用友
yonyou

用友云 安全白皮书
yonyou cloud

用友云
yonyou cloud

安全、值得信赖！

用友云 | 企业服务都在这
yonyou cloud

地址：北京市海淀区北清路 68 号用友产业园（100094）
客户专线：4006 815 456　QQ 服务：4006 815 456
网址：www.yonyou.com

用友云订阅号　用友云应用服务号

说明

用友云对安全问题非常重视，本白皮书是用友云安全在当前阶段的理念、战略、框架与关键策略解读。这些内容会不断发展变化，本白皮书也会根据用友云安全的最新变化而更新。

本白皮书的目的是让用友云的合作伙伴和客户更加系统、深入地了解用友云安全，以此促进整个用友云生态的安全。

安全问题涉及领域众多、纷繁复杂，本白皮书撰写时间仓促，难免有疏漏之处，欢迎大家就用友云安全提出各种批评建议，我们将随时改进。

敬请联系：陈杰，chenjie2@yonyou.com

目录
Contents

1.1 用友云定位

用友云，是用友在云服务时代，结合云计算、大数据、移动、社交、智能等新一代企业计算技术，以PaaS +SaaS +DaaS +BaaS等全新理念而构建的社会级商业应用基础设施，并以此为基础向用户提供一站式企业服务。

用友iUAP云平台是用友云的核心，是面向社会化商业应用的基础平台。它为企业提供开放的PaaS平台服务，解决云模式下企业应用及服务的开发问题、运维问题、运营问题；基于用友iUAP云平台，用友云提供包含社交与协同办公云、财务云、人力云、采购云和营销云在内的全面SaaS应用服务，以及连接内外的DaaS数据服务、专业的BaaS运营服务，并适配多种IaaS服务平台。

基于iUAP云平台，用友云还致力于建设云市场，在开发核心应用之外，开放联合第三方合作伙伴以及开发者，为企业提供面向社会化商业的一站式社会级企业服务，为企业管理创新、商业模式变革、全球化发展提供“面向未来”的社会化商业平台。

1.2 云安全发展态势

1.1.1 云安全定义

云安全，主要包含两个方面的含义。第一是云计算自身的安全，也称为云计算安全，包括物理安全、网络安全、应用安全以及数据安全等方面，云计算安全是云计算技术健康可持续发展的基础；第二是使用云的形式提供和交付安全，也即云计算技术在安全领域的具体应用。

用友云安全主要是针对第一方面，同时用友云会和第二方面的云安全服务商进行紧密合作，共同为客户提供良好的安全服务。

1.1.2 云安全存在的问题

对于云安全，云安全联盟（CSA）发布了七大主要安全威胁，具体如下：

- 云计算的滥用、恶用、拒绝服务攻击
- 不安全的接口和API
- 恶意的内部员工
- 共享技术产生的问题
- 数据泄漏
- 账号和服务劫持
- 未知的安全场景

根据这些威胁，一般而言，可以将云安全问题分为以下六类：

云本身的安全

“云”计算实际上对外部是不透明的。云计算的服务商并没有把员工情况、所采用的技术以及运作方式等许多细节对用户进行具体说明，尤其是在计算服务被一系列的服务外包商提供时，每一家外包的服务提供商基本上都是以不可见的方式提供计算处理或数据存储的服务。这就造成了服务商使用的技术不可控的结果，用户会担心服务商以用户未知的方式越权访问用户数据的情况发生。

云安全标准

在本地化部署阶段，很多标准用于衡量IT系统的安全性，其中等级保护制度便是其中最具代表性的标准体系。随着IT系统不断地迁移到云计算环境上，过去的等级保护体系出现了一些不太适用的情况。因此，GB/T22239.2专门针对云计算作了扩展要求，形成全新的云等保体系，并开始全面推广。

物理安全

物理安全是需要确保云计算基础物理设备的正常运转，如服务器、机房、供电、网线等。在实际运转过程中，不论是地震、高温等自然因素还是恶意损坏等人为因素，都有可能导致这些物理设备损坏或者其他形式的中断服务。

网络安全

网络安全是指通过网络边界流量控制等手段来确保网络通信安全。用户向云端迁移后，网络边界逐渐模糊化，原先的物理隔离以及边界流量控制设备等手段已经难以用来控制边界网络流量。目前，常见的网络安全威胁包括VPC隔离性差、DDoS攻击、DNS劫持等。

数据安全

企业内部数据向云端迁移后，企业用户将不直接控制数据，传统的用来保护数据安全性的措施无法直接采用。云中存储数据的安全性核查需要在不能掌握全局数据的条件下进行。考虑到用户存储在云中的数据的多样性和长久的安全性，数据安全性面临着更大的挑战。目前数据安全面临的主要威胁有拖库、撞库、弱口令、木马、钓鱼等。

应用安全

应用安全是需要确保业务应用的可用性、真实性、完整性和连续性。部署在云端的业务应用变得更加难以控制，尤其部署在公有云上的业务，所有用户都可以访问企业的业务应用，这就更增加了应用安全隐患。常见的应用安全威胁包括SQL注入、XSS跨站脚本、Webshell、网站挂马等等。

1.1.3 云安全发展态势

当前，云安全发展呈现以下三个特点：

自动化与智能化

云计算的发展让企业IT规模成倍扩大，通过安全自动化与安全智能技术，可以逐步解放以前以手工为主的安全部署、安全配置、安全分析、安全调查等环节，以获得更强的预测、检测与响应能力。

云管端协同化

防御协同方面，终端、网络与云端之间的配合越来越紧密，呈现出云管端协同化的趋势。抗DDoS技术的云化便是安全协同的一个重要演进趋势。DDoS攻击正在向全球化、大流量发展，管道拥塞频发。因此，通过各类资源的云化池化，再基于流量牵引智能调度的技术，在攻击发生时，自动集中优势资源，实现智能清洗，确保用户业务连续性。

管防控一体化

单纯的防御难以应对云计算时代无处不在的网络威胁。就国内来看，随着《中华人民共和国网络安全法》和云等保政策的推出，行政管理、云安全防御与企业安全控制会逐渐形成一体化的安全策略。

1.3 用友云的安全观

“可信、可靠、保障、贴心”是用友云提供服务的核心理念；与安全领域领先厂商强强联合，共同维护云应用安全，是用友云的重要安全策略；保障用户在用友云上的数据安全、业务安全是用友云服务的基准生命线。

在保障用户云安全方面，用友开放在企业服务领域30年的能力积累，联合安全领域的领先服务商，从安全治理到安全技术、从安全开发到安全运维、从安全生产到安全运营，按照国家安全标准和业界领先的安全实践进行严密的战略、流程和技术的设计与实现，为客户和伙伴提供社会级的安全保障，服务覆盖从物理环境、访问控制、配置管理、应急响应、安全审计、持续监控、供应链等多个环节的安全控制要求。

2.1 安全治理架构

用友云的安全治理结构在业界独树一帜，组织架构非常科学。用友云的安全治理由安全管理委员会、安全专家工作小组、产品安全接口和保障组为核心，并在开发团队、测试团队和运维团队都配置相应的安全技术实施、保障和服务人员，为客户和伙伴提供覆盖全生命周期安全保障的企业服务云平台。

用友云安全实行安全问题一票否决制。

用友云安全治理架构

资料来源：用友云，2017

2.2 人员安全管理

用友云在工作人员本身的安全管理方面非常重视，并且有一套完备的相应制度来确保其安全运营。

2.2.1 尽职调查

在入职前，用友在国家法律法规允许的情况下,通过一系列背景调查手段来确保入职的员工符合公司的行为准则、保密规定、商业道德和信息安全政策,背景调查手段涉及刑事、职业履历和信息安全等方面,背景调查的程度取决于岗位需求。

2.2.2 安全生产

在入职后,所有的员工必须签署保密协议,确认收到并遵守用友的安全政策和保密要求,尤其关于客户信息和数据的机密性要求将在入职培训过程中被重点强调。此外,用友公司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。最后,用友通过企业价值观考核的方式检验每位员工是否以诚信、敬业的态度来管理每位客户的云端数据,保证其对客户、合作伙伴和竞争对手的尊重；用友提供机密报告机制以确保员工可以匿名报告任何违反安全政策、商业道德的事件。

2.3 安全法务

公司配备完备的安全法务团队，从业人员都是专业的法务人员，对法律、法规的了解和掌握透彻，对安全责任的裁定、审计和跟踪提供专业的服务和咨询，为客户和伙伴在用友云上的安全提供强大的服务基础保障。

安全体系

用友云安全体系采用业界主流的通用框架，主要包括安全管理、安全运维、安全技术三个层面。其基本框架如下图所示。

用友云安全体系图

资料来源：用友云，2017

3.1 安全管理

用友云的安全体系建设，从管理、运维到具体的技术保障，遵循业界的主流的框架和规范。在安全管理上，用友严格遵循相关法规制度和标准，通过对企业业务和运营风险的评估，确定其风险管理框架，安全策略管理框架，确立信息安全文档管理体系。对信息安全战略上的过程、结构与联系进行梳理与监控，以确保组织信息系统的安全管理沿着正确的方向。

用友云符合ISO/IEC 27001/27002，推动信息安全体系(ISMS)建立与实施，采用以风险管理为核心的方法管理公司和用户信息，保障信息的保密性、完整性及可用性；安全审计团队依据该安全标准，审核用友云技术方案与技术框架内部信息安全管理同国际信息安全最佳实践接轨。

用友云符合等级保护基本要求，根据国家下发的《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》开展信息安全等级保护工作，主要是指对国家、法人和其他组织及公民的专有信息， 公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护,对信息系统中使用的信息安全产品实行按等级管理,对信息系统中发生的信息安全事件分等级响应与处置。

用友云符合政策法规，根据国家信息安全相关法律、法规要求，设置与信息安全监控机构之间的联络员，制定实施程序，以确保用友云符合国家关于知识产权相关法律和法规要求。用友云同所有企业及开发者签署保密协议，并通过定期检查识别、记录、评审保密协议中数据安全的相关控制要求(如访问控制、防泄露及完整性要求)， 防止不正当披露、篡改和破坏数据。

3.2 安全运维

用友云运维工作符合ITIL的规范要求和标准，并在安全运维方面进行了加强。对每一个企业服务，都会从检测和评估、修复与加固、监控与防护及响应和审计等方面提出具体的安全检查要求。在安全策略的指导下，利用安全技术来达成用友云的安全保护。

用友云安全运维框架

资料来源：用友云，2017

尤其要指出的是，用友云为企业提供包括很多第三方应用在内的一站式云服务，因此用友云非常强调安全运营管理，以确保所提供的云服务都是安全可靠。用友云产品的运营团队统一对外提供运营服务，以确保运营的安全。在这方面主要涉及用友云合作伙伴和客户的安全运营管理，所有进驻用友云的客户和伙伴都在用友云安全运营的指引下工作。具体包括：实名认证、企业资质认定、企业信用考察、合同条约审定、法律法规的审查、法务工作的指导等。

3.3 安全技术

用友云采用了业界领先的、全面的安全防护技术和产品来确保云安全，具体包括物理安全、基础架构安全、应用安全、数据安全、身份认证和访问安全五个方面。后面会对这五个层面展开详细阐述。

应用安全

应用安全是保障云应用使用的整个生命周期过程中所有过程和结果的安全。 用友云提供全面的应用安全保障，包括用友云使用安全开发流程保障应用开发生命周期安全，通过安全性评估过程保障业务流程安全。用友云提供的应用安全服务包括身份管理和访问控制、日志和监控、 应用安全管理、资源控制，以此达到应用本身的安全，同时支撑企业安全运维管理的需求。

4.1 安全开发生命周期

在安全开发流程上，引入了SDL，借鉴了微软推广SDL的经验，并结合企业级安全需求以及用友云自身的项目开发流程，控制项目整体的安全风险。 SDL 如下：

用友云应用开发安全过程保证

资料来源：用友云，2017

安全开发流程参照软件安全开发周期（ Security Development Lifecycle ）建立：

- 安全需求分析环节：根据功能需求文档进行安全需求分析，针对业务内容、业务流程、技术框架进行沟通，形成《安全需求分析建议》进行审计备案。
- 安全设计环节：根据项目特征，与测试人员沟通安全测试关键点，形成 《安全测试建议》《质量目标》进行审计备案。
- 安全开发环节：整合 OWASP 指南、CERT 安全编码等材料，编制各类编程语言的安全编码规范，避免开发人员写出不安全的代码；使用开发代码扫描工具fortify并结合人工审核代码漏洞，对产品代码进行白盒、黑盒扫描。
- 系统发布环节：安全部门依据上述环节评价结果决定代码是否发布。 服务器资产梳理，形成《服务器资产清单》备案 。对用友云线上环境进行安全漏洞评估，使用绿盟极光远程安全评估系统扫描漏洞，形成《安全漏洞扫描记录》备案。对用友云线上环境进行安全配置评估，形成《安全配置检查记录》备案 。

4.2 安全开发组件

用友云安全在开发组件上提供了丰富的安全组件选择和支持，在框架上要求应用选择工业级别的安全框架，如Spring-security、shiro等；在认证和授权上遵循OATH2规范，单点登陆的最佳实践框架采用CAS；用友云的安全日志组件，集中了安全日志事件，可监控可审计，并在敏感信息上过滤脱敏，去除用户的日志安全顾虑；数据加密组件采用符合国家标准的安全加密算法，用户数据的保密性得到有效保障等。

4.3 日志和监控

用友云提供上机日志、 业务日志和安全日志，通过日志对各个模块的运行情况和用户关键操作进行监控并跟踪记录。UAP 日志遵循 W7 原则，即记录谁、在什么时候、从什么地方、在什么地方、对什么对象做了什么事情、事情的结果是什么。

4.3.1 上机日志

上机日志通过系统管理日志（ system 的上机日志 ）、集团管理日志（集团管理员的上机日志 ）、普通业务日志（其他用户的上机日志 ）来分别记录用户进入或退出的某个功能节点及其时间。系统管理日志和集团管理日志是关键用户日志。

4.3.2 业务日志

业务日志记录用户对业务数据的有效操作内容。业务日志的记录配置支持记录到业务对象的操作和属性级，可以通过配置把敏感的业务对象的哪些操作和哪些属性记录业务日志，业务日志会记录这些属性的变化。对重要的业务对象，系统预置为必须记录业务日志，不可配置为不记录业务日志。

4.3.3 安全日志

安全日志记录发生了哪些与安全有关的活动，谁对这个活动负责。安全日志的目的是追踪和记录发生在涉及安全对象上的事件。 安全日志关注包括身份认证、登录，权限相关（权限管理、授权、权限访问控制 ）、访问控制、特权用户操作、安全配置变更、对关键功能的访问等等。安全日志作为 UAP 系统关键日志默认打开并且不可关闭。

4.3.4 安全事件监控和响应支持

安全事件监控主要包括安全事件的收集、安全事件的归并和过滤、安全事件标准化、安全事件显示和报表。通过安全事件监控可以帮助企业积极监控整个组织内的 IT 资源，过滤并关联事件，迅速定位安全威胁，并为安全事件响应提供支持。用友云提供灵活可扩展的安全事件监控机制，提供包括用户认证异常、权限异常、权限变更、特权用户操作等等安全事件监控。相应的，用友云提供灵活可扩展的安全事件自动响应处理机制，提供发送警告、通知外部安全事件处理系统、邮件、短信等自动响应，提供统一的服务拒绝处理，供事件响应处理调用，如按用户拒绝、按 IP 拒绝、按服务拒绝等，提供安全事件处理方法。同时对第三方安全信息与事件管理系统（ SIEM ）的提供支持。

4.3.5 对审计的支持

用友云通过记录系统各个层次发生的事情， 保留审计线索。通过审计工具能够进行各种系统审计、业务审计、 IT 审计等等，满足企业内控要求。通过安全审计达到对潜在的攻击者起到震慑和警告的作用，对于已发生的系统破坏行为提供有效的追责的证据，为系统管理员提供有价值的系统使用日志，帮助其发现系统入侵行为或潜在的系统漏洞的目的。

4.4 Web应用安全

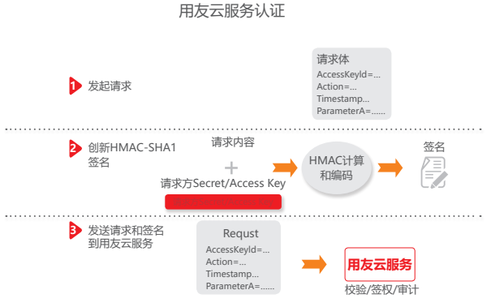
4.4.1 会话安全

会话安全采取如下措施：

- 在每次认证后打开一个新的会话： 即使已经有与用户关联的会话标示符，在用户认证成功之后仍要重新建立一个会话。
- 强制执行一个会话最大空闲时间： 用于缩短那些未能及时注销的用户暴露在外的时间， 减少了可供攻击者猜解的会话ID的平均数目。
- 强制执行一个会话最大生存周期： 增加安全性和稳定性。只有在不超过会话 ID最大生存周期的时候，才允许一个会话不用再次进行对用户的认证。通过进行重新认证，可以防止攻击者窃取会话 ID。

4.4.2 API的服务认证

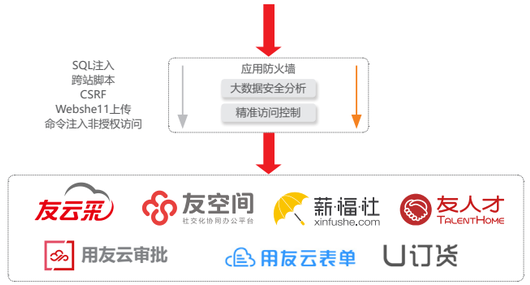
用友云服务会对每个访问的请求进行身份验证，所以无论使用 HTTP 还是 HTTPS 协议提交请求，都需要在请求中包含签名（Signature）信息。通过使用Access Key ID和Access Key Secret进行对称加密的方法来验证请求的发送者身份。Access Key ID和Access Key Secret由用友云官方颁发给访问者（可以通过用友云官方网站申请和管理），其中Access Key ID用于标识访问者的身份；Access Key Secret是用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密，只有用友云和用户知道。



资料来源：用友云，2017

4.4.3 Web应用防火墙

用友云通过阿里云应用防火墙WAF防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，过滤海量恶意CC攻击，避免您的网站资产数据泄露，保障网站的安全与可用性。



资料来源：用友云，阿里云，2017

4.5 企业通讯录安全

企业通信录采用加密存储， 可分级管理通信录，针对不同人群设置不同权限； 同时企业可以设置对重要部门进行保护， 该部门的信息会自动隐藏， 即使是企业内的员工，没有相应权限无法访问。

对于不同公司的信息， 存储空间是相互隔离的，当员工离职后，会被踢出对应的企业群， 自动剥离员工在该企业的权限。

企业可以设置对员工的手机号进行隐私保护， 在对外展示员工信息时隐藏手机号码，防止信息泄露，但不影响电话通讯和电话会议等相关功能的使用。

4.6 电子邮件与短信安全

用友云服务中大量使用到了电子邮箱和短信等服务。用友提供的电子邮箱服务如微邮，结合大数据的技术，能够对垃圾邮件数据进行了有效的清洗，保障用户邮箱不受侵扰和攻击。通过用友云提供的服务在客户端存储是加密保密的，用友云服务发出的邮箱和短信，对链接的使用非常谨慎，防止盗链、跨站攻击的出现。

身份认证和访问

5.1 身份认证

身份认证的目的是在双方建立信任关系。身份认证是信息安全的第一道防线，一个人想要进入一个具有安全机制的系统获取资料，首先必须向系统证实自己的合法身份，才能得到授权访问系统资源。

用友云通过友互通提供统一用户身份管理服务，提升用户的生成效率，减低用户的管理成本。

用友云身份认证

资料来源：用友云，2017

用友云使用密码强制策略用于密码或密钥管理。包括密码定期修改频率、密码长度、密码复杂度、 密码过期时间等。 用友云针对生产数据及其附属设施的访问控制除去采用单点登录外，均强制采用双因素认证机制，例如像证书和一次性口令生成器。

强制密码策略如下：

- 最低长度:密码最低8位
- 错误允许数:密码输入错误最多3次，超过则锁定
- 有效天数:密码的最长可使用天数，默认无限制但会提示修改密码
- 生效日期:密码生效开始日期，账号激活后
- 是否强制修改:如果密码失效必须强制要求修改，并且密码不允许复用
- 有效期提示天数:密码提示修改的时提示的最大300天
- 旧密码记忆数:系统保存历史密码的最多5个
- 密码强度:密码由字母、数字或符号等组合的复杂度
- 密码存储:加密MD5存储，保障不会密码泄露
- 暴力破解和防撞库:通过二次验证保障，同时基于后端风控体系，实时监测账号破解、撞库与刷库等攻击行为并作出响应

5.2 访问控制

访问控制是网络安全防范和保护的主要核心策略，它的主要任务是保证网络资源不被非法使用和访问。访问控制规定了主体对客体访问的限制，并在身份识别的基础上，根据身份对提出资源访问的请求加以控制。它是对信息系统资源进行保护的重要措施，也是计算机系统最重要和最基础的安全机制。

用友云访问控制由权限管理体系实现， 权限管理体系以 RBAC 为核心的权限模型，支持功能、数据等多类权限资源，借助职责实现权限继承，简化、规范企业业务权限体系的规划，支持集中与分层的授权体系，支持内控与审计。

用友云权限管理特点：

- 严格的权限安全控制：支持基于数据实体（组织、档案、单据等）的数据权限控制，可以控制到每一个操作。并且支持所有者权限和主管权限。
- 租户间严格隔离：不同租户间数据完全隔离。
- 管理权与业务权分离：支持管理权与业务权互斥，管理人员不能直接操作业务
- 权限审计：多角度权限控制，支持权限审计，权限管理业务日志，保留完整审计信息。
- 关键业务权限：关键业务要求二次权限认证，以加强保护。

数据安全

信息安全主要目标之一是保护业务系统和应用程序的基础数据安全。依据数据安全生命周期，用友云从数据创建、存储、使用、共享、归档至销毁，使用了数据分级、数据加密等措施，保障了数据的保密性、完整性、可用性、真实性、授权、认证和不可抵赖性。

6.1 数据分级

用友云对所有用户和企业数据提供存储安全保护;根据存储与使用的数据，实施数据等级保护策略，按照数据价值和敏感度对数据进行等级划分，根据数据安全分级，有对应的保护策略和要求，对用户和企业数据进行安全存储与保护。

6.2 数据加密

用友云通过数据分类分级、数据加密和密钥管理为敏感数据提供可持续的信息保护，实现数据的灵活性、可靠性和可管理性；借助密钥管理中心和加解密产品实现数据安全保护和控制，将安全技术嵌入至整个数据安全生命周期中，以保障数据安全属性。

6.3 内容安全

用友云对上线的产品进行持续监控，特别是对动态发布的内容进行重点的防护，防止网页篡改、盗链、发布不符合国家法律法规的内容和言行等。用友云与多家领先的安全服务伙伴一起，借助大数据的技术，为用户的应用内容提供了一级防护能力。

6.4 数据访问权限

用友云数据权限遵循以下原则：

- 严谨的权限安全控制：支持基于数据实体的数据权限控制，支持所有者权限和主管权限
- 管理权与业务权分离：支持管理权与业务权互斥，管理人员不能直接操作和访问数据
- 数据权限审计：多角度权限控制，支持权限审计，权限管理业务日志，保留完整审计信息。
- 关键业务数据权限：关键业务要求二次权限认证，以加强保护。

6.5 数据安全审计

安全审计覆盖所有数据活动的详细跟踪记录，并进行实时的语境分析和行为过滤，从而实现对用户访问行为的主动控制，生成审计员所需要的信息。生成的结果报表使所有数据活动详细可见，如登录失败、权限升级、计划变更、非法访问、敏感数据访问等，这些行为是否合规一览无余并做到所有用户操作有踪可寻。

6.6 数据存储

用友云应用数据存储在阿里云中，阿里云的存储保护和备份机制在用友云产品中得到有效使用，为用户提供了安全存储服务。

用友云对数据进行全面性备份和关键数据备份，采用多备份、异地备份等方式，保障数据的存储安全。

6.7 数据销毁

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 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。

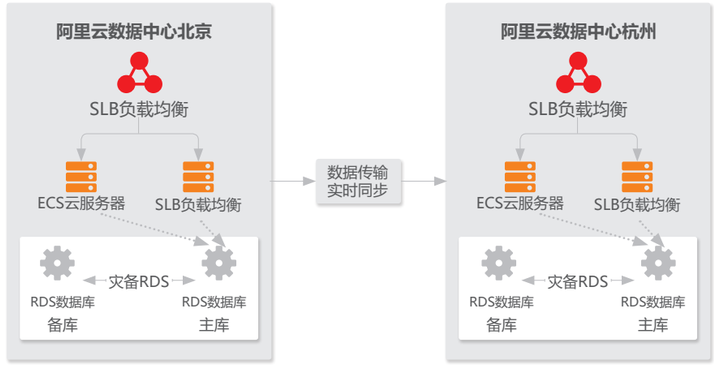
6.8 数据灾备及恢复

6.8.1 应急与灾备技术

用友云建立了本地应急系统及容灾系统，本地应急系统、容灾系统与生产系统相互配合共同保证整体业务连续性。

灾备采用双机房互备，数据库主备库热备，通过自动化运维平台， 实时故障检测，切换无需人工干预，保障核心应用不中断，系统恢复方便快捷，可进行自动伸缩扩容，在突发事件及自然灾害时，为用友云可用性及可持续服务提供保障能力。

用友云应急与灾备技术



资料来源：用友云，阿里云，2017

6.8.2 应急与灾难恢复管理

用友云建立了完备的应急响应及灾难恢复流程。应急响应组由安全专家、业务专家、技术专组成，制定了完备的应急响应制度及灾难恢复流程，并定期组织灾备演习和维护。

应急响应机制如下：

- 响应阶段

了解事件发生情况，技术人员判断事件类型，确认是否需要启用应急响应服务。

- 检测阶段

启用应急响应服务后，应急响应实施人员通过现场或非现场等方式进行信息收集，使用检测搜集流量信息、检测搜集系统信息及主机检测等多种技术手段对事件进行详细分析，并查找入侵痕迹。

最后确定安全事件类型，评估安全事件的影响。

- 抑制阶段

应急响应实施人员及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏，同时要与相关系统负责人沟通，确保抑制方法对涉及相关业务影响最小。

抑制阶段通常采用的技术手段如下：

1）确定受害系统的范围后，将被害系统和正常的系统进行隔离，断开或暂时关闭被攻击的系统，使攻击先彻底停止；

2）持续监视系统和网络活动，记录异常流量的远程IP、域名、端口；

3）停止或删除系统非正常帐号，隐藏帐号，更改口令，加强口令的安全级别；

4）挂起或结束未被授权的、可疑的应用程序和进程；

5）关闭存在的非法服务和不必要的服务；

6）使用反病毒软件或其他安全工具检查文件，扫描硬盘上所有的文件，隔离或清除病毒、木马、蠕虫、后门等可疑文件；

- 根除阶段

应急响应实施人员检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件整体安全解决方案，排除系统安全风险。

- 恢复阶段

应急响应实施人员恢复安全事件所涉及到的系统，并还原到正常状态，使业务能够正常进行，恢复工作应避免出现误操作导致数据的丢失。

基础架构安全

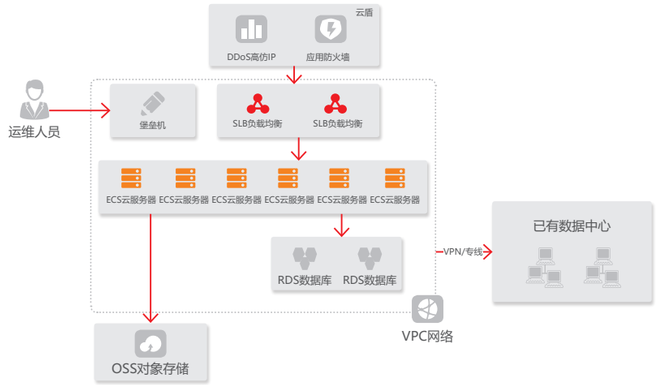
7.1 网络安全

为确保系统的网络访问安全，系统需要采用的安全手段主要有：访问控制（含 VLAN）、防火墙、线路备份、CA认证、VPN技术、入侵检测等。用友云使用了多种手段实现网络传输安全。 用友云还使用了阿里云高防IP抵御 DDoS攻击。

7.1.1 安全的网络架构

在网络架构方面，用友云基于阿里云专有网络 VPC（Virtual Private Cloud）构建隔离网络环境。

用友云安全网络架构



资料来源：用友云，阿里云，2017

7.1.2 网络访问控制

用友云采用了多层防御，以帮助保护网络边界面临的外部攻击。在公司网络中，只允许被授权的服务和协议传输，未经授权的数据包将被自动丢弃，用友云网络安全策略由以下组件组成：

- 控制网络流量和边界，使用行业标准的防火墙和 ACL 技术对网络进行强制隔离；
- 网络防火墙和ACL策略的管理包括变更管理、同行业审计和自动测试；
- 使用个人授权限制设备对网络的访问；
- 通过自定义的前端服务器定向所有外部流量的路由，可帮助检测和禁止恶意的请求；
- 建立内部流量汇聚点，帮助更好的监控；

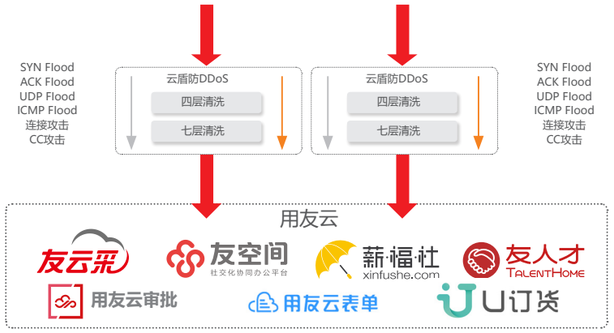
7.1.3 传输层安全

用友云为全站HTTPS，任何于云平台内的数据传输皆受256位密钥加密强度的保护，完全满足敏感数据加密传输需求。通过 HTTPS 协议，信息在用友云端到接受者计算机实现加密传输。

7.1.4 DDOS安全防御

用友云使用阿里云高防IP来抵御DDoS的攻击。阿里云成功防御全球最大DDoS攻击，能有效抵御所有各类基于网络层、传输层及应用层的DDoS攻击。

用友云DDos安全防御



资料来源：用友云，阿里云，2017

7.1.5 入侵检测

用友云使用阿里云态势感知进行入侵检测。借助大数据分析，对成千上万的网络日志等信息进行自动分析处理与深度挖掘，对网络的安全状态进行分析评价，快速感知到网络中的异常事件与整体安全态势。

7.2 主机安全

7.2.1 网络设备加固内容

云安全，主要包含两个方面的含义。第一是云计算自身的安全，也称为云计算安全，包括物理安全、网络安全、应用安全以及数据安全等方面，云计算安全是云计算技术健康可持续发展的基础；第二是使用云的形式提供和交付安全，也即云计算技术在安全领域的具体应用。

用友云安全主要是针对第一方面，同时用友云会和第二方面的云安全服务商进行紧密合作，共同为客户提供良好的安全服务。

用友云的网络设备安全加固包含但不限于以下内容：

- OS升级
- 帐号和口令管理
- 认证和授权策略调整
- 网络与服务加固
- 访问控制策略增强
- 通讯协议、路由协议加固
- 日志审核策略增强
- 加密管理加固
- 设备其他安全配置增强

7.2.2 主机操作系统加固内容

用友云的主机操作系统安全加固包含但不限于以下内容：

- 系统漏洞补丁管理
- 帐号和口令管理
- 认证、授权策略调整
- 网络与服务、进程和启动加固
- 文件系统权限增强
- 访问控制管理
- 通讯协议加固
- 日志审核功能增强
- 防DDOS攻击增强
- 其他安全配置增强

7.2.3 数据库加固内容

用友云的数据库安全加固包含但不限于以下内容：

- 漏洞补丁管理
- 帐号和口令管理
- 认证、授权策略调整
- 访问控制管理
- 通讯协议加固
- 日志审核功能增强
- 其他安全配置增强

7.2.4 中间件及常见网络服务加固内容

用友云的中间件及常见网络服务安全加固包含但不限于以下内容：

- 漏洞补丁管理
- 帐号和口令管理
- 认证、授权策略调整
- 通讯协议加固
- 日志审核功能增强
- 其他安全配置增强

7.3 移动终端安全

用友云会对所有登录的用户进行设备认证，如果该设备没有通过认证则不允许登录；可信设备认证需要经过账号或密码及验证码的认证。

对移动客户端的数据库进行了整库加密存储， 根据用户设备信息通过加密算法生成的唯一密钥，保护用户客户端存储的敏感信息不被攻击者非法获取，保障用户的隐私数据不被泄露。

物理安全

用友云采用阿里云提供基础设施服务，阿里云采用一系列措施来保障运行环境：

电力

为保障数据业务 7*24 持续运行，数据中心采用冗余的电力系统（交流和高压直流），主电源和备用电源具备相同的供电能力，且主电源发生故障后（如电压不足、断电、过压、或电压抖动），会由备用发电机和带有冗余机制的电池组对设备进行供电，保障数据中心在一段时间的持续运行能力，这是用友云数据中心一个关键的组成部分。

气候和温度

均采用空调（新风系统冷却或水冷系统冷却）保障服务器或其他设备在一个恒温的环境下运行，并对数据中心的温湿度进行精密电子监控，一旦发生告警立即采取对应措施。空调配电柜采用不同的双路电源模式，以应对其中一路市电电源发生故障后空调能正常接收供电。且在双路市电电源发生故障后，由柴油发电系统提供紧急电源，减少服务中断性的可能，以防止设备过热。

火灾检测及消防

自动火灾检测和灭火设备防止破坏计算机硬件。火灾探测系统的传感器位于数据中心的天花板和底板下面，利用热、烟雾和水传感器实现。在整个数据中心，也安装手动灭火器。数据中心接受火灾预防及灭火演练培训，包括如何使用灭火器。

用友云安全发展趋势

总体来看，云安全呈现以下三个重要发展趋势：

更加注重云平台的API价值

云平台提供的API是获取安全信息、推送安全策略的便捷渠道，安全产品开发要充分挖掘、利用这一资源，将云平台功能与安全功能整合，加强产品的自动化。

安全手段通过调用云平台的API，能够自动识别云中服务的变化，从而自动调整相应的安全防御策略。

安全可视化

随着云数据中心的到来，由于其规模要远远大于传统数据中心，因此对安全管理的可视化、联动提出了更高的挑战。

目前，大多数云平台的安全组策略均以表格形式展示，并不直观。安全服务需要通过收集云服务上的安全组策略信息，并进行分析整理，而后将租户的安全信息从安全域的角度用图形加以展示，便于管理员理解并进行后续操作。

云管端联动

由于大规模的云数据中心需要云安全管理产品更加注重安全状态的细粒度的、可视化的呈现以及策略快速部署能力，因而对不同安全产品之间的联动提出了更高需求。

目前部分安全企业可以做到对本地防火墙和云中安全组进行统一的策略管理，并以业务互联为需求，在网络发生变化时，协助用户对本地的、云中的安全策略进行自动化调整。

用友云会根据上述变化及时调整自己的策略，在安全治理、认证合规、云安全架构、产品/服务、内部流程保障、物理环境等各个环节，给客户和合作伙伴提供周密完整的安全保障，能保障用户享受到安全的用友云服务。

用友云将自己拥有多年安全经验与历练的云安全团队和技术过硬的云安全合作伙伴紧密团结在一起，共同为客户提供安全的服务和产品，为客户的管理运营、顺利发展保驾护航。