见知安全白皮书 V4.0

2023 年 02 月 01 日

目录

一、安全责任总述

见知是一家创新型人工智能数据分析公司，专注于企业财务和资金管理方向的数据挖掘和应用。团队成员平均拥有十数年的各业务领域经验，包括企业经营管理、财务和资金管理、机器学习等人工智能技术、企业级 IT 技术开发和实施等。

公司以帮助企业实现智能化经营为愿景，以专业的数据管理经验为基础，通过人工智能等技术手段，为企业提供智能的财资管理解决方案。公司现有产品包括资金管理系统和流水尽调系统等企业应用系统，其中资金管理系统含银企直连，流水数据智能分类、资金风险自动预警、滚动预测、智能对账、发票自助查询、经营性现金流数据分析等，尽调系统含流水上传，余额分析，收支分析，关联方分析等，利用多维度精准的数据来支持多层次的企业经营管理和尽调的需求。

作为精细化现金流管理服务的先行者，见知同样也将服务安全、数据安全和业务流程安全视为企业的生命线。公司竭力在为客户带来专业化、高智能产品和服务的同时保障客户的数据和隐私安全。

根据见知产品的类型，白皮书将分为 SaaS 产品（搭建在公有云平台上的软件服务）和客户本地部署产品（搭建在客户内部局域网中的产品）进行阐述。

1、 见知 SaaS 服务产品安全责任总述

作为 SaaS 服务的提供方，见知主要涉及如下五大块的安全责任范畴：

1）数据存放及基础设施安全：指见知 SaaS 服务所依托的硬件的设施安

全，主要包括其物理和基础架构的安全和主机安全等。

2）功能运作及应用安全：指为保障见知的 SaaS 服务能够持续不间断运作的相关应用系统的安全管理，包括系统防御等。

3）用户使用及终端安全：指使用见知 SaaS 服务相关的终端或移动终端的安全管理，包括终端的硬件、系统、登录等相关的安全控制。

4）数据保护及用户隐私安全：指客户数据在见知 SaaS 服务系统中受到的保护措施，包括数据的分级与加密，以及用户使用见知服务时所提供的个人信息及隐私安全。

5）数据访问及控制权限管理：指对各种数据的访问、运维和使用流程管理，主要包括身份验证、权限管理和日志的生成与审计等。

2、 见知客户本地部署产品安全责任总述

作为客户本地部署产品的提供方，见知主要涉及如下两条安全责任：

1）产品访问管理功能的完善性：在客户本地部署的产品同样具有账号权限的设置功能及完善的访问日志追踪、审计功能，一切访问权限均可以由管理员账号进行管理控制。

2）产品数据传输功能的封闭性：见知承诺，只要用户不私下修改程序代码，在客户本地部署的产品将不包含向外网传输数据的功能，包括但不限于对账单数据和用户上传的附件。

3）免责声明：见知客户本地部署产品相关问题的免责声明。

二、见知 SaaS 服务产品安全责任

1、 基础设施及数据存放安全

1.1、基础设施安全

见知使用的平台满足 GB50174《电子信息机房设计规范》A 类和 TIA942《数据中心机房通信基础设施标准》中 T3+标准，一个服务周期内服务可用性不低于 99.99%。

另外，为避免极小可能性的云服务不可用，见知采用主从多地域服务部署和数据备份，当单地服务不可用时迅速切换至备用服务，竭力保证服务的 7*24 小时可用。

1.2、数据存放安全

见知采用可靠的服务器和文件系统进行数据的备份，保证数据存放的安全可靠。

见知的数据库每 12 小时创建镜像进行完全备份，常规保存 60 天的镜像，共 120 个镜像点，保证用户可以回退至过去 60 天中的任意镜像点。数据操作日志则是每小时备份，随时防备突发灾害，最大限度避免客户数据资产的损失。用户上传的附件会自动以多副本冗余方式存储，避免数据的单点故障风险，提供高达 99.999999999%的数据可靠性。

另外，存放于服务器上的客户数据资产已经过见知的数据安全保护系统进行加密和脱敏，这部分内容具体参见后文“数据保护及用户隐私安全”模块阐述。

2、 功能运作及应用安全

为使 SaaS 服务能在安全的环境下运作、不被恶意访问攻破或是影响服务质量，见知总共构建了三道防御体系。每道防御体系又根据具体情况分为若干道防御机制。

第一层防御体系构建于见知 SaaS 服务使用的平台。平台使用了先进的安全防护系统，应用网络防火墙并进行定期的漏洞扫描，有效抵御 SQL 注入、木马上传、DDoS 攻击等恶意访问。

第二层防御体系构建于见知在其所处的平台中所划定的一个片区。即便恶意软件攻破了平台的防御机制，其也没有权限访问见知在平台中使用的、与其他功能区域隔离的独立片区。

第三层防御体系构建于见知在使用的服务片区中单独为 SaaS 服务和数据存放所使用的空间，该部分进行了各种行为检测和数据保护，即便恶意软件攻破了平台的防御、进入了见知的私有空间，也无法轻易访问客户的服务和数据。

此外，见知还采用了多种安全手段如黑产情报收集、反代理 IP 保护、防刷引擎保护和风险分级验证等从多维度进行客户身份验证，及时有效地识别出批量注册、盗号登录和爬虫等多种恶意交互行为，防止正常用户的服务资源受到影响，保障业务的顺利进行。

这些防御机制使见知有充足的时间应对和防御任何攻击行为、发现潜在风险行为，从而避免了客户数据资产泄露和服务瘫痪，保障了服务的持续可靠性、可用性和安全性。

3、 用户使用及终端安全

见知为客户提供终端设备类型识别、登录保护等终端安全保护能力，对异常、不安全的终端访问行为（如异地登录等）进行提示、警告或是拒绝，同时提示用户进行登陆限制抑或是安全机制升级。

同时，见知还提供终端授权管理功能，使得用户在使用非可信设备登陆账户时必须经由用户本人或是管理员的授权、二次验证（譬如手机辅助验证）。这种机制可以有效防止网络黑客进行账户的暴力破解和撞库。每个用户账户的终端授权可随时由该用户或是管理员取消。

客户方则应合理地运用见知提供的终端安全能力来获得相应的保护。

4、 数据保护及用户隐私安全

4.1、数据分级保护

见知根据《(GB/T 22239-2019)信息安全技术信息系统安全等级保护定级指南》（下称《等保 2.0》），对不同客户、不同数据适用的信息安全等级进行分级，根据对应的标准采取相应的措施。

此外，见知也可以根据客户的要求采取标准以上的安全性处理，但需要注意的是，这可能会造成客户访问、使用和下载数据时速度和性能下降。

4.2、数据保护措施

见知不会触碰或知悉客户数据，客户数据被见知内部定义为绝密级别。没有客户授权、内部审批及相应的许可和支持，任何见知的员工无权访问。为此，见

知采取了以下一系列数据保护措施，以确保客户对数据保护方面的需求得到满足。

4.2.1、数据完整性

见知依据《等保 2.0》对数据完整性管理的要求，采用 CRC64 算法定期对存储介质中的数据进行完整性校验，同时对数据传输过程中的数据完整性进行校验，保证了客户存储、传输数据的可靠性。

见知还可以提供数字签名，用于数据完整性的校验和建立防抵赖机制。对于使用了这项服务的客户，见知将会要求使用管理员 / 业务员的证书对其产生的数据做签名，证明数据创建者和数据的产生单位。一切未经签名的数据和文件均无法上传或录入。

4.2.2、数据安全性

见知依据《等保 2.0》对数据安全性管理的要求，采取了一系列的完善措施防止数据通讯被监听、劫持和篡改，确保数据存储和传输过程中的安全。

见知为用户访问（包括读取和上传）数据提供了 SSL/TLS 协议和 SSL 证书服务来实现网页的 HTTPS 化，保证数据传输的安全。见知所有产品都为客户提供了支持 HTTPS 的访问点，并提供高达 256 位密钥的传输加密强度，满足敏感数据加密传输需求。

在数据存储中，见知使用 AES 加密算法并提供 256 位密钥的存储加密强度，满足敏感数据的加密存储需求。存储加密中密钥层次会至少分为两层，并通过信封加密的机制实现对数据的加密：第一层为客户主密钥，第二层为数据密钥。其中主秘钥为数据秘钥进行加解密操作和保护，数据秘钥为真实数据进行加解密操作和保护。

在信封加密机制中，见知为客户提供了密钥管理服务，实施强逻辑和物理安全控制以防止未经授权的访问。在整个信封加密过程中，主密钥的明文不会在秘钥管理服务之外进行存储和使用。同时，数据密钥明文也永远不会以明文形式存储在任何永久介质上。

在存储加密功能中，见知支持用户自选，或在秘钥管理服务中生成秘钥作为主密钥对数据进行加密，并允许客户对主秘钥的生命周期进行全程管理。需要强调的是，用户自选的主秘钥是用户的资产，见知必须得到用户的授权才可以使用其对数据进行加解密操作。用户也可以随时取消相对应的主秘钥授权，达到对数据加解密操作的可控。

4.2.3、数据脱敏

为保护数据隐私，见知提供 Hash、加密、遮盖、替换、洗牌、变换等脱敏算法，确保脱敏后的数据能够适应各种业务场景。

见知竭力满足客户对数据脱敏的需求，同时严格保证不脱敏数据边界范围，使客户可以在保证安全的前提下，低成本、高效率地完成各种业务需求以及与见知方面的合作。

4.2.4、数据生命周期

客户拥有数据的唯一所有权，并可以在具备权限的情况下，在任何时间完全管理其数据资产的完整生命周期，包括上传、使用、下载和销毁。当客户销毁数据时，见知将自动为其备份销毁的数据并保留 30 天，或是保存到客户所购买的服务到期为止。保存时长可以根据需求改变，包括拒绝备份。

但需要注意的是，拒绝备份或当备份的数据到期后，客户数据将无法恢复。

在客户确认终止或不再为客户提供服务后，见知会及时、彻底地删除客户数据资产，或根据相关协议要求返还其数据资产。同时需要注意的是，一旦上述流程执行完毕，见知将不再对客户的数据资产负责。

4.2.5、个人信息保护

长期以来，见知坚持致力于保护每位客户的个人信息，保证客户对所有提供给见知的个人信息拥有所有权和控制权。

见知通过权威机构的认证，证明了个人信息保护能力和数据安全保护能力，详细信息请见 ISO 27001 等。见知将持续建设整体的个人信息保护管理体系，并进一步投入力量建设见知作为数据处理者的角色时相应的产品与服务中的个人信息保护能力。客户若有任何隐私相关的问题都可以通过见知的在线或电话客服进行反馈。

5、 数据访问及权限管理

5.1、客户访问与权限管理

5.1.1、访问身份验证

见知在各项需要身份认证的业务情境中，为客户提供了完善的身份认证机制，主要包括：

a) 账号密码验证：见知提供多账号管理功能，并配合可选的强密码安全策略和密码错误次数限制，以防范暴力破解等攻击行为。

b) 二次验证：见知可以提供动态验证登录（如短信验证码登录、微信二维

码验证），确保执行敏感操作时（如删除数据时）的账号安全。

5.1.2、管理权限分级访问

见知各产品均有独立的访问控制权限的管理和鉴别功能，企业可以针对每项服务、每条数据及表单设置对应的可见范围、可见用户，访问控制的精度能细化到个人或部门。其他任何管理员未授权的账号在非授权情况下无法访问目标数据或文件。

同时，见知还提供了网页面水印功能、PDF 数据导出水印功能，截图上带有登录的用户名称、其所属集团及当前时间信息。一旦发现截图流出，将截图经由 Fourier 变换等特殊处理后，便可显示截图上的水印。

另外，该功能为了防止被篡改，相关代码已被设置为被改动时自动填补并向管理员发送邮件等告警提示，使得管理员可以及时确认情况。

但需要注意的是，管理员应当小心地保管、分发、使用和收回账号与权限，见知无法在身份验证通过的情况下，对管理员授予权限的账户造成的结果做出任何客户未授权的、或是超出产品功能范围的干涉与处理。

5.1.3、管理员登录安全

见知账号与访问安全体系依托身份验证和访问权限控制，对管理员账户禁用弱口令。对其他账户，见知将结合终端安全系统非法登录行为进行监控并向管理员账户报警，发现攻击行为后尝试阻止登录行为。

管理员账号还支持与微信进行绑定，绑定后管理员账号会在微信上收到本账号的登录提醒，以及该账号所管辖的其他账号的疑似非法登录提醒，此时管理员可及时确认情况，或是上线修改密码。

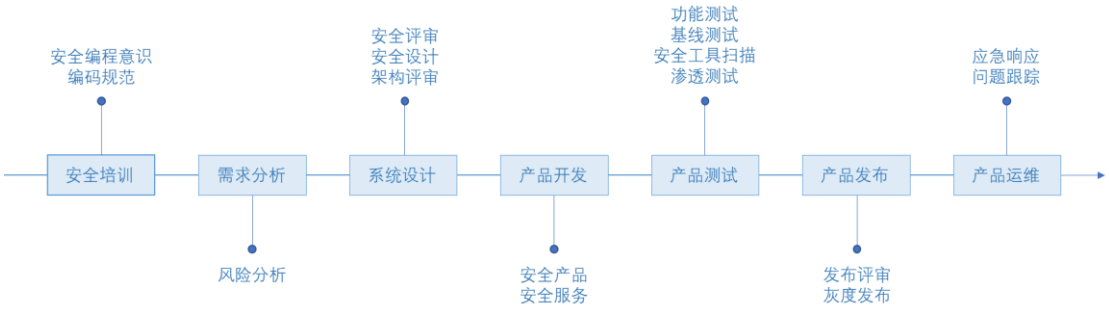
5.2、服务运营与权限管理

5.2.1、安全开发周期

见知在项目开发流程中引入了 SDL（软件安全开发周期）。在为客户提供的每一个产品和每一项服务的背后，见知着力将 ISO/IEC 20000 信息技术服务管理标准和 ISO/IEC 9001 质量管理体系标准融入到产品 SDL 安全开发流程中。

在产品开发各个阶段中，见知竭力消除信息安全和隐私中存在的问题，确保所有的产品在其生命周期内均能获得足够的安全管控与评估。

我们的软件生命周期主要由安全培训、需求分析、系统设计、产品开发、产



 # 软件安全开发周期示意图

品测试、产品交付、产品运维等不同环节几个部分组成：

安全培训：针对开发人员推广安全编程意识，我们严格要求相关人员遵循安全编码的规范；

需求分析：针对业务内容、业务流程、技术框架，我们有专业的人才进行全面的沟通，寻找安全嵌入的最优方式；

系统设计：针对系统设计所包含的可能威胁，我们有专业的人才进行建模并对采用的架构进行安全技术评估；

产品开发：在开发过程中，我们提供自行设计的各种安全开发组件与开发环

境供研发人员使用；

产品测试：针对服务的漏洞，我们将进行规范化的渗透测试和代码审计；

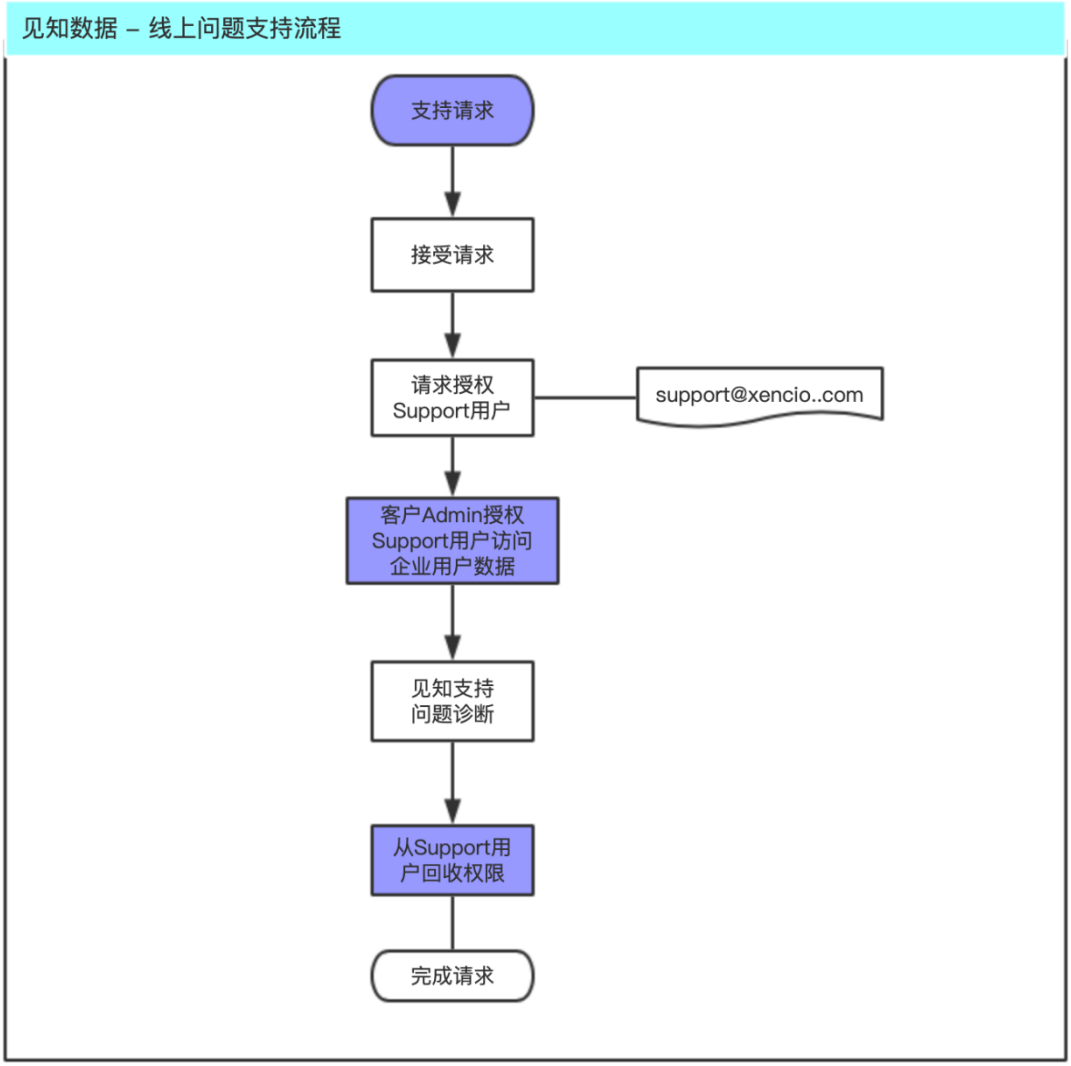
产品发布：经过测试和技术专家的全面评估，以及信息安全部门的最后检查确认后，我们的系统才能发布到线上环境供客户使用,最大限度防止携带漏洞的产品和服务在客户的生产环境中运行。

产品运维：对于客户提出和见知自行检测到的的各项运维请求和问题反馈，见知将 24 小时采取快速、规范、有效的应对，并严格控制解决问题的时间窗口。

5.2.2、生产与运维权限管理

见知每年都会处理大量的运维请求，并通过内部运维管理机制严格控制时间窗口，使得所有运维请求均能在指定的时间内完成，从而持续为客户提供无风险、不间断的业务运维支撑。

在客户所订购的任何见知提供的服务中，客户拥有的业务数据在见知内部均受到最高级别的保护。只有当客户提出需求、认可并授权时，我们才会安排专人在客户确认能够进行监控的情况下（如远程线上的方式）来访问客户数据，否则任何人无权访问客户的数据库。



具体来说，见知对于客户数据的访问，将遵循如下流程：

同时，见知员工在运维的过程中，同样处于截图、PDF 数据导出水印功能的作用范围之内。关于截图水印功能，详见 5.1.2 节管理权限分级访问。

此外，见知根据运维请求的重要/紧急程度、变更范围等属性进行影响等级划分。针对影响较大的运维变更操作，见知将及时通过官网、微信、短信或邮件等渠道发布变更通告，并向可能受到影响的客户发出变更通知，以便客户能更好的协调业务资源，确保各项安全事宜。

我们还会与客户签署保密协议，确保见知的相关人员不会以任何形式泄露客

户数据和隐私。

见知团队的每一位成员在加入前，都将接受严苛的背景调查和能力评价，只有满足所有必要条件的候选人才能正式成为见知的员工。见知还会与每一位员工签署具有法律效力的保密协议，并在员工调职、离职后及时收回相关权限。

5.2.3、访问、操作行为的监控与审计

见知的生产环境已全面部署堡垒机并将见知后端系统组件的管理员账号权限进行集中管控。运营管理团队人员仅能使用堡垒机新赋予的账号并通过二次身份校验进行登录，自动获得适当的系统操作权限，并适用最小权限原则。

见知所有后台、运维的操作记录均由日志平台集中加密存储并每小时备份，由见知内部的审计团队定期对日志信息进行审核，并随时接受由客户指派的外部审计。

所有涉及客户数据的导出、增删均有完整的操作日志可以查询，操作人、操作时间、操作结果一并记录在案。客户在使用见知产品和服务的过程中，如有发现异常操作记录，可以及时发现并处理相关责任人，或通过见知的在线或电话客服进行咨询或寻求技术支持。

涉及客户数据的操作日志只有客户的管理员账户有权限进行主动删除。日志默认保留 120 天，客户也可以修改为不低于 120 天的保留天数。

在接受客户的授权进行服务的运维和数据访问后，见知团队也不允许以任何方式保存数据，包括但不限于截图、屏幕录制、连接外部存储设备或是使用任何网络存储软件，并提供完备的操作日志记录以供审计。

三、见知客户本地部署产品安全责任

1、 产品访问管理功能的完善性

客户本地部署的产品同样具有账号权限的设置功能及访问日志追踪、审计功能，一切访问权限均可以由管理员账号自行管理控制。 同时，若有疑似不正当的操作，系统将会向管理员终端发布警告。详细内容请参见在 SaaS 产品相关内容中的"客户访问与权限管理"章节与"服务运营与权限管理"章节。

2、 产品数据传输功能的封闭性

只要客户不私下修改程序代码，在客户本地部署的产品将不包含向外网传输数据的功能，包括但不限于对账单数据和用户上传的附件。

3、 免责声明

见知在交付客户本地部署产品时保证上述功能的完备性。同时，见知向客户提供的服务终止前，承诺在客户授权的情况下提供与上述功能相关的各种技术支持和必要的软件更新。但是在产品的使用过程中，客户需要在充分理解产品各项功能的前提下对产品进行恰当的使用和设备的管理，对于不明确的地方应寻求与见知方面的沟通，避免操作不当而造成的损失。

对于因客户的设备损坏、客户操作不当等客户方原因造成的客户损失，见知只能竭力在产品功能的层面上、在获取了所必要信息以及在满足法律法规和合同条款的情况下协助客户解决问题，但无法做出这之上的协助。

在终止服务前，见知建议客户应根据数据的重要性和敏感程度，定期对数据进行额外备份，同时慎重地进行数据的更改、清理、销毁或者其他敏感操作。

在客户终止服务、或是非法使用见知产品后，见知将不对产品提供任何保障，并不会对客户此后的任何损失承担赔偿和责任。

四、见知已经获得的行业安全认证

目前，见知已获 GB/T 22080-2016/ISO/IEC 27001:2013 的安全管理体系认证，对应提供的 SaaS 云服务，也通过了 ISO/IEC 27017:2015 云服务器信息安全管理体系的认证，并持续遵守相关法律规定的要求进行生产活动。