文档密级：公开

钉钉安全白皮书

版本（V2.0）

■ 声明

■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

目 录

1 前言

随着移动互联网的普及，即时通信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经济体 6 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 4300 万中小企业提供“简单、高效、安全”的服务。

为加强 4300 万中小企业对钉钉安全的认知，本文档重点从安全文化、全链路安全防护、生态安全、安全合规四个维度，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。

1.1 术语定义

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 为算法的参数。

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，采用 TLS1.3 加密，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 是对称加密算法强度，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。

2FA: 双因子验证，是一种安全密码验证方式。

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。

2 安全文化

2.1 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、传输通信以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。

2.2 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、团队合作、拥抱变化、诚信、激情、敬业”的价值观和“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。

2.3 社会责任

中国有 4300 万中小企业组织，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，秉承阿里巴巴服务中小企业，让天下没有难做的生意的使命，钉钉通过“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。

3 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。

3.1 客户端安全

钉钉通过应用完整性、环境可信性、数据机密性以及账号安全风控等四个维度的强化加固，有效保障了钉钉客户端安全。

3.1.1 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、加壳保护、修改指令调用顺序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。

3.1.2 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完成数据加密和解密。

病毒检测：钉钉 APP 提供钱盾病毒查杀功能，用户可选择进行病毒检测和查杀。

3.1.3 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 在客户端的整个加解密过程均在安全沙箱中完成，对外不暴露任何密钥和加密算法。

安全签名：基于 HMAC_SHA1 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。

3.1.4 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，如双因子验证(2FA)、生物特征识别、同事关系识别等方式，为用户账号提供更多维度的安全保障。

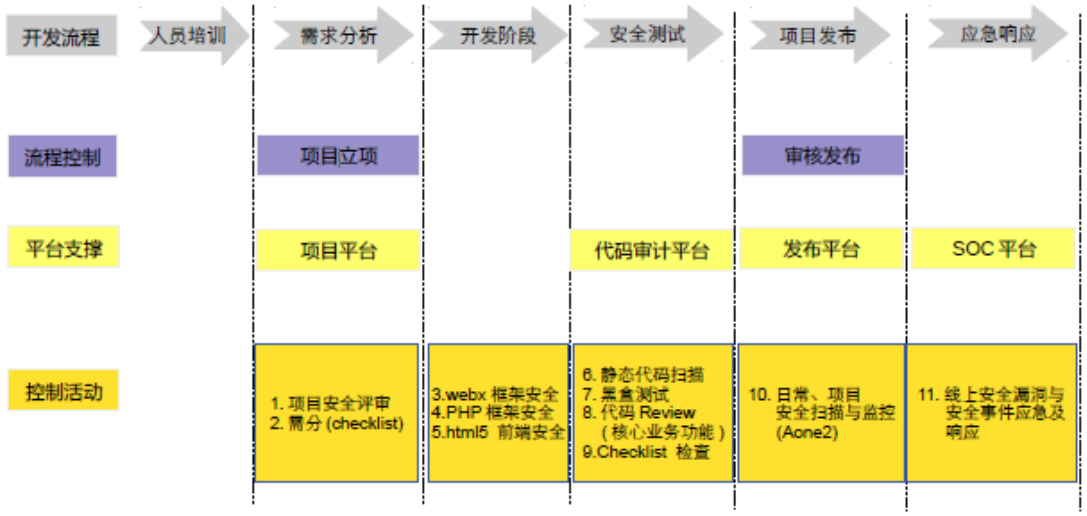
3.2 传输安全

基于 SSL/TLS 协议，钉钉构建了一套完整的私有安全通信协议 LWS。通过这种私有安全通信协议，实现钉钉端到端的通信链路加密、签名，防止窃听、篡改，以确保数据信息的传输安全。

3.3 服务端安全

3.3.1 应用安全

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。



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 review，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 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 bug 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。

3.3.2 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。

3.3.3 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。

3.4 基础设施安全

3.4.1 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。

3.4.2 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。

3.4.3 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。

3.5 数据安全

钉钉以数据安全为愿景，严格遵循 DSMM 的各项安全要求，在数据生命周期各阶段如数据产生、数据存储、数据使用、数据传输、数据共享、数据销毁等都无缝嵌入阿里巴巴集团各项成熟的安全控制措施，确保用户数据的机密性、完整性、可靠性。

3.5.1 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。

3.5.2 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，避免密钥离开加密机的同时，保障数据机密性、完整性、可用性和不可否认性。

3.5.3 数据使用

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。

3.5.4 数据存储

客户端，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，同时企业可按需设置用户聊天信息自动销毁，确保本地数据的机密性。

服务端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。

3.5.5 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。

3.5.6 数据销毁

钉钉使用的信息处理设施，存储介质出数据中心前遵照 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。

3.5.7 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。

3.6 安全运营

3.6.1 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。

3.6.2 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。

3.6.3 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。

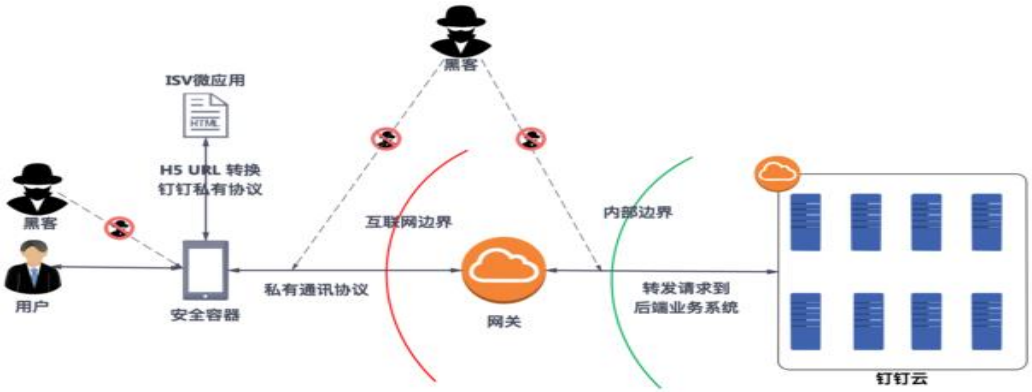
在安全事件溯源阶段，溯源取证团队将按需收集受影响的业务端、管、云的活动日志，并进行综合分析，全面还原安全事件发生过程，并进行针对性的整改加固，如有需要还将配合公检法部门进行立案处理。

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。

4 生态安全

4.1 生态闭环

钉钉通过安全端容器、私有安全加密通道、安全云容器、为 ISV 提供高效、弹性、安全的一体化解决方案，在保障访问速度的同时，大幅提高微应用稳定性，并有效防止劫持。



钉钉微应用业务拓扑图

同时针对应用市场存在的高危业务风险，如数据泄漏、暴力下线等，钉钉通过专项治理和持续监测审计，不断健全端、管、云的安全方案，持续加强 ISV 的安全管控，保障用户数据不被泄漏以及 ISV 提供的应用安全、稳定、高效。

4.2 安全赋能

钉钉生态安全建立了第三方应用上线审核流程及标准，通过发布 ISV 准入要求以及 PHP、JAVA、H5 等安全开发规范，以共建合作的方式为第三方 ISV 以及企业开发者建立和培养安全梯队，为钉钉应用市场开发者及企业提供安全保障能力。

4.3 应用监管

微应用在应用市场上线前，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。微应用上架后，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，符合规范要求的微应用将在钉钉应用市场获得安全认证的标签。

此外，针对第三方开发者上线的微应用，钉钉通过应用市场异常监控和安全扫描，及时发现可能存在安全漏洞、违规违禁的微应用，打造一个绿色、可信的钉钉开放平台。

5 安全合规

5.1 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 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。

5.2 拥抱监管

在阿里巴巴集团安全部的“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每一位“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。

SOCⅡ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。

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 SOCⅡ类型一安全审计报告，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。

5.3 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。

5.4 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。

6 总结

在阿里巴巴集团安全部的“九字方针”指导下，钉钉通过技术创新和大数据运营，持续改进各项安全控制措施，探索研究前沿技术，如漏洞自动化分析与挖掘、同态加密、差分隐私等，加强安全体系建设，积极拥抱国内外各级安全监管，规范内部安全运营活动，但难免还是存在一些风险，尤其在当前复杂的互联网形势下，内部业务快速迭代，外部攻击层出不穷，钉钉每天都在经受严峻的考验。为切实保障每一位钉钉用户安全，在阿里巴巴集团的强大资源支持下，每一位钉钉人将持续努力前行。