云之家信息安全白皮书

深圳云之家网络有限公司

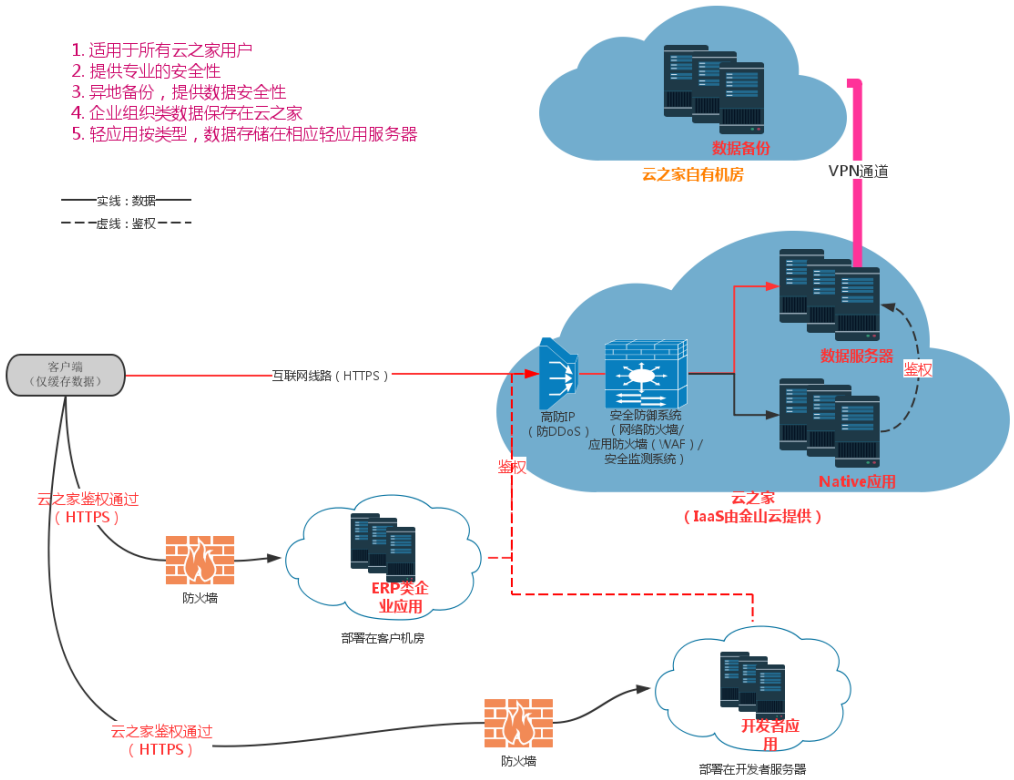
1 云之家安全概述

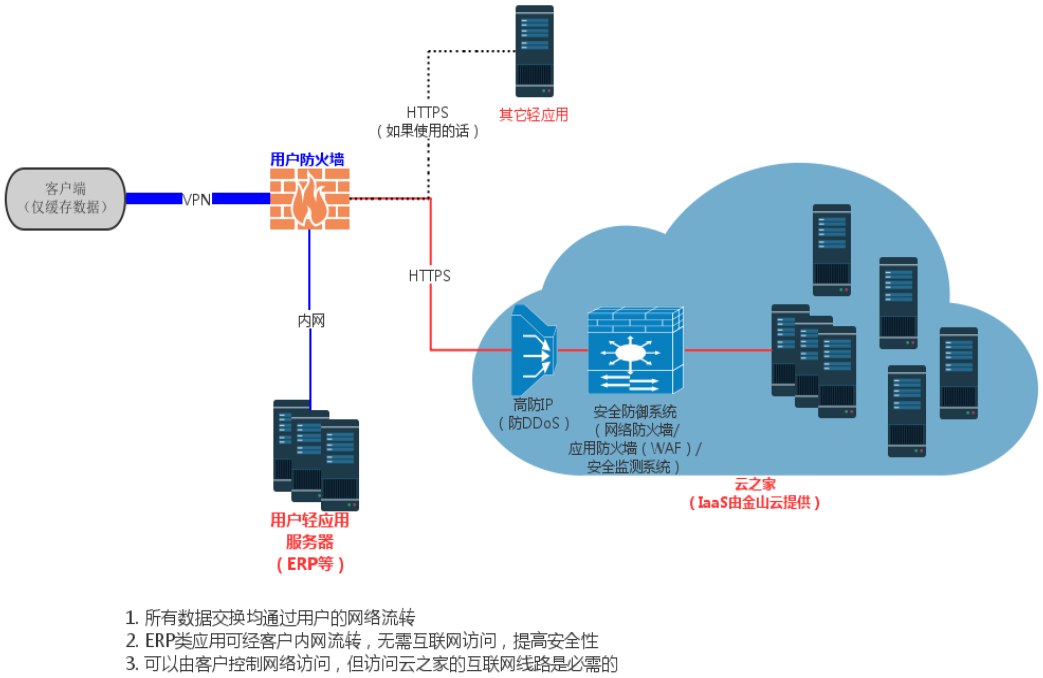
云之家整体信息安全参照 CSA 云安全指南、信息系统安全等级保护第三级、ISO27001 信息安全管理体系要求及 ISO27018 公有云个人信息保护管理体系标准进行建设，在管理和技术上实施纵深防御体系，多重保护实施，保障用户安全。

云之家是 SaaS 级企业应用，其中 IaaS 服务由金山云提供。

1.1 网络部署示意图

网络安全：（要求至少 HTTPS 通信，可支持 VPN 方式）
云之家：拥有 IDC 级高防 IP（防 DDoS）、网络防火墙、应用防火墙（WAF）等安全防御系统
ERP 类企业应用：客户自建安全、云之家鉴权、ERP 应用本身鉴权、授权、审计等安全功能不受影响
其它开发者应用：云之家鉴权、开发者可托管（敏感信息类）或自建服务器管理



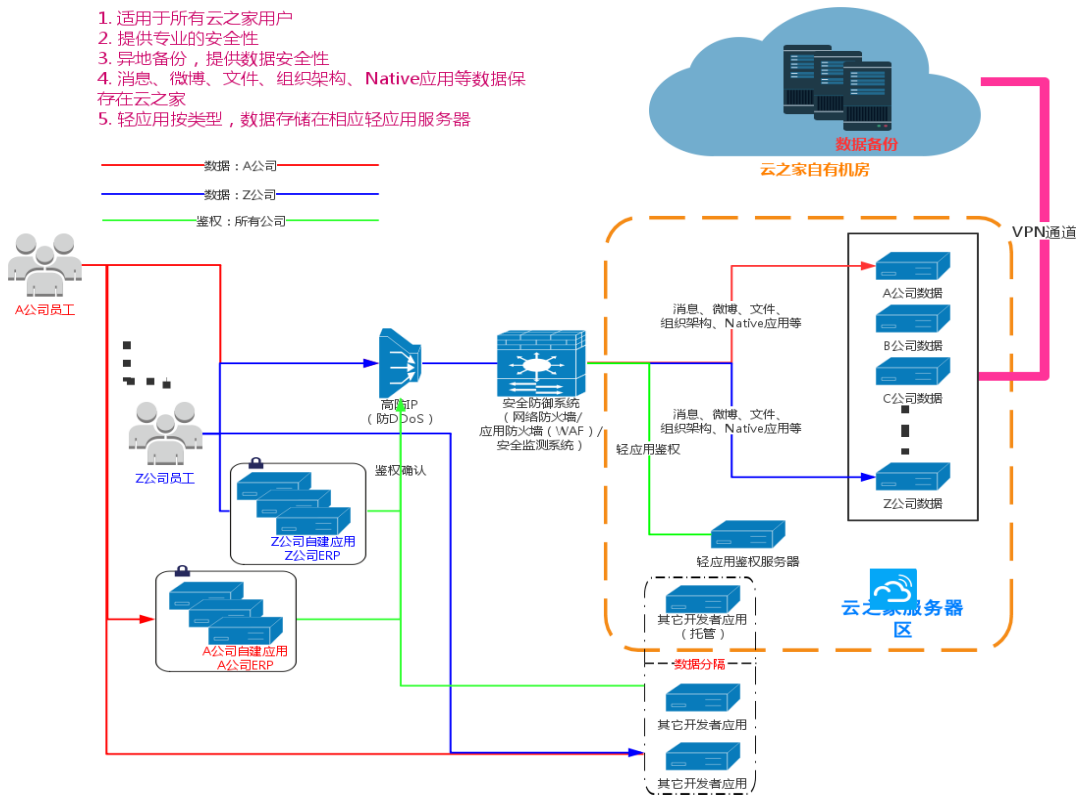


VPN 方案示意图

1.2 数据流转示意图

数据保存：

- 云之家：保存消息、同事圈、文件、企业组织信息、Native 应用数据等
- ERP 类轻应用：保存在客户服务器中，云之家**只处理鉴权信息**
- 其它开发者应用：托管在云之家（敏感信息类）或开发者自建服务器



2 云之家安全实现

2.1 物理及设备安全与基础架构安全

云之家为 SaaS 应用，物理设备安全与基础架构安全，包括机房安全、服务器安全、网络设备安全等，均由云之家合作伙伴金山云提供。

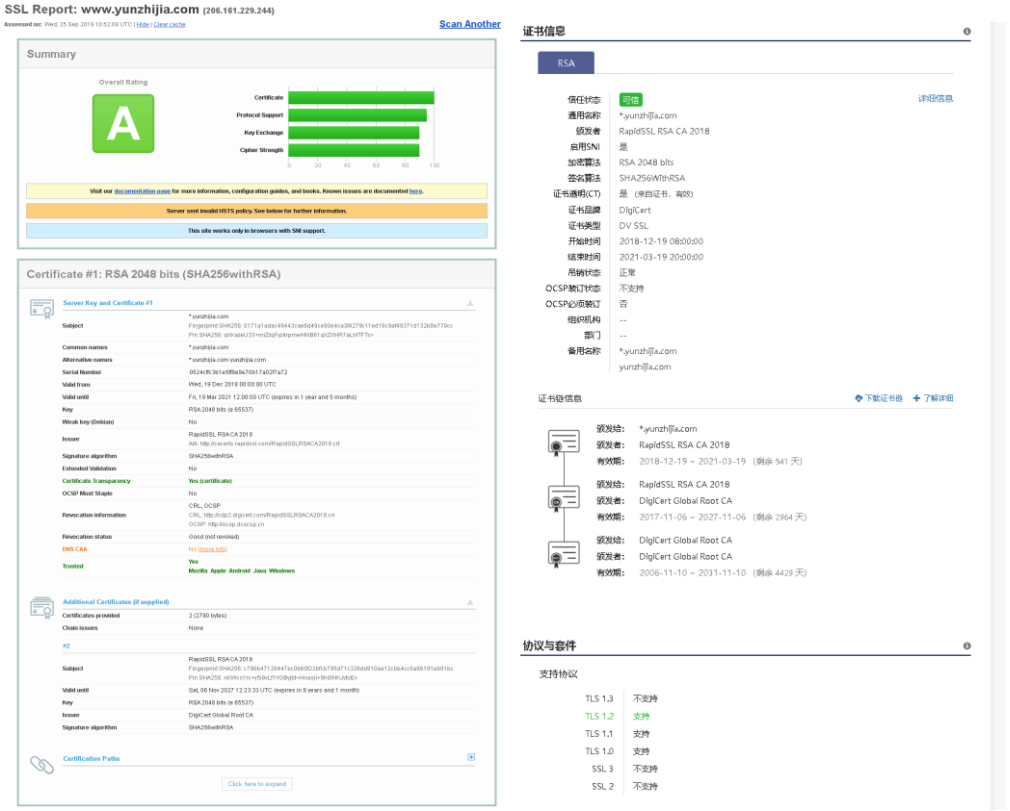
- 机房多活技术：金山云提供多处机房接入，提高机房可用性
- 网络多活技术：金山云提供多线接入方式，国内、国外均可流畅访问
- 数据存储多活：云之家除在金山云进行数据存储外，还在同城异地机房备份有在线数据和离线数据，保障数据的可用性
- 同时，云之家对于 OS 安全和网络安全进行实时监控，每日检查；
- 所有 OS 操作、应用变更操作及 DB 操作均需要授权，并实时记录并转发至日志中心进行存储，实时展现日志，并对危险动作进行告警提示。

2.2 SaaS 业务应用安全

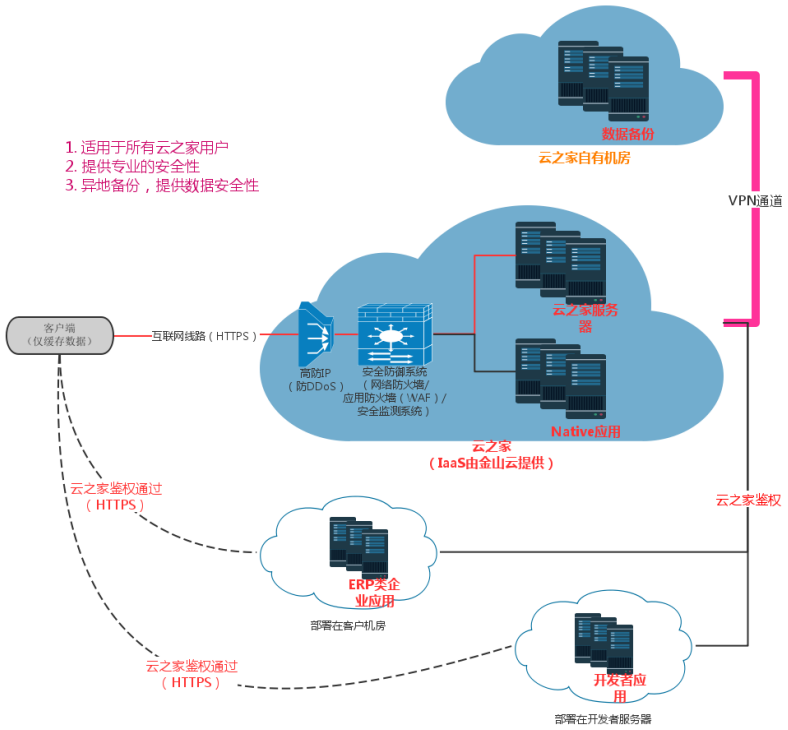
云之家通过部署纵深防御体系，从各方面防止被攻击，保障用户安全。包括

但不限于：

- 网络防火墙
- 网络访问控制
- 安全域控制
- 应用防火墙 WAF
- IAM 身份认证管理
- MFA 多因子认证
- 业务数据隔离机制
- 数据实时备份
- 数据离线备份
- 数据异地备份等
- 定期的安全扫描、渗透测试及测评，通过 PDCA 方法不断提升安全体验
- 安全的 HTTPS



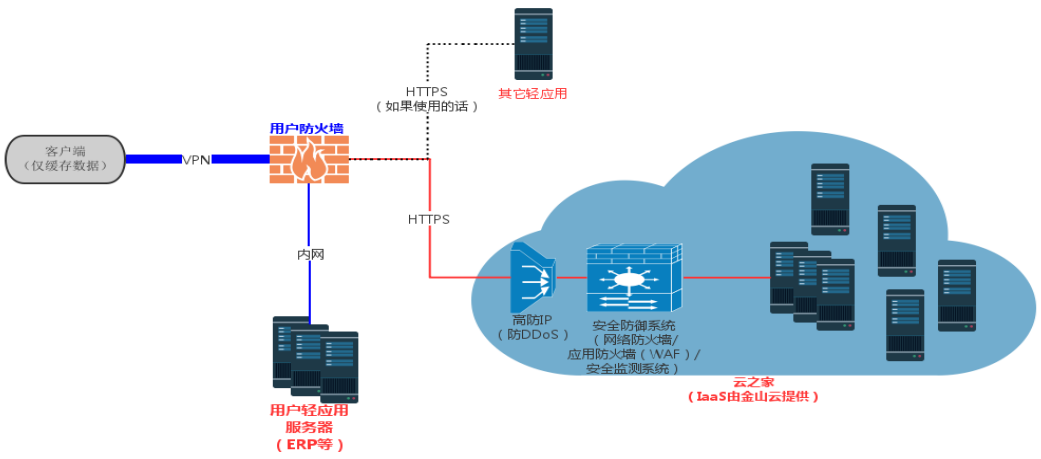
- 多种安全的网络访问方式：
  - **通用网络访问图示**



  - **通过 VPN 方式保护数据安全**

当使用的第三方应用部署在用户服务器端时，可以采用更安全的 VPN 方式，这样，所以有数据都经过了用户网络中转，用户可以严格把控数据安全性。在使用时需要特别注意：必须开发访问云之家的网络权限才可以正常访问；如果有其他第三方应用，而应用的 server 不在云之家或用户服务器时，也需要开通相应的网络访问权限。

下图基于《通用网络访问图示》改造，未描述数据备份内容。



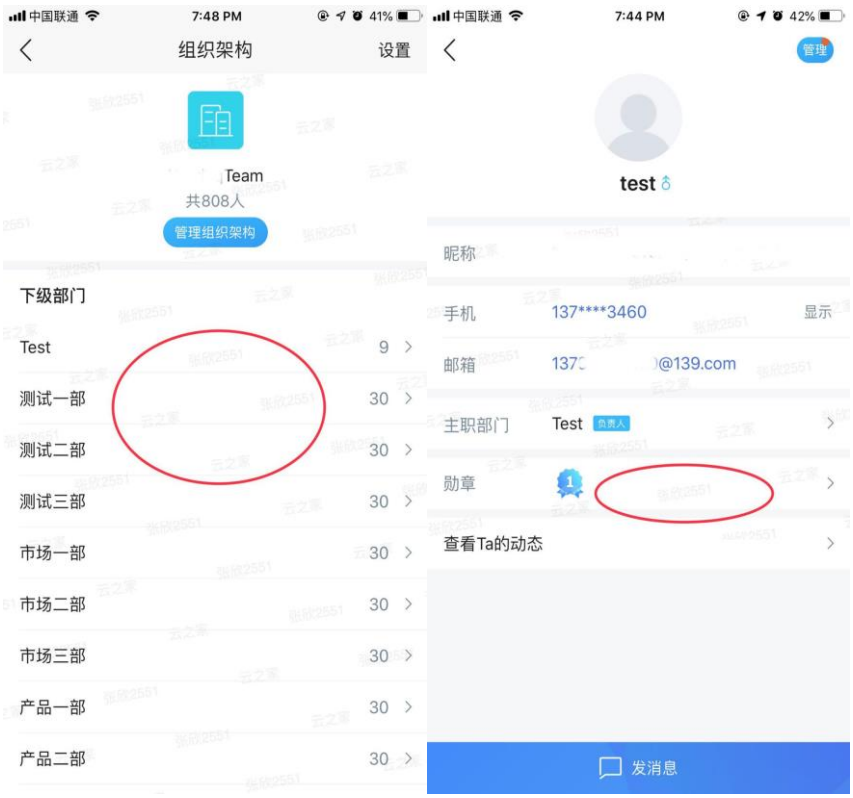
1. 所有数据交换均通过用户的网络流转
2. ERP类应用可经客户内网流转，无需互联网访问，提高安全性
3. 可以由客户控制网络访问，但访问云之家的互联网线路是必需的

2.3 用户隐私与企业数据安全

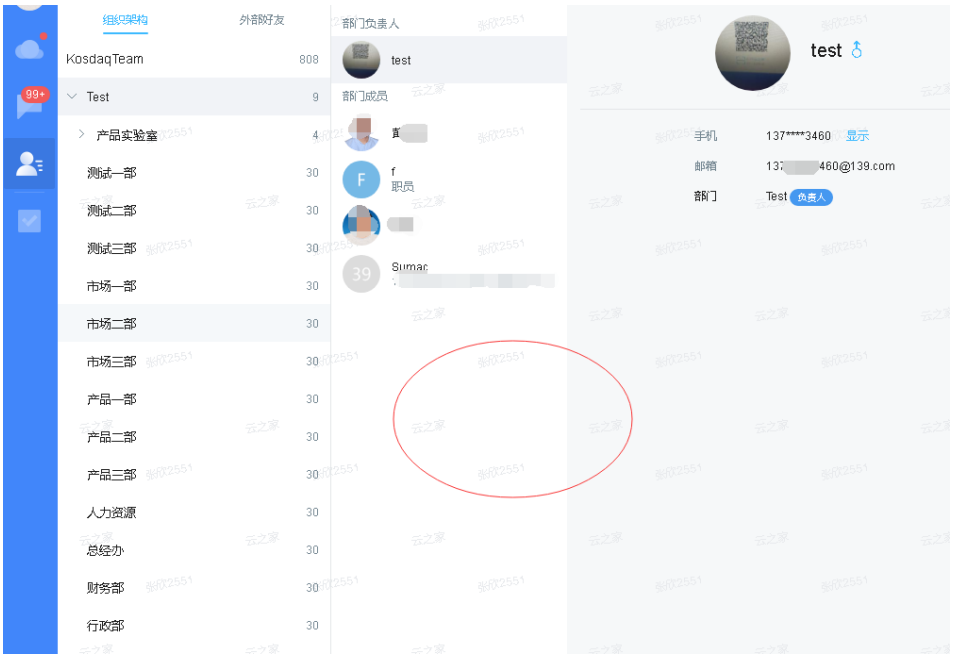
2.3.1 用户隐私安全

在保障用户隐私方面，云之家提供多种安全措施保障用户信息不被窃取、滥用、盗用。

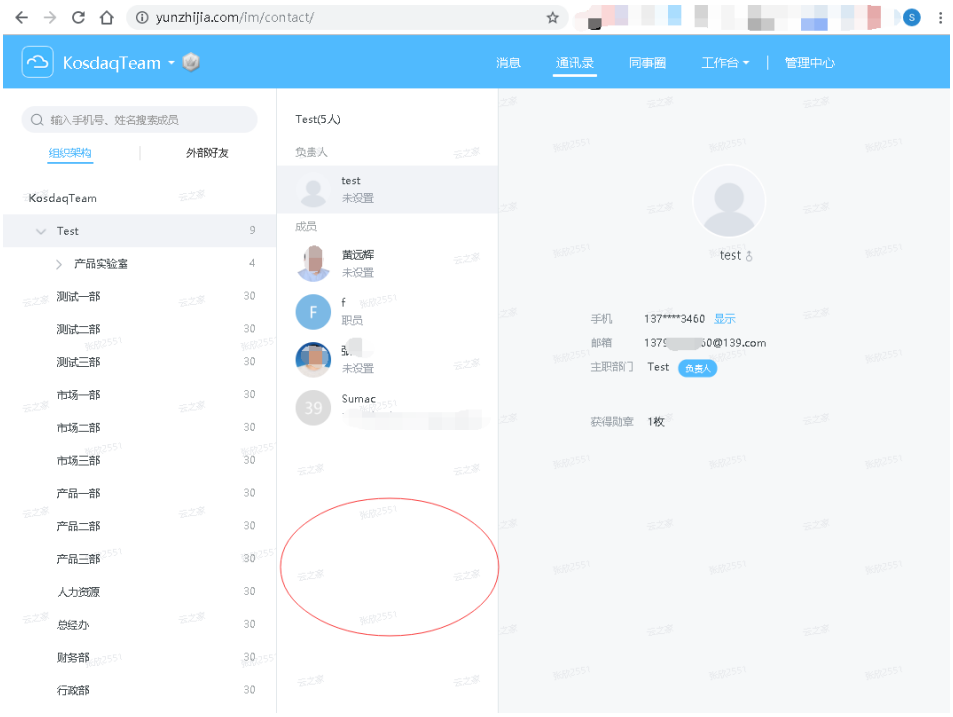
- 云之家对用户注册、登录进行了多重保护，能够有效防止暴力尝试密码，破解账号，冒用账号等行为。
  - 图形验证码机制，防止暴力尝试密码
  - 请求频次控制，对多次失败的登录行为进行限制
  - 恶意 IP 处理，对 IP 信誉度较低或多次仅有登录尝试 IP 进行封禁
- 对于员工离职等行为，云之家将归档其历史数据，禁止其他人员访问其历史信息。
- 通讯录安全：针对员工手机号信息，可在管理中心设置全部隐藏或部分隐藏（仅隐藏中间 4 位），当员工批量查看同事手机号超过指定次数时，系统会自动提醒企业管理员哪位员工在批量查看通讯录手机号信息。
- 在使用上，云之家提供多种安全体验：
  - 文件方面：提供溯源能力，谁看过，谁下载过，谁分享过，均留下记录；
  - 组织架构：提供水印技术，截图或分享时，将显示用户名缩略标志；



移动端组织架构水印

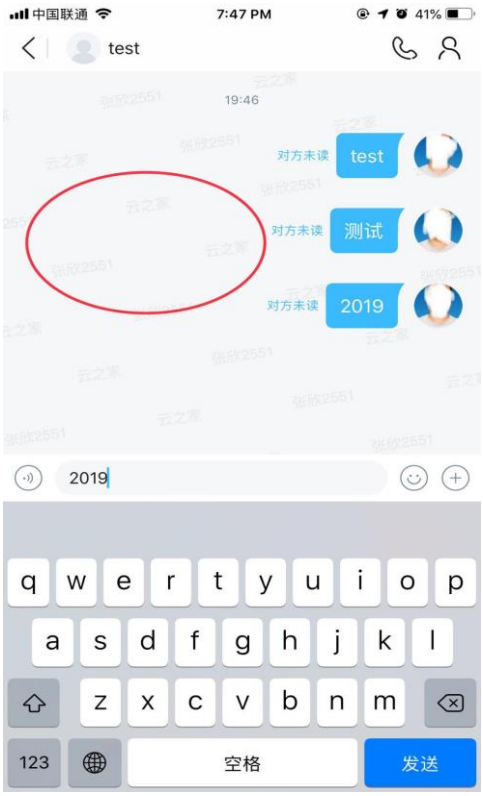


桌面端组织架构水印



网页端组织架构水印

- 消息方面：提供会话水印技术，截图或分享时，将显示用户名缩略标志；无痕消息，指定消息可以在一定时间内撤回或自动删除



消息水印

- 设备管理：提供可信设备功能，可以查看每个账号已经登录的移动设备信息（限 android 和 ios）

同端互踢功能

新设备强制验证

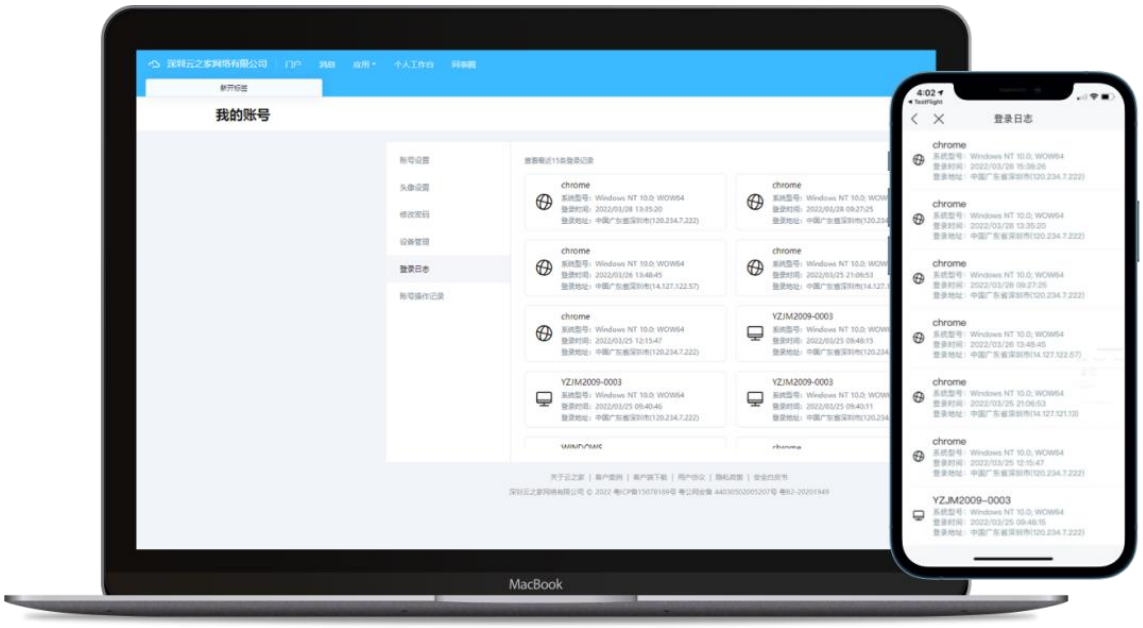
可信设备管理

2.3.2 用户账号安全

云之家账号安全，让账号操作记录留痕，让个人信息安全更可控。

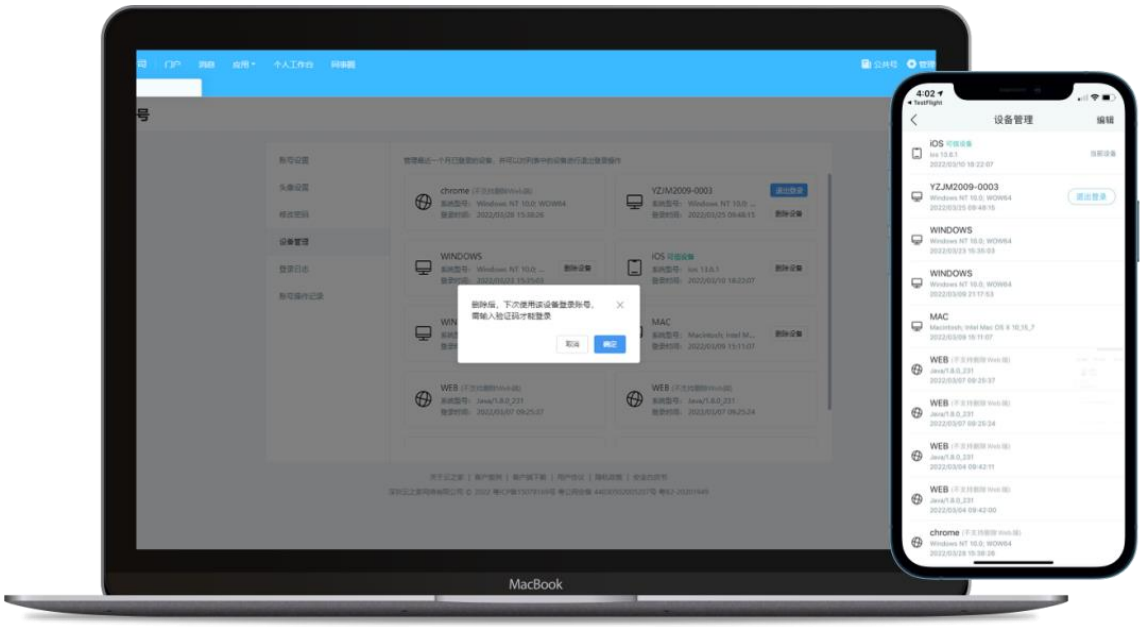
- 操作留痕，对登录日志支持查看最近 30 条登录记录，账号操作记录支持查看最近一个月内，本人账户修改、密码修改、解绑定等相关高危敏感

记录



操作留痕，账号安全更安心

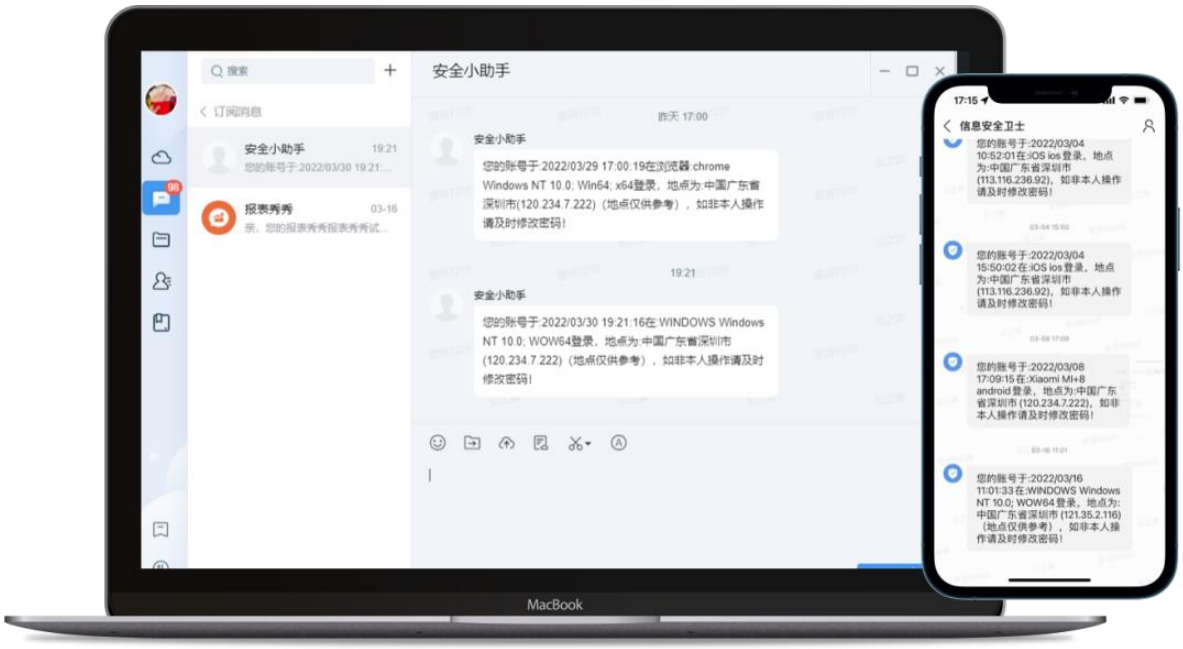
- 设备管理，对设备管理支持管理最近一个月已登录的设备，并可以对列表中的设备进行退出登录、和删除设备操作。删除移动端设备后，下次使用该设备登录账号，需输入验证码才能登录



设备管理，为登录安全保驾护航

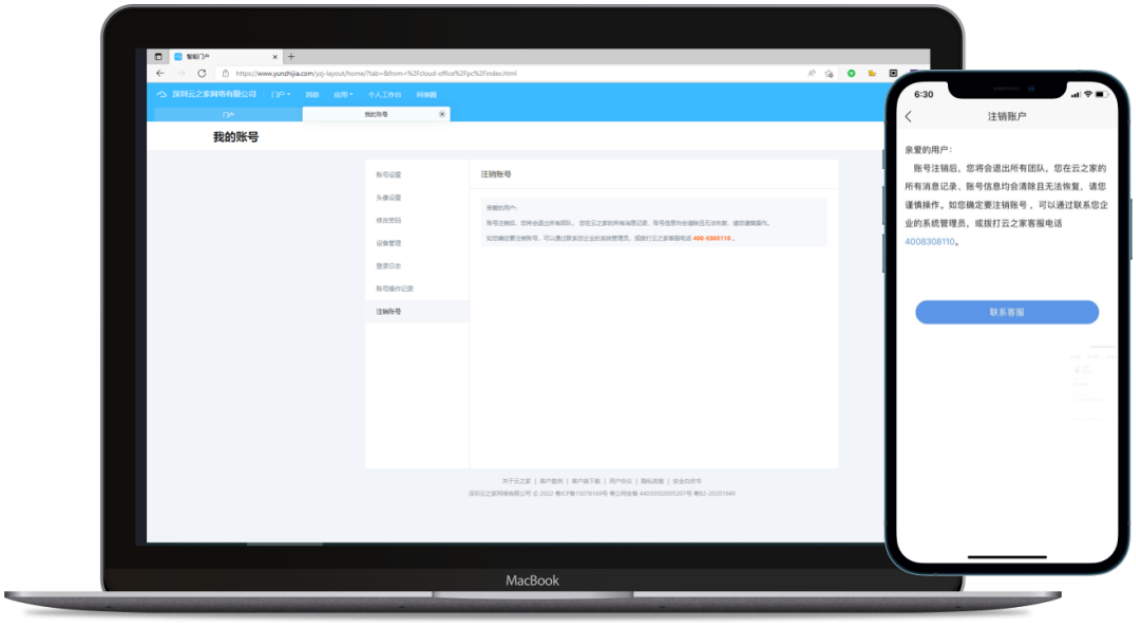
- 异常提醒，账号新设备登录、账号非常用地登录、多次尝试登录失败等

场景，将会通过云之家公共号“信息安全卫士”给本人发送异常提醒，及时预警安全风险



异常提醒，保障信息安全最后一公里

- 账号支持注销，符合《个人信息安全规范》要求，成功注销后，所有消息记录、账号信息等均会被删除，保障个人信息安全



满足合规，保障个人信息安全

2.3.3 企业数据安全

云之家数据采取实时备份、多重备份、异地备份等多种方式并行，保障数据的可用性、完整性及机密性。

同时，对于可后台接受数据的人员进行严格控制，所有针对数据的操作均需要授权后方可进行，对所有人员均需要签订保密协议及员工信息安全手册。

对于第三方应用（开放者平台应用），云之家并未介入具体的数据通讯和存储过程。根据技术实现的不同，数据存储发生在客户服务器端（如 ERP、OA 类）或开发者服务器端。

- 数据安全存储：
  - 以数据流方式存储数据，除非知道相关数据结构，否则无法得到明文内容
  - 通过多主多从技术，对数据实现多重实时备份
  - 通过多机房部署，实现数据的异地备份
  - 为进一步保障数据安全，云之家还将离线备份数据，避免因恶意损坏而造成的数据丢失、损毁
- 数据安全运维：数据是云之家的生命，对于可接触数据的人员均严格限制
  - 所有人员均签订有保密协议，防止数据泄露
  - 运维人员的所有操作访问均有记录，并实时发送至日志中心存储、分析，对于危险操作将进行告警
  - 数据运维人员操作或管理数据库前，需要先授权，再访问
  - 数据运维人员对数据的所有操作均记录并发送至日志中心存储、分析。对于危险操作将进行告警
- 数据安全传输
  - 所有通讯数据均通过安全的方式进行传输：安全的 HTTPS 或 VPN 通道
- 数据可访问性
  - 所有数据被业务用户访问前，均需要完整鉴权信息
    - 校验用户是否属于当前工作圈正式成员
    - 校验用户是否属于当前会话组正式成员
    - 校验用户是否有对应资源的访问权限
    - 检验是否需要管理员审批等
- 数据归档
  - 对于已离职人员，将归档存储其历史信息，包括但不限于用户的签到记录、消息内容、微薄内容、文件内容、各种操作记录、设备使用情况等
  - 归档记录当前不删除

2.4 灾备与业务连续性

云之家拥有完备的灾难与应急事件响应预案，并定期对预案进行演练、更新。同时，为应对灾难与应急事件，云之家通过多项技术提前预防：

- 多机房部署
- 多网络接入
- 数据在线备份
- 数据异地备份
- 数据离线备份
- 应用自动部署
- 应用自主恢复
- 统一运维管理
- 日志集中记录并分析等

2.5 移动设备安全

云之家通过多项措施来保障用户的设备使用安全：

- **可信设备认证**：避免账号意外泄露时在其他设备上登录，造成信息泄露
- **可信设备管理**：可查看所有已信任的设备，及时发现异常设备，并进行处理（目前暂支持反馈至云之家进行处理）
- **移动设备安全通讯**：使用安全可靠的 HTTPS 技术，防止通过过程中被劫持、窃取信息，造成数据泄露
- **组织架构安全**：通讯水印技术，对组织架构进行渲染，防止无法追踪因组织架构泄露而无法追查的情况
- **人员详情安全**：通过水印连锁反应，对人员详情信息进行渲染，追踪使用人员
- **截屏通知**：对用户截屏进行通知并后台记录，方便追踪因截屏而造成的信息泄露
- **设备异常登录下线**：对不可信任设备，可进行下线处理（目前暂支持云之家后台处理）
- **图案解锁支持**：支持应用切换至后台重新唤起或重启应用时，进行图案解锁，避免其他人员不经意查看
- **账号冻结安全**：支持临时冻结账号，避免手机丢失后用户信息被泄露。冻结后，该账号将无法登录，直至解冻前
- **无痕消息**：消息发出后，可在短时间内撤回或在预定时间内销毁

3 合规安全及安全荣誉

云之家通过不断努力，提升安全性，获得了多项荣誉，包括：

3.1 ISO27001-信息安全管理体系

bsi.

Certificate of Registration

信息安全管理体系 - ISO/IEC 27001:2013

兹证明：

深圳云之家网络有限公司
中国
广东省
深圳市
南山区科技园
科技南十二路2号
金蝶软件园A座10层北区
邮编：518057

Shenzhen Cloudhub Network Co., Ltd.
North of Floor 10, Tower A
Kingdee Software Park, 2 KeJi 12 th Road South
High-tech Industrial Park
Nanshan District, Shenzhen
Guangdong
518057
China

持有证书： **IS 679017**

并运行符合 ISO/IEC 27001:2013 要求的信息安全管理体系，认证范围如下：

提供“云之家”SaaS（软件即服务）云服务。
这与2019年5月15日版本5.0的适用性声明相一致。
注册地址：深圳市前海深港合作区前湾一路1号A栋201室
The provision of "Cloudhub" SaaS (Software as a Service) Cloud Services.
This is in accordance with the Statement of Applicability version 5.0, dated on May 15, 2019.
Registration address: Room 201, Building A, No.1 Qianwan Yi Lu, Qianhai Shenzhen-Hongkong Cooperation Zone, Shenzhen

BSI代表：

Chris Cheung，亚太地区 合规风险主管

首次发证日期： 2017-10-31
最新发证日期： 2020-10-30

生效日期： 2020-10-31
有效期至： 2023-10-30

Page: 1 of 2

...making excellence a habit.™

此证书以电子版本方式发放，所有权属BSI并受合同条款的约束。
可以 在线 查询电子证书的有效性
打印的证书可以通过网站 http://www.bsi-global.com/ClientDirectory或者致电 +86 10 8507 3000 查询。
本证书信息亦可在国家认证认可监督管理委员会官方网站 (www.cnca.gov.cn) 上查询。
关于证书范围及 ISO/IEC 27001:2013 要求的适用性的进一步说明请咨询BSI。
获证组织必须定期接受监督审核并经审核合格此证书方继续有效。
此证书只在提供完整正本时才有效。

信息查询及联系方式：BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. 电话：+44 345 080 9000
BSI保证英国有限公司，注册地英国，注册号码7805321，地址：389 Chiswick High Road, London W4 4AL, UK
英标管理体系认证（北京）有限公司 北京市建国门外大街甲24号东海中心2008室 邮编：100004 电话：+86 10 85073000
BSI集团公司成员。

持有证书： **IS 679017**

地点	认证活动
深圳云之家网络有限公司 中国 广东省 深圳市 南山区科技园 科技南十二路2号 金蝶软件园A座10层北区 邮编：518057 Shenzhen Cloudhub Network Co., Ltd. North of Floor 10, Tower A Kingdee Software Park, 2 KeJi 12 th Road South High-tech Industrial Park Nanshan District, Shenzhen Guangdong 518057 China	提供“云之家”SaaS（软件即服务）云服务。 这与2019年5月15日版本5.0的适用性声明相一致。 注册地址：深圳市前海深港合作区前湾一路1号A栋201室 The provision of "Cloudhub" SaaS (Software as a Service) Cloud Services. This is in accordance with the Statement of Applicability version 5.0, dated on May 15, 2019. Registration address: Room 201, Building A, No.1 Qianwan Yi Lu, Qianhai Shenzhen-Hongkong Cooperation Zone, Shenzhen

首次发证日期： 2017-10-31
最新发证日期： 2020-10-30

生效日期： 2020-10-31
有效期至： 2023-10-30

Page: 2 of 2

此证书仅与获证组织的信息安全管理体系相关，不涉及获证组织的产品和服务。
此证书编号、认证机构和/或认可机构标志不得出现在产品或与产品、服务相关的文件中。
在宣传资料、广告或其他文件中使用证书信息、认证机构商标或认可标志必须与认证目的一致。
该证书本身并不免除获证组织应当承担的法律义务。

此证书以电子版本方式发放，所有权属BSI并受合同条款的约束。
可以 在线 查询电子证书的有效性
打印的证书可以通过网站 http://www.bsi-global.com/ClientDirectory或者致电 +86 10 8507 3000 查询。
本证书信息亦可在国家认证认可监督管理委员会官方网站 (www.cnca.gov.cn) 上查询。
关于证书范围及 ISO/IEC 27001:2013 要求的适用性的进一步说明请咨询BSI。
获证组织必须定期接受监督审核并经审核合格此证书方继续有效。
此证书只在提供完整正本时才有效。

信息查询及联系方式：BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. 电话：+44 345 080 9000
BSI保证英国有限公司，注册地英国，注册号码7805321，地址：389 Chiswick High Road, London W4 4AL, UK
英标管理体系认证（北京）有限公司 北京市建国门外大街甲24号东海中心2008室 邮编：100004 电话：+86 10 85073000
BSI集团公司成员。

云之家 ISO 27001 认证

3.2 ISO27018-公有云个人信息保护管理体系

bsi.

Certificate of Registration

公有云个人信息保护管理体系 - ISO/IEC 27018:2019

兹证明：

深圳云之家网络有限公司
中国
广东省
深圳市
南山区科技园
科技南十二路2号
金蝶软件园A座10层北区
邮编：518057

Shenzhen Cloudhub Network Co., Ltd.
North of Floor 10, Tower A
Kingdee Software Park, 2 KeJi 12 th Road South
High-tech Industrial Park
Nanshan District, Shenzhen
Guangdong
518057
China

持有证书： **PII 706147**

并运行符合ISO/IEC 27018:2019控制要求的公有云个人信息保护管理体系，认证范围如下：

提供“云之家”SaaS（软件即服务）云服务。
这与2019年5月15日版本5.0的适用性声明相一致。
（关联ISO27001:2013证书编号IS 679017）
注册地址：深圳市前海深港合作区前湾一路1号A栋201室
The provision of "Cloudhub" SaaS (Software as a Service) Cloud Services.
This is in accordance with the Statement of Applicability version 5.0, issued on May 15, 2019.
(ref. ISO27001:2013 certificate number IS 679017)
Registration address: Room 201, Building A, No.1 Qianwan Yi Lu, Qianhai Shenzhen-Hongkong Cooperation Zone, Shenzhen

BSI代表：

张明，董事总经理，英标管理体系认证（北京）有限公司

首次发证日期： 2019-09-11
最新发证日期： 2020-10-30

生效日期： 2020-10-31
有效期至： 2023-10-30

Page: 1 of 1

...making excellence a habit.™

此证书以电子版本方式发放，所有权属BSI并受合同条款的约束。
可以 在线 查询电子证书的有效性
打印的证书可以通过网站 http://www.bsi-global.com/ClientDirectory或者致电 +86 10 8507 3000 查询。
关于证书范围及 ISO/IEC 27018:2019 要求的适用性的进一步说明请咨询BSI。
此证书只在提供完整正本时才有效。

信息查询及联系方式：
英标管理体系认证（北京）有限公司 北京市建国门外大街甲24号东海中心2008室 邮编：100004 电话：+86 10 85073000
BSI集团公司成员。

云之家 ISO 270018 认证

3.3 信息安全等级保护第三级

信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，深圳云之家网络有限公司单位的：

第3级 云之家 系统

予以备案。

证书编号：440317-13105-00001

中华人民共和国公安部监制

备案公安机关公章

2019年03月18日

云之家等保备案证明

深圳市信息安全等级保护
测评结果通知书

编 号：
SZCP20210711

依据《信息安全等级保护管理办法》等有关规定，深圳云之家网络有限公司单位已按规定开展2021年度等级保护测评工作。

特此通知

测评系统信息：
1、云之家系统，三级，良。

深圳市信息安全等级保护工作协调领导小组办公室
2021 年 07 月 26 日

测评机构：深圳市网安计算机安全检测技术有限公司
测评日期：2021.05.16-2021.07.12

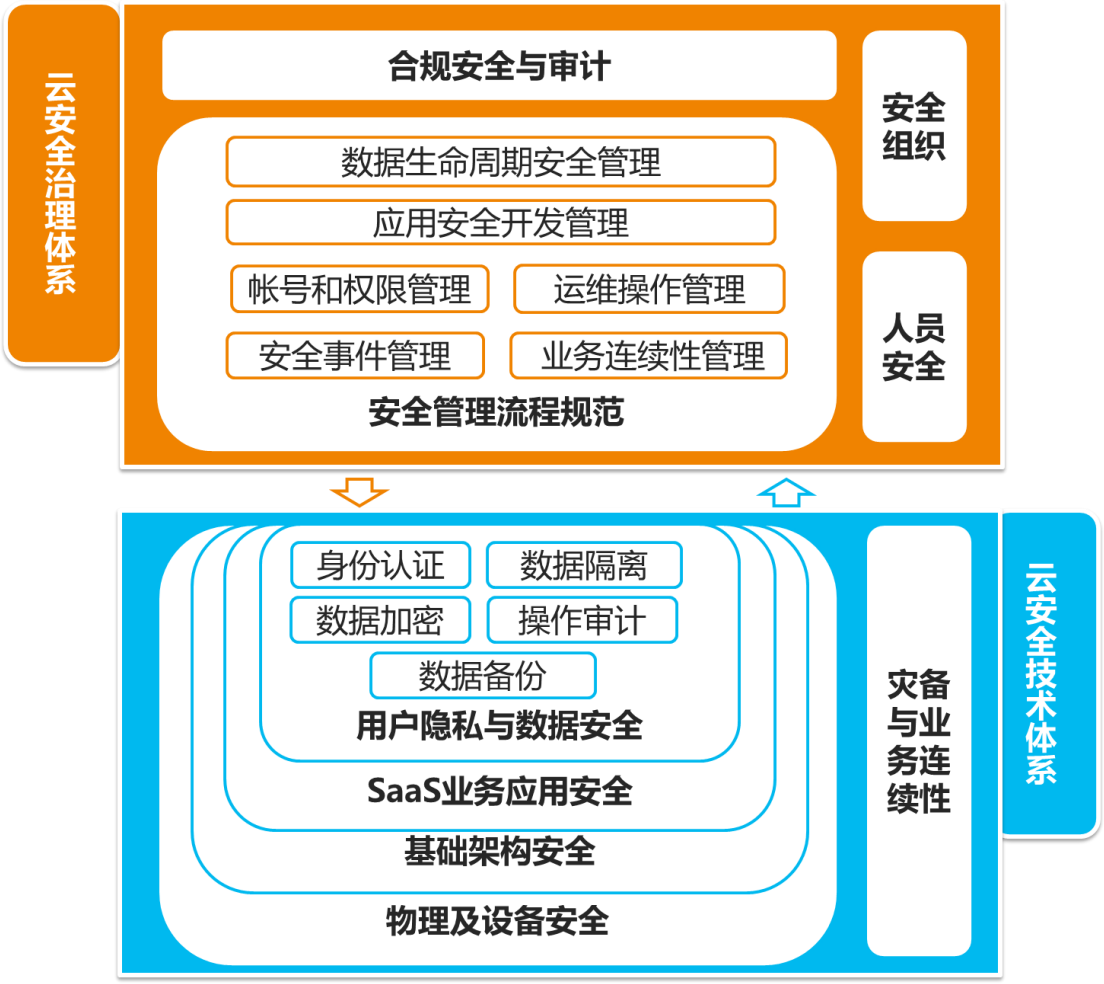
2021 年云之家等保三级测评结果通知书

3.4 CSA 云安全指南体系（参照）

云之家根据 CSA 云安全指南进行建设：

在管理上，云之家制定了各种管理规范，对人员、开发、账号管理、运维、事件、审计等多方面进行严格要求，并不断复核、改进；

在技术上，云之家严格筛选和监督 IaaS 供应商的安全，关注 SaaS 应用安全，对于数据安全，层层把控、严密防御、实时监督并制定各种数据安全策略，来保障数据的可用性、完整性和机密性。



3.5 IaaS 供应商—金山云安全资质及荣誉

3.5.1 ISO27001—信息安全管理体系

bsi.

Certificate of Registration

信息安全管理体系 – ISO/IEC 27001:2013

兹证明：

北京金山云网络技术有限公司
中国
北京市
海淀区
西二旗中路33号院小米科技园E座
邮编：100085

Beijing Kingsoft Cloud Network Technology Co., Ltd.
Tower E, Xiaomi Campus
No. 33, Xierqi Middle Road
Haidian District
Beijing
100085
China

持有证书： **IS 716522**

并运行符合 ISO/IEC 27001:2013 要求的信息安全管理体系，认证范围如下：

请见认证范围页

BSI代表：

Chris Cheung，亚太地区 合规风险主管

首次发证日期： 2019-10-09
最新发证日期： 2021-09-15

生效日期： 2019-10-09
有效期至： 2022-10-08

Page: 1 of 9

...making excellence a habit.

此证书以电子版本方式发放，所有权属BSI并受合同条款的约束。
可以 在线 查询电子证书的有效性
打印的证书可以通过网址 http://www.bsi-global.com/ClientDirectory或者致电 +86 10 8507 3000 查询。
本证书信息亦可在国家认证认可监督管理委员会官方网站 (www.cnca.gov.cn) 上查询。
关于证书范围及 ISO/IEC 27001:2013 要求的适用性的进一步说明请咨询BSI。
获证组织必须定期接受监督审核并经审核合格此证书方继续有效。
此证书只在提供完整证书时才有效。

请查询关联系方式：BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. 电话：+44 345 080 9000
BSI保证英国有限公司，注册地英国，注册号码7805321，地址：389 Chiswick High Road, London W4 4AL, UK
英标管理体系认证（北京）有限公司 北京市建国门外大街甲24号东海中心2008室 邮编：100004 电话：+86 10 85073000
BSI集团公司成员。

3.5.2 信息安全等级保护第三级


信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，北京金山云网络技术有限公司单位的：

第 3 级 金山云服务平台系统 系统

予以备案。

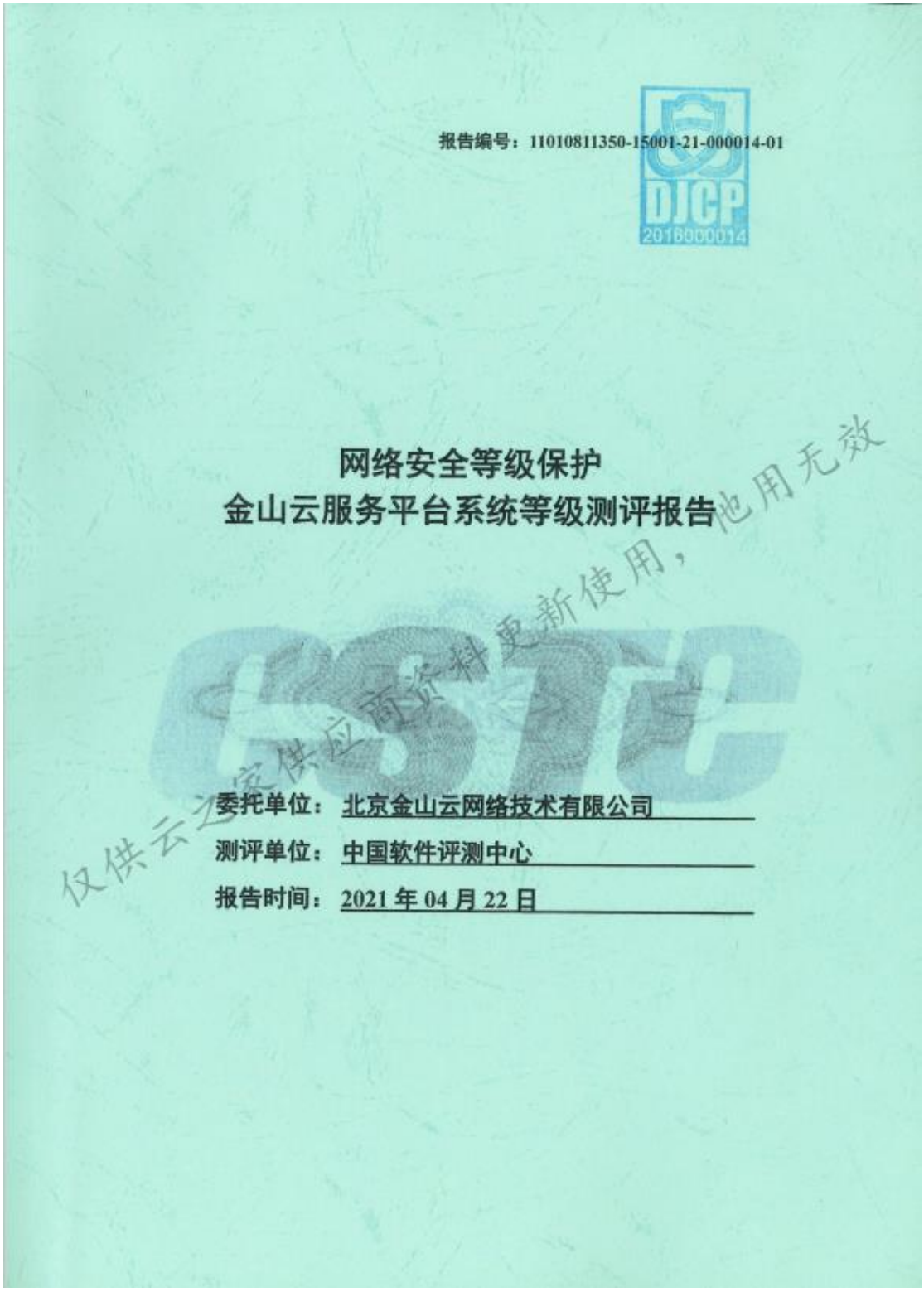
证书编号：11010811350-15001

中华人民共和国公安部监制

备案公安机关公章

201 年 月 日

金山云等保备案证明



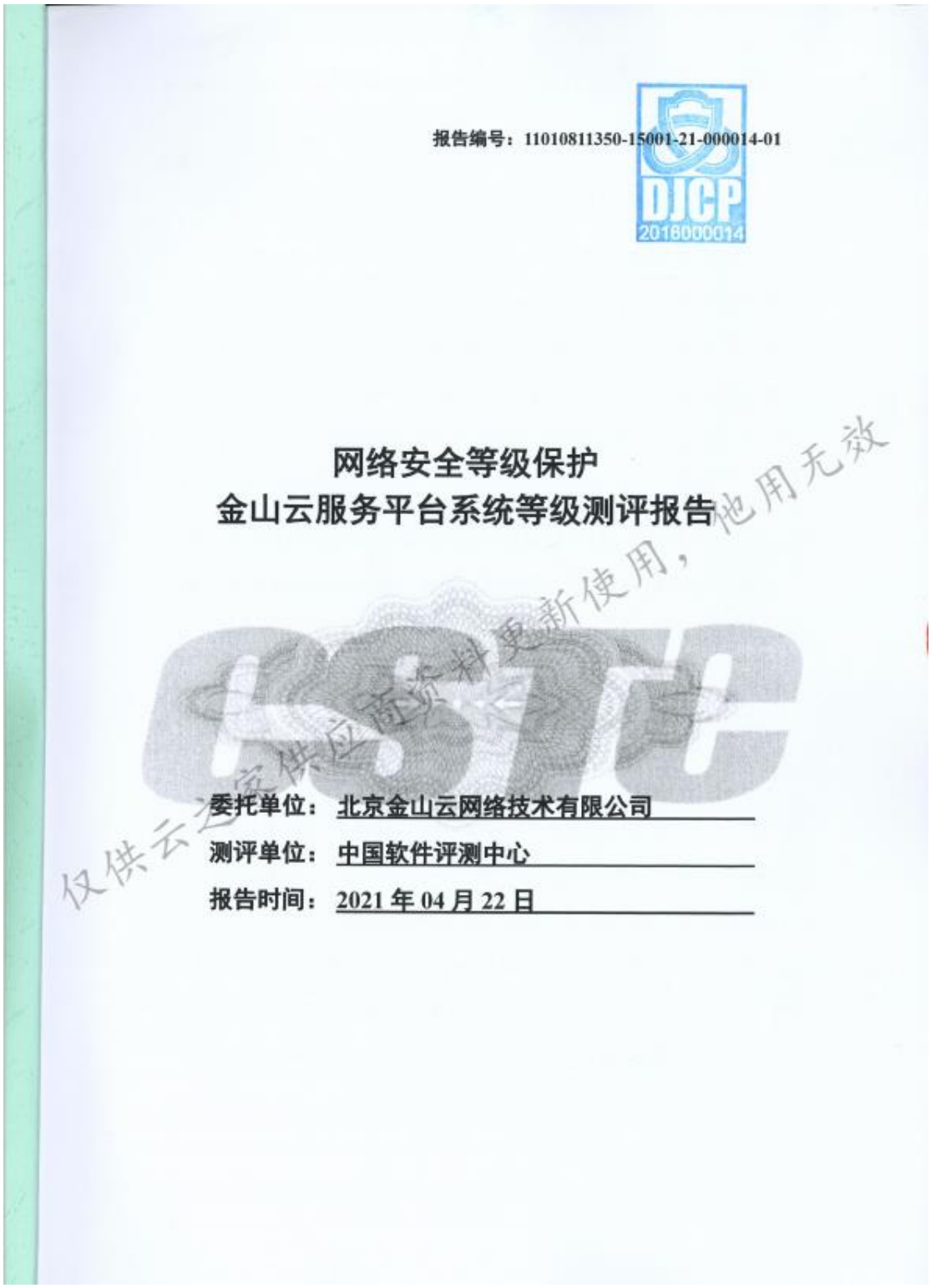
报告编号：11010811350-15001-21-000014-01

网络安全等级保护
金山云服务平台系统等级测评报告

委托单位：北京金山云网络技术有限公司

测评单位：中国软件评测中心

报告时间：2021 年 04 月 22 日



报告编号：11010811350-15001-21-000014-01

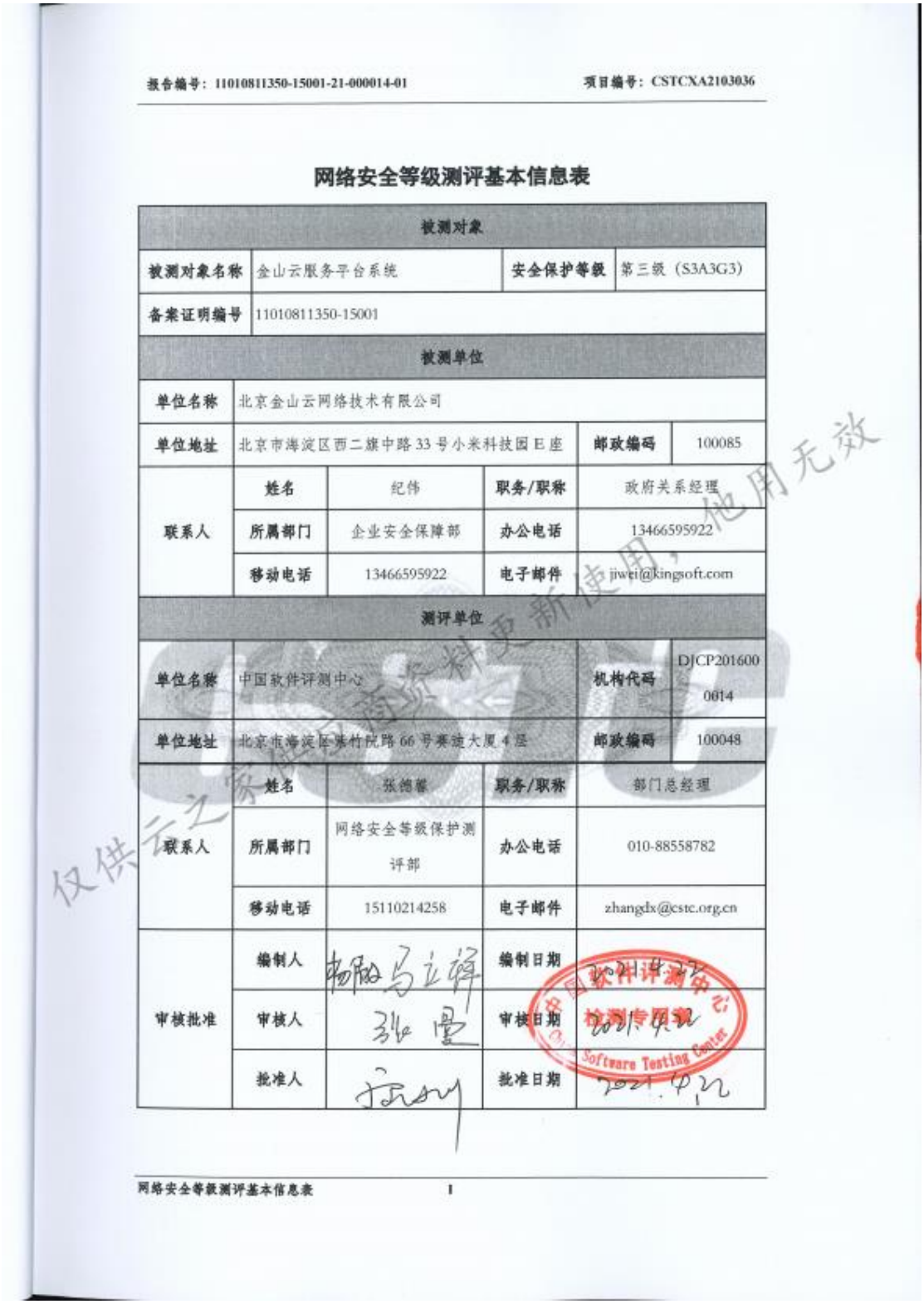
DJCP 2018000014

网络安全等级保护
金山云服务平台系统等级测评报告

委托单位：北京金山云网络技术有限公司

测评单位：中国软件评测中心

报告时间：2021 年 04 月 22 日



报告编号：11010811350-15001-21-000014-01　　项目编号：CSTCXA2103036

网络安全等级测评基本信息表

被测对象				
被测对象名称	金山云服务平台系统		安全保护等级	第三级（S3A3G3）
备案证明编号	11010811350-15001			
被测单位				
单位名称	北京金山云网络技术有限公司			
单位地址	北京市海淀区西二旗中路33号小米科技园E座		邮政编码	100085
联系人	姓名	纪伟	职务/职称	政府关系经理
	所属部门	企业安全保障部	办公电话	13466595922
	移动电话	13466595922	电子邮件	jiwei@kingsoft.com
测评单位				
单位名称	中国软件评测中心		机构代码	DJCP2016000014
单位地址	北京市海淀区学院路66号赛迪大厦4层		邮政编码	100048
联系人	姓名	张德馨	职务/职称	部门总经理
	所属部门	网络安全等级保护测评部	办公电话	010-88558782
	移动电话	15110214258	电子邮件	zhangdx@cstc.org.cn
审核批准	编制人		编制日期	
	审核人		审核日期	
	批准人		批准日期	

网络安全等级测评基本信息表　1

声明

本报告是金山云服务平台系统的等级测评报告。

本报告是对金山云服务平台系统的整体安全性进行检测分析，针对等级测评过程中发现的安全问题，结合风险分析，提出合理化建议。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效，当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）都应重新进行等级测评，本报告不再适用。

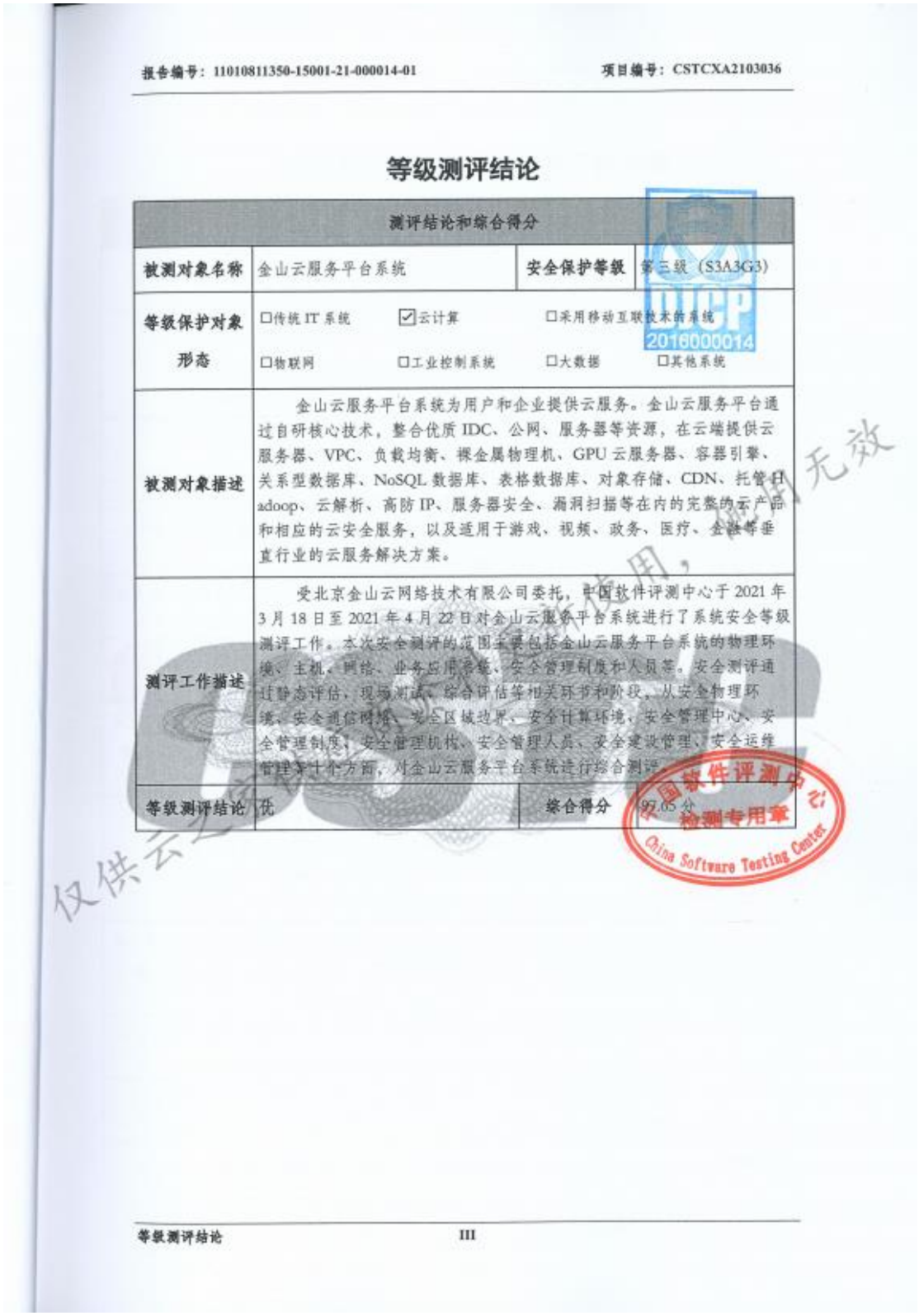
本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

中国软件评测中心

（加盖单位公章）

2021 年 04 月 22 日



报告编号：11010811350-15001-21-000014-01　　项目编号：CSTCXA2103036

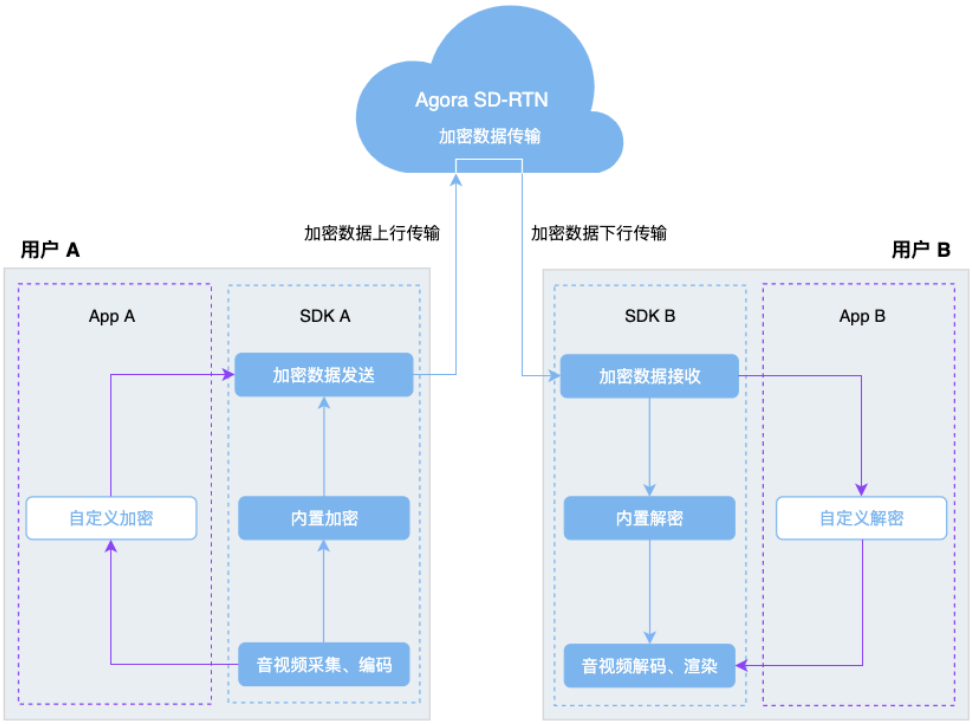
等级测评结论

测评结论和综合得分			
被测对象名称	金山云服务平台系统	安全保护等级	第三级（S3A3G3）
等级保护对象形态	□传统 IT 系统　☑云计算　□采用移动互联技术的系统 □物联网　□工业控制系统　□大数据　□其他系统		
被测对象描述	金山云服务平台系统为用户和企业提供云服务。金山云服务平台通过自研核心技术，整合优质 IDC、公网、服务器等资源，在云端提供云服务器、VPC、负载均衡、裸金属物理机、GPU 云服务器、容器引擎、关系型数据库、NoSQL 数据库、表格数据库、对象存储、CDN、托管 Hadoop、云解析、高防 IP、服务器安全、漏洞扫描等在内的完整的云产品和相应的云安全服务，以及适用于游戏、视频、政务、医疗、金融等垂直行业的云服务解决方案。		
测评工作描述	受北京金山云网络技术有限公司委托，中国软件评测中心于 2021 年 3 月 18 日至 2021 年 4 月 22 日对金山云服务平台系统进行了系统安全等级测评工作。本次安全测评的范围主要包括金山云服务平台系统的物理环境、主机、网络、业务应用系统、安全管理制度和人员等。安全测评通过静态评估、现场测试、综合评估等相关环节和阶段，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个方面，对金山云服务平台系统进行综合测评。		
等级测评结论	优	综合得分	97.65 分

等级测评结论　　III

2021 年金山云等保测评三级测评结果

3.6 语音/视频 供应商—声网（agora）信息安全说明



声网（agora）数据传输示意图

云之家的语音/视频会议均由合作伙伴声网（agora）提供技术支持，其产品信息安全说明详情如下：
https://docs.agora.io/cn/Agora%20Platform/security?platform=All%20Platforms

4 安全指标速查

- 通信安全
  - HTTPS 技术，无已知漏洞，使用 AES256 及 RSA2048 加密，DH2048 密钥交换技术，TLS 1.0-1.3 协议
  - 支持 VPN
- 数据安全性
  - 可用性（Availability）
    - 多重在线备份、异地备份、离线备份技术同时使用
  - 完整性（Integrity）
    - 数据库备份机制，保障完整性
    - 通过监控手段，对数据偏离超过阈值时进行告警并安排处理
  - 机密性（Confidentiality）
    - 纵深防御体系

- 网络防火墙
- 网络访问控制
- 应用防火墙 WAF
- 租户数据隔离
- IAM 统一身份认证
- MFA 多因子认证
- 安全检查（每天）
- 审计检查（每天）
- 日志审查（实时）

- 安全标准和规范
  - ISO 27001 《信息安全管理要求》
  - CSA 云安全指南（参照）
  - 可信网站荣誉（商务部认证）
  - 安全联盟行业认证
- 业务安全
  - 水印功能
  - 截屏通知功能
  - 可信设备管理
  - 新设备验证
  - 敏感内容检测
  - 移动设备管理
  - 用户账号防暴力破解
  - 无痕消息

附录：云之家安全 Q&A

关于数据泄露

问题1： 云之家储存了什么数据，会不会被攻击泄露？

答：云之家并不存储企业任何业务系统，自有应用和第三方应用的数据，仅保存了用户的消息、消息附件、企业组织信息、部落微博内容及文件、Native 应用产生的信息（指由云之家提供的轻应用：签到、我的文件、我的客户等）。

云之家采用纵深防御体系，多重机制保护数据安全，包括但不限于：物理安全防御、网络防火墙、应用防火墙（WAF）、数据加密存储、数据隔离、访问控制、实时安全监测、安全预警及分析、数据追踪溯源等。通过以上各种安全手段

和安全管理方法，我们有信心保障用户的数据不被泄露。

问题2：　云之家用户跟手机是怎么捆绑的？手机丢失怎么办？

答：云之家用户通过唯一标识号与手机号绑定。如用户手机丢失，可用同事手机拨打 4008-308-110，与银行卡挂失一样将该用户立即冻结。

问题3：　员工截屏、转发受限文件怎么办？

答：敏感信息界面如会话消息、通讯录等均有水印保护，同时还有截屏操作警醒；机密文件禁止转发、下载，非机密文件转发、下载保存操作记录以备审计所用。

问题4：　云之家会不会偷看客户的数据？

答：客户在云之家上产生的数据均属客户所有，必须使用最终用户账号、密码方能访问。除非经用户授权协助特定需求处理，云之家运维及数据库管理员不能查看用户数据，并且，云之家公司与相关岗位人员均签署《保密协议》从法律层面进一步保障。

问题5：　公有云其他客户能看到我的数据吗，譬如组织架构和人员信息等？

答：云之家使用符合国际 SaaS 标准的信息隔离机制，在云之家中建立的每个企业都是独立的信息空间，用户不能访问非本企业的数据。

问题6：　开发轻应用连接公司现有业务系统是否安全？内网或本地化管理的业务数据是否会被拦截？

答：云之家不存储任何接入的轻应用及相关业务系统的数据，连接访问采用 HTTPS 保障传输安全，还支持有条件的企业采用 VPN 技术加固，所以不会降低已有业务系统的安全性，也没有数据被拦截的风险。

问题7：　连接第三方应用会不会导致公司数据被第三方窃取？

答：所有接入云之家的第三方应用都经过云之家认证，未经客户授权并由客户 IT 部门开放接口无法访问客户现有系统数据，并且和云之家公司签署《开发者协议》从法律层面进一步保障。

问题8：　员工或公司的数据是否可以被导出？

答：为保障用户隐私，仅支持个别与企业业务直接相关的数据导出，如企业通讯录、签到数据等，且只允许企业管理员使用。

问题9：　员工离职后，他的历史数据是否安全？

答：客户在云之家上产生的数据均属客户所有，员工离职后，与公司直接相关的数据转交企业系统管理员归档处理，离职员工本人不能再登录公司访问任何与公司直接相关的数据。

问题10：　离职员工是否能看到原工作圈中的内容？

答：员工离职后不能登录原公司查看任何信息。

问题11： 云之家的人谁能看云之家系统数据？云之家是怎样管理的？

答：云之家存储的数据只有运维人员和数据库管理员可以接触，云之家公司和相关人签署《保密协议》从法律层面进一步保障，并且对每次操作都有详细记录和审计。

问题12： 账号是否很容易被盗？

答：云之家采用纵深防御措施，多重保护用户安全。除非用户使用易被猜测的账号、密码或无意识泄露账号信息，否则账号将非常安全。

问题13： 弱密码账号如何保证安全性？

答：云之家推荐使用 8 位以上包含数字、大小写字母及特殊字符组合的密码。如账号不小心泄露给别人了，他用我的账号登录，系统会自动识别设备信息并要求通过手机验证码登录。

问题14： 云之家后台运行的时候再次打开是否有密码保护？

答：后台唤起支持图案解锁，可以在“我-设置-手势密码”中设置。

问题15： 同商务伙伴的聊天信息是否有外泄风险？

答：同商务伙伴的聊天如果属于机密内容可以采用无痕消息（阅后即焚）的方式，同时云之家也提供了水印、截屏警醒功能增强安全性。

问题16： 云之家会不会拿客户的数据去做大数据分析或者卖给别人？

答：云之家用于实时分析系统运行状况并持续优化所用的数据不包含任何用户隐私类信息和业务信息，不可能贩卖数据，云之家公司和客户签署《用户使用协议》从法律层面进一步保障。

问题17： 云之家、云之家员工、用户、第三方开发者之间有什么的保密协议约束？

答：用户与云之家有用户使用协议约束，云之家员工有保密协议约束，开发者与云之家有开发者协议约束，开发者与用户有授权关系约束。

问题18： 遇到黑客攻击怎么办、是否可以提供专业文档给企业 IT 人员评估？

答：云之家通过应用安全防火墙（WAF）有效防御黑客攻击，系统运维定期进行安全检查、渗透测试，及时升级安全防护技术动态保障安全性。云之家运维团队定期和企业 IT 分享防攻击动态及相关技术文档。

关于数据防丢失

问题19： 客户的数据是否有备份？是否会丢失？

答：云之家服务器端数据采用多重异地在线备份，至少现时存在 3 份可用数据。即使 1 台或 1 个机房的设备出现故障，云之家也能保障数据不丢失。

问题20： 服务器防攻击能力如何？

答：云之家采用了应用防火墙（WAF）、网络防火墙、安全监测、实时安全告警、每日安全检查、每日日志分析、审计检查等多种安全手段，保障服务器安全。

问题21： 哪些应用是云之家的？它的数据是怎样保障安全的？其他第三方的应用数据是怎样保障安全的？

答：通过消息、微博发送的文字内容及附件内容，将被存在在云之家服务器。云之家通过多重在线异地备份机制保障数据的可用性和完整性，通过纵深防御体系保障数据的安全性。 云之家支持第三方应用采用云之家的云服务平台（IaaS 采用的金山云）及相关安全技术保障数据安全，同时要求第三方应用开发商和云之家公司签署《开发者协议》从法律层面进一步保障。

问题22： 用户手机丢失或更换手机后，数据是否能找回？比如签到记录是否会受影响？

答：所有数据都存储在服务器端，可以随时找回历史数据，所有数据均不会受影响。

问题23： 云之家在手机、ipad、电脑之间的数据迁移安全性怎么保障？

答：用户产生的数据都保存在服务器端，这些数据都有备份和多重保护，客户端仅缓存展示数据。