码上开启·数字金融

新华三集团

北京总部
北京市朝阳区广顺南大街8号院 利星行中心1号楼
邮编:100102

杭州总部
杭州市滨江区长河路466号
邮编:310052

www.h3c.com

CN-191030-20190923-BR-SD-V1.0

紫光集团 | H3C
核心企业 | 数字化解决方案领导者

Digital Finance

数字金融 NAVIGATE

— 第02期 —

可控安全体系建设

基础运维应急管理

云等保 | 物联网 | AI防火墙

金融安全科技人才培养

主动安全

目录 CONTENTS

【主办】

新华三集团金融事业部

【总编】

李乔

【编辑】

闫军、纪钟、张静华、韩喆、朱崇银、宿梦婷

刊首语

刊首语

数字金融时代的
可控安全体系建设

新华三集团金融事业部总经理 李乔

数字经济时代来临，金融行业得益于长期以来的投入和建设，其自身业务的数字化能力处于业界领先位置。随着各行各业数字化的不断推进，出现了更多的数字化外部场景，推动了金融科技围绕着网络化、数字化、智能化等相关方向的技术快速演进，大大拓展了金融服务的数字化外延，打开了金融服务的新空间。数字货币，移动支付，开放金融等进一步拓展了数字金融的边界。外部边界的变化，数字金融领域的广泛对接，也同时带来与之前不一样的风险和安全需求。而金融行业作为社会经济活动的重要支柱，如果安全得不到保障，将给生产、经营、资产、隐私等方面带来严重损害，直接影响社会稳定和国家安全。因而迫切需要在金融数字化安全领域具备能打硬仗的能力。

首先——需要重新认识和定义安全的边界

数字化时代将给金融带来更多的数字化边界，并引入更多的新型技术，我国已经发布5G牌照，移动计算已成为金融业务前端不可或缺的技术，物联网技术也得到广泛的推广和应用，IPv6逐步在新的互联世界中普及，云计算也逐步成为各个金融客户的IT基础设施。这些新技术在支持新一代数字化应用的同时，也对安全防护的基础和技术提出了新的要求。而来自内网的攻击也让终端安全成为重要的边界，在复杂的内部网络进行认证、识别和侦测，更需要有匹配的技术手段来支持。有针对性的加强边界防护，不仅需要加强相关技术应用水平，同时也需要不断将相关领域的最佳实践引入。

其次——安全技术与管理并重

数字金融时代的应用快速创新会给安全防护技术带来持续的挑战，跟进最新的安全技术将成为一个常态。在学习先进技术的同时，也要认识到各种技术的应用最终是为管理服务的，很多安全问题的解决不仅仅要从技术角度，也要从企业管理的视角，通过管理手段来进一步完善。因此需要设计整体和全局的安全观，从整体、全局的角度来看待、规划和管理网络安全，而不是仅仅关注单点安全、单个安全防护手段，或单个防护设备。通过构建合理的整体安全体系，满足等保合规要求，并配合金融对业务连续性的要求，设置好整体的风险防护和安全应急措施，再配合引入智能化技术手段增强决策能力和管理效率。只有这样才能确保围绕金融企业的整体业务目标，实现主动安全。

最后——坚实的基础离不开安全团队建设

从攻防的角度来看，网络安全的本质在对抗，对抗的本质在攻防两端能力的博弈。而数字化时代安全会涉及到多个层面和场景，因此安全防护工作并不是可以简单的通过个别人的能力一蹴而就达到的，只有知识技能协同的安全团队才具备强大的对抗和防护能力。从这个视角来看，技术手段只是一个工具，其实质是团队与团队，即人和人之间的对抗，因此决定安全防护手段应用能力，安全管理水平是否执行到位，依赖的是强大的人才团队。因此加强安全科技人才培养将是保持长期防护能力的基础。

新华三基于多年在安全领域的投入，在面向敏态和稳态数字金融架构方面积累了大量的实施和防护经验（ABC融合平台、IPv6、物联网、5G、边缘计算），同时以新华三大学多年来在科技人才培养方面的资源和能力，期望能为各个金融机构的安全体系建设，提供更多的有力支撑。

李 乔 新华三集团金融事业部总经理

李乔（George Li）先生作为高级管理人员拥有18年丰富的IT行业从业经验，非常熟悉企业级软件、硬件和服务市场，深谙IT对客户业务战略的促进，并对金融、互联网、政府等核心行业有深刻理解。

李乔先生从2003年到2016年在杭州华三工作期间先后历任数据通信产品行销部经理，政府系统部总监等职位，实现所负责领域的快速增长。紫光旗下新华三集团成立后，李先生于2016年至2017年就职新华三集团副总裁，分管集团技术咨询销售工作，建立了完善的技术咨询服务团队，实现了原中国惠普与原杭州华三两个技术咨询板块的整合优化，自2018年起在金融事业部任职。

新华三资讯

INNOVATION

新华三半导体技术公司成立 发力高端路由器芯片自主创新

2019年4月4日，新华三集团正式宣布在成都市高新区成立新华三半导体技术有限公司，将聚焦于新一代高端路由器芯片的自主研发，为相关客户提供高性能的高端路由器产品与解决方案。在未来的市场竞争中，新华三将本着高技术、高标准的原则，在继续采用全球技术领先的商用芯片合作伙伴解决方案的同时，按需融入自主创新的解决方案配套芯片，形成优势互补。未来，新华三半导体技术公司的自主芯片研发，还将逐步扩展至物联网以及人工智能等领域。

2019领航者峰会，新华三重磅发布多款新品

2019年4月20日，在以“数字赋能 智启未来”为主题的2019领航者峰会第二天全体大会上，新华三围绕“数字大脑计划”发布了“智能数字平台”，致力于成为智能数字世界的基石。围绕智能数字平台具备的六大能力，新华三重磅发布了多款产品，主要包括业界领先的ABC融合平台Cloud OS 5.0，AD-NET 5.0新一代智能网络解决方案，新华三U-Center 2.0新一代统一运维平台，全系列AI防火墙，5G边缘解决方案，旗舰产品AI交换机S12500-X智能模块SeerBlade，H3C SCM存储及特有的本地智能管理系统和多款新安防产品，为“数字大脑计划”的打造奠定了坚实基础。

主动出击、智慧防护 新华三发布全系列AI防火墙

紫光旗下新华三集团重磅发布全系列的新一代AI防火墙。该防火墙首创融合AI技术，采用高性能的双GPU+双CPU+AI模块架构，具备超强运算能力，每秒达到万亿次。拥有感知、学习、智动三大特点，能够支持近百种安全AI模型。同时，AI防火墙能够结合智慧安全解决方案，协同全网和云端防护，做到云网安融合高密度集成、运维精简，实现全网的态势可视。AI防火墙的发布，标志着新华三信息安全在智能领域能力的全面升级，新华三新一代AI防火墙大大提升了对未知安全威胁的分析准确度，以及安全事件处置的效率，为数字经济提供全方位的安全保障。未来通过人工智能技术在系列安全产品的应用，将主动安全体系推到全新高度，为企业数字化转型构筑更智能的主动安全防御体系，引领主动安全防护进入智能新时代。

新安防产品发布，新华三引领安防行业智能化变革

在紫光旗下新华三集团与重庆紫光华山智安科技有限公司联合举办的主题为“融汇数字技术 引领新安防时代”的新安防产品发布会中，隆重发布了公安视频云、雪亮工程、智慧社区、智慧交通、智安园区五大新安防解决方案以及多款新产品，由此揭开“智能+”时代新华三引领安防行业智能化变革的序幕，新华三“智能数字平台”与紫光华智智能安防技术强强联合，通过携手广泛联合的生态合作伙伴，为客户完整交付满足不同行业、场景需求，涵盖端、边、云、网的领先的新安防解决方案。

新华三U-Center 2.0新一代统一运维平台发布

新华三以场景为驱动，以智能化的方式重新定义运维，推出了U-Center 2.0统一运维平台，从应用视角出发提供全域融合的运维解决方案，以AI赋能，提升敏捷交付体验，开启智能运维时代。

作为有实力驱动企业运维全域创新的平台，U-Center 2.0将有能力在AIOps智能运维、混合架构全域资源管理、数字化服务体验管理、新一代网络智能运维管理、数据中心自动化运维等领域提供卓越的创新服务。

同时发布了针对金融行业的五大运维解决方案，其中包括生态合作，例如与清华大学做AIOps智能运维共研。

H3C SecPath M9000-AI-E16

- **业界首款**集成双GPU+双CPU+AI模块的防火墙，深度学习浮点运算能力达到**万亿次**每秒
- 全业务智慧防火墙吞吐量可达到**3.2T**，纯应用层能力提升**200%**达到**600G**
- 支持**开放**业务平台，可集成第三方应用软件
- 结合威胁情报+云端大数据+神经网络学习算法实现**更智能**的安全分析

基于GPU+CPU+AI芯片架构的新一代“AI防火墙”旗舰M9000-AI系列，具有超强算力，并支持近百种安全智能模型，为用户带来智慧感知、智慧分析、智慧运维的极致安全体验。

《信息安全技术 网络安全等级保护基本要求》（等保2.0）发布，新华三助力安全产业迈向新高度

《信息安全技术 网络安全等级保护基本要求》正式发布，紫光旗下新华三集团全程配合公安部参与了该系列标准的起草和修订工作，与众多科研单位、安全厂商及业界专家同心协力，形成了包括网络安全等级保护要求、网络安全等级保护测评要求和网络安全等级保护设计要求在内的一整套先进、科学、完善的标准体系。

新华三云服务安全防护系统入围工信部“网络安全技术应用试点示范项目名单”

新华三集团“基于云服务的新一代安全防护系统”项目成功入选工信部发布的“网络安全技术应用试点示范项目名单”，这标志着新华三全面系统的方案设计能力、扎实的技术实力、丰富的项目实施经验获得了国家、市场和用户的充分认可。信息安全已经上升到国家战略，面对日益严峻的信息安全挑战，新华三在业界率先提出主动安全理念，致力于打造具有“主动发现 · 预知未来 · 协同防御 · 智能进化”为特色的新一代主动安全防护体系。

SECURITY

国产虚拟化第一，如何C位出道

近20年间，金融行业X86服务器计算虚拟化几乎被VMware vSphere垄断。随着国内自主创新的深入发展，目前国产虚拟化软件从功能性、稳定性、可靠性等已经与外资厂商看齐，甚至在场景化、定制化、即时服务方面有了一定的超越。市场占有率方面，据最新权威第三方机构显示（计世资讯），国产厂商占比已接近50%。国产虚拟化崛起势不可挡。

新华三从2009年预研服务器虚拟化到多商用版本的持续发布，至今，已走过10个年头，2019年3月新华三发布了最新版CAS6.0，其达到了7个9的高可靠性。截止2019年6月，新华三的H3C CAS虚拟化产品，已连续4年排名国产计算虚拟化第一，刷新全球SPECvirt虚拟化测试记录（2018年第一名），在功能和性能上已达到完全替换vSphere的业务要求。CAS产品已在国内装机超过7000名客户，其中，金融行业有近百个客户使用了新华三H3C CAS虚拟化产品，得到了业界广大客户的认可。H3C CAS以低延时、高性能、内核级安全、全栈IPv6等特性，承载了金融客户如手机银行、资金核算、移动支付等关键性业务场景，为金融客户提供了充分的技术保障。

人工智能支撑平台（AIOS）

近几年来，人工智能应用已进入金融行业的业务系统，但对于很多金融企业来说，机器学习和深度学习依然繁杂，算法模型使用困难，并且缺乏大量AI科技人才。针对这一困惑，新华三集团在2019年新华三领航者峰会上发布了软硬件一体化的人工智能支撑平台（AIOS），其支持TensorFlow、Caffe/Caffe2、MXNet/Torch、CNTK等主流计算框架。平台提供模型训练、模型评估、模型预测、模型导出、在线预测服务等功能，同时为了辅助用户管理开发资源，也提供了文件存储、资源监控、资源申请、工单管理等功能。为解决部署难的问题，平台提供基础软硬件集群环境的一键安装功能；通过AIOS可以实现资源的统一监管、作业监控、训练数据可视化、工程化的模型开发管理，满足用户的不同业务场景的开发需求。通过AIOS无需太多投资，即可将深度学习和机器学习用到实际业务中，帮助客户提高GPU资源利用率，降低AI实验室搭建成本；帮助AI专家脱离底层环境的困扰、更加聚焦于算法研究；帮助应用开发者快速上手构建第一个模型，降低AI技术门槛。

新华三自研关键业务服务器H3C UniServer R8900 G3重磅发布

紫光旗下新华三集团发布了全新一代自研8路关键业务服务器H3C UniServer R8900 G3，凭借其自身的高性能、可靠性和扩展性，在内测期间斩获德国红点奖，基于下一代处理器和卓越的架构设计，提供强大处理能力的同时，在存储能力、网络性能、扩展性和稳定性等诸多方面也得到了全方位加强。企业可以通过部署该平台解决多种重型工作负载，如核心数据库、高性能运算胖节点、内存计算、重型云计算及虚拟化环境等应用场景。

智能时代闪存演进 新华三推出全新一代关键业务存储系统Primera

8月8日，紫光集团旗下新华三集团（以下简称“新华三”）以“天生极智 · 闪耀未来”为主题在天津正式发布全新一代关键业务智能存储系统Primera。

全新的Primera存储系统不仅实现了存储介质从HDD到SSD的质变，更做到了前所未有的100% SLA。而通过存储协议、互联架构、控制器、OS和应用层面的创新，Primera也实现了在性能、体验和感知层面的全面超越，成为新时代核心存储产品的代表。

新华三关键业务智能存储系统Primera全新内核包括：

122%性能提升——在存储介质的选择上，Primera全面转向性能更高的SSD闪存介质，对应的存储协议也从之前的SAS升级为延迟更低的NVMe。

100%系统可用性——Primera还提供了包括横向扩展和纵向扩展在内的多种无需停机的升级方案，以满足不同用户的现实应用需求。同时，借助新一代全互联架构控制器，只要节点中的任意一个仍旧在线，整套存储系统便不会中断。

降低93%部署时间——在硬件全面进化的基础之上，Primera还完全重构了存储的软件功能，将过去环环相扣、层层嵌套的存储功能彻底拆分为相互独立的数据服务，从而实现无需重启且方便灵活的升级与维护。

新华三发布5G融合解决方案 引领5G融合应用之路

新华三成功发布“5G融合解决方案”，围绕产业的核心需求，以全云化的理念，积极促进电信业务与政企业务的融合，让技术更好的惠及产业发展，提升各个应用之间更为高效的有机协作，促进运营商业务与政企业务的充分合作。该方案的发布不仅是新华三为产业打开发展空间的全新尝试，也提供了一种更具价值的商业发展模式，由此揭开5G时代下，新华三数字大脑计划促进5G与行业深度融合的序章。

紫光恒越项目开工仪式在杭举行 打造萧山数字经济新名片

2019年8月5日，“紫光恒越自主创新实验室和数字化产品研发生产基地”项目正式启动，作为萧山区数字经济新名片的“领头”项目，紫光恒越项目将充分利用5G、工业互联网、人工智能、虚拟现实、工业机器人、无人工厂等最先进的工业4.0与数字化技术，结合最先进的生产运营管理实践，打造出国内领先的智能制造基地，并形成可复制的数字化工厂解决方案。项目建成后，紫光恒越将为国家网络安全自主创新领域提供新一代通信网络、计算、存储和信息安全等先进产品。

重庆市政府与紫光集团签订项目合作协议 唐良智会见紫光集团董事长赵伟国并见证签约

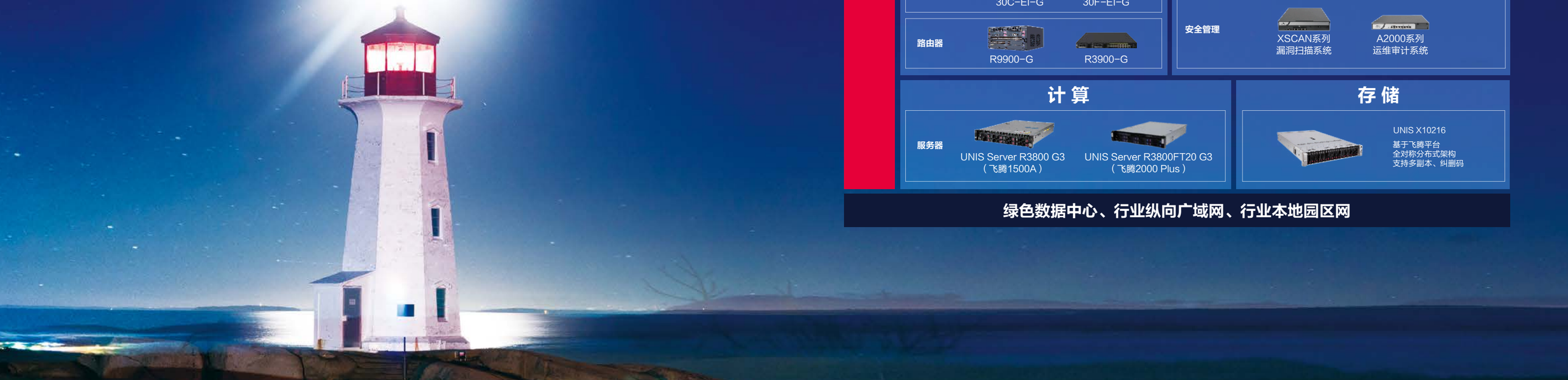
重庆市政府与紫光集团签订重庆紫光存储芯片产业基地项目合作协议，双方将聚焦存储芯片领域开展全方位深层次合作，共同加大产业投资，在渝组建存储芯片领域核心产业集团，设立紫光国芯集成电路股份有限公司和重庆紫光集成电路产业基金。完善存储芯片产业链，在渝建设12英寸DRAM存储芯片工厂，布局包括DRAM总部研发中心在内的紫光DRAM事业群总部，建设紫光科技园，引入产业链上下游企业。

紫光恒越，网信安全捍卫者

关键资质　　核心技术　　知识产权

使命

作为网信安全捍卫者，致力于通过自主创新助力国家关键数字基础设施安全保障与网络治理体系建设。



UNIS产品全家福

拥有计算、存储、网络、安全、云计算、大数据等完整的自主创新数字化基础设施提供能力

运营管理

- 云操作系统 Cloud OS
- 云应用引擎 Cloud AE
- 云容器引擎 Cloud CE
- 运维中心 U-Center
- 大数据引擎 DateEngine

虚拟化层

- CAS 服务器虚拟化平台
- ONEStor 分布式存储系统
- SDN 软件定义网络
- VDI 桌面虚拟化平台
- UIS 超融合系统

基础架构

网络

数据中心级核心交换机

S12600X-08-G

高端多业务核心交换机

S8600X-03/06-G

CPU:飞腾/龙芯
交换芯片：盛科
FPGA：紫光同创
内存：紫光国芯

万兆汇聚交换机

S6600X-54XG-EI-G

千兆交换机

S5600-54C/30C-EI-G　　S5600-54F/30F-EI-G

路由器

R9900-G　　R3900-G

安全

网络安全

F5000-M06 多业务安全网关

F5000系列防火墙

F1000系列防火墙

T5000系列入侵防御系统

T1000系列入侵防御系统

应用安全

ACG1000系列网络安全审计系统

W2000系列Web应用防火墙

D2000系列数据库安全审计系统

安全管理

XSCAN系列漏洞扫描系统

A2000系列运维审计系统

计算

服务器

UNIS Server R3800 G3（飞腾1500A）

UNIS Server R3800FT20 G3（飞腾2000 Plus）

存储

UNIS X10216

基于飞腾平台
全对称分布式架构
支持多副本、纠删码

绿色数据中心、行业纵向广域网、行业本地园区网

媒体专访

应势而生，新华三发布“数字金融架构”

——专访新华三金融事业部总经理李乔

文 / 转载金融电子化记者专访文章

2015年12月16日，习近平总书记在第二届世界互联网大会开幕式上宣布：“中国正在实施‘互联网+’行动计划，推进‘数字中国’建设”。正是从这一刻起，吹响了我国全面数字化的前进号角，各行各业纷纷提出自己的数字化发展战略。金融业更是不甘落后，“数字金融”—“数字银行”、“数字保险”、“数字证券”成为各大金融机构未来一段时期最重要的发展方向。

国家网信办2018年5月发布的《数字中国建设发展报告（2018年）》显示：2018年中国数字经济规模达31.3万亿元，占GDP的比重达到34.8%。可以说，数字化已经成为驱动经济转型升级的重要动力引擎，同时金融数字化能力也成为全社会数字化水平的重要指标。

面对蓬勃兴起的数字化大潮，紫光旗下新华三集团通过加速整合产品线，持续在研发方面发力，推出适应行业数字化转型需求的新产品和解决方案。特别是针对金融行业，在云计算、人工智能、大数据等技术领域深耕，推出了一系列金融行业的解决方案。

记者

当前的金融业，正处于多重变革期，既有数字化变革的推动，又有深化金融供给侧结构性改革的需要。同时，以云计算、人工智能、区块链为代表的新兴技术的风起云涌，给传统金融业的管理模式、运营模式、服务模式等，都带来极大的改变。在您看来，这样一个时期，金融业需要如何应对这些变革？

李乔

“互联网＋”战略和“数字中国”发展战略的提出，为中国的经济发展提供了崭新的驱动力。金融行业也顺应互联网化、数字化的浪潮，在金融科技的引领和推动下，谋求商业模式的变革。网络支付、供应链金融、智慧网点、开放银行的兴起，充分说明了科技在金融产品创新中的巨大作用。

我们认为，金融行业在步入全面云化时代之后，已经开始向智能化方向持续演进，即从“互联网+”向“智能+”演进。随着移动互联网的高速发展，以及即将到来的物联网时代，在5G和“智能+”的推动下，人与人的互联、人与物的互联，以及人机融合，将使全社会的数字化发展迈入新阶段。随着金融行业数字化能力的不断提升，越来越多的金融机构开始运用金融科技将场景服务向外延伸。未来，“数字金融”将成为主要发展方向，无摩擦服务、无缝衔接、实时体验、高效监管、安全等将成为数字金融的几个明显特征。而数字金融发展需要三个核心能力——数字化、网络化、智能化，这三个能力我们认为不是金融科技演变的路径，而是在各自的纬度当中不断发展，并且互相影响互相促进。

记者

新华三集团推出了“数字金融新架构”，并提出“通过数字金融架构的“4+N”模式与合作伙伴一起共同赋能行业数字化转型”。请您剖析“数字金融新架构”的内涵，以及如何推进金融业数字化能力建设?

李乔

在数字金融成为主要发展方向的趋势下，新华三发布数字金融架构，通过“4+N”模式与生态伙伴共同赋能行业变革。“4+N”听起来似乎有点抽象，其实它们都是实实在在助力企业快速平稳实现数字化转型的有力平台、工具、方法和路径。其中，“4”是依托紫光集团和新华三强大的平台技术能力构建行业使能的智能数字平台，包括以ABC融合平台和数字中台为核心的业务能力平台、数字基础设施、主动安全和智能运维；“N”则是在智能数字平台的基础上与生态伙伴和客户共建数字金融应用生态，为金融行业客户提供全面的数字化、智能化业务支持。新华三智能数字平台与金融行业客户的数字化需求、应用结合在一起，构成完整的“数字金融架构”。

新华三致力于将数字化技术转变为贴合用户场景需求的全栈解决方案，通过移动互联、边缘计算、IoT等技术方案对接各类数字化场景，助力金融实现无缝衔接；通过以ABC为核心的业务能力平台使能无摩擦服务，特别是AI能力的引入，让金融数字化、智能化的升级有的放矢。今年，新华三在其人工智能平台和PaaS平台中加入了很多金融行业的应用属性，希望通过一两年的快速迭代，为金融客户提供更加强劲的智能化支撑。近些年，新华三在智能化领域不断加大投入，一方面在自身解决方案中全面引入智能化能力；另一方面，构筑智能化应用支撑平台，对接各类智能应用。这些改变体现在产品端，就是一系列创新产品和平台的推出，比如AIOS人工智能平台、数据计算引擎DataEngine（Hadoop/MPP集群），以及对接金融云不同场景和特性需求的IaaS及PaaS平台等。

记者

AIOps成为今年金融行业年度热词，智能运维也是大势所趋。作为金融行业智能化应用的一个典型场景需求，新华三华重点推出了哪些平台和方案?

李乔

智能化在金融行业虽然用得很多，但运维系统是科技部门唯一的业务系统，运维系统对其自身提高故障的排障能力，对上层应用提供保障能力至关重要。在运维系统方面，新华三致力于成为国内IT运维与运营服务的领先提供商。场景驱动，以智能化的方式重新定义运维，新华三推出了U-Center 2.0统一运维平台，同时发布了针对金融行业的五大运维解决方案，其中包括生态合作，例如与清华大学做AIOps智能运维共研。我们认为“科技+生态”是核心价值。金融科技不仅仅是技术，也是业务展现。通过运用金融科技构建底层基础平台，并在其上创新金融产品与服务，与专业技术服务商紧密协作，与表示层的用户共同构建起应用生态，形成良性循环发展的态势。这才是金融机构和专业技术服务商共同希望的结果。

记者

您曾谈到新华三推出的“数字金融架构”是面向金融的稳态和敏态融合的IT架构，应该说这种“双态融合”的架构转型理念更加符合当前大多数金融机构IT架构转型的现实情况与需要。请您介绍一些有关这方面的应用实践。

李乔

当今的金融业，极大地依赖金融科技的强力支撑。由于行业特性，其对安全、可靠性的要求远高于其他行业。特别是伴随着互联网金融服务的全面兴起，金融机构对基础设施的可扩展性有了更多的需求。

我们提出“双态融合”的技术架构，就是为客户提供安全、可靠、弹性的交付能力，我们称之为“稳态”和“敏态”融合的IT架构。核心业务承载需要高可靠、高品质的产品及解决方案，新华三不仅具备传统核心业务承载的广泛实践，而且在开放核心和云核心平台上也有很多成功实践，满足多场景的客户需求。值得一提的是，新华三助力中国人民银行清算总中心、中国太平洋保险等金融核心客户实现云化转型。新华三在践行全栈云服务战略的过程中，实现金融生产云、互联网金融云、行业云、开发测试云全场景落地。同时，作为SDN市场领导者，新华三拥有最丰富的金融SDN实践经验，在全生产环境规模部署SDN架构。截止目前，新华三为50+中国核心金融机构构筑新一代网络，包括大型银行保险金融机构、股份制银行、及城商农信等更多金融行业客户。在安全领域，新华三凭借全系列的AI防火墙以及态势感知系统，可实现全面主动化。区别于以前的被动，我们实现主动的防御及主动发现、预防，将引领主动安全防护进入智能新时代。

作为中国领先的金融云与金融IT基础设施提供商，新华三自成立以来创新成果显著（截至2019年5月底累计申请专利达10141件），具备计算、存储、网络、云计算、大数据、安全等全面的自主创新能力并成功向市场提供多款领先产品。未来，新华三全面自主创新与安全可靠的解决方案也将服务于更多金融行业用户。

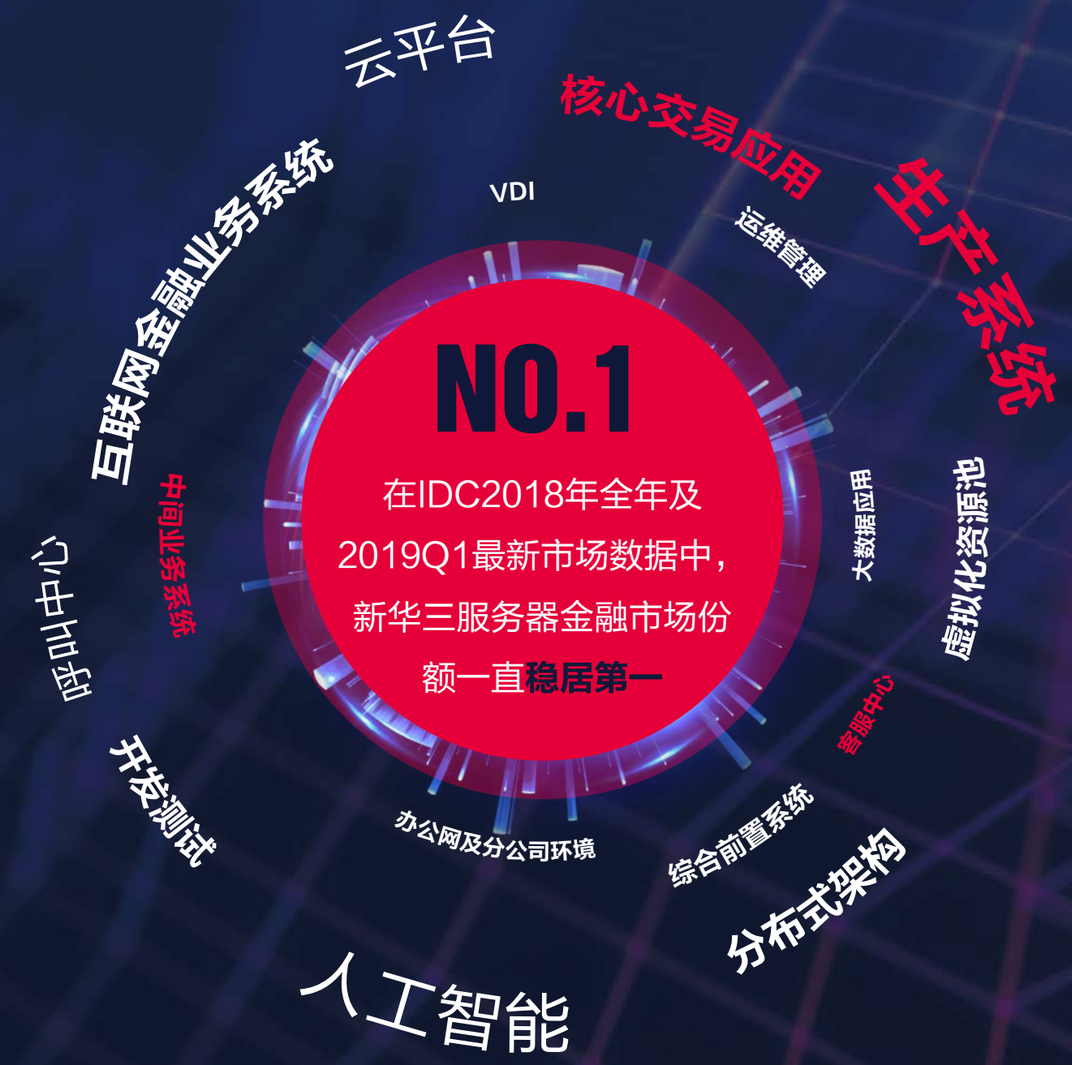
在金融行业智能化以及无边界化的大趋势下，新华三已经做好准备，将全面助力金融科技，共绘数字金融新未来!

紫光集团 | H3C
核心企业 | 数字化解决方案领导者

新华三**自研服务器**
在金融场景应用中大放异彩

在自研服务器产品线中，新华三不仅成功向市场推出工业标准服务器完整产品序列，更将研发重点放在新技术研发与产品的场景化领域。H3C UniServer服务器在30+核心金融机构实现规模部署，有力承载金融生产、核心等关键业务系统。

中国建设银行	中国银行	中国农业银行	中国邮政
中国农业发展银行	农信银资金清算中心	互联网金融协会	中国金融电子化公司
太平洋保险	中国人保	深圳证券通信有限公司	大连商品交易所
光大银行	北京银行	中国人寿	安徽农信
中原银行	中国邮政储蓄银行	中邮证券中国银联	上海银行
台州银行	北京农商银行	广发证券	国盛证券
交通银行	浦发银行	申万宏源证券	方正证券
红塔证券			



UniServer R4300 G3
为大数据应用定制的海量存储服务器

UniServer R4900 G3
在云化基础架构框架内提供
多维度均衡能力的2U双路机型

UniServer R5200 G3
在4U空间内部署最高20个
单宽GPU的AI负载优化型服务器

UniServer R6700 G3
在2U空间内提供四路处理器的
数据库业务服务器

UniServer R8900 G3
借鉴小型机设计思想追求极致单机可靠性
和模块化的关键业务服务器

UniServer B16000
紧跟市场趋势的塑合架构刀片服务器

安全与风控

郑商所数据中心
基础运维应急管理实践

文 / 郭建生、蒋三庆、张学谦

背景概述

郑州商品交易所（以下简称“郑商所”）是国务院批准的首家期货市场试点单位，是全国四家期货交易所之一，郑商所数据中心是承载期货交易结算和风险控制等期货业务的信息技术基础平台，将在未来10年或更长时间内运营其核心技术系统并向行业客户提供高质量托管服务，保障郑商所数据中心运营的安全极其重要。

郑商所数据中心基础运维部负责风、火、水、电等基础设施实时监控，定期定时巡检、预防性计划保养和应急预案制定等，为数据中心各类IT设备提供持续安全稳定的运行提供支撑。

郑商所数据中心投入试运营以来，发生过因大雨导致的积水、柴油发电机切换测试出现电缆温度超标等问题，基础运维部基于郑商所数据中心现在情况，梳理了应急场景，建立应急管理体系框架，并制定了应急管理综合解决方案和应急演练计划，形成定期进行桌面推演、模拟环境演练和生产环境演练机制，为数据中心的安全运营提供了保障机制。

应急管理体系框架

应急管理目标

应急管理目的在于针对不同的风险应急场景制定相应的应对策略和具体处置措施，以便在紧急事件发生后，有针对性地在第一时间，对特定风险应急场景有计划、有步骤地采取一系列处置措施，应尽可能在最短时间内使企业、组织、系统恢复正常运营，尽快恢复关键业务服务，并且在最大限度范围内减少该风险所带来的损失。

应急和故障的区别

应急管理	故障管理
应急事件 对用户层面或公司运营造成重大影响的业务支撑系统的关键业务不可用	**故障事件** 对IT基础架构中组件的非正常操作，从而导致或可能导致IT服务中断；降低或可能降低IT服务质量的事件
与故障的区别 从用户和业务角度出发	**与应急的区别** 从运行维护的角度出发
与故障的关系 故障处理是应急处理的基础	**与应急的关系** 引发应急 故障处理能力的提高可以提高应急能力

应急管理体系

针对本数据中心基础设施运维的特点，建立基础设施运维应急处理体系，应急体系建设原则如下：

- 总则：包括基础设施运维应急处理体系目的、工作原则、编制依据和适用范围。
- 数据中心基础设施运维应急处理组织指挥体系及职责：包括组织机构和职责、组织体系框架描述。
- 数据中心基础设施运维应急处理的预防和预警机制：包括对预防机制、预警监测、预防预警行动、预警分级和发布的介绍。
- 数据中心基础设施运维应急处理的应急响应：说明应急响应的阶段划分、应急响应各阶段的工作内容和要求。
- 数据中心基础设施运维应急处理的后期处置：包含情况汇报和经验总结、奖惩评定及表彰。
- 数据中心基础设施运维应急处理的保障措施：从信息资源、人力资源、财力资源、物力资源四个方面，说明为应对突发或重要事件所应配备的资源及相应的管理办法。
- 附则：包括名词术语和缩写语、预案的管理与更新、沟通与协作、制订与解释部门等内容。

应急管理综合解决方案

应急管理综合解决方案内容

应急管理研讨会

研讨会简介

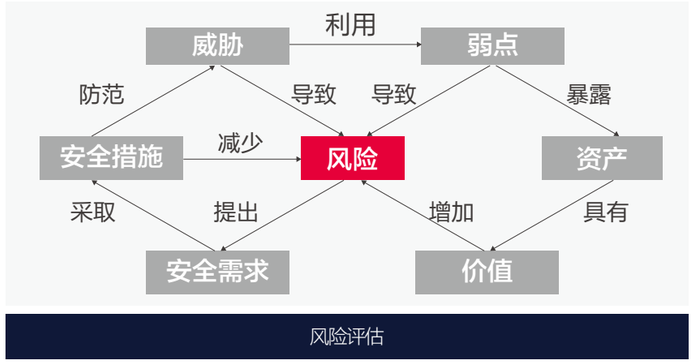
根据客户的特定需求，以研讨会的方式，针对应急管理相关内容和客户现状开展讨论，并分享HP在应急管理方面的经验。

研讨会目的

- 帮助客户系统了解应急管理的核心理念和方法
- 帮助客户建立规范应急管理的理论和意识基础
- 帮助客户梳理应急管理的思路与需求
- 帮助客户全面了解应急管理的有效实践内容，用以持续提升客户应急管理水平

研讨会内容

- 应急管理的范围与目标
- 风险定义及其两面性
- 风险分类与分级
- 风险评估机制
- 应急组织结构
- 应急管理流程
- 应急保障
- 应急管控
- 应急项目实施过程
- 应急实施举例

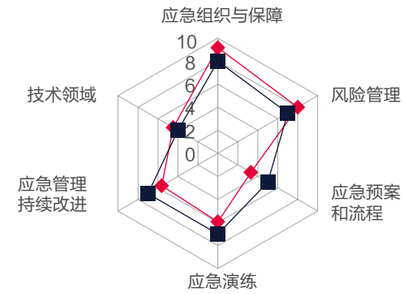


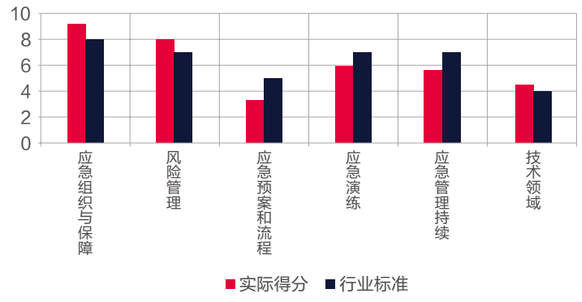
应急管理成熟度评估

采用业界应急管理标准以及最佳实践出发，通过了解郑商所数据中心的应急管理现状，对应急管理的成熟度进行评估，量化应急管理水平，识别差距并提出改进建议。

成熟度评估

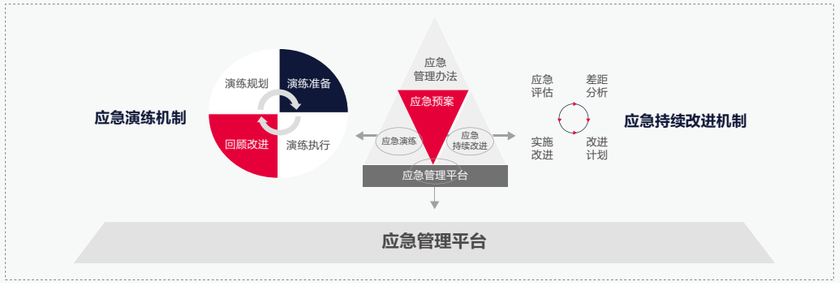
对评估结果进行分值量化，图形展示，将评估结果与业界标准对比，识别差距并提出改进建议。



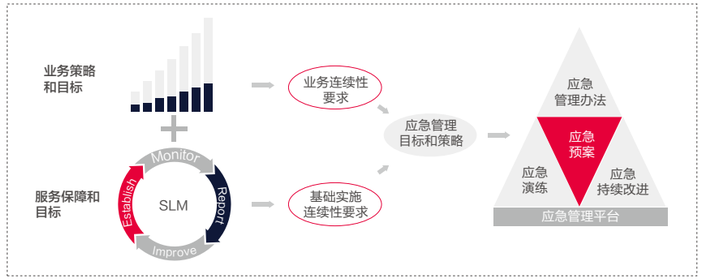


应急管理体系规划

应急管理体系规划以业务为目标，来保障业务的连续性和基础实施运行的连续性。



应急演练机制和持续改进机制的建立



应急组织、流程、应急保障的定义，以及构建风险管控机制

应急预案库的建立和RTO、RPO的确定

应急预案建立

应急预案主要内容

业务背景：应急场景跟什么业务相关？业务流程概述，本应急预案处于业务流程什么环节？

启动条件：简单明了说明发生什么故障时需要启用本应急预案，方便用户快速决策。

业务影响：上述故障发生时会影响哪些业务，会影响哪些用户？影响程度如何？

管理预案：本预案是否会触发其他应急预案？其他预案是否会触发本应急预案？

处置流程：应急预案最关键部分，详细描述应急处置流程和步骤。

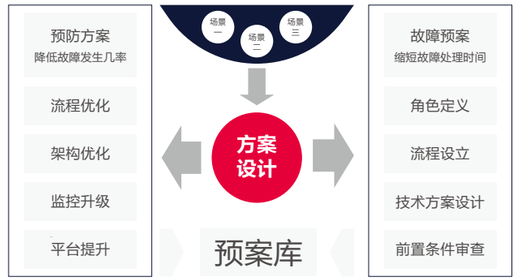
应急处置流程和步骤主要内容

应急处置流程：当业务不可用时，如何通过技术处置流程，使业务尽快恢复，满足业务RTO要求。这些技术流程包括：技术应急措施、切应急系统、切容灾系统。

应急恢复流程：当业务系统恢复功能以后，需要把业务恢复到正常处理环境中。应急恢复流程包括取消技术应急措施、从应急系统切回生产系统、从容灾系统切回生产系统。

回退方案：应急处理（特别是恢复过程），可能出现关键步骤无法继续，这时候必须尽快回退，保证业务连续性。

应急方案设计



应急预案梳理

从系统可用性的角度进行梳理，全面梳理和识别潜在的故障模式，基于风险量化结果，选取优先级较高的故障模式来制定相应的技术处置措施。

实施应急演练

应急演练的总体目的是保障在重大突发事件出现时，应急处置及时有效，指挥调度迅速有序，信息沟通渠道畅通，信息口径统一、内容准确，尽可能在最短时间内恢复业务正常运行，以达到缩短故障历时，降低业务影响，有效防范和化解业务风险，降低损失的目标。

事件优先级定义

优先级代码定义：

优先级代码		影响范围			
		一级（最高）	二级（中级）	三级（中级）	四级（中级）
紧急度	一级（紧急）	1级	1级	1级	1级
	二级（高）	1级	2级	2级	2级
	三级（中）	1级	2级	3级	4级
	四级（低）	1级	3级	4级	4级

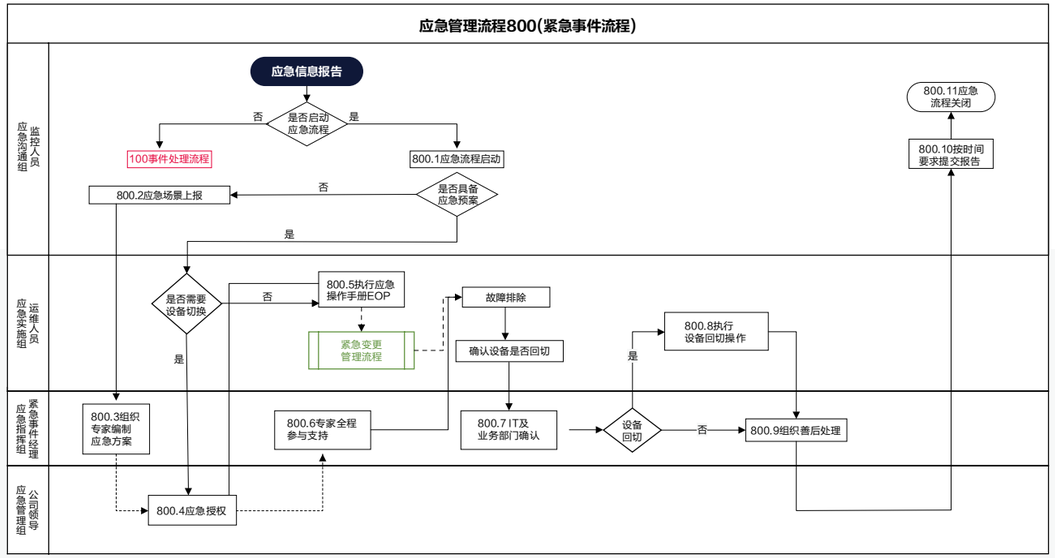
事件影响度用于衡量影响业务的严重程度：

编号	影响度代码	描述
1	一级（重大）	• 导致交易盛程序化交易系统停止，或停止1小时没有解决 • 交易系统不能在允许时间内切换至灾备系统
2	二级（严重）	• 非核心交易系统停止
3	三级（一般）	• 不影响交易系统
4	四级（轻微）	• 不影响交易系统以及IT相关服务请求

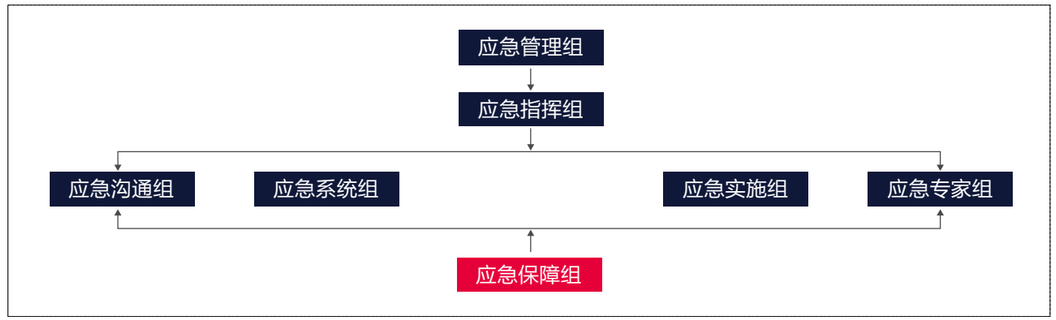
紧急程度决定事件需要处理的急迫程度：

编号	紧急度代码	描述
1	一级（重大）	• 交易系统停止，或停止1小时没有解决 • 技术中心2楼核心机房/1-2机房断电，且没有备用供电支持
2	二级（严重）	• 交易系统将要在2-4小时内停止，或有停止的风险，并且不能解决 • 技术中心2楼核心机房/1-2机房断电，有备用供电支持 • 仅有1路电源供电给2楼核心机房/1-2机房 • 2楼核心机房/1-2机房没有冗余精密空调支持
3	三级（一般）	• 仅有1路电源供给某个机房，不包含2楼核心机房和1-2机房 • 某一个机房精密空调没有冗余支持，不包含2楼核心机房和1-2机房 • 仅有1路电源供给某个机柜
4	四级（轻微）	• 冗余精密空调故障，不包含2楼核心机房和1-2机房 • 服务请求 • 巡检维护

应急演练流程图



应急演练组织架构



应急管理组

在应急管理中要做出决策的角色，通常由公司管理层担任。

应急指挥组

在应急管理中指挥整个应急过程的角色，通常由部门主管或业务主管担任。

应急沟通组

在应急管理中起沟通和协调的角色，通常由ECC值班组长担任。

应急实施组

在应急管理中参与制定和实施应该方案的角色，通常由运维工程师担任。

应急专家组

在应急管理中对应急事件进行分析和指导，参与制定应急方案，通常由二线、三线专家担任。

应急保障组

在应急管理中对应急事件提供后勤、安全的支持，通常由行政、安保、物业等部门担任。

应急管理平台

郑商所数据中心应急管理平台

演练方式：模拟环境演练　**演练场景**：ATS BO1切换故障应急演练　**应急紧急度**：二级

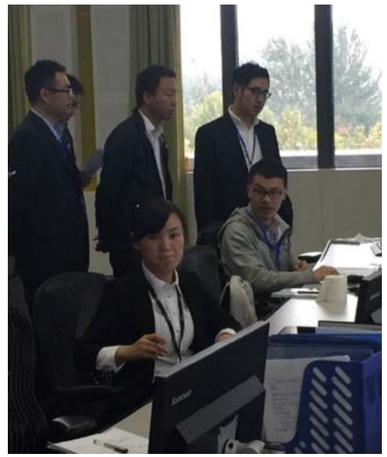
应急操作状态

#	应急流程节点	负责人	执行操作	操作内容	完成情况	状态	备注
1	紧急事件通知	ECC	建立应急响应电话会议 通知相关责任人	● 建立应急电话会议、接通相关人 ● 应急事件简述：包括发生的时间、地点	100%	已完成	
2	紧急事件分析	事件经理	事件的详细分析 （值班班长参加）	● 应急事件详情：包括发生可能的原因 ● 应急事件的影响度、紧急度		正在进行	
3	紧急事件通报	指挥组长	紧急事件通报和升级	● 应急事件通报至相关部门和人员 ● 应急事件升级给管理层			
4	应急方案确认	事件经理	确认应急方案	● 使用现有应急方案 ● 形成应急方案			
5	应急方案 实施授权	指挥组长	指挥组长向应急 领导申请获取授权	应急方案概述、实施时间			
6	应急方案实施	实施组	实施应急方案	按照应急方案实施、检查			
7	应急实施完成	事件经理	确认实施完成	● 实施完成后的检测 ● 通知相关方实施完成、恢复操作			
8	应急总结报告	事件经理	制作应急报告	此次事件及应急措施的总结和回顾			
9	应急方案优化	事件经理	优化应急方案	更新应急预案库			

应急操作状态：应急操作状态 / 应急组织架构 / 应急管理联系方式 / 应急等级定义 / 应急操作流程 / 应急预案库

郑商所数据中心应急管理平台对应急管理提供了支撑，跟踪和显示应急演练的主要运行节点，快速查询应急组织架构、联系方式、应急等级定义和操作流程，管理应急预案库。

应急演练实施



郑商所数据中心应急演练实施场景的选择、方案制定、从脚本定义、演练动员和培训、演练实施和总结分析的过程。

应急管理的总结和展望

CONCLUSION

应急管理通过建立应急框架体系、应急管理综合解决方案和应急演练，从而形成应急预案库，保障在重大突发事件出现时，应急处置及时有效，以达到缩短故障历时，降低业务影响，有效防范和化解业务风险，并且在最大限度范围内减少该风险所带来的损失。

目前郑商所数据中心应急管理的架构、应急综合解决方案和应急演练机制已经形成，应急架构、方案和演练不断优化，桌面推演、模拟环境演练、生产环境演练按照计划在实施，对已经发生的故障提炼出应急场景，对现有的风险进行分析并形成应急场景，进而对应急场景的不断演练，固化成应急预案，从而快速应对可能出现的急紧情况和提高处理紧急事件的能力。

应急管理综合解决方案将在跨部门跨专业间进行，训练不同部门和专业间的协作和配合能力，应对更复杂的问题和事件。应急管理平台将在流程自动控制，和监控系统的联动方面进行优化，使得郑商所数据中心应急管理能力更上一层楼，为郑商所的商品交易业务保驾护航。

“云等保”解读

新华三云等保解决方案

文 / 新华三集团云安全解决方案部部长 贾楠

随着云计算技术的成熟和稳定，众多企业、政府等客户上云速度的加快，金融企业出于自身成本、运维效率和资源弹性伸缩的考虑，也在积极启动金融云建设。金融行业的业务数据都是真实公民的账务数据，因此相比于其他行业，金融行业对数据的机密性、完整性、真实性有着更高的要求，要严格防范泄露和篡改，对不同安全等级的网络也需要实行严格的分区及隔离。

金融行业重要的信息系统，是国家信息安全重点保护对象，因此金融行业是落实和实施信息安全等级保护的重点行业之一。《网络安全等级保护基本要求》等系列标准的发布，标志着国家网络安全要求进入了2.0的时代。2.0要求和1.0相比，最大的变化莫过于涵盖了云计算、物联网、工业控制和大数据等新的技术领域。尤其是在云计算安全方面，业务、数据等上云后，安全问题不再由用户方独立负责，更多的依赖云平台的安全防护等级以及能够提供的安全能力。云计算安全扩展要求即“云等保”的出台，无疑为云安全建设思路指明了方向。

和通用安全要求一致，云计算安全也将围绕“一个中心，三重防护”的思路进行建设。一个中心指安全管理中心，三重防护包括安全通信网络、安全区域边界、安全技术环境。“云等保”中也重点对这四个方面进行了详细的要求阐述。但又与传统网络不同，云计算环境中存在云平台和租户多重视角，从而使得云网络更加立体，防护手段也需多维立体。

图1 一个中心三重防护思路框架

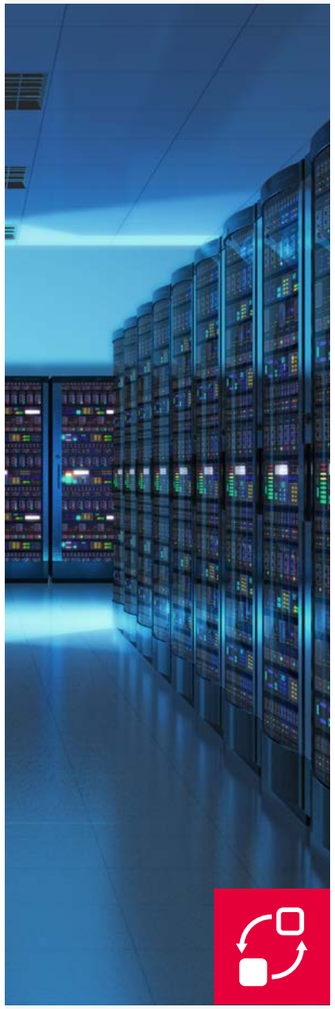
云等保的出台，对云网络安全建设方案提出新的挑战：

金融云网络如何分区分域?

分区分域一直以来都是等保要求的核心保障，做好区域划分是网络安全等级保护的第一步。而云计算网络的优势则是动态的、弹性的、可扩展、可迁移的，难以将边界固定下来。业务上云后，如何恢复安全域的划分和隔离，一直是困扰用户的问题。当前金融数据中心的组网安全架构，主要依据《人民银行信息系统信息安全等级保护测评指南》所提出的安全域模型，其中提出“通过划分安全域的方法，将金融行业信息系统划分为不同的安全域，并针对每个安全域给出相应的保护措施，从而建立纵深防御体系，实现深度防护的目标。同时，《人民银行信息系统信息安全等级保护测评指南》中还要求“原则上禁止从外联区直接访问内部网络”，因此内网业务区域与外联区域无法合并。上述几项要求成为金融数据中心分区分域的基本原则。

云租户如何配置安全策略?

传统网络中，安全的建设和运维仅由用户独立负责，金融用户可直接维护安全策略；而云网络中，安全产品主要部署在云中，用户接触不到实际环境，对用户来说可能形成一个管理盲区，用户方作为其中一个租户，无法完全自主掌控策略。而在云等保中，提出了“应具有根据云服务客户业务需求自主设置安全策略的能力”，对租户维度的策略管理能力提出了明确的要求，使得金融用户可以根据自身需求从服务目录中选择安全能力。



如何通过云平台实现安全资源的统一管理?

等保2.0和1.0相比，着重强调了集中管控，要求“应能对物理资源和虚拟资源按照策略做统一管理调度与分配”。云计算环境中，存在资源分配、调度等操作，管理、维护成本更高。另外，云网络与传统网络相比又增加了运营属性，金融云平台应能够实现安全资源的统一管理，则会有利于形成一体化的运营。

新华三云等保解决方案

新华三集团，通过多年网络安全领域技术的积累并结合丰富的金融云项目建设经验，提出了“云网安一体化”建设方案。通过将安全资源池与云平台的深度融合形成“一个云平台三种资源池”的云安全等级保护解决方案。

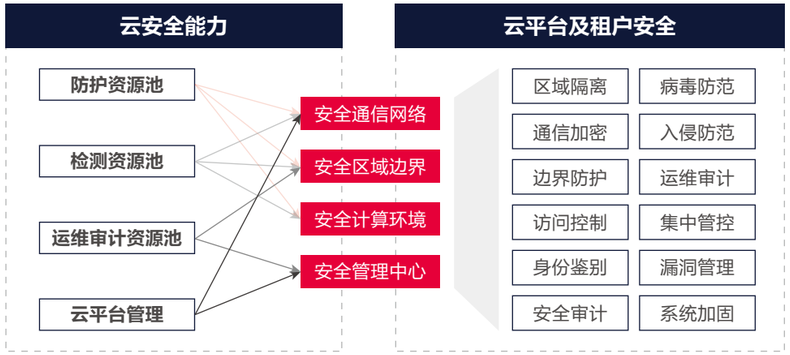


图2 云安全等级保护方案

三种资源池包括了防护资源池、检测资源池、运维审计资源池，一个云平台指的是仅需通过一套云管理平台即可实现安全资源、网络资源、计算资源的统一管理。安全能力覆盖区域隔离、通信加密、边界防护、访问控制、身份鉴别、安全审计、病毒防范、入侵防范、运维审计、集中管控、漏洞管理、系统加固等。

新华三集团多年来一直致力于打造安全即服务的云计算平台，将安全能力资源化，并作为一种云端服务提供给租户。租户登录云平台后既可同时申请网络、计算、存储、安全等多种资源，又可以在云平台上直接配置和管理，既可满足等保要求的安全策略管理和集中管控要求，又能按需购买、灵活部署，进而实现成本投入的合理规划。在云安全等级保护方案中，通过将安全和网络打通形成有效的边界防护，利用VPC技术以及安全服务链技术实现云网络的分区分域，通过东西防护资源池与SDN控制器的配合完成VPC内部的区域划分，进而形成虚拟数据中心的三级网络划分。

图3 安全即服务

新华三成功为某大型保险公司云等保建设提供咨询服务，解决方案的设计充分考虑了网络安全等级保护的基本要求和安全设计要求，面向云化安全技术框架，实现弹性扩展，自适应安全防御，模块化、独立生存和服务的能力，同时符合网络安全法、等保等监管合规要求；满足数据保护、关键信息基础设施合规要求，为用户打造既合规，又实用的安全云环境。

新华三能为用户带来的价值包括：

整体交付

新华三集团是为数不多的具备云、网络、安全整体交付能力的综合厂商。云、网络、安全深度融合，形成安全与网络协调联动、安全和云的高度集成。丰富的金融云实施经验可为用户提供成熟的实施解决方案。

安全合规

新华三云等保解决方案充分适配等保要求，除安全技术能力外，还具备强大的安全服务能力，能更好的应对等保要求中安全技术和安全管理两大部分。同时，安全服务能力也与云平台形成联动，用户可在云端申请安全专家服务，即可体验风险评估、安全协维、渗透测试、应急响应等服务。

成本节约

新华三云等保解决方案以软件定义安全为核心，将安全服务化。用户可以根据不同业务系统所需的不同安全等级的，按需使用，而不需要按传统方式前期购置大量的软硬件设备。大大的节约了成本。

新华三全场景物联网方案
助力金融风险防控

文 / 新华三物联网解决方案 杜利征

随着物联网、云计算和大数据等数字化技术的发展，百行百业拥抱数字化转型的步伐也在不断加快。金融一直是数字化技术应用落地的先锋行业，全渠道的数字化运营已成功应用云计算和移动互联网技术。伴随物联网技术的成熟，越来越多的银行客户开始借助物联网技术实现银行精细化管理，构建完整的数字银行。

物联网，即将无处不在的业务设备（如资产抵押物等），通过有线/无线、长/短距网络连接技术实现互联互通，借助物联网平台进行数据汇聚与应用集成，在专网或互联网环境下，采用适当的信息安全保障机制，提供远程资产管理、安防监控等垂直场景应用。新华三结合多年服务银行客户的经验，提供从抵押物监控、银行网点环境监控到银行园区安防的全场景解决方案。

物联网助力金融抵押物实时监控

银行“贷后管理”即贷款发放或其他信贷业务发生后到本息收回的全部信贷管理行为，包含贷款资金管理、日常检查和风险预警和贷款收回等。当前贷后监管面临如下挑战：

- 由银行定期派人现场检查、人力成本高，重复的贷后调查工作消耗了大量的人力和时间；
- 原有贷后调查流程及时性差造成不能及时掌握重要抵押物的情况；
- 当前贷后管理完全依赖信贷人员的反馈，信息不对称造成内部管理漏洞。

图1 资产管理平台

针对贷款管理中的日常检查和风险预警，新华三利用自身网络、定位技术及强大的平台能力，提供针对金融抵押物监控的整体方案，可对贷款企业抵押物进行远程监控，准确反映抵押物安全情况。

方案由UWB定位终端、WLAN承载网络、绿洲物联网平台和资产管理平台共4部分组成。在贷款企业的抵押物上部署UWB定位标签，抵押物的位置信息可通过物联网平台采集后发送到资产管理平台。基于UWB定位技术，可实现抵押物在30-50厘米的高精度定位。依托资产管理平台，通过对抵押物的位置进行实时监控，可建立电子围栏，一旦抵押物离开电子围栏，即可触发告警。资产管理平台还可提供资产自动盘点、轨迹回放和资产标签拆卸告警等功能。

通过物联网技术对贷款企业抵押物进行无遗漏监管，可提供银行贷后管理效率、降低贷款风险。

物联网助力银行网点精细化管理

目前各大银行已提供虚拟柜台机等客户自助服务，有部分银行已建立了“无人银行”。银行开始依托数字技术为客户提供了线上与线下融合的服务，而在银行网点本身的安防和消防等环境信息尚没有数字化手段进行实时监控。为了帮助银行为客户提供一个安全、舒适的银行网点环境，新华三提供银行网点环境监控解决方案。

图2 数字园区综合管理平台

整个方案基于低功耗LoRa物联网技术作为网络承载，包含环境感知终端、低功耗LoRa网络、绿洲物联网平台和数字园区综合管理平台共4部分组成。方案通过绿洲物联网平台进行各类物联网终端的数据汇聚，同时可与网点视频监控等系统进行数据联动。环境感知终端包含无线烟感报警器、温湿度探测传感器、无线应急按钮终端和用电安全监测设备。以无线烟感报警应用为例，一旦出现吸烟或者火灾引起的烟雾，可立即进行现场报警，同时报警信息同步到数字园区综合管理平台，支持通过发短信、打电话等方式通知安全管理员等责任人员。

通过低功耗物联网技术采集银行网点的消防、温湿度、紧急呼叫和用电安全数据，可实现银行网点的精细化管理，提高银行网点的运营效率、提升客户满意度。

依托物联网构建银行园区的两道安全防线

银行作为高安全级别机构，安防是银行园区建设的重点。目前所有银行园区都已构建了基于IP摄像头的视频监控系统，但视频监控大部分是在事后才能发挥作用，不能提前杜绝安全事件的发生。新华三针对银行当前在园区安防所面临的问题，提供智能“门锁+门闸”安防物联网解决方案，帮助银行客户构建园区两道安全防线。

第一道安防防线：人脸识别门闸

传统的银行园区面临外来人员随意出入，存在安全隐患。当前银行园区管理者的通常做法是增加安全管理人员进行监管，但由于出入人数庞大及高度集中，这种办法收效甚微。新华三推出基于人脸识别安全认证的门闸方案。整个方案的核心由人脸识别门闸硬件和信息管理系统软件两部分组成。银行员工提前在信息管理系统录入人脸信息，通过人脸识别门闸进行安全认证后可放行员工出入园区。信息管理系统提供员工出入信息记录，同时可与员工考勤等系统进行打通。银行园区人脸识别门闸的建设，可有效防止未被授权人员进出银行园区，从很大程度上提升了银行的安全化管理程度。

第二道安防防线：智能门锁

银行园区内办公场景的出入安全同样非常重要。特别是针对银行内部高机密的房间，采用传统机械门锁的方式，员工出入记录无法查询。同时传统钥匙易复制，若私下被复制，会出现安全管理漏洞。新华三推出针对园区办公场景的智能门锁方案，方案的核心包含无线联网智能门锁和智能门锁管理应用。无线联网智能门锁可支持指纹、密码、一卡通、微信小程序、管理应用和机械钥匙6种开锁方式。通过智能门锁管理应用，可实时记录什么人，在什么时间、采用何种开锁方式等信息。银行部署无线联网智能门锁，授权的员工才可进入房间、同时员工开门记录实时上传，加强银行办公区安全管理手段、提高了智能化水平。

物联网的本质是数字化物理世界，物联网技术与人工智能、区块链等数字化技术的融合将为金融行业提供更丰富的产品及服务创新。新华三聚焦“绿洲物联网平台+丰富网络连接技术”物联网核心能力，面向银行各类场景提供端到端解决方案，帮助银行客户构建完整的数字银行。

先智先觉 守护平安

新安防 4 大优势

应用驱动

以应用为驱动，以实战为目标，效果体验释放平台技术架构优势、基础硬件性能优势和算法多样性优势。

全面云化

面向海量数据接入、计算；灵活构建、资源动态调度，充分利用算力和存储，节省成本。

全栈智能

算法仓库和软件定义实现端、边、云、网的智能协同，快速响应客户不同场景的需求。

开放生态

应用、算法、视频云、软件定义摄像机全部开放、分层解耦、可融合业界最先进技术构建最优方案。

重庆紫光华山智安科技有限公司 | 网址：www.unisinsight.com | 客户服务热线：400-688-6363

紫光华智官方微信

H3C 数字化解决方案领导者 | 紫光华智 UNISINSIGHT

软件定义摄像机

有生命力的摄像机

开放平台

摄像机平台化，软件和硬件解耦，系统和算法解耦

应用生态

开放平台之上搭建应用生态，按需加载各种算法

自我生长

算法与时俱进，持续更新迭代

智能协同

赋能原有普通摄像机，使普通摄像机具备等同于智能摄像机的能力

有视觉的边缘计算平台

视图云存储与极云

视图云存储——智能安防基石

稳 | 快 | 灵

极云——园区智能安防大脑

业务功能 | 智能性能 | 智能应用 | 平台管理

解析平台与视图库

解析平台

- 算法全面开放、按需动态调度
- 更兼容，更精准，更灵活

视图库

- 多维融合，高并发，高速查询历史数据，数据库容按需扩展

以科技和风险控制能力为依托，**推进开放平台战略**

文 / 访马上金融首席技术官 蒋宁

导言

从2009年中国银监会颁布《消费金融公司试点管理办法》至今，消费金融已经发展十年。

十年来，24家消费金融公司先后成立。他们不仅丰富了我国的金融机构类型，促进了金融产品创新，而且为银行无法惠及的个人客户提供了新的可供选择的金融服务。

2009年，银监会在北京、上海、成都、天津四个城市率先启动消费金融公司试点工作，2013年消费金融公司试点增至16个城市。随着政策的支持和互联网经济的快速发展，2015年-2017年迎来了高速发展阶段，消费金融公司试点扩大至全国范围。

2015年6月，马上消费金融批复开业。作为第二批试点的消费金融公司，马上消费金融没有像第一批消费金融公司依赖于线下模式展业，而是逐步形成了以科技为驱动线上线下相结合的商业模式。目前，马上消费金融已跻身消费金融公司前列，提出聚焦开放平台，在云平台、人工智能、大数据、区块链、生物识别五大技术持续创新，重点布局金融科技与零售科技两大领域的战略目标。

根据已披露的2019年上半年19家消费金融公司的业绩数据，从资产规模看，马上消费金融以511.11亿元位列第三名；在净利润方面，以3.01亿元位列第四名。

近日，马上消费金融CTO蒋宁在采访中表示，马上消费金融三大业务板块；同时，对其业务模式、智能贷后管理、客群上移、息费降低以及发展趋势等热点问题进行了解读，并加以探讨。

马上消费金融提出，希望到2020年业务可以达到442的占比，40%是自营、40%是开放平台、20%是金融云。蒋宁解释，开放平台的战略核心是以公司的科技能力和风控能力为依托，有效拓展非风险利差的业务收入。我们会在几个方面，加强开放平台的建设。一，积极构建资产和资金撮合平台，需要满足不同风险水平的资产端和相应风险偏好的资金方的适配。二，是推进智能化金融云平台的产品化和商业化，包括风控云，催收云，客服云的对外服务体系的建设。

他提出，行业未来五大发展趋势，场景金融是发展方向，建立万物互联的能力；打造轻资产的运营模式，如开放平台模式；用户体验决定一切，打造极致的用户体验；提高运营效率，减少边际服务成本；注重产品服务创新，提供智能化服务水平。

在技术方向上，他指出，马上金融已经发展了四年，未来五年要升级科技平台的能力，包括私有云和人工智能；去年私有云已经开始导入，之后会进一步优化私有云能力。

三大业务模式：自营+开放平台+金融云：40%+40%+20%

马上消费金融的科技能力是如何在三大业务上体现的?

蒋宁：从开放平台的战略来讲，开放平台是从利差的模式转为服务模式，所以科技是我们最重要的手段。开放平台的战略包括2个部分：积极构建资产和资金撮合平台，需要满足不同风险水平的资产端和相应风险偏好的资金方的适配。二是推进智能化金融云平台的产品化和商业化，包括风控云，催收云，客服云的对外服务体系的建设。

从资产和资金端来讲，资产的收益率不同，资金诉求不同以及资产的风险水平不同，需要资产的收益率水平和资产的偏好对接上。对接不同类型的资产是否能有足够的风控能力，这在

业界还是比较挑战的。但是马上已经具备了风控经验，整体上，我们对应了180多个场景，对应不同渠道的资产和不同风险级别的资产。

在金融云方面，现在已经有70多家贷后管理公司用我们的系统，有近20家持牌或者大型的机构使用我们的贷后管理平台。我们希望客服在云上，现在正在完善相关的技术产品工作。

在自营业务方面，我们逐步对优质客户提供20万元以内的大额信贷产品。相对来讲，马上大额信贷产品占比较小，现在需要投入大额信贷产品的研发，例如建立新的风控模型。

马上消费金融的开放平台业务，与同行相比有什么不同?

蒋宁：马上金融与很多场景都合作过，有很强的风控能力。另外，我们的风控是具备差异化的能力。并且，马上金融作为持牌机构，在资金端和数据源的优势会越来越明显。目前，开放平台已经对接了十多家银行几十家场景方，包括滴滴和唯品会等。

智能贷后管理

是否可以结合扫黑除恶的环境下，介绍一下智能催收?

蒋宁：贷后管理是集用户体验、合规和管理效率三个方面平衡的一个领域。首先，让用户体验好；第二是符合法律法规；第三是需要高效。在这三个方面，科技可以起到很大作用。比如，智能贷后管理完全没有人的介入。我们对用户有几十个分群和几百上千个执行策略，按照不同的客群提供差异化的用户体验，使用不同的手段、不同的话术、不同的策略进行回款。

智能催收意义在哪里?

蒋宁：第一，是智能化和多轮对话的挑战，使它接近人的效果。第二，更看重合规的效果，用户体验更好。

由于机构各自定位、业务产品以及用户客群的不同，是否会为不同的机构提供不同的贷后管理系统?

蒋宁：是的，我们可以提供平台、决策引擎、基本策略和模型，并且提供咨询方案。第一个方案，与我们业务形态相似的机构可以用我们的系统，把客群导过来。第二种方案，与我们的客群差异比较大的机构，可以由我们来帮助他们做这块业务。

业务模式

马上消费金融是打造线上线下相结合的产品线，线上的成本是否较线下便宜？怎么评价马上消费金融的线下业务?

蒋宁：首先，线上线下相结合的模式使马上金融覆盖的人群更加广泛，展业的范围更大，从而可以锻炼马上的风控能力。线上和线下人群是有显著差异的，线下有征信记录的人非常少，其中80%-90%是征信白户；而线上持有信用卡的人比例可以达到60%以上。

第二，线下业务与消费场景联系的更加紧密，对把控风险是有帮助的。但是线下业务相对更加复杂。

第三，资产组合的策略也更加丰富。资产组合指高风险客户、中风险客户、低风险客户资产的组合。这对开放平台的资金和资产有很重要的支持作用；例如，一些资金就非常偏好线下资产。

第四，在政策上，发放ABS必须与场景强关联，线下场景的资金更有利于发放ABS。

之前马上消费金融的CEO赵国庆总提到信贷产品降低费率的问题，是什么原因促使费率下降?

蒋宁：下降费率是公司履行社会责任，践行普惠金融的主要举措，也是公司既定的战略方针，也是和马上消费金融综合能力的提升密不可分的。首先，我们规模越来越大，规模效应已经起来了。第二，经过四年风控技术的积累，不良率处于历史最低水平。我们有180多个场景在合作，

我们作为独立的金融机构，我们的客户来源是跨互联网巨头的数据孤岛的，通过四年的数据积累，我们有全渠道、全场景、全风险图谱的客群数据，这些客群数据让我们有更精准的风控模型。第三，运营成本较低，我们积极投入人工智能技术，像智能客服、智能催收、智能电销和智能回访。这些手段让运营成本都能够控制在很好的水平。

客群上移

从2018年初马上消费金融主动将客群上移，这样的策略是否会造成与银行争夺同类的客群？但是与银行相比，消费金融公司在资金方面优势相对较弱，这是否会加大竞争压力?

蒋宁：首先，中国信用卡渗透率不高，在银行体系下信用卡和虚拟信用卡的渗透率在20%左右，但是美国和发达国家的信用卡都占60%左右，相当数量的客户的信贷需求并没有得到满足。

银行在优质客群和资金成本上也有优势，但是消费金融公司的风控能力和运营能力更高，运营成本和风控能力足以抵消银行在资金上的优势。

有的公司在做上移客群，有的在做下沉用户，您怎么看上移和下沉这两个过程?

蒋宁：首先，现在每家公司的市场定位和能力是不同的。有的公司上移客群会与银行竞争，但通过风控能力和运营效率可以降低成本。二是，有的公司在做下沉用户，这类公司产品收益率比较高，收益对这类公司很重要。

未来趋势

您认为在未来消费金融行业发展趋势上科技是如何应用的?

蒋宁：首先，场景金融是发展方向，未来金融的产品服务跟场景结合的程度越来越紧密。从场景金融的背后来看，需要依靠技术处理与不同场景和不同业务的适配能力，包括开放平台和金融云。

第二，打造轻资产的运营模式，如开放平台战略。现阶段，银行要向零售转型，这就需要构建开放平台的能力，把自己的能力开放出来，从完全是闭环的世界变成开放的世界。

第三，用户体验决定一切，打造极致的用户体验。在移动的世界里市场竞争是没有边界的，用户切换产品和服务的成本是零。从产品服务上看，尤其与场景金融结合之后，打造极致的用户体验是非常重要的，包括额度和利率定价等。这背后需要科技把风控能力、资金成本及运营能力整合好，以提高额度和降低利率。

第四，提高运营效率，减少边际服务成本。随着移动时代的到来，人能接触的服务逐渐增多，传统零售金融的运营成本非常高，其优势变成劣势，所以一定要用科技手段降低边际服务成本，包括从审批、贷中到贷后管理。

第五，注重产品服务创新，提供智能化服务水平。这不仅是服务的创新也是产品的创新。例如，马上在做征信白户就是风控能力的创新，还有智能催收、智能电销和智能客服等。

鹰视——金融终端安全护航者

文 / 新华三金融解决方案 韩喆

对于大型金融企业用户来说，网络毫无疑问是维系金融业务运行和内部管理的关键。我们甚至可以用“业务的血管”来形容网络之于金融企业的重要性。随着金融企业规模的扩大、分支机构的增加以及网络设备规模的飞速累积，越来越多的应用服务暴露在公众视野，攻击者通过网络和终端设备侵入企业内网的途径也随之增加，方式也是多种多样，企业内部网络和终端的安全防护变得日趋重要。面对这样一张规模庞大、内外网并存、类型多样的终端设备网，金融企业已投入大量人力物力来保障其信息安全，但接入客户端因素造成的信息泄漏和破坏，仍然是摆在企业网络信息安全前的拦路虎，这就需要对网络的末梢进行更精细化的准入控制、管理和监控。

金融企业核心痛点：

常言道，“我是谁、我从哪里来、我要到哪里去？”，人生如此，网络设备亦是如此。

痛点一：无法准确的识别网络中的终端设备。

许多金融企业网络中，经常会出现私接个人设备的现象，此行为不仅会危及金融企业安全，也让网络管理变得更加棘手。由于私接设备节点在管理标准和功能上与企业传统网络管理规范相去甚远，网络的管理者在很多情况下对基层单位私接设备不甚了解。信息安全就像一场战争，知己知彼才能百战不殆，如果内部设备信息都无法全面掌控，也就谈不上所谓的管理和安全。

痛点二：无法对识别出的终端设备进行统一的控制管理。

为了解决痛点一提到的识别终端问题，有些企业部署了终端准入控制系统，但是准入控制系统对网络设备存在支持认证的要求，对于一些不支持认证的边缘网络设备、电信运营商的PON网络，其上接入的设备就存在无法管控的情况，传统的终端准入控制系统此时也就没有了用武之地。

另一方面很多已经授权过的终端是否存在仿冒？一般采用的MAC地址认证存在很大的仿冒风险如何解决？这些问题目前传统的准入控制系统没有很好的解决方案。随着金融行业物联网、视频监控网等场景应用，大量无人交互的哑终端像洪水一样涌入网络，不可避免存在黑客等不法份子仿冒终端和私接网络设备行为，严重威胁企业网络安全。

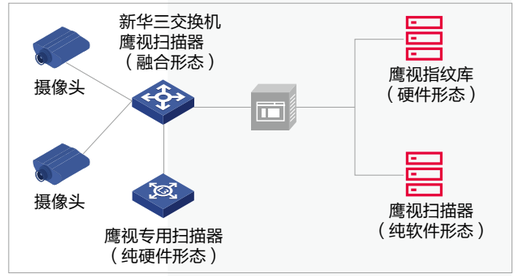
痛点三：对于业务终端的行为审计和资产盘点。

金融行业客户存在大量的业务移动终端（如离行ATM、移动业务PAD等），这类终端设备涉及到金融客户的核心交易业务，如何对这类移动终端进行控制管理和行为审计就上升到了非常高的安全级别。

另一方面由于接入网络的终端类型繁杂、厂商众多，无论是传统的网管系统还是终端准入控制系统，都很难有效地对接入网络的所有终端进行统一可视化管理。高效、精细化的行为审计和资产盘点，不仅有利于合理化配比金融企业的科技投入，而且对企业网络安全审计、智能化运维提供有力数据支撑。

新华三集团结合鹰视和金融园区网AD-Campus方案为金融客户提供一体化的园区网络、终端安全管控的产品和解决方案。解决了以上提到的金融行业用户的核心痛点。在传统化的被动防御方式已经捉襟见肘的情况下，为金融客户提供基于指纹的数据统计库和多样化的AI主动探测等主动出击的立体式防御手段。

新华三自研的鹰视准入系统（Endpoints Profiling System）具备多种产品形态的部署方式。灵活的部署方式使鹰视准入系统在不改变客户现网架构的前提下，能够主动出击准确识别所有端点的类型；实现端点的基线化管理；及时发现行为异常端点。从而有效的对网络接入进行全方位的管控和资产盘点，达到全面捍卫金融网络安全的目的。



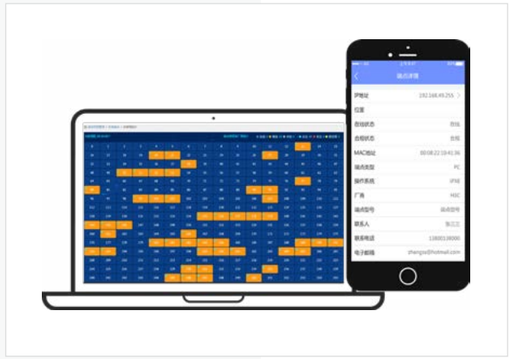
多样化AI主动出击

◉ 客户可以通过增加扫描器（扫描器可为纯软件或专用硬件设备）对现有网络进行全网扫描探测。

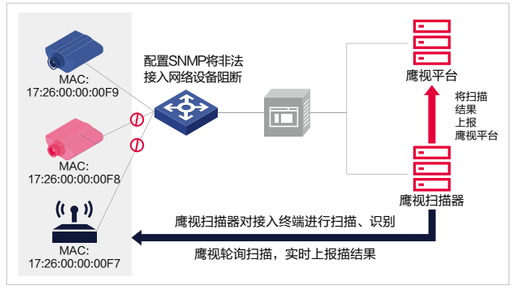
◉ 在采用新华三路由器、交换机（扫描器可集成在新华三网络设备中）办公网络中不仅可满足传统网络设备特性和能力，也兼具扫描器主动探测能力。减少故障点和简化网络管理同时，也将安全防护能力进一步下沉到网络边界。

鹰视核心功能

“感知识别”： 鹰视通过主动的雷达扫描和被动触发识别，能够快速发现端点入网行为，对接入的端点进行精准识别。鹰视系统可收集有关端点的类型、IP、MAC、厂商、操作系统等信息，并持续监控端点运行状态，根据用户需求输出资产报表。鹰视的感知识别能力和端点类型、厂商无关。



“连接管控”： 鹰视能够通过RADIUS、SNMP、物联准入网关等多种手段对接入网络的非法端点进行主动阻断。同时可以对端点的各种变更，包括IP地址变更、MAC地址变更、终端类型变更等事件及时发现和告警。



“可视化管理”： 鹰视GIS地图模块区别于传统的在线地图服务，用户业务数据完全部署于金融企业内部，通过物理隔离和用户授权，充分保障金融企业数据的安全性。能够将全网终端信息统一可视化展示。

通过鹰视的可视化管理，可以对金融客户移动业务终端的安全进行有效的控制和管理，并对其运行的金融业务进行系统化的行为审计。

鹰视同时具备传统准入控制系统的能力，对用户接入有丰富的控制方式。因此，通过鹰视可以对网络全局接入进行合规性的管控：

对办公网中用户接入进行安全有效的准入控制。通过双因子认证、802.1x认证、证书认证等方式以及基于用户身份权限的下发，保障用户身份的合法性。

解决了仿冒哑终端MAC地址接入的问题。通过对MAC地址认证的完善，使得哑终端入网不再仅仅是校验MAC地址，同时还要校验哑终端的终端类型、厂商信息、操作系统等，一旦发现有变化，鹰视就能及时阻断。

网络设备接入有了可靠的管控方案。鹰视对入网设备进行精准识别，待管理员审批后自动加入网络资产管理库。如果有新的网络设备接入，鹰视能够及时发现并和资产库进行比对，如果是私接设备，及时阻断。

对网络接入进行全局监控，并对网络资产进行全局的可视化管理。鹰视对入网端点持续监控，一旦发现有端点掉线及时通知管理员。同时，鹰视对网络资产详细信息进行图形化管理，大大节省管理成本。

金融办公网

某金融企业在全国有多个二级单位，由于总部对全网各二级单位网络设备运行情况缺少统一的监控和管理手段，网络资产的统计与核查也非常不完善，经常出现设备私自接入等安全违规问题。客户希望对全网设备进行摸底，消除设备私接的安全隐患。

鹰视可以对网络中终端设备的接入敏锐感知、精准识别，并对这些终端设备在线情况做统一的监控，一旦发现未授权的终端设备接入网络中，即可通过短信、邮件告知管理员；同时，鹰视可以根据客户需求输出资产报表，快速帮助客户将网络资产盘查清楚。

金融生产网

某金融机构ATM自助设备、排号机等非管控终端需要接入网络，对网络安全接入管理带来挑战，传统准入客户端管理模式无法管控这些设备。

鹰视可以对网络中ATM自助设备、排号机等非管控设备的接入敏锐感知、精准识别，并对这些终端设备在线情况做统一的监控，一旦发现未授权的终端设备接入网络中，即可通过短信、邮件告知管理员。

金融视频监控网

某金融企业大型园区视频监控网有数千个摄像头，都分散部署在公共区域，基本上处于无人值守的状态，极易被私接仿冒，网络存在被非法入侵的安全隐患。同时，由于这些的摄像头属于不同的厂家，在统一监控和管理上存在诸多困难和问题。

鹰视能够主动扫描视频网络中终端状态，及时发现仿冒和私接终端，并实时将异常信息报警，监管人员第一时间获取异常详细信息。鹰视能够主动下线接入视频网络的仿冒和私接终端，确保视频网络前端接入的安全。

同时，鹰视采用全球领先的AI与图像识别技术能够自动检测图像故障和各类视频故障。减少人工检查工作量，降低人力成本。

体系化攻防能力建设

助力金融安全

科技人才培养

文 / 新华三大学安全技术学院 李毅

在国内网络安全形势愈发严峻、信息安全内控机制逐步精益的情况下，为了确保企业关键信息基础设施和网络安全的综合防御能力和水平，需要企业全面提升“监测发现、安全防护和应急处置”的能力。金融的发展与技术的进步相辅相成，而金融安全则为整个产业的发展起到了至关重要的保驾护航的作用。面对新时代的安全挑战，金融企业需要有针对性地构建攻防专家团队，并通过系统化的人才培养实现攻防团队专家化、梯队化。从而进一步推动网络安全红蓝队建设持续走向深度发展，全面提升金融安全防护能力和实战水平。

对攻防团队专家进行分阶段培养的目标是重点提升攻防团队成员的以下能力：

提高动手能力

通过丰富的演练与实操提高团队成员的实际动手能力，让团队成员能够熟练掌握工具和方法的使用，从而得心应手地快速完成特定任务要求的操作。

提高分析能力

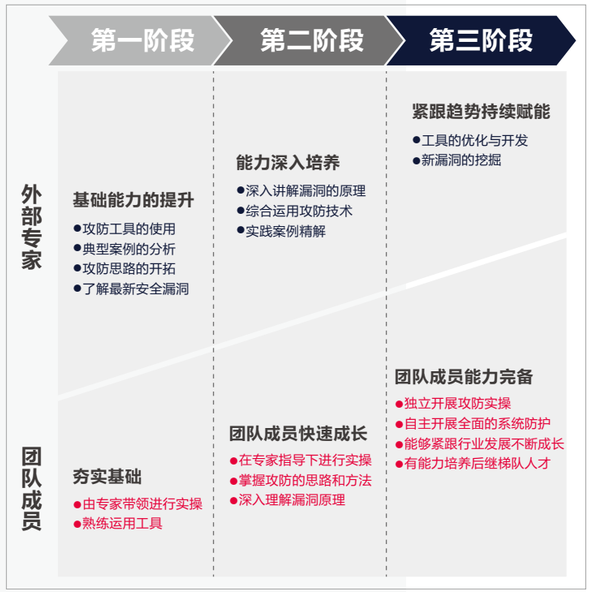
解决攻防团队成员实践需求，培养他们对各种安全事件具有独立分析能力，也能够主动分析复杂系统中的多种信息，快速定位漏洞与风险。

提高实战能力

让团队成员在专家的辅导下针对实际业务环境的需求，开展一系列实战实操，持续提升对现网业务和环境的理解，并通过不断开展监测攻击行为、修筑防御工事的方式切实提高网络安全攻与防的实战能力。

提高应变能力

不拘泥于传统的教学模式，而是采取向理论与实践相融合的模式改革，不断开展红蓝对抗的演练，在真实对抗中磨练团队成员应变能力，使其具备充足的技能从而切实提升公司网络安全主动防御水平。



能力提升的实施步骤

为了达成攻防专家团队的培养目标，需要分阶段分步骤地开展一系列的培养活动。不仅有体系地培养专家成员，也通过广泛的安全培训活动使所有安全岗位相关人员的安全意识和能力得到提升。

分阶段地专家培养

作为一个长期的专家人才培养项目，需要把人才培养的目标分解到每一个阶段，并在每个阶段中有所侧重地组合不同的培养手段。

如下图所示，团队成员的培养在三个阶段内逐渐实现能力的提升，外部专家在整个过程中的定位和培养输出也相应进行着调整。总体的思路是初期外部专家承担更多的培养任务，后期则更多地强调团队成员自身的主动学习和实战实操。

第一阶段

第一阶段的培养目标聚焦在基础能力的提升，因此外部专家将更多地讲解攻防工具的使用、并结合典型案例的深入分析让团队成员对安全攻防的思路和方法有深入的了解。在本阶段中攻防专家团队成员能够掌握常用的工具与方法，在外部专家的带领下开展“红蓝队”攻防实战演习，切实达成夯实基础的目标。

第二阶段

第二阶段是攻防专家团队快速成长的阶段，外部专家对其培养的目标从常用工具和方法的使用转变为深入理解典型漏洞的原理，而且能够在复杂环境中综合运用攻防工具进行实战对抗。在本阶段团队成员应该仅需要专家的指导就可以主动开展“红蓝队”攻防实战演习，实现从被动执行到主动独立开展工作的转变。在不断实战实操的训练中不断磨练动手、分析、实战与应变的能力，并自然转入主动学习的状态。

第三阶段

第三阶段是团队成员能力培养最终的阶段，他们对于攻防的理解已经非常深入，而且能够理解业界对攻防工具的优化并且开始参与新漏洞的挖掘。本阶段外部专家的定位是持续赋能，更强调团队成员的自主学习和实战实操的能力锤炼过程。

在分阶段的专家培养过程中，每个攻防专家团队成员都要经历从基础知识到深度安全的成长过程。为了达成培养目标，还要综合考虑以下原则：

一专多能

安全攻防涉及到众多的专业领域，每一个团队成员不可能在所有的技术领域都做到最强。因此，在培养的过程中需要结合每个成员的兴趣和专业经历，突出某个专业领域的特长培养。

这意味着每个成员在熟练掌握通用的技能后，将深入学习互联网攻防和内网渗透等专项领域。每个团队成员一专多能的模式，将保障整个攻防专家团队的能力完备而且专项精深，从而构建一个专业全面且实力精深的综合团队。

实践出真知

在传统的课堂授课之外，还需要更多地通过对抗性演练来提升团队成员的真实技能。一方面在专家的辅导下充分结合现网真实案例，深入剖析从而加深理解，另一方面则在通过“红蓝队”攻防实战演习等方式开展真实环境的实操，促进技能的灵活运用、具备解决复杂问题的能力。

教学相长

为了达成最终的专家培养目标，就需要把被动接受转变为主动学习，激发团队成员的成长诉求。为此鼓励学员根据专家推荐的资料开展自主学习并在系统内部进行分享。从而强化对理论、方法和思路的理解与掌握，并且有助于人才梯队培养机制的形成。

多种培养手段并举

由于攻防专家团队的培养的特点是周期长而且涉及领域广，所以需要灵活组合多种培养手段才能达成最佳的效果。每一个培养手段都有其目的和价值，结合培养步骤的规划，将有助于团队成员快速成长并不断夯实基础。

专题培训

作为攻防专家培养的重要手段，攻防专家团队成员将接受系统的课程培训。专题培训覆盖了多个方面的信息安全教学内容，包括实验原理、教学虚拟化环境、实验指导书，能够让学员扎实掌握相关的知识和工具。培训内容主要包括渗透测试的目的、方式、途径、分类、手段等，以及Web安全中涉及到的文件上传漏洞、文件解析漏洞、Webshell的介绍、文件包含漏洞、逻辑漏洞以及SSRF、反序列化漏洞等新型的Web漏洞，并在漏洞利用的基础上进行权限提升与内网渗透的讲解，让学员掌握整个渗透测试流程中涉及到的所有技术要点。

“红蓝队”应急演练

作为一名优秀的信息安全人员，信息安全攻防工具是必备的。信息安全攻防平台为用户提供多类工具的使用，如：综合扫描、字典、抓包改包、注入、提权、破解、旁注、目录扫描、漏洞利用、后门、XSS、ARP嗅探、MD5破解等工具。基于攻防平台提供的丰富场景，团队成员得到充分的攻防锻炼。将工作中可能经历的各种安全对抗，通过一种特殊的竞赛模式提升成员的动手、分析、实战与应变能力。在演练中促使成员既要了解如何利用这些漏洞进行攻击，也必须了解如何快速针对发现的漏洞进行修复与防护。

培训案例

为了整体提升安全从业人员的专业能力，某农信以农信联全国安全竞赛为契机，选拔了安全技术骨干开展了攻防专项培训。新华三大学安全技术学院提供了两期八天的专项培训，内容包括：Web安全、加解密、信息隐藏、取证分析、逆向分析、二进制漏洞等，并通过AWD演练的方式让学员能够在平台的支撑下实现对专业知识的灵活运用，从而实现了对动手能力、分析能力、应变能力及实战能力的综合提升。参训团队成员在全国竞赛中取得了多个奖项，为专业化金融安全科技人才梯队建设走出了扎实的一步。

紫光集团 核心企业 | H3C 数字化解决方案领导者

新华三国产化网络

在网络国产化方面，

新华三网络规模部署多家金融机构，

助力中国建设银行、中国银行、中国邮政储蓄银行、

中国人民银行、网联、农信银、中信银行、民生银行、中国平安、

中国人民财产保险、中国太平洋保险、中信证券、上海证券交易所

等核心金融机构生产网建设，有力承载金融生产核心业务。

2019最新中标

数据网络中心

- 中信银行数据中心及中国尊大厦网络项目
- 中国光大银行总行PAAS云平台网络项目
- 北京农商行数据中心互联网区及IPv6网络建设项目
- **中国建设银行公有云网络项目**
- 中国人民银行总行云平台网络建设
- 平安集团网络集采项目
- **招商银行成都站点项目**
- 北京银行数据中心网络、存储、服务器项目
- 红塔证券同城数据中心项目
- 宁波银行新数据中心网络建设
- **贵阳银行数据中心及备份网络项目**
- 重庆银行数据中心网络改造
- 厦门国际银行同安数据中心项目
- 青海省农村信用社网络安全采购项目
- **上海农商银行交换机采购项目**
- 四川农信云平台网络采购
- 山西农信灾备网络、服务器及咨询项目

SDN、广域骨干网、分行及办公网

- 中国人民银行武汉分行广域网SDN项目
- **中国人民银行金融城域网高端路由器采购**
- **中国银行安全生产项目（园区SDN、数据中心SDN、鹰视、交换机）**
- 中国人民财产保险股份有限公司超融合项目
- **中信证券灾备数据中心网络**
- 中国银行合肥云中心基础网络设备（SDN、网络）
- 国家开发银行全行网络管理及运维自动化项目
- 北京农商行核心骨干网项目
- **国开证券新一代数据中心网络**
- **中国人民银行江西分行全省路由交换项目**
- 上海证券交易所园区SDN

金融行业IPv6演进、改造与安全

文 / 新华三金融解决方案 朱崇银

当代中国，互联网是关系国民经济和社会发展的重要基础设施，深刻影响着全球经济格局、利益格局和安全格局。我国是世界上较早开展IPv6试验和应用的国家，在技术研发、网络建设、应用创新方面取得了重要阶段性成果，已具备大规模部署的基础和条件。

我国早在十三五规划中就提出要超前布局下一代互联网，全面向IPv6演进升级。并于2017年11月26日中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》，提出了规模部署IPv6的路线图和部署目标。金融行业作为重点行业，也于2019年1月10日，由中国人民银行、银保监会、证监会（以下称为“一行两会”）联合发布了《关于金融行业贯彻<推进互联网协议第六版（IPv6）规模部署行动计划>的实施意见》，其中指出的行动目标分为三个阶段：

初期阶段（截至2019年底）

年底前完成本单位总部及下辖机构门户网站IPv6改造工作，并在其首页标识该网站已支持IPv6。除有用户权限登录控制的定制应用系统外，门户网站主域名内全部静态页面、动态页面、多媒体资源和第三方应用插件等均支持IPv6连接访问；页面链接的全部子域名网站均完成IPv6改造。

其中示范机构要求至少选择一个活跃用户规模在本机构内排名前3位（含）的移动APP应用系统，使其支持IPV6连接访问，并在其首页标示该应用已支持IPv6。

规模推广阶段（截至2020年底）

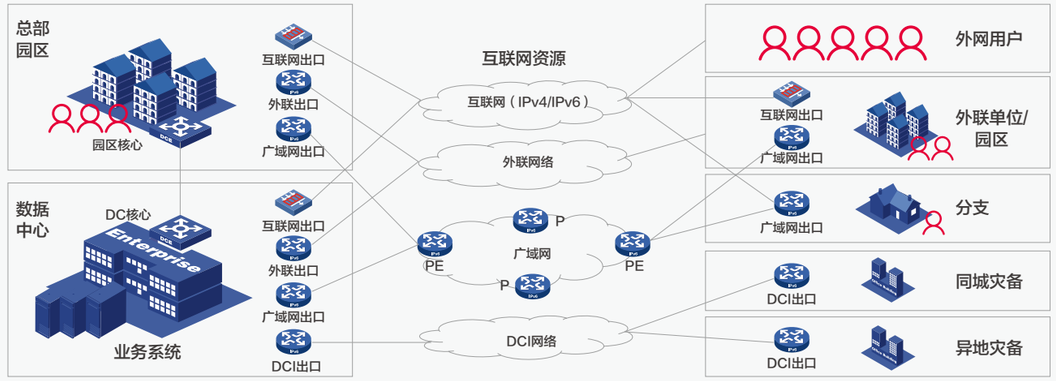
金融服务机构完成所有面向公众服务的互联网应用系统相关软硬件基础设施升级改造工作，全部支持IPv6协议，并具备与IPv6改造前同等的业务连续性保障能力。

持续建设阶段（自2021年起）

2021年起，在做好面向公众服务的互联网应用系统IPv6改造基础上，持续开展网络、应用、终端的IPv6升级改造工作，推进IPv6规模部署，逐步构建高速率、广普及、全覆盖、智能化的下一代互联网。

金融行业IPv6改造全景

基于一行两会对金融行业规模部署IPv6行动计划的要求，金融行业IPv6改造典型场景和网络包含互联网、数据中心、广域网（含数据中心互联DCI）、园区网、外联网，此外还要考虑如何保证安全、如何进行运维、如何解决过渡阶段可能出现的天窗问题。



从IPv4网络到IPv6网络的演进过程主要有如下阶段：

改造过程中将有长期的过渡阶段，对于过渡阶段，过渡技术用于解决两类问题，IPv4与IPv6的共存问题和IPv4和IPv6的互通问题。其中双栈技术、隧道技术用于解决IPv4与IPv6如何共存的问题，而隧道技术用于解决IPv4和IPv6如何互通的问题。

改造升级要点

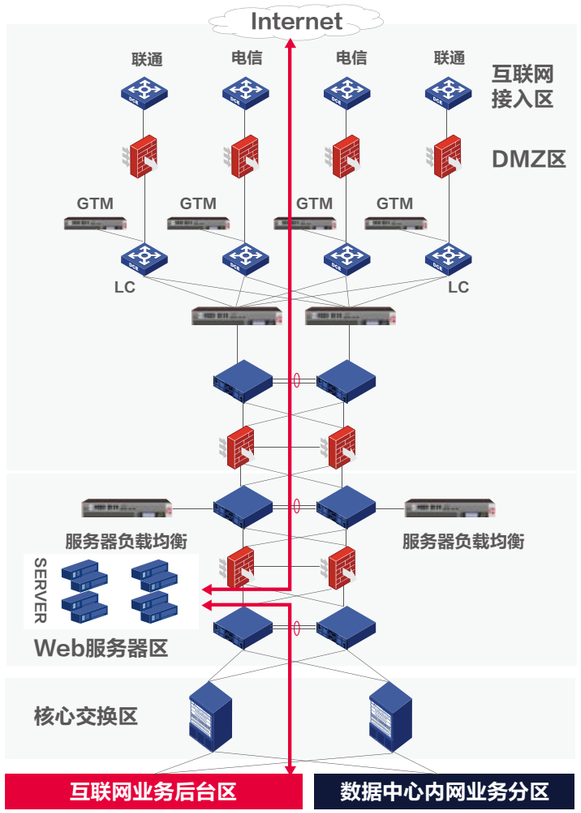
IPv6改造升级是一个系统性的工作，不仅仅是网络改造，还要对众多的应用系统周边进行改造，如应用层面可能涉及的代码、应用软件、APIs、中间件、数据库、操作系统、驱动；如基础硬件层面是否支持、表项能力、终端层面操作系统、应用程序等都要做大量的技术升级改造。整个改造过程中技术组织架构需要整齐划一，通力合作，完成IPv6改造的任务。

整个改造的宗旨是2个不变，3个改造，即总体架构不变、访问流程不变；DNS改造、网络/安全改造、网站应用改造。

金融互联网业务改造

对金融互联网类业务进行改造，首要目标是既要保证实现对外提供IPv6服务，又要保证现有IPv4服务不受影响。改造前首先需要基于互联网类业务进行分析。下图是一个典型的金融互联网业务区的网络架构。从业务视角看，总体上可分为互联网接入边界、DMZ（Web）、后台服务（App+DB）三个层面。外部用户访问金融Web网站的业务操作可大致分为前端和后端两个部分：

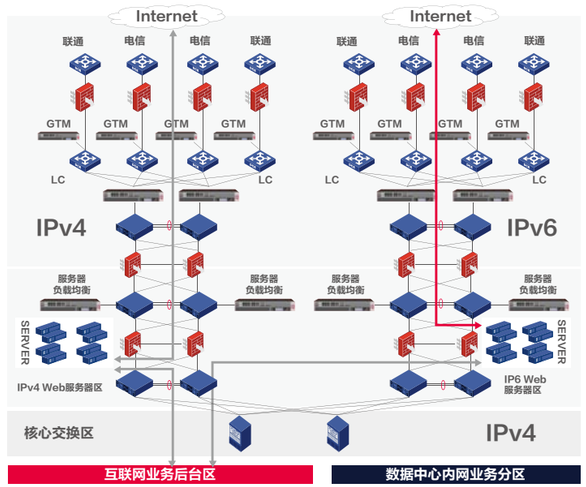
- **前端：**从Internet接入区到DMZ中Web server部分。用户通过Internet访问Web server，用户HTTPS连接和Session在Web层终结。
- **后端：**Web server到内网中的各App server建立连接，进行相关应用和数据访问。



基于该架构，我们可以得出结论：前端对外提供服务，后端为前端提供服务。那么初期的改造可以考虑只改造前端而后端保持不变的方式实现。

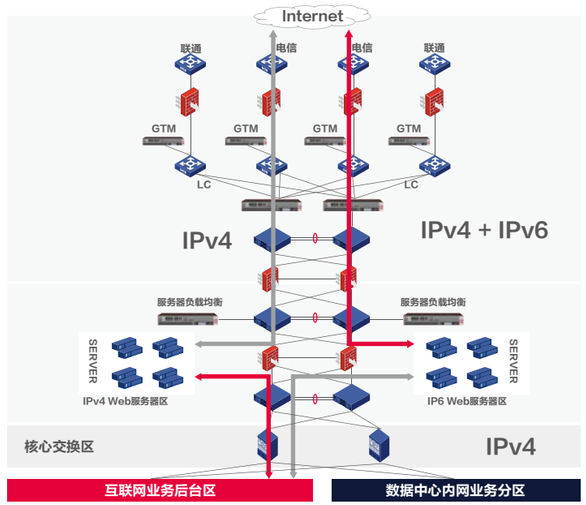
大致方案有如下几个：

完全新建纯IPv6互联网接入区



通过完全新建纯IPv6互联网接入区，外部IPv6连接在Web层终结，Web层采用双栈网络建设，请求后端沿用IPv4方式。完全不影响原有IPv4业务，实现IPv6改造。

新增IPv6 Web集群



考虑到目前网络设备对IPv6的支持能力已经较好，而服务器改造由于涉及到硬件、操作系统、中间件、应用软件、代码等涉及面众多可能改动较复杂，在不影响原IPv4业务的基础上，新建双栈Web集群对外提供IPv6业务，对内采用IPv4访问后端，实现IPv6改造。

其他方案

此外还有原业务区之间开启双栈方案和Web前端通过负载均衡或防火墙使用地址翻译技术实现改造。其改造方案和业务访问流程不再赘述。

总结

在2个不变、3个改造基础上，整体思路为通过双栈或转换技术实现在不改动应用架构、不改动访问流程、不影响现有IPv4业务的基础上实现IPv6的改造。

通过在金融行业客户的调研，目前主要选择的方案为新建纯IPv6互联网接入区方案。

数据中心IPv6改造

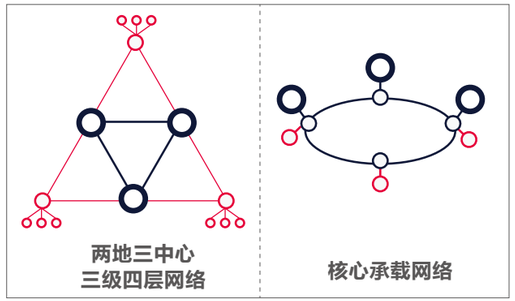
由于业务逻辑架构整体也基本分为Web、APP、DB三个层面，所以金融数据中心改造主要与互联网类业务改造类似。只是新建IPv6单栈数据中心投资过大，所以不太具备可操作性。数据中心整体改造优先选用双栈技术实现真正的业务平滑过渡，同时可获得较多IPv6过渡技术积累。而地址翻译技术一般在资金预算紧张，尽量减少部署IPv6对现网的冲击与风险时使用。

数据中心内部双栈改造主要考虑数据中心网络路由协议的改造。IPv6相关的路由协议中，OSPFv3，RIPng、IS-ISv6、BGP4+都是从相关的IPv4路由协议演变而来的，其应用场合、路由思路及优缺点并没有发生根本改变，从维护等角度看，建议使用与IPv4一致的支持IPv6的路由协议。

	IPv4	IPv6
单播路由	• RIP • OSPFv2 • ISIS • BGP4	→ • RIPng • OSPFv3 • ISISv6 • BGP4+

广域网IPv6改造

金融广域网视规模大小，一般有如下两种架构：

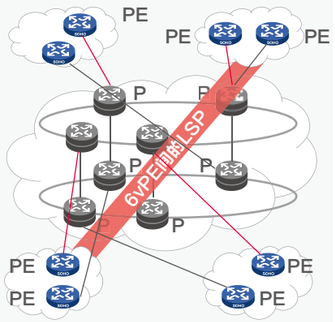


- 两地三中心架构：中小型银行以数据中心为核心，各地分支机构通过专线连接到数据中心。通过IP路由方式实现分支机构与数据中心的互通。

- 核心承载网架构：大型银行广域网发展逐渐运营商化，以核心承载网为核心，各地分支机构和数据中心通过专线接入到核心承载网。通过MPLS VPN承载整个机构的所有流量。

基于两类广域网组网架构，可采用不同的改造方案。

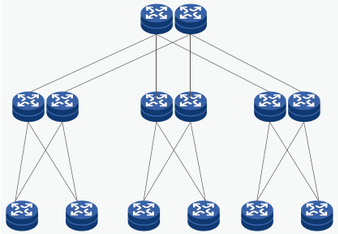
MPLS组网：6vPE方案



PE双栈改造: PE升级双栈，使能6vPE；绑定6vPE VPN实例，使能6vPE地址族，接入IPv6业务

P保持不变

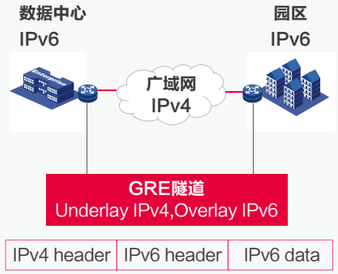
IP组网：双栈方案



对全网设备进行双栈改造评估（CPU/内存），升级或替换不满足要求的设备

配置IPv6地址、部署IPv6路由协议等

孤岛互通：隧道方案



在孤岛出口(例如数据中心、园区出口)间配置IPv4 GRE隧道，承载IPv6业务

- 在MPLS组网环境，可通过6vPE方案实现，基于MP-BGP MPLS VPN技术的实现原理，通过在PE设备上启用IPv6 VPN实例与CE端IPv6路由器互联，而P设备无需做任何改动即可实现广域网的改造。

- 在IP组网环境，可通过所有设备启用双栈方案实现广域网的改造。

- 在IPv6改造过程中，可能出现部分单协议孤岛。可通过隧道方式实现跨IPv4广域网的多个IPv6孤岛环境的互通或跨IPv6广域网的多个IPv4孤岛环境的互通.

广域网改造中，涉及对路由协议的改造，从维护等角度看，建议使用与IPv4一致的支持IPv6的路由协议。

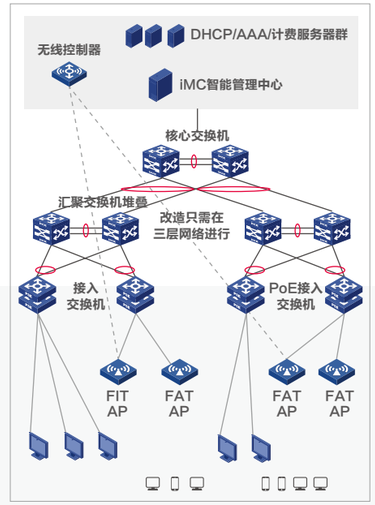
园区网改造

金融园区网一般包含有线网络和无线网络。改造应自上而下、分批逐次改造。

对于有线网络，改造范围仅限于三层网络的路由及IP业务改造，如OSPF、DHCP等，普通二层网络无需改造，二层网络设备如需感知网络应用数据也需进行IPv6改造升级，如DHCP Snooping等。

对于无线网络，推荐采用AC+Fit AP的方案，AP零配置，降低IPv6网络运维部署复杂度。AP注册隧道同时支持IPv4/IPv6，灵活随选。用户业务数据通过CAPWAP隧道承载，隧道对用户业务透明，支持双栈隧道。

在无线部署时候，由于部分Android终端不支持DHCPv6技术，着重需要考虑为安卓终端支持RDDNS特性，满足为Android终端分配DNS，解决Android终端上网问题。



网管运维改造

网管系统对IPv6网络的管理和IPv4类似，最大差别是要求网管运维服务器配置双栈。

针对网管运维改造，只涉及对IPv6的改造，所以总体网管运维组网不变、网管功能模块部署不变、带内带外管理模式不变。需考虑对IPv6地址的管理与分配。

网络安全加固

对于IPv6网络安全需要重点关注解决三个方面内容：

- 解决IPv6与IPv4的共性安全问题，IPv6与IPv4同为网络层协议，有着共同的安全威胁，这些安全威胁在IPv4网络中已经有了成熟、有效的解决方案，可以通过继承和发展现有IPv4攻击防范安全技术和规范，来解决IPv6网络中遇到的同样的安全威胁。

- 解决IPv6协议和协议簇自身的安全问题，包括：

IPv6相对于IPv4在协议簇上发生了较大的变化，同时也新增了一些已知的或未知的安全威胁。解决IPv6协议簇安全问题，需要针对不同协议特性实施有针对性的安全策略，同时修补协议漏洞。

IPv6协议报文格式新增安全威胁。解决此类安全威胁，需要针对IPv6协议特点实施有针对性的安全策略，同时修补协议漏洞。

基于IPv6的应用实现新增的安全威胁。解决此类安全威胁，需要加大IPv6应用代码审查力度、强制IPv6应用程序漏洞检测，同时对已知漏洞要求及时修复。

- 解决IPv4向IPv6过渡的过渡技术安全问题，IPv4向IPv6过渡是一个长期的过程，在IPv4和IPv6共存时期，为解决两者间共存、互通所采取的各种措施如双栈、隧道、翻译等技术都将带来新的安全风险。需要通过优化协议、算法和设备实现、引入认证、加密、防篡改机制、制定和执行严格的安全策略等措施，来解决IPv4向IPv6过渡的过渡技术所存在的安全问题。

天窗问题

当访问的IPv6网页包含其它网站内容的链接（外链），并且该外链是IPv4部署未进行IPv6改造时，因为引用的其它网站未升级，IPv6用户访问该网站时会出现响应缓慢，部分内容无法显示，部分功能无法使用等情况。该问题被称为“天窗”问题。

出现天窗问题的场景主要有IPv6单栈用户访问包含IPv4外链的企业IPv6网、双栈用户访问包含IPv4外链的企业IPv6网站。在IPv6迁移改造过程中，双栈终端是一个长期过程。重点考虑双栈用户的天窗问题解决方案。因为外链网站是IPv4应用，IPv6 DNS中不包含外链网站的AAAA记录。IPv6 DNS回复外链网站的AAAA：空记录。双栈终端无法与外链IPv4网站建立连接获取相应内容，则出现天窗。

天窗问题的解决思路主要有如下两个：

- Happy Eyeballs（RFC6555、RFC8305），如果在DNS解析时延（50ms）内未获取AAAA记录，双栈终端将选用A记录建立IPv4 TCP连接、终端在解析时延内获取AAAA，优选IPv6建立TCP连接。如果在连接发起时延（由应用实现具体设定，通常为250ms）内未获取TCP SYN+ACK，则双栈终端尝试使用A建立IPv4 TCP连接。

- 通过建设CDN方式、负载均衡或防火墙设备上使用协议转换代理方式解决。

新华三IPv6技术实力

新华三20余年的自主研发、1000W+行Comware平台代码、9800+功能模块、数百项IPv6专利，设备原生支持IPv4/IPv6双栈，10余年IPv6部署实践。可提供云-网络-终端的全栈IPv6解决方案，为IPv6建设提供从咨询规划、方案设计、到实施交付、增值服务的全生命周期服务，帮助用户实现从IPv4到IPv6的升级改造和平滑迁移。