计

随着钉钉业务飞速发展，业务的创新引起的技术变革让内控合规工作变得充满挑战，因此钉钉根据阿里巴巴集团安全管理要求和安全度量体系实践，定期邀请集团安全合规团队对钉钉安全管理工作的合理性、安全控制措施的有效性开展定量和定性的风险评估和安全审计，全面推行集团安全策略要求，及时发现可能存在的安全合规风险，提升安全水位，实现安全体系持续改进。

2.4 廉正合规

钉钉日常业务开展过程中，一旦发现泄露用户隐私、恶意篡改用户数据、非授权执行违规操作等异常行为，廉正合规部门将依据《商业行为准则》、《员工纪律制度》、《安全红线》等安全规章制度开展安全合规审查，视情况给予处罚，严重情况下予以辞退处分，并永不录用；特别严重将保留追究民事责任乃至刑事责任的权利。

3 安全文化

3.1 安全组织

钉钉自成立以来，充分认识到信息安全在业务发展中的战略地位和对业务的支撑作用，在阿里巴巴集团 CRO 领导下，建立了规范的信息安全管理组织架构，设立安全管理委员会，下分安全产品团队和安全运营团队。

其中安全产品团队主要来自集团安全部，全面负责钉钉业务客户端、传输通信及服务端的防御产品研发、接入、监控、加固和风险识别、评估、处置等工作。安全运营团队由集团安全部以及钉钉各产品线相关人员组成，主要负责安全技术运营以及业务合规检测和审计，通过各类异常信息计算、分析、建模、预警，快速响应业务系统潜在的网络运行风险，并在不断对抗中，推动优化各项安全措施，全面提升钉钉整体安全水位。

此外，为快速响应业务，钉钉事业部建立了灵活的 Scrum 小组，按需与集团安全部经过多年沉淀的安全技术、安全业务、安全生态以及数据安全等安全能力无缝对接，快速复用集团全链路的动态防御体系，全力保障钉钉业务安全稳定运行。

同时，针对特殊时期以及业务需要，建立各种各样的工作小组，如安全架构评审小组、数据隐私治理小组、应用安全专项攻关小组，docker 安全小组，加强跨团队协调沟通，快速响应钉钉各种业务需求。

3.2 人才理念

为支撑组织的安全运营，阿里巴巴为全体员工建立“客户第一、员工第二、股东第三；因为信任、所以简单；唯一不变的是变化；今天最好的表现是明天最低的要求；此时此刻、非我莫属；认真生活、快乐工作”的新六脉神剑价值观和“聪明、乐观、皮实、自省”的人才理念，这种价值观和人才理念的影响已经以显而易见的方式渗透至钉钉员工招聘、员工入职、员工持续教育以及离职审计活动中，确保钉钉的员工安全管理符合集团安全策略要求。

其中在员工招聘录用时，用人团队主管通过电话面试、现场面试等方式对候选人的技术能力进行仔细考察，确保候选人符合岗位职责要求。技术面试通过后，还必须经过 HR 面和背景调查，确保应聘人员品行性格、职业道德符合要求。

员工入职时，首先必须签署劳动合同和保密协议，关键岗位人员视接触信息的敏感程度还需单独签署专项保密协议。然后参加《商业行为准则》培训，明确我们作出的、为客户提供公平公正、安全可靠的承诺。同时还会开展《数据权限安全》、《员工行为纪律》、《安全红线》等相关培训，明确组织对于安全管理的要求和规定，了解个人在日常工作中所承担的义务以及违反相关安全管理要求时面临的惩戒措施。

日常工作过程中，钉钉员工通过线上学习平台和线下专题分享的方式自主选择参加感兴趣的技能培训，同时定期接受组织的强制性安全意识培训和考试，考试成绩和认证通过情况在平台上进行留存和管理。

员工调岗离职时，HR 和部门主管共同确定岗位应回收的信息资产、关闭应用权限，对于关键岗位员工还需视情况签署竞业协议并开展离职审计；对于违反安全管理要求的员工，依据员工纪律条款和约定进行处理。

3.3 社会责任

中国有 4300 万中小企业组织，以及数十万中小学教育组织，目前市场上的软件服务企业只为大约 10 万家大型企业服务，而小型企业分散，平均生存周期约 2 年，社会资源为一家中小企业服务的投入往往是没有性价比的，因此如果能聚合广大中小企业的共性需求，打造一个公平，透明，高效的生态共享平台，那么所有企业将在社会资源利用、企业办公协同等多个维度都在同一条起跑线上出发。

为实现大企业和中小企业之间社会资源平等，秉承钉钉“让工作学习更简单”的愿景，通过“简单、高效、安全、快乐”的方式为中小企业提供企业协同办公服务，这也是钉钉的产品初衷和社会责任。

4 安全责任共担

钉钉的产品形态中主要包含三种形态：SaaS 版、专属版、专有版。



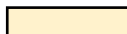
SaaS 版的客户群体主要包含中小企业单位等组织，可在公开的应用市场中下载，运营主体为钉钉。所有用户使用相同的客户端、服务端。由钉钉统一管理、维护。

专属版主要服务于部分定制化要求较高的企业等组织，服务端使用 SaaS 版相同的服务器，服务端的运营主体为钉钉。但客户端可进行较多的定制，可集成一些第三方的 SDK 满足客户定制化要求。

专有版主要服务于大型政府、企业。钉钉作为技术服务提供方交付整个平台给客户。运营主体为客户，客户端、服务端可根据客户需求高度定制化，满足客户高级别安全需求。

在这三种不同的交付形态下，钉钉与客户分别承担不同的责任，定制化程度越高代表客户需要承担更多的责任。而安全责任与运营主体密切相关，根据《网络安全法》、《信息安全等级保护管理办法》等法律法规的要求，网络运营者应承担保障网络安全、稳定运行的责任。因此，钉钉在不同的产品形态下会与用户分担不同的安全责任。

钉钉（SaaS 版）	钉钉（专属版）	钉钉（专有版）
业务安全运营	业务安全运营	业务安全运营
用户数据安全	用户数据安全	用户数据安全
钉钉应用安全	钉钉应用安全	钉钉应用安全
基础架构安全	基础架构安全	基础架构安全

图例说明：钉钉的责任： 客户的责任： 共担责任：

钉钉将安全责任按照不同分类划分为四种：

4.1 基础架构安全

基础架构安全主要是指钉钉服务器所在的基础环境的安全，包括部署钉钉服务器所依赖的物理环境、操作系统、数据库、中间件、等基础服务的安全措施。包括服务器所处的物理环境安全，如：物理位置、物理访问控制、防盗窃和防破坏、防雷击、防火、防水、防潮等措施。操作系统层面的安全，如：操作系统访问的身份鉴别、操作系统层面的访问控制、主机及网络的入侵防范、恶意代码防范。数据库等其他中间件的安全，如：数据库的身份鉴别、数据库的访问控制、数据库的加密、其他中间件的身份鉴别及访问控制等。

对于钉钉的 SaaS 版和专属版，钉钉负责管理、运维这些基础环境，因此有钉钉负责这些基础架构环境的安全。而对于专有版，由于整体基础架构平台由客户提供，钉钉不负责其基础环境的运行维护，因此在专有版的部署形态下，由客户负责基础架构安全，而钉钉不承担这部分责任。同时，我们也推荐客户采购阿里云专业的安全服务，保障基础架构的安全。

4.2 钉钉应用安全

钉钉应用安全包括钉钉服务端的安全、钉钉客户端的安全。主要包括代码层面的安全，包括常见的 WEB 安全漏洞、客户端安全漏洞等因钉钉应用代码编写产生的漏洞发现及修复。同时也包括钉钉应用因引入第三方组件而产生的安全风险控制需求，也属于应用安全。

对于钉钉服务端安全，钉钉均需要保障平台代码的安全。包括客户端及服务端的漏洞发现及修复方案制定。钉钉鼓励各界用户积极挖掘钉钉系统的应用漏洞，并通过阿里巴巴集团应急响应中心上报给钉钉进行处理。对于 SaaS 版和专属钉钉，钉钉应在漏洞修复补丁发布后及时修复。而对于专有版钉钉，客户应在收到更新通知后及时更新版本修复漏洞，保障钉钉平台及时更新，修复最新的安全漏洞。专有版钉钉的客户应设立安全负责人，对钉钉平台的安全运营负责。

对于钉钉客户端安全，对于钉钉主动引入的第三方组件，钉钉有责任通过事前预防、事中监控、事后处置等安全手段保障供应链安全。而对于专属版和专有版钉钉，由于部分三方组件由客户提供，因此客户需要对这部分三方组件的安全进行保障。客户有责任对其要求引入的第三方 SDK 进行安全审查，并从机制上保障第三方 SDK 可持续更新，修复自身存在的漏洞及避免非法行为。

对于在钉钉工作台上访问的第三方应用或企业自建应用。应由其开发者保障应用安全，开发者有责任对其开发的代码进行漏洞发现及修复。钉钉可对开

发者进行安全开发的指导，帮助开发者开发更安全的应用。但开发者需要对其编写的代码承担安全责任。第三方应用的开发者应与客户明确权利责任，防止权责不清。

4.3 用户数据安全

用户数据安全主要包括用户个人信息的安全、组织架构信息的安全、聊天消息的安全等用户在钉钉平台中录入的数据的安全。这部分数据由用户产生，在钉钉平台中承载，部分数据经过用户授权会传输到第三方产品。用户对这些数据拥有运营的权利，包括增、删、改、查等。

对于钉钉 SaaS 版、钉钉专属版，用户的数据在钉钉运营的服务器上承载，钉钉承担保护这部分数据机密性、完整性及可用性的责任。而对于钉钉专有版，用户的数据在客户的服务器上承载，因此需要客户承担这部分责任。

在钉钉的管理后台中或钉钉的客户端上，钉钉的用户也可接触到这部分数据，因此，钉钉的客户需要采用一定的管理和技术手段防止使用钉钉的用户泄露这部分数据，客户应当负责由于用户侧泄露数据导致的风险。用户应使用钉钉平台的能力，进行合理的安全配置，以降低数据泄露带来的风险。

4.4 业务安全运营

业务安全运营主要包括业务的安全风险管理、组织架构设立、运营机制等方面。这部分内容主要由客户负责，客户可根据自身组织的需要评估使用钉钉过程中容易导致的各种风险，并建立风险管理制度，通过激励及处罚机制保障制度落地。如：禁止用户发布非法言论，禁止将组织敏感数据发送到组织外部，禁止截屏泄露组织敏感消息等。

这部分安全运营机制由于与客户的业务息息相关，根据客户业务的不同而应设立不同的机制，这部分的主要责任由客户承担。客户应在符合相关法律法规的要求下使用钉钉，客户应仔细阅读并理解用户使用协议，合理使用钉钉平台帮助自己的业务发展。当客户对钉钉的使用与国家有关要求冲突时，钉钉有权根据用户使用协议禁止或限制客户对钉钉的使用。

5 全链路安全防护

在阿里巴巴集团安全部“轻管控、重检测、快响应”的九字方针的指导下，钉钉在客户端，包括 PC 端和移动端以及传输管道、服务端等多个维度完整复制了阿里巴巴集团各项成熟的、经过多年验证的安全控制措施，建立了完整的事前动态管控、事中实时防御、事后快速响应的纵深防御体系，确保钉钉用户使用安全。

5.1 标准钉钉

5.1.1 客户端安全

钉钉通过应用完整性、环境可信性、数据机密性三个维度的强化加固，有效保障了钉钉客户端安全。

5.1.1.1 应用完整性

钉钉 App 基于阿里聚安全的核心技术，在应用发布前，通过重新编译、代码混淆、加壳保护等安全加固措施以及自主研发的安全组件接入，快速复制了淘宝、支付宝等超级 App 的移动安全保护能力，极大保障了钉钉客户端安全。

代码混淆：通过将代码中的变量名和方法名转换成不具备语义的乱码名称，并增加代码分支跳转逻辑复杂度，提高逆向工程阅读代码的难度。

应用加壳：对二进制文件加入壳保护，隐藏程序实际入口，防止被逆向工程反汇编、动态调试等。

自研安全组件：钉钉 App 自主研发了安全组件，提供安全加解密、加签验签、防重打包等安全能力。

5.1.1.2 环境可信性

钉钉 App 通过模拟器检测、越狱和 Root 检测、防恶意调试及进程注入检测等安全措施对应用运行环境提供了安全保障。

模拟器运行检测：钉钉 App 在每次程序唤醒时可检测应用是否运行在模拟器中。

越狱和 Root 检测：钉钉 App 每次程序唤醒时可检测终端操作系统是否已经被 Root。

终端进程注入检测：钉钉 App 运行时，对用户终端运行环境是否有异常进程加载进行动态监测。

提供应用沙箱环境：钉钉 App 的进程空间和数据存储空间均在安全沙箱内，与其他进程完全隔离，外部无法访问。

5.1.1.3 数据机密性

钉钉 App 对缓存在客户端的数据信息，采用安全沙箱和安全加密方案，保障用户数据信息的安全性。针对信息安全要求较高的企业，提供三方加密服务，实现数据信息二次加密。

安全加密：钉钉 App 在客户端加解密过程中使用随机生成的密钥，并与设备绑定。破解者即使拿到了用户手机上的加密数据，在自己的手机上也无法完成解密操作，极大的保证了存储在客户端本地的数据安全。

安全沙箱：钉钉 App 在客户端的整个进程数据都在安全沙箱中隔离，对外不暴露任何密钥和加密算法。

安全签名：基于 HMAC_SHA256 算法和指定密钥对数据进行加签，在传输数据时，可以利用加签的结果对传输数据进行安全校验。

5.1.2 传输安全

基于 TLS 1.3 协议，钉钉构建了一套完整的私有安全通信协议 LWS，使用 ECDH Curve25519 作为非对称加密算法，对称加密算法支持 Chacha20-Poly1305 与 AES-256-GCM。通过这种私有安全通信协议，实现钉钉整个通信链路上的加密、签名，防止窃听、篡改，以确保数据信息的传输安全。

5.1.3 服务端安全

5.1.3.1 应用安全开发生命周期

阿里巴巴面向互联网的应用每天至少面临数百万次攻击，基于每一次安全响应经验的积累，参考业界 SDL 实践经验，阿里巴巴安全部已形成一套规范的应用安全开发生命周期管理体系，并全面覆盖钉钉所有业务。

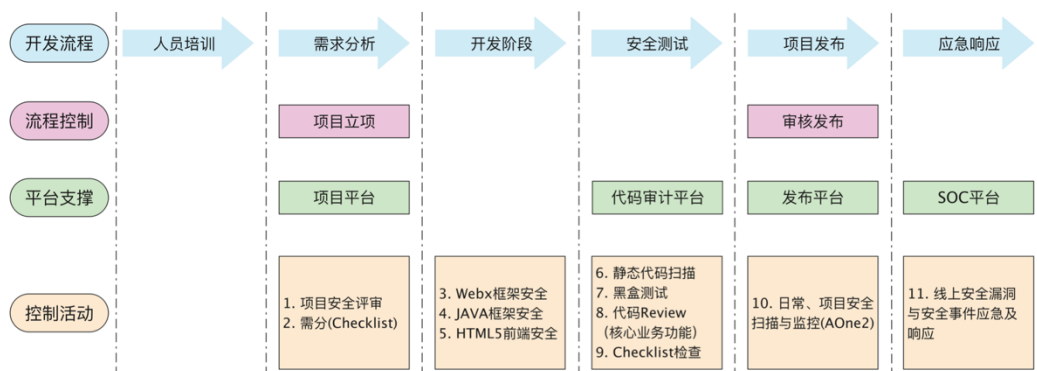


图 4.1 钉钉 SDL 流程图

在人员培训环节，安全工程师通过线上平台和线下安全课堂的方式，为开发人员提供安全开发规范、安全技能培训，提高开发人员的安全意识；

在安全需分环节，根据功能需求文档进行安全需求分析，针对业务场景、业务流程、技术框架进行沟通，形成《安全需求分析建议》；

在安全开发环节，开发工程师必须安装阿里巴巴自研的 IDEA 插件，实现编码规范性和安全性实时检测和提醒，确保代码编写符合《阿里巴巴 Java 开发手册》和相关安全编码规约要求；

在安全测试环节，通过自主研发的扫描工具进行黑白盒扫描，并结合人工审核评估代码缺陷和漏洞，降低各个阶段来自人员知识技能、业务场景逻辑所带来的安全风险；

在项目发布环节，安全工程师必须对应用系统进行一系列的上线前安全检查，包括代码审查，黑白盒测试，检查相关的测试结果并确保发现的问题都被处理完毕之后才可上线。

在安全运营与应急响应阶段，安全工程师通过 SOC（Security Operation Center）安全运营平台实现安全事件分析、处置、复盘和跟踪。

另外，基于 SDL 各阶段数据沉淀，钉钉建立了应用安全量化分析模型和监控体系，形成各条产品线的安全开发度量地图和基于项目组、项目成员在每个阶段的行为画像，一旦发现异常行为（如未执行白盒扫描、违规带高危漏洞发布、未通过安全培训上岗编码等），及时告警从而监督相关人员进行整改，最终实现需求人员理解安全、开发人员知道安全、测试人员懂得安全、安全人员可以管理安全的目标，从而提高业务系统安全编码质量，保障应用安全稳定运行。

5.1.3.2 数据库安全

阿里巴巴通过对 MySQL 的定制优化形成 AliSQL，在大幅提高性能的同时，还按需进行功能定制和服务裁剪，为钉钉的数据库稳定运行提高了强大的支持。同时，为安全便捷的对数据库进行统一操作管理，阿里巴巴自主研发了一套数据库管理平台 iDB，实现数据库统一认证、权限管理、数据变更、库表同步以及操作安全审核，确保每一条 SQL 语句都符合安全要求和性能规范。此外，阿里巴巴自主研发的 CloudDBA 产品为钉钉提供系统化、专业化的数据库诊断优化能力，可轻松对数据库实例进行一键全面诊断，包括资源使用、慢 SQL、会话/事务，锁，空间，配置，安全等，并给出详细诊断报告和优化建议。

5.1.3.3 中间件安全

钉钉服务端使用的中间件，采用分布式权限系统进行身份识别和访问控制，有效保护数据源、消息等敏感信息的保密性。

5.1.4 基础设施安全

5.1.4.1 物理安全

在物理环境管理方面，温度、湿度、电力、消防等物理环境安全是数据中心安全可靠运行的必要前提。因此钉钉业务所在数据中心严格按照《电子计算机机房设计规范》（GB50174）、《电信专用房屋设计规范》（YD5003-2014）的 A 类要求进行选址、建设或租赁，确保空调、电力和消防等系统均采用智能化、高稳定性、全冗余设计，在任意单点设备故障或异常事件情况下，均能自动触发告警并进行快速响应。

在访问控制管理方面，进入数据中心必须提出申请，并提供个人身份信息证明，经过授权后方可进入机房，进入前需由安保人员查验证件和登记，且值班人员全程陪同。数据中心内部根据业务重要性和功能划分不同安全区域，不同区域之间拥有独立的门禁系统，重要区域采用指纹等双因素认证，特定区域采用铁笼进行物理隔离。

在物理监控巡检层面，阿里巴巴设立 GOC（Global Operations Center），实时监控数据中心物理环境、设备运行、流量分布等状态，实现运营指标数字化、运营流程自动化，运营响应智能化，打造高效准确的故障处置能力。

此外还采用专业团队 7*24 小时值班，线上业务定时自动巡检和定期人工检查，有效发现异常报警信息，及时、准确地通知处理人，跟踪处理进度，并定期进行复盘总结，直到最后解决。

在运营安全管理层面，IDC 管理团队为数据中心建立物理安全指引和操作安全管理规程，梳理物理安全检查基线和资产安全检查基线，定期开展安全审计，及时盘点现有管理措施的合理性、执行的有效性，并持续改进。

5.1.4.2 网络安全

阿里巴巴集团整体网络主要分为 ABTN 和 ACTN，其中 ABTN 由各地数据中心出口路由器与各大运营商互联，并通过 BGP 协议建立冗余、扩展的广域网络；ACTN 是阿里巴巴集团为各地数据中心运营管理、数据同步交互而建立的内部网络。互联网用户访问请求流经外部骨干网，经过异常流量清洗平台监测管控，实现四层到七层的 DDoS 防御、机器行为和 Web 攻击流量的清洗后，访问数据流到达目标服务器，从而提高业务访问的可靠性和纯净度。

在每个数据中心内部，建立统一标准化的网络拓扑，并划分不同安全区域，依据每个区域承载业务的重要程度，又划分多个安全级别，不同级别区域之间部署严格的访问控制和路由策略，同时通过流量分光镜像和 flow 采样，实现流量 DPI/DFI 分析和监控，有效识别异常行为。

5.1.4.3 主机安全

为加强钉钉业务主机系统安全管理，遵循阿里巴巴集团“九字方针”要求，在管控机制上，阿里巴巴集团定制优化 Docker、Nginx 等系统组件，裁剪不必要的服务、最小化开启业务所需的服务和端口，统一配置模板，从源头加强自主管控，降低漏洞发生的可能性。在访问管理时，通过 SSO 集成 AD 域和阿里安全客户端的 OTP 实现主机登录双因素验证鉴权，同时利用网络层访问控制策略和虚拟安全访问组实现基于 IP 地址和端口的安全控制，并通过自动化的访问控制策略 review 工具每天检查策略合规情况，一旦发现违规开放端口信息，立即通过短信、邮件、钉钉消息进行告警，确保相关人员迅速处理。

在事中检测机制上，通过主机部署入侵检测 agent，实现系统异常进程、主动外连、后门程序、暴力破解、系统权限提升等异常行为的风险监测；操作通过堡垒机的运维监控以及目标主机日志审计，实现多粒度的安全分析，及时发现可能存在的风险；另外定期通过镜像漏洞扫描工具直接扫描软件仓库，确保系统组件安全稳定；每天通过基线扫描工具，自动化实现系统服务、端口进

程、软件包、流量等基线指纹探测识别，及时发现可能存在的异常行为。同时在 APT 对抗上，自研 agent 覆盖办公终端和生产服务器等服务深度集成，保证全天候、无死角的异常行为收集，并通过云端多款国际领先的杀毒软件，结合业务场景和多监测引擎的综合评分机制，有效降低漏报误报，提供业内领先的 APT 检测服务。

在事后响应机制上，利用不断迭代的安全算法模型，计算钉钉业务云、管、端的异常行为分布以及入侵特征，反哺优化防御策略，实现已知漏洞一键止血、未知漏洞快速响应、恶意文件云端查杀、系统补丁使用 ksplice 实现快速灰度验证和更新。

5.1.5 安全运营

5.1.5.1 反入侵

钉钉业务每天都产生海量的日志数据，包括终端行为日志、网络安全日志、系统运行及入侵检测日志、WAF 防护日志以及网络流量、基线检查等信息。基于这些日志，阿里巴巴通过大数据安全分析平台，借助模式匹配、沙盒分析、机器学习、专家经验等规则，有的放矢提取情境数据，建立用户行为画像，实现异常行为数据的自动识别、分析和关联，还原攻击路径并进行全链路风险打标和综合评分，精准有效感知业务系统可能存在的风险隐患以及特定的 APT 攻击，同时与异常流量清洗平台联动，实现一键处置，保障业务系统的安全性和客户数据的隐私性。

5.1.5.2 红蓝对抗

阿里巴巴安全部组建独立的攻防演练团队，以攻击者视角全面梳理攻击途径，有计划性进行渗透测试工作；同时建立攻防演练平台，内置历史攻击数据、漏洞库、基础资产信息和专家经验，每日开展攻防一练、每月开展全链路演练；另外定期邀请 ASRC 白帽子开展安全众测。在持续对抗中，快速、高效、全面的发现阿里巴巴各类业务系统的（包括钉钉）安全漏洞，推进业务整改的同时，沉淀攻击特征，优化安全检测和防护管控策略，保障业务系统安全稳定运行。

5.1.5.3 应急响应

阿里巴巴集团通过统一的安全事件应急管理平台，实现安全事件发现、处置、溯源、复盘等闭环管理并持续运营，全面提升突发安全事件的应急管理水平，确保业务系统安全稳定运行。

在安全事件发现阶段，该平台通过 OpenAPI 与黑白盒扫描产品以及威胁情报系统、ASRC 等平台打通，并与资产管理系统进行关联，实时收集安全事件相关域名、IP 信息，根据这些信息自动将事件详情流转至相关安全应急响应专家。

在安全事件处置阶段，安全应急响应专家 7x24 小时实时响应，一旦收到短信、邮件、钉钉消息提醒后，在规定时间内，确认安全事件是否误报、影响范围、风险等级等信息。如确认误报，终止流程；如确认是已知类型安全事件，关联已有解决方案并将流程转至事件受影响业务的开发和运维工程师。如确认是未知类型安全事件，安全应急响应专家协调安全研究、产品防御、攻防对抗人员提取事件特征，制定临时止血措施，同时加强流量和行为监控，明确安全解决方案，并协助业务方进行整改。

在安全事件溯源阶段，溯源取证团队将按需收集受影响的业务端、管、云的活动日志，并进行综合分析，全面还原安全事件发生过程，并进行针对性的整改加固，如有需要还将配合公检法部门进行立案处理。

在安全事件复盘阶段，安全事件应急管理平台运营人员根据事件类型、事件排名、业务分布等信息，定期组织人员进行复盘，总结分析事件根本原因，以针对性提升事前管控、事中检测机制和流程。

5.1.5.4 账号安全风控

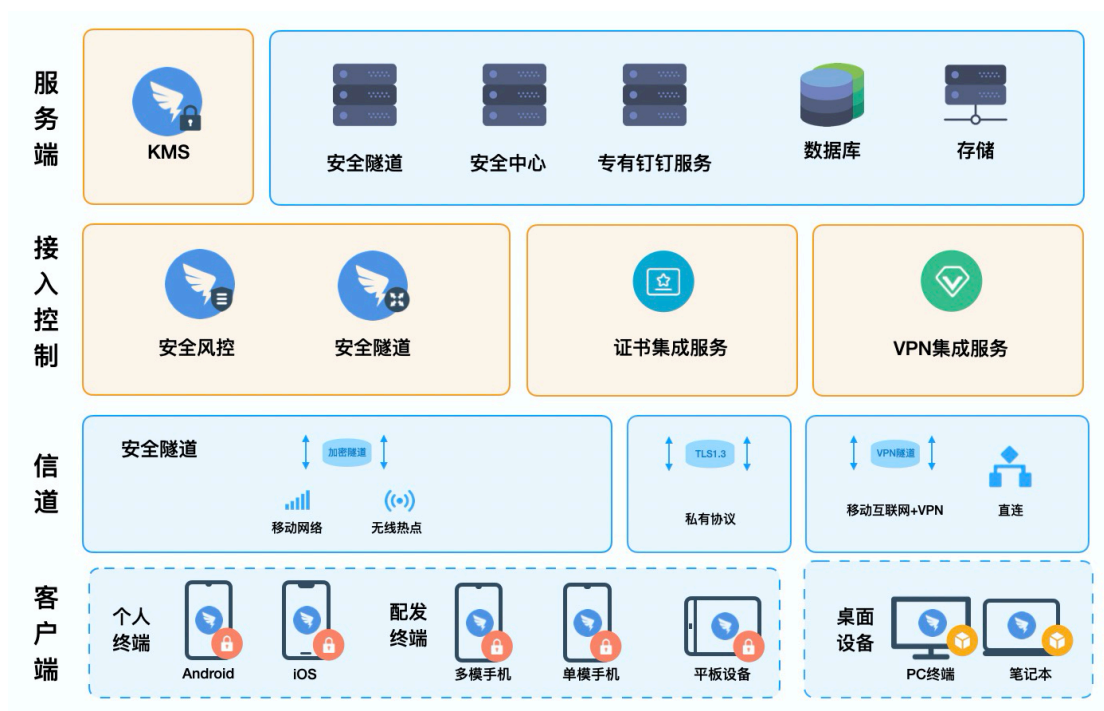
钉钉通过阿里巴巴自建的账号安全风控体系，实现账号和设备风险打标，一旦检测到非可信设备登陆立即触发双因子验证。同时，通过账号监测平台，对同设备批量登录等异常行为进行检测、告警，并通过一键配置黑名单实现迅速处理。

除已有的账号安全风控体系外，钉钉还提供其他扩展的账号安全控制措施，如短信验证码、生物特征识别、好友关系识别等方式，为用户账号提供更多维度的安全保障。

5.2 专有钉钉

5.2.1 专有钉钉安全设计

为了满足移动办公系统的部署要求，消除移动办公潜在风险威胁，专有钉钉提供一体化解决方案，如下图：



专有钉钉系统以客户端、网络、接入控制以及服务端组件构成。

客户端：支持 Android 和 iOS 系统，同时支持特定的双系统多模式场景；桌面端 Windows 和 macOS 系统；

信道：专有钉钉通过互联网、安全隧道、移动专网、政务外网或企业办公网直连、VPN 等方式安全接入专有钉钉服务；

接入控制：由访问控制服务和接入中继服务组成，支持与证书服务和 VPN 网关对接集成。

安全中心：提供规则、用户、设备、应用、审计等维度的安全风控管理。

服务端：由专有钉钉用户服务、消息服务、设备服务、应用服务、开放平台、数据库存储等服务组成。

加密服务：部署于服务端，为客户端加密套件提供密码认证、通道保护密钥协商、群组密钥分发、组织结构信息加密及文件加解密等功能。

5.2.2 客户端安全

专有钉钉支持多种场景、多种终端的安全使用需求，通过终端程序安全、终端数据安全及终端管控安全三个维度的强化加固，有效保障了专有钉钉客户端安全。

5.2.2.1 终端兼容场景

专有钉钉覆盖多种场景安全使用，包括个人设备、专用配发设备以及桌面设备的使用。

个人设备场景：移动办公设备为个人所有，用户使用个人智能设备（包括 Android 和 iOS）接入网络进行移动办公的场景也是目前远程办公的主要场景。

配发设备场景：配发场景的移动设备一般分为两类，一种是提供到专职人员的工作专用终端，一般为平板或手机；另一种为配发到员工的日常办公手机。

专用业务终端场景：专用工作终端一般工作于特定的专网模式下，终端无个人数据，采取按需申领，结束归还的模式。在安全要求上则采取较高标准，从终端安全、信道安全、接入安全、应用数据安全等维度进行全方位防护；

专用配发办公场景：专用配发终端一般为政府或企业统一采购终端，配发到具体的使用人员，使用者可安全使用个人常用应用，但主要最为日常办公终端。

1、专用普通单模式手机：专用普通单模式手机，远程办公选择一般为单 Android 系统的智能终端；

2、专用双系统/双域终端：专用双系统或双域终端一般为统一采购为特殊行业的专业终端，系统搭载双 Android 系统或单一 Android 系统可进行多种模

式切换，个人数据一般放置于生活系统/模式，办公应用和数据则部署于工作模式/系统中。

配发桌面终端办公场景：台式机和笔记本电脑一般处于政府或企业专用网络中，采用传统的桌面端接入方式。

5.2.2.2 终端程序安全

专有钉钉使用专业的加固技术，在应用发布前，通过重新编译，安全加固，实现了对终端程序的应用完整性校验、防篡改保护等多个维度的强化加固，有效保障了专有钉钉终端程序的安全性。

应用完整性校验：攻击者时常会通过篡改终端程序安装包代码，再使用编译工具，如 apktool、dex2jar、JEB 等，对应用程序进行二次打包、分发，从而窃取用户敏感信息、盗取用户账户等。专有钉钉通过安全加固，实现在安装时，对应用进行完整性校验，如果存在风险，则无法正常安装应用，有效的避免了由此造成的相关风险；

防篡改保护：攻击者时常通过篡改应用程序的核心代码、资源文件、配置文件等，实现程序挂马、开挂等高风险攻击行为。专有钉钉通过安全加固，高度混淆和加固了终端程序的重要文件，极大的保障了终端程序的安全性；

5.2.2.3 终端管控安全

专有钉钉自带终端应用管控能力，可支持终端应用级安全合规管理能力，包括终端应用控制、终端合规管理等能力。

终端准入控制：可支持设置准入的终端系统版本号、用户常用设备绑定及新设备登录开启二次验证等；

终端应用控制：可支持管理员远程数据擦除、远程毁钥等；

终端合规管理：可要求终端合规使用，如终端 ROOT/越狱后自动删除专有钉钉客户端数据并销毁密钥。

5.2.2.4 终端数据安全

专有钉钉自带客户端数据安全管控能力，可支持客户端应用级数据安全合规管理能力，包括客户端程序数据脱敏、客户端本地沙箱文件存储加密、客户端日志防泄漏、安全遮罩等能力。

客户端数据脱敏：客户端安装程序（APK 包、IPA 包）中清除敏感信息、测试信息、后门信息，确保客户端安装程序的安全性；

客户端本地沙箱加密：客户端本地沙箱中的敏感问题，如 Database 目录、SD 卡存储的信息，均实现了数据级别的加密存储，同时专有钉钉也对客户端本地沙箱中的文件权限进行严格限制，多方位确保本地文件的安全性；

客户端日志防泄漏：专有钉钉会对日志输出接口进行拦截和敏感信息过滤，确保日志中不会泄露用户的敏感信息；

安全遮罩：专有钉钉客户端应用切换到后台时，自带安全遮罩效果，坚决守护用户的隐私安全。

5.2.3 传输信道安全

基于 TLS 1.3 协议，专有钉钉构建了一套完整的私有安全通信协议 LWS，使用 ECDH Curve25519 作为非对称加密算法，对称加密算法支持 Chacha20-Poly1305 与 AES-256-GCM。通过这种私有安全通信协议，实现专有钉钉整个通信链路上的加密、签名，防止窃听、篡改，以确保数据信息的传输安全。

同时专有钉钉还提供了安全隧道集成能力，可以给客户提供安全接入内网的 SSL 隧道，且支持集成第三方 VPN 产品。

私有协议安全接入：专有钉钉采用私有协议构建客户端与服务端的安全隧道，采用 TLS1.3 方式加密，保护传输安全；

双层加密信道：可使用双层加密信道构建安全连接，对于高敏内网应用提供传输链路高级保护，同时避免内部端口对外暴露，降低入侵风险。

移动互联网+VPN 接入：移动互联网+VPN 方式为最为常见的智能终端、桌面终端接入政务外网或企业办公网的方式，可为支持的 VPN 厂商提供空载隧道或 VPN 配置加载服务(需 VPN 厂商支持)。

直连接入：政务外网或企业办公网的台式机、笔记本办公的主要接入方式。

VPN 集成服务：专有钉钉可支持 VPN 集成，可针对客户现有部署的 VPN 产品进行集成服务(需 VPN 厂商支持)；

国密服务：可选择使用国密算法对数据进行加密，保障数据传输安全。

5.2.4 接入控制安全

安全风险控：可针对接入终端、接入应用和接入用户进行控制授权，确保合法请求接入，为请求分配最小化权限；

安全隧道：支持向移动端提供接入中继服务，业务请求可安全快捷的访问政务外网或企业办公网区域业务，且无需开通防火墙入站端口，减低网络攻击威胁；

证书集成服务：可支持 PKI 证书相关的集成服务及配置；

VPN 集成服务：可支持集成原有的政务外网或企业办公网 VPN。

5.2.5 服务端安全

专有钉钉严格遵循阿里巴巴应用安全开发生命周期管理体系，保障应用全生命周期的安全性。专有钉钉服务端由安全中心、加密服务、专有钉钉服务、数据库及存储服务组成。

安全中心：专有钉钉安全中心提供规则、用户、设备、应用、审计等维度的安全风险控管理。

加密服务：部署于服务端，为客户端加密套件提供密码认证、通道保护密钥协商、群组密钥分发、组织结构信息加密及文件加解密等功能。

专有钉钉服务：由专有钉钉用户服务、消息服务、应用服务、开放平台、数据库存储等服务组成。

数据库：主要包括专有钉钉数据库服务。

存储服务：主要包括专有钉钉存储服务。

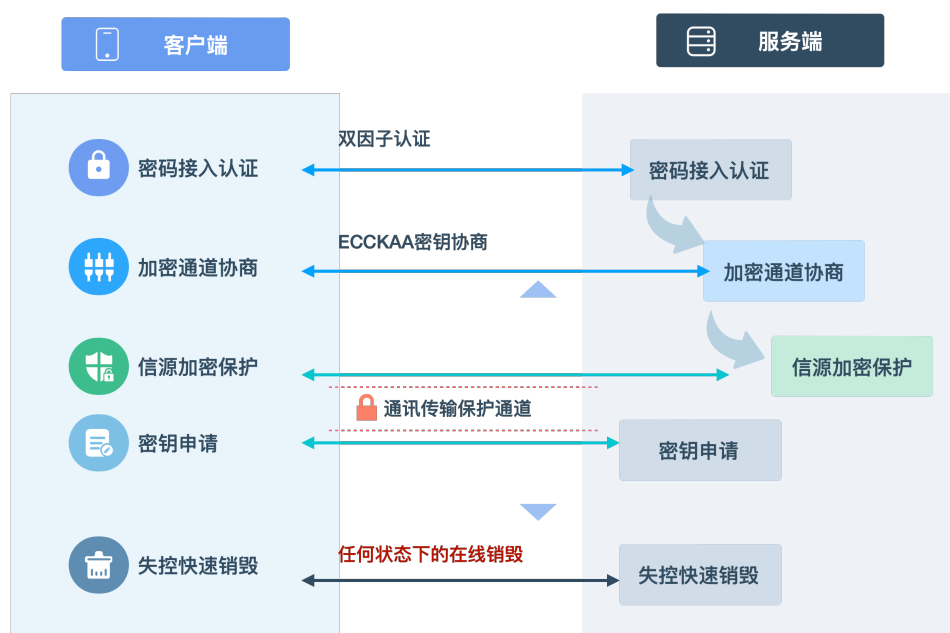
5.2.6 密码安全

5.2.6.1 全要素国密保护强度

基于国家密码管理局批准的国密算法构建了专有钉钉全业务的密码安全防护体系，设计了满足业务加密需求的多层密钥体系，保证用户体验不受影响的情况下，同时为业务信息流提供国密算法强度的密码保护。

同时，专有钉钉在密码部件上采用国家密码管理局认可的物理噪声源，在业务执行过程中对噪声源进行自检，以确保所产生的随机数满足 GM/T 0005-2012 规定的随机性检测规范。

5.2.6.2 全体系密码内生安全



密码接入认证：密码服务以用户及终端特性为基础，结合 PKI 公钥密码认证技术，设计满足专有钉钉多种使用场景的“一人一证”实体身份鉴别与身份认证，密码接入认证结合专有钉钉安全机制，构建接入信任链，实现密码与安全双重保险的接入认证能力。

加密通道协商：专有钉钉在通过密码接入认证后，在客户端与服务端之间基于 SM2 椭圆曲线公钥密码算法的 ECCKAA 协商，构建安全保密的密钥交换传输通道，为后续密钥分发和业务指令提供高保障的传输加密能力，该安全保密通道具备前向安全，确保以前的信息丢失不影响现在以后的信息安全。

信源加密保护：专有钉钉除了在密钥交换传输通道进行加密外，对本地数据及需要交互的数据均做了信源加密，进一步降低应用数据丢失风险，所有信源加密密钥均加密保护或者保存在不可读取的密码部件中。

密钥实时保障：专有钉钉在多层密钥体系中设计了完善的保障机制，用于实时加密的工作密钥随机产生，一次一变。

失控快速销毁：专有钉钉为安全控制台提供按终端、按用户的失控快速销毁功能，同时在密码设计上，对用户密钥进行两两分割设计，所有客户端使用的用户密钥各不相同，确保任何一个客户端的密钥失控，不会影响全网用户的安全性。

5.2.6.3 全流程会话一次一密



一次一密：专有钉钉采用密码技术实现了端与端之间的消息级的“一次一密”，确保单聊、群聊等业务中产生的每条消息的密文均不一样，满足用户消息传递的安全保密。

一话一密：专有钉钉的密码体系实现了每个会话使用不同密钥加密的特性，同时不影响文件转发等业务的高效运转。设备密钥泄露风险较一个组织一个密钥的方案风险降低为 $1/N$ (N =单组织产生的会话数量*单个设备具有的会话数量)

5.2.6.4 全业务数据加密服务

专有钉钉可支持应用内所有业务数据（包括客户端和服务端）加密，除了即时消息加密外，还为其他应用数据提供加密服务。

组织结构信息加密：专有钉钉支持对组织结构、通讯录等信息的业务数据加密。

即时消息加密：专有钉钉支持对即时消息进行加密，如文字、语音、图片、视频、文件消息等。

其他业务加密：专有钉钉支持对专有钉钉种的其他非即时消息业务进行加密，如：钉盘、待办、日志等。

6 产品安全

限于篇幅，本章重点介绍钉钉的典型产品及其安全功能，更多的软硬件产品和服务可以访问钉钉官网（<https://www.dingtalk.com/>）。

6.1 即时通讯

6.1.1 全链路数据加密

钉钉消息的传输从发送方客户端发出，经过网络传输到钉钉服务器，再由接收方客户端接收的全链路通信过程，涵盖端、管、云三个方面，均经过高强度加密算法的保障。

在传输层，钉钉通过基于 TLS 1.3 实现的自研加密算法 LWS 对所有数据加密，握手阶段通过非对称密码算法 ECDH Curve25519 交换密钥，并支持 Chacha20-Poly1305 与 AES-256-GCM 对称加密算法对消息内容进行加密。在客户端上，存储的数据库经过 AES-256 算法实施的整库加密。在服务端上，通过 OSS 对象存储实施加密。

此外，所有内部群的聊天对话框均包含数字水印处理，如发生截屏泄露事件可准确溯源。钉钉还支持企业使用第三方加密服务，由企业自主掌管密钥并对企业内部信息二次加密，任何外部人员均无法解开。

6.1.2 聊天记录

钉钉客户端的聊天记录与服务端实时同步，支持消息的撤回和删除，一端操作，多端同步。在群聊场景下，支持管理员对指定人员禁言及其消息的撤回，防止因员工误操作导致的信息泄露事件。对于企业员工，企业管理员无权看到员工的个人聊天记录，员工隐私得到有效保障。

6.2 音视频

6.2.1 加密语音通话

钉钉提供基于网络的免费语音通话功能，对通话双方语音实现了实时双向加密保护，且通话过程无法被手机录音，保障了沟通双方内容机密性的要求。

6.2.2 安全视频会议

钉钉视频会议功能提供了丰富的权限管理功能，确保多种使用场景下的安全管控需求，核心功能包括：

录制管理：会议主持人可开启禁止录制功能，除主持人外所有参会人员均无法录制会议内容。

共享屏幕管理：会议主持人可选择仅主持人共享屏幕，避免会议成员误操作、恶意操作影响会议的有序进行。

锁定会议：会议主持人可开启仅允许主持人可邀请其他成员加入会议功能，严格控制与会人员名单。

入会口令：通过分享链接入会时，需要输入 11 位数字口令，避免口令猜解的可能性。

内部会议：仅允许组织内部成员加入，外部人员即使获得会议链接和口令也无法进入。

全员强制静音：开启后仅主持人可发言，保证大型会议能有序进行。

6.3 文档和钉盘

6.3.1 云端安全存储

文档主要包括聊天中产生的文档和存储到钉盘的文档。聊天文档多端同步，对于单聊文件、普通群文件等，提供至少 6 个月的云端免费保存服务。如果需要长期保存，单聊文件可以手动转存到私人钉盘，群文件可以由群管理员开启群文件同步到钉盘功能。

6.3.2 权限管控

企业的文档，所有者可以按需配置文档的查看、下载和编辑权限，权限从小到大依次为：“仅可查看”、“可查看/下载”、“可编辑”，最大程度避免了文档外泄的风险。权限设置的范围支持按部门、群维度设置，即便人员变动，也能智能同步权限变更。此外，支持对文件或文件夹独立设置权限范围。

根据使用对象，企业用户的钉盘分为企业盘和私人盘两个部分，两类云盘之间互相隔离。私人盘只归属于个人，企业和其他员工均无法看到个人的私人盘。企业盘归属于企业，企业管理员可以针对部门或个人灵活分配权限，包括文件的查看、下载等。当员工需要分享企业文件到外部时，可以通过文件外链分享功能，最大支持外链分享 7 天，且必须提供正确的文件提取码。

6.4 钉邮

6.4.1 账号安全

钉邮是钉钉的邮件功能模块，管理员可通过管理后台统一绑定企业邮箱。钉邮与阿里邮箱深度集成，可以在钉钉客户端或阿里邮箱客户端使用。钉邮支持多种登陆方式，包括钉钉扫码登陆、账号密码登录、阿里邮箱扫码登录，并设有异地登陆提醒、防暴力破解、防撞库扫号等安全保障。

6.4.2 加密传输

钉邮使用 POP3、IMAP、SMTP 等标准邮件通讯协议，并支持 SSL/TLS 标准加密传输协议，满足敏感数据加密传输的要求。

6.4.3 日志查询

钉邮提供详细的日志查询功能，记录用户钉邮的登陆日志和行为信息。登录日志记录了每一次登陆的时间、地点、IP 地址、登陆结果；行为信息记录了用户对信件的收取、发送、删除日志。满足了事后审计邮箱行为安全的需求。

6.4.4 防欺诈

钉邮对接了阿里云防钓鱼库，每日有专业的安全团队负责更新防钓鱼库规则，一旦邮件正文中检测到疑似钓鱼 URL 会将邮件分配到隔离区，并提醒用户警惕邮件安全。

6.4.5 反垃圾和反病毒

钉邮接入了阿里云邮箱自研的智能反垃圾系统，基于先进的大数据分析和人工智能算法，能够智能识别可疑的发件人、操作行为、邮件内容等，综合提升对用户垃圾邮件的拦截率。同时，反垃圾系统还具备病毒查杀引擎，提供对附件安全性的扫描能力，为邮件内容安全赋予双重保障。

6.5 通讯录

6.5.1 对内权限分级

钉钉通讯录代表了一个企业的组织架构，是每个企业的敏感信息。钉钉提供了分级权限管控来保障通讯录安全。针对部门层面，钉钉支持隐藏企业敏感部门，企业其他部门的人不可见该敏感部门人员，进一步还支持配置部门人员仅可见自己，更细粒度保证企业通讯录的最小够用。针对个人层面，钉钉支持隐藏若干个人信息字段，充分保护企业高管和员工的信息。

6.5.2 对外保护隐私

针对第三方应用开发者需要调用企业通讯录数据以提供更多定制化服务的情况，钉钉制定了严格的接口审批和权限审批制度，并提供了通讯录开放平台作为统一数据出口，避免由 ServerAPI 或 JSAPI 导致的敏感字段泄露。

6.6 专有钉钉安全中心

专有钉钉支持应用级数据安全解决方案，可针对专有钉钉自身以及第三方原生应用和 H5 应用提供应用和数据安全管控。

6.6.1 应用账号安全

专有钉钉应用身份安全为办公应用的使用，构建完整的身份保障体系，包括多端登陆管理、APP 锁定方式、登陆地域限制。

多端登录管理：支持用户与登录设备的相关配置管理，包括：可登录平台设置、登录设备数量等；

APP 锁定方式：可支持设置手势密码、指纹锁等方式保护应用安全；

6.6.2 应用数据安全

专有钉钉数据安全能力保障整体的办公落地数据安全，主要通过禁止文件下载到本地、企业/个人数据隔离、应用数据远程擦除等能力保护专有钉钉数据安全。

禁止文件下载：用户在专有钉钉中传输的文件，可支持通过在线预览的方式进行查看或编辑，可禁止用户下载到移动终端本地，防止移动终端丢失带来的本地数据泄露威胁。

安全沙箱：构建安全沙箱空间，对企业和个人数据进行隔离，办公区数据存储于隔离区域，保障非授信应用无法进行数据访问或被读取，在安全沙箱内可启用数据防泄漏策略，禁止应用内截屏、禁止应用内数据转发以及禁止应用内文件使用第三方应用打开等。

应用数据远程擦除：对于终端丢失或者被窃的突发情况，可支持对客户端数据进行远程擦除，保障数据泄露。

密钥销毁：针对设备丢失或密钥泄漏、敏感时期防止暴力破解的情况，专有钉钉提供密钥的远程销毁能力确保数据安全。

6.6.3 应用数据防泄露

专有钉钉数据防泄漏可防范办公人员对敏感信息、涉密信息、文档等数据有意识，或者无意识泄露的行为。具体能力包括专有钉钉自身及办公应用数据被第三方应用打开管理、应用水印溯源、应用内复制粘贴管控、应用截屏/转发/分享控制。

应用数据被第三方应用打开管理：可限制应用内文件或者链接通过第三方应用打开，防止数据外泄；

应用水印溯源：可针对办公应用进行应用级水印覆盖，水印内容可关联用户信息、账号信息以及应用信息，并可对水印内容进行编辑；

应用内复制粘贴管控：可限制办公内应用向非安全应用进行拷贝、粘贴、复制等，防止数据外泄；

应用截屏/转发/分享控制：可限制自身客户端和第三方应用进行截屏、转发、链接分享等操作，防止数据外泄。

H5 应用水印：可针对 H5 应用进行应用级水印覆盖，对所访问的 H5 应用全部启用水印，同时可对水印自定义配置。

6.6.4 访问控制

专有钉钉访问控制能力保证用户信息及组织架构可见性的安全，包括跨部门的可见性控制及功能的权限控制。

跨部门的可见性控制：可设置部分用户仅可查看本部门的通讯录、部分部门通讯录对其他部门不可见、根据任职属性和职级不同设置不同的权限。

功能的权限控制：部分用户可限制他人查看自己通讯录中的敏感字段、可限制其他用户对特定用户的功能权限，如电话、DING 等功能。

6.6.5 安全审计

专有钉钉的安全审计能力，可以对专有钉钉应用访问操作进行审计，同时提供对移动终端的状态变化及用户违规行为等安全事件进行审计，审计记录包括：登陆事件审计、查看手机号行为审计、管理员操作审计、用户截屏审计、设备异常审计等。

6.6.6 软件容错

使用过程中，对于软件本身出错导致无法正常使用，专有钉钉提供有效的软件容错能力，保证业务不间断的情况下启用备用方案，如：高可用、降级使用等方案。

7 数据安全

数据安全和隐私保护是钉钉的生命线，打造用户的持续信任是钉钉的第一要务。钉钉为全球 1900 万家中小型企业提供组织数字化协同服务，已经拥有超过 5 亿的用户，广泛分布于企业、政府、学校等各种组织。钉钉按照高标准、严要求的行为准则，主动承担起保护用户数据安全的责任和义务，充分践行用户第一的安全标准。

钉钉凭借深耕企业服务领域的多年经验，以保障用户隐私和数据安全为首要职责。充分遵守阿里巴巴集团提出的“数据保护倡议”，用户数据的所有权归用户所有，绝不会将数据移作它用；严格遵循 DSMM 的各项安全要求，在数据安全生命周期各个阶段，从数据产生、数据存储、数据使用、数据传输、数据共享到数据销毁，都无缝嵌入阿里巴巴集团各项成熟的安全管控措施，确保用户数据的机密性、完整性、可靠性。充分做到数据有度，管理有方。

钉钉深知数据是一个企业组织最有价值的核心资产，针对数据生命周期的各个环节，围绕数据的三种状态，建立了以数据为中心的安全技术体系。数据的三种状态由数据科学家 Daniel Alleni 提出^[1]，分别为静止态数据（Data at rest）、传输态数据（Data in transit）、使用态数据（Data in use），以数据为中心的安全体系更加关注于采用技术手段保护数据本身，为数据整个生命周期安全性提供完整的三重保障。充分做到数据为本，技术为盾。

7.1 数据生命周期安全

7.1.1 数据产生

钉钉制定数据安全策略规范，按照数据类型、敏感程度、数据价值等相关属性明确数据分类分级标准。在数据产生时，统一对数据进行分类分级打标，确保业务流转过程中，所有数据按照策略规范要求实施分类管控、分级授权。

7.1.2 数据传输

钉钉面向互联网的应用，必须接入统一应用网关，实现 TLS 加密以及证书统一管理，保障全站 HTTPS 安全访问；面向内部涉及签名认证或加密类业务，必须统一接入加密机，数据交互通过加密机 API 实现不同应用的签名、认证和加密。密钥托管和密码服务由经过严格安全设计和审核的 KMS 服务提供，且与各种云产品集成加密，方便实现自定义加密和数字签名。密钥自始至终只留存于 KMS 加密机内，任何方式均无法导出，保障数据的机密性、完整性、可用性和不可否认性。

7.1.3 数据使用

[1] Wikipedia.Data in use[DB/OL].https://en.wikipedia.org/wiki/Data_in_use, 2020-07-23.

在钉钉前端应用层面，涉敏页面全部数字水印处理，敏感信息已默认打点隐藏。

在服务端应用层面，必须统一接入权限管理系统，访问主体必须根据权限、角色和风险级别按需申请，并详细说明访问内容、访问理由、访问时长等相关信息，获得的访问权限定期复核，离职转岗后权限自动关闭。

在数据库操作层面，增删改查的操作命令全程监控，操作日志集中存储，操作流量实时分析，一旦发现高危 SQL 语句、批量违规操作、危险时段异常操作等违背安全管理要求的行为，及时告警并可实时在线拦截。

7.1.4 数据存储

客户端的用户聊天信息（包括消息文本、图片、音视频和其他文件）采用高强度的对称密钥算法 AES-256-GCM 实施整库加密保护，并根据用户可信设备信息生成唯一的密钥，保护存储在客户端的敏感数据不被攻击者非法获取，确保本地数据的机密性。

服务端的每个应用采用独立密钥，通过高强度对称密钥算法 AES-256-GCM 加密数据，且每个企业密钥各不相同，由硬件加密系统统一管理，保证了服务端数据存储的安全性。

7.1.5 数据共享

在对外数据开放共享方面，钉钉严格遵循《网络安全法》要求，以用户隐私信息保护为首要前提，制定对外数据披露细则，明确要求所有对外数据输出必须遵循以下原则：

保护用户隐私：涉及用户隐私数据未经客户的充分授权，不得收集、分析或向任何第三方输出。

必要性和最小化：对外数据输出时必须将数据的范围、数量及知情者控制在最小范围内，因法律法规要求需向公众公平公开输出数据的情况除外。

合规性：对外数据合作必须遵循适用于阿里巴巴集团的法律、法规、政策、行业标准等要求。

7.1.6 数据销毁

钉钉使用的信息处理设施，存储介质在退出数据中心前遵照 DoD 5220.22-M、NIST 800-88 标准进行清除数据、磁盘消磁以及物理销毁，避免数据泄露风险。

7.1.7 数据安全审计

在数据生命周期，钉钉建立了全链路风险检测感知体系，通过语境分析、行为过滤和专家运营，实时检测分析异常数据访问记录，如登录失败、权限升级、非法访问、敏感数据下载等，一旦发现异常行为及时告警，确保违规操作有迹可循。

7.2 以数据为中心的安全

7.2.1 静止态数据 (Data at rest)

静止态数据指的是以任何形式存储在物理介质上，完全未被访问或使用的非活跃数据。例如，设备内部存储的文档、云端数据库、外部硬盘驱动器上的文件、存储区域网络中保留的数据、异地备份服务器上的文件，都属于静止态的数据。静止态的数据通常处于稳定状态，它不在系统或网络中移动，也不受任何应用程序或 CPU 的处理。

钉钉采取了多种技术手段来保护静止态数据，防止用户数据泄漏。

数据加密：存储在钉钉本地客户端和云端服务器上的数据库、文件均经过高强度密码算法加密，加解密密钥由 KMS 服务统一管理，做到密钥与数据隔离存放，确保用户数据安全。用户的即时聊天消息、图片、企业通讯录、个人信息、企业信息等数据均通过数据库的方式统一存储，用户的文件通过阿里云对象存储 (Object Storage Service, OSS) 服务存储。

对于数据库加密，在钉钉客户端，数据库采用 AES-256-GCM 算法进行整库透明加密，即加解密操作对数据库访问程序无感知，仅在存储到磁盘时进行，既保证了存储丢失情况下数据库的机密性，又保证了终端设备处理速度的高效性；在钉钉云端服务器，数据库采用记录型加密，即所有数据内容经过加密后再存储到数据库中，既保证了用户数据在云端不可信环境下的机密性，又能保持原有的数据结构，为数据库维护提供了便捷性。

对于文件加密，采用了云端服务器 OSS 加密方式。上传数据时，OSS 对收到的用户数据进行加密，然后再将得到的加密数据持久化保存下来；下载数据

时，OSS 自动对保存的加密数据进行解密并把原始数据返回给用户，并在返回的 HTTP 请求 Header 中，声明该数据进行了服务器端加密。

移动设备管理（Mobile Device Management, MDM）：针对移动办公场景，钉钉企业定制版本支持由启迪国信提供的移动设备管理策略，包括应用防截屏、防分享、防剪贴板外泄、远程擦除等能力，也支持由企业根据自身需求自建相关能力。

7.2.2 传输态数据 (Data in transit)

传输态数据指的是通过网络从一个端点移动到另一个端点的数据。例如，通过钉邮、即时消息发送的信息都是传输态数据。在现代化企业办公方式下，人员的跨地区移动和移动办公设备的增多都给数据传输的网络环境引入了极大的风险，数据容易遭受中间人攻击而被窃取。

钉钉采取了多种技术手段来保护传输态数据，防止用户数据被窃取。

加密传输协议：钉钉自主研发的私有安全通信协议 LWS，基于 TLS 1.3 进行定制和优化，支持 ECDH Curve25519 非对称加密算法、Chacha20-Poly1305 和 AES-256-GCM 对称加密算法，具备防重放攻击、弱网优化等特性。钉钉所有端上消息传输均通过 LWS 协议传输，保证了整个通信链路的加密，有效杜绝中间人窃听和篡改。

三方加密：三方加密指的是在钉钉自有加密的基础上，由第三方加密服务提供商对企业消息数据进行二次加密，加密后的密文存储于钉钉服务器上，加密密钥托管于第三方密钥服务器。通过密文和密钥分离保管的方式，保证了除信息所有者外，任何第三方包括钉钉和服务提供商在内均无法解密查看聊天信息，确保了企业数据的安全性及私密性。

钉钉目前支持由安恒密盾提供的第三方加密服务，具备国密算法资质，采用 SM2、SM3、SM4 标准国密算法，所涉及到的密码相关模块均获得国密局授权商用密码产品批号。通过密钥密文分离的理念、完善的密钥管理体系、高可用的热备灾备方案，充分保证数据上云的安全性，提升用户与平台间的信任程度，增强用户对自身数据的可控性。

7.2.3 使用态数据 (Data in use)

使用态数据指的是系统正在更新、处理、访问的处于活跃状态的数据。例如，正在解压的文件、查看的文档都是使用态数据。常规的对称加密技术、公

钥加密技术等加密手段，虽然能够保证数据处于静止态和传输态时的机密性，但无法对位于 CPU、内存中运行的使用态数据提供有效保护。

隐私计算技术是解决使用态数据安全问题最为有效的手段。隐私计算指的是一类在不泄露原始计算信息给其他合作方前提下，保持数据和计算方法处于持续加密状态的安全计算技术^[2]。为了解决钉钉云环境下计算安全问题，钉钉在建设以数据为中心的安全技术体系过程中，推出了基于可信执行环境的密文检索方案落地执行。

在实际工程实践中，还可以辅以令牌化、格式保留加密、数据脱敏等数据安全手段，从策略上保证数据的使用安全，提供密码学安全以外的另一类选择。

8 隐私保护

一直以来，钉钉始终把用户的隐私保护视作安全职责的重中之重。为了确保用户对所有提供给钉钉的隐私信息的所有权与控制权，钉钉严格按照国家相关法律法规的各项要求，积极响应国家监管部门的号召，主动承担起用户隐私信息保护的责任。通过建立完善的隐私保护管理体系，配置专业的隐私安全团队，全方位提升隐私保护技术手段，为用户的隐私信息提供了全生命周期安全的保障壁垒。

此外，钉钉出台了详细的《钉钉隐私权政策》，向用户披露钉钉对用户隐私信息的收集、使用、共享以及用户如何管理自身隐私数据等各个方面的详细信息。可通过

<https://page.dingtalk.com/wow/dingtalk/act/privacypolicyen> 访问。

8.1 隐私采集保护

为了向用户提供钉钉产品和服务的基本与附加功能，钉钉会采集一些使用信息、设备信息、日志信息、企业信息、用户信息等内容，并严格遵循以下几点采集原则。

最小够用原则：当且仅当在用户使用的业务场景下需要相应权限时，才会请求用户授予必需的权限，不会进行冗余权限申请。

^[2] 宋双杰, 孙含儒, 吴振宇. 隐私计算: 动态的加密技术[J/OL]. http://pdf.dfcfw.com/pdf/H3_AP201905311333143548_1.pdf, 2019-05-30.

合法正当原则：钉钉所请求的权限都是合理、合法、合规的业务强相关权限，所收集的数据都用于维护钉钉服务的正常运行和持续改进优化用户的使用体验。

公开透明原则：钉钉对所有业务场景需要使用到的权限进行了明确的分类，在使用相关权限前，都会给出明确的用户授权提醒并告知用途；并且，在其他场景下不会使用与当前业务逻辑无关的权限。

此外，钉钉还通过多种技术手段建立起事前、事中、事后的纵深防御体系，保障使用钉钉第三方服务的用户的隐私安全。

8.1.1 黑白盒扫描

钉钉接入了阿里巴巴集团的隐私黑白盒扫描能力，用于检查钉钉产品和服务上的代码规范，防止隐私数据外泄事件发生。钉钉每次发布和变更前，都会对源代码进行白盒扫描，内建安全源码保障；在自建应用和小程序运行期间，持续进行黑盒漏洞扫描，一旦触发风险规则实时告警。

8.1.2 隐私 API 监控

钉钉自主研发了客户端离线隐私 API 监控工具以实现运行时监控。钉钉定义了完整的用户隐私数据范围，并筛选出常用的隐私权限操作 API 列表，通过运行时 hook 结合自动化测试的方式对隐私 API 的调用进行实时监控。实现了隐私 API 调用链路监控的完整化、透明化，具备检查出第三方 SDK、小程序、服务等触犯用户隐私行为的能力。对于检测到的违规第三方服务提供者，钉钉将予以通知整改、下架处罚等整治措施。

8.1.3 代码审计

钉钉通过内部安全专家进行代码评审的方式，对涉及到漏洞修复、代码变更、方案发布等安全开发生命周期的各个环节进行严格把控，保障钉钉产品和服务的代码安全质量。代码审计过程中，通过自动化工具和人工评审结合的方式，分析代码中潜在的隐私泄露风险，并着重把控隐私的收集、传输、使用三个环节。针对隐私收集，做到有的放矢，将代码行为和业务需求逐一比对，防止出现过度采集隐私的情况；针对隐私传输，传输前对隐私进行最大程度的脱敏，传输中必须采取加密手段；针对隐私使用，确保隐私只在数据闭环内流转，防止数据外泄的情况。审计结果中如果包含上述风险，将会给出专业的代码修复建议或缓解措施，增强用户业务安全的健壮性。

8.2 隐私共享保护

钉钉不会主动与钉钉服务提供者以外的公司、组织和个人共享用户的个人信息。钉钉仅会在业务场景需要时，即只有共享用户的个人信息，才能提供所要求的第三方产品和服务情况下，充分告知用户详情并取得用户授权后才会共享用户数据。

钉钉建立了用户隐私信息共享代理平台，任何外部组织对用户敏感数据的请求均通过代理统一访问，钉钉将视业务场景需求对数据适当脱敏，最小程度地进行敏感信息共享。同时，钉钉会保留敏感数据请求日志，定期对日志进行安全审查，做到事前有回应，事后可溯源。

8.3 隐私使用保护

钉钉在取得用户授予的系统权限后，不会滥用权限获取与业务无关的用户信息，如后台录音、频繁读写文件等，所有权限的使用均遵循最小够用原则。

9 生态安全

近年来，企业上云已成为企业数字化发展的潮流，且持续保持高位增长趋势。依托于阿里云全球领先的 PaaS 云服务，钉钉建立了专属的企业级 SaaS 平台，通过制定统一的接入标准、开发流程和健全的审核监管机制，提供丰富的行业定制化解决方案，致力于打造全中国乃至全球最具备影响力的企业级 SaaS 生态，充分满足企业自建应用、企业使用第三方 SaaS 应用、企业接入钉钉身份认证体系的多样化需求。由钉钉开放平台承载的生态入口，不仅连接了企业、用户、SaaS 服务提供方三种角色，更是将多个具有价值相关性的链路聚合到一起，打通了企业数据信息孤岛，使封闭的数据流动起来，从而持续产生价值。以钉钉为基石，钉钉生态内的每一种角色都能够找到自身的价值互补，探索出合适的企业数字化经营模式，并在发展过程中持续反馈、不断优化，进而形成良性循环的生态闭环体系。

9.1 生态安全体系建设

建立企业级 SaaS 生态，最重要的是保证各个生态参与方的全方位信息安全。钉钉通过建立完善的生态安全体系，打通数据孤岛，但不打破数据安全壁垒，以合理、合法、合规的方式挖掘数据的使用价值。钉钉生态安全体系建设如图 8.1 所示，以安全责任共担模型作为基础，于各处落实平台责任，并为

SaaS 应用开发商、企业、个人提供多维度的安全能力，帮助或指导其实现应承担的主体安全责任。



图 8.1 生态安全体系框架图

在安全责任共担模型下，安全的责任不只在钉钉一方，各个生态参与方都需要负担属于自己的一部分责任，共同维护良好的生态环境。钉钉作为生态建设的基石，为整个生态提供基础安全、内容安全、数据安全、SaaS 应用生命周期安全等多个维度的安全保障。与此同时，对于已经成熟的安全技术，钉钉积极整合自身安全能力并引入安全生态合作伙伴，构建安全能力矩阵；对于尚未落地的前沿安全技术，钉钉始终保持着前瞻性视野，敏锐洞察行业风向并以进取的心态积极探索。通过多维度的安全保障和高水准的安全能力矩阵，持续为生态安全体系赋能。

9.2 安全责任共担

围绕钉钉 SaaS 生态，存在四个责任参与方和三种责任场景。责任参与方包括钉钉平台、应用开发商、企业和个人用户。责任场景主要围绕钉钉上的 SaaS 应用展开。所有企业和个人用户均可以使用钉钉的上架应用（包含免费和收费）；对有定制化需求的企业，钉钉可以接入企业自建应用，也可以接入应用开发商为企业开发的企业定制应用。以上三种应用类型对应三种责任场景。

9.2.1 平台安全责任

钉钉首先负责基础云服务的安全性。钉钉云基于阿里云构建，继承了阿里云的安全属性，负责云服务基础设施、物理设备、云操作系统、云服务产品等云上服务的安全。并结合云产品的安全功能增加了一系列安全限制，用于更好的保护企业数据安全。

对于应用开发商提供的上架应用，钉钉需要负责平台侧的身份和访问控制、管理、监控和运营，并提供安全风险管控指导意见及要求。应用开发商必须严格遵循规定的要求开发应用，在应用上架前通过安全审查；此外，钉钉还负责建立风险检查机制。当平台上的应用出现内容层面、合规层面或数据层面的高危风险时，具备即时止血和事后追溯处罚的能力。

对于企业内部应用，包括企业自建应用和企业定制应用，均由企业自主管控，钉钉仅承担基础云服务安全责任。

9.2.2 开发商安全责任

开发商主要负责上架应用的开发和企业定制应用的开发，并相应承担两方面的安全责任。

对于上架应用，开发商需要按照钉钉的风险管控要求进行开发，接受钉钉的安全审查，并以安全的方式配置并使用钉钉云提供的安全产品，构建自己的云上 SaaS 应用及业务。

对于企业定制应用，开发商需要全权负责定制应用的运营和管控，在符合法律法规的情况下进行开发，对其所产生的内容、合规、数据风险负责，并保障应用的自身安全性。

9.2.3 企业安全责任

企业即可作为应用的使用方，也可作为应用的开发方，可以灵活使用钉钉上架应用、企业自建应用、企业定制应用中的一种或多种，并承担三方面的安全责任。

企业使用上架应用前，应当仔细阅读并同意应用的使用协议，如果使用过程中出现企业不可控制的安全风险，将按照协议中规定的内容进行事后判定和处治出现过失的一方。在使用过程中，企业需要适当的授权给上架应用一些企业权限，用于满足应用的正常业务逻辑需要。

企业接入自建应用，需要企业自主负责应用的运营和管控，在符合法律法规的情况下进行开发，并保障应用自身的安全性。

企业接入定制应用前，需要向开发商提供完备的安全性要求以指导开发商，保证企业定制应用符合企业自身要求。

9.2.4 用户安全责任

个人用户不归属于任何企业，因此仅能使用钉钉的上架应用，承担一方面的安全责任。使用上架应用的个人，需要仔细阅读并同意应用的使用协议，并在使用过程中适当的授权给上架应用一些个人权限，用于满足应用的正常业务逻辑需要。

9.3 基础安全

作为企业级 SaaS 平台，钉钉开放平台主推钉钉云安全方案，提供基础安全分层能力，包含主机安全、网络安全、应用安全三个方面，保障云环境下的 SaaS 应用安全。

9.3.1 主机安全

钉钉开放平台为所有开发商提供了云安全中心基础版（安骑士）服务，只需在主机上部署云安全中心 Agent，即可无缝接入云安全中心并享受其提供的实时入侵检测能力，包括异常登录检测、异常行为检测、异常账号检测、网站后门查杀、系统关键文件异常检测等多方面的入侵检测防护。

提供本地化部署的专有钉钉，同样支持接入本地部署的云安全中心基础版（安骑士）服务，享受其提供的全方位安全防护。

9.3.2 网络安全

钉钉开放平台建立在专属 VPC 网络内，基于隧道技术实现数据链路层隔离，提供独立隔离的安全网络环境。钉钉为每个开发商提供预配置的安全组，以虚拟防火墙的方式在钉钉云内划分出各个 ECS 实例间的网络安全域，不同安全组的实例之间默认内网无法互通，保证了各个开发商之间的完全隔离。钉钉云启用了阿里云自主研发的 DDoS 防护系统，支持防护全类型 DDoS 攻击，保证云上服务的高可用性。钉钉云还接入了阿里霸下防护系统，以七层流量清洗的方式，提供恶意流量攻击防护、反爬虫等功能。

提供本地化部署的专有钉钉，同样支持接入本地部署的 DDoS 防护系统，为单位和企业提供全类型 DDoS 攻击防护服务。

9.3.3 应用安全

钉钉使用由阿里集团提供的漏洞黑盒扫描服务，持续对运行在钉钉云上的 SaaS 应用进行安全扫描，对发现的漏洞进行实时告警，减少漏洞的数量和暴露时长。此外，钉钉引入第三方生态合作伙伴，提供渗透测试和白盒代码审计服务，充分保障上线前和线上应用环境的安全性。

提供本地化部署的专有钉钉，同样支持引入第三方生态合作伙伴，提供渗透测试和白盒代码审计服务，充分保障上线前和线上应用环境的安全性。

9.4 内容安全

钉钉 SaaS 生态中的内容主要来自各式各样的应用，面临着涉政、涉黄和涉赌三种风险。钉钉内容安全的治理目标是尽量缩短风险内容外露时长，减少风险内容带来的不良影响，营造钉钉 SaaS 平台绿色、健康的内容生态。

提供本地化部署的专有钉钉，需要单位和企业去自主运营内容安全相关防护。

9.4.1 风险发现

钉钉作为生态平台，应对监管要求对公开流量进行内容管控，旨在即时发现内容风险，一旦确认风险会采取应对措施。

9.4.2 反馈机制

钉钉通过建立完善的风险反馈体系，包含用户投诉举报机制、网络舆情监测机制、监管部门同步机制、内部蓝军演练机制，一方面扩充流量分析手段的风险发现面，一方面反馈于流量分析技术，持续改进流量分析的策略和 AI 模型的训练。

9.4.3 监管对接

钉钉积极配合国家监管部门的相关要求，对于发现的第三方内容风险，即时上报给监管；对于监管下达的处罚，即时同步给应用开发商，并根据处罚内容采取对开发商采取整治措施。

9.5 数据安全

为了保证钉钉生态圈内的数据只在钉钉允许的范围内流动，守住生态核心价值，钉钉将主动协助应用开发商一起解决数据外泄风险。除了遵循数据全生命周期安全和以数据为中心的安全两大方法论之外，钉钉还将“定机制、推产品、抓管控、设巡检”的十二字方针作为维护生态数据安全的指导思想，使得生态数据安全有法可依、有章可循、有源可检。钉钉通过部署多种云上安全产品，对内进行整个生态应用的漏洞扫描和流量审计，对外提升云安全防护水平，防止主机入侵、DDoS 攻击等黑客攻击。钉钉制定生态安全数据分类分级标准并对各类数据进行打标，根据实际业务场景需要，对开发商申请使用的数据类型进行接口审批和权限审批，确保数据流出均经过钉钉的统一审核。同时，钉钉具备自动化日志审计功能，能够主动探测数据泄露行为，第一时间感知到数据泄露事件的发生；钉钉也建立了内外情报收集平台，持续被动接收情报反馈。通过审计为主情报为辅的方式，具备数据泄露的发现和溯源能力。

提供本地化部署的专有钉钉，从产品层面提供了多种数据安全防护和管理能力，方便单位和企业自主运营应用生命周期全流程管理。

9.6 应用生命周期安全管理

钉钉对开发商提供的上架应用进行全生命周期的安全管理，确保从应用进入到退出开放平台的每一个环节都存在安全风险发现机制和治理办法，保障整个平台应用的安全性。

提供本地化部署的专有钉钉，从产品层面提供了多种应用生命周期安全管理能力，方便单位和企业自主运营应用生命周期全流程管理。

9.6.1 入驻签约

需要识别开发商主体资质风险，以及对签约主体身份的真实性进行核验。钉钉通过人工审核的方式进行风险治理。

9.6.2 创建应用

需要判别创建应用的合规性，不能是国家法律明确禁止的应用，也不能是涉黄、涉赌、涉政等钉钉明确禁止的应用类型，涉及到金融、支付、传媒等需要资质的应用需要审核对应主体资质。还需对应用的服务器域名备案信息进行验证，确保应用和域名归属于同一开发主体所有。钉钉通过人工审核的方式进行风险治理。

9.6.3 开发应用

钉钉开放了丰富的服务端接口能力，开发者可以借助这些接口能力，实现企业应用系统与钉钉的集成打通。需要防止应用滥用钉钉接口数据，以及未经申明使用钉钉 App 权限。钉钉通过设立数据接口审批和权限申请审批的模式，应用业务逻辑需要使用到的数据均需经过数据接口使用审批，应用需要使用到的权限需要向钉钉申请通用或特殊权限审批，做到数据和权限的最小够用原则。

此外，需防止因应用架构设计缺陷导致的风险。钉钉提供安全咨询服务，由专业的安全专家提供安全架构设计建议，还通过钉钉云安全组、权限限制等云安全配置，尽可能收缩攻击面。

9.6.4 产品共创

钉钉会主动寻求合适的生态伙伴进行产品共创，在共创过程中，钉钉内部人员和生态伙伴会进行密切合作沟通，整个过程中需要严格防止数据泄露的风险。钉钉通过技术手段用于内部数据泄漏的发现治理。

9.6.5 产品验收

产品验收阶段，需要对应用进行全面的安全风险评估，防止逻辑缺陷导致的漏洞、开发编码引入的漏洞、系统架构安全性不足等缺陷。钉钉通过验收应用开发商提交的安全测试报告，以及验收应用安全实施情况两种手段进行风险治理。

9.6.6 产品运营

应用上架后，由开发商负责产品的日常运营，钉钉维护服务的正常运转。需要防止应用泄露企业数据的风险，防止技术能力导致的产品不可用或服务资源不足导致的服务不可触达，以及防止应用违规使用推送功能传达不当的信息

言论。钉钉通过技术手段用于应用数据泄漏的发现治理。在安全网关上布置 DDoS 防御服务，保证服务持续稳定的高可用性。设立推送安全审核机制，具备内容风险发现和拦截能力。

9.6.7 退出市场

开发商因各种原因想要下架应用时，需走正规的应用下架流程，但需要防止操作不规范的开发商暴力下线应用服务器或对在架产品冻结销售。为此，钉钉通过设置钉钉云主账号托管服务器的方式，为开发商开通子账号，限制其暴力下线的操作权，并对高危产品轮询监控，避免开发者冻销产品的情况，维持开放平台的生机与活力。

9.7 安全赋能

钉钉自身具备多维度、可复用的安全能力，同时还积极引入第三方安全生态合作伙伴，为客户提供个性化的行业安全解决方案，进一步扩充钉钉的安全能力矩阵，以安全服务、安全组件的形式提供给开发商或企业，在提升应用安全性的同时降低应用安全开发投入的成本。

应用在钉钉开放平台上线前，开发者需提交安全测试报告，经过钉钉安全专家审核并验收通过后，才允许应用上架。应用上架后，开发者按照钉钉的规范要求，授权钉钉安全专家进行安全评估。

对于国际前沿的安全技术领域，钉钉一直保持开放进取的心态，以前瞻性的视野进行安全预研，广泛布局，洞见未来，并与客户以共创的方式一齐探索前沿技术的落地方案，致力于成为下一代安全技术领域市场的开拓者，打造企业服务行业领先的安全 SaaS 平台。

附录

术语/缩略语

全链路：从用户端到服务端的数据交互全路径。ASRC：阿里巴巴集团安全应急响应中心。

ECDH (Curve25519)：基于 ECC (Elliptic Curve Cryptosystems, 椭圆曲线密码体制) 的 DH (Diffie-Hellman) 密钥交换算法，交换双方可以在不共享任何秘密的情况下协商出一个密钥，其中 Curve25519 为算法使用的椭圆曲线类型。

SDL：Security Development Lifecycle 的简称，安全开发生命周期。

LWS：钉钉自主研发的私有安全通讯协议，基于 TLS1.3 设计和实现，密钥协商采用椭圆曲线算法 ECDH (Curve25519)，对称加密算法采用：AES-256-GCM/ChaCha20。

AES-256-GCM：AES 对称加密算法，256 是密钥长度，GCM (Galois/Counter Mode) 指的是该对称加密采用 Counter 模式并带有 GMAC 消息认证码。

ChaCha20：CHACHA20-POLY1305 的加密方法，是一种新式加密算法，性能强大。

MFA：多因子验证，是一种更为全面的访问控制方式。

AliSQL：MySQL 官方版本的一个分支，应用于阿里巴巴集团业务以及阿里云数据库服务，该版本在社区版的基础上做了大量的性能与功能的优化改进。

iDB：阿里巴巴自主研发的数据管理、结构管理、诊断优化、实时监控和系统管理于一体的数据库管理产品。

CloudDBA：阿里巴巴自主研发的智能数据库诊断优化产品，提供自助化数据库诊断和优化服务，致力于成为 DBA 身边的数据库专家。

DSMM：阿里巴巴牵头制订的数据安全成熟度模型 (Data Security Maturity Model)，该标准从组织建设、人员人力、制度流程、技术工具等四个维度对数据安全生命周期提出了明确的安全要求和度量体系。

SaaS：软件即服务（Software as a Service）的简称，是一种云上软件交付模式。

PaaS：平台及服务（Platform as a Service）的简称，是一种云计算服务，提供运算平台与解决方案服务。

OSS：阿里云提供的对象存储服务（Object Storage Service），是一种海量、安全、低成本、高可靠的云存储服务，支持存放任意类型的文件。

MDM：移动设备管理组件，提供对移动设备端上的管控和响应服务。

EDR：终端检测与响应组件，提供对 PC 设备的端上管控和响应服务。

BYOD：员工携带个人设备办公的一种方式，设备通常包含手机、平台、笔记本电脑等。

BYOK：企业自带密钥进行加密，密钥由企业自主管理。

KMS：阿里云上的密钥管理服务，提供安全合规的密钥托管和密码服务。支持追踪密钥的使用情况，配置密钥的自动轮转策略，以及利用托管密码机所具备的中国国家密码管理局或者 FIPS 认证资质，以满足监管合规需求。