有孚云安全白皮书

2020 年 9 月 25 日

目　录

1 有孚云概述

上海有孚网络股份有限公司创立于 2001 年，公司总部位于上海，在北京、深圳设立有分支机构，是国内领先的企业级云计算运营商。有孚网络在全国拥有多个高等级云计算数据中心，通过丰富的网络和带宽资源，全力打造了云计算数据中心平台，以承载企业 IT 的核心基础设施，提供按需、实时、具备弹性与自动化的 IT 交付能力。在此基础上，2016 年研发具有自主知识产权的有孚云平台，帮助企业通过对存储、网络、安全以及 PaaS 平台的软件定义，成功实现了基于云计算形态的 IT 管理，帮助企业租户提升资源利用率、减少运营成本，同时实现了 IT 任务自动化、管理合规性、业务连续性，将各种规模的企业数据中心更加灵活高效的运用。

有孚云坚持以客户为中心，并致力于提供高于行业标准的 SLA，让企业能够以租用服务的方式建设其全部信息化架构，不仅可以打破信息化壁垒，消除数据孤岛，同时无需担心信息化平台的安全稳定，从而可以更专注于自身业务。

有孚云平台具备如下服务优势：

- **安全稳定：**云上业务承诺 99.95%的服务可用性，数据可靠性不低于 99.999999%。租户之间 100%的完全网络隔离，确保数据安全。
- **支持多混合架构：**供 yovolestack+虚拟化技术的多种云服务架构，支持多虚拟架构混合管理与网络互通，适应企业多元的应用场景。
- **管理灵活方便：**根据业务的发展趋势，企业客户可随时对云资源进行横向和纵向的自由伸缩管理，杜绝资源浪费。更提供开放 API，满足批量管理、自动化管理需求。

- **数据中心：**超过 15 年的数据服务经验，从资源到服务的全面监控和响应处理。依托高品质硬件资源和基础设施，为租户提供优质的带宽资源。
- **快速部署：**强大的技术团队，实现灵活的响应服务，计算、网络、存储均秒级响应，快速一站式解决所有架构部署问题，让企业客户身心专注业务发展。

安全保障体系是有孚云平台的重要组成部分，有孚云高度重视客户使用云服务的稳定性和可靠性，以及租户数据的隐私性和安全性。本白皮书主要介绍有孚云在安全与合规方面所遵循的策略和采用的方法，以求展现这些安全管控措施对客户的透明性。

2 责任共担模型

云安全包括保护云服务本身在 IaaS、PaaS 和 SaaS 等各类云服务以及云服务数据中心内部运维运营所需的技术资源，以确保各类应用和服务持续、高效、安全、稳定运行。云服务不同于传统 IDC，对云安全整体设计和实践更侧重于为租户提供完善的、多维度的、按需定制、组合的各种安全和隐私保护功能和配置，涵盖基础设施、平台、应用及数据安全等各个层面，同时进一步为租户提供各类可自主配置的高级安全选项。这些云安全服务需要通过深度嵌入各层云服务的安全特性、安全配置和安全管控来实现。

在云服务模式下，真正的安全不只是安全平台，更重要的是企业使用安全平台的人，有一个广为全球企业所遵循的总体原则是：“服务可以外包，但风险不能外包，责任更不能外包”。

安全责任	IaaS	PaaS	SaaS
数据安全	客户	客户	客户
客户端安全	客户	客户	客户 有孚云
身份和访问管理	客户	客户 有孚云	客户 有孚云
系统和支撑应用	客户	客户 有孚云	有孚云
网络控制	客户 有孚云	有孚云	有孚云
主机设施安全	客户 有孚云	有孚云	有孚云
物理安全	有孚云	有孚云	有孚云

在 SaaS 模式下，客户需承担自身数据安全，有孚云与客户分担客户端安全及身份访问管理责任，并承担其他安全责任。

在 PaaS 模式下，身份访问管理、系统及支撑应用的安全责任由客户和有孚云分担，客户负责自己开发和部署的应用及其运行环境、客户端、身份访问管理、数据的安全，其他安全由有孚云负责。

在 IaaS 模式下，网络和主机设施的安全责任由客户和有孚云分担。客户负责自己部署的支撑应用及操作系统、自己开发的应用及其运行环境、客户端、身份访问管理、数据的安全，对这些资源的操作、更新、配置的安全和可靠性负责。有孚云承担其他安全责任。

2.1 有孚云责任

有孚云作为云服务提供商（Cloud Service Provider，CSP），其安全责任在于保障 IaaS、PaaS 和 SaaS 各类各项云服务自身的安全。有孚云将基础设施安全与隐私保护视为重中之重。有孚云主要是研发并运维运营有孚云 IDC 物理基础设施、有孚云提供的各项服务，也包括各项服务内置的安全功能。有孚云应负责构建物理层、基础设施层、平台层、应用层、数据层的多维立体安全防护体系，并保障其运维运营安全。

有孚云首先务必保持从研发到运营的整个流程的安全质量基线，一方面确保各项云技术的安全开发、配置和部署，另一方面负责所提供云服务的运维运营安全。这些安全责任包括但不限于：适合 CSP 运维周期的快速发布和不影响租户服务的持续部署；不断优化云产品默认安全配置；适合云服务的漏洞管理机制；针对安全事件的快速发现、快速隔离、快速响应、快速恢复；对集成的第三方安全技术或服务本身的安全运维。

对租户数据，有孚云提供完整性、完整性、可用性、持久性、认证授权等方面的全面保护功能。但是，有孚云只是租户数据托管者，只有租户自身才对其数据拥有所有权和控制权。有孚云绝不允许运维运营人员在未经授权的情况下访问租户数据，例如只有在受到客户授权的情况，有孚云运维运营人员才可以进入租户的环境中提供技术支持和故障排除服务，并承诺只访问这一服务所必需范围内的租户数据。

此外，有孚云密切关注内外部合规要求的变化，切实遵从有孚云服务所必需的安全法律法规，并向租户分享合规实践，保持应有的透明度。

2.2 租户责任

租户的主要责任是在租用的有孚云基础设施与服务之上配置并运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对有孚云服务的定制配置和对租户自行部署的平台、应用等服务内部及相关安全防护措施的运维运营。租户所使用有孚云的各项服务最终决定租户的安全责任细节，具体到租户负责执行什么默认和定制的安全配置。有孚云只提供租户执行特定安全任务所需的所有资源、功能和性能，而租户需负责各项租户可控资源的安全配置工作。

大多数情况下，租户只需配置自己的账户对资源的逻辑访问控制并妥当保管账户凭证，而少数云服务则需要执行其他任务，才能达到应有的安全性，例如使用云数据库服务时，有孚云负责执行数据库整体安全配置，而租户还需设置租户账户和访问控制规则。

无论使用哪一项有孚云服务，租户始终是其数据的所有者和控制者。租户负责各项具体的数据安全配置，对其保密性、完整性、可用性、持久性进行有效保障。尤其是，租户应妥善设置和保管服务登录账户、密码密钥等登录和身份鉴别信息。

租户应负责对其自行部署在有孚云上的任何应用程序和实用程序进行安全管理。租户还负责对其自行部署于有孚云上且不属于有孚云提供的各项应用和服务所必需遵循的安全法律法规，并自行开展相应的安全评估。有孚云对于租户的违法违规业务、侵权行为采取自动化监控和接受举报相结合的措施，并有权采取强制措施以维护有孚云平台本身的安全性和有孚云自身的法律遵从性和声誉，相关内容详见《有孚云服务协议》有关违规处理的部分及有孚云《侵权投诉流程》。

3 组织与人员安全

3.1 安全架构

有孚云管理层成立了信息安全委员会，负责决策有孚云的重大信息安全问题，指引有孚云信息安全建设方向。

有孚云建立了专职的、专业的安全技术团队与标准合规团队，他们是有孚云的重要组成部分，其任务在于维护有孚云的网络安全防御体系、落实有孚云的信息安全体系和策略，并协助研发团队进行安全检测，提出安全建议，帮助整改问题。有孚云也会通过接受各种标准体系的第三方专业审核、审计，持续改善自身的信息安全体系。

有孚云配有研发团队，专门协助安全技术团队开发各类安全工具，逐步实现外购+自研的安全工具模式，实现快速部署，逐步自主可控。

3.2 人员安全

有孚云会在国家法律法规允许的情况下，在员工加入有孚云团队之前，验证应聘人员的教育情况、过往工作经验等背景信息，保证有孚云员工诚实可靠。

全体有孚云员工都必须接受持续的安全意识培训。在入职期间，新员工需要认同我们的行为准则，即强调我们作出的、为客户信息提供安全可靠保障的承诺。有孚云每年会多次开展针对所有员工的安全意识培训，并通过考试等方式，验证培训的有效性。根据具体职能方向，员工还会接受与安全领域特定方向相关的专业技能培训。如针对开发人员开展的安全编码培训，安全技术人员开展的安全技术培训。

4 租户服务安全

4.1 租户间隔离

租户间的资源隔离通过不同租户的账号加以隔离，通过 VPC 实现虚拟网络隔离。针对专有云租户，可通过指定物理节点实现物理隔离，云节点与租户企业内部之间的通信可通过专线或 VPN 隔离。

租户的账户由租户自行管理、维护、分配子账号、分配权限。有孚云仅在租户明确邮件授权的情况下，协助租户激活账户。

云服务客户执行对资源的敏感操作，如创建、删除资源，有孚云提供了双因子认证功能，需要密码和短信验证码双重认证，并支持通过日志记录操作。

4.2 租户与有孚云的隔离

有孚云严格限制员工的线上运行环境和客户资源的访问权限，员工只能访问云环境的资源以及云环境的性能数据。

仅在客户向客服邮箱明确授权的情况下，且经过有孚云管理层审批，才会协助租户操作其资源，并且操作过程也均通过云管平台的日志进行记录。

5 数据安全保障

5.1 隐私保护

有孚云充分考虑合规与安全风险，在有孚云产品与服务的开发生命周期中，数据安全的要求融入到了各个环节，以降低云产品在技术、流程上的安全风险和合规风险。

对于客户的敏感数据，尤其是个人隐私数据，有孚云将数据安全保护作为优

先考虑因素，强调：

- 权责一致原则：有孚云对因自身原因导致信息主体合法权益造成的损害承担责任；
- 目的明确原则：有孚云对收集到的客户数据，具有合法、正当、必要、明确的处理目的；
- 最少够用原则：只处理与信息主体相关且信息主体授权同意的目的所需的最少信息类型和数量，目的达成后有孚云根据约定删除个人信息；
- 授权同意原则：向信息主体明示信息处理目的、方式、范围、规则等，征求其授权同意，信息主体有权撤回同意；
- 公开透明原则：以明确、易懂和合理的方式公开处理信息的范围、目的、规则等，并接受外部监督。

关于有孚云的隐私保护相关措施，详见有孚云的隐私权政策。

5.2 数据保障

当租户通过负载均衡（Load Balancer）在互联网上传输数据时，有孚云提供基于 HTTPS 的加密功能，帮助强化公网上数据传输的安全性。云管平台提供 HTTPS 访问。

当租户提出需求，要导出其云平台中的数据时，需要租户提供纸质签字的授权书并扫描，基于授权书在内部系统上发起流程，由专人携硬盘或 U 盘，到机房中使用专门的中转机，在机器上就地加密后拷到硬盘上，再专人送达租户或租户现场来取。

有孚云向租户提供数据备份功能，租户可自行启用该功能，并自定义备份周

期、执行时间、保留策略等，备份功能将根据客户指定的备份策略执行数据备份，数据将自动备份到同一 AZ 下的专用备份集群中。系统级别提供快照备份功能，租户可将系统还原到备份的任意时间点。租户可自行选择备份的节点进行回滚，也可以自行导出备份数据，执行恢复测试。

对于备份的数据，客户可自行设置 1-100 天之间的任意保留时长，到期后自动清理，客户也可自行删除备份数据。

同一 region 下的 AZ 之间默认联通，不同 regiong 之间默认隔离，不同 AZ、region 之间，租户可自行配置，实现跨地域的灾备。

有孚云所有租户数据均采用三副本方式存储，不同副本位于不同硬件设备，采用不同的网络链路。云管平台采用三节点集群数据库，分钟级备份到异地机房。小范围异常时，可基于三副本机制自动进行恢复，租户的业务层面无感知。

如果租户停止使用有孚云，或过期欠费，有孚云不会立即删除租户数据，而会预留一个月的确认时间，并会通过人工与联系人确认之后，才会清除租户的数据。租户删除数据时，数据碎片被删除，且相应数据碎片的 Mapping 关系也被清除。

6 开发安全

有孚云在开发流程中运用了 DevOps 模式，并将安全融入到 DevOps 流程中：

- 人员培训：开发人员接受安全开发规范、安全意识方面的培训教育以提升开发人员的安全意识和安全能力；
- 安全需求分析：根据功能需求进行相应的安全需求分析，也相关技术框

架等进行安全评估；

- 安全开发：有孚云参考 OWASP 发布的安全规范，针对有孚云自身的开发环境，本地化为有孚云的安全编码规范，并通过内部晨会分享、培训等方式，帮助开发人员熟悉安全编码规范，在开发阶段规避已知的安全问题；
- 安全测试：在开发完成后，有孚云通过代码白盒扫描工具，发现代码中存在的安全问题，禁止问题代码带病合并。在发布上线前后，有孚云的安全团队会通过专业的安全扫描工具，以及人工渗透测试的方式，及时发现应用中存在的安全漏洞，第一时间予以进行修复；
- 发布评估：系统上线前开展的评估也包括安全评审，通过安全方面的评审才可以发布的线上环境。

7 运维安全

7.1 安全防护

有孚云在公网前端已经部署了一些安全防护工具，包括常规的 IPS、WAF 等，关键的服务器、宿主机通过 HIDS 进行完整性检查，检测外部攻击和篡改。

所有服务器、应用都开启了日志记录功能，日志统一收集至有孚云的大数据平台中进行分析，并长期保存留以追溯。所有检测工具在发现异常后邮件告警，由安全团队负责进行处理。

有孚云已借助补天平台建立了 SRC，白帽子可通过补天平台，或官方公布的邮箱，向有孚云反馈已发现的问题。

7.2 日常运维操作

有孚云资源的基础设施只开放了内网访问，无法通过互联网直连。当员工需要远程开展生产运维操作时，需要通过 VPN 连接，通过 CA 认证进行身份认证，通过 VPN 连接到内部的，堡垒机/跳板机，再通过 SSH 或 https 方式在内网访问和操作。

7.3 虚拟机加固

有孚云向租户提供的镜像已根据内部的加固要求进行加固，每次发布新的镜像时，会将系统补丁库更新到最新版本，并由安全技术团队进行安全扫描。

当有孚云的安全技术团队发现严重的安全漏洞时，将以安全预警的方式告知到所有客户，并立即为线上镜像模板打补丁。租户需自行对已投入使用的虚拟机的安全加固负责。

7.4 资产分类分级

为便于客户进行云资源的资产分类分级，有孚云支持客户自行定义资产的标签，可自行设置标签的名称和颜色，作为不同类型、不同级别资产的标识。同时，资产标签可绑定“生产环境”或“测试环境”，以区分不同环境。

7.5 介质管理

有孚云采用 OpenStack 的数据分片功能，当设备下线后再上线时，其中保存的数据为分片后的数据，无法直接被读取内容，并被 OpenStack 统一重写数据。

有孚云对服务器磁盘介质采用 7 次复写的方式进行回收再利用，对不再使用的介质采取物理销毁。

如果磁盘故障后下线，将不返回厂商，而是直接数据擦除，无法擦除的在配件库房中保存，当攒到一定数量时，由现场人员执行物理销毁，比如铁锤砸碎，并用水浸泡。

7.6 变更发布

有孚云依据 ISO/IEC 20000，建立了完整的变更流程。有孚云的各项变更，都会充分考虑对生产环境的影响，包括网络、主机、应用服务的变更，都会经过标准的变更管理流程。在变更前会经过测试环境下的模拟测试，对变更的影响进行充分评估，重大变更提交管理层审批。在经过严格论证后，才会执行变更。

有孚云的变更与发布，主要通过有孚云自研的蓝鲸 DevOps 平台，实现自动化发布部署，非自动发布部分，由人工通过堡垒机执行。

如果可能会影响到客户业务或导致云管平台不可用的变更，会通过网站公告、邮件或通过有孚云商务人员提前线下沟通等方式通知到租户。

7.7 日志监控

有孚云云管平台支持记录云服务客户各账号的操作日志，包括具体操作、资源名称、资源 ID、精确到账号的操作者信息、精确到分钟的操作时间。云管平台也提供监控功能，查看系统/网络异常信息。

有孚云在 IaaS 环境中部署了 NTP 时钟服务器，各台硬件服务器与 NTP 自动进行时钟同步，租户的虚拟机默认与硬件服务器同步时间，租户可以在无感知的情况下同步到统一的系统时钟。

有孚云云管平台提供资源分配、配额管理功能，租户可查看单个项目的资源分配和跨项目的资源分配。云管平台也支持对资源的监控功能，例如：针对云主

机的 CPU 和内存监控。

8 物理环境安全

有孚云在北京、上海分别设有机房，分别部署了两个 AZ。机房选址时已经选择了不易发生洪水、地震等自然灾害的低风险区域。

有孚云团队有超过 15 年的机房维护经验，形成了一系列的 IDC 应急预案，如火灾、台风汛期、爆炸等。机房周边已设置了物理围墙和电子围栏，物理安全由专门的安保部门负责，日常门卫值守，定期进行周边巡逻。7*24 小时交替值班，定期对网络和动力进行巡检。

机房配有四路供电，并通过 UPS，柴油发电机等保障异常情况下的稳定供电。机房内空调四主一备，并在六楼设有冷冻柜，日常备有冰块，保证机房内冷起供应。机房内配有水泵可直接抽走空调的冷凝水，防止空调漏水影响设备。

为预防火灾，机房外有专门的消防控制柜，机房内设置有烟感探头、温感探头，并配有气体灭火装置。

人员进出均需要进行登记，仅工作人员有门禁卡，申请门禁权限需要安保部门领导审核。人员进出需要由工作人员陪同，刷卡进出。机柜均配锁，钥匙由值班人员管理。机房内通过固定角度的视频监控，实现机房全覆盖。

机房以半年为周期，安排需要执行的演练，并按照计划执行演练，熟悉应急预案，在演练后进行总结和回顾，发现演练中的潜在问题，不断优化和改进。

9 信息安全事件响应

有孚云通过对外公示 400 电话（400 720 0606），以及有孚云平台服务邮

箱（service@yovole.com），7*24 小时响应租户的信息安全事件咨询、安全报障等。针对 VIP 客户，开放客户经理的直线咨询报障通道。

有孚云值班团队在 SLA 的约定时间内，响应租户的报障，转派专业团队进行处理，并由首问人员负责跟进事件的处理进度，按需主动与报障客户交流处理进展，通报处理结果。

当信息安全事件影响到客户时，有孚云也会及时通过线上公告、邮件通知、线下联系等方式，及时告知受影响的客户事件的影响范围、事件级别、有孚云响应团队的联系方式，以及客户可采取的临时补救措施。

租户如想获得与其相关的信息安全事件的记录，可通过 400 电话或服务邮箱向有孚云申请，有孚云将严格验证租户身份，筛选数据记录，确保其他租户信息不泄露的前提下，可向申请人提供。

10 安全合规

目前为止，有孚云已经通过了多项国内外权威机构的认证和检查，有孚云在向租户提供安全、合规的云计算服务体验的同时，也与租户积极分享有孚云的合规实践。

权威认证不仅证明了有孚云在信息安全、隐私保护、业务连续性等方面的能力，当租户也期望通过类似认证时，通过证明使用了有孚云的能力，展示有孚云的认证结果，还能够减少自身通过认证审核的成本，更快速、便捷地通过认证。

10.1 通过多项 ISO 认证

ISO/IEC 27001 是被广泛采用的全球安全标准，有孚云通过了 ISO/IEC 27001 认证，体现了有孚云对安全的承诺，表明有孚云建立了系统化的、持续

的方法来管理信息安全风险，以保障自身和客户信息的完整性、完整性和可用性。

ISO/IEC 27018 是 ISO 发布的聚焦于云上个人信息保护的一套标准，该标准基于 ISO/IEC 27002 和 ISO 29100，细化出了针对云和个人信息保护的安全与隐私保护要求，从而更好地保护租户的个人信息安全。

CSA-STAR 是云安全联盟和英国标准协会（BSI）在 ISO/IEC 27001 的基础上，开发出的针对云安全控制矩阵（CCM）的成熟度评估模型。CSA-STAR 将云企业的云安全成熟度分为了金银铜牌三个级别，有孚云已经获得了 CSA-STAR 的金牌认证。

ISO/IEC 9001 是世界范围内最广泛采纳的标准，有孚云通过了 ISO/IEC 9001 体系认证，体现了有孚云有能力、有信心去持续地提供质量稳定的云服务。

ISO/IEC 20000 是 IT 服务管理体系，有孚云通过了 ISO/IEC 20000 的认证，意味着有孚云已经建立了标准化的服务管理体系，能够以国际认可的服务流程，为有孚云的租户提供规范化的服务，在提高服务效率的同时降低了租户和有孚云的风险。

ISO 22301 是业务连续性管理体系，有孚云通过了 ISO 22301 的认证，意味着即使遇到不可抗力导致有孚云中断，有孚云也能够保证在与租户约定的时间范围内重新启动业务，为租户提供服务，保证云业务的连续。

10.2 通过信息安全等级保护认证

有孚网络是数据中心运营商中唯一通过此认证的企业（数据中心基础架构认证），获得该二级等保认证，说明使用有孚网络的数据中心服务的企业，可直接申报公安部信息安全等级三级认证。

10.3 首批通过“可信云服务认证”

获得可信云认证说明有孚网络云服务从服务协议（SLA）标准性、数据存储可靠性、租户数据私密性、业务可用性、功能完备性、运维系统完善性等多方面达到国内顶级云服务评测系统的认证标准。