

美·创物志

MEI CHUANG WU ZHI

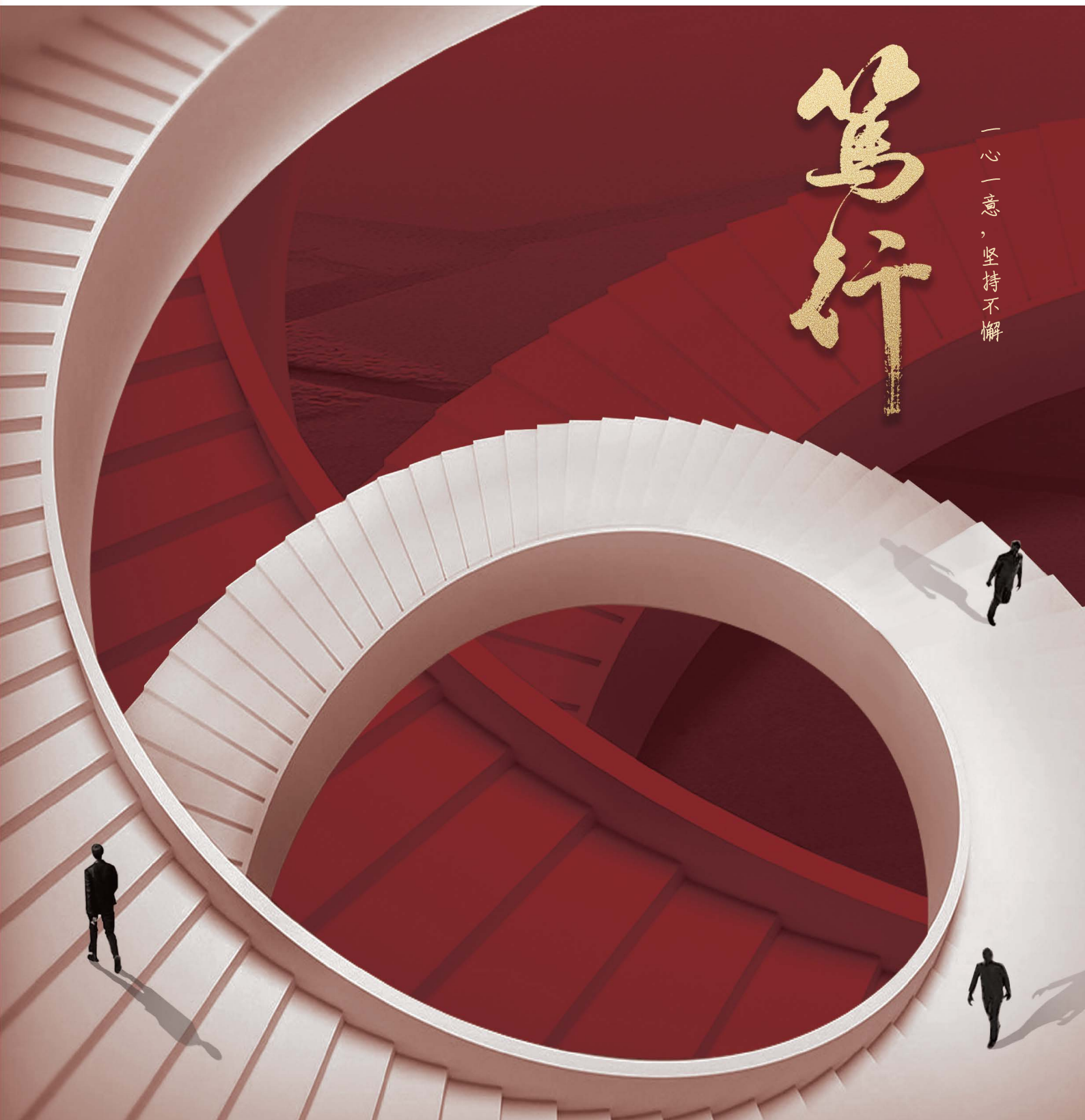
在这里读懂美创 Understand Meichuang Right Here

5

2023年 第5期

笃行

一心一意，坚持不懈





2023年总第5期

出品：杭州美创科技股份有限公司

编审委员会

柳遵梁、闻建霞、胡江涛、徐荣星、沈武林、罗亮亮
刘宇洁、应以峰、顾皓天、王利强、周杰、王平

主编

高司辰

副主编

霍杰华、何怡、罗剑芳、谭双林

采编部

李阳

全国服务热线

400-811-3777

邮箱：marketing@mchz.com.cn

网址：www.mchz.com.cn

总部地址：

浙江省杭州市拱墅区丰潭路 508 号天行国际中心
7 号楼 12、14、15 层



FOREWORD

卷首语

2022 年是美创寄托着无限希望的奋进之年。《数据安全法》、《个人信息保护法》在 2021 年 9 月和 11 月陆续生效了，注定了 2022 年是数据安全发展史的转折之年或者数据安全元年，成就数据安全步入大江大河时代。这是美创从 2010 年开始的数据安全的云开月明之路，是对美创十几年数据安全坚持道路的最好嘉奖。在这一年的阳春三月，我们开启了三年战役，从数据安全探索之路迈进到决胜之路。

2022 年是美创成立以来最为复杂艰难的一年。世上从来没有不经历艰难困苦的伟大胜利，在乍暖还寒的最好三月，上海疫情掀起了惊涛骇浪，三年疫情迎来了最为艰难困苦的一年。在这种艰苦复杂的环境中，我们唯有对未来的坚定信念，咬紧牙关，克服一切困难，砥砺前行。

在这一年里，我们完成了股改，从一家有限公司转变为一家股份制公司，跨出了 IPO 之路的坚实一步。在这一年里，我们开启了三年战役，开始了我们走向伟大的序章。在这一年里，巨大的市场不确定性在无限蔓延开来。从来没有什么一帆风顺的事业，无限光明的事业总是在密布的阴云之后，我们命中注定，在数字化浪潮迎风踏浪，承受八方风雨，但是前面光芒万丈！

美创科技 CEO 杨明华



CONTENTS

	美·纪事	01
	2022 美创大事记	02
	全年活动掠影	06
	区域活动风采	10
	美·实力	13
	美·载誉	21
	资质认证	22
	荣誉奖项	23
	美·上新	25
	新产品：API 安全监测与访问控制系统	26
	新产品：流动安全管控平台	29
	新产品：数据安全综合评估系统	34
	新服务：数据安全治理咨询 V3.0	38
	新服务：数据出境安全的“知”与“行”	42
	新服务：个人信息安全风险评估服务	48
	新解决方案：金融业务应急切换管理解决方案	52
	新解决方案：美创全院级数据中心解决方案	57
	新解决方案：8 个医疗数据安全场景化方案推出	61

 美·实践	76
浙江省农业农村厅政务数据安全治理实践	77
许昌职业技术学院数据安全防护体系建设实践	80
宁波市第一医院：基于大数据的公立医院智慧运营分析平台的建设及应用	84
美创助力全国首批省级中医院数据安全建设	90
看，金华最安全的“一朵云”	93
容灾切换演练实例	97
 美·共赢	99
美创科技与中国东信举行生态合作协议签约仪式	100
开启校企合作 2.0，美创科技与杭州电子科技大学开展联动互访	101
美创科技加入阿里云飞天生态合作伙伴 - 服务生态合作计划	103
美创科技入围中国电信成员单位 - 数据安全产品供应商	104
美创科技与联通（浙江）产互签署战略合作协议	105
北京、福州、广州、南京等地渠道会合集	106
 美·祈愿	107
 美·杂谈	109
 美·聚力	110
团建拓展活动	111
美创俱乐部	112
节日趣味活动	113
美创欢乐跑	114
爱心助学，暖心起航	115

美·纪事

MEICHUANG · CHRONICLE

2022 美创大事记

杭州美创科技有限公司

2022年度网络安全支撑单位

中共浙江省委网络安全和信息化委员会办公室
二〇二二年二月

杭州美创科技股份有限公司
创立大会暨首次股东会隆重召开

股改

品牌活动掠影

第三届国际零信任峰会暨首届西塞论坛

区域活动风采

2022年第四届全球工业互联网大会

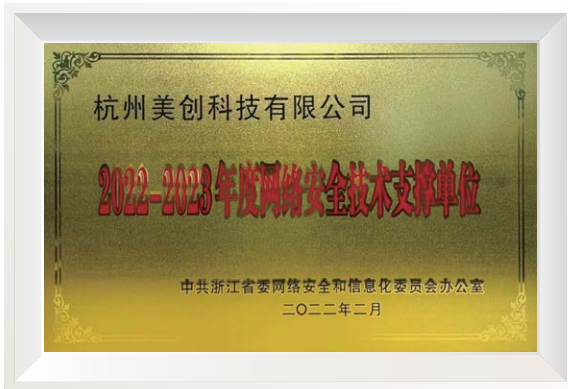
2022 美创大事记

▶▶▶ 事件按发生的先后顺序排列

美创科技入选浙江省委网信办 网络安全技术支撑单位

01

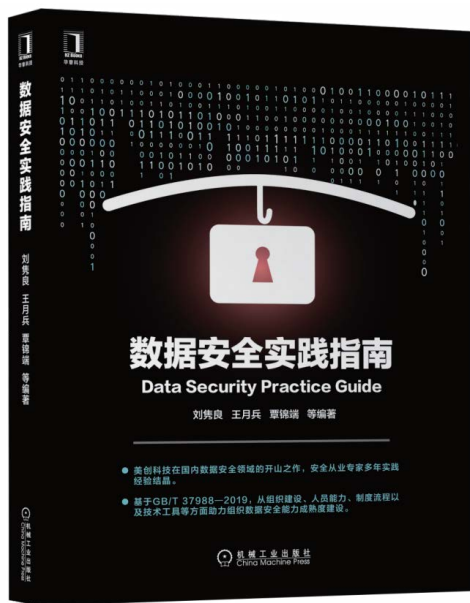
3月，浙江省委网信办公布“2022-2023年度网络安全技术支撑单位”评选结果，美创科技被授予“2022-2023年度网络安全技术支撑单位”！根据浙江省委网信办《关于遴选网络安全技术支撑单位的公告》，此次评选共遴选出22家在网络安全、数据安全等领域技术实力强、服务能力突出、社会责任感强的单位作为中共浙江省委网络安全和信息化委员会办公室网络安全技术支撑单位。工作会议上，美创科技联合创始人、副总裁闻建霞作为数据安全代表企业发言。



美创科技新书 《数据安全实践指南》上市

02

4月，由美创科技数据安全从业专家主编的《数据安全实践指南》一书正式上市！《数据安全实践指南》以国内GB/T 37988-2019为依据，系统介绍了DSMM中三级（充分定义级）定义下各过程域对应组织建设、人员能力、制度流程以及技术工具相关要求，在此之上结合美创科技多年数据安全治理实践经验，对上述各过程域逐一进行解读以及提供实践指南操作建议，并总结归纳DSMM全部要求，整合生成基于数据安全风险评估的量化观察指标和建议实践目标，为组织后续基于DSMM相关实践和自评提供实践指南和参考依据。



美创参与编写的《信息安全技术 数据备份与恢复产品技术要求与测试评价方法》(GB/T 29765-2021)正式实施

5月1日,《信息安全技术 数据备份与恢复产品技术要求与测试评价方法》(GB/T 29765-2021)国家标准正式实施,替代2013年9月18日发布的标准号GB/T29765-2013版本。美创科技作为起草单位之一参与了标准的编写。

美创 DBRA 数据级容灾、CDP 灾备一体机等产品可充分满足新国标中基本级数据备份与恢复产品的要求。



美创数据安全管理平台荣获 2022 数博会“领先科技成果奖”

5月26日,2022年中国国际大数据产业博览会上,“数博发布”重磅揭晓全球大数据领先科技成果奖,美创科技数据安全管理平台凭借创新领先的技术与实践,荣获“2022 领先科技成果奖—新产品”。

目前,领先科技成果奖已入选国家《社会科技奖励》目录,成为国家科学技术奖励工作办公室备案的唯一以博览会名义设奖和唯一以大数据为主题的专业奖项。



美创科技与中国东信举行生态合作协议签约仪式

5月27日,杭州美创科技股份有限公司与中国—东盟信息港股份有限公司举行生态合作协议签约仪式。签约仪式上,美创科技 CEO 柳遵梁,中国东信联席总裁李珩共同见证签约,双方代表进行了签约。美创科技希望能够与中国东信进行深度资源整合,在市场协作、技术融合、推动数据安全等方面加强合作。



美创科技入选“2022 年度杭州市人工智能重大科技创新项目”计划

8月15日，杭州市科技局公布“2022年度杭州市人工智能重大科技创新项目计划”名单，美创科技申报的“面向数据流动安全的智能风险防控关键技术与应用”获批入选。

此次获批入选的“面向数据流动安全的智能风险防控关键技术与应用”项目技术骨干由美创核心技术人员联合杭州电子科技大学团队共同组成，团队骨干成员先后获得浙江省科学进步奖一等奖、浙江省教学成果奖一等奖等诸多重要荣誉奖项，同时基于公司深厚的实践沉淀，均为该项目的开展奠定了扎实可靠的工作基础。



美创荣获“国家信息安全漏洞库 (CNNVD) 技术支撑单位等级 (三级)”证书

10月，美创科技经过多层审核评定，荣获中国信息安全测评中心颁发的“国家信息安全漏洞库 (CNNVD) 技术支撑单位等级 (三级)”证书，成为 CNNVD 技术支撑单位之一。

成立以来，美创科技高度重视在数据库方向上的漏洞研究、挖掘与应对能力，并设立 59 号安全实验室和安全服务部，专注于数据安全攻防技术研究及漏洞挖掘，多次向国家信息安全漏洞共享平台 (CNVD)、国家信息安全漏洞库 (CNNVD) 提交高价值原创漏洞，积极完成各项漏洞挖掘、漏洞处置、漏洞分析、漏洞响应任务，在多个网络安全应急响应及漏洞处置事件中，获得用户高度评价。



杭州美创科技股份有限公司创立大会暨首次股东会隆重召开

10月11日，杭州美创科技股份有限公司创立大会暨首次股东会隆重召开，股份公司全体发起人及股东代表、董事候选人、监事候选人、核心管理团队以及为公司辅导上市的中介机构代表等出席了本次会议。会议进行了首次股东会、董事会和监事会的议案宣读与表决等事项，选举产生了公司第一届董事会、监事会成员。这是美创科技走向资本市场的重要节点，未来，将继续秉承“聚焦数据安全，释放数据价值”的战略愿景，坚定信心，不断创新，为加快数字化转型添砖加瓦。



世界互联网大会 | 美创新品发布——流动安全管控平台

09

11月8日，2022年世界互联网大会“互联网之光”博览会上，美创科技流动安全管控平台正式发布。流动安全管控平台，是聚焦数据流转业务场景，通过数据资产梳理、数据流转监测、安全风险监测、泄密审计追溯等能力，建立数据在跨界、跨境流转过程中的数据安全治理及风险进行监控的一体化平台。流动安全管控平台广泛适用于各行业数据流动场景，如：政府行业各委办局到大数据局间的数据归集、省到各地市/县大数据局数据回流；医疗行业中医联体、医共体内部通过API接口的方式进行数据流转等。



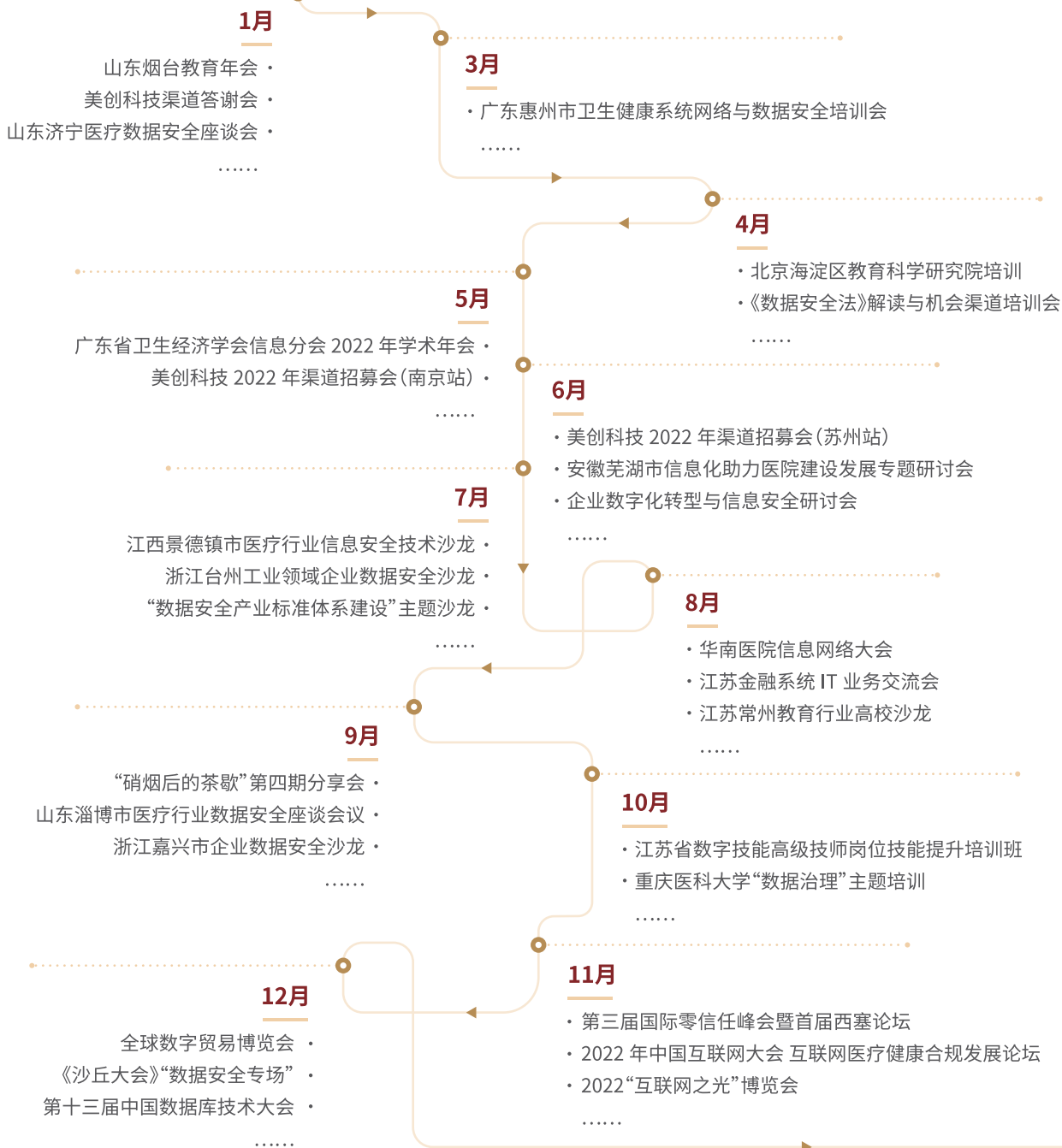
位列 30 名!美创科技入选 《中国网络安全企业 100 强》

10

11月15日，安全牛正式发布第十版《中国网络安全企业100强》报告，美创科技成功入选中国网络安全企业“百强”，位列30名，并入选信创能力10强及数据安全领域代表厂商。十余年坚持自主创新，积累全栈安全能力，美创科技可为行业用户提供API安全监测与访问控制系统、流动安全管控平台、数据库防水坝、数据库防火墙、数据库加密、数据脱敏、数据水印、数据库审计、诺亚防勒索、数据安全管理平台等一整套自主研发的产品及解决方案。



全年活动掠影





数据交易思享会

5月17日，2022数据安全发展大会系列活动“数据交易思享会”在温州举办，美创科技副总裁王利强出席并分享《数据交易准入安全》。分享中，王利强表示，目前我国数据交易产业仍处于初级阶段，数据流通环节存在诸多风险与难点，如：数据归属权及使用权的权属不清晰、数据安全责任不明、数据定价和利益分配机制不明确等。随着《数据安全法》、《个人信息保护法》的相继实施，数据安全合规需求愈发重要，因此在推进数据要素市场化改革的过程中，对安全风险要及早研究并加以防范，不断加强数据安全合规管控，促进数据要素市场稳健发展。



“数据安全产业标准体系建设”主题沙龙

7月8日，数据安全产业标准体系建设主题沙龙在京成功举办。

本次沙龙由工业和信息化部网络安全管理局指导，由中国软件评测中心、中国信息通信研究院联合主办，杭州美创科技股份有限公司、中国计算机行业协会数据安全专委会共同承办。会上，围绕数据安全产业发展面临的标准问题与挑战、当前数据安全产业标准的急迫需求等议题进行了分享和交流。

美创科技副总裁王平为本次会议致辞。美创科技数据安全合规负责人王泽带来《数据安全标准实践视角下思考与归纳》主题演讲。



第三届能源企业数字化创新发展论坛

7月28日，以“数字驱动，助推智慧能源创新发展”为主题的第三届能源企业数字化创新发展论坛在北京成功举办。美创科技北京中心技术总监李航进行《数字化转型下的数据安全治理实践》主题演讲，为能源企业构建扎实的数据安全防护能力带来新思路。

基于十余年积累，美创以 Gartner DSG、DSMM 数据安全能力成熟度模型、Gartner CARTA、等保 2.0 以及零信任 2.0 数据安全架构为参考模型，沉淀总结出适合能源企业的数据安全治理实践路径，并在实践中不断优化，有效落地。



2022 年华南医院信息网络大会

8月12-14日，“2022年华南医院信息网络大会”在广州白云国际会议中心成功召开。扎根医疗多年，美创科技携最新实践成果及产品方案出席此次大会。

C13 展位现场，美创向参会的医院领导及行业伙伴重点展示了公司在医疗行业的最新实践成果及医院数据安全、精细化数据资产管理方案、勒索病毒防御、临床业务连续性容灾等场景解决方案，充分展示了美创积极响应数据安全发展需求，为医疗行业客户提供多层次、体系化的安全防护能力。



全国民航互联网+智慧机场建设发展高峰论坛

8月18日，第七届全国民航“互联网+”智慧机场建设发展高峰论坛在贵阳成功举办。美创科技应邀参会，并获评“最佳机场数据综合解决方案引领者”奖项。此次获奖，充分印证了行业对美创多年民航服务经验及优质方案和服务的认可。

凭借产品优势和技术创新，该方案还曾获得“年度民航互联网技术优秀解决方案”等荣誉。此外，美创科技还以民航技术服务优秀厂商代表入选民航信息化相关标准制定专家库，积极参与团体标准建设。



BCS 大湾区网络安全峰会

8月17-18日，BCS 2022 大湾区网络安全峰会在深圳成功举办，美创科技 CTO 周杰应邀出席，并在零信任安全论坛发表《基于零信任的数据安全风险治理》主题演讲。

美创认为，数据安全风险治理首先需要在零信任理念和思想的指导下，建立合规认知、数据资产梳理、数据安全风险管控、持续监管运营的数据安全理念，在数据安全建设过程中把握从身份、资产、行为三个层面，结合风险治理六大维度实现切实有效的数据安全防护。



美创亮相 G60 科创走廊（浙江段）专题会议路演活动

9月22日，浙江省科技厅、G60 科创走廊（浙江段）六城市科技局在嘉兴召开 G60 科创走廊（浙江段）建设专责小组专题会议。美创科技作为优秀拟上市企业参与了会议同期举行的路演活动。联合创始人、副总裁闻建霞表示：“非常感谢 G60 科创基金能够给美创提供这样一个平台，我们受到投资人的推荐，有幸获得了这次路演的机会。得益于浙江省数字化改革，让美创的产品在浙江落地，铺向全国。接下来，我们努力走向上市之路。”

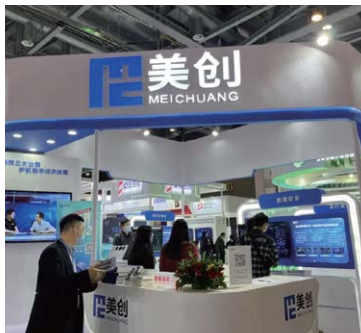


江苏省数字技能高级技师岗位技能提升培训班

10月中旬，第二期“江苏省数字技能高级技师岗位技能提升培训班”在盐城开班。江苏省工匠、高级技师等近 50 名一线高级技能人才参加本次培训。本次培训，美创科技 CTO 周杰受邀并以《数字化时代的企业数据安全建设》为主题，分享“智改数转”背景下，制造企业如何优化数据安全防御理念、构建坚实的数据安全防御体系。

第三届国际零信任峰会暨首届西塞论坛

11月3日，第三届国际零信任峰会暨首届西塞论坛在浙江湖州西塞科学谷成功举办。会上，美创科技 CTO 周杰围绕零信任发展现状、体系建设、市场落地等方面，在“对话用户”圆桌论坛环节作相关分享，并获颁 CSA GCR 专家聘书。同时，美创科技承建的吴兴区大数据发展管理局 DSM 项目荣获“零信任产业发现奖—安全革新奖”。



美创科技亮相首届全球数字贸易博览会

首届全球数字贸易博览会于 12 月 11 日至 14 日在杭州国际博览中心举办，美创科技以“聚焦数据安全新阶段 护航数字经济新发展”为主题，亮相本次盛会，全方位呈现美创科技在数据安全、数字化转型、运行安全领域的创新能力，展示美创科技推动数字经济建设的成果实践，并重磅发布——美创暗数据发现和分类分级平台 - 重要数据版！

区域活动风采

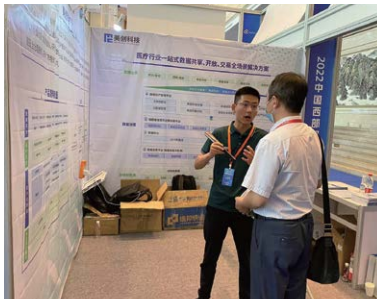


广东：广东省卫生经济学会信息分会 2022 年学术年会

5月14日，广东省卫生经济学会信息分会2022年学术年会在广州举行，会议汇聚了省内医疗信息化领域的大批专家学者，深入探讨医疗卫生信息化的管理经验与发展趋势。会上，美创成功入选广东省卫生经济学会企业理事单位，是对美创在地区医疗行业实力的认可与肯定。

安徽：芜湖市“信息化助力医院建设发展”专题研讨会

6月2日，芜湖市“信息化助力医院建设发展”专题研讨会在芜湖海螺国际大酒店成功举办。芜湖市各医院信息中心、安全管理部分负责人共计20余人参会。美创技术专家现场发表了《医院数据安全建设规划分享》主题演讲。



陕西：2022 西部智慧医疗大会

6月25日，2022西部智慧医疗大会在陕西西安开幕。陕西省卫健委相关领导、知名专家、医院负责人、相关企业代表出席会议。美创科技以展位形式参与本次会议，展示了医疗行业数据分类分级、医疗防勒索等最新的医疗场景化解决方案。

广东：广东教育信息化安全新技术应用创新研讨会

7月9日，广东教育信息化安全新技术应用创新研讨会在广州举行，来自省内近四十家高校信息中心分管领导出席，美创技术专家就教育行业数据安全建设方案作现场分享，并与现场参会嘉宾展开积极交流。





山东：济南市医疗行业数据安全座谈会

7月15日，由美创科技主办的“济南市医疗行业数据安全座谈会”成功举办，济南市儿童医院、济南市中医医院等20多家济南当地医院的信息化负责人莅临现场。美创科技的领导和专家为与会嘉宾带来了主题分享，并与客户进行了交流和研讨。

吉林：吉林市卫生健康行业信息化与网络安全工作会议

7月29日，美创科技亮相吉林市卫生健康行业信息化与网络安全工作会议。美创技术专家进行了《医院数据安全建设方案分享》主题分享，为与会嘉宾介绍了美创敏感数据分类分级等多个医疗场景化防控思路与措施。



浙江 嘉兴：2022年第四届全球工业互联网大会 - 工业数字化人才资源分论坛

7月29日，2022年第四届全球工业互联网大会 - 工业数字化人才资源分论坛在乌镇会议中心召开，美创科技受邀参加，技术专家进行了《勒索病毒安全防护和数据安全治理》主题演讲。同时，美创科技在展台也与多家企业相关负责人进行深度交流，进一步开拓嘉兴企业市场。

浙江 宁波：大数据发展管理局组织开展周二夜学暨“大数据讲堂”活动

8月10日，宁波市大数据局周二夜学暨“大数据讲堂”在宁波城市大脑运营指挥中心召开，宁波市大数据发展管理局及各处室负责人参加。各个处室的负责人以及全体宁波大数据局人员参加培训。售前总监张建林受邀进行分享，现场发表了《构建五大体系 实现全域数据安全治理》的主题演讲，反响热烈，获得高度认可。





福建：2022 高校信息化创新研讨会

8月16-17日，2022 高校信息化创新研讨会在福建福州隆重召开，福建地区近半数高校信息化负责人应邀出席，美创技术专家现场分享《高教行业数据安全建设与探索》，备受关注。期待在福建团队持续跟进下，地区教育市场稳步开拓。

江苏：苏州生物医药行业研讨会

8月26日，苏州生物医药行业研讨会在苏州园区顺利召开。美创技术专家分别围绕数据要素市场化进程中的安全合规风险问题以及当下生物医药行业数据安全面临的内外部威胁分享了美创科技数据安全建设实践以及勒索病毒主动防护与体系化数据安全建设等内容。



内蒙古：2022 年第三届内蒙古 IT 行业论坛

9月22日，美创科技以“展位 + 演讲”的形式亮相内蒙古数据安全高峰论坛暨 2022 年第三届内蒙古 IT 行业论坛。美创技术专家带来主题分享《新形势下数据安全治理实践思考》。

重庆：重庆高校数字化转型下的数据安全治理研讨会

9月23日，由美创科技主办的“重庆高校数字化转型下的数据安全治理研讨会”顺利举办，西南大学等二十余所高校的40多名客户出席。美创技术专家带来《高校数据治理体系化解决之道》主题分享，美创科技产品与解决方案支持中心总监胡大海带来《高校数据分类分级与数据安全落地之法》主题分享。





美 · 实力

MEICHUANG · STRENGTH

数说安全牛 嘶吼安全 中国信通院 数世咨询
IDC 数说安全 嘶吼安全 中国信通院 数世咨询
FreeBuf 数说安全 嘶吼安全 中国信通院 数世咨询
FreeBuf 中国信通院 数世咨询
嘶吼 IDC CCIA

美创入选 IDC 《中国数据智能市场概览》报告

国际知名的市场调研机构 IDC 发布《Market Glance: 中国数据智能市场概览, 2022》报告。作为国内专注数据安全的厂商, 美创科技凭借领先的产品技术及品牌综合影响力成功入选该报告, 位列数据安全供应商版块, 有力彰显了美创在数据安全领域的实力。



美创入选《IDC TechScape: 中国数据安全技术发展路线图, 2022》 报告两大技术领域推荐厂商

全球权威 IT 市场研究和咨询公司 IDC 重磅发布《IDC TechScape: 中国数据安全技术发展路线图, 2022》报告。美创科技两款产品“暗数据发现和分类分级系统”、“数据脱敏系统”, 以强有力的技术优势、创新能力、市场竞争力, 成功入选主导型技术领域推荐厂商, 再一次彰显美创科技在主导型数据安全产品技术领域的实力。

IDC PeerScape: 医疗数据安全实践洞察入选案例

滨州医学院烟台附属医院

滨州医学院烟台附属医院汇聚着大量的、样本丰富的病理研究、药物开发等多个领域的医疗数据。为了更深入地挖掘数据的价值，医院成立了数据治理工作领导小组和数据治理工作办公室，并与启明星辰信息技术集团股份有限公司达成战略合作，共同建设了以场景化为依据的数据安全治理平台。

基于上述实践，医院建立了统计数据信息资源目录，设计了适合于院内业务需求的内部数据安全分类分级标准，并在此基础上完善了安全管理的技术措施。医院基于数据的全生命周期风险分析管控，建设了实用的、动态的、可持续性的数据安全管控体系。

湖北省医疗保障局医疗保障信息中心

湖北省医疗保障局医保信息平台数据量大、业务复杂，数据安全面临严峻挑战。同时，面对网络和数据安全监管的升级，及《国家医疗保障局关于印发加强网络安全和数据保护工作指导意见的通知》的发布，平台亟待转型和升级。

经过仔细的调研和分析，湖北医保局决定同杭州美创科技股份有限公司展开合作，共同以信息安全等级保护为目标，统一规划和提供从网络安全到数据安全方面的双重加固。

湖北省医保局通过部署数据安全管控平台，优化安全策略，高效完成业务访问审计和监督告警，从而保障项目上线至今尚未发生过数据泄露、失密等安全事件。

济南市儿童医院

济南市儿童医院的业务增长使得院内的各类系统逐渐增多，传统的网络及数据安全防范手段难以满足快速增长的数据和业务需求，也无法满足等保2.0时代的合规要求及医疗数据安全规范和指南。医院需采取更具针对性数据安全措施手段。

医院与杭州美创科技股份有限公司开展合作，首先从数据脱敏和数据库运维安全建设两方面入手，提升防护手段。

医院通过应用静态数据脱敏系统，实现数据脱敏流程的标准化、自动化、智能化处理；通过部署数据库防水坝，解决数据库运维场景面临的越权访问、非法/无意操纵数据、敏感数据外泄的难题。

清华大学附属北京清华长庚医院

清华大学联合清华长庚医院、青海大学附属医院、青岛大学附属医院进行医疗数据汇集并建设国家肝胆数据平台。如何保障医疗数据安全，尤其是跨多个医院的远程医疗数据集成和远程读取数据的安全保障成为该项目成功的关键。

医院选择天融信科技集团股份有限公司为该项目的安全服务商，共同从管理和技术两个方面完善数据安全治理策略。

通过安全升级，院端已完成交互数据68435条敏感数据的去标识化处理；实现传输时数据的加密处理；阻止非法外联行为193次，阻断无意识数据泄露行为3856次；累计审计日志71986条。



© IDC |

美创医院客户入选《IDC PeerScape: 中国健康医疗数据安全实践与案例》

国际知名市场调研机构 IDC 发布《IDC PeerScape: 中国健康医疗数据安全实践与案例》，美创科技助力济南市儿童医院进行的数据安全建设项目，成功入选报告。

2022年中国网安产业竞争力50强

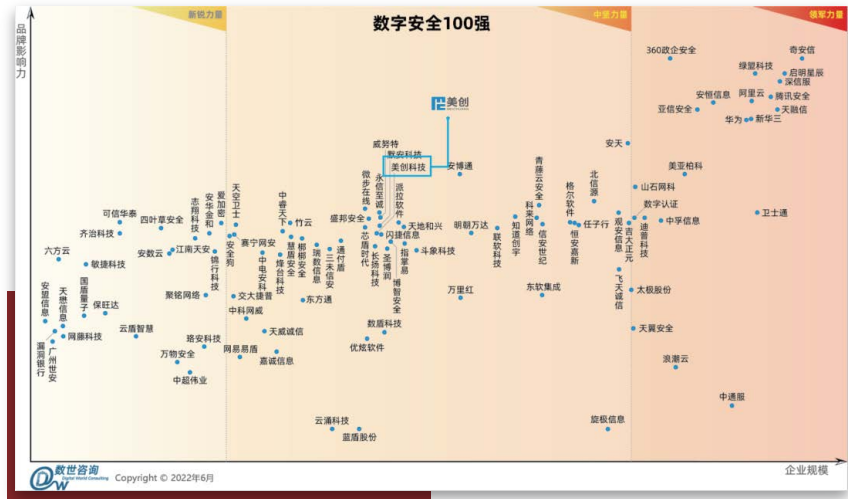
1 奇安信科技集团股份有限公司	11 360数企安全集团	21 长春吉大正元信息技术股份有限公司	31 北京威盾技术有限公司	41 北京安华金和科技有限公司
2 深信服科技股份有限公司	12 亚信安全科技股份有限公司	22 北京长亭科技有限公司	32 远江康邦(北京)网络安全科技股份有限公司	42 北京蓝博河高新技术股份有限公司
3 启明星辰信息技术集团股份有限公司	13 成都卫士通信息产业股份有限公司	23 北京信安世纪科技股份有限公司	33 杭州网安技术有限公司	43 北京优炫软件股份有限公司
4 天融信科技集团股份有限公司	14 杭州迪普科技股份有限公司	24 北京北信源软件股份有限公司	34 北京翰步在线科技有限公司	44 北京梆梆安全科技有限公司
5 华力技术有限公司	15 山东网科通信技术股份有限公司	25 沈阳东软系统集成工程有限公司	35 长藤科技(北京)有限公司	45 深圳市联软科技股份有限公司
6 绿盟科技集团股份有限公司	16 中孚信息股份有限公司	26 北京安博通科技股份有限公司	36 杭州美创科技有限公司	46 山东华软金盾软件股份有限公司
7 腾讯云计算(北京)有限责任公司	17 上海观安信息技术股份有限公司	27 恒安高新(北京)科技股份有限公司	37 格尔软件股份有限公司	47 上海斗象信息科技有限公司
8 阿里云计算有限公司	18 北京数字认证股份有限公司	28 北京升腾腾拓科技有限公司	38 北京永信至诚科技股份有限公司	48 博智安全科技股份有限公司
9 新华三技术有限公司	19 厦门市美星创科信息股份有限公司	29 成都科来网络技术股份有限公司	39 网信科技股份有限公司	49 融数信息技术(上海)有限公司
10 杭州安恒信息技术股份有限公司	20 安天科技集团股份有限公司	30 北京知创字节信息技术股份有限公司	40 任子行网络技术股份有限公司	50 北京天地和兴科技有限公司

美创入选“2022 CCIA 中国网络安全竞争力 50 强”榜单

由中国网络安全产业联盟（CCIA）发起，数说安全提供研究支持的“2022 年 CCIA 中国网络安全竞争力 50 强”正式发布。凭借在数据安全领域的领先优势，美创科技再次入选，综合排名第 36。

美创入选《2022 年中国数字安全百强报告》

国内数字化产业第三方调研与咨询机构数世咨询正式发布《2022 年中国数字安全百强报告》。百强报告中的“综合实力百强”，通过品牌影响力和企业规模两大维度，以数轴点阵图的形式予以展现。美创科技以在数据安全领域的专业领先实力，入选“综合实力百强”的中坚力量序列。



排名	企业名称	分数
1	中孚信息	9.36
2	天融信	9.20
2	亚信安全	9.20
4	奇安信	9.10
5	美创科技	9.06
6	华为	9.04
7	格尔软件	8.90
8	信安世纪	8.89
9	安天	8.83
10	安博通	8.81

美创多领域入选

《中国网络安全企业 100 强》（第十版）

安全牛正式发布第十版《中国网络安全企业 100 强》报告，美创科技成功入选中国网络安全企业“百强”，位列 30 名，并入选信创能力 10 强及数据安全领域代表厂商。

美创科技作为国内领先的数据安全厂商，积极推动核心技术自研及行业信创实践，可为行业用户提供信创版本数据安全产品和解决方案，包括：数据安全管理系统、数据脱敏系统、数据库审计系统、数据库防火墙系统、数据库加密系统等，并已在政府、金融行业成熟应用并获得认可。



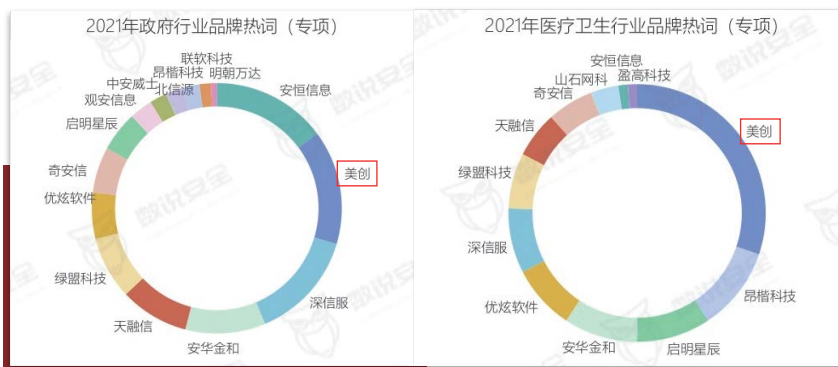
美创入选《2022 数据安全产业竞合力洞察报告》

嘶吼安全产业研究院正式发布《博观约取·精微入神：2022 数据安全产业竞合力洞察报告》。美创成功当选数据安全专精特新型厂商，并入围数据安全产业需求行为图谱，入围解决数据安全合规问题、数据资产梳理 / 分类分级、数据安全防护等 10 个细分领域。



美创多领域、行业、案例入选《2022 年数据安全市场报告》

网络安全产业机构“数说安全”发布《2022 年数据安全市场报告》，美创数据安全品牌、行业、案例全体现，入选数据安全厂商全景图数据分类分级、数据库加密、数据脱敏、DLP、数据库安全、存储备份与恢复等 8 项细分领域，某政务大数据局数据安全平台建设案例同样入选报告。



美创入选 《2022 中国网络安全产业势能榜》

网络安全垂直媒体嘶吼网络安全产业研究院正式发布《嘶吼 2022 中国网络安全产业势能榜》评选结果。凭借在政务数据安全领域的服务深耕以及广泛的市场认可，美创科技入选势能榜“政务篇”，获评政务行业“专精型”安全厂商。

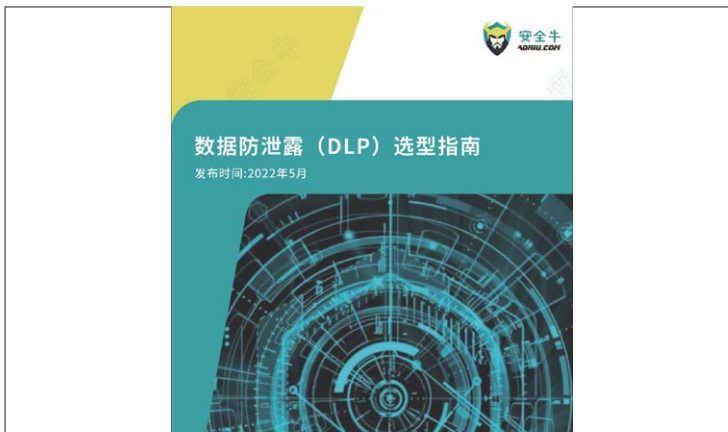


美创入选 《企业勒索软件防护应用指南》 代表性厂商

安全牛正式发布《企业勒索软件防护应用指南》报告，美创科技入围代表性厂商，并受邀分析研究勒索防护方案及勒索软件防护成功案例，为各行业用户勒索软件防护体系建设，以及专业勒索软件防护产品的选型提供思路与实用建议。

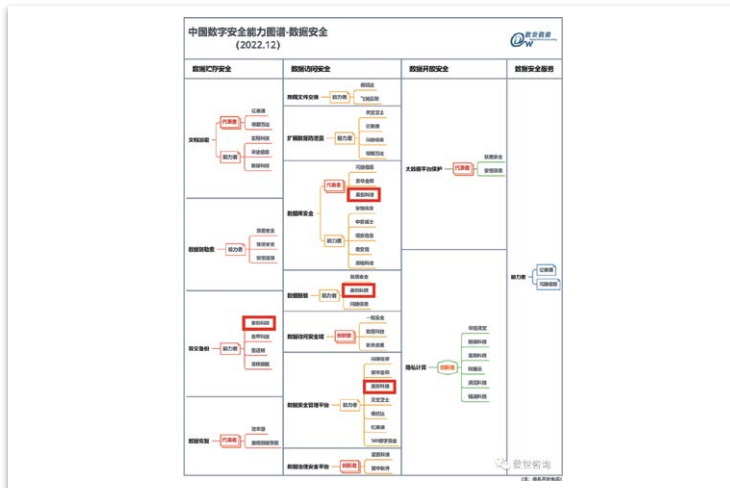
美创深度参编 《数据防泄露（DLP）选型指南》

安全牛正式发布《数据防泄露（DLP）选型指南》报告，融合了甲方、产品厂商、研究机构、测试机构的专业知识和丰富经验，为组织根据自身的需要进行精准地 DLP 产品选型提供支持和帮助。作为我国领先的数据安全厂商，美创科技在敏感数据保护技术的研发和应用方面积累了丰富的经验和能力，本次参与《选型指南》的编写，美创从安全厂商视角提供了相关建议。



美创入选《2022 年度中国数字安全能力图谱》“数据安全代表者”

数字产业领域第三方调研机构数世咨询发布《2022 年度中国数字安全能力图谱》，美创科技以出色的产品能力及市场表现入选“数据库安全代表者”，同时入选“数据脱敏”、“数据安全管理平台”、“容灾备份”版块的能力代表厂商！



美创入选《数据安全产品与服务图谱 1.0》

中国信息通信研究院在 2022 大数据产业峰会上正式发布《数据库发展研究报告 (2022)》暨《全球数据库产业图谱》、《数据安全产品与服务图谱 1.0》。美创科技入选《全球数据库产业图谱》数据库安全阵营代表企业，产品服务全面覆盖《数据安全产品与服务图谱》数据安全防护检测、数据安全运维运营、数据安全共享流通、数据安全服务 4 大版块，入围 12 项细分领域。



美创入选

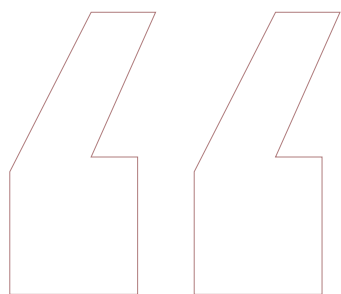
《中国网络安全行业全景图》（第九版）

安全牛《中国网络安全行业全景图（第九版）》正式发布。美创科技实力入选“数据安全”、“网络安全服务”、“身份与访问”、“业务与应用安全”、“云计算安全”五项一级分类及13项二级分类。



美创多领域入选《CCSIP 2022 中国网络安全产业全景图》（第四版）

FreeBuf 咨询正式发布《CCSIP 2022 中国网络安全产业全景图》（第四版）。美创科技入选“数据安全”、“身份识别与访问管理”、“安全服务”、“事件管理 & 响应”四大模块，涵盖 14 个细分领域。其中，数据安全模块各细分领域美创全面入选。



美 / 载誉

MEICHUANG
PRESTIGE

荣誉是企业实力的彰显，是企业持续快速发展的见证；荣誉是对企业的肯定和嘉奖，更是激励企业前行的力量。美创科技始终以“数据安全的领导者和引路人、数字化转型的推动者”为愿景，在过去一年中得到了众多认可和荣誉。



资质认证 (部分)

- 入选“2022-2023年度网络安全技术支持单位”
颁奖单位: 浙江省委网信办
- 入选“国家信息安全漏洞库(CNNVD)技术支持(三级)单位”
颁发机构: 中国信息安全测评中心
- 获得四项“安全服务资质(二级)”证书
颁发单位: 中国网络安全审查技术与认证中心
- 入选“信创政务产品安全漏洞专业库技术支持(三级)单位”
颁发单位: 国家工业信息安全发展研究中心
- 获得“2023年度工业信息安全监测应急支撑单位”
颁发单位: 国家工业信息安全发展研究中心
- 数据安全平台获得“数据安全产品能力验证计划”评测证书
颁发单位: 中国信息通信研究院
- 数据安全平台获得“IT信息安全认证证书”
认证机构: 中国网络安全审查技术与认证中心
- 数据安全平台完成与华为鲲鹏的兼容性互认
认证公司: 华为技术有限公司
- 数据水印溯源系统获得“数据安全产品能力验证计划”证书
颁发单位: 中国信息通信研究院安全研究所
- 数据水印溯源系统获得“IT产品信息安全认证证书”
颁发单位: 中国网络安全审查技术与认证中心





- 数据库审计产品通过IPv6 Ready Logo认证
认证机构:下一代互联网国家工程中心—全球IPv6测试中心
- 数据库审计、数据库防水坝等7款产品完成与联通数御安全管理平台的兼容性互认
认证公司:(广东)产业互联网有限公司
- 数据备份与恢复系统获得中国国家信息安全产品认证证书
认证机构:中国网络安全审查技术与认证中心
- 数据安全平台、数据库审计产品、数据脱敏系统完成与OceanBase的产品兼容性互认
认证公司:北京奥星贝斯科技有限公司

荣誉奖项 (部分)

- 荣获“数据安全服务前十家企业”
颁奖单位:中国互联网协会
- 荣获“2021大数据产业创新服务企业”
“2021大数据产业最具投资价值企业”
“2021大数据产业创新服务产品”
颁发单位:数据猿、上海大数据联盟
- 荣获“CSA 2021安全创新奖”
颁奖单位:CSA云安全联盟
- 荣获“2022杭州准独角兽企业”
颁发单位:杭州市创业投资协会、微链
- 入选江苏省《2022年工业领域数据安全防护方案供应商、优秀产品及解决方案》名单
单位:江苏省工业和信息化厅
- 入选海南省2022年《工业领域数据安全优秀产品、服务和应用解决方案》名单
单位:海南省工业和信息化厅



- 荣获杭州数据安全联盟“最佳贡献奖”

颁奖单位:杭州数据安全联盟

- 荣获CCIA“2021年度先进会员单位”

颁奖单位:中国网络安全产业联盟

- 入选“浙江省网络安全规模十强企业”

颁奖单位:浙江省网络空间安全协会

- 获批成为“电子信息人才能力提升工程”培训基地

颁发机构:中国电子学会

- 入选“数据安全共同体计划”首批成员单位

发起单位:中国信息通信研究院

- 入选信通院“业务安全推进计划”首批成员单位

颁奖单位:中国信息通信研究院

- 荣获“信息技术应用创新工作委员会技术活动单位”证书

颁发单位:中国电子工业标准化技术协会

- 荣获“年度创新力十强企业”

颁奖单位:ISC

- 数据安全平台荣获2022数博会“领先科技成果奖”

颁发单位:中国国际大数据产业博览会组委会

- 暗数据发现与分类分级系统、诺亚防勒索入选“数据与隐私安全领域”、“端点安全领域”热点赛道创新产品

颁奖单位:ISC

- 高校数据安全建设实践入选创新案例报告

颁奖单位:ISC

- 入选“2021年数字赋能促进新业态新模式典型企业和平台”

主管单位:浙江省发展和改革委员会

- 入选“2021年度网络安全工程项目典范实践案例”

颁奖单位:中关村网络安全与信息化产业联盟

- 浙江省农业农村厅项目在中国信通院“星熠”案例评选中荣获数据安全技术与产品应用优秀案例

颁奖单位:中国信息通信研究院

- 台州市大数据局公共数据平台数据安全建设实践获“CSA 2021数字化转型安全支撑优秀案例奖”

颁奖单位:CSA云安全联盟

- 杭州市人社局“数字驾驶舱”项目入选“互联网助力经济社会数字化转型”特色案例

颁奖单位:中国互联网协会

- 浙江省农业农村厅重点应用数据安全服务项目入选“数据安全技术与产品应用优秀案例”

颁奖单位:中国信息通信研究院



美 · 上新

MEICHUANG · INNOVATION

新产品

API 安全监测与访问控制系统

流动安全管控平台

数据安全综合评估系统

新服务

数据安全治理咨询 V3.0

数据出境安全的“知”与“行”

个人信息安全风险评估服务

新解决方案

金融业务应急切换管理解决方案

美创全院级数据中心解决方案

8 个医疗数据安全场景化方案推出

新产品：API 安全监测与访问控制系统

数字化转型已深入各行各业，伴随着数据流动、使用场景大幅增加，API 作为连接数据和应用的重要通道，在各类数字业务中广泛应用，API 接口数量与日俱增，但由此而衍生的安全风险也更为严峻，近年来，针对 API 攻击已成为主要的非法数据获取手段，是影响数据安全和个人信息保护的重要风险来源，加强 API 安全管理，亟需各单位组织重点关注。

API 数据安全问题越来越严峻

SaltSecurity 《State of API Security Report, Q32021》报告显示，2021 年上半年，整体 API 流量增长了 141%，API 攻击流量则增长了 348%，针对 API 的攻击流量正在以普通 API 流量的 3 倍速度增长。

据 Gartner 研报预测，到 2022 年 API 滥用将是最常见的攻击方式；到 2024 年，API 安全隐患导致的相关数据泄露将近乎翻倍。

政企单位落地建设 API 安全却依然存在不少挑战

- 现有 API 资产不清，版本迭代过程中的历史 API 缺乏跟踪，如何进行 API 资产统一管理？
- API 资产面临各种风险，如何有效识别和防护？
- 如何识别 API 访问中的敏感数据并进行过滤和拦截？
- 如何有效管理 API 的访问行为，识别异常的访问行为？
- 数据泄露后，如何自证清白？如何追溯数据从哪个系统被谁泄露的？

美创 API 安全监测与访问控制系统

美创 API 安全监测与访问控制系统是为解决应用 API 接口访问场景下的安全问题推出的一款 Web 应用侧数据安全产品。系统基于 API 资产治理、身份治理、流量管控、访问鉴权、机器学习等多种核心技术，帮助用户梳理庞杂的应用及接口，绘制接口画像和接口访问轨迹，监测敏感数据流动风险，识别接口调用的异常用户行为，为应用系统的业务数据合规正常使用和流转提供数据安全保障。



目 API 安全监测与访问控制系统核心能力



资产识别

通过对流量进行智能分析，配合机器学习引擎识别并过滤静态资源以及 html 响应中的资源，自动发现流量中的 API 接口，实现 API 接口自动识别和分组管理。



API 资产画像

基于全量分析技术精准构建 API 资产画像，快速统计各个业务的 API 情况，包括资产的请求数、访问日历、Web 站点统计、API 列表统计、发现时间、活跃时间等。



身份梳理

基于 http/https 网络、数据库通讯协议解析和流量分析，从人、应用、账号、终端四个维度自动发现网络中的身份，并对发现的身份信息进行管理。



风险监测

系统利用各种检测与分析引擎，从资产脆弱性、资产暴露面、账户共用、异常访问等维度，检测 API 接口资产风险，并对风险进行实时告警处置。



访问控制

基于资产、身份、行为权限矩阵，采用主动防御机制，实现应用数据的访问行为控制、危险操作阻断、可疑行为审计。根据预定义的禁止和许可策略让合法的操作行为通行，而对非法违规操作进行拦截阻断，实现应用 /API 请求的危险操作行为的主动预防、实时审计。

产品能为各行业提供的安全价值

资产全面掌握

智能自动化实时发现、识别网络中的资产信息，内嵌敏感数据识别智能算法，快速识别接口和应用中流转的敏感数据，方便企业及时进行合规检查和整改。

数据流动风险全可控

配合风险预测结果，提供审计、脱敏、访问控制等管控手段，做到风险检测、风险告警、风险响应的全流程安全管理机制，达成数据安全智能管控的“可视化”、“可量化”、“可感知”、“可管控”、“可追溯”。

数据流动全了解

通过对数据流量的监控及分析记录，并以敏感数据与正常数据为维度，对数据的流转趋势进行分析并记录，以数据流的展现形式，将整个数据流转的情况记录在系统中，通过大屏进行数据流动态势展示，从而实现一眼能够掌控数据全部流动情况。

数据流动过程全可审

支持应用程序对敏感数据调用及输出以及业务操作行为的记录，满足法规和监管机构对日志记录要求。

新产品：流动安全管控平台

数字经济时代，数据如水，流水不腐，生生不息，但从安全角度而言，数据流动得越频繁却意味着越不安全：

数据通常从相对安全的环境流动到非安全环境。比如，数据从安全级别较高的生产系统流动到安全级别较低的开发测试系统、分析系统，或流动到其他部门，甚至机构外部。

这一过程数据所有者逐渐会失去对资产的可见和掌控，与数据相关的应用、人员复杂且快速变化、盘根错节，一旦数据流动到不该去的地方，被不该访问的人接触，或流动到不受控的环境，其危害性远远大于数据可能创造的价值。

数字化转型不断推进，大量的数据流动势必成为业务的刚性需求，相应的，流动安全问题也应上升到数据安全建设中的基本命题来高度对待，但从现实情况而言，流动数据安全管理的难度要远大于不流动的数据，政府企业单位面临不少难点：



资产难识别、数据暴露面难监测

组织单位积累了庞杂的接口、应用和数据资产，且不断新增，导致有些接口和应用看不到、管不了，难以有效对API接口、应用、敏感数据流向自动化识别。



数据流转全链路难监控

各个安全设备分散在各个节点，各自为政，无法横向关联由点及面实现内外部数据全流程监控。



数据流动风险难分析

由于缺乏数据关联分析能力，告警中存在大量误报，运维人员需要花费大量时间进行告警研判。



数据流动全局态势难掌控

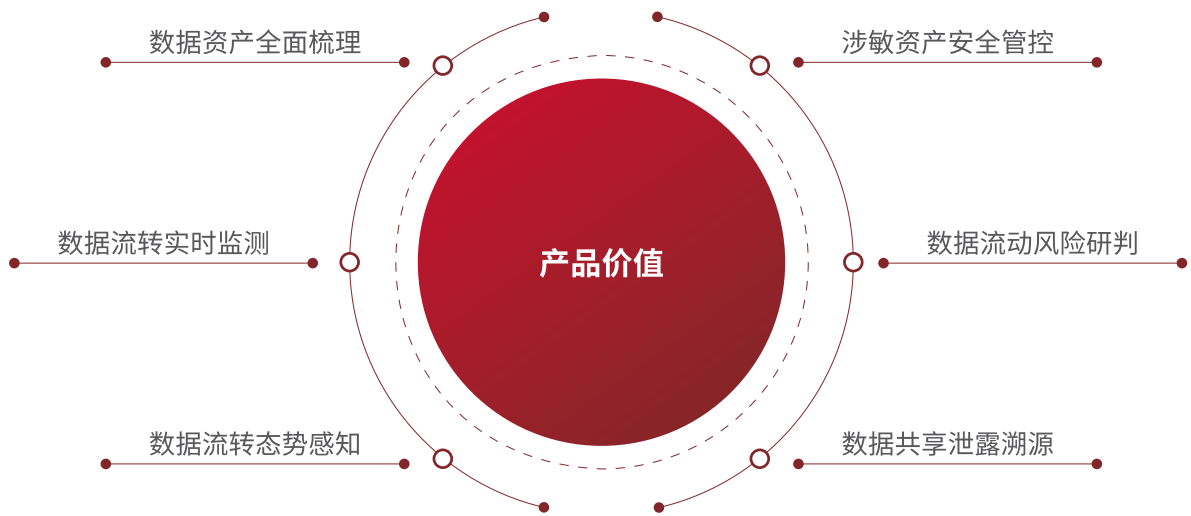
缺少对全局数据安全态势的集中展示，无法直观地感受到安全策略实施效果，监控、接收风险告警和应急指挥。

为解决这些难题，美创科技推出流动安全管控平台，帮助用户有效实现数据流动现状可知、安全可管、风险可视、泄露可溯。



流动安全管控平台

流动安全管控平台，是聚焦数据流转业务场景，通过数据资产梳理、数据流转监测、安全风险监测、泄密审计追溯等能力，建立数据在跨界、跨境流转过程中的数据安全治理及风险进行监控的一体化平台。



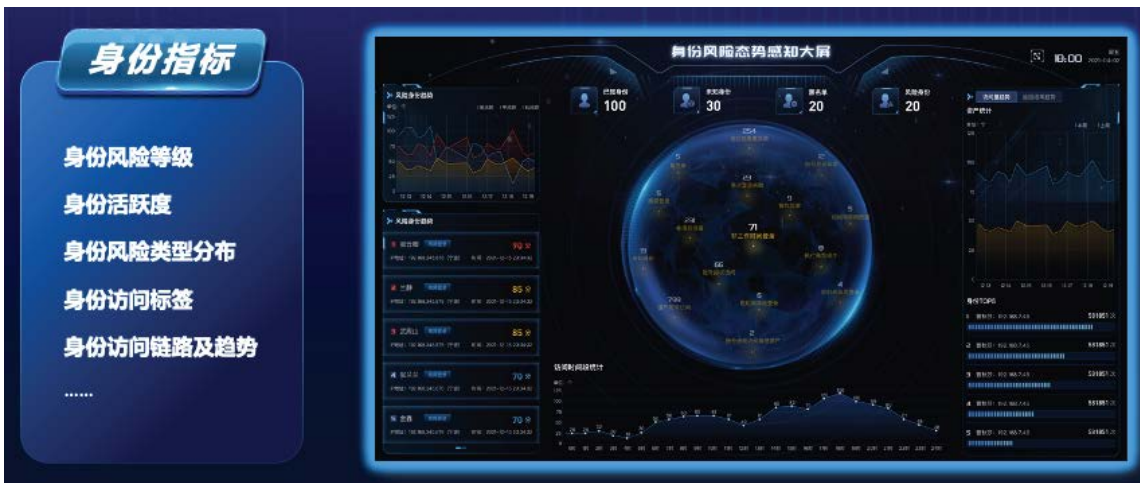
核心功能一：资产治理展示数据全景

流动安全管控平台通过对数据、应用和 API 等资产进行智能数据收集和自动化梳理,识别哪些接口存在敏感数据传输,哪些接口存在对外访问,并对发现的敏感资产结果进行分级分类,统一管控,形成数据资产全景视图,同时可通过采集业务动态访问过程中的流量进行智能涉敏分析,形成数据流转视图。



核心功能二：身份治理建立身份画像

对各类访问来源 / 主体进行实时监测、识别、梳理,通过对访问上下文、访问行为等因素深度分析,建立来访身份画像,形成可统一动态管理的身份资源池,可视化展示访问流量中的已知身份、未知身份、黑名单身份及风险身份总数量,以及风险身份访问趋势、风险身份动态评分、风险身份 top10 以及发布情况,所有清单均可下钻查看详情。



核心功能三：数据流转全流域监测

针对数据访问流转全流域监测,并结合数据安全策略持续优化。流动安全管控平台通过 API 网关及库到库、库到文件、文件到库等监测,对数据内部流动、自内向外流动、自外向内流动情况进行分析和监测,得出数据使用方、数据流出状况等信息,形成数据流向分布图,并持续监测敏感数据访问行为,发现敏感数据泄露风险,并提供追溯能力,管理数据资产全生命周期。



核心功能四：事件溯源定责

联动数据安全组件脱敏、水印、审计等能力,对共享交换过程中可能泄露的数据进行追溯,利用自动化分析技术,快速定位可能的泄露源头,提升追踪溯源的效率和能力,做到事前防范、事中预警、事后追溯,责任到人。



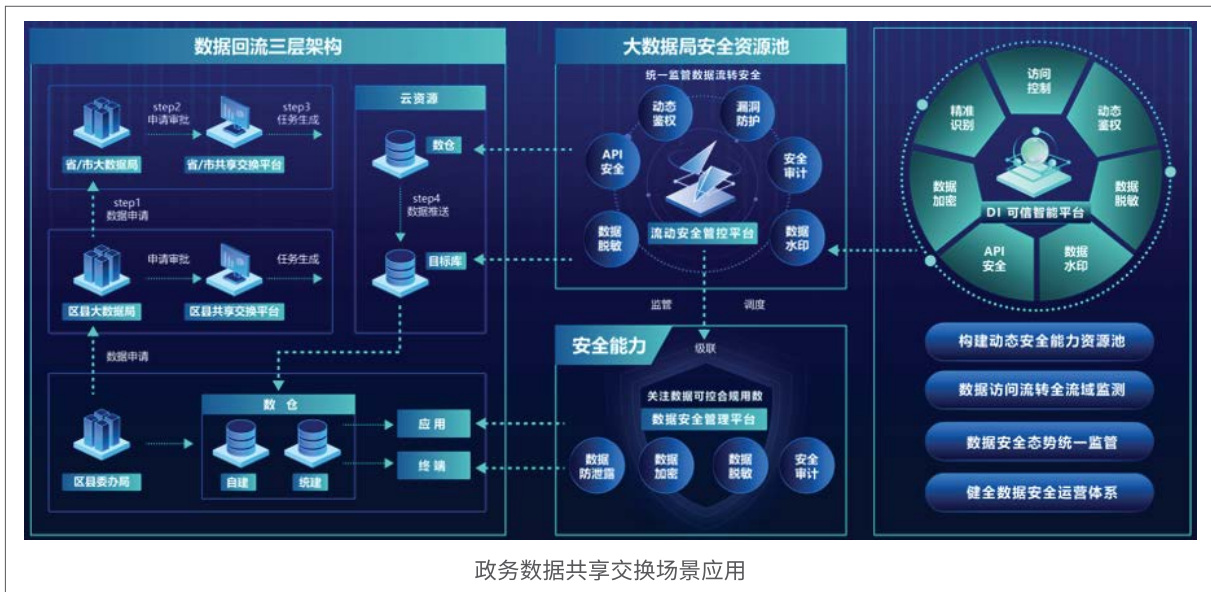
核心功能五：安全态势全局洞悉

从数据流转业务场景出发，围绕敏感资产进行全面分析，对数据流转介质及数据流转链路进行检测，多维度多视角展示敏感资产及数据流转介质分布及使用情况，全方位掌控数据流动安全态势。



应用场景

流动安全管控平台广泛适用于各行业数据流动场景，如：政府行业各委办局到大数据局间的数据归集、省到各地市 / 县大数据局数据回流；医疗行业中医联体、医共体内部通过 API 接口的方式进行数据流转等。



政务数据共享交换场景应用

在数据资产价值不断提升的当下，实现安全有序流通显得异常重要，让资产从未知变为可知、风险难测变为可测、安全从失控变成可控，美创流动安全管控平台持续助力，护涓成流，无惧涛澜。

新产品：数据安全综合评估系统

数字化深入的今天，数据价值和风险相伴相生，让数据要素发挥更大价值，提高风险预见预判，数据安全评估日益紧迫和必要。《数据安全法》提出：“重要数据处理者应对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。”《个人信息保护法》、《数据出境安全评估办法》等法律法规及相关条例规范也均对此明确规定。

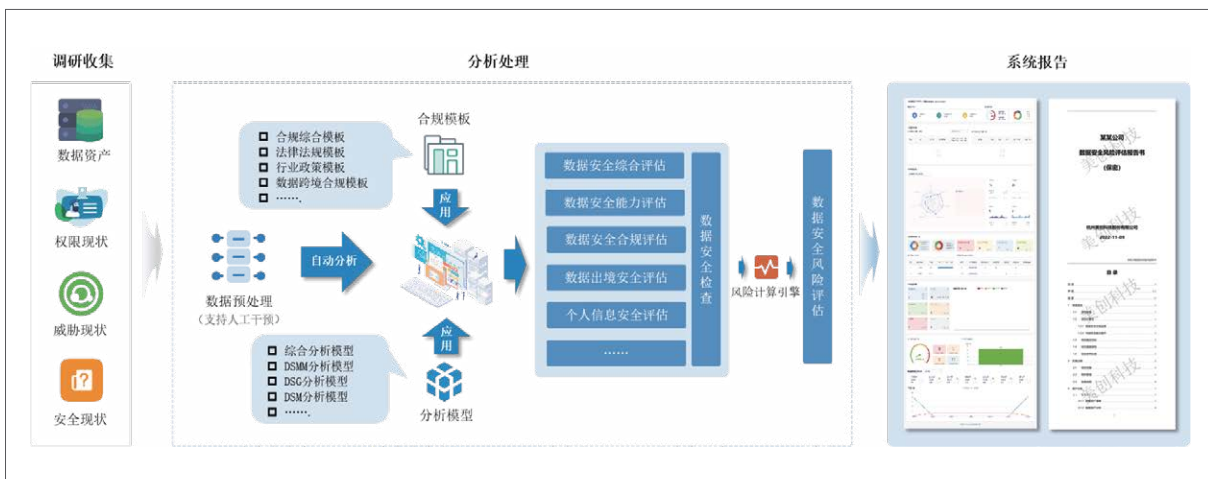
无论是安全之需还是监管合规之要，开展数据安全评估工作都势在必行，然而日益高涨的安全评估需求和当前“缺人才、缺工具、缺方法”的现状形成矛盾，不少单位组织做好这个工作存在诸多难题：

- 数据梳理更多偏向于“台账”的盘点，未对数据资产以及使用权限进行梳理；
- 传统安全评估方式，过高依赖人工核查，落地周期长、成本高；
- 过程评估和过程计算复杂，取决于评估人员能力要求，评估质量难保障；
- 评估工具多种多样，工具之间数据无法互通或关联，导致结果分析存在出入。

深入数据安全评估服务一线，美创熟知应对上述“窘况”，离不开成熟全面的评估方法，兼具行业认知和丰富安全经验的复合型咨询团队。工欲善其事，必先利其器，全面高效的评估工具更是必不可少。

基于数据安全治理咨询团队丰富的项目实战经验沉淀转化，美创科技正式发布数据安全综合评估系统(DCAS)。

数据安全综合评估系统(DCAS)融合数据资产梳理、数据权限梳理、安全现状分析、数据合规基线分析、安全能力差距分析、数据安全风险分析等多重能力，基于强大内置知识库、丰富分析模型、自动计算以及简单操作等特点优势，可对多种风险因素进行多维可视化分析展示，自动化输出高质量报告，帮助单位组织全面、准确、高效、便捷地识别安全风险与合规差距，满足合规需求。



针对目前一对一调研和评估模式下多重采集信息的痛点，美创数据安全综合评估系统采用“流式”产品设计思路，内置多种分析模板、合规模板，通过信息收集和分析松耦合方式，实现“一次采集、多维分析”。

四大能力融合 覆盖各类评估诉求



数据资产梳理分析

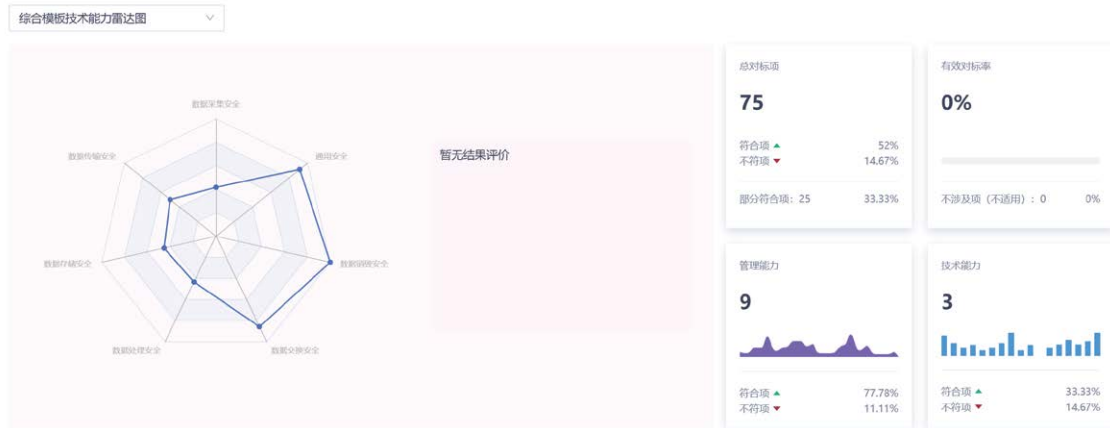
数据安全评估过程中，数据资产梳理分析是基础工作，数据安全综合评估系统支持暗数据发现与分类分级系统接口连接，或结果数据导入，自动多维度分析数据资产，明确数据资产构成、特征、范围及流转情况，自动分析数据权限现状，为后续数据安全风险分析、安全建设规划提供前置信息。



安全能力差距分析

数据安全综合评估系统通过多对象调研，结合对数据基础环境进行安全基线检查、漏洞扫描结果，自动关联匹配和识别组织当下的数据安全保护现状，重点分析存在的安全漏洞和薄弱环节。基于调研结果，自动完成能力评估，包括过程域检查与测试、级别评定、能力缺陷分析、整改建议，实现能力级别和能力差距的详细评估。

能力差距分析





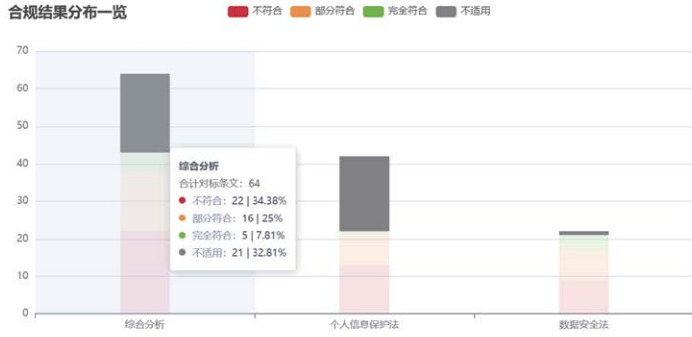
数据合规风险分析

数据安全综合评估系统集合信息采集、评估分析、结果判定、处置跟踪四步，可自动识别并关联分析法律法规、政策规范，以及组织相关条款、现状描述等，最后输出合规评估报告，包括合规统计结果、合规风险情况等，帮助组织充分了解合规义务、安全现状、合规风险，及早规避和关注可能存在的风险。

合规风险分析



合规结果分布一览



生命周期风险分析

针对单位组织数据生命周期各阶段活动，数据安全综合评估系统可依据前置数据采集和分析结果，自动完成生命周期各阶段的风险分析，生成数据资产的全面风险清单和风险预估，同时评估完成后可自动形成可视化报表，如下图所示：



强大知识库 兼备高效与易用



全面

系统内置极为丰富的知识库，全面覆盖法律法规、标准规范、各类分析模型及规则等，数据安全合规库（覆盖 300+ 文件）、数据安全风险库（覆盖 17 大类、83 子类）、安全处置策略库（覆盖 5000+ 条策略），实现评估检查更精准、更全面。



高效

系统以风险计算引擎为核心，以多维知识库、各类分析模板为辅助，通过资产价值、生命周期各阶段安全能力系数、系统脆弱性、风险类型、漏洞数据等各类数据构建一个关联关系的复杂计算网络。

依托该引擎，安全评估人员可分钟级输出完整的数据全生命周期风险评估报告，大幅提升安全评估效率。



易用

系统充分考虑产品的易用性体验，模块化作业功能同步关联内置知识库，安全评估人员根据作业目标，可灵活的对各功能模块自由组合，根据生成的流程路径按部就班地执行，有效降低使用门槛。

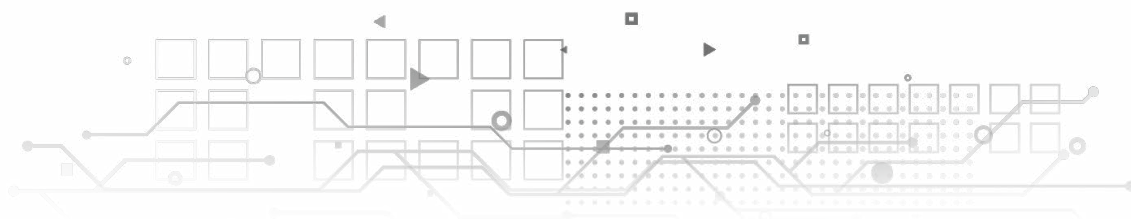


便捷

系统追求出色的计算性能的同时，基于安全评估人员不同环境下的使用诉求，支持一体机部署、软件部署、PC 部署、云服务订阅等多种部署，“只要网络可达即可使用系统”。

此次美创科技发布的数据安全综合评估系统，为用户、合作伙伴数据安全评估工作高效地开展，提供专业落地支撑工具，实现自动化检测、自动化分析、可视化展示、自动化报告，大幅度缩短项目周期，降低人员门槛。

目前，美创数据安全综合评估系统已在高校、金融、政府、跨国企业数据出境等实践中应用，依托该工具，人员投入量有效降低 90% 以上，交付时间缩短 84% 以上。



新服务：数据安全治理咨询 V3.0

让数据安全建设少走弯路，有效落地，美创科技“数据安全治理咨询服务”从率先推出到广泛实践，已获得诸多认可。从实践中来，美创科技也在不断进化自身能力，持续对“数据安全治理咨询服务”优化、迭代、升级。

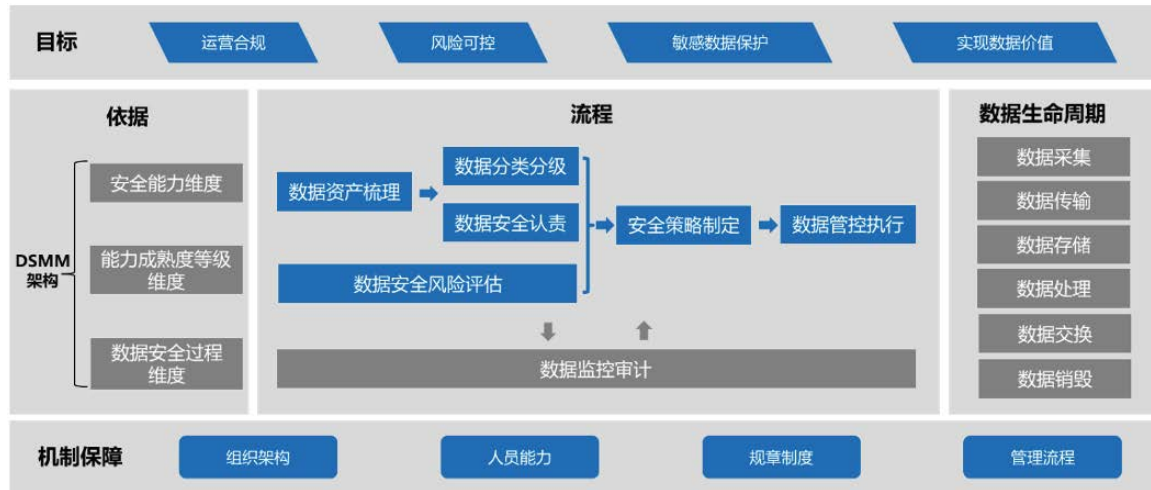
时值《数据安全法》实施一周年，美创数据安全治理咨询 V3.0 新版本，正式亮相！

本次发布的新版本在 V2.0 敏捷版的基础上，对整体方案实践路径进行全面升级，既融合了全新的建设框架，新增 GDPR 等评估服务能力，同时引入更为成熟的落地支撑工具等，使数据安全治理服务更体系、更标准。

从 1.0 到 3.0，数据安全治理咨询服务的演进

V1.0 版本（专项评估）

参考 DSG、DSMM 模型发布数据安全治理解决方案，构建美创数据安全治理咨询服务 1.0 体系框架，数据资产梳理和数据安全风险评估作为快速评估依据。



【关键字：DSMM 模型；探索】



V2.0 版本 (评估 + 规划)

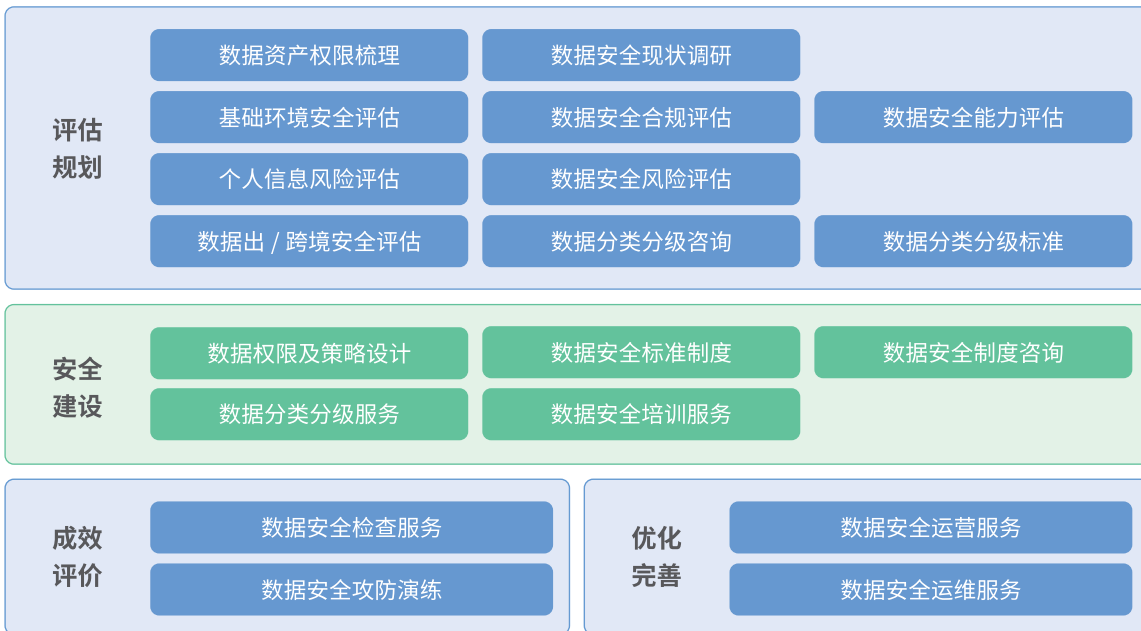
在 1.0 的基础上细化服务内容, 结合美创咨询服务优势、自身数据安全产品特征, 完成 2.0 方案重构。根据实际项目需求, 调整数据分类分级服务, 以咨询和实施两种模式交付, 同时结合参编经验, 建立美创数据安全风险评估方法论, 成为首家以定性和定量相结合的方式分析数据安全生命周期风险情况的数据安全厂家。



【关键字：数据分类分级；数据安全风险评估方法论】

V3.0 版本 (评估 + 规划 + 建设 + 跟踪)

以体系化建设的思想对数据安全治理进行服务闭环, 提供落地建设指导, 体现美创咨询能力和技战能力, 完成 3.0 方案重构。根据客户定制需求, 新增数据出 / 跨境等评估、个人信息风险评估、安全监督检查等服务。



【关键字：客户定制；体系化建设；落地指导】

数据安全治理咨询服务 3.0 升级要点

敏捷型数据安全治理咨询服务 (2.0)

- 周期短，快速评估
- 通过系统试点的方式了解组织大部分现状
- 更偏向于咨询指导，侧重中长期效果
- 建立初步的数据安全制度规范和管理流程
- 适用于应对上级安全合规自查整改、测评认证需求的客户



建设型数据安全治理咨询服务 (3.0)

- 周期长，评估充分
- 以体系建设的思路摸清组织管理、技术现状
- 耗时较长，但更具指导和落地性
- 建立完善的标准化数据安全管理机制
- 适用于想与现有体系融合、有行业标杆或典型案例需求的客户

敏捷型数据安全治理咨询服务 (2.0)

2.0 服务侧重于咨询评估，以 DSG、DSMM 为代表的主流数据安全治理框架作为方法论，以系统试点的方式了解组织大部分的安全现状，开展周期短，主要交付内容为咨询报告和建设规划方案。

适用于快速评估，应对上级监管安全合规检查、自查整改、对数据安全治理需要思路规划以及有测评认证需求的客户。

建设型数据安全治理咨询服务 (3.0)

3.0 服务侧重于咨询评估完成后的安全建设，融合 ISO27001、美创零信任 2.0 等建设框架作为方法论，在 2.0 的基础上对安全管理体系、技术体系、运营体系进行建设或落地指导，虽然耗时较长，但更具指导和落地性，咨询报告和建设规划方案作为第一阶段过程件，并作为服务后期建设依据，最终交付内容体现为安全服务、安全产品等形式。

适用于大型或周期型项目，建立完善的标准化数据安全管理机制，与现有安全管理体系融合、有行业标杆或试点案例需求的客户。

美创数据安全评估系统

在开展数据安全治理服务过程中，美创数据安全评估系统作为最主要的技术工具，是基于美创数据安全治理咨询团队丰富的项目实战经验沉淀转化，系统采用“流式”设计思路，内置多种分析模板、合规模板，将信息收集和分析松耦合方式，实现“一次采集、多维分析”，较好地解决了现有调研方式中一对一调研和评估模式下多重采集信息的痛点。

能够自动化进行数据资产梳理、安全现状识别、数据合规基线分析、安全能力差距分析、数据安全风险分析等服务，直观地展现组织存在的风险，同时该系统也可与美创科技其他安全产品进行联动，帮助组织切实有效地改进数据安全“需求不明确、责任不清晰、管理不规范、建设不匹配”等问题。



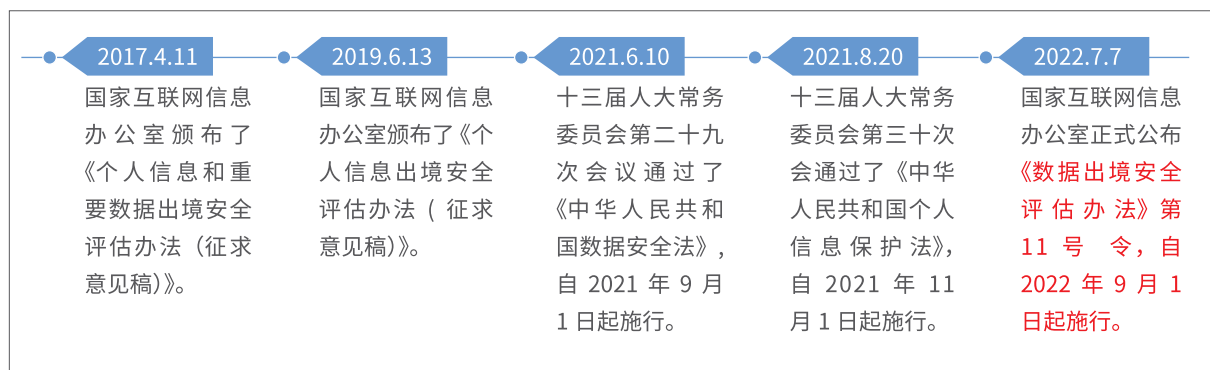
美创数据安全治理服务内容



新服务：数据出境安全的“知”与“行”

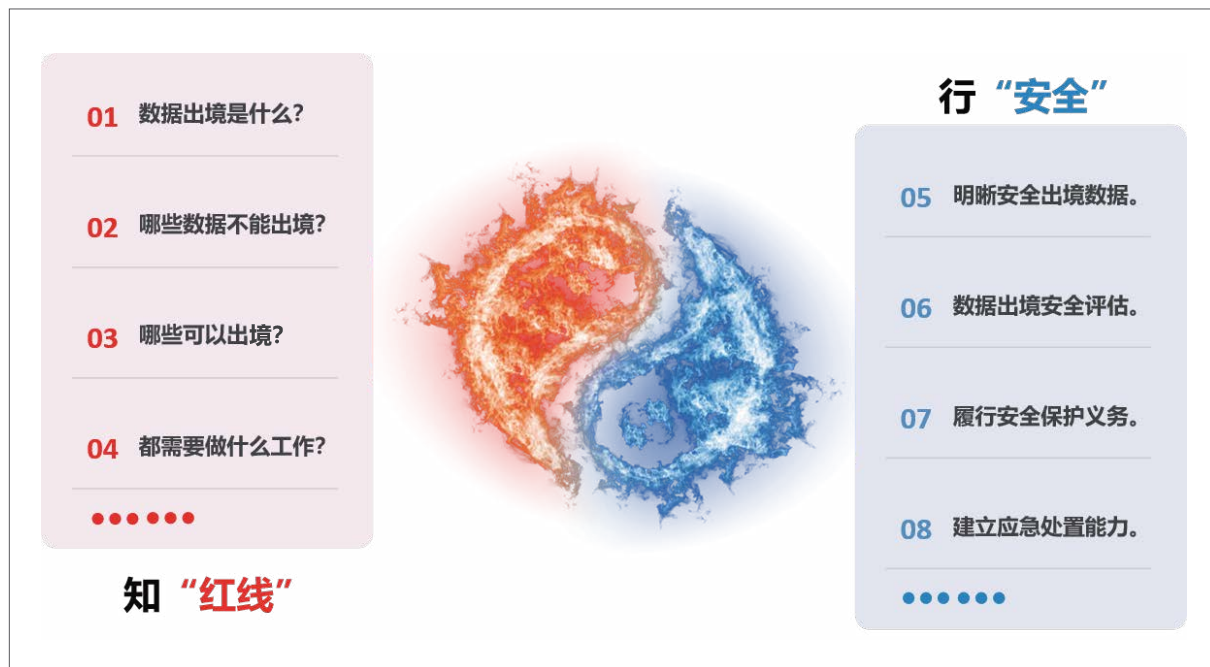
全球数字经济的发展催生海量的跨境数据流动，已经从个人信息泛化到包括非个人信息的一切数据范围，数据跨境成为最重要的话题之一。数据跨境包括国内的数据出境、国外的数据入境以及第三国的数据过境，今天聊一聊我国的数据出境。

我国对于数据出境的监管早在 2017 年就有迹可循，随着全球竞争格局的变化，我国数据出境的管辖法律法规体系日趋成熟，2022 年 7 月 7 日正式发布了《数据出境安全评估办法》，使得出境要求日渐清晰明朗，如：出境情形、开展安全评估、签订法律文件、安全技术保障等，有效指导出海组织降低安全风险，提升数据保护整体水平。



目 数据安全出境的“知”与“行”

知红线、行安全，知行合一，保数据安全出境。



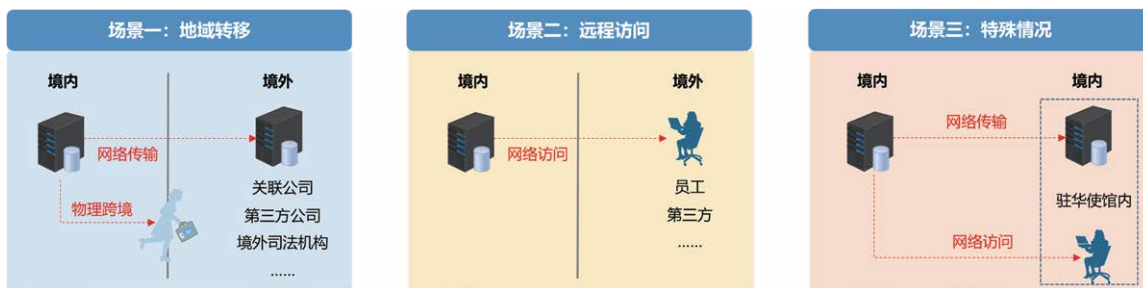
数据出境安全“知多少”

数据出境的定义

《信息安全技术 数据出境安全评估指南（草案）》中数据出境的定义：将在中华人民共和国境内收集和产生的电子形式的个人信息和重要数据，提供给境外机构、组织、个人的一次性活动或连续性活动。（注：境外数据经由中华人民共和国中转，未经任何变动或加工处理的情形不属于数据出境。）

哪些行为是数据出境？

- 1、地域转移：数据通过网络传输或物理转移到境外；
- 2、远程访问：在境外通过网络访问境内的数据；
- 3、其他情况：国外机构获取境内数据，例如境内的驻华使馆通过网络传输或者网络访问获取数据。



哪些数据可以出境，哪些不可以？

数据处理器在境内收集和产生的个人信息和重要数据，如需出境，需要根据要求进行安全评估，根据评估结果确定是否可以出境。（法律、行政法规另有规定的，依照其规定。）



- 1、严禁出境：国家秘密等；
- 2、评估 / 审查 / 许可后出境：重要数据、敏感个人信息、大量个人信息、出境管制技术数据等；
- 3、可自由流动：其他类型数据、国际 / 区域协议明示数据。

目 数据出境安全“如何行”

数据安全出境保障做哪些，怎么做？

组织可根据自身实际情况和需出境数据，由法务和技术人员进行基础的保障判断，可参考如下保障措施进行数据出境准备：

第一步：数据出境安全评估要求确认

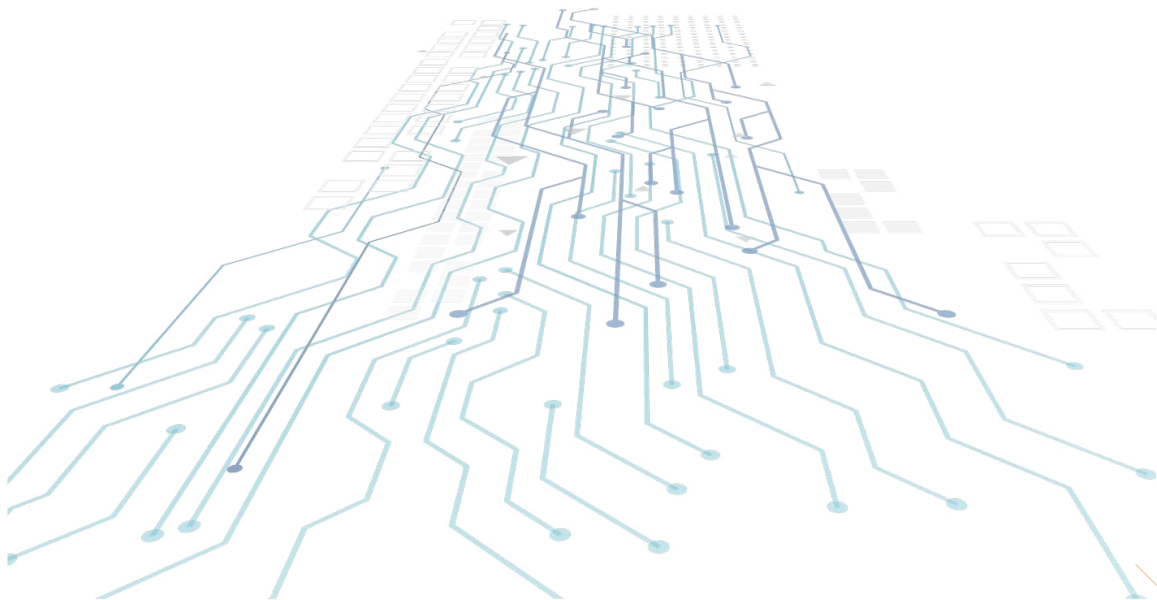
严格按照国家法律法规要求，在重要数据和个人信息的出境活动之前履行数据出境安全评估责任和义务，并将评估结果报送监管单位；根据《数据出境安全评估办法》，符合以下情形，需要进行安全评估：

- ① 数据处理者向境外提供重要数据；
- ② 关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；
- ③ 自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；
- ④ 国家网信部门规定的其他需要申报数据出境安全评估的情形。

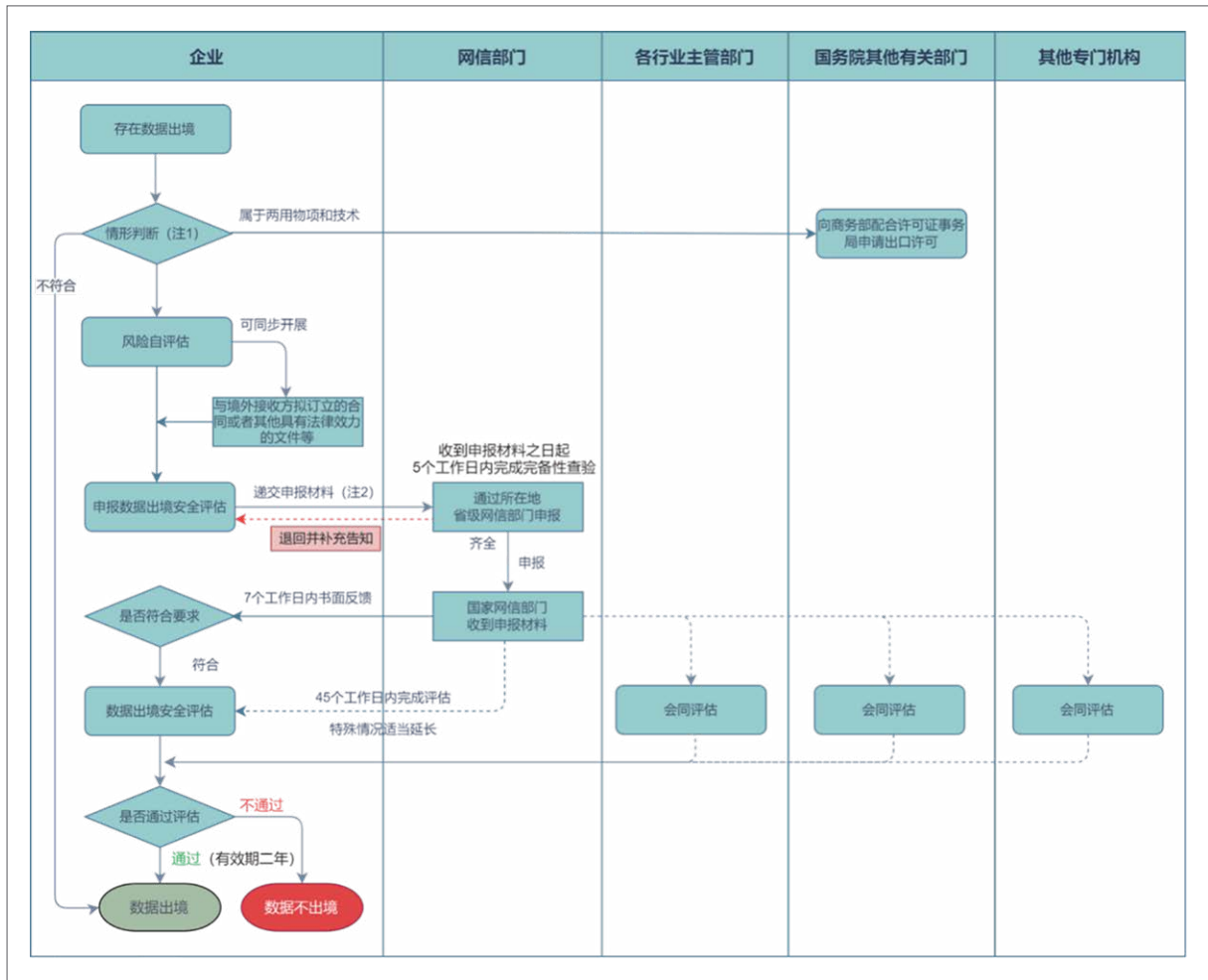
1) 申报材料如下：

- ① 申报书；
- ② 数据出境风险自评估报告；
- ③ 数据处理者与境外接收方拟订立的法律文件；
- ④ 安全评估工作需要的其他材料。

如向境外提供个人信息时，应当事前进行个人信息保护影响评估。（来源：《个人信息保护法》）



2) 安全评估流程如下:



第二步：数据出境安全评估

根据数据出境合规要求，组织开展出境活动所必需的自评，并提交风险自评报告。

美创数据出境风险评估服务：以第三方中立视角协助组织更有效地完成风险自评工作，并提供符合监管审查要求的自评报告。



个人信息保护影响评估服务：协助组织有效评估在各项数据处理活动中的所存在个人信息、特别是个人敏感信息所可能存在的各项风险情况，同时结合对出现个人信息相关安全事件时所造成的影响进行分析的结果，给予相关的处置措施建议。



第三步：数据出境安全保障

1) 数据出境安全加固：建立数据安全保障机制，特别加强数据转移环节的管理和技术措施、能力等，以防范数据出境时的泄露、毁损等风险。

美创数据出境合规指引和加固服务：基于数据出境风险评估结果，提供体系化的数据出境合规指引和针对性的防护策略，并可协助完成策略落地。

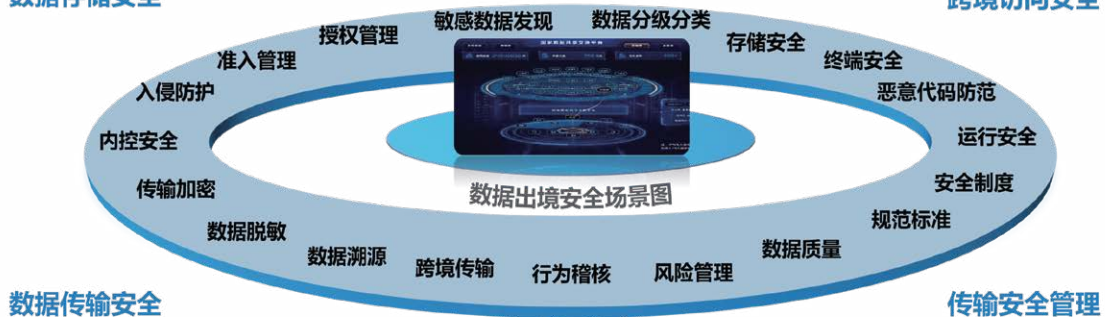
在整个共享交换环节，前置设备作为边缘节点，安全措施做得较为薄弱；

目标：让数据跨境传输安全保障工作更完善、更有效！

数据跨境访问安全容易被忽视，同时由于通道多样化，安全保障工作更难。

数据存储安全

跨境访问安全



数据传输安全

传输安全管理

数据在跨境准备和传输阶段的安全，是数据安全工作的重中之重；

跨境数据安全工作的开展，除了技术保障，更离不开组织和制度保障；



2) 数据出境安全应急响应机制 组织需具备应急响应机制,发生数据泄露、数据损坏等风险时,妥善开展应急处置,并保障个人维护个人信息权益的通畅渠道。

美创可根据组织数据出境实际情况,提供数据出境应急响应制度、应急预案、应急处置流程,以及应急响应服务,协助组织能够在第一时间响应并完成处置工作,最大程度降低损失。

组织进行数据出境自评估和充分安全保障后,数据出境更安全,申报出境安全评估的材料也更充足。

《数据出境安全评估办法》第二十条 本办法自 2022 年 9 月 1 日起施行。本办法施行前已经开展的数据出境活动,不符合本办法规定的,应当自本办法施行之日起 6 个月内完成整改。

美创数据安全服务能力

基于十七年数据安全领域深耕,美创科技贯通安全咨询、架构设计以及安全技战能力,不仅提供全面完整的咨询和建设服务,同时在服务、团队、产品能力上不断提升,旨在为组织提供一站式的数据安全治理服务。

权威的服务资质

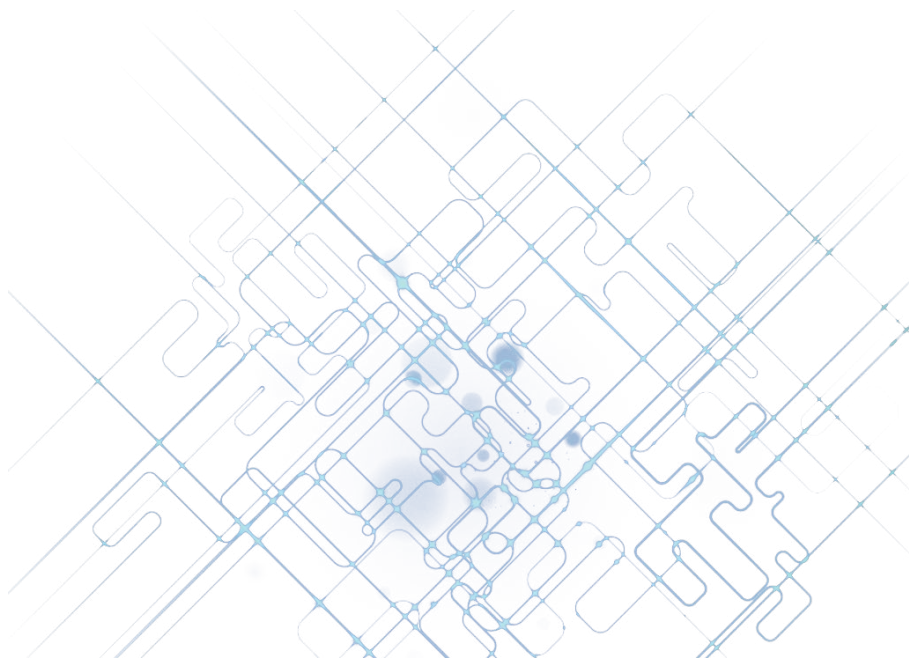
具备 CCRC 颁发的风险评估、安全集成、安全运维、应急处理等多项信息安全服务资质证书。

专业的服务团队

美创数据安全服务团队拥有安全咨询顾问 20+、各类安全服务人员 80+, 以及公司各产线专业的人才资源库。

优秀的产品能力

拥有暗数据发现和分类分级、数据库防水坝、数据库审计、数据库透明加密、数据库防火墙、数据脱敏、数据安全管理平台等众多产品,协助组织落地数据安全防护策略。



新服务：个人信息安全风险评估服务

随着大数据时代的到来，各行业侵犯公民个人信息的违法行为持续增多，个人信息安全问题已经成为一个严重的社会问题，正引发社会高度关注。

2022年7月21日，国家互联网信息办公室公布了此前引发高度关注的“滴滴网络安全审查”案件的处罚决定：对滴滴公司处人民币80.26亿元罚款，同时对滴滴董事长、总裁分别处人民币100万元罚款。

“滴滴网络安全审查”案件回顾

据报道，滴滴公司共存在16项违法事实，主要为8个方面

以体系化建设的思想对数据安全治理进行服务闭环，提供落地建设指导，体现美创咨询能力和技战能力，完成3.0方案重构。根据客户定制需求，新增数据出/跨境等评估、个人信息风险评估、安全监督检查等服务。

- 一是违法收集用户手机相册中的截图信息1196.39万条；
- 二是过度收集用户剪切板信息、应用列表信息83.23亿条；
- 三是过度收集乘客人脸识别信息1.07亿条、年龄段信息5350.92万条、职业信息1633.56万条、亲情关系信息138.29万条、“家”和“公司”打车地址信息1.53亿条；
- 四是过度收集乘客评价代驾服务时、App后台运行时、手机连接桔视记录仪设备时的精准位置（经纬度）信息1.67亿条；
- 五是过度收集司机学历信息14.29万条，以明文形式存储司机身份证号信息5780.26万条；
- 六是在未明确告知乘客情况下分析乘客出行意图信息539.76亿条、常驻城市信息15.38亿条、异地商务/异地旅游信息3.04亿条；
- 七是在乘客使用顺风车服务时频繁索取无关的“电话权限”；
- 八是未准确、清晰说明用户设备信息等19项个人信息处理目的。

同时存在严重影响国家安全的数据处理活动，依据《网络安全法》《数据安全法》《个人信息保护法》《行政处罚法》等有关规定，特对滴滴作出网络安全审查相关行政处罚。

目 强监管下，组织机构如何应对

在全球共同呼吁个人信息保护的趋势下，继欧盟颁布《General Data Protection Regulation (通用数据保护条例)》(简称“GDPR”)之后，我国在2021年颁布并施行了《个人信息保护法》。

《个人信息保护法》正式对个人信息处理规则、跨境提供、个人权利和义务等做出了明确的规定，第五十五条规定：有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录。

- 处理敏感个人信息；
- 利用个人信息进行自动化决策；
- 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
- 向境外提供个人信息；
- 其他对个人权益有重大影响的个人信息处理活动。

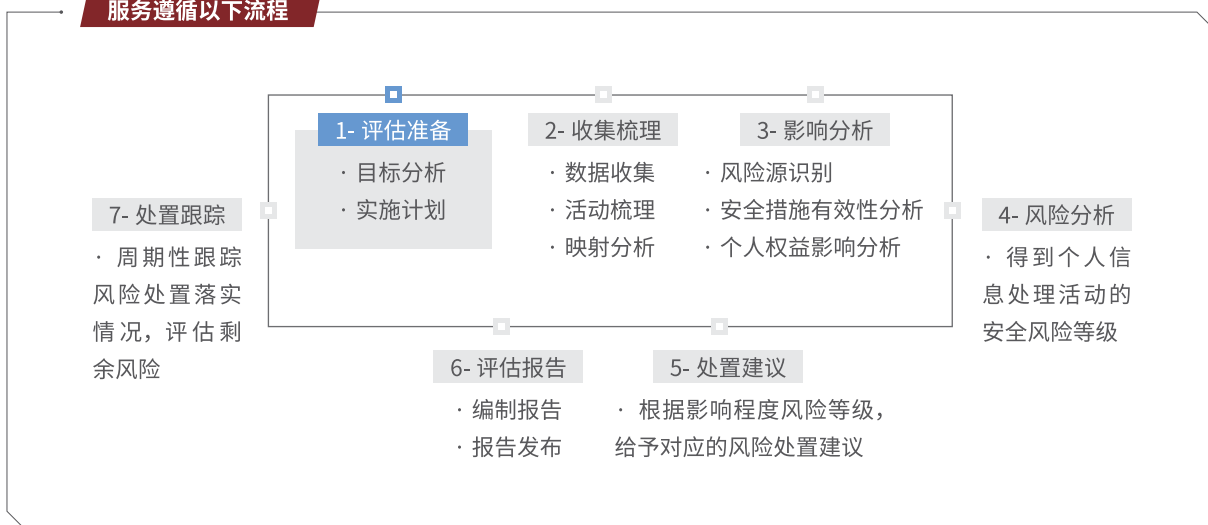
对组织机构（个人信息处理者）而言，为避免个人信息的丢失、泄露、滥用，满足监管合规要求，需尽快开展个人信息安全风险评估工作，充分了解个人信息保护现状和可能存在的影响，再通过相关处置措施，加强个人信息保护，以实现监管合规。

目 美创个人信息安全风险评估服务

美创个人信息安全风险评估服务旨在帮助客户有效评估在各项数据处理活动中的所存在个人信息、特别是个人敏感信息所可能存在的各项风险情况，同时结合对出现个人信息相关安全事件时所造成的影响进行分析的结果，给予相关的风险处置建议。

以符合《个人信息保护法》为基线要求，以遵从《GB/T 35273-2020 信息安全技术 个人信息安全规范》为目的，利用美创个人信息安全风险评估模型，对客户单位的个人信息相关处理活动进行评估。

服务遵循以下流程



评估准备

- 1) 目标分析：或称必要性分析，以确定评估所要达成的目标，并根据设定目标确立评估过程的评判准则，作为风险处置依据的界定性要求。
- 2) 实施计划：依据个人信息保护相关监管和规范要求，组建评估团队，明确各项职责，确定评估对象和范围，制定完整的评估实施计划等。

收集梳理

- 1) 数据收集：通过现场访谈、工具探查、文档审阅等方式对评估范围的个人信息处理过程进行全面的调研。
- 2) 活动梳理：对评估范围内的个人信息处理活动进行归纳整理，输出个人数据流向图，识别并确认所有活动是否被有效记录。
- 3) 映射分析：对调研结果进行分析，对个人信息处理活动进行分类，并描述每类个人信息处理活动的具体情形，形成清晰的个人信息处理活动清单及个人信息映射表，其结果将用于影响分析和风险分析。

影响分析

- 1) 风险源识别：对要素进行简化，归纳为数据环境和技术措施、个人信息处理流程、参与人员与第三方、业务特点和规模及安全趋势。
- 2) 安全措施有效性分析：根据前阶段收集的现有安全措施信息，结合威胁源识别情况，分析安全措施的有效性情况，例如当前采用身份鉴别和访问控制措施是否在个人信息处理各活动场景得到有效应用。
- 3) 个人权益影响分析：分析特定的个人信息处理活动是否会对个人信息主体合法权益产生影响，以及可能产生何种影响，主要包括四个维度：限制个人自主决定权、引发差别性待遇、个人名誉受损或遭受精神压力、人身财产受损。

风险分析

开展个人信息安全风险综合分析，评价安全事件发生的可能性等级，评价以及对个人权益影响的程度等级，综合考虑安全事件可能性和个人权益影响程度两个要素，最终分析得出个人信息处理活动的安全风险等级。

处置建议

根据风险等级，分别给予采取立即处置、限期处置、权衡影响和成本后处置、接受风险等处置方式的相关建议。

评估报告

- 1) 编制报告：综合所有材料及分析结果，汇编输出个人信息安全风险评估报告，报告内容包括但不限于：评估目标、涉及业务场景、个人信息处理活动清单、风险清单、风险分析结果、安全控制措施清单、剩余风险一览表等。
- 2) 报告发布：依据客户组织的报告发布管理策略，并选取适当内容，编制评估结果简报，报送相关监管单位，并依据实际需要向相关方进行披露。

处置跟踪

对客户单位采纳的处置建议等安全控制措施，周期性跟踪风险处置落实情况，评估剩余风险等，完成评估闭环。

个人信息安全风险评估服务价值

实施个人信息安全风险评估，能够有效加强对个人信息主体权益的保护，有利于组织对外展示其保护个人信息安全的努力，提升透明度，增进个人信息主体对其的信任。主要体现在以下三个方面：

- **风险预防**：在开展个人信息处理前，组织可通过影响评估，识别可能导致个人信息主体权益遭受损害的风险，并据此采用适当的个人信息安全控制措施。
- **合规遵从**：个人信息安全风险评估及其形成的记录文档，可帮助组织在政府、相关机构或商业伙伴的调查、执法、合规性审计中，证明其遵守了个人信息保护与数据安全等方面的法律、法规和标准的要求。
- **责任减轻**：在发生个人信息安全事件时，个人信息安全风险评估及其形成的记录文档，可用于证明企业已经主动评估风险并采取一定的安全保护措施，有助于减轻企业的相关责任和名誉损失。



新解决方案：金融业务应急切换管理解决方案

伴随各行业数字化转型的不断深化，业务系统的持续稳定运行已成为信息化建设的最基础诉求。作为业务连续性基础保障的灾备建设，也成为各行业最基础的运行安全设施。

以金融行业为例，金融系统和数据具有全行业高标准的业务连续性和监管安全要求，其具有信息化程度高和信息安全需求高两大特征。以最严格的银行容灾架构为例，大部分均完成本地容灾或本地 + 异地容灾建设，确保银行的数据不丢，业务不停。

但金融机构业务系统复杂多样，各系统、各数据库采用的容灾技术各不相同；同时各金融机构受银保监会、央行等强监管。整体来看，目前金融信息中心在灾备管理及运营方呈以下现状：

- 数据中心灾备实现方式“散、杂、多、乱”；
- 银保监会、央行等监管机构对责任单位的应急预案有突击检查机制；
- 银保监会有明确要求：商业银行应当至少每三年对全部重要业务开展一次业务连续性计划演练；
- 不敢“切”，系统故障时的容灾切换不能确保业务的连续可用；
- 日常演练和应急切换需提交标准报告满足合规审计和归档要求；
- 容灾切换责任大，风险高，需求急，缺乏安全授权机制；
- 面临各类监管和测评考核要求，缺乏日常容灾运营机制。

基于以上现状分析，为提升金融机构应急处置效率，保障灾难场景下的容灾顺利切换和业务的连续，对于应急切换管理系统建设应基于以下原则：

01

资产统一管控

实现数据中心核心容灾资产的统一集中纳管和监控，并实时展示资产运行状态以及 RPO 等信息，并对异常资产提供主动预警机制。

02

一键式容灾演练和灾难切换

平战结合，满足计划内的演练场景和灾难时的切换场景下，对容灾资产的灵活编排和一键切换：1) 面对监管部门发起的突击式容灾演练任务，和计划内的演练任务，支持一键容灾演练切换，确保在数据不丢失情况下的演练切换和一键回切；2) 面对数据中心灾难场景，支持一键业务级容灾切换，确保核心业务连续运行，保障 RTO。

03

报告自动输出

对演练和切换场景提供过程自动截图留存、切换报告自动输出，报告内容满足合规要求。

04

安全授权机制

满足面对内外网完全隔离情况下，业务管理员不在现场的切换任务顺利进行；满足先获取领导或管理员授权，再进行切换的需求。

05

可视化灾备运营

对建设完成的容灾系统，提供日常运营服务，如搭建切换指挥和状态监控大屏，实时显示灾备状态、应急切换过程和切换时长，给灾难发生时的决策指挥提供有力支撑；提供便捷可视化及可持续更新的组织容灾预案管理能力；提供常态化桌面演练和一键自动切换能力。

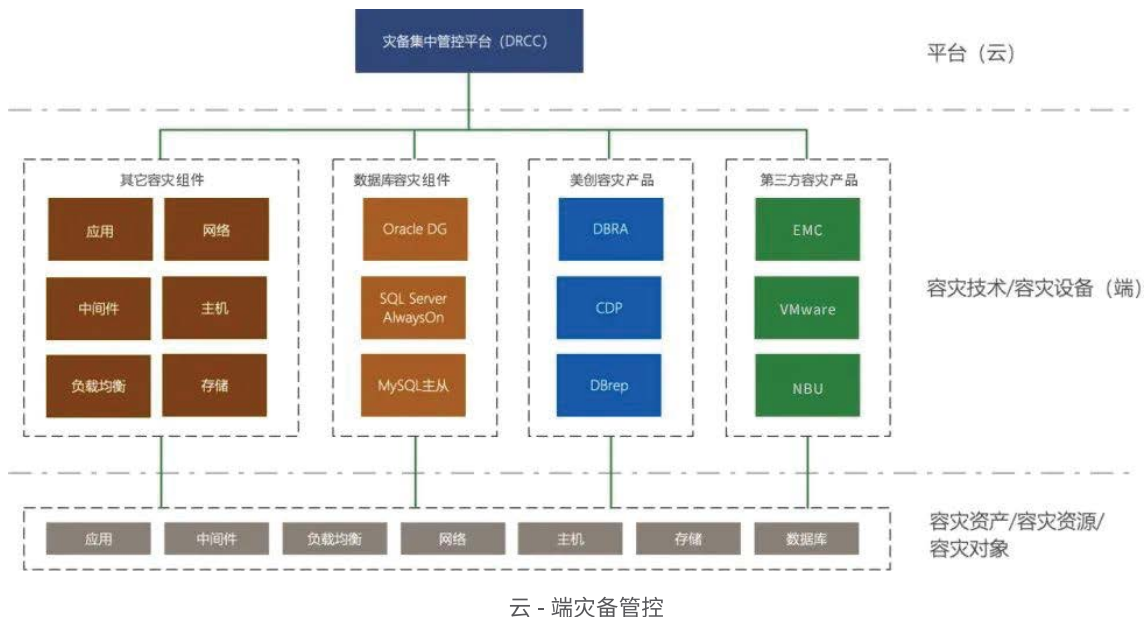
目 美创 DRCC 助力金融应急切换管理系统建设

面对金融行业的灾备建设呈现出多样性、复杂性、规模化等特征，以及相关监管要求和容灾管控现状。美创基于已有的灾备集中管控平台 DRCC 进行优化，持续匹配金融行业的应急切换管理需求。

DRCC 是一款以业务连续性为目标，以业务系统为视角单元的灾备集中管控平台，具备灾备集中管理、故障自动预警，以及应用级一键式切换等业务连续性保障功能，可有效提升银行等金融机构重要业务系统灾备运维自动化水平及应急响应能力，保障辖内业务系统持续稳定运行。



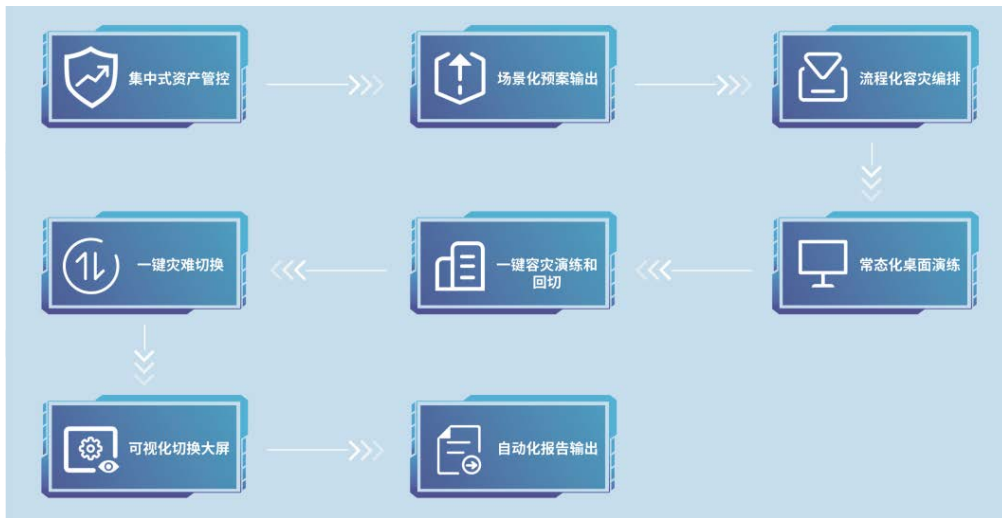
DRCC 灾备集中管控平台为应急切换管理系统建设提供云 - 端架构的解决方案：支持以 DRCC 为中心平台，容灾技术 & 容灾设备为端，实现容灾资产管理、调用和切换，真正做到容灾管控平台化、一体化、智能化。



DRCC 以业务连续性时间 (RTO) 为目标，针对不同类型的灾备接入端实现集中管控，并提供切换预案、切换编排、桌面演练、容灾演练、灾难切换等功能，实现容灾切换流程标准化、自动化和可视化，缩短容灾切换时间，保证容灾切换成功率。

实践路径

为满足合规需求以及真实用户场景需求，美创 DRCC 平台提供从资产接入到容灾运营的最佳实践路径。



容灾实践路径

容灾技术自动发现

DRCC 内置数据级容灾管控能力,用户将搭建好的容灾资产接入平台后,平台通过自动检测技术,实现容灾技术的自动发现,并将发现后的容灾技术及资产进行列表分类展示,并对添加到平台的所有资产,如:数据库、应用、网络、中间件、负载均衡、消息队列等,进行集中式管控。

场景化预案输出

DRCC 内置行业灾备预案模板,覆盖常见灾难场景。同时支持自定义灾备预案内容,支持对添加的灾备预案进行大屏监控和管理,完整的灾备预案信息支持导出,满足归档和审计诉求。

可视化自由编排

用户根据每个业务流以及实际切换需求进行可视化自由编排。通过切换编排功能,彻底改变了传统容灾产品及方案的运行方式,以所见即所得的模式让流程的配置更为自由高效。

可视化编排,灵活设计容灾切换预案。兼顾并行和串行,支持可视化拖拽,可根据用户业务场景,自由编排。以业务 RTO 为目标,持续优化切换流程。切换流程标准化,简单化,为一键切换操作提供基础。

三种演练切换机制

平台目前提供三种切换演练场景:桌面演练、容灾演练以及灾难切换:

- 常态化高频次的桌面演练,在不影响生产端的前提下,提供了数据库级和业务级灾备端可用性的验证机制;
- 计划内或满足上级监管部门考核的容灾演练能力,在保证数据零丢失前提下,验证灾备可用性,通过模拟容灾切换实战的演练过程;
- 灾难场景下的一键容灾切换,创新性的解决传统容灾产品切换过程不完善、切换复杂、流程耗时、易出错、切换不成功等问题。整个容灾切换流程自启动后全程自动化完成,大大减少了误操作风险,保障了切换成功率,降低了 RTO。

切换大屏

平台提供一键切换能力的同时,支持切换过程的可视化展示,提供切换监控大屏和切换指挥大屏,支持多人、全局、动态的切换过程视图,可以让领导直观感知并参与和指挥切换过程,同时为应急场景提供决策依据。

安全授权机制

基于 OTP 技术,平台为现场值班人员、切换负责人员提供切换操作安全授权能力,确保安全性的同时,保障切换任务顺利进行。

自动化报告输出

灾备管理工作一方面有内容归档诉求,要便于审计追溯,另一方面有内容标准化要求,便于规范化管理。面对日常的桌面演练以及容灾演练、容灾切换过程,自动化的输出报告,同时支持报告的自定义,便于归档和审计。

目 美创 DRCC 建设价值

实现应急切换管理系统建设

提升重要业务系统运维自动化水平及应急响应能力，保障辖内业务系统安全稳定运行，维持各业务系统长期安全稳定运行，避免系统因故障产生服务中断、业务数据丢失而产生的各类损失。实现灾备管理、故障预警及应用系统一键式自动应急切换等业务连续性保障功能，并且最大程度满足了 RTO 和 RPO 的要求。

提高运维效率

无需登录多个容灾平台和资源挨个进行状态查看和配置，满足所有容灾的统一管理和监控。

降低技术人员能力要求

预先排好切换手册，对切换流程进行标准化、规范化和可视化；切换流程标准化、规范化、可视化，降低切换操作人员的技术能力要求。

保障业务连续性

灾难发生时，通过战前切换演练，以业务 RTO 为目标，持续优化切换流程，缩短切换时间，确保灾备快速、成功切换。

灾备管控可视化

通过大屏可视化，直观展示散杂多乱的灾备运行状态。形象展示切换状态，进程统计，包括切换完成百分比、切换资源数量、耗时，实时感知切换过程、助力决策指挥。

输出报告且满足监管需求

由于灾难切换任务重大，涉及部门众多，需要事后追溯。DRCC 支持自动输出演练报告，灾难切换报告，便于审计和归档，同时满足相关监管合规要求。



新解决方案：美创全院级数据中心解决方案

随着医疗卫生信息化建设进程的不断加快，医疗数据的规模和类型正以前所未有的速度迅猛增长，多场景数据应用需求暴增，跨部门、跨系统数据流动需求日渐迫切，“传统信息集成平台 + 数据仓库”的模式已不能满足海量数据管理利用以及医院长远发展的需求，需要新建一个“全院级数据中心”。

“集成平台 + 数仓”模式需更新

传统医疗卫生信息化主要是以业务流程、医管政策、医保管理等为驱动，建设过程主要考虑功能实现和业务需求的满足，独立采购标准系统软件。由于各个系统的开发厂商、操作系统、数据库、数据结构存在差异，彼此间很难做到信息的互联互通，导致医院内部形成多个数据孤岛，必要的基本信息共享只能通过一对一接口模式实现，不仅需求调用复杂、数据交互效率低下，而且当子系统和系统间接口越来越多，开发和维护更加困难。

01 信息集成平台

目前基于 ESB 集成总线的信息集成平台替代接口模式成为链接医院内各系统的主流方式，其工作原理是把独立的 HIS、LIS、EMR、PACS 等系统按照统一标准实现交互、集成与协同。



但问题在于，信息集成平台并不能解决数据层面的问题，例如数据质量、数据管理等，数据可用性低。而且随着链接的业务系统增多，接口数量增多，接口的种类和对接方式也随之复杂，在大流量、高并发场景下，信息集成平台承受着巨大压力，可能给医院带来风险，例如：

业务系统与平台的数据交互越来越紧密，一旦平台发生故障，存在业务中断的风险；

平台需要对接众多质量不可控的第三方服务，高峰期业务量过大时，容易出现数据传输延迟或者消息积压；

平台后续的运维、接口开发依赖厂商，费时费力费钱且数据不透明。



02 数据仓库

通常与信息集成平台同一时期建设的还有临床数据中心（CDR），运营数据中心（ODR）、科研数据中心（RDR），原理是按照不同领域模型的不同要求，将数据处理后分别存入。三大数据中心解决了部分数据孤岛问题，并为其上的业务应用提供数据支撑。

但是随着医院业务的推进，技术、流程和方法的日趋成熟，传统方式建设的 CDR、ODR、RDR 在数据体量、数据交互、运维管理等方面已经不能满足医院发展需求，主要表现为：

数据整合缺乏完整性

此前，医院建设 CDR、ODR、RDR 主要由应用系统驱动，例如建设 CDR 支撑患者 360 视图等应用。建设过程仅仅考虑部分业务流程数据，数据体量不大、数据元涵盖范围有限，无法支撑数据的深度挖掘和新的数据应用需求。

数据重复利用率低

随着应用需求增多，一个医院存在“各式各样”甚至多个同样类型的数据中心成为常态，这些数据中心缺乏统一标准、无法交互，无形中形成了新的数据孤岛，且这些数据经过处理后原始性已被破坏，很多时候业务科室依旧需要通过信息科重复获取数据。

给业务系统和信息集成平台造成压力

数据中心通过信息集成平台或通过接口从业务数据库中分别获取数据，例如 CDR、ODR、RDR 都需要从 HIS 获取数据，数据引入费时，多重数据同步会给业务系统和集成平台增加额外的性能负担，同时也增加了不可靠因素。

可拓展性和可维护性差

传统方式下的数据中心与应用系统高度绑定，除了支撑特定的应用系统外，其是否对医院开放数据访问接口因厂商政策而异，部分数据中心是封闭的，即医院用户只能通过厂商提供的应用系统来访问数据而不能直接操作数据。综合以上原因，出于医疗数据管理利用以及医院长远发展考虑，医院需要新建一个“全院级数据中心”。

目 前瞻性方案：全院级数据中心

作为一家深耕医疗健康领域的科技企业，美创科技深刻理解医院在信息化建设、数字化转型不同发展阶段对数据的需求，创新性提出「全院级数据中心解决方案」，帮助医疗机构从根本上解决数据孤岛，理顺各业务系统数据关系，减轻业务系统和信息集成平台的数据压力与维护负担，满足数据应用灵活性的同时避免底层数据中心架构的重复建设，让数据更好的“用起来”。

全院级数据中心具备以下三大特点

01 数据与应用分离，具备弹性与灵活性

全院级数据中心不与信息集成平台或任何应用系统绑定，其内部结构对医院完全开放，医院可以完全的自主使用、自主运维。其拥有极大的弹性与灵活性，可以很大程度改善并发处理能力和存储空间的问题，满足医院业务不断拓展的需求，同时数据统一集中管理，可有效降低医院的运维成本。

02 高度保真性，完整备份原始数据

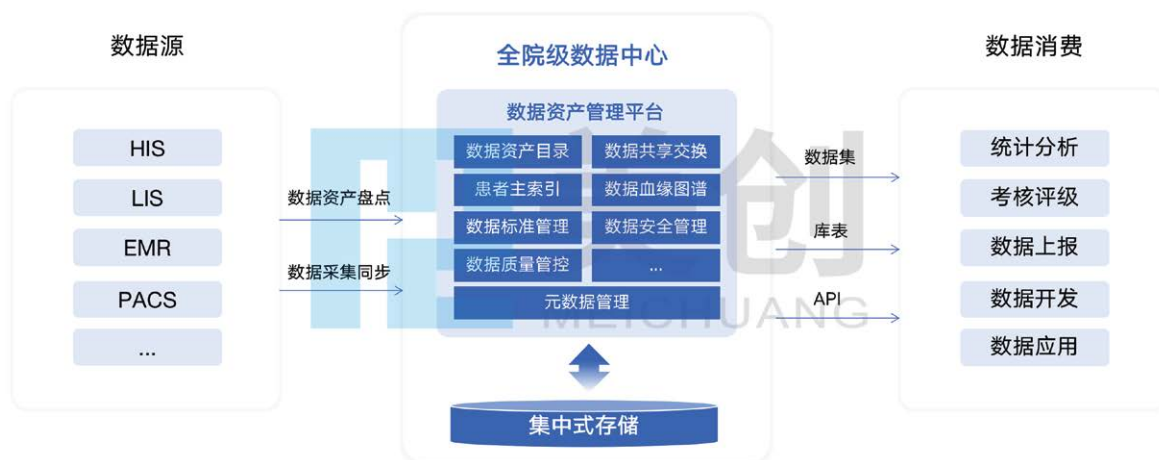
与传统将数据经过处理后存入 CDR、ODR、RDR 的方式不同，全院级数据中心不对数据进行预处理，而是将原始数据直接复制到“数据源湖”形成完整备份，保证数据的完整性、一致性，避免信息损失，同时通过统一的数据资产目录来分类管理这些数据信息，不但可以满足数据共享复用的需求，而且出现问题可快速定位产生问题的源头。

03 作为“统一数据源”，为应用供数

全院级数据中心作为“统一数据源”，可将数据实时分发到 CDR、ODR、RDR 甚至教学数据中心（EDR），或基于数据检索工具供数据使用者按需取用，医院不需要依赖厂商即可完成统计分析、数据开发、数据上报、医院评审等工作。

后续医院在搭建多个数据应用系统时，不需要重复投入底层数据中心的建设，只需要针对特定问题抽取数据进行处理，这样不仅能够最大程度地减少对业务系统的打扰，而且极大地提升了数据处理的效率与质量。

美创全院级数据中心建设方案



「全院级数据中心解决方案」建设框架

目前，美创已帮助多家三级医院、二级医院构建了全院级数据中心，在医院运营管理、临床科研、单病种质控、公立医院绩效考核、医保自查自纠等多个领域发挥数据的价值。

美创基于领先的数据产品和服务经验，为客户提供咨询规划、数据中心建设（包括数据资产盘点、数据分类分级、数据入“源湖”、数据资产目录建设等服务）以及平台搭建等服务。

建设思路如下：**01 采用分布式数据存储架构**

伴随医院数据量增长及数据应用需求的快速增加，需考虑数据中心的可扩展性，以及扩展后保证数据性能、数据时效性等方面不会下降。

方案采用 MPP (大规模并行处理) 架构, 计算和存储资源分离, 解决效率和管理成本之间的矛盾, 可根据业务发展所需, 敏捷扩展更多信息节点, 同时能够与大数据平台其他组件结合 (如 Hadoop), 保证对上层数据应用的充分支撑。

02 多数据源支持

医院内部业务数据源非常多且结构复杂, 如关系型数据库、分布式大数据库、国产数据库以及各种文件类型。因此选择的平台工具需尽可能多的支持数据库环境。

美创数创平台套件具备丰富的数据源适配能力, 支持多数据源接入, 实现数据资产盘点以及多源异构数据的有效采集同步。

03 数据资产盘点, 数据分类分级

合理有效的数据资产盘点是全院级数据中心建设的第一步, 清楚数据在哪里, 数据的流向, 数据的敏感程度, 如何分类和分级, 数据和业务的关系是什么, 将为数据中心架构规划提供指引, 也是后续数据利用和管控的重要依据。

工具的选择上, 方案采用美创自研工具平台, 自动化程度高、内置丰富的医疗模版和指标、接口齐全, 具备目录化、可视化分析管理能力。

04 无侵入式数据采集, 实时捕获数据变化

数据采集主要考虑以下几点: 1、摆脱接口依赖; 2、采集过程不能影响业务系统正常运行; 3、实时性 + 稳定性; 4、减少人工操作。

方案基于美创自研的数据采集工具抽取业务系统存量 2~3 年的业务源数据 (热数据), 同时采用非侵入式增量日志挖掘技术, 通过解析数据库日志文件, 实时捕获数据变化, 所有采集过程对源端无影响, 操作上高度便捷化、可视化, 节省人力投入和运维成本。

05 建设数据资产管理平台

为了更便捷、安全的数据共享和利用, 数据中心需要统一、开放、易用的管理平台支持, 让数据始终拥有一致的控制权限, 丰富友好的信息视图, 实现“一次存储、多人使用、统一管理”。

美创数据资产管理平台建设涵盖元数据管理、数据资产目录、数据质量管理、数据安全管理等模块, 提供数据血缘、数据质量评估、自助查询与取数、API 接口、数据脱敏等功能, 同时针对医院业务特点和习惯, 不断进行功能和交互上的优化。

06 满足政策合规需求

严格执行等保 2.0 的相关要求, 满足《数据安全法》《个人信息保护法》等相关法律法规要求, 关注架构的合理、流程的规范、举措的到位。

07 充分考虑高可用及兼容性

确保后续第三方厂家都可以通过数据中心高效获取数据。

美创始终围绕着“性能、成本、合规、可持续”等医院最为关注的核心问题, 在产品和方案上超前布局。面向未来, 美创将继续积累医疗行业数字化转型服务经验, 不断丰富产品的颗粒度, 助力医院“管好数、用好数”, 向全新的数字医疗时代迈进。

新解决方案：8 个医疗数据安全场景化方案推出

对医疗行业用户来说，数据安全建设已成为“刚需”，但不断变化的临床业务场景和安全形势，如何让安全无缝贯穿医疗数据产生、使用、共享的全流程，是一项庞大、系统性的工作，难点诸多。

解决用户难题，基于多年实践积累和全栈安全能力，对准医疗机构复杂业务场景下面临的不同防护诉求，美创科技正在持续带来更多解决方案。

01

医疗行业数据分类分级场景

医疗行业开展数据分类分级建设是一项实质性难题，由于医疗行业业务复杂、数据带有大量业务属性、数据体量大、格式复杂多样，分散各处，只能单纯依靠人工梳理，准确率低、周期长，且受限于人员专业能力，分类分级工作推进进度缓慢。



数据分类分级实践路径

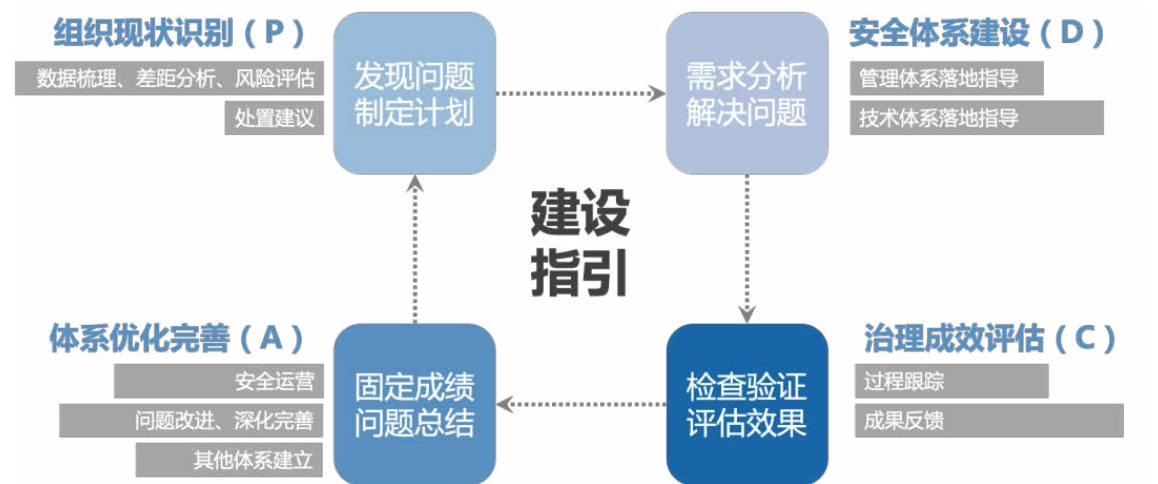
从率先探索到广泛实践，美创数据资产分类分级方案涵盖成熟自动化工具和专业分类分级咨询服务团队，帮助医疗用户智能、快速、准确的梳理和盘点医疗数据资产。

目前，暗数据发现分类分级工具已推出医疗行业版，内置专业医疗行业的数据分类分级模板（可落地参考标准），并引入自然语言处理、统计模型、特征分析、机器学习等技术，实现高精度识别率和流程自动化能力，可大幅缩短建设周期，同时，产品还具备目录化管理和可视化分析、动态扩展能力等优势。

02

轻量级数据安全治理咨询场景

组织内有哪些敏感资产?现状如何?存在哪些合规风险,怎么对数据资产面临安全风险进行消减及转移?明晰以上问题是提高数据安全防护水平必不可少的环节,但传统咨询服务项目周期长、投入大、收尾难,多数医院又通常面临信息安全建设预算有限等问题。



帮助医疗用户在预算有限的情况下,最大化实现数据安全优化和完善。美创科技轻量级数据安全咨询评估与规划,以数据资产安全为出发点,依据法律法规及医疗行业标准,通过数据资产识别、脆弱性识别、威胁识别,及风险分析计算,识别组织数据面临的各种风险,并出具安全风险评估报告、安全处置建议等一系列成果。

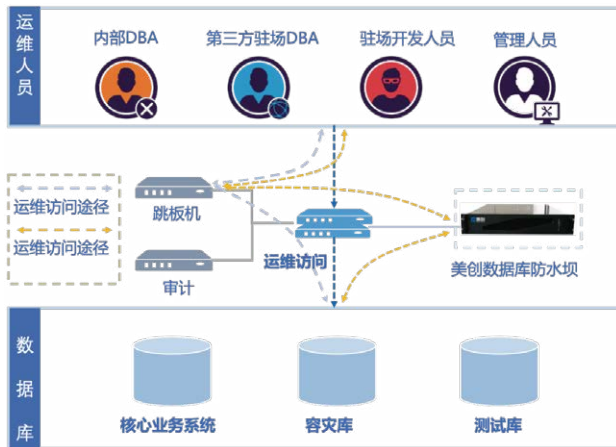
03

信息中心数据安全场景

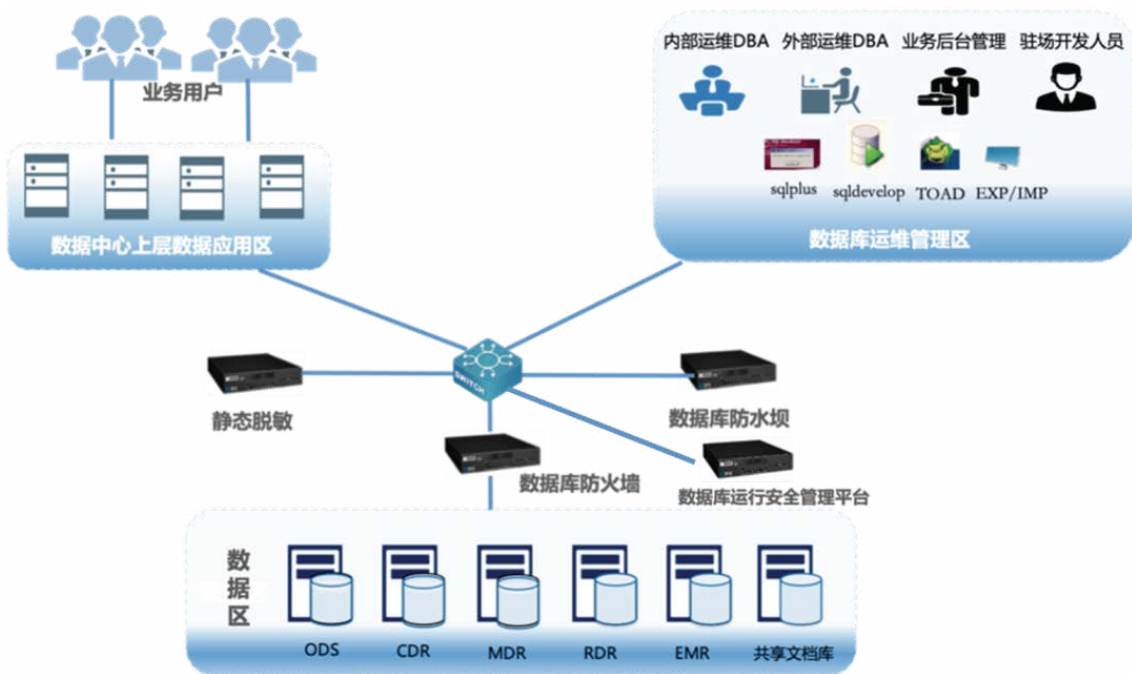
医院信息中心内部人员素质参差不齐,尤其运维人员作为靠近数据最近的角色,权限较大,管理混乱,内部统方事件频发;人为误操作无法避免;新系统上线,老系统运维人员有意无意破坏等产生巨大的安全缺口。

美创科技以数据库防水坝、动态脱敏产品为核心,提供以“数据、身份”为中心的零信任安全管控方案。包括:

- 敏感数据自动发现,以表/列为基础进行管理;
- 运维人员合规管理,多因素接入管控;
- DBA 权限分离控制,防止越权;
- DML/DDL 操作指令控制,防止误操作;
- SQL 操作过程事件回溯,运维合规审计;
- 通过引用数据分类分级结果对敏感数据资产进行管控和审计。



医疗大数据中心汇集着医院所有临床数据与运营数据，数据高度集中汇集，也成为内外部威胁觊觎的“财富密码”，存在如非法登录、越权访问、异常调阅、批量窃取等数据安全风险。



借助静态脱敏、数据库防火墙、数据库防水坝、数据库运行安全管理平台等产品，美创科技提供一站式防护方案。例如：

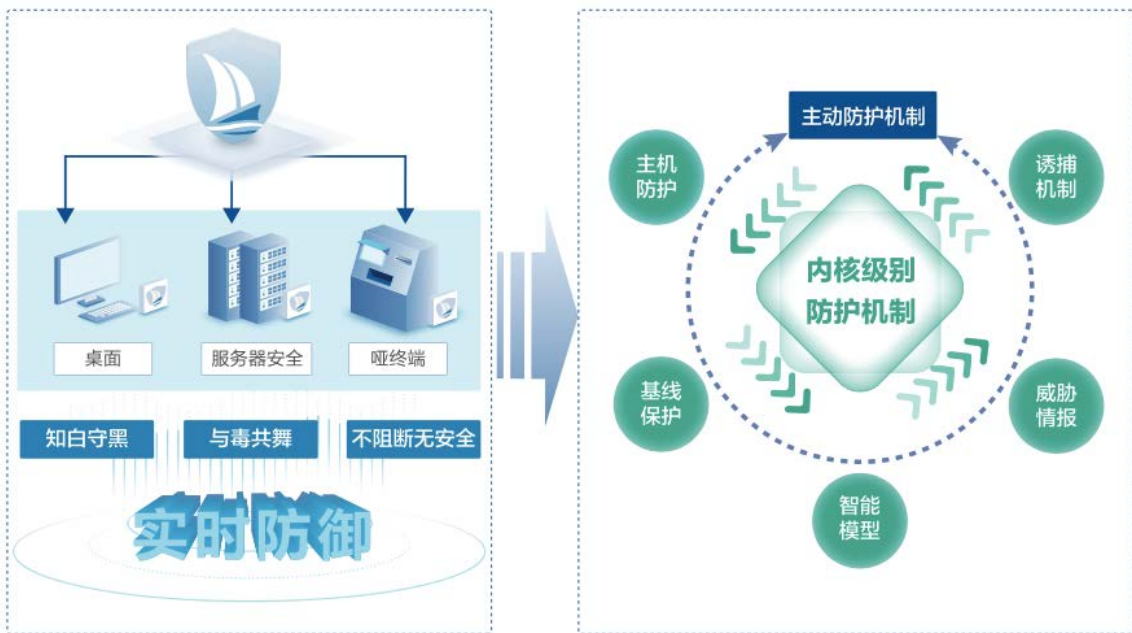
- 大数据中心为各类应用提供支撑数据，美创数据脱敏以丰富的数据源和复杂场景下的脱敏支持能力，帮助实现对提供数据进行分类分级与自动化脱敏处理。
- 大数据中心涉及各类数据的大量采集与清洗，数据库运行安全管理平台作为一款功能强大的数据库运维管理平台，可实时监控数据库运行状态，提前感知运行风险，智能定位问题，利用工具箱快速解决故障，易用性和专业运维闭环能力，真正做到运维高效省心。

05

医疗防勒索安全场景

虎视眈眈的勒索病毒，是医疗行业的主流威胁之一，目前，勒索病毒解决方案仍然以杀毒软件为主，但勒索病毒的变异特征较为明显，会通过更新 / 修改自身代码以绕过杀毒软件的查杀，因此，传统以黑名单为主的勒索病毒防护产品需要频繁地更新特征库，以适应病毒的变化，逐渐捉襟见肘。

怎么做到主动预防？知其白，守其黑，为天下式！



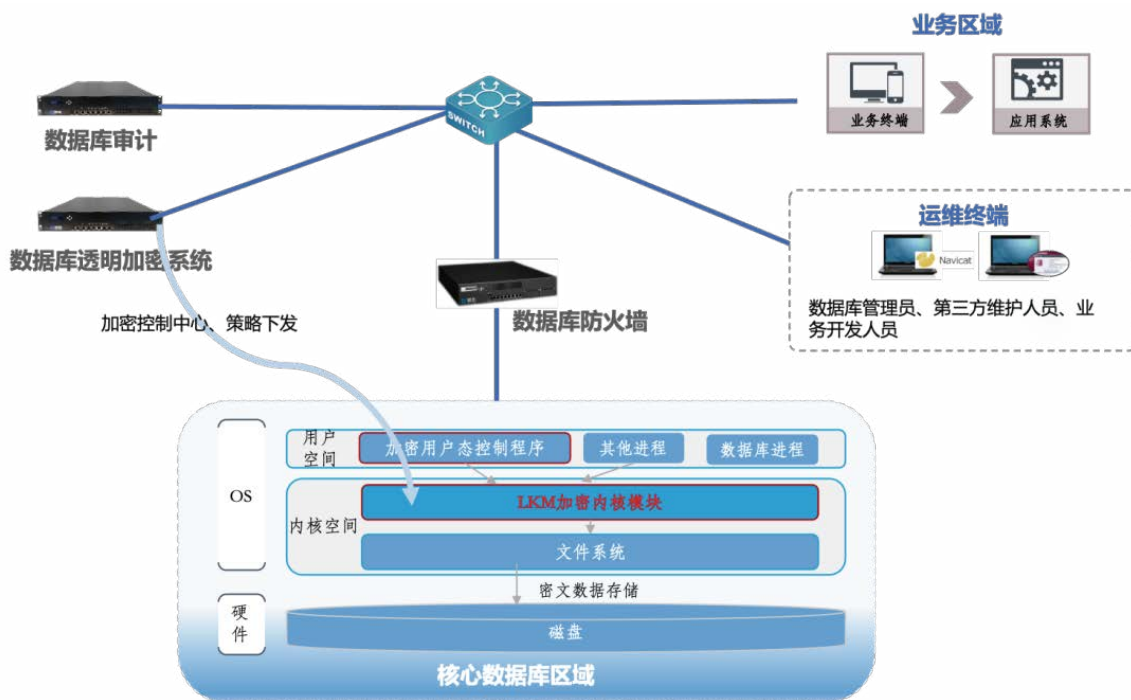
美创诺亚防勒索系统以“知白守黑”、“不间断无安全”的防御理念，快速识别、阻断已知、未知病毒的入侵行为，全面满足医院用户在文档、数据库、哑终端等场景下的勒索防护需求，同时统一的策略，安全管控各主机，无需额外增加安全管理和人力成本，大大节省医院在管理上所需花费的开销。

目前，美创科技已形成多维度勒索病毒防御体系，通过“针对勒索的应急响应服务、诺亚防勒索、容灾备份、勒索防护保险”一体化方案组合拳，帮助医疗用户有效抵御勒索威胁。



医院 HIS、EMR、LIS、NIS、PACS 等核心数据库安全不容有失，需通过技术手段，减少核心数据库的运行风险，杜绝核心数据外泄，并满足互联互通与电子病历测评要求。

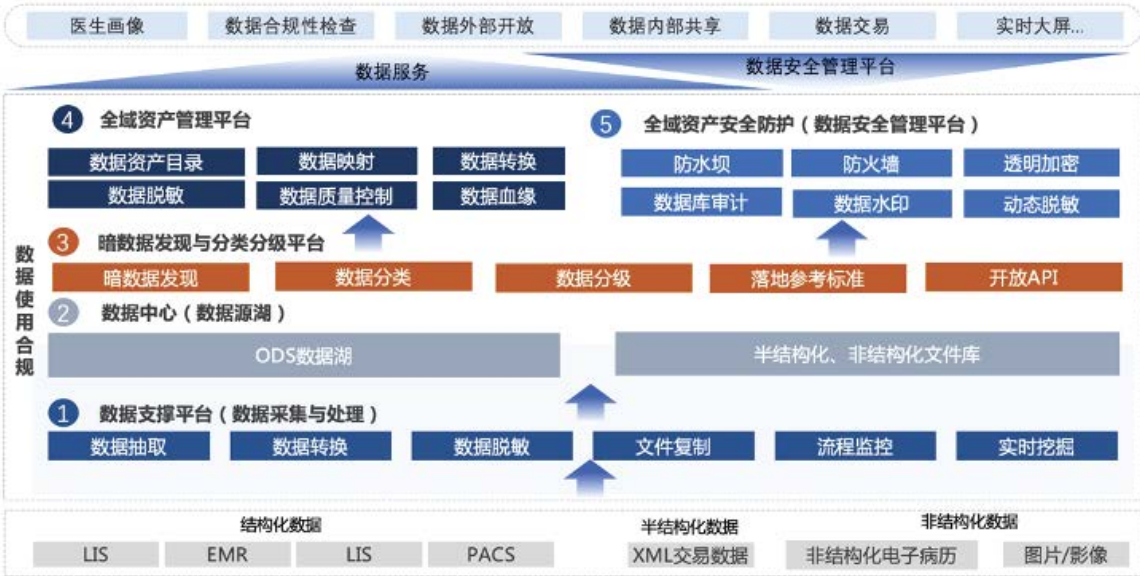
美创数据库防火墙、数据库审计、数据库透明加密等产品打造完善的纵深防御体系，在不影响正常业务流程与保证业务性能稳定的前提下，实现攻不进，看不见，看不懂，拿不走，可追溯。



基于医疗行业特性，美创科技也在不断聚焦用户所需，深入实践，如数据库安全审计系统内置的防统方功能，实时检测针对HIS系统的非法统方行为，针对医院Cache数据库的运维和安全防护需求，数据库安全审计已满足Cache数据库M语言双向审计支持，其他产品完成兼容适配，所推出的医疗影像云脱敏，可针对医疗影像文件中的患者隐私信息（拼音姓名、出生年月、ID）进行脱敏，最大程度避免调阅、医疗教育及临床科研场景下的医疗信息泄露。

医疗数据在临床教学、临床科研、数据上报等均面临流动安全风险隐患。

美创科技以医疗数据分类分级为抓手，从医疗数据合规使用维度，通过全域资产管理与全域敏感资产安全防护两个方面，采用数据脱敏、水印技术、数据流动管控平台等能力，让医疗数据更加安全地进行共享、开放与交易。



如：流动安全管控平台通过API接口、应用与数据资产自动发现梳理、数据流转监测、安全风险监测、泄密审计追溯等能力，实现现状可知、安全可管、风险可视、泄露可溯，让数据共享流转更安全，数据价值释放更充分。

公立医院高质量发展促进行动（2021-2025 年）中明确提到“到 2022 年，全国二级和三级公立医院电子病历应用水平平均级别分别达到 3 级和 4 级，智慧服务平均级别力争达到 2 级和 3 级，智慧管理平均级别力争达到 1 级和 2 级，能够支撑线上线下一体化的医疗服务新模式。”其中基于临床业务联系性的电子病历容灾备份需求是电子病历系统应用水平分级评价体系中重要的评价指标。

作为数据备份与恢复产品国家标准参与制定厂商，美创由 DRCC 灾备集中管控平台、DBRA 数据级容灾、DBrep 数据复制系统、数据备份等组成灾备产品体系，有效满足建设“三位一体”智慧医院背景下多样化的数据安全和业务连续性要求，以及电子病历应用水平分级评价标准第 36 条“系统灾难恢复体系”评价项目全部评价内容。



- 底层搭建备份+容灾的架构多维度保证数据不丢失，灾难来临时按流程恢复数据；
- 应用+数据的编排切换流程，带有整套电子病历系统的切换预案设计，数据库层分钟级切换，应用层脚本切换，降低人为切换带来的时间风险，真正做到一键切换，切换大屏可跟踪、可指挥；
- 桌面演练可感知到备端状态，不影响生产环境，无需回切，保证切换成功率；
- 灾备侧数据安全得到充分关注，在容灾搭建的过程中保护了备端环境，让数据安全真正贯彻到每一个角落。

《数据安全法》、《个人信息保护法》一系列法律法规接连落地，不断增加与升级合规监管呼啸而至，《电子病历系统应用水平分级评价》、《医疗健康信息互联互通标准化成熟度测评》、《公立医院高质量发展评价指标》、《医院智慧服务分级评估标准体系》等医疗机构测评指南中，均对数据安全保护设置评审内容、评审指标、等级要求，数据安全能力成为医院数字化发展的重要指标。

数据安全正当时！从基于数据安全治理的咨询规划、围绕数据全生命周期的安全产品体系、再到综合数据安全运营平台及服务，美创科技全力守护数据安全，面对瞬息万变、不确定的风险与挑战、美创科技也将竭尽所能，不断深入业务场景和持续创新，让数据流通使用变得更加合规、高效、安全。



HI,我是美创数据安全平台
 研发爸爸说我是哪吒
 孕育了三年
 产品妈妈给我起名叫 **DSM**
 UI姐姐给了我这样皮肤



我是谁?

有人说
 我是日志集中管理平台
 有人说
 我是改了名字的网络安全态势感知平台



日志集中管理平台



不就是日志集中管理平台嘛!!



安全态势感知平台

我觉得是改了名字的网络数据安全态势感知平台



其实都不是



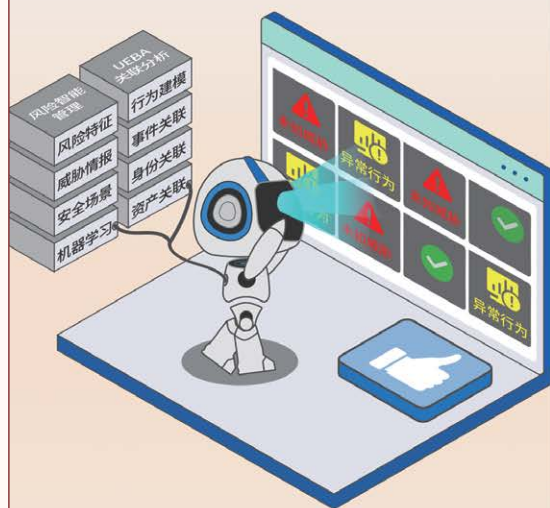
我是新一代数据安全智治产品
IDC的研究显示
我是数据安全基础设施管理平台



数据安全资产、身份、风险智能治理
是对我最好的注释

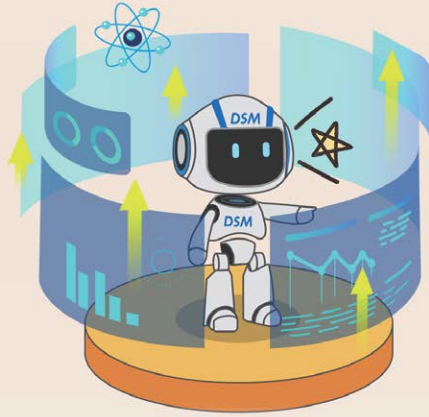


身份合规治理
智能身份分析引擎
形成可统一动态管理的身份资源池

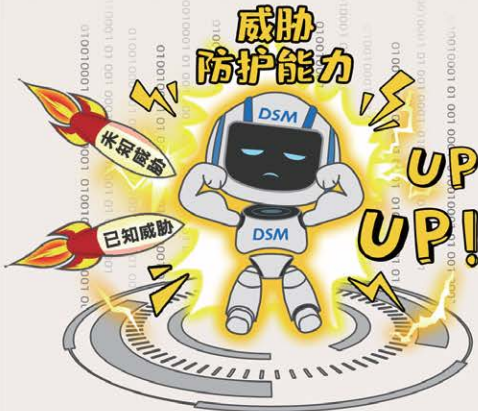


我有什么价值？

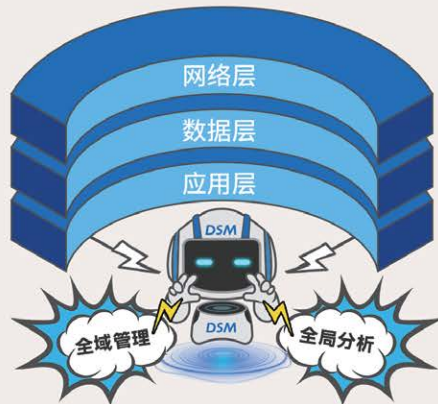
资产透视化、提升运营效率



数据协同分析, 提升威胁防护能力

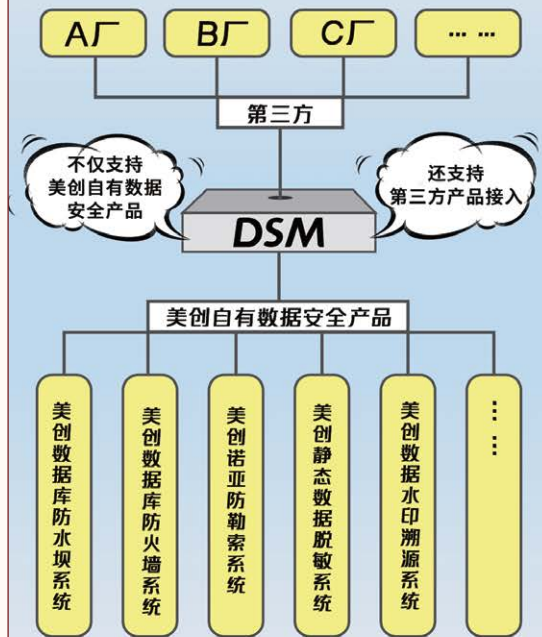


数据安全全域管理、全局分析、协同防御



我的成长

2022年我已经成熟稳定、快速发展



我有多租户版
面向云上租户和业务提供安全服务



我的荣光

OH!

2022年
我是院士评审出来的
数博会领先科技成果

我通过
信通院的检测
我有完备的
市场准入资质证书



Q4许愿

进入甲方爸爸法眼，写入明年预算文件！

甲方爸爸

DSM这么好的平台
我就写进
明年的预算中！





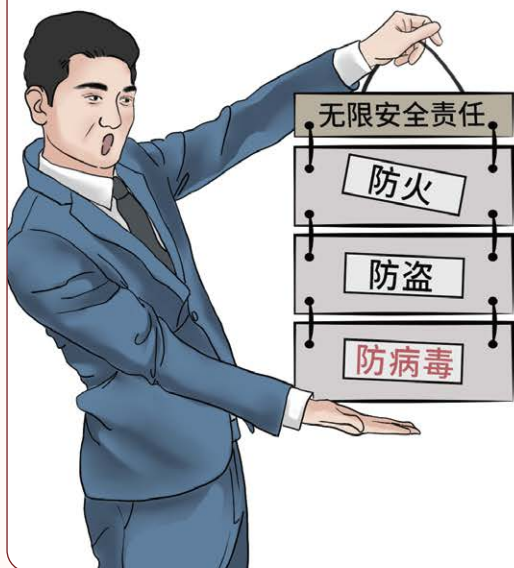
8:30 XX集团

CEO赵总进行Q4安全保障动员会



集团是有限责任制

可我承担着无限安全责任



勒索病毒防护成难题

没落实网络安全防护轻则被罚，重则.....



01:00 忧思难解

伏案入睡，浅眠多梦



心随梦走，追梦而行
爬山奔赴“数安寺”

祈福：

祝 国泰民安
愿 疫情消散
求 集团年底不出事
.....

偶得美创安全锦囊

哇！勒索病毒防护妙计

锦囊
勒索病毒防护
4个1
保安全无忧

美创诺亚防勒索
以数据资产防护为核心的
以零信任为基础的勒索病毒防护软件

1个利器

核心文件、文档、哑终端
数据库防勒索有效防护

1个机制

被动防御到主动防御
内置诱捕系统、堡垒模式
防止勒索病毒修改操作系统引导区

1个保险

勒索病毒防御+保险



兜底勒索病毒造成的经济损失

1个底线防御措施

- 做好离线备份
- 做好异地备份
- 做好异地容灾

部署上线 高枕无忧

终于
部署上线!



今天可以
高枕无忧了



< 完 >

美·实践

MEICHUANG · CASE

浙江省农业农村厅政务数据安全治理实践

许昌职业技术学院数据安全防护体系建设实践

宁波市第一医院：基于大数据的公立医院智慧运营分析平台的建设及应用

美创助力全国首批省级中医院数据安全建设

看，金华最安全的“一朵云”

容灾切换演练实例



浙江省农业农村厅政务数据安全治理实践

政务数据安全性是确保数字政府良好运行的重要因素，围绕数据开放共享的安全问题是数字政府建设工作过程中的关注重点。国务院印发《关于加强数字政府建设的指导意见》中提出，要依法依规地促进数字高效共享，确保各类数据和个人信息的安全，提出要加强对政务数据统筹管理，全面提升数据共享的服务、资源汇聚、安全保障等一体化水平。加强数据安全保障，满足《网络安全法》、等保 2.0、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规要求，浙江省农业农村厅以相关业务系统为切入点，与美创科技共同开展重点应用核心数据安全治理工作。

项目建设内容

本项目依据《数据安全法》、《个人信息保护法》等法律法规标准要求，截止目前已完成对该单位重点应用的数据安全现状摸底、数据安全风险评估和分析，涵盖合规安全、组织建设、制度建设、技术工具等模块。

具体数据安全治理服务内容如下：

在组织建设方面

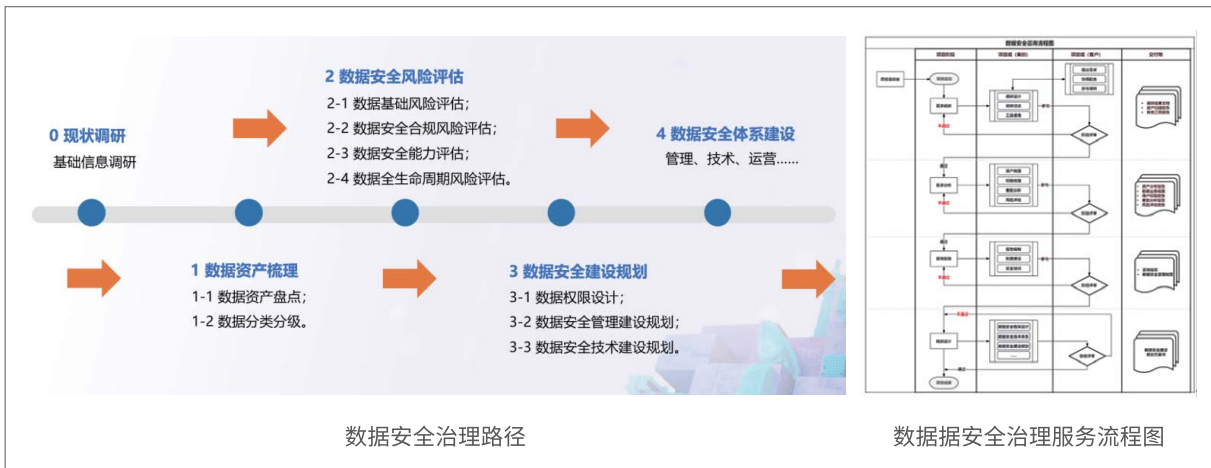
明确该单位数据安全的管理层、执行层和监督层，建立安全保障小组或责任人机制，明确职责。

在制度建设方面

该单位目前已经具备较为完整的信息安全保障体系和制度，本期数据安全治理服务项目中新增《XXX 公共数据安全治理实施细则》、《XXX 公共数据合作方管理规范》和《XXX 数据安全应急演练预案》等。

在技术建设方面

通过对重点业务系统进行安全基线、安全漏洞、第三方权限审批、密码口令、数据采集、数据处理等安全检查，排查数据安全漏洞并提供加固建议，防范安全事件发生，避免发生高危操作等安全风险点，保障业务连续性。



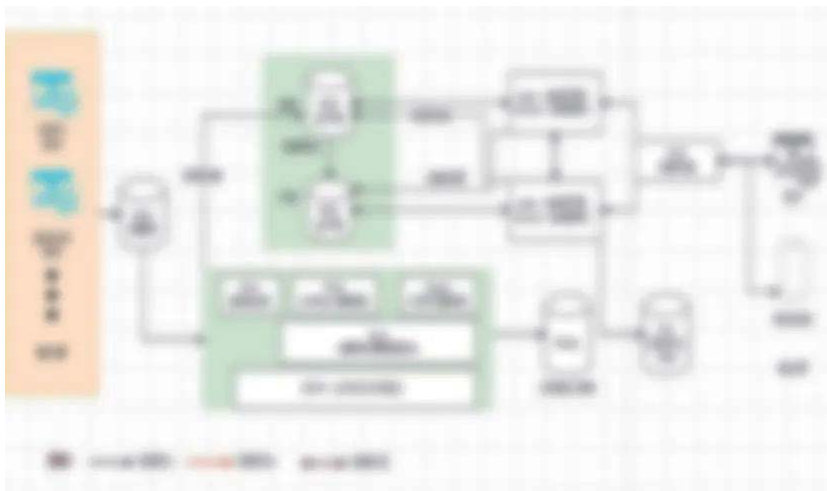
项目成果展示

根据《数据安全法》、《个人信息保护法》等法律法规和地方监管要求，为规范和完善数据安全管理体系，启动数据安全治理服务项目。

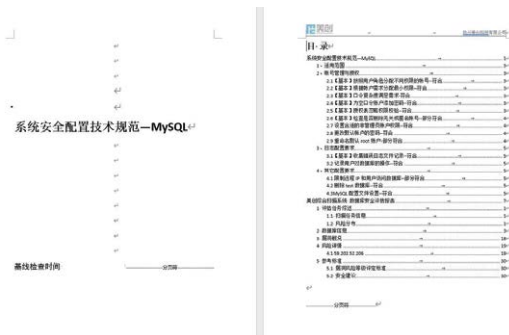
本期交付物可总结为 1+2+1，其“1”是协助该单位建立了一套数据安全管理制度规范，包括数据安全实施细则、合作管理制度等，该套规范体系是落实数据安全风险管理防范的抓手；其“2”是对该单位数据安全现状进行评估，厘清其在管理和技术方面与目标能力的差距，识别相关重要业务系统在数据全生命周期各阶段的风险和综合风险。组织对重点业务系统展开了应急演练服务，输出数据安全事件应急演练模拟演练报告；最后一个“1”是根据评估现状和加固建议，结合单位业务规划提供针对性的数据安全规划建设方案。

部分交付物示例：

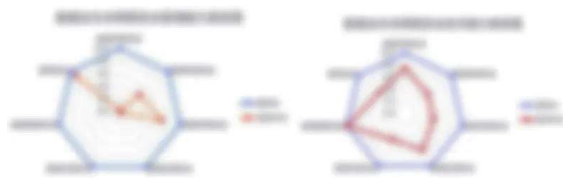
◦ X 厅局基础评估报告（其一）



◦ 数据业务流向图

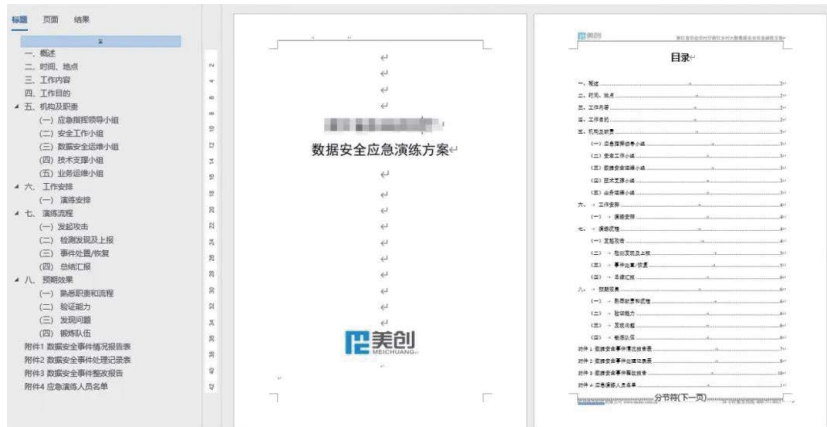


数据安全能力差距评估结果示例



数据安全相关制度

X 厅局数据安全应急演练方案



数据安全事件应急演练模拟演练报告



项目亮点

本期数据安全治理服务，为该厅局后续建立数据安全精细化防护策略落地提供依据，为数据共享交换保驾护航，同时也为同类行业数据安全项目树立了标杆。

项目基于组织发展战略和合规要求，自上而下规划建设，从组织、制度、技术和人员四个维度进行数据安全建设和持续改进。以数据资产的视角对整个数据生命周期过程进行监管，保障该单位重点应用的核心数据资产安全。覆盖组织建设、制度流程、技术工具和人员能力各个维度，涵盖数据资产分布、数据安全风险分析、业务数据流向以及安全能力赋能等，实现常态化的数据安全监管。

同时，数据安全制度编撰并发文后，将为该单位提供数据安全治理依据，且在管理和执行上有较大提升，后续根据业务发展和实际情况进行优化。

许昌职业技术学院数据安全防护体系建设实践

为进一步促进信息技术与教学科研的深度融合，夯实自身数据安全保障能力，许昌职业技术学院立足学校现有信息化建设基础，以敏感数据防护为核心，携手美创科技落地数据安全技术保障体系，提高数据资产安全，为学校业务发展提供可靠支撑。

建设背景

作为一所入围国家“双高计划”的高等院校，许昌职业技术学院目前已建成一卡通平台、网站、OA、财务、招生管理系统、科研情报系统、学生管理系统等众多系统。随着信息化管理业务、服务系统不断增加，系统中积累了海量敏感数据资产。

但面对愈演愈烈的数据安全威胁，高校数据要想真正发挥潜在价值，对教学科研、管理服务、决策分析直接起支撑作用，驱动学校数字化转型，必须加强数据安全治理，将数据安全贯穿始终。

从国家和行业层面而言，近年来对数据安全愈发重视。一系列法律及相关规定陆续出台，数据安全建设逐步有据可依。

面临现状

目前，学校已建立了较为完善的网络安全防护体系，但传统网络安全设备的部署和防护位置决定了其无法对核心数据进行全面有效的保护。因此，基于数据资产角度，如何建立起全面的数据安全保护体系，成为学校信息安全建设的重点。面临现状如下：

01

不清楚数据在哪里，风险有哪些，数据安全建设无从下手

学校涉及系统多、流程复杂，数据各类多、格式多、数量大，同时需与第三方对接需求多。经年累月下来，很难理清有哪些数据，数据都存在哪里，为哪些人员开放了哪些数据操作权限，存在哪些数据安全风险，数据安全建设无从下手。

02

“共享交换”带来新的数据安全挑战

根据国家政策要求，各部门各机构间要打破数据壁垒，消除“数据孤岛”和“数据烟囱”，加强数据共享交换，让数据流动起来，挖掘更大的数据价值。数据流动产生更多新的场景，接触更多的组织和人员，导致数据不可控，从而加大了数据安全风险。

03

缺乏有效的勒索病毒防御措施

当前勒索病毒攻击事件频发，当其对文件、数据加密和修改时，往往是无法恢复，只能就范或舍弃数据。因此，学校迫切需要有效的技术手段防御新型病毒。

04

缺乏业务连续性安全保障

学校一卡通系统、财务、网站等核心业务系统一旦出现故障，将会导致与其相关的业务均无法开展，甚至会造成毁灭性的业务数据永久性丢失。因此，对于重要的业务系统，必须具有不间断的可用性或者能以最快的速度进行恢复，使灾难造成的风险降到最低。

建设方案

针对该院校当前数据安全现状，美创科技以国家和地方的相关政策为指导，以《数据安全法》等相关法律法规为标尺，从数据安全内部管控、数据流动安全、勒索病毒防御、数据存储安全四大场景出发，通过“数据库防水坝 + 数据脱敏系统 + 诺亚防勒索系统 + CDP 灾备一体机”等产品建立起多层次、立体化的数据安全防御体系，全方位保障学校数据资产安全。

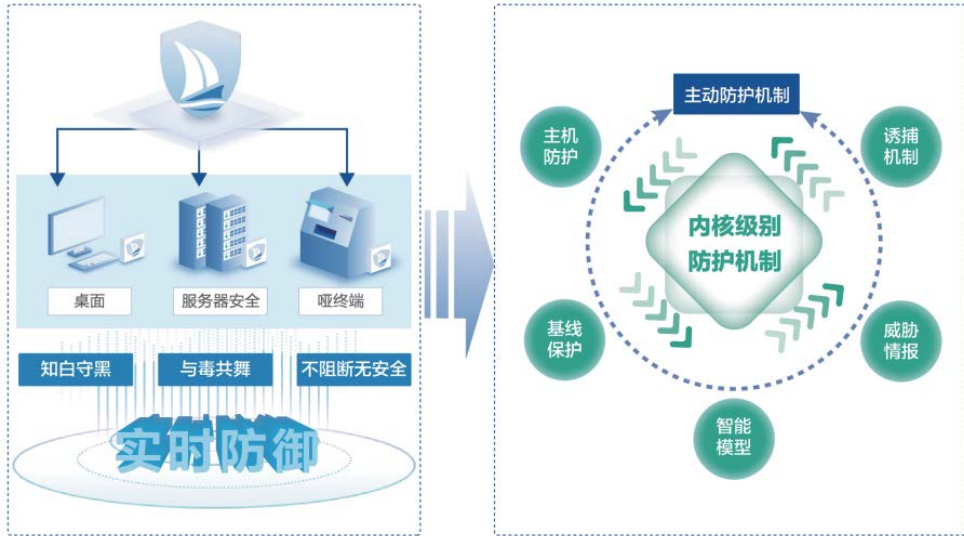
数据安全内部管控

学校各类核心业务系统数据库服务器中存放了大量的核心业务数据，对学校而言，这些数据举足轻重，一旦遭到破坏、篡改或窃取，可能会给学校日常各项业务的正常开展带来巨大影响。通过数据库防水坝对学校内部及第三方运维访问人员权限进行细粒度控制，对敏感数据的分级分类，重点监测所有敏感数据的操作行为，防止非法操作以及授权用户违规操作造成的严重后果。



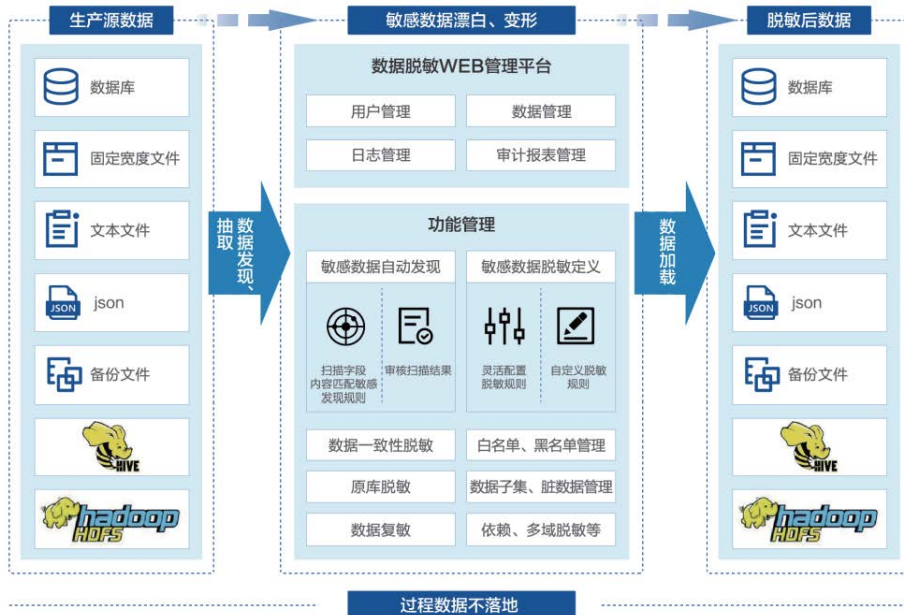
勒索病毒防御

诺亚防勒索系统采用主动防护的模式，通过白名单机制监控所有进程，精准识别文件、数据库的操作行为，利用底层驱动技术，监控所有进程的写操作，对文件、数据库的“写”操作判断，对于非法写操作进行阻断。通过控制“写”权限，从而对勒索病毒的写操作进行控制，就算被植入勒索病毒，勒索病毒也无法对文件和数据库进行加密，保证文件、数据库彻底免除勒索病毒的困扰。



流动数据安全防护

涉及到开发、共享及分析等数据是流动的，因此，为防止数据流动过程中出现敏感信息泄露的风险，在数据流出安全防护的领域之前，需要通过美创数据脱敏系统对其中的敏感数据进行安全脱敏处理。在测试环境中形成一份“仿真数据”，保障开发测试场景中流动数据的安全、可靠、有效。



业务连续性保障

针对学校一卡通平台、网站、OA、财务、招生管理系统、科研情报系统、学生管理系统等系统采用实时备份策略，对操作系统、数据库、应用环境、文件等数据进行实时捕获并完成同步整机备份，当被保护数据 / 业务系统出现故障或数据损坏后，能快速接管应用系统或则恢复数据。为学校数据提供 7x24 小时的无间断保护，保障学校业务系统数据的完整性和业务的连续性。

方案价值

01

数据资产驱动的安全体系

以数据资产保护对象为核心构建，把所有需要进行保护的数据和高风险操作都定义为资产，使其可以统一进行资产管理和风险管理。当我们需要扩展或者分离保护目标的时候，只需简单的定义一类新的数据资产就可以提供完善的保护措施。

02

体系化安全防护

体系化的设计思想是从全局性策略出发，以整体的设计思路打造全局性的安全防御，辅以长期可靠的安全运维保障和规范化的安全管理，搭建出真正能够有效对抗威胁，保障应用的安全体系。

03

细粒度定向安全防护

采取强度一致的安全措施，并采取统一的防护策略，使各安全措施在作用和功能上相互补充，形成动态的防护体系。

04

安全合规

支持各种自定义告警方式，同时内置支持各种法规遵循所需的管理性报表，满足网络安全法、数据安全法、等保 2.0、数据安全管理办法等合规要求。

宁波市第一医院：基于大数据的公立医院智慧运营分析平台的建设及应用

目 导读

医院通过数据分析平台实现精准化数据预测，对提升工作效率、降低医疗风险、提高服务质量、建立整体发展思路、预测学科发展方向、辅助制定发展战略起到了重要作用。

医院发展规模日益扩大，医院运营管理向精细化发展，需要积极探索运营平台建设，深挖运营业务数据，满足医院高质量发展需求，提升医院科学决策和精细化管理能力。在国务院办公厅印发的《加强三级公立医院绩效考核工作的意见》、《关于推动公立医院高质量发展的意见》等文件中，都明确提出公立医院要强化信息化支撑，健全运营管理体系，推动医院运营管理的科学化、规范化、精细化。

根据医学规律和行业特点，发挥大数据优势，强化考核数据分析应用，提升医院科学管理水平，推动三级公立医院在发展方式上由规模扩张型转向质量效益型，有助于提高医疗效率，减轻患者负担。

宁波市第一医院基于大数据技术，在公立医院智慧运营分析平台的建设及应用方面进行了探索。

目 项目基础与原则

医院运营分析系统的设计应遵循统一性、先进实用性、安全性、标准性、可拓展性、发展性、易操作性、可维护性八项原则。

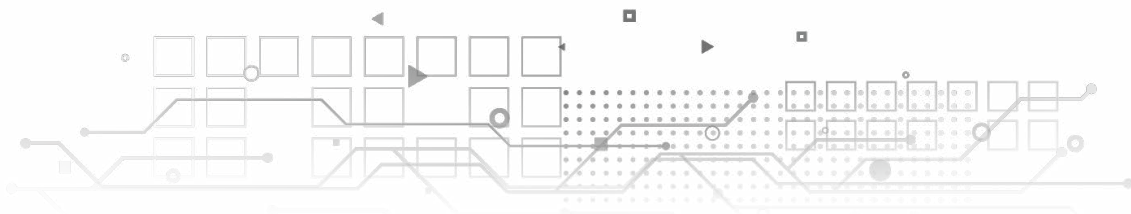
在建设之初，应从全局角度考虑应用系统建设架构、数据模型结构、数据存储结构搭建以及系统扩展规划等内容，采用领先产品和技术，适应与日俱增的数据处理要求，满足医院运营管理信息系统长期数据和业务快速增长的需要，并为将来可预见和不可预见的系统性能扩充留有余地。

系统应展示总体与分类数据、表现翔实细节，让使用者重新理解、洞察其所发生的有效数据，同时具备良好的用户操作界面、运行监视系统、远程控制台等功能，提供全面、完善、便捷、统一的系统管理和应急处理预案，真正实现整体效益，提供高效能与高效益的医院信息服务。

目 项目平台架构及主要应用

架构设计

宁波市第一医院的智慧运营分析平台整体架构设计为“四横四纵”八大体系，其中“四横”为数据源、数据平台、数据应用、应用场景，“四纵”为政策制度体系、标准规范体系、组织保障体系、网络安全体系，总体实现纵向贯通、横向协同。如图 1 所示。



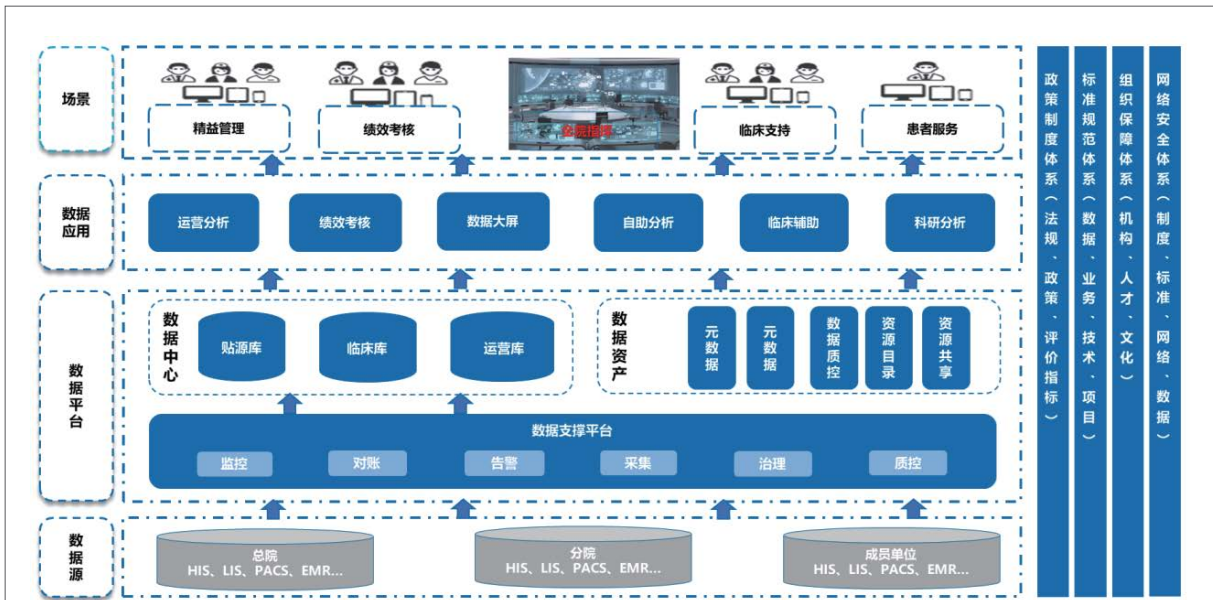


图 1 “四横四纵”八大体系示意图

在数据平台建设中，由于传统 ETL 抽取过程需要从业务系统数据库提取数据，对业务系统的性能影响大，而且数据抽取的及时性已无法满足快速的数据应用需求，为此医院搭建了统一的数据支撑平台，进行数据同步、数据治理，对数据进行清洗、加工及统计，最终实现统一的数据中心。在数据处理过程中，平台可对数据质量进行控制与可视化提示，并能自动告警。

该平台可整合 HIS、LIS、PACS、体检、电子病历、病案等系统数据，提供实时、准确、标准的数据支持，打造坚实的数据底座。利用 BI 平台的分析功能，建立运营分析、收益分析、医疗质量、内控合规等数据汇聚平台，完善信息资源汇集、管理、使用体系，衔接医院门诊、手术、住院、转诊患者等相关业务数据集成、查询统计、分析展示等功能，同时实现各院区的信息资源交换与共享。

医院决策支持平台

如今，面向管理者的决策支持正从“信息系统的定期统计报告”变为“集成信息的实时反馈”。随着信息化知识的扩展、管理水平的提高和管理重点的变迁，医院管理者对决策信息支持提出了更广泛、更精细、更个性化的需求。

宁波市第一医院的智慧运营分析平台建立了以医院战略为导向、院领导决策为支持的运营多维分析数据模型。平台对医院大数据进行挖掘和分析，建立医院数据决策分析模型，对财务、医疗、医保、设备、物资、人力资源等多维度数据进行深度分析。医院管理者可通过数据实时大屏（图 2），及时掌握全院动态，实现数据实时分析监管。

为分析展示门诊实时数据，为门诊效能提升提供管理依据，医院设置了门诊实时大屏驾驶舱，展示内容为实时门诊人次、待诊人数、预约未到人次等，可对诊间繁忙情况进行预警提示，帮助医院管理者及时处理问题，实现门诊效能与患者满意度的双提升。



图 2 数据实时大屏

科室及医疗组决策支持平台

科室及医疗组决策支持平台可为科室管理者及临床医生提供决策支持，快速掌握科室运营数据，发现经营决策问题。平台利用大数据分析技术，并结合当前业务现状，实现对已归集历史数据的合理使用，对业务关键指标以仪表盘、柱状图、饼状图、折线图、进度图等方式进行展示，为科室管理者全面掌握当前业务现状、后续学科发展决策、制度修订等提供数据支撑和服务；通过展示围绕门诊急诊服务、住院服务、质量安全等模块数据支持（如表 1 所示），帮助医院管理者从指标中发现、查询、分析问题，利用业务报表陈述业务事实，预警监控反映业务状态，为科室合理、高效开展业务以及工作重心调整等提供了充分的信息化手段，助力实现管理精准化和服务高效化。

模块	内容
门急诊服务	门诊急诊体检人次 核酸人次
住院服务	住院人次 床位使用率 平均住院日 住院收入
患者服务	医生出诊 停诊情况 检验检查互认率
手术统计	日间手术占比 出院患者手术占比 微创占比 三四级占比
质量安全	切口感染率 并发症发生率 病理诊断符合率 术后康复时间 死亡人数 围手术期死亡率 治愈率 死亡病种 不良事件
合理用药	门诊住院药占比 抗菌药物使用占比 DDD 值 外配处方占比 基药使用金额占比 住院患者基本药物使用率
服务流程	预约就诊率 预约患者等候时间 准时接诊率 手术人次 平均住院日 床位使用率 病床周转次数
收支结构	门诊收入构成 住院收入构成 住院人均费用 体检总收入
人员结构	医护比 护士床位比 人员编制情况 学历结构图
学科发展	期刊发表 每百人科研经费 成果转化金额
DRGs	CMI DRG 组数 疑难病例占比 日间手术情况 重点监控病种数量

表 1 科室及医疗组决策支持平台模块内容

5G 移动数据支持平台

宁波市第一医院的智慧运营分析平台建立了“5G 移动驾驶舱”实现数据随时看，建立了“手机钉钉驾驶舱”，围绕医院内部管理和患者服务进行建设，优先医院内部管理，有助于医院管理层实时查看医院运营状况。

在手机端，设置院长、临床科室管理者、普通员工三级运营分析模块查询（图 3），能够随时随地掌握全院及科室运营数据，及时发现经营决策中的问题，同时为科室、医生提供多维自助分析报表（图 4），可自主选择主题、自由选择分析维度和指标进行自助探索分析。

通过自定义选择维度、度量（指标），聚焦关注重点，平台可实现不同维度、层次、指标的信息资源查询，自动生成报表、图表（饼图、柱状图、趋势图、雷达图等）。以住院主题为例，可选的维度包含：时间、院区、科室、病区等；可分析的指标包含：收入构成、出入院人次、手术量，平均床日等。通过各种维度、指标的综合分析，建立起可视化的数据库。



图 3 运营分析模块



图 4 多维自助分析报表

全生命周期视窗 360 平台建设

传统模式下,临床医生不能很方便地共享患者的所有诊疗信息,医院管理人员很难拿到完整、准确的运营管理数据。宁波市第一医院的智慧运营分析平台建设了全院统一的临床主数据管理标准,实现数据共享和流程整合,从全景视图、时间轴视图、住院视图以及门诊视图等角度进行串联,以患者为中心,为临床及居民健康分析提供数据支持,提升就诊体验。

患者健康全景视窗的数据具体包括:基本信息、历史就诊、诊断、过敏、用药记录、检验、检查、手术、体检、病历、病案等。平台可纵向展示患者诊疗周期的临床数据,满足健康信息的检索、展示、临床等需要,详见图 5。

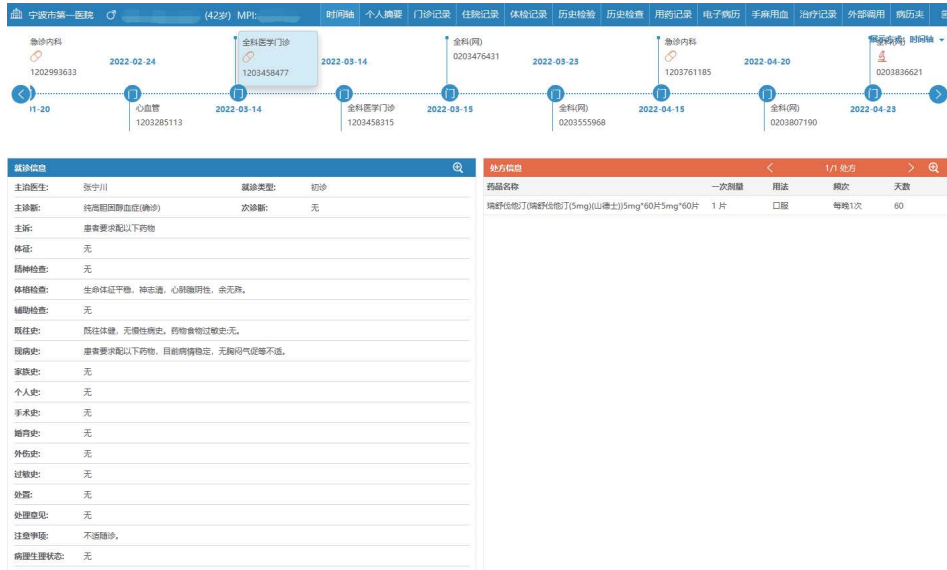


图 5 全生命周期信息视窗



医务工作者关怀应用

基于数据业务底座，通过指标的加工分析，平台对医生全年工作进行回顾，直观展示医生当年的接诊数量、患者分布等情况，赋予数字以温度，利用数字化手段表达医院对医生付出的关怀与感谢。

其中，“医生年报”包括工作量统计、患者信息统计、重点时刻统计、结尾总结四个维度；“工作数量”包括病患者数量、接收门诊人次数量、收治住院人次数量、手术数量、健康出院人数等维度；“患者信息”统计医生收治患者分布，包括患者年龄区间范围、年龄阶段分布、患者男女占比等；通过数据展示医生年度“重要时刻”，如接诊患者数量最多的一天、完成手术数量最多的一天等，全方位展示医生年度工作量。针对各具特色的医生年报，医院授予其不同称号，例如“勤劳楷模”、“手术达人”、“最受年轻人喜爱”、“最受老年人喜爱”等，详见图 6。



图 6 医生个人年度医疗账单

项目实施成效

01

医院运营数据分析多元化

通过智慧运营分析平台汇聚医院数据分析和报表，提供完善的统计学分析工具和灵活的自定义统计模式，这对管理人员而言非常重要。平台为数据统计提供了自定义分析方法，管理者可以自由定义分析的变量以及分析模式，导出不同形式的统计分析图表，进行运营数据的多元化分析，提高医院科学决策水平，助力建立院内精细化考核机制，同时满足国家三级公立医院绩效考核指标要求。

02

医院运营效率提升

医院通过数据分析平台实现精准化数据预测，对提升工作效率、降低医疗风险、提高服务质量、建立整体发展思路、预测学科发展方向、辅助制定发展战略起到了重要作用。在全国三级公立医院绩效考核中，宁波市第一医院连续四年进入 A+ 序列；2022 年上半年 CMI 值为 1.0659，位列浙江省第二；平均住院日为 5.49，全省排名第五；医院日间手术占比 33.03%，全省排名第一。经过数据监测分析及改善措施实施，近三年待术时间、检查预约时长、床位使用率均有明显改善。

目前，宁波市第一医院的数字化智慧医院主要围绕院内数字化、智慧化开展，主要建设任务包含数据平台、数据应用两部分。后续，医院将以患者为中心，打造互联网+精准服务，聚焦慢病分析、健康风险评估、健康处方制定、个性化健康管理知识推送、日常健康信息异常提醒等功能，为患者就医的院前、院中、院后提供全流程的智慧健康服务。

美创助力全国首批省级中医院数据安全建设

江苏省中医院联合美创构建数据安全防护体系，面对 HIS 等核心业务系统数据库，以数据资产防护为基准点，实现对内部操作风险管控、数据库审计等诸多场景下的安全防护，有效保障医院数据资产的安全性和业务连续性。

江苏省中医院创建于 1954 年 10 月，创建初即荟萃江苏一代名医，历经半个多世纪几代人的艰苦创业，医院规模与声誉日益扩大。现已成为一所集医疗、教学、科研、预防保健、急救等为一体大型综合性三级甲等中医院。

背景 & 现状

近年来，随着国家新医改方案的出台及逐渐推行，信息化建设在各级医疗机构的管理中发挥了越来越重要的作用，利用信息化手段提高医院整体管理水平，实现医院社会效益和经济效益最大化将是必然趋势。

作为全国首批成立的省级中医医院之一，江苏省中医院积极推进“以病人为中心，电子病历为核心”的新型数字化智慧医院信息系统建设，当前已全面覆盖院内医疗、行政、运营等各部门各项日常业务。

为加强医疗质量管理，保障医院信息化系统正常运行，医院内部及第三方配备了大量运维人员，但医院信息科室对这部分运维人员缺乏有效的管理手段；特别是在数据层，急需运维管理、数据访问监控以及数据库监控解决方案。具体如下：

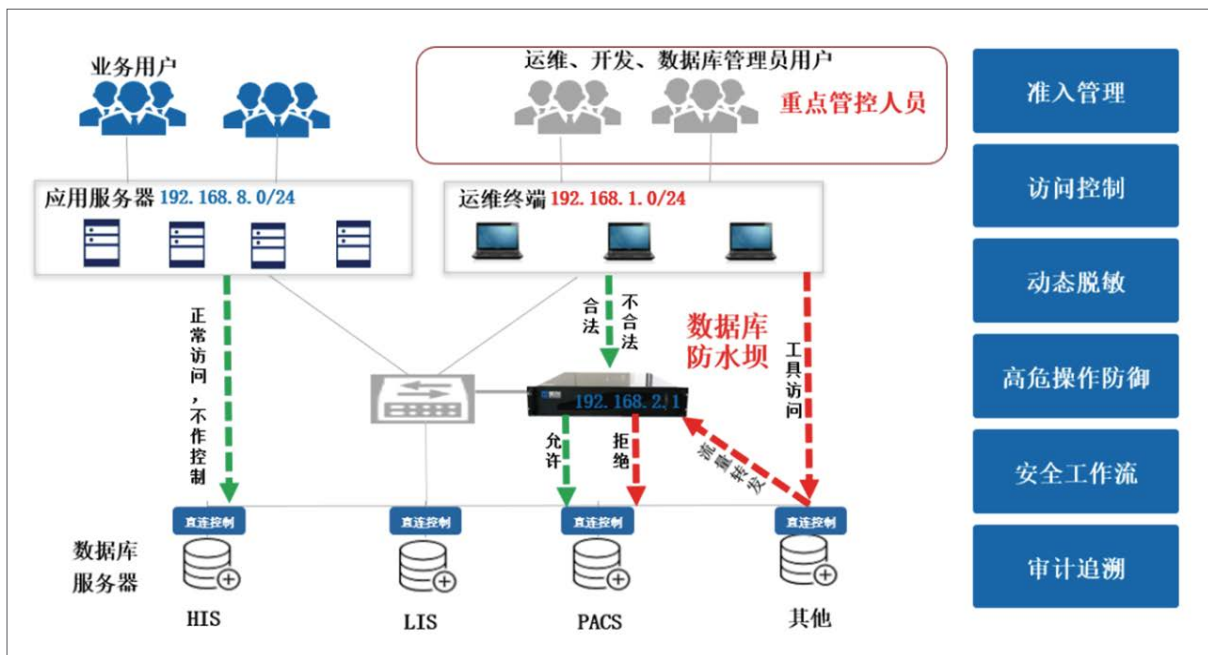
- 数据库敏感信息查询管控，特别是对于病人健康隐私、用药情况，要严格管控，做到非法查询可管理、可控制、可告警；
- 敏感信息存储安全防护，防止第三方运维人员拥有过高的数据库运维权限，避免敏感信息被恶意删除或误删除，保障数据安全；
- 数据库运行安全管控可视化，需可视化平台时刻监控数据库状态，及时发现数据库故障，保障业务可持续运行；
- 需建立数据库操作可回溯机制，记录所有访问数据库的流量，供事后查询。

建设方案

针对等级保护三级要求以及智慧医院互联互通评级监管等相关要求，江苏省中医院联合美创科技通过部署“数据库防水坝+OSM 数据库运行安全管理平台 + 数据库安全审计系统”，实现内部操作风险管控、一体化保障等场景下的安全防护，有效保障了病人隐私数据安全及业务系统的可靠性。

数据库内部操作风险管控

江苏省中医院通过部署美创数据库防水坝系统，从源头上对运维人员和业务人员实行分离管控，实现基于数据库访问用户的细颗粒度管控，将访问控制策略与敏感数据相关联，避免越权访问；多因素的数据访问身份认证，满足数据库实名制管理需求，同时解决数据库 SysDBA、DBA、SchemaUser 等特权用户权限过大的问题。



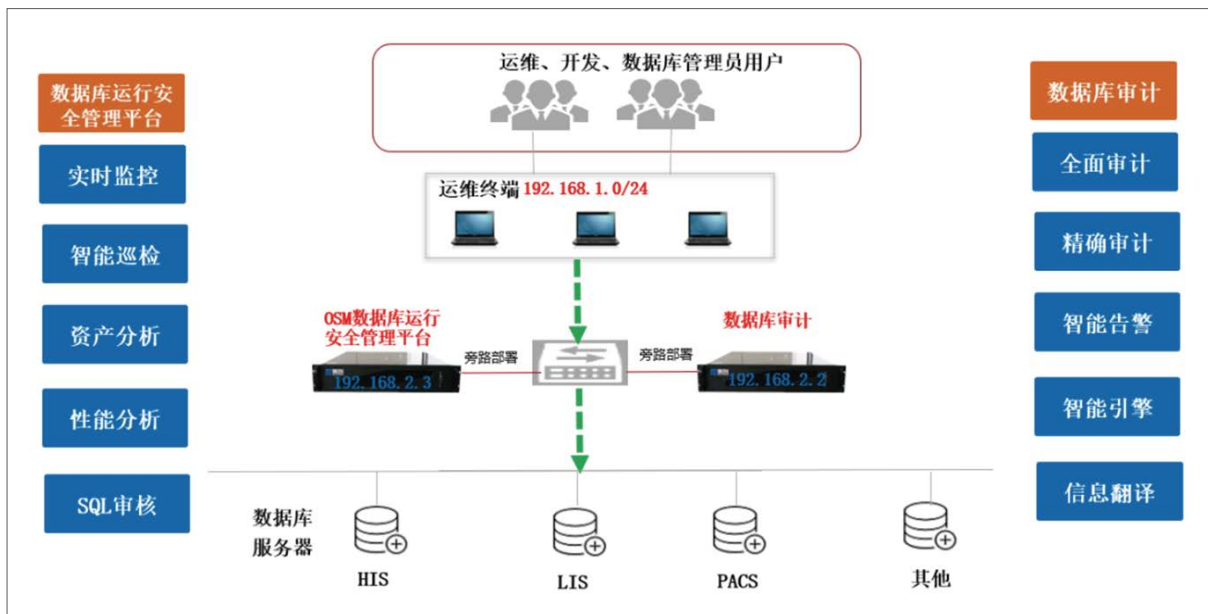
数据库安全审计

针对江苏省中医院数据库缺乏详细审计记录，安全事件一旦发生，无法进行有效的追溯和审计；数据库操作无准确全面的记录，操作人员容易抵赖等问题。

通过部署美创数据库安全审计系统，建立起数据库操作可回溯机制，通过对数据库的各类操作行为进行监视并记录，以便定位事件原因，提供日后查询、分析能力，使数据操作行为有据可依，防止抵赖。

数据库主动、智能化运维

通过部署美创 OSM 数据库运行安全管理平台，可针对医院核心系统数据库实现 7*24 小时自动巡检，高效率安全地完成故障提前感知、问题智能定位以及故障智能解决，实现数据中心一体化监控以及数据库的智能化运维。提供多元化的工具，帮助运维人员高效便捷的保障数据库的运行安全，实现数据库巡检、锁处理、安全检测、数据库自动化部署；同时实现对数据库运行发展的趋势分析和预测，保证医院业务系统数据库的运行可用。



客户收益

建立健全医院运维安全管理措施

通过此次安全建设，健全了医院运维安全管理措施，对重要敏感数据的动态脱敏机制，减少生产库中客户敏感数据泄露风险。

运维安全管理更专业、简便

实现运维网络与业务网络的分离，网络管理通过普通堡垒机进行管控，数据库运维管控则通过数据库防水坝，让管理更专业、简便。

提高医院数据库运维效率

解决了运维过程中账号管理混乱、运维操作不透明等安全访问控制和授权管理问题，在保障运维安全的前提下，简化了操作流程，提高了运维效率。

安全合规

符合国家规定的医疗系统的统方法规，实行对处方表、药品表等敏感资产的访问控制；符合等保三级、网络安全法、HIPAA、PCI-DSS、SOX、GLBA等要求。

看，金华最安全的“一朵云”

在八婺大地金华，美创助力市大数据局加强政务云基础设施建设，形成完整的容灾备份架构，通过可视化大屏指挥系统展现灾备系统运行状况，实现政务云灾备的集中可视化监控，提升云资源使用效率。

政务云当前已成为各地智慧城市和智慧政务建设的根基，据了解，金华地区的所有政务信息系统均运行在政务云平台，如：政务公开信息查询、面向市民和企业的事务主动提醒、在线自助经办、网上办事及面对大中型企业的工业数据中心和金融服务渠道等……

随着开放程度不断深化，政务数据的海量汇聚，各业务系统运行安全及数据安全威胁问题也随之增长。如果整个业务系统一旦发生故障，如硬件损坏，火灾、地震等，将会导致整个业务中心宕机，对整个政务系统造成不可估量的损害。

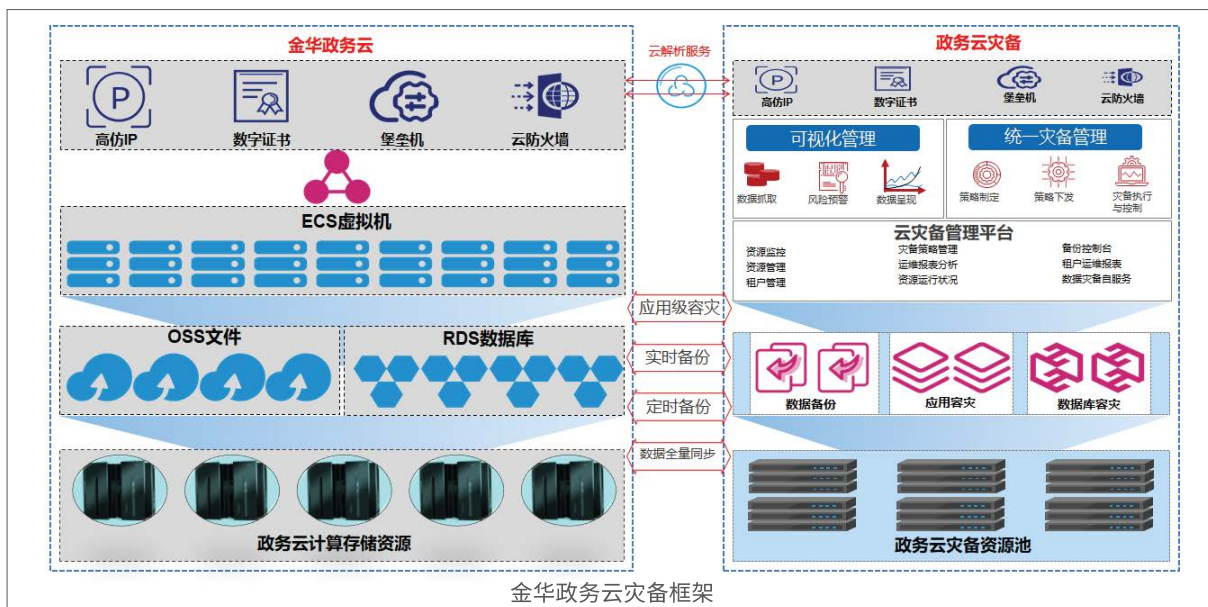


目前，在政务云底层架构中，云平台已经为政务云上的各类数据提供了多份副本快照保护，能够满足云中心业务运行过程中的各级 RTO/RPO 的需求。

但是政务云的生产数据和快照数据均存放在同一套的硬件资源池中，目前承载了业务系统多达上百套，且业务系统和应用分开部署。为此，从政务安全、业务系统运行安全双向角度出发，金华政务云亟需建设一套独立于政务云资源池的灾备体系。

建设方案

经过前期多次现场调研、线上沟通，美创科技了解到金华市内各类公共服务以及企业服务系统均运行在政务云平台中，故决定根据不同应用场景，设置不同应对容灾策略。具体如下：



应用级容灾

面向业务系统中最为核心的数据库系统，以数据资产的视角，确保数据库可用性为基准点，并最大限度地满足数据级容灾的 RPO、RTO 需求。

通过应用级容灾建设可以实现核心业务容灾和灾难切换，并通过一键切换指挥大屏进行切换指挥演练。应用级容灾实现分为应用数据同步和数据库数据同步。

实时备份

ECS 虚拟机实时备份采用持续数据保护实现，在不影响主要数据运行前提下，持续捕捉或跟踪目标数据所发生的任何变化，可以在数据发生任何变化时将数据有效地保护起来，能独立对主要数据进行持续捕捉或跟踪数据修改，并保存变化，从而实现从过去的任何非预设点恢复的方法。

数据全量同步

数据库同步是整个容灾方案中最为重要也是最为关键的一环。所以在数据库数据同步设计时，需要考虑灵活的数据库同步方式。

在多数据库环境下，依据业务系统的不同要求灵活制定数据同步的方式。例如可以选择同步复制或异步复制，针对部分数据库例如（Oracle 数据库）也能够支持 copyonlog 的传输模式。

多租户管理

对于云备份运营方：构建 SaaS 化云备份服务，实现备份服务的云化运营，达到集中运维，甚至是盈利等目的。

对于云备份使用方：借助该备份服务，无需投入任何软硬件，即可实现数据的异地备份，极大简化数据备份流程，降低数据备份投入，达到降本增效的目的。

运营方：多租户统一管理

- | | | |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|
| 租户管理 | 存储资源管理 | 运维管理 |
| <ul style="list-style-type: none"> · 租户分配 · 配额管理 | <ul style="list-style-type: none"> · 资源总览 · 资源分配 | <ul style="list-style-type: none"> · 工单管理 · 日志报表 |

租户：租户间逻辑隔离、独立使用

- | | | |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| 自助管理 | 备份管理 | 运维管理 |
| <ul style="list-style-type: none"> · 资源申请 · 备份策略 · 恢复策略 | <ul style="list-style-type: none"> · 作业管理 · 作业监控 | <ul style="list-style-type: none"> · 账号管理 · 工单申请 · 监控告警 |



指挥大屏管理

通过可视化的大屏指挥系统，让灾备系统的全局可视更近一步，灾难应急切换更为高效。指挥大屏功能价值主要体现在状态可视、过程可视和指挥高效三个方面：

◦ 状态可视

通过简洁的页面将关键指标提炼展示出来，解决了原来信息过多而无法及时掌握有效信息，避免冗余信息干扰；

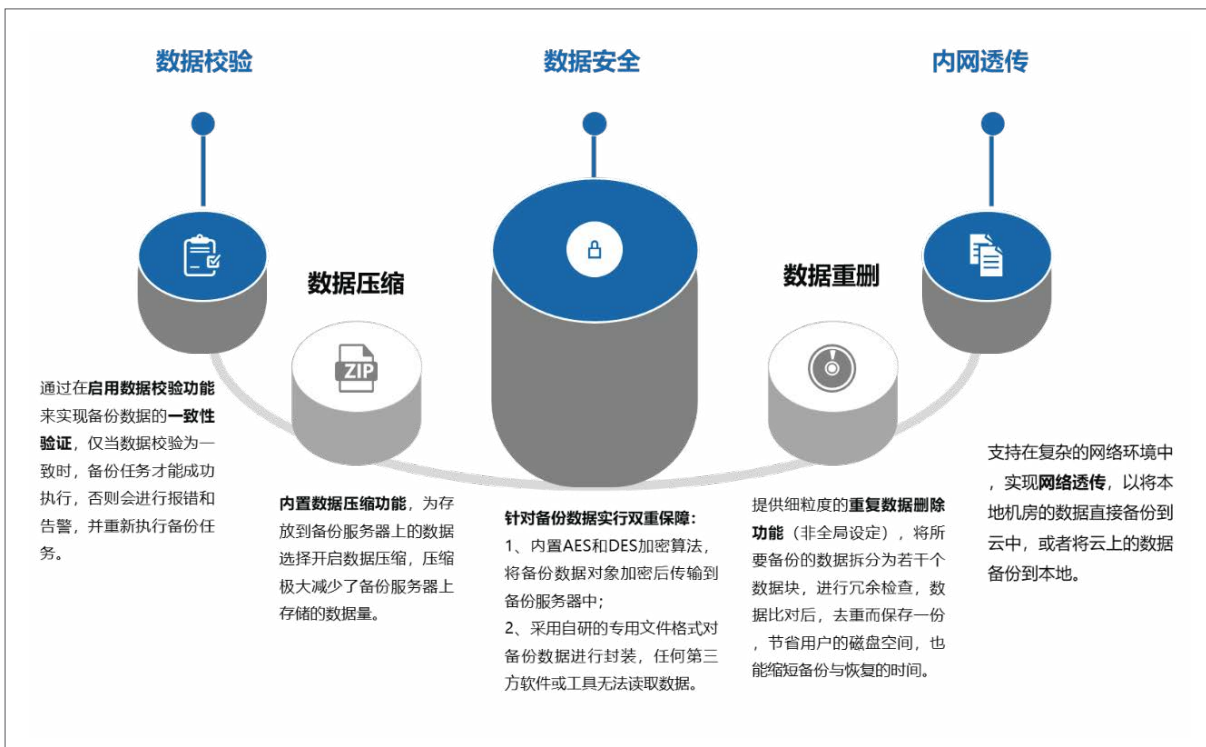
◦ 过程可视

通过实现容灾切换和业务验证进度一屏展示，让整个切换过程可视，有效解决了原来过程状态无法及时感知的问题；

◦ 指挥高效

通过状态可视和过程可见，为现场应急指挥提供了有效的依据，提高应急决策的时效性，有效保障故障恢复的成功。

政务云灾备产品技术亮点



◦ 高效传输

压缩、重传、断点续传等技术提供了海量数据在远距离、窄带宽、低质量链路环境下传输的能力；

◦ 安全传输

内置丰富的加密算法，所有数据均经过加密后进行传输，提供了极高的数据传输过程中的安全保障；

◦ 及时同步

采用实时增量复制技术，将数据及时同步到备用系统上，当出现灾难时，能够保障数据零丢失；

◦ 快速恢复

通过编排及一键切换功能，让整个故障转移的过程非常快速，整个灾备系统具备业务快速恢复的能力。

目 项目建设收益

- 1) 为政务跨业务较复杂的核心数据业务系统构建连续性保障，解决数据遗漏问题；
- 2) 解决了一直以来海量数据无法实时同步，数据无法一致的问题；
- 3) 灾备一体化且可进行可用性验证，具备数据误操作即时恢复能力；
- 4) 通过活动站点功能，分流非生产性作业，提高生产数据库系统利用率；
- 5) 满足《中华人民共和国网络安全法》、《中华人民共和国数据安全法》以及《电子政务总体设计要求》、《电子政务标准化指南》系列标准、《基于云计算的电子政务云平台》系列标准等相关政策法规要求。



容灾切换演练实例

美创科技在 2022 年持续与医疗、金融等多个不同行业的上百家客户完成容灾切换演练，有效验证了用户单位的信息安全应急响应能力、灾难恢复能力及应对突发事件的处理能力，也彰显着美创科技在容灾备份领域扎实的经验 and 深厚的实力。在此特选取 1 例进行详细介绍。

目 绍兴银行四大业务系统完成容灾切换演练

2022 年 9 月，美创科技与医疗、金融、政府、电力等行业，共 21 家用户完成容灾切换演练，并成功完成两次灾难切换，有效验证了各用户单位的容灾系统的高可用性！

绍兴银行

9 月 25 日凌晨，绍兴银行 ESB、柜面、加密平台、电子银行四大业务系统容灾切换演练顺利完成。

演练开始前，绍兴银行迅速完成了方案设计、评审，并进行多轮桌面演练，充分体现了银行各部门技术保障、管理指挥、流程操作、协调配合等方面的综合能力。



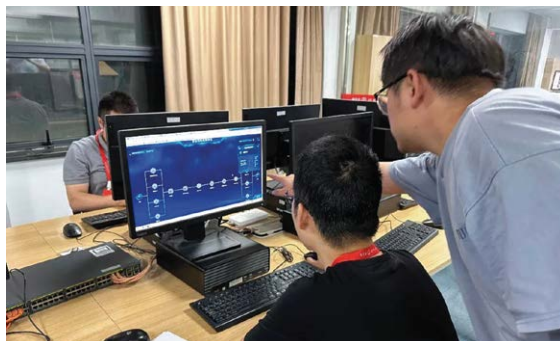
以下为切换演练过程

演练目标 01

本次演练的最终目标是验证容灾系统的可用性，优化银行应急演练流程，保障各项业务的持续性运行。

演练流程 02

本次演练为绍兴银行真实业务切换演练，通过美创灾备集中管控平台，有序完成了 ESB、柜面、加密平台及电子银行系统的一键式正切和回切。



9月23日，ESB系统容灾切换，耗时1分47秒。柜面业务系统容灾切换，耗时7分11秒。

9月24日凌晨，加密平台容灾切换，耗时5分04秒。

四套业务系统切换完成后，按照原定方案，在备库稳定运行一天。运行期间，银行各项业务均正常对外接待，用户侧几乎无感知。

9月25日凌晨，各业务系统顺利完成回切，业务运行稳定。

演练效果 03

对于金融机构而言，数据中心容灾系统的建设不仅要做到“防患于未然”，还要真正做到在故障发生后能够迅速响应，保障业务连续性、安全性。

本次演练充分验证了绍兴银行容灾系统的可用性、可靠性、有效性，以及业务连续性设计指标的科学性。同时，为绍兴银行积累了宝贵的容灾切换经验，进一步提升了业务部门与科技部门的配合能力以及灾难恢复能力。

精耕细作、持续打磨，美创容灾备份产品目前已广泛应用于运营商、金融、政府、公安、医疗、工商、社保、证券、信托、制造业、交通、教育等众多事关国计民生的重要行业，并获得一致好评。

部分典型客户



浙江省人民医院
ZHEJIANG PROVINCIAL
PEOPLE'S HOSPITAL



福建医科大学 附属第二医院
Fujian Medical University
Second Clinical College



中国科学院大学附属肿瘤医院
浙江省肿瘤医院(浙江省癌症中心)



浙江大学医学院附属第四医院
THE FOURTH AFFILIATED HOSPITAL ZHEJIANG UNIVERSITY SCHOOL OF MEDICINE



锦州医科大学附属第一医院
THE FIRST AFFILIATED HOSPITAL OF JINZHOU MEDICAL UNIVERSITY



玉環市人民醫院
THE PEOPLE'S HOSPITAL OF YUHUAN



中国南方电网
CHINA SOUTHERN POWER GRID



新华书店
XINHUA BOOKSTORE



金华银行
JHBank



中国人民银行
THE PEOPLE'S BANK OF CHINA
武汉分行
Wuhan Branch



雅安市商业银行
Yaan City Commercial Bank




紹興銀行

.....



美 · 共赢

MEICHUANG · COOPERATION



美创科技与中国东信举行生态合作协议签约仪式

开启校企合作 2.0，美创科技与杭州电子科技大学开展联动互访

美创科技加入阿里云飞天生态合作伙伴 - 服务生态合作计划



美创科技入围中国电信成员单位 - 数据安全产品供应商

美创科技与联通（浙江）产互签署战略合作协议

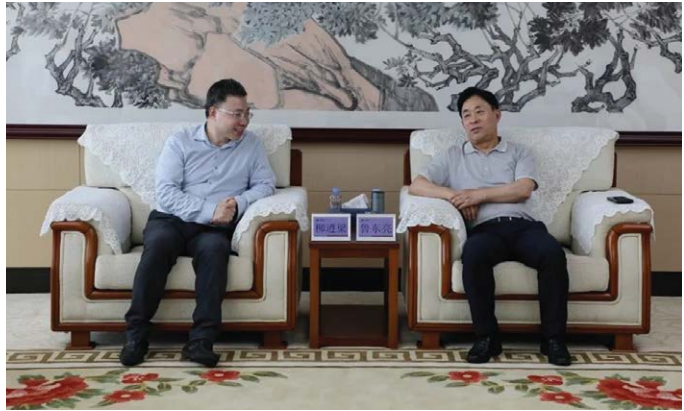
北京、福州、广州、南京等地渠道会合集

美创科技与中国东信举行生态合作协议签约仪式

2022年5月27日,杭州美创科技股份有限公司(以下简称“美创科技”)与中国—东盟信息港股份有限公司(以下简称“中国东信”)举行生态合作协议签约仪式。

柳遵梁表示:美创科技拥有自主可控的数据安全产品,市场竞争力大、发展前景广阔,希望能够与中国东信进行深度资源整合,在市场协作、技术融合、推动数据安全等方面加强合作。持续推进中国东信与美创科技公司在数据安全领域的业务合作,提升数据安全能力建设,推广数据安全最佳实践,引领数据安全建设高质量发展。

鲁东亮表示:中国东信对安全赛道充满信心,聚焦于数据安全和风险全生命周期安全防护,希望以此交流为契机,在政企、医疗、金融等行业展开推进合作,实现资源共享、优势互补,构建互利双赢、高质量发展的合作伙伴关系,护航信息化发展,大力促进安全产业发展壮大。



签约仪式前,美创科技 CEO 柳遵梁与中国东信党委书记、董事长兼总裁鲁东亮进行座谈交流。



签约仪式上,美创科技 CEO 柳遵梁,中国东信联席总裁李珩共同见证签约,双方代表进行了签约。

开启校企合作 2.0 美创科技与杭州电子科技大学开展联动互访

6月26日，杭州电子科技大学网络空间安全产业学院共220名师生赴美创公司总部，开展专业认知实习活动，在美创运维和安全服务部总监应以峰的陪同下，杭电师生实地参观公司总部办公环境、研发中心、展厅，并深入了解美创发展及产品实践。



6月28日，数据安全治理产品部王彦翔受杭电邀请，开展《数字经济时代下的数据安全认知及实践》专题讲座，会上，王彦翔从数据安全定义、数据安全与传统安全区别、法律法规下数据安全的重要性、开展数据安全建设，结合安全事件、实践案例，为杭电学生带来生动有效、理论结合实际的一课。



双向奔赴，开启校企合作 2.0

杭州电子科技大学网络空间安全学院在密码学、数据恢复与取证、工业互联网安全、内容安全、数据安全分析、网络安全等具备领先的科研实力，2017年中共浙江省委网信办依托网络空间安全学院建立“浙江省网络空间研究院”。

2018年，美创科技与杭州电子科技大学网络空间安全学院首次牵手，签署“校企战略合作协议”，此次美创科技与杭州电子科技大学双向奔赴，联动互访，在此前良好、坚实的合作基础上，再次开启合作新篇章，就人才培养、技术研发、安全竞赛、共建实训基地等方面打造产教融合的“美创-杭电”样板，实现成果转化和资源落地。

美创科技加入阿里云飞天生态合作伙伴 服务生态合作计划

9月,美创科技正式加入阿里云飞天生态合作伙伴 - 服务生态合作计划。

据悉,该计划由阿里云计算有限公司发起,旨在寻找具备独立提供咨询、交付、运维等相关服务的合作伙伴,联合阿里云在万亿赛道上将云化技术与客户需求对接,实现客户价值和伙伴成长。

自成立以来,美创科技安全运维服务致力以专家级支撑服务体系、自动化工具赋能敏捷高效服务,安全运维服务涵盖:数据运维服务、数据安全治理咨询服务、数据分类分级咨询服务、个人信息风险评估服务、数据安全检查服务等。

目前,美创安全运维服务团队具备 ACED 1 名, ACE 3 名、OCM 大师 20 名、OCP 专家 60+ 名,一大批拥有阿里 ACP、达梦、WEBLOGIC、RHCA、RHCE、DB2、AIX、MSCE、Vmware、HP 等认证技术专家,以及 DSMM 测评师、CISSP、CISP、CSA CZTP、ITIL、PMP、ACP、ISO 27001 等业界相关认证。

在自动化工具方面,数据库运维过程中,美创提供全场景工具化能力,通过自动化的工具服务,实现高效的故障发现及故障前置能力,针对数据安全治理咨询过程中的资产盘点分析、现状调研分析、风险 / 能力评估等环节,美创通过内置的数据安全咨询算法体系、结构化、模型化工具,使过程自动化完成,高效达成敏捷咨询。

近年来,美创科技服务能力已获得 CNCERT、中国网络安全审查技术与认证中心等权威机构认可,获得国家网络与信息安全信息通报机制技术支持单位、CNCERT 网络安全应急服务支撑单位(省级)、CCRC 信息安全应急响应服务资质、ITSS 运行维护服务能力三级等。

此次加入阿里云飞天生态合作伙伴 - 服务生态合作计划,美创科技将依托自身服务优势,以开放之姿,用更创新的技术、更专业的团队、更细致的服务,为用户创造价值,与头部机构建设可持续发展的健康行业生态。



美创科技入围中国电信成员单位 - 数据安全产品供应商

9月，中国电信成员单位 - 天翼安全科技有限公司开展了数据安全能力供应商评选。美创科技凭借专业实力和丰富的落地案例经验成为本次入围的8家厂商之一，入选数据安全产品及服务总计19个。



美创科技与联通（浙江）产互签署战略合作协议

10月24日，杭州美创科技股份有限公司（以下简称：美创科技）与联通（浙江）产业互联网有限公司（以下简称：联通（浙江）产互）在美创科技杭州总部签署战略合作协议。美创科技 CEO 柳遵梁、联合创始人 & 副总裁徐荣星、闻建霞、胡江涛，联通（浙江）产互总经理钱建华、副总经理陈叶能、杨亚伟及双方公司相关领导出席了签约仪式。



签约仪式前，联通（浙江）产互总经理钱建华等一行参观了美创科技产品及解决方案展示中心，美创科技 CEO 柳遵梁陪同参观，并详细介绍了公司数据安全的整体优势，以及数字化转型、运行安全等业务的发展情况。

签约仪式上，双方代表先后致辞，美创科技 CEO 柳遵梁首先对联通（浙江）产互总经理钱建华一行的到访表示热烈欢迎，他指出：联通（浙江）产互是美创科技一直以来非常看重的合作伙伴。美创内部在三五年前就提出一句话，顺云者生逆云者亡。数据上云是大势所趋，也是美创产品线关注的优先事项，“云优先”和“解决云上数据安全复杂型管理问题”，是美创科技产品方案着力的两个基础方向。联通云是中国云计算服务市场中的重要一极，近年来，取得高速发展，此次战略合作，希望我们基于双方优势，共同深化研发、市场的配置与整合能力，为各行业用户提供更优质的数据安全技术与解决方案，期待我们能够在未来快速增长道路上相互扶持，相互合作，取得胜利。



美创科技 CEO 柳遵梁及相关领导



联通（浙江）产互总经理钱建华及相关领导

联通（浙江）产互总经理钱建华对美创科技一直以来的关心支持表示感谢，并表示：数字化改革大背景下，网络数据安全已经成为护航经济发展、保障社会安全的重要基石。作为网络强国、数字中国、智慧社会建设主力军，公司在网络安全、数据安全等领域已开始探索实践。美创在数据安全产品研发、安全运营服务等方面经验丰富，希望双方后续能够整合优势资源，早日结出硕果，打造出坚实、可靠的立体安全防护盾，为推动浙江数字经济社会高质量发展做出更大贡献！

签约仪式后，双方举行座谈交流，美创科技售前专家葛宏斌对公司业务及数据安全能力进行了详细分享。面对复杂的数据安全现状，美创科技以专业的数据安全治理咨询服务、数据安全产品能力，数据安全运营保障，着力构建五大体系，全面加强对数据的安全管控。具体包括：规范体系建设、技术防御体系建设、防控运营体系建设、安全监管体系建设、应急指挥体系建设。

交流中，钱建华总经理对美创全栈数据安全能力予以肯定，他表示：2022年是中国联通落实新战略的开局之年，联通（浙江）产互将不断探索网络数据安全治理新技术、新领域。希望今后能通过高层互访、联席会议等机制，切实推进各个合作项目的落地，达成实质性的深度合作。

作为国内领先的数据安全厂商，美创科技在数字政府、智慧城市、智慧交通等相关领域与联通（浙江）产互天然契合，在业务、产品层面上有着良好的资源互补。双方将以此次战略合作为契机，充分发挥各自优势，双向赋能，共同发展。

北京、福州、广州、南京等地渠道会合集



南京

5月20日，“共建生态 共创美好”美创科技 2022 年渠道签约会（南京站）成功举办，美创江苏省省级总代及白金 / 金牌级合作伙伴共 50 余人参加会议，共同探索数据安全背景下的合作商机。会议为大家带来了美创科技 2022 年全新的合作伙伴政策规划，现场近 20 家渠道伙伴与美创现场进行合作签约，成功加入美创合作伙伴体系。



苏州

美创科技 2022 年第二场共渠道签约会（苏州站）于 6 月 2 日在苏州苏苑饭店顺利召开。本次会议以“共建生态 共创美好”为主题，美创科技苏州总代以及白金、金牌合作伙伴共计 40 余人参加会议。现场我们与与合作伙伴分享了全新发布的渠道政策和美创的产品方案、对数据安全法、个保法等法规政策进行全面解读。



杭州

6月24日，“共建生态 共创美好”美创科技 2022 年渠道招募会（杭州站）成功举办。会上，美创科技联合创始人、副总裁胡江涛致欢迎词，浙江大区总经理成林林对公司整体情况及过往工作成绩进行总结，并对美创在浙江的本土化优势进行分享。来自浙江省内的 150 余家客户参加会议，现场超 20 家渠道与美创进行合作签约，成功加入美创合作伙伴体系。



北京

7月8日，全国业务有序复苏，美创北京分公司作为美创科技在北方市场的重要阵地，落实公司渠道战略，成功举办北京渠道招募会，现场签约 9 家合作伙伴。



广州

7月15日，“共建生态 共创美好”美创科技 2022 年渠道招募会（广州站）成功举办。会议带来了美创科技 2022 年全新的合作伙伴政策规划和数据安全解决方案。现场，100 余家合作伙伴参加会议，12 家渠道参与现场签约及授牌仪式。



福州

8月19日，“共建生态 共创美好”美创科技 2022 年渠道招募会（福州站）顺利召开，吸引到来自福州地区 60+ 位渠道伙伴出席，现场签约白金及金牌渠道 13 家，并与福建信实律师事务所达成战略合作，后续将在数据合规领域业务展开深入合作。

美 · 祈愿

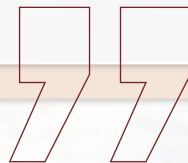
MEICHUANG · PRAY

闻建霞

杭州美创科技股份有限公司联合创始人、副总裁

2022 年是《数据安全法》和《个人信息保护法》正式实施一周年，也是数字经济高速发展的一年，数据安全作为数字经济的基础和保障，一个全新的赛道正在形成。新赛道下有更多的机遇和挑战，在此感谢美创所有同仁们，全面提升了全路径数据安全能力，特别是信创和云安全的能力，感谢美创所有合作伙伴，让更多用户使用美创产品和服务，更要感谢全国用户们，持续的新需求推动了我们的进步。新的一年，美创将继续紧跟国产化和数字经济的步伐，持续研究数据安全新技术，推出更好的产品，更好的服务。

最后衷心祝愿全社会的数据将越来越安全。



胡江涛

杭州美创科技股份有限公司联合创始人、副总裁

2022 年是极具挑战的一年，我们按计划实现了『稳住基本盘、持续做增量』的阶段性目标：保持了政府和医疗两大行业的总体产出，同时开拓了企业市场的良好增量。渠道建设作为公司发展战略之一，在 2022 年完成了体系搭建及全国布局，为美创 2023 年的腾飞做好了准备。

随着数字化政府的进展，数据作为新型生产要素，必定会在很长一段时期内推动中国信息化的发展。而数据安全的基石，数据安全成为 IT 市场的高增长领域已成现实。作为数据安全行业的领导者，引领市场、抢占市场是美创人责无旁贷的使命！让我们一起为 2023 年的 IPO 努力！



周杰

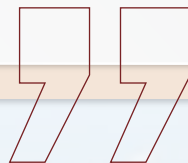
杭州美创科技股份有限公司 CTO

回望 2022 年，面对数据安全产业快速发展机遇和不断变化的市场环境，坚定“唯创新者胜”的信念，在困难中不断突破，在危机中孕育新机，与变局中开新局。

2022 年狠抓重点项目快抢拼，打造产品文化出精品，聚焦云端架构、复杂性管理、云环境优先的产品战略，打造核心产品竞争力，并且高质量打赢四季度项目交付攻坚战。

2023 年在强化现有成果的基础上，继续深化客户价值提质效，以业务为导向，以客户为中心，结合客户业务场景做实产品功能、做精产品易用性，强化策略内置、开箱即用的能力，打造流量产品。

2023 年将继续坚持锐意创新的勇气、敢为人先的锐气、蓬勃向上的朝气，同心聚力，乘势而上，奋力攻坚，砥砺前行！



王利强

杭州美创科技股份有限公司副总裁

回顾过去一年，公司业绩稳步增长，巩固优势行业的同时积极扩展了水利等关基行业，同时渠道销售体系完成了优秀产品输出到渠道生态的工作，为全市场覆盖打下了坚实基础。公司产品线也取得了长足进步，数据安全产品持续领跑细分赛道，并通过数据安全体系建立了高一纬度的领先优势，配合运行安全和数字化产品线的进展，足以满足客户刚需的数据安全体系建设，以及关基保护所需的业务连续性体系建设，以及数字化转型所需的数据资产管理体系建设。在这些成绩背后离不开组织级赋能计划，拉通前后端取得了良好效果，新产解中心的定位和职责为销售团队提供了商机指导方案和打通了产品到客户的转化通道，促进了产品线与售前体系无缝对接来服务客户，同时交付服务体系的打通也取得了明显效果，为组织效能提供了有力保障。

2022 年是艰难的一年，也是希望开启的一年，国际形势变化带来了很多的“危”与“机”，随着新的“十四五”规划中的国家经济投资结构性转移，众多工业企业与国计民生行业都在未来 5 年内得到重点关注和资金支持，围绕安全与数字化的发展规划思路将是对美创的最大利好消息，在美创固有的优势行业包括金融、交通、能源、水利等关键基础设施行业会带来巨大增长机会，美创需要抓住时机在高速增长的市场中保持竞争力和扩大市场占有率。为促进战略落地和目标达成，公司将继续围绕客户提供解决方案，高举产品大旗，构建积极可扩展的商业生态，并为此积极建设组织能力，提高组织响应和高效流程执行能力，加强人才配置和培养机制，为未来 5 年高速发展奠定公司级别的竞争力。



美 · 杂谈

MEICHUANG · OPINION

看过来!“老柳杂谈”专栏持续更新中

“老柳杂谈”是美创科技 CEO 柳遵梁总在 2022 年 7 月开辟的内部发声平台，传递柳总对于行业发展、企业管理等方面的思考和体悟，每篇文章简短精炼、高屋建瓴，半年来已更新百余篇内容。

如何看见
从看得到到看得见
如何重现感知世界
人(身份)的安全
业务逻辑安全

美·聚力

BEAUTY · COHESION

团建拓展活动



美创俱乐部

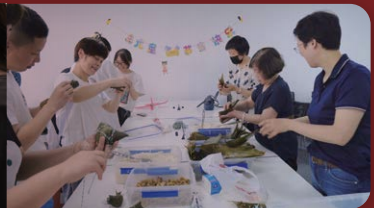
美创科技瑜伽俱乐部



美创科技篮球俱乐部



节日趣味活动



美创欢乐跑



爱心助学，暖心起航



团建拓展活动

提升团队活力和战斗力，建立更好的信任感，提高工作当中的紧密配合度，部门团建发挥着重要的作用。劳逸结合，携手前行，一“七”赢未来。快来看看活力四射、充满凝聚力的团队吧。



浙江大区



运维和安全服务产品线



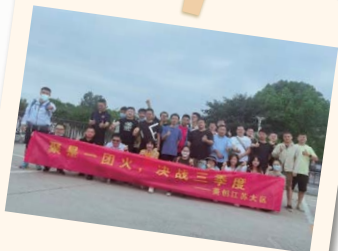
通用技术中心+安全实验室



数据安全产品线



数据安全产品线



江苏大区



苏皖大区

美创俱乐部

为了加强企业文化建设，丰富员工的业余体育生活，增强员工体质，促进员工间的理解和沟通，美创工会运动健身俱乐部于7月正式成立了！

篮球、足球、羽毛球、乒乓球、瑜伽、游泳、亲子、跑步八大俱乐部的活动开展得如火如荼。



节日趣味活动

▼ 妇女节



▼ 儿童节



▼ 端午节



▼ 端午节



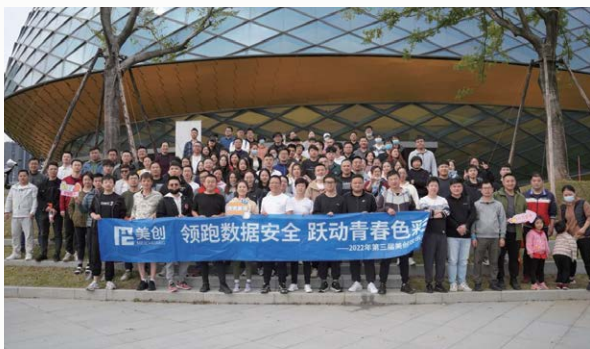
美创欢乐跑

领跑数据安全，跃动青春色彩

“自古逢秋悲寂寥，我言秋日胜春朝”，秋日正是户外跑步的好时候。

10月，一年一度的美创欢乐跑在全国多地开跑。

大家你追我赶、斗志昂扬，脸上都洋溢着自信，充分展现了朝气蓬勃、健康向上的精神风貌。



▲ 杭州总部



▲ 广州办事处



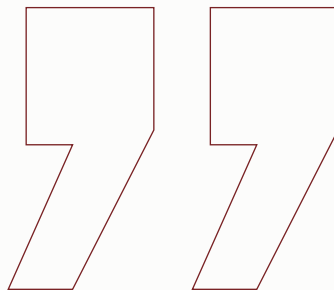
▲ 北京中心



▲ 成都办事处



▲ 江苏大区



爱心助学，暖心起航

美创科技在曲河小学开展爱心捐赠活动

天地有爱，化生万物；自然有爱，云行雨施；人间有爱，生命不息。

12月7日上午，杭州市美创科技股份有限公司来到曲河小学进行爱心助学捐赠活动，为孩子们送来冬日的温暖。



杭州美创科技股份有限公司联合创始人胡江涛先生，潜心躬耕企业发展，热心致力公益事业。从2021年11月起，陆续向曲河小学捐赠联想笔记本电脑、学生冬季冲锋衣校服、图书、球类、益智棋设施等物资，总计10万元。



社会爱心人士的善举，不仅改善了学校的条件，更浸润了学生们的心田。学生们纷纷表示将铭记爱心人士的深情关爱，并以此为动力，刻苦学习，提高素质，练好本领。同时也将以他们为榜样，帮助身边的人，用实际行动将爱传递下去。



杭州美创科技股份有限公司
HANGZHOU MEICHUANG TECHNOLOGY CO.,LTD



美创资讯