CAICT 中国信通院 HUAWEI

集智 蓝皮报告

金融云安全体系建设与实践研究报告

（2022 年）

中国信息通信研究院泰尔终端实验室

华为云计算技术有限公司

2022年11月

版权声明

前　言

随着金融科技的发展，云服务市场的产品不断更新迭代，公有云、私有云、混合云等多种云服务架构逐渐进入金融厂商的选择视野，越来越多的金融厂商逐渐将业务系统迁移上云，实现更便捷的系统管理和升级迭代。与传统 IT 技术相比，云计算架构具有迭代创新方面的独有优势，有力推动了产业金融、供应链金融、数字货币、智能投研等创新应用的发展。

金融上云已成行业大势，安全是对金融云的基础要求。金融云作为金融科技重要的基础设施之一，其支撑的金融业务多关系到国计民生，所以金融云安全是整个信息领域的安全高地。近期，央行发布的《金融科技发展规划（2022-2025 年）》重点围绕数字化转型建设，再次强调了金融上云、数据基础建设以及数据安全的重要性。

本研究报告通过回溯金融云安全体系的历史变迁，详细阐述了金融云安全变化趋势、金融安全事件类型、国内宏观调控政策、头部金融厂商的安全实践等；通过聚焦金融云安全发展现状，详细阐述了宏观环境、金融安全新生问题的挑战，金融厂商应对措施；通过展望金融云安全未来发展，详细阐述了新科技与安全伦理、新监管与业务发展的相互作用；最后，面对金融云安全的不断发展变化，提出了产业界应主动预判、拥抱、谋求变化的倡议。本研究报告主要面向以下几类读者：

金融企业相关人员：金融企业或组织内信息安全相关的决策人员、方案规划和实施人员、安全管理人员、技术培训人员。帮助其更加深

入全面地了解在企业或组织的数字化转型过程中正在和将要面对的金融云安全威胁、风险和合规性要求以及行业内场景化治理实践，从而更积极主动地筹划和开展系统化的金融云安全评估，确保企业或组织能够有效应对新形势下的安全挑战。

金融云服务提供商相关人员：金融云安全行业的方案及产品策划人员、安全咨询服务人员及项目实施人员。通过研究报告中对安全体系框架、技术应用与实践案例等内容的介绍，使其更好的为产品开展方案编制、为实施服务工作提供启迪参考。

金融云安全领域其他相关读者：此外，本研究报告也适用于关注金融云安全领域的政府机构、研究机构、媒体等。

目 录

图 目 录

表 目 录

一、回溯过去——变迁

近年来，我国金融行业信息化建设快速发展，助力金融机构不断提升业务效率、降低运营成本，已成为数字化建设的重要应用领域之一。金融信息系统需要实时处理、分析海量的信息数据，云计算因具备强大数据运算与同步调度能力，在提供弹性的信息基础资源方面具备天然优势，“金融云”的概念应运而生。

金融云是指面向银行、券商、保险等金融机构的业务需求，集互联网、行业解决方案、弹性 IT 资源为一体的云计算服务。具体而言，是指金融机构通过利用云计算技术与服务，提升运算能力、重组数据价值，为客户提供更高水平的金融服务。本章节对金融云安全体系分别从技术发展演进、国内外通用云安全合规、国内金融行业云安全要求三个角度进行了梳理和阐述，并介绍了当前金融安全事件类型、国内宏观调控政策、头部金融厂商的安全实践等。

（一）金融云安全体系的历史沿袭

1.金融云安全趋势

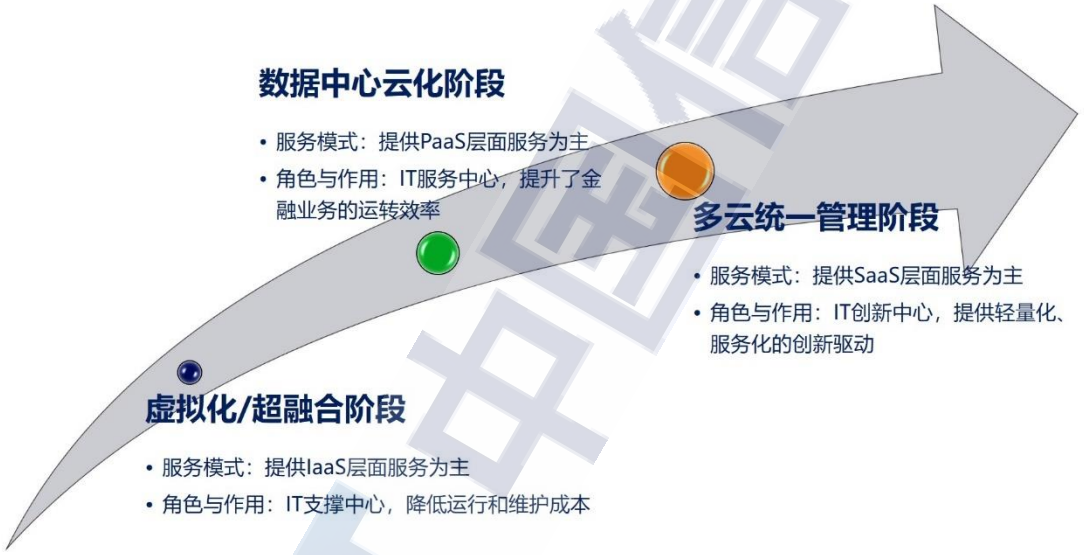
从金融云的发展演进路径来看可以分为三个主要阶段。

虚拟化/超融合阶段：该阶段金融云通过虚拟化/超融合架构实现承载部分金融业务系统，主要用于提高资源利用率，并实现统一管理和动态维护。在此阶段，金融云作为 IT 支撑中心以提供 IaaS 层面服务为主，有效帮助金融厂商降低运行和维护成本。

数据中心云化阶段：该阶段金融云提供了对金融业务应用完整生命周期的支撑，逐步实现了完整的数据中心云化，并将中间件能力深

入融合云平台，保证业务的高可靠和智能化。在此阶段，金融云作为 IT 服务中心以提供如容器服务、数据库服务为代表的 PaaS 层面服务为主，有效提升了金融业务的运转效率。

多云统一管理阶段：该阶段金融云通过混合云或多云架构的统一管理，直接面向金融客户提供业务支撑。在此阶段，金融云作为 IT 创新中心以提供软件为代表的 SaaS 层面服务为主，向金融业务提供轻量化、服务化的创新驱动。

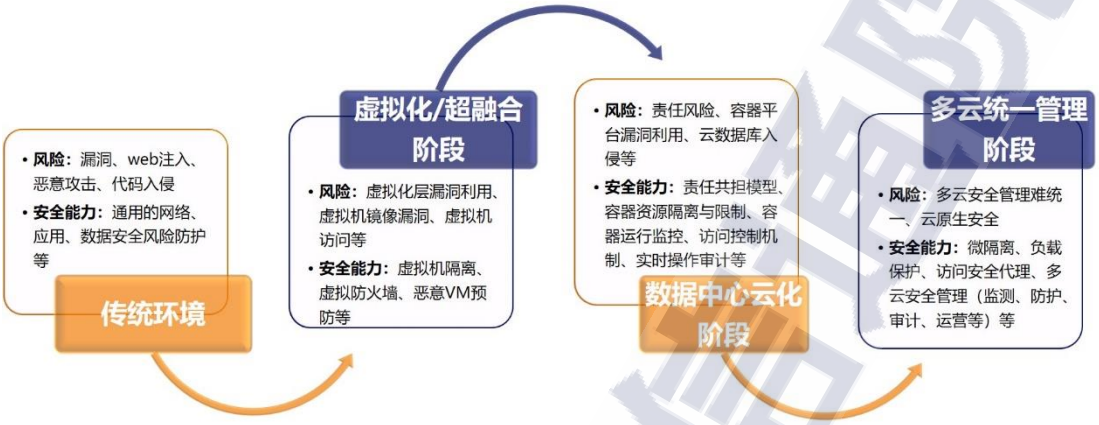


来源：中国信息通信研究院整理

图 1 金融云的发展演进路径

随着金融云的发展演进，金融云安全风险也随之发生变化。传统金融信息系统环境中更多的是已部署的应用层数据存在风险，随着金融业务云化的不断深入，虚拟化层面的漏洞攻击、海量数据安全风险、云服务权责分离、多云安全、云原生安全等都成为新形势下金融云安全的重点关注点。金融云安全风险的变化也促进了金融云安全技术的不断发展，金融云安全技术发展路径包括安全能力的虚拟化、云化、

云原生等，衍生了如多云管理平台、云上安全开发平台、多云安全管理、云原生安全等安全产品和防护能力。



来源：中国信息通信研究院整理

图 2 金融云风险特征发展趋势

2.金融云通用安全合规

在 2018 年金融云行业标准发布之前，金融云主要需符合通用的国际、国内云安全规范要求。其中，国内的云安全审查、网络安全等保 2.0 体系目前仍然是金融云必须满足的合规要求。

表 1 金融云通用安全规范与合规

时间	发布部门	发布文件	安全要求
1999 年	国际标准化组织 ISO	《ISO 15408信息技术安全技术-IT安全评估准则》	提供了通用的信息技术产品和系统安全功能要求和安全保证要求，并在保证要求的基础上提供衡量IT安全性的尺度（即评估保证级 EAL），使得独立的安全评估结果可以互相比较。
2014 年	原国家质	《GB/T 31167-2014	规定了云服务商征信、经营基本情

	量监督检验检疫总局、国家标准化管理委员会	信息安全技术 云计算服务安全指南》、《GB/T 31168-2014信息安全技术 云计算服务安全能力要求》	况、平台稳定性、技术供应链安全、安全管理能力、云平台的整体防护能力等。金融云作为关键信息基础设施需依据该要求通过云安全审查。
2014年	国际标准化组织ISO	《ISO 27018:2014信息技术—安全技术—在充当PII处理器的公共云中保护个人身份信息(PII)的行为准则》	该准则规定了公有云服务中个人数据保护的安全要求。
2017年	国际标准化组织ISO	《ISO 29151:2017个人可识别信息保护管理体系》	该体系为国际通用的个人身份信息保护实践指南，聚焦于个人数据处理的全生命周期的管理措施。
2017年	英国标准协会BSI	《BS 10012:2017个人信息安全管理体系》	BS 10012是BSI发布的个人信息数据管理体系标准，规定了个人数据保护的体系要求。
2017年	支付卡行业安全标准委员会（PCI SSC）	PCI 3DS安全核心标准	PCI 3DS标准旨在保护执行特定3DS功能或者存储3DS数据的环境和实施安全，具体对3D协议执行环境的过程、流程、人员管理等方面进行了规定。
2017年	原国家质量监督检验检疫总局、国家标准化管理委员会	《GB/T 35279-2017信息安全技术 云计算安全参考架构》	规定了云服务中的角色安全职责、安全功能组件以及它们之间的关系。这个架构适用于指导所有云计算参与者在进行云计算系统规划时对安全的评估与设计。
2019年	国际标准化组织ISO	《ISO 27701:2019隐私管理体系标	规定了建立、实施、维护和持续改进隐私、个人数据保护相关所特定

		准》	的管理体系的要求。
2019、2020 年	原国家质量监督检验检疫总局、国家标准化管理委员会	“网络安全等级保护”2.0核心标准	《定级指南》明确了云环境下的定级对象，即云计算平台及云上的业务应用系统；《基本要求》明确了云计算环境的安全要求；《安全设计技术要求》明确了云计算的设计与建设问题；《测评要求》明确了第三方机构对云计算的安全测评要求。

来源：中国信息通信研究院整理

3.金融云行业安全要求

在遵循云服务通用规范的同时，金融云还需要符合金融行业专属的安全技术标准。2020 年 10 月 16 日，中国人民银行正式发布三项金融行业标准，从基本能力、网络安全、数据保护、运行环境安全、业务连续性保障等方面提出了有针对性的技术要求，确保金融云在安全性、稳定性、适配性等满足监管要求和行业需要，防范因云服务缺陷引发的风险向金融领域传导。

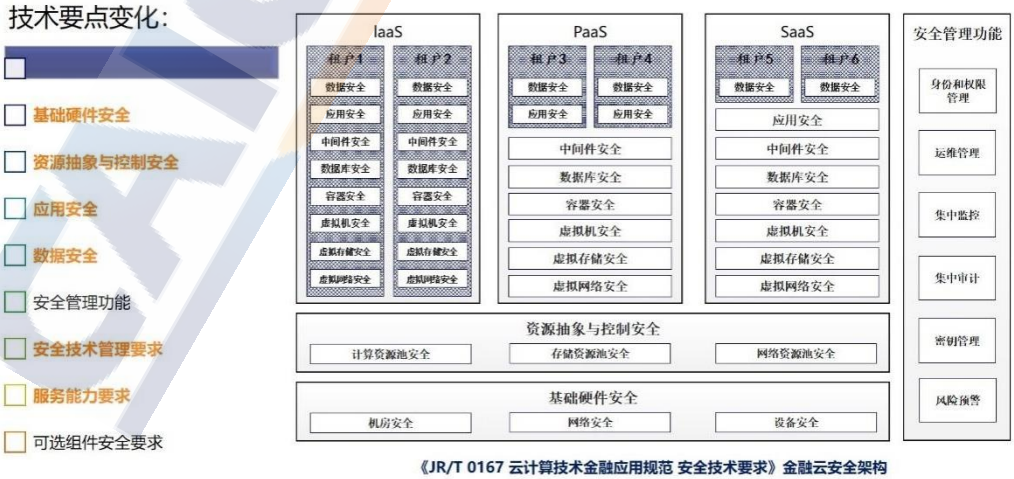
表 2 金融云行业安全体系

时间	发布部门	发布文件	安全要求
2018、2020 年	中国人民银行	《JR/T 0166 云计算技术金融应用规范 技术架构》	基于云计算技术特征，结合金融业云计算平台的主要实现方式，将云计算技术架构自下而上划分为基础硬件资源层、资源抽象控制层、云服务层，以及贯穿各层的运维运营管理层，并分别提出相关技术要求。
2018、	中国人民	《JR/T 0167 云计	围绕云计算金融应用潜在风险，在

2020 年	银行	算技术金融应用规范 安全技术要求》	兼容国家和金融行业现有信息系统安全要求基础上，从基本要求、扩展要求和增强要求三个类别分类施策，提出基础硬件安全、资源抽象与控制安全、应用安全、数据安全、安全管理、服务能力和可选组件安全等方面安全技术要求。
2018、2020 年	中国人民银行	《JR/T 0168 云计算技术金融应用规范 容灾》	规定了云计算各参与方在衡量云计算平台容灾能力、开展云计算平台灾难恢复工作时应遵循的技术要求。按照系统故障的影响范围、危害程度等将容灾能力划分为六个等级，并分别从关键指标、数据备份、数据处理、网络能力、运维能力等方面提出相应技术要求。

来源：中国信息通信研究院整理

金融云安全框架由基础硬件安全、资源抽象与控制安全、应用安全、数据安全、安全管理功能以及可选组件安全组成。云服务提供者和使用者共同实现安全保障。金融机构是金融服务的最终提供者，其承担的安全责任不应因使用云服务而免除或减轻。



《JR/T 0167 云计算技术金融应用规范 安全技术要求》金融云安全架构

来源：中国信息通信研究院整理

图 3 2020 年金融云行业安全标准架构

与 2018 年的行业标准版本相比，2020 年发布的金融云安全标准重点对金融云服务提供商在数据安全、安全管理、服务能力等方面提高了要求，并增加了金融云服务使用者对金融云方案兼顾效率和安全的综合考量要求。

表 3 2020 年金融云行业安全标准要点变化

序号	安全维度	变化要点
1	基础硬件安全	增加了云计算平台部署的机房安全要求
2	资源抽象与控制安全	增加了云服务提供者每年安全审计的要求
3	应用安全	增加了云服务使用者对于金融云方案的安全考量要求
4	数据安全	增加了云服务提供者跨境数据迁移时的要求
5	安全管理	增加了云服务提供者在升级或变更前应制定回退方案并充分测试评估要求；增加了云服务提供者应每年至少开展 2 次应急演练，并滚动完善应急预案
6	服务能力	明确了金融云应符合的通用安全要求，增加了金融云服务提供者的安全服务要求，增加了风险补偿机制要求。

来源：中国信息通信研究院整理

（二）金融安全事件频发

近年来，金融行业数字化转型不断深入，并且随着云计算、大数

据、人工智能等技术的发展和应用，金融行业也在加速与新技术的业务融合。与此同时，针对金融信息系统的安全威胁持续升级，全球出现了很多重大金融信息安全事件，本节重点梳理了金融行业面对安全挑战的三个维度，包括关键信息基础设施安全、数据安全和个人信息保护、供应链安全等类型的攻击事件。

1.关键信息基础设施攻击

金融行业特别是国有大行的部分系统作为关键信息基础设施，承载个人与对公的账户和账户处理等功能，涉及民生保障和国家稳定。近年来，针对金融关键信息基础设施的攻击事件时有发生，应当引起监管机构和金融厂商的重视。

2022 年 2 月，乌克兰两家国有银行都受到了 DDoS 攻击，导致两家银行的 Web 服务被迫中断，致使银行客户无法正常访问网上银行账户。2021 年 10 月 29 日，巴基斯坦国家银行遭受了破坏性网络攻击，影响了其部分服务，包括银行的 ATM、内部网络和移动应用程序。2021 年 6 月 4 日，为金融机构提供技术服务的德国公司 Fiducia&GADIT 遭到 DDoS 攻击，扰乱了该国 800 多家金融机构。

2.个人信息和数据泄露

金融行业保存了大量客户数据，近年来国内外均发生多起金融厂商的数据泄漏事件，不仅为金融厂商和客户带来最直接的经济损失，最终导致的是金融厂商的声誉、信誉的降低，丧失行业竞争力。

2021 年 9 月 22 日，南非收债公司 Debt-INConsultants 遭到重大勒索软件攻击，导致消费者和员工个人信息遭受重大数据泄露。2021

年 11 月，青岛市人民检察院提起的青岛首起侵犯公民个人信息民事公益诉讼案开庭，案件中涉及倒卖近四万条股民信息，造成社会公共利益损害。

3.软件供应链安全威胁

除了传统的网络攻击，针对金融机构上游基础设施及软件供应商的供应链安全攻击事件已经不足为奇。2021 年 9 月份，SushiSwap 社区的 MISO 密币交易平台遭到软件供应链攻击，攻击者劫持平台交易过程并盗取约 300 万美金的以太坊币。供应链攻击是通过感染合法应用分发恶意软件来访问源代码、构建过程或更新机制。

软件供应链攻击具有危害大、攻击隐蔽、难以发现等特点。传统安全防护体系通常情况下只针对边界进行防御，对供应链不做过多恶意代码检查。金融行业的业务系统往往涉及很多上下游应用，也使用大量外购、免费和开源软件，这些场景一般缺少对应的安全检查，存在供应链攻击的风险。

（三）宏观调控与政策发布

面对金融信息安全面临的新形势，国内从中央部门、监管机构、研究机构等不同层面均出台了法律法规、调控政策、行业标准等，对关键信息基础设施安全、数据安全和个人信息保护、供应链安全等提出了明确要求，引导金融厂商在充分利用和不断提升信息化、数字化的便捷性、高效性的同时，坚守住不发生重大风险和安全事件的底线。

1.保障金融基础设施安全

金融安全是国家安全的重要组成部分，是经济平稳健康发展的重

要基础，而金融基础设施的安全性对于保障金融安全至关重要。2021 年以来，中央及相关行业监管部门不断出台相关规划和政策，为金融基础设施建设和安全性保障指明了方向。

相比其他行业，金融业务数字化、网络化的特征更加明显，不同业务和不同主体之间的关联性也更强。在宏观政策的推动下，金融机构从核心系统、数据库到各个业务环节，普遍有着旺盛的上云以及更多深度服务的需求，金融云的安全性必将是金融厂商的首要关注。

表 4 推动金融基础设施安全相关政策

时间	监管部门	发布文件	政策要点
2021.12	中央网络安全和信息化委员会	《“十四五”国家信息化规划》	到 2023 年，金融业数字化转型成效明显；到 2025 年，先进可靠、富有弹性的基础设施服务体系基本形成，金融业初步实现数字化、智能化。
2021.12	中国人民银行	《金融科技发展规划（2022-2025 年）》	《规划》的六项目标重点围绕数字化转型建设，强调了金融上云、数据基础建设以及数据安全的重要性；八项重点任务强调了数字能力、金融网络、金融应用、金融创新的安全性要求。
2022.06	中央全面深化改革委员会第二十六次会议	《关于构建数据基础制度更好发挥数据要素作用的意见》	数据基础制度建设事关国家发展和安全大局，要维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。
2022.06	中央全面深化改革委员会第二十六次会议	《强化大型支付平台企业监管促进支付和金融科技规范健康发展工作方案》	推动大型支付和金融科技平台企业回归本源，健全监管规则，补齐制度短板，保障支付和金融基础设施安全，防范化解系统性金融风险隐患。

来源：中国信息通信研究院整理

2.重视个人金融信息保护

金融行业的业务特点决定了其信息系统掌握了大量个人敏感信息，如身份信息、征信信息、账户信息、鉴别信息、金融交易信息、财产信息、借贷信息等客户金融信息，既有客户在金融业务过程中积累的业务数据，也有个人隐私数据。个人敏感信息如果发生泄露，将直接侵害客户合法权益，还会为金融机构的正常运营带来影响，更严重的还会造成系统性金融风险，侵害公众利益、社会秩序甚至国家安全。因此，加强客户身份、账户等重要电子信息的保护，综合运用多因素认证、访问控制、边界防护、泄密检测、密码算法和技术、数据脱敏和安全审计等手段，防范敏感数据泄露、篡改、丢失和非授权访问等风险一直是金融监管机构的监管方向和金融机构的工作重点。

金融机构在选择云计算服务商前，应当预先了解云计算服务商机房和信息基础设施的设置地点，充分审查、评估云计算服务商保护个人金融信息的能力。此外，相关监管部门也颁布了数据保护法律法规和标准要求，值得重点关注的是，中国人民银行发布《个人金融信息保护技术规范》（JR/T0171-2020），对金融机构在个人金融信息的收集、传输、存储、使用、删除、销毁等生命周期各环节提出了具体安全防护要求。

表 5 个人金融信息保护相关法规和标准

时间	发布部门	发布文件	内容要点
2020.02	中国人民银行、国家市场监督管理总局	《JR/T 0171-2020 个人金融信息保护技术规范》	对金融机构在个人金融信息的收集、传输、存储、使用、删除、销毁等生命周期各环节提出了具体安全防护要求。

2021.09	全国人大常委会	《中华人民共和国数据安全法》	从法律层面明确数据安全保护义务，为开展数据处理活动的组织和个人提供了行为指引，填补了我国数据安全保护立法的空白。
2021.11	全国人大常委会	《中华人民共和国个人信息保护法》	立足于数据产业发展实践和个人信息保护的迫切需求，从法律层面更全面地保障了个人权利，及时回应了国家、社会、个人对个人信息保护的关切。

来源：中国信息通信研究院整理

3.提升金融软件供应链安全

2021 年，国家互联网应急中心公布《2021 年开源软件供应链安全风险研究报告》，报告中指出 2020 年开源软件漏洞数量达到 5728 项。随着金融行业信息化、数字化的不断深入，开源软件的漏洞也同步渗透到金融行业中，提升金融软件供应链安全刻不容缓。我国行业监管单位和标准制定单位，在多项法律法规及标准规范中，对供应链安全提出管控要求。

表 6 提升金融供应链安全相关政策和标准

时间	发布部门	发布文件	内容要点
2019.05	国家市场监督管理总局、国家标准化管理委员会	《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》	在通用要求中，主要从对供应商的选择、监督、评审等角度进行说明； 在云计算扩展要求中，主要从供应链安全事件信息、安全威胁信息以及供应链上其它重要信息同步的角度进行说明。
2021.09	中华人民共和国国务院	《关键信息基础设施安全保护条例》	要求建立供应链安全管理制度、明确安全管理策略、供应商选择保障、采购过程规范、响应处置及时。

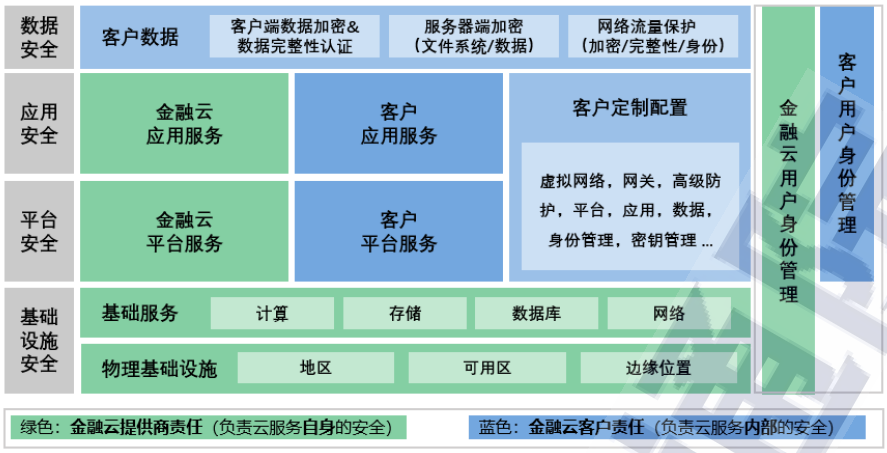
2021.10	中国人民银行、中央网信办等	《关于规范金融业开源技术应用与发展的意见》	要求金融机构在使用开源技术时应遵循安全可控、合规使用、问题导向、开放创新的原则。 应建立健全金融机构使用开源技术的协调机制、制度体系、技术路线、风险管控、合规审查、标准制度与知识产权保护能力。

来源：中国信息通信研究院整理

4.安全责任共担政策需求

随着金融行业数字化转型不断深入，金融科技能力不断加强，国内自上而下、由点到面已形成了较为完整的金融云安全体系建设。各头部金融厂商积极响应政策，在金融上云的建设实践中不断形成完善的安全保障体系，为金融行业的网络安全、数据安全等提供了有力保障，为金融行业的数字化转型打下了坚实的基础。

但目前，金融云安全的责任划分仍未能形成行业共识，已成为金融厂商核心业务上云的主要顾虑之一。与传统 IT 系统架构不同，云计算将资源和数据的所有权、管理权和使用权进行了分离，云上安全由云服务提供商和云服务客户共同分担。但不同行业、不同规模的云服务客户的安全能力和对云计算的认知存在差异，因安全事件引发的与云服务提供商的纠纷时有发生。**建立金融云安全责任共担模型，明确划分双方责任成为关键。**



来源：中国信息通信研究院整理

图 4 金融公有云安全责任共担模型参考

在金融云服务客户的长期实践中，已形成较为常规的金融云安全责任划分机制。以提供金融公有云服务为例，金融云提供商和金融云客户分别承担如下主要责任：

金融云提供商：主要责任是研发并运维运营金融云数据中心的物理基础设施，金融云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，金融云提供商还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理层的多维立体安全防护体系，并保障其运维运营安全。

金融云客户：主要责任是在租用的金融云基础设施与服务之上定制配置并且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，包括对金融云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，金融云客户还负责其在虚拟网络层、平台层、应用层、数据层和用户身份管理层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效

管理。

云端体系的运营和维护是提供方与使用方双方受益的局面，不公平的风险分摊不利于实现全局风险的最小化。相关金融行业监管部门应尽快完善配套政策和法规，明确云安全责任的分担机制，实现金融机构安全风险最小化。同时，在顶层设计层面应尽快建立金融企业和云计算厂商的职责定位导向，加快明确根技术、平台技术、应用技术的主体，将有利于推动金融机构加速业务上云。

（四）金融厂商的安全实践

在宏观调控与政策的不断推动下，国内金融厂商积极响应监管号召，在推动金融业务上云的过程中，不断加强安全技术手段、完善管理配套机制，切实履行金融厂商的安全责任与义务，为用户和企业提供更优质、更安全、更可靠的金融服务。本节重点梳理了金融厂商的安全实践案例，覆盖了银行、保险、证券等主流金融领域，对推动核心业务上云的安全实践进行详细介绍。

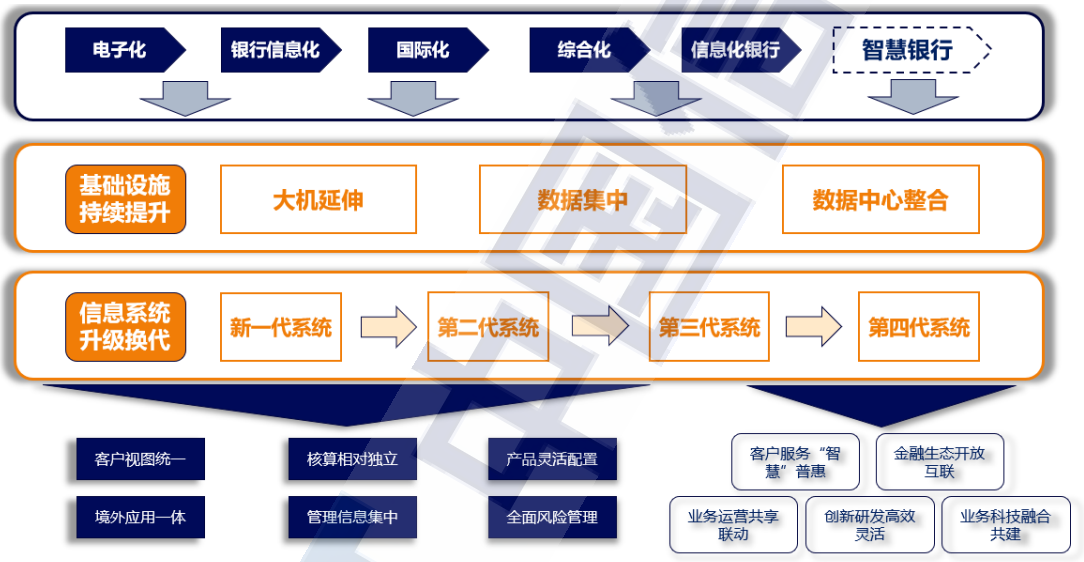
1.分布式金融云基础设施

国内某银行积极响应金融业务上云政策，推动超大规模金融云基础设施建设，支持核心业务系统上云，实现了超大规模、安全可靠高可用、交易数据库易在线扩展等目标。

该银行发布的智慧银行生态核心系统，包括提出生态化业务架构建模及落地方法、实现大型银行全分布式系统架构以及大型银行主机下移、银行系统生态化转型、大规模交易型分布式数据库、全栈国产化大数据平台。该银行利用自身在人工智能、区块链、云计算、大数

据、物联网等技术储备，在持续赋能和迭代提升业务应用。

金融生态云采用多种安全机制和手段保障基础设施安全：一是采用租户隔离机制，保障租户数据的安全隔离；二是支持个性化定制，灵活满足满足不同租户的差异化需求；三是全方位的云安全体系，从身份认证、访问控制、数据安全、安全检测和处置多方面实现安全加固，覆盖安全准入、安全处置、安全防护等全生命周期安全运营。



来源：中国信息通信研究院整理

图 5 分布式金融云基础设施

2.云原生数据湖风控支撑

国内某保险集团通过云原生数据湖支撑大数据集群统一管理，实现跨多版本滚动平滑升级业务零中断。在实现统一管理前，集团各业务部门大数据集群零散式自建，现网的集群数据无法互通，存在数据冗余。分散维护效率低、资源利用率低、升级难、易中断。

通过跨多版本平滑升级演进方案，建设了统一大数据平台，实现

大数据集群从传统物理机向云服务模式平滑升级，通过滚动升级能力，实现分批次升级，故障节点自隔离。通过多租户、多实例，实现资源统一管理、调度和运维，全局一份数据共享，资源利用率大幅提高；70 多项业务系统日均超 1 万作业的升级过程零中断，实现构建可持续的大数据平台能力。

云原生数据湖方案采用存算分离架构，将数据和环境变量解耦，根据运行环境自动关联所需要的数据和环境变量。通过隔离敏感数据，在云网络层面判断访问的客户端 IP、访问协议、访问端口是否有可访问权限；对于高敏感度数据，采用子网络再次进行隔离，多方面多层级保障个人信息和数据安全。

来源：中国信息通信研究院整理

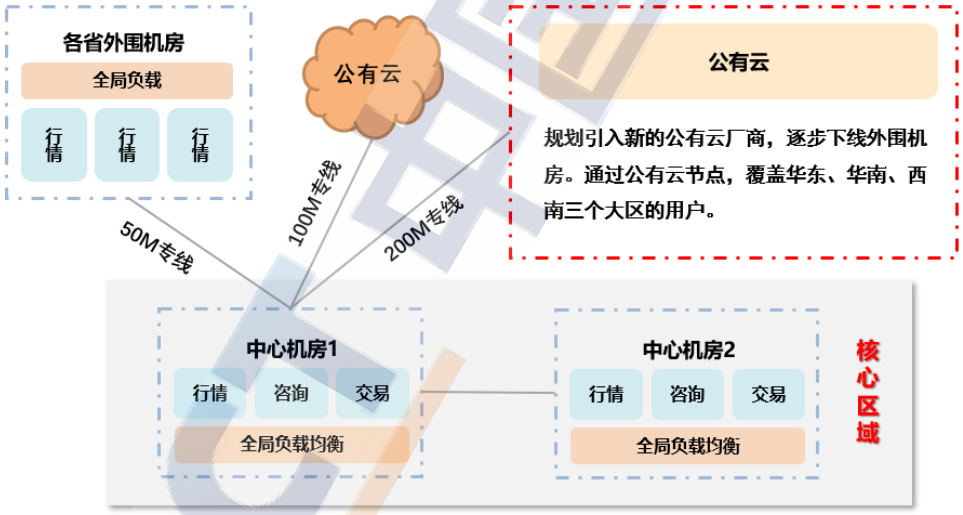
图 6 云原生数据湖风控支撑

3.公有云安全风险监控

国内某证券公司是证券行业信息化领先企业，年信息化投资超 10 亿。2020 年上半年启动数字化转型工作，决定将部署在线下多个城市 IDC 机房的行情资讯业务上公有云。

证券行情资讯业务主要包括两大类，一是主要面向移动终端用户，二是主要面向 PC 终端用户。初期靠自建物理机、私有云以及租用公有云承载上述应用，公有云接入节点较少，且私有云弹性扩容较慢，峰值情况体验不佳。采用公有云方案来承载行情业务，实现了高性能、安全可靠、高扩展性的目标。

在部署公有云过程中，根据安全策略、流程及操作指导，对产品和服务进行安全管理以确保安全性。此外，还建立了一般环境以及云环境下的安全监测、处置能力，实时掌握业务环境中资产间的网络互访关系，实现持续监控安全风险，及时发现并处置突发事件。



来源：中国信息通信研究院整理

图 7 基于公有云的行情资讯业务建设

（五）总结

传统安全管控的策略和特征主要从当下业务特征入手，策略相对于问题具有一定的滞后性，而云服务系统将所有业务与数据上网上云，利用云端数据实时监控技术，可以更快地发现系统安全风险，立即响

应并实现云端系统及时更新，不仅提高了风险响应能力，更提高了风险解决效率与解决质量。云服务为安全策略与安全系统特征的快速迭代创造了技术条件与动力，云服务安全体系的快速反应和调度能力都是传统安全管控难以达成的。实践证明，无论在公有云、私有云还是混合云领域，云安全都被验证是成熟可靠的服务模式。

同时，在纷繁复杂的国际形势变化下，鼓励信息系统国产化是必行趋势，而金融厂商一直是传统信息系统的重度用户。在全面上云的大背景下，云数据库、云原生应用等技术不断发展，金融云方案兼具云计算的弹性能力、云数据库的易用开放等特点，为金融行业逐步替代传统信息系统创造了条件，将大大提升信息基础设施的安全保障水平。

二、聚焦现在——变化

（一）宏观环境的挑战

1.疫情影响下的行业动向

近两年，随着疫情的影响，金融行业出现了新的不确定性。同时，企业及个人在金融业务的需求上都产生了显著的变化，这为金融业务带来挑战的同时也带来了新的机遇，并给金融安全提出了更高的要求。

（1） 行业韧性面临挑战，不确定性因素增加

全球疫情蔓延导致经济受到了较大影响。大量中小企业和受疫情影响较为严重的行业企业陷入困境，导致资产负债表失衡，陷入技术性破产的窘境，如果不能及时补充流动性，可能引发企业及居民的债务突发性违约，进而导致金融机构坏账增加，金融资产质量恶化，特

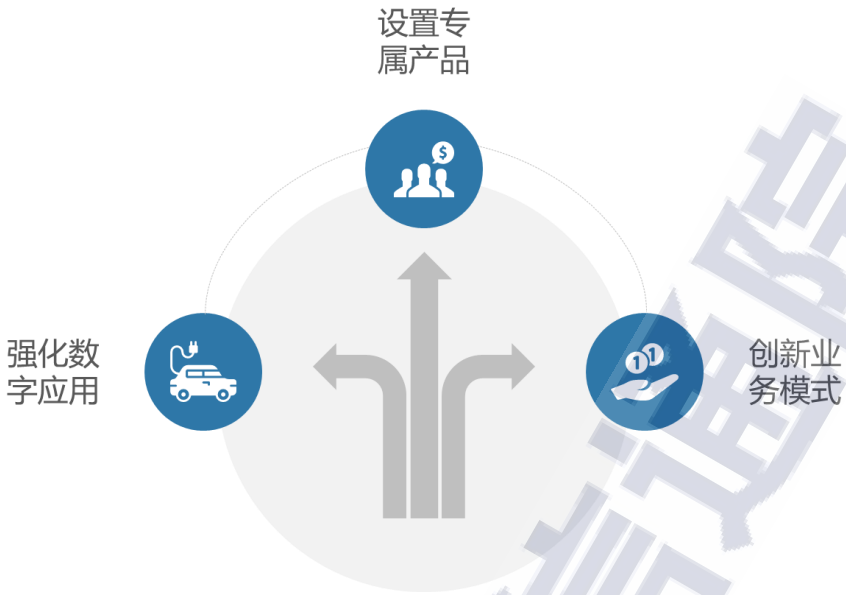
别是中小银行风险提升，整体金融行业的韧性面临考验。

（2） 线上场景不断涌现，重塑原有金融模式

从历史角度来开，疫情的到来，也会一定程度上重塑原有的金融服务模式，催生“零接触”的金融服务需求。2003 年的“非典”促进了电子银行业务的超预期发展，在国内银行电子银行的发展史上留下浓墨重彩的一笔。以某国有银行为例，2003 年 1 至 5 月份，个人业务的网上银行业务在新增客户、交易笔数、交易金额分别是上年同期的 2.6 倍、3.3 倍和 5.6 倍，企业客户的网上银行业务在新增客户、交易笔数、交易金额分别是上年同期的 2.8 倍、13.3 倍和 2.5 倍。在新冠疫情到来的今天，行业主管机构也在引导并鼓励金融机构采用在线方式开展金融服务，鼓励积极运用技术手段，在全国范围特别是疫情较为严重的地区，加强线上业务服务，引导企业和居民通过互联网、手机 APP 等线上方式办理金融业务。此类线上的金融服务方式，既满足了疫情防控工作的要求，又有力地保障了个人及企业群体的金融需求。

（3） 新兴业态持续发展，催生全新安全需求

金融机构面对疫情，也通过设置专属产品、强化数字应用、创新业务模式多措并举以支持社会经济从纾困到发展。



来源：中国信息通信研究院整理

图 8 金融机构多措并举发展新业态

设置专属产品。商业银行向科创企业及创始人提供分阶段、梯度化的专属短期信用贷款，并针对各级政府出台的重点白名单内小微企业提供专属“抗疫贷”等产品，协助企业加速恢复生产经营。保险公司推出防疫险以帮助个人应对疫情隔离风险。

强化数字应用。金融机构强化数字应用，为企业提供普惠边界的金融服务。如工商银行经营快贷、e 企快贷等线上产品，提供自动审批、随借随还的线上无接触融资服务。同时，紧急上线“普惠金融线上云服务”，企业在线提交融资申请后，系统就近分派至分布于全市逾 400 家服务网点，无盲点快速对接。

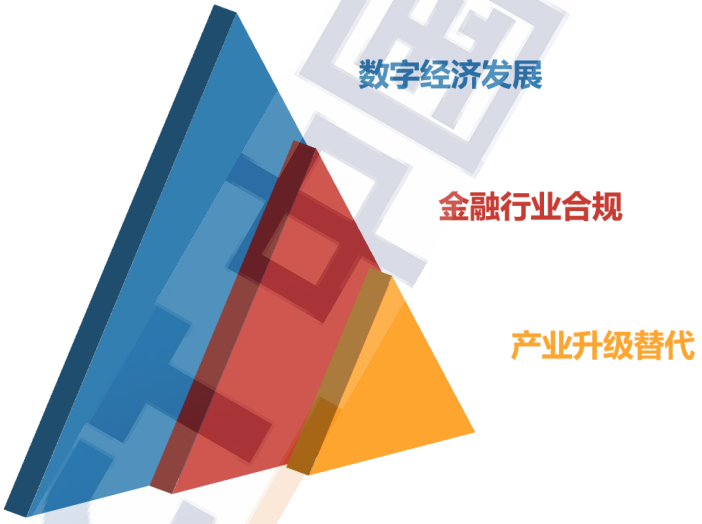
创新业务模式。金融机构突破原有服务模式，创新云服务，通过远程方式开展尽职调查，运用多维数据手段交叉验证，实行业务“云审议”模式，提高信贷审查效率，灵活便捷地保障信贷服务质量效率。

疫情使得金融机构意识到了数字化的刚性发展需求，并进一步明

确了未来金融数字化的发展趋势。疫情所重塑的金融新服务模式将给中国金融业，尤其是传统中小银行带来新的转型发展浪潮。另一方面，上述多方面举措，都高度依赖于线上服务模式及相关金融云服务。在线业务的蓬勃发展，也必将使得金融机构的数字化从产品、渠道的数字化，向组织架构转型、IT 架构升级等更深层面延展，这也给其安全防护体系带来了全新的挑战。

2.全新形势下的安全要求

当前，从宏观数字经济发展，到金融行业合规，到细分领域的升级替代，金融行业面临全新形势下的安全要求。



来源：中国信息通信研究院整理

图 9 全新形势下的安全要求

（1） 数字经济发展的安全要求

数字经济是继农业经济、工业经济之后的主要经济形态，是以数据资源为关键要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要素数字化转型为重要推动力，促进公平与效率更加统一

的新经济形态。数字经济发展速度之快、辐射范围之广、影响程度之深前所未有，正推动生产方式、生活方式和治理方式深刻变革，成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。“十四五”时期，我国数字经济转向深化应用、规范发展、普惠共享的新阶段。为应对新形势新挑战，把握数字化发展新机遇，拓展经济发展新空间，推动我国数字经济健康发展，国务院日前印发《“十四五”数字经济发展规划》（以下简称《规划》），明确了“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务和保障措施，其中重点提出了“着力强化数字经济安全体系”的相关要求。

其中，《规划》提出了要增强网络安全防护能力，提升数据安全保障水平等方面要求。在**增强网络安全防护能力方面，**《规划》要求提升网络安全应急处置能力，加强电信、金融、能源、交通运输、水利等重要行业领域关键信息基础设施网络安全防护能力，支持开展常态化安全风险评估，加强网络安全等级保护和密码应用安全性评估。在**提升数据安全保障水平方面，**《规划》要求推动提升重要设施设备的安全可靠水平，增强重点行业数据安全保障能力。进一步强化个人信息保护，规范身份信息、隐私信息、生物特征信息的采集、传输和使用，加强对收集使用个人信息的安全监管能力。

（2） 金融行业合规的安全要求

在安全方面，金融监管机构也对金融机构在金融科技安全领域提出了要求。在 2022 年初，中国人民银行印发《金融科技发展规划（2022-

2025 年）》，提出新时期金融科技发展指导意见，明确金融数字化转型的总体思路、发展目标、重点任务和实施保障。这是央行编制的第二轮金融科技发展规划，着重在解决金融科技发展不平衡不充分等问题，推动金融科技健全治理体系，完善数字基础设施，促进金融与科技更深度融合、更持续发展，更好地满足数字经济时代提出的新要求、新任务。《规划》总体部署第二节“基本原则”要求坚持数字驱动，在加快金融数字化转型的过程中践行安全发展观。第三节“发展目标”提出新时期金融科技的发展目标之一在于数据安全和个人隐私得到有效保障，以及“健全安全高效的金融科技创新体系，搭建业务、技术、数据融合联动的一体化运营中台”等要求，都为金融机构业务上云用云的安全提出了新的要求。

进一步，“数据要素”是本轮规划的新增内容。数据要素被升级成为金融业的生产要素，是金融科技行业和企业发展的核心。如何在保障数据安全和以技术作为驱动的前提下，充分激活数据要素潜能，推动数据的高效治理、有序共享和综合应用是各家金融机构接下来的发力点。目前，大型金融机构已逐渐布局高效的算力体系，加大对隐私计算的投入，不断完善可信技术底座，但中小型金融机构在数据要素的体量、治理和流通上均与前者存在较大差距。应严格落实数据安全保护法律法规，同时利用先进技术手段严防数据的不当使用，保护数据主体隐私权不受损害。

（3） 产业升级替代的安全要求

2022 年 1 月，银保监会发布《银行业保险业数字化转型的指导

意见》，明确提出：“提高新技术应用和自主可控能力。对业务经营发展有重大影响的关键平台、关键组件以及关键信息基础设施要形成自主研发能力，降低外部依赖、避免单一依赖。加强自主研发技术知识产权保护。加强技术供应链安全管理。鼓励科技领先的银行保险机构向金融同业输出金融科技产品与服务。”上述要求，也为金融云及其上下游产业链、供应链安全可控提出了更高的要求，全栈安全将提升到新的高度。

（二）安全态势的挑战

1.数字业务全面覆盖，新安全场景不断衍生

目前，利用数字化和信息化手段，各家金融机构都在力争做到传统业务数字化。

来源：中国信息通信研究院整理

图 10 金融云领域新型数字业务

如**精准营销领域**，金融机构在进行拓客时，通过精准画像、知识图谱等技术确定客户身份，识别客户特征，提供差异化的客户体验和金融产品；在**大数据风控领域**，金融机构在风险管理过程中，基于人工智能算法和大数据的深度融合，构建可信的，合理的，科学的智能风险评估模型，采取全面、全程、全新的风险管理措施，形成对贷前调查、贷中评级授信，贷后监测催收的全方位、一体化的风控体系；

在**智能客服领域，**金融机构在客户服务过程中，采取深度学习等智能算法分析客户的特征需求和风险偏好，为期定制个性化的金融产品或投资组合，设置人工智能服务机器人，专业化、智能化开展咨询，提升客户服务体验与效率；在**智能投顾领域，**金融机构提供实时线上投资建议，解决信息不对称问题。上述传统服务的线上化、智能化、数字化的转型，都衍生出了新的安全场景。

2.机构海外业务拓展，新安全需求亟需解决

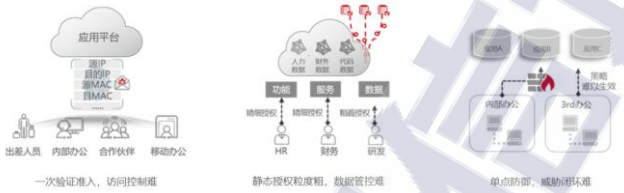
随着金融机构的海外拓展，众多高净值人群或离岸公司出于支持境外业务或减少跨境资金流动频率等系列原因，更多地通过离岸银行开设离岸账户或者需求跨境金融业务，包括境外财务管理、境外资产管理、跨境投融资、移民金融服务等跨境金融业务日益增加。

业务拓展也带来系列安全风险。首先，认证技术存在风险，跨境金融服务主体身份难以核查。以跨境开户为例，传统方案已然不能杜绝投资者事先录制视频或拍摄照片上传至网上开户系统，难以控制实名制认证中的技术性风险。其次，跨境服务信息涉及到敏感数据，安全性难以保证。跨境服务系统面向互联网开放，面对各种网络安全攻击，DDoS 攻击、木马植入等一系列风险，对业务数据的安全提出更高要求。

3.体系架构快速变革，新安全技术尚待完善

随着多云、混合云成为主要形态，以数据中心内部和外部划分的传统安全边界被打破，IT 架构面临更多的安全信任危机。如海量连接，打破了网络的边界，原有的一次验证准入，使得访问控制难；数

据融合，打破了数据的边界，原有的静态授权粒度粗，使得数据管控难；业务上云，打破了应用的边界，原有的单点防御手段，使得威胁闭环难。同时，随着容器、微服务、DevOps 等领域的快速发展，云原生已经被广泛应用，业界也开始形成更完整的云原生技术架构。云原生在显著提升云计算产品能力的同时，也带来了更为复杂的安全技术需求。



来源：华为云计算技术有限公司

图 11 现有安全体系面临的痛点问题

因此，默认一切不可信任的零信任等新型安全体系开始兴起，但零信任等新兴安全体系走向产业化仍需持续完善技术架构，并解决如部署方式等相关问题以更好的满足客户要求。

4.产业链条涉及众多，新安全生态需要协同

公有云服务商为海量租户提供服务，面对不同层次的安全需求，很难完全依靠自身的技术和服务能力保护云租户的数据和业务安全。因此，云安全生态应致力于构建开放、协作、共赢的安全生态体系，与业界领先的安全产品与服务供应商一起，基于责任共担模式，为云租户提供易部署、易管理、完善的安全解决方案，对已知、未知的安全威胁，保障租户的数据和业务安全。但网络空间安全变化多端、安全问题发展迅速、安全威胁危害巨大，如何构建开放、协同的快速检

测、深度防御、及时恢复的新安全生态，是云计算产业面临的巨大挑战。

（三）新生问题的挑战

云服务提供商作为承载业务的基础平台，在注重自身安全的同时，关注云上业务安全。当前，行业当中涌现了大量的黑灰产应用云计算技术进行电话诈骗、洗钱、虚拟货币等非法金融类业务，这给云业务安全带来了新的挑战。

1.金融诈骗手法不断更新

在数字技术与金融行业融合发展，催生数字金融新业态的同时，新型的欺诈形式和手段也不断衍生，金融欺诈风险不断扩大，反欺诈形势严峻。近年来，无论是根植于数字技术的金融业务还是传统金融的数字化，欺诈事件均层出不穷。诸如薅羊毛、虚假流量、身份伪造、电话诈骗等新型犯罪案件呈现出持续高发多发、黑灰产业日益专业化等特点，影响了消费者对数字化金融服务的信任程度。这一方面不利于数字金融行业的良性发展，为传统金融的数字创新业务带来诸多消极影响，另一方面也对金融云的风控反欺诈能力提出了更高的要求。

2.虚拟货币活动更加隐蔽

2021 年 9 月，央行等国家行业主管机构已通知明确虚拟货币不具有与法定货币等同的法律地位，虚拟货币兑换、作为中央对手方买卖虚拟货币、为虚拟货币交易提供撮合服务、代币发行融资以及虚拟货币衍生品交易等虚拟货币相关业务全部属于非法金融活动，一律严格禁止，坚决依法取缔；境外虚拟货币交易所通过互联网向我国境内

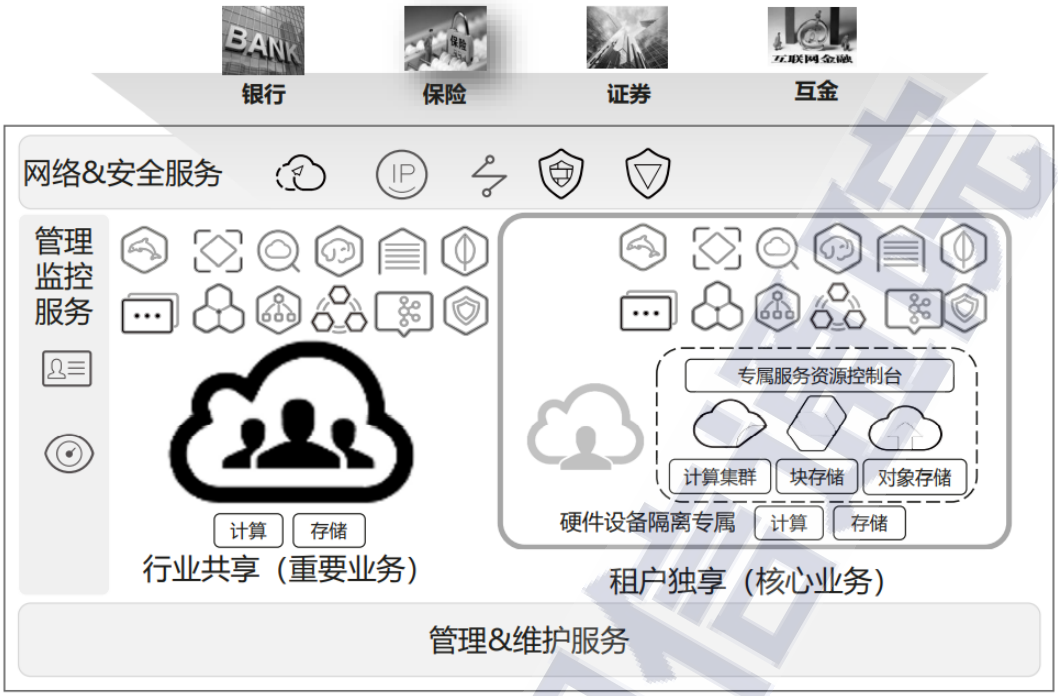
居民提供服务同样属于非法金融活动。但仍有非法份子以更加隐蔽的手段进行获利。如在去年下半年，包括 BlackMatter、HelloKitty 和 REvil 等在内的多个勒索软件团伙使用一种 ESXi 服务器对 Linux 系统进行攻击，这种服务器需要事先装好 ELF 加密器。加密货币挖矿一般由两部分组成，加密挖掘与加密劫持，网络攻击者通过劫持云计算资源并保持不被发现进而实时获利。

（四）金融厂商应对举措

面对**宏观环境的挑战、安全态势的挑战、新生问题的挑战，**金融机构对安全问题的忧患意识也日益紧迫，并高度重视在网络安全和云安全技术能力、合规及生态上的投入。采取了自建或专属云基础设施、软硬一体化全栈自研、云网融合协同促安全等新模式新技术，构建起了多维立体、纵深防御和合规遵从的基础设施架构并加速开发或联合云生态伙伴构建完善的云安全技术和服务体系，以进一步提升云安全的合规性。

1.自建或专属云基础设施

当前，金融自建或专属云基础设施是金融行业的主要云服务部署模式，是金融云安全可靠的重要保证。金融机构通过自建云服务可享受完全物理隔离的计算、存储、网络等资源，以满足其对安全合规的较高要求。同时，云服务商也在提供金融专属云服务，以满足金融客户对于核心关键业务系统对高性能的要求以及业务在网络安全、运营安全、数据安全、容灾备份方面的各项合规要求。



来源：华为云计算技术有限公司

图 12 自建或专属云基础设施

具体而言，在网络安全方面，云服务商提供了虚拟私有云、虚拟专用网络、漏洞扫描服务、应用防火墙、DDos 流量清洗等服务以满足金融机构在网络隔离、混合云部署、流量安全等方面的要求；在运营安全方面，云服务商提供了云监控服务、应用运维管理服务、云审计服务、态势感知等服务以满足金融机构在监控、运维、审计、威胁告警等方面的要求；在数据安全方面，云服务商提供了数据存储加密、数据加密、云备份、对象存储迁移、主机迁移等服务，以满足金融机构在数据生命周期中的各项安全要求；在容灾备份方面，云服务商可提供存储容灾服务（SDRS），可帮助金融机构在容灾站点迅速恢复业务，缩短业务中断时间。

如，国内某银行的“新一代分布式核心系统”于 2021 年 4 月顺利

完成第一批次技术平台投产并同步启动旁路验证。该系统采用了安全的云原生基础设施作为全行级技术底座，自下而上划分为微服务框架、技术中台、业务中台三层，结构稳定灵活，具备多活容灾切换、单元水平在线扩容、微服务治理、故障感知转移、业务强一致性、灰度发布等能力。

2.软硬件安全全栈提升

为了应对金融行业关于安全方面的要求，金融机构应本着“保留建设成果、保持技术领先，应升尽升、真升真用、增量优先、迭代展开”的建设原则，联合行业生态伙伴，从外围的办公系统、一般业务系统入手，逐渐深入到关键业务系统及核心系统，以达到软硬件安全全栈提升的目标。

来源：中国信息通信研究院整理

图 13 软硬件全栈能力提升

如图所示，具体而言：

办公管理层面，金融机构逐步从公文管理、邮件管理、事件管理方面着手建设。中国工商银行、中国农业银行、中信银行、民生银行等机构已经试点并逐步开始广泛使用。在试点初期，金融机构通过云应用解决升级适配难题，以保证后续在应用实现升级后平稳过度。

一般业务系统层面，金融机构逐步从渠道服务、数字化营销、数字化业务、风控合规、内部运营与管理支持等方面着手建设，包括中国工商银行、中国建设银行、光大银行及一些股份制银行等都逐步对本机构的一般业务系统开展改造。如某国内股份银行，从 2020-2021 年，建成开发测试、生产内网、生产外网、同城灾备四朵云。在一般业务系统中，从经营分析类系统着手，到 2023 年底，完成升级。

关键业务系统层面，金融机构逐步从核心应用及支付结算两方面着手开展工作。核心应用方面，包括借记卡核心、信用卡核心、互联网核心系统；支付结算方面，包括国际结算、支付清算等方面的核心系统。包括中国建设银行、中国邮政储蓄银行、贵阳银行、泸州银行等传统大行和地方银行都已经开始试点。

基础设施层面，金融机构逐步构建了芯片、网络、存储、服务器的硬件底座。同时，在 IaaS 层，将计算服务、存储服务、网络服务、安全服务、灾备服务等方面逐步替换；在 PaaS 层，逐步实现分布式数据库、微服务框架、数据仓库、AI 等底层能力的升级。

3.云网边融合协同安全

在 5G 网络的加持下，传统上相对独立的云计算资源、网络资源与边缘计算资源不断趋向融合，即需要在云计算、边缘计算以及网络

之间实现云网融合、云边协同才能实现算力及安全的最优化。深度融合“云＋网”IT 系统的云网融合一体化服务，已成为助力基础电信运营商从单纯通信类业务向综合信息服务转型的重要抓手与业务着力点。同时，云网边融合协同也可同步促使安全能力的提升，也成为了金融机构用云上云时，在安全方面的重要考量。

金融机构使用云服务时，通过云网边融合协同，打通原先云、网、各自独立的安全架构，建立具备防御、检测、响应、预测能力的一体化安全体系，维护金融等关键领域的信息安全。在此基础上，还进一步实现了基于业务、权限、敏感等级、风险情况等对数据细粒度的动态防护，以及安全能力的灵活部署及按需服务等需求。

三、展望未来——变局

（一）新科技与安全伦理相互交织

《金融科技发展规划（2022-2025 年）》提出加强金融科技伦理建设。坚持促进创新与防范风险相统一。当前，区块链、元宇宙等新兴技术的推陈出新，在带来更先进技术特性、更优质用户体验的同时，也带来了新的安全及伦理问题。

区块链技术的出现，**一方面**，为全球金融业信用体系提供了新思路、新方法。作为一项创新性技术，其技术基础是分布式存储数据库，同时数据存储、记录和更新都是基于分布式网络。这些特性也被看作是可以应用于金融场景，降低传统金融体系集中式支付、结算和清算的系统压力，提高货币支付系统的弹性和容量。同时，区块链系统采用非对称加密，信息更新需要全体节点验证，并用时间戳技术标记数

据更新，确保区块链信息不可篡改和数据记录的可追溯，有效保障了区块链系统和数据安全。**另一方面，**这些特点是一把双刃剑，即使不考虑分布式账本技术运行在存储容量和能源消费上的弊端，其未知安全风险和技术缺陷必须引起高度关注。这为金融信息系统的安全和科技伦理提出了新的命题。

元宇宙也成为了金融机构和科技企业的探索之地。**一方面，**元宇宙的沉浸感体验能突破传统金融的时空限制，打开客户的科技体验的同时，打开金融拓客与触点营销的新机遇。元宇宙可以从模拟、仿真、体验等方面创新应用场景，丰富金融产品营销的内容和手段，围绕个性化、沉浸式体验打造金融业务新场景。伴随元宇宙概念诞生的沉浸式体验技术正逐步走向应用与推广，而这一趋势早在疫情之初线上办公与线上会议软件的普及就已现端倪。VR 设备、可穿戴设备、智能设备、机器人服务等智能体验将逐步进入金融业务，无论是成为业务的主要推广手段，还是优先利用科技感体验为核心业务辅助推广，元宇宙概念的想象与尝试是金融领域革新的重要突破口之一。**另一方面，**也应该看到元宇宙也存在着诸多信息安全和科技伦理问题。首先，AR/VR 设备等元宇宙终端，不像手机具备较高的安全防护能力，容易成为恶意软件入侵和数据泄露的门户。其次，随着虚拟身份的概念盛行，尚未出现对其信息保护的指引，攻击者易通过收集个人数据的虚拟化身来收集用户信息。这些都会成为元宇宙在金融业务应用中的安全和伦理挑战。

（二）新监管与业务发展互相适应

中国人民银行印发《金融科技发展规划（2022-2025 年）》中提到要加强金融科技审慎监管。按照金融持牌经营原则，坚持所有金融活动必须依法依规纳入监管，严格厘清金融业务边界，对金融科技创新实施穿透式监管。金融云业务作为金融科技中的数字底座，也面临如何平衡监管要求与业务发展相适应的问题。

例如，个人隐私保护的监管要求与大数据征信业务之间存在目标差异。前者要求数据私密性，后者要求数据公开透明、可查可验。如何利用如隐私计算等新型技术手段将二者差异化进行化解，使得监管和业务发展相适应，在尊重用户隐私数据的同时，安全储存并合理使用相关数据，成为了金融云安全未来需要更重点关注的新趋势。

四、总结——不变的是变化

（一）主动创新预判变化

伴随金融科技的发展，中国云服务行业整体迎来发展加速，而云安全体系的部署长期存在时间滞后。随着数据流通的加速，金融领域的安全失序将带来更大的风险与损失。**从发展视角来看，**金融技术的迭代速度与安全体系的实施速度的矛盾要求金融云体系提前做出系统架构与基础设施部署。**从业务视角来看，**金融客户对数据隐私安全的诉求和云存储与大数据平台征信体系的要求之间同样存在矛盾，这要求金融平台提前开发新兴金融技术的应用场景，在实践与尝试中寻找平衡与突破。**从市场视角来看，**金融客户对新兴技术的尝试与合作打开了新型金融业务的市场，为创新业务体系创造了动力，但也带来

了全新的安全挑战。金融机构应将安全合规摆在与业务发展同等重要甚至更加重要的位置上，积极探索安全新技术、新体系、新理念，超前创新，预判安全态势的变化并做好技术储备等相关布局。

（二）全栈自主拥抱变化

面对纷繁复杂的国际局势和业内监管要求，金融机构应持续打造包括芯片、服务器、存储、网络、操作系统、数据库、中间件、云服务的软硬一体的“全栈自主”的安全技术架构以拥抱变化。具体而言，应推进传统架构向分布式架构转型，主要业务系统实现平台化、模块化，逐步形成对分布式架构的自主开发设计和独立升级能力。加快数据库、中间件等通用软件技术服务能力建设，支持大规模企业级技术应用。加强创新技术的前台应用，丰富智能金融场景，强化移动端金融服务系统建设。加强对开放金融服务接口的统一管理，实现安全可控运行。同时，金融机构应对业务经营发展有重大影响的关键平台、关键组件以及关键信息基础设施要形成自主研发能力，降低外部依赖、避免单一依赖。

（三）开放共赢谋求变化

更进一步，金融机构保持开放合作的态度，持续联合业内云服务厂商、安全厂商伙伴等携手一道构建开放、协作、共赢的安全生态体系。在**技术体系方面**，基于责任共担模式，探索易部署、易管理、完善的安全技术体系，应对已知、未知的安全威胁，保障数据和业务安全。在**技术趋势方面**，产业应携手主动谋求变化，探索如零信任理念和原生安全理念等新安全技术趋势，以应对身份安全、网络安全、终

端安全、应用安全、数据安全等多领域的问题，最大限度保障数字基础设施中各资源和动态行为的可信。产业链上下游应深刻意识到安全没有终点，应不断的携手合作，谋求安全技术创新、架构创新、体系创新才能形成合力，超前布局，决胜千里。

中国信息通信研究院 泰尔终端实验室

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：13811959962

传真：010-62304364

网址：www.caict.ac.cn