在线新经济系列报告

2022
非接触新经济安全治理报告

GOVERNMENT OF
SECURITY ON TOUGHNESS ECONOMY

SICSI
CYBER RESEARCH INSTITUTE
赛博研究院

安恒信息
DAS-SECURITY 安全中国

版权声明

COPYRIGHT STATEMENT

编写组成员

上海赛博网络安全产业创新研究院

惠志斌、李宁、唐巧盈、朱哲、周雪静

杭州安恒信息技术股份有限公司

周俊、李艳、王程程、罗剑东、夏先宁、

毛润华、叶鹏、张磊、郑舟

出品方

上海赛博网络安全产业创新研究院

杭州安恒信息技术股份有限公司

ABSTRACT | 内容摘要

当前，距离新冠疫情爆发已逾两年，我们发现，当年疫情催生的非接触新经济各个领域依然保持着新鲜活力，在互联网、云计算、大数据、人工智能、VR/AR、5G 等新一代信息技术的加持下，非接触新经济在办公、商业、教育、医疗、消费、文旅、会展等众多领域百花齐放，推动各个领域与数字化深度融合，为生产带来更高效率，为生活带来更便捷体验。在疫情常态化防控阶段，虽然线下的生产生活模式日益恢复常态，但人们线上化的交互习惯已经养成，线上服务已形成用户依赖度，使得非接触新经济得以保持持续稳定增长，加速我国数字经济高质量发展。

但与此同时，网络空间的规模和运行速度在快速扩张，网络安全威胁和风险日益加剧，网络攻击的真实案例每天都在上演。目前，普遍来看，组织的网络安全意识仍然非常薄弱，尤其是大量的中小企业，由于网络安全防护措施严重不足，已经成为网络攻击的重灾区。对此，国家相关监管部门已在医疗、教育、直播等领域发布了相关政策法规，要求加强网络安全和数据安全防护，保障用户切身利益。但对于在线办公、无接触配送、虚拟会展等其他非接触在线场景，目前法律法规、标准制定等仍较为欠缺，无法保障这些服务的安全应用。

对此，本报告在国家监管层面和组织管理层面分别提出了安全治理建议，包括在监管层面，需要国家相关部门进一步加快法律法规建设，加大对非接触线上化产品和服务的监管，将网络安全纳入产品和服务的硬性质控指标，提升产品和服务提供商的安全风险意识和合规意识，切实保障用户权益。同时，相关监管部门和标准化组织应为企业提供具体的、易于使用和清晰的网络安全指南、指引和实践手册，指导企业落实和部署法规要求的管理和技术措施。在组织层面，报告从短期和长期角度为组织提供了需重点关注的安全措施，供组织提升安全治理能力，确保数据、服务和系统安全。最后，报告在远程办公、智慧医院、在线教育、物联网等方面为组织提供了具体场景下的网络安全解决方案，供业内相关企业参考。

CONTENTS | 目录

PART 1
非接触新经济持续保持强劲活力

新冠疫情爆发已经两年多时间，截至目前，我国疫情防控取得阶段性成果，在“动态清零”总方针下，除少数中高风险地区外，经济社会已全面复工复产，人们生活基本回归常态。在生产生活需求和新一代信息技术的驱动下，2020 年疫情催生的非接触新经济当前仍保持着新鲜活力，疫情培养的用户习惯在这两年得到了延续，例如在线会议、互联网医院、无接触配送、线上教育等模式，都持续重塑人们的生产生活方式。

在《2020 非接触新经济安全治理报告》中，我们曾经预测，在后疫情时代，“非接触经济”将与“接触经济”互补发展，满足人们的个性化和多样化需求，传统行业对数字化更紧迫的需求将推动非接触新经济蓬勃发展，非接触新经济形态将为我国经济转型带来重大机遇，成为经济发展的新力量。当前来看，非接触新经济发展印证了我们之前的预测，其作为新业态新模式保持着稳步增长，已成为国民经济持续增长的关键动力。据国家税务总局数据显示，2021 年数字经济核心产业销售收入同比增长 30.7%，两年平均增长 22.8%，较全国企业销售收入增速高 8.6 个百分点。其中，智能设备制造同比增长 64.3%，互联网相关服务增长 61.5%，软件开发增长 28.2%。另据国家统计局数据显示，2021 年信息传输、软件和信息技术服务业增加值增长 17.2%，增速明显高于同期服务业其他领域。

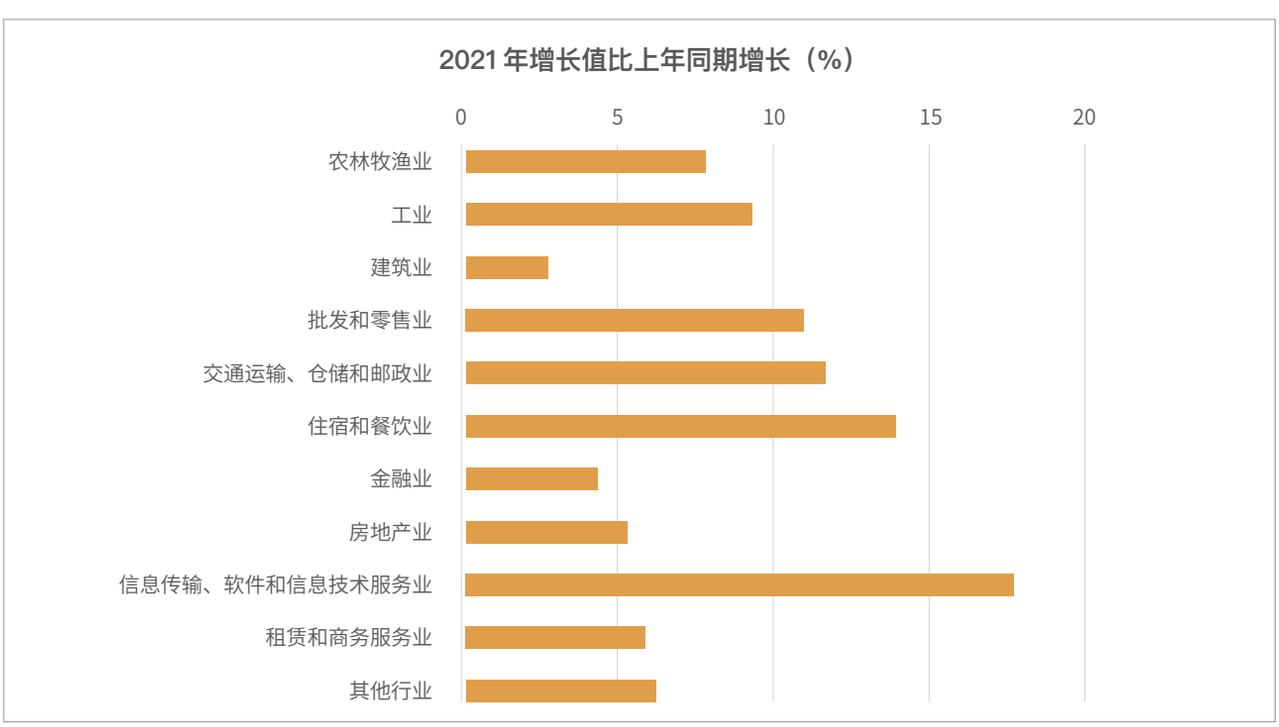

图 1 2021 年各行业增加值同期增长率对比

1.1 | 在线办公

2020 年新冠疫情为远程办公带来了极佳的市场培育机会，如今，远程办公成为了现场办公的一种有效的补充方式，例如在线视频会议，可以高效解决远程沟通问题，现已成为职场沟通的重要渠道。虽然随着疫情好转线下办公恢复常态，但在线协助办公的需求没有消失，使得行业得以持续增长。

在线协同办公平台

过去两年，在线协同办公平台已形成较大规模的普及。2020 年初疫情爆发期间在线办公平台呈现流量井喷的增长态势，行业 MAU 在 2020 年 2 月开始大幅增长，并在 4 月达到峰值 4.68 亿 。随着疫情好转以及线下办公恢复常态，在线协同办公平台的用户活跃度有所回落，但在 2021 年 1 月 –12 月，行业 MAU 均值仍有 3.47 亿的量级，行业渗透率保持在 60%以上。表明在线协同办公行业并不只是短期内的爆发，而是已经形成了长期的发展趋势，在未来将会持续大规模地普及。

在线会议

相关数据显示，疫情以来，美国平均每天举行 1100 万场在线会议，平均时长为 30—60 分钟。腾讯会议的用户数也持续攀升，在 2021 年 11 月达到 2 亿，同比增长一倍，2020 年 11 月至 2021 年 11 月一年时间内用户的参会次数超过 40 亿。据腾讯研究院 & 野村综合研究所发布的《2021 在线会议平台社会价值中日联合调查报告》显示，中国大、中型企业中在线会议的渗透率分别为 73.34% 和 79.51%。此外，微软旗下的通信和协作平台 Microsoft Teams 在 2021 年 12 月的月活跃用户数量突破 2.7 亿，而这一数据在 2020 年 3 月仅为 4400 万。这些数据表明在线会议开启了人们办公协作的新模式，形成了用户依赖度，满足了持续存在的远程协作需求。

1.2 | 互联网医疗

2020 年疫情爆发以来，互联网医疗在慢病管理、术后患者随访管理等方面发挥了重要的作用，帮助慢病患者足不出户实现网上复诊购药。这种新的诊疗方式被催生后，逐渐受到患者的信赖，为患者开辟了更加便捷、高效的就医渠道，满足了特定人群的就医需求，有效分解了线下诊疗压力。不管是否处于疫情时段，这种需求都是持久存在的，在信息技术的加持下，互联网医疗迎来了高速增长。

目前在国内，新冠疫情影响下的互联网医院建设已呈全面铺开之势。国家卫健委数据显示，截至2021 年 6 月份，全国互联网医院已超 1600 家，已经有超过 20% 的中国医生进入互联网医疗平台提供在线医疗服务，7700 余家二级以上医院提供相应的网上诊疗服务。并且随着政策加码，互联网医疗企业获得资本青睐，行业融资提速。2021 年以来，医渡科技、鹰瞳科技等企业都传来上市的消息。此外，微医、叮当健康、智云健康、思派健康、圆心科技、科亚医疗、数坤科技等互联网医疗相关企业也向港交所递交了招股书。

顺应互联网医疗的发展，国家有关部门也积极制定了相关的监管政策。先后发布《互联网诊疗管理办法（试行）》《互联网医院管理办法（试行）》《互联网诊疗监管细则（征求意见稿）》《远程医疗服务管理规范（试行）》《关于推进医疗机构远程医疗服务的意见》等文件。此外，目前，全国已有 30 个省份建立省级互联网医疗服务监管平台，实现了对辖区内医疗机构开展的互联网诊疗活动进行监管。

此外，互联网医疗已纳入医保范围。2020 年 11 月 2 日，国家医疗保障局公布《关于积极推进“互联网 +”医疗服务医保支付工作的指导意见》指出，支持符合规定的“互联网 +”医疗服务发展，对线上、线下医疗服务实行公平的医保支付政策。《意见》明确，根据地方医保政策和提供“互联网 +”医疗服务的定点医疗机构的服务内容确定支付范围。例如，各地可从门诊慢特病开始，逐步扩大医保对常见病、慢性病“互联网 +”医疗服务支付的范围。同时，结合门诊费用直接结算试点，按照相关规定的异地就医结算流程和待遇政策，探索“互联网 +”医疗服务异地就医直接结算。

互联网医疗的本质是实体医疗的延伸，是将实体医疗变得更加方便、高效、快捷，让患者就医更具可及性。通过院前的线上咨询、预约挂号，到院中的导医导诊、消息服务、在线缴费、报告查询，再到院后的查看处方、患者随访、医患互动，互联网医疗将不断改善患者就医体验。随着支持与监管相关政策的不断完善，预计未来几年互联网医院的数量将保持持续上升的趋势。**据预测，到 2024 年，中国互联网医疗市场规模将接近 5000 亿元 。**

1.3 | 在线教育

疫情爆发后的两年多时间里，虽然防疫取得一定成果，但疫情仍此起彼伏，在中高风险地区，学校正常线下教学仍不时受到影响，在线教育作为重要替代方案，成为疫情期间教学的重要补充，保证了学生的停课不停学。

2020 年疫情爆发后，在线教育行业飞速发展，迅速成为资本新宠。然而 2021 年 7 月以来，双减等监管措施对K12 阶段学科类在线教育形成重大打击。但在线素质教育和在线职业教育仍保持稳步增长。目前，在线教育行业进入了高质量发展阶段。

在线职业教育

在政策推动、需求扩张和大众认知提升等多重因素推动下，在线职业教育有了更加完善、健全的体系，行业也渐渐走向了发展快车道。2020 年市场规模已达 3222 亿元，占职业教育市场比重达 50% 左右。预计未来五年在线职业教育市场规模增速将保持在 14% 以上，2025 年市场规模有望达到 6497 亿元 。

在线职业教育也受到了资本的追捧。据网经社旗下电商大数据库“电数宝”监测数据，2021 年我国在线职业教育有 36 家平台获得融资，融资总额超 61.9 亿元。在国家政策支持与市场资本的加持下，我国的在线职业教育行业已在多个领域发展出多个龙头企业，如聚合了语言培训、大学生考试、财经、公考、教资、留学、管理、医疗等多类型职业教育业务的高途集团，开设了实用英语、教师、财会、公考等主流职教品类的作业帮，聚焦成人职业技能培养，创新性在声音培训、写作培训等多种职业培训上赋能行业与个人的互联网新职业在线教育平台十方融海梨花教育等。

从头部 APP 月活用户规模来看 ，2021 年 6 月，仅粉笔教育一款 APP 月活用户数量就达 547.7 万人，其余 APP 月活用户数量也均在百万以上，涉及职业包括公考类、综合类、教师类、会计类、企业培训类、法考类以及编程类等。

在线职业教育快速发展，主要源自于消费者人群大幅拓展，同时，供给端内容更加丰富多元，类目不断拓展。此外，在线职业教育的便利性使得消费者可以利用碎片化时间随时随地学习。未来，随着技术的不断升级，在线职业教育可以实现更加丰富的线上互动，满足消费者的职业再教育需求。

在线素质教育

随着监管部门对 K12 学科类教育培训的审查收紧，以思维训练、艺术培养为主的素质教育在疫情催化下，呈现“线上化”趋势。其中音乐教育的 AI 陪练、直播工具等软硬件配套产品不断提升用户体验，并推动音乐教育向智能、高效的方向前行。此外，随着 5G 应用逐步落地，诸如舞蹈、体育等对线上要求更高的领域，也在逐步尝试在线化。

就业：网络招聘会 & 线上面试

2020 年招聘季，线上招聘会在疫情期间发挥了重要作用。两年后的今天，由于疫情原因，线上招聘会依旧是毕业生就业的重要途径，多地通过线上方式举办大型招聘会。当前，由于技术的发展，线上招聘会的功能更多丰富和便捷，例如通过 VR 招聘会，毕业生可以了解具体招聘企业及岗位，毕业生进入活动展厅入口后，企业的展位可以像线下招聘会一样，分布在各层的展厅中。毕业生可以选择心仪的公司投递简历、预约面试，也可以与 HR 在线面对面沟通。

某企业 HR 对应届毕业生进行线上面试

1.4 | 无接触配送

智能取餐柜

2020 年，疫情催生外卖自提新模式，智能快递柜行业迎来发展机遇，美团外卖率先在全国分批投放 1000 台外卖智能取餐柜。之后，智能取餐柜由于具有取餐时间灵活、避免外卖食品错拿丢失、提升食品安全防护、保护隐私等优势得到了广泛普及。目前，据估计，美团、饿了么铺设的智能取餐柜已达到上万台。

配送机器人

2020 年疫情期间，为避免人群聚集和过密接触，配送机器人迎来一展身手的机会，在医院等重点场所，配送机器人为病患配送药物、餐食等物资，在抗疫中发挥了重要作用。在疫情常态化防控下，配送机器人仍然发挥重要作用。上海疫情爆发后，配送机器人得到了广泛应用：达闼以 5G 云端机器人等先进科技，助力上海打造智慧方舱，分阶段

部署无接触配送机器人 Cloud Ginger Lite、Cloud Patrol；行深智能科技有限公司在上海方舱医院、多个街道和社区，投放无人配送车运行，通过无接触配送的方式，安全保障居民群众生活物资、工作人员防疫物资的及时送达；在临港方舱医院，无人车为病患、医护提供物资配送服务；上海多个酒店隔离点引入配送机器人，为隔离的高风险人群提供送餐服务。此外，2022 年 4 月初，美团从北京紧急调配一批自动配送车到上海，助力社区抗疫。该车一次性载重超 150 公斤，通过无接触配送，可有效缓解当下上海社区抗疫中最后一公里的配送难问题。

此外，在非疫情时期，配送机器人在酒店、餐厅等场所也得到了广泛应用。在餐饮行业，送餐机器人的成本越来越低，使其在诸如火锅店等场所的利用率大幅提高，可大大节省人力。

冬奥会酒店机器人自行乘坐电梯

餐饮场所配送机器人

1.5 | 虚拟会展

近年来，由于疫情原因，以及云计算、虚拟现实等技术的快速发展，虚拟会展得到了广泛普及，国内外多场大型峰会和展览活动采用线上方式，参会者可便捷高效的参与其中。线上虚拟展览以营造虚拟体验为主要目标，通过 3D 建模、VR/AR/MR、数字孪生、多媒体动画、视频技术、社交技术等技术手段相结合，实现会展参与对象、会展空间、展台、展品、对接项目等展示对象的虚拟化、数字化，为展会观众营造身临其境的沉浸式展示环境。AI/VR 数字化展览展示，支持语音、文字、视频动画等丰富的内容载体，通过直播远距离的交互，让更多生动有趣的讲解可以直达用户端，带来冲击力与吸引力。此外，“会展 + 元宇宙”技术和创新场景正在进一步丰富会展的内涵和外延。

据《2022 年虚拟会展发展报告》 调查显示，1250 名被调研的组织者和参与者中，有 92% 的组织者已在 2021 年将会展活动转向线上，94% 的组织者计划在 2022 年举办线上虚拟会展。另有 75% 的与会者表示即使线下活动完全恢复，他们仍将参加虚拟活动。84% 的与会者希望始终拥有可供他们使用的在线参与选项，以便他们可以选择以虚拟 / 远程与会者的身份参加任何活动。2021 年对全球 8227 名营销人员进行的一项调查显示，预计到 2022 年，他们 40% 的活动将采用虚拟方式举办，

35% 的活动预计将采用线上 + 线下的方式举办，另外 35% 的活动预计将采用线下方式举办。这表明，虚拟会展模式在未来将继续激增。据《2022–2030 虚拟会展市场规模和发展趋势分析报告》 预测，2021 年全球虚拟会展市场规模为 1141.2 亿美元，预计 2022 年到 2030 年将以 21.4% 的复合年增长率增长。

1.6 | 非接触式消费

直播电商

2020 年新冠疫情的爆发大大加快了直播电商的发展，直播行业爆发，大批线下实体商店把直播作为“云复工”首选，无论是创新不断的新品牌，还是较为传统保守的老字号，都在积极通过直播线上卖货。如今，消费者直播购物习惯不断深化，直播电商继续高歌猛进，用户交易规模持续膨胀，产业链不断完善，直播渠道与参与者更加多元化，行业获得爆发式增长，成为品牌主无法忽略的带货方式。数据显示，2021 年，抖音 & 快手带货直播场次超 7500 万场，同比增长 100%，直播带货商品链接数超 3.9 亿个，同比增长 308% 。

生鲜电商

受新冠疫情影响，2020 年中国生鲜电商市场快速发展，生鲜电商行业规模达 4584.9 亿元 。随着生鲜电商的发展及模式的成熟、用户网购生鲜习惯的养成，生鲜电商用户覆盖数量愈发广泛，据网经社“电数宝”电商大数据库显示，2021 年生鲜电商交易规模达 4658.1 亿元，同比增长 27.92% 。预计未来生鲜电商仍将保持高速增长，到 2023 年行业规模将超万亿。

社区团购

2020 年疫情期间，社区团购也迎来爆发式增长，美团、京东、拼多多、阿里、滴滴等相继将社区团购作为重点拓展业务，资本的投入大大提升了社区团购行业的发展速度，社区团购开始在全国范围内拓展。不过 2021 年 3 月，市场监管总局依法对橙心优选、多多买菜、美团优选、十荟团等社区团购企业的劣性竞争行为处以天价罚款，同时大量团长由于佣金大幅降低纷纷申请退出平台，用户也流失严重，导致行业发展减速。

此轮上海疫情爆发后，生鲜快消供应链受压，自发的社区团购成为了人们的“救命稻草”，居民纷纷利用微信小程序、接龙等方式采购生活物资。除了自发的团购模式外，为解决上海疫情期间需求激

增、运力不足等问题，叮咚买菜、美团买菜、盒马生鲜等电商也推出“邻里团”“社区团餐”“社区集单”等社区团购新模式，全力保障居民“菜篮子”。以叮咚买菜为例，其紧急推出了“叮咚邻里团”，进行集约式保供，把基础民生商品如蔬菜、水果、肉禽蛋、米面油做成组合套餐，每天统一配送到每个小区的自提点，将配送效率最大化，尽可能满足特殊时期居民们的菜篮子需求。此波疫情可能再次推动社区团购模式兴起，催生一批线上团购的新业态新模式。

自助收银

结账时无需排长队等待，在挑选好商品后，经自助收银机“放入商品、扫码支付、自助装袋”等步骤后，即可结账走人……2021 年，无接触自助收银服务在盒马鲜生、沃尔玛、家乐福、优衣库等全国各地各商业门店悄然兴起，让消费者体验到什么叫“收银速度”。

自助收银的结算方式比人工收银更加方便，它结合了条码扫描器的自动识别、采集并实时传输的功能特性，结合自助收银系统可以实现快速购物，加速超市购物人员的流通。整个结算过程，消费者自己扫码支付就能操作完成，节省了很多排队结账的时间。数据显示，自助收银机和自助结算终端的确能大幅提升超市便利店的收银效率，优化人员调配。据调查，平均 3 台自助收银机，可以节省 1 个员工人工。

PART 2
非接触新经济网络安全风险与挑战

2.1 网络空间迅速扩张

疫情下非接触的需求以及人们对更快捷便利服务的需求，驱动各种业务和服务由线下转线上，使得由各种信息技术支撑的网络空间不断扩张，这些技术将共同构成一个创新平台，其架构、组件、关系和流程不断变化，以支持新兴的想法、服务和商业需求。当前，网络空间的体量正在发生变化：

规模：随着新的互联设备、网络、服务和数据的出现，网络空间正在迅速发展。这不仅带来了网络规模的变化，也带来了数据量、存储容量、处理系统和知识空间的变化。对大多数人来说，网络空间的规模已经难以概念化。

速度：通信和数据处理可以以不断加快的速度进行，这使得商业交易和流程、关系创建、内容和思想的发布和共享以及价值的生成得以不断加快。

互联性：在网络空间、组织和供应链中，系统的互联性和行为者的相互依赖程度都在不断提高。

2.2 网络安全事件频发

非接触新经济的本质是传统行业的线上化、网络化和数字化，其高度依赖互联网、云计算、人工智能、大数据、智能硬件、5G、物联网、VR/AR 等新一代信息通信技术作为支撑。非接触新经济的这一特性使得网络安全因素成为其发展的重要风险和挑战。近两年，在非接触新经济各个领域，网络攻击事件频发，为产业发展和用户体验带来不利影响。全球范围内，与疫情相关的恶意电子邮件、网络钓鱼攻击、诈骗和恶意软件显著增加。另外，值得注意的是，中小企业群体成为网络攻击的重要目标，因为他们普遍缺乏足够的网络安全防御措施。

远程办公

2020 年 7 月推特大规模黑客攻击事件由远程办公导致。2020 年 7 月，美国著名社交媒体推特（Twitter）多名知名人士账户被黑客盗用，其中包括奥巴马、拜登、比尔盖茨和特斯拉 CEO 马斯克。盗用者发布虚假信息称，只要向某个账户转账价值 1000 美元的比特币就会返还 2000 美元的比特币，据悉黑客至少获得了价值 11.3 万美元比特币的转账。2020 年 3 月，全面推行远程办公的升温给推特的技术基础设施带来了压力，员工在连接虚拟专用网络时经常出现问题。黑客利用这些问题，假装从推特的 IT 部门打来电话询问虚拟专用网络问题，然后劝说员工将自身凭证输入到近似的假冒虚拟专用网络登录网站。黑客由此获得了推特虚拟专用网络登录凭证。

欧洲 IT 服务提供商公司遭勒索软件攻击。欧洲的一家 IT 服务公司使用托管在数据中心的 15 台服务器为其客户提供软件更新。通常，该公司仅允许从公司自己的办公网络访问这些服务器。然而，新冠疫情期间，公司的所有员工都被迫采用了居家办公模式。为了方便其开发人员进行远程工作，该公司允许开发人员通过 Microsoft 远程桌面协议 (RDP) 访问其数据中心中的 15 台服务器。 然而，该公司并没有对他们的 RDP 连接采取保护措施，这使得犯罪分子通过 RDP 破坏了他们的系统，导致 14 台服务器遭到了勒索软件攻击。

远程办公使得电子邮件帐户被劫持以实施欺诈。欧洲一家营销和品牌公司将其电子邮件系统迁移到云端，以方便其员工在新冠疫情期间远程工作。其中一名员工遭到了网络钓鱼攻击，攻击者假装来自电子邮件提供商，要求该员工提供帐户验证详细信息，通过这种方式攻击者接管了他们的电子邮件帐户。然后，攻击者从被劫持的账户向营销和品牌公司的客户发送电子邮件。这些电子邮件混合了网络钓鱼电子邮件和发票重定向欺诈电子邮件。发票重定向欺诈电子邮件被发送给一些客户，告诉他们营销和品牌公司的银行详细信息已更改，并且所有未来的发票付款都应发送到新的银行账户（由攻击者控制）。该攻击是由一位客户发现的，随后该客户因担心网络安全而取消了所有与此营销和品牌公司的未来业务，每年价值 200000 至 300000 欧元。

互联网医疗

意大利地方疫苗接种预约系统因网络攻击被迫关闭。2021 年 8 月，黑客攻击了管理意大利罗马周边的拉齐奥地区 COVID–19 疫苗预约公司的 IT 系统，导致该系统被迫关闭，接种计划受到延误。黑客通过复制管理员密码侵入了拉齐奥大区政府的网络数据中心，并植入名为 Cryptolocker 的勒索软件。包括政府采购招标、证件发放、疫苗预约在内所有部门的门户网站以及政府社交网络账号均处于无法登录的瘫痪状态。

加拿大纽芬兰等多省遭受网络攻击，导致医疗服务严重中断。2021 年 10 月，加拿大纽芬兰和拉布拉多省的卫生网络遭到网络攻击瘫痪，导致全省数千人的医疗预约取消，多个地方卫生系统被迫重新使用纸张。受影响的医疗中心也被迫取消或重新安排化疗、X 光扫描、手术和其他专科服务的预约。

在线教育

印度最大在线教育平台 Unacademy 发生大规模数据泄露。2020 年 1 月，印度最大的在线教育平台 Unacademy 发生数据泄露事件，暴露了大约 1100 万用户的个人信息。该数据库在暗网上的售价为 2000 美元。Unacademy 泄漏的数据包括用户 ID、加密密码、电子邮件地址、加入日期和上次登录

时间等信息。

英国赫特福德大学遭受大规模网络攻击被迫停止网络授课。2021 年 4 月，英国赫特福德大学遭受了大规模的网络攻击，导致老师和学生们无法通过网课进行教学和学习，此外造成英国赫特福德大学的 WiFi 和电子邮件及服务器都被迫中断运行。

在线授课工具 Zoom 被曝存在两个严重漏洞。2021 年 11 月，Google Project Zero 安全研究人员发现在线授课软件 Zoom 存在两个重要漏洞，可能会让用户遭受攻击。这两个漏洞会影响 Windows、macOS、Linux、iOS 和 Android 平台上的 Zoom 客户端，这意味着几乎所有的用户都处于漏洞的威胁之中。俄罗斯网络安全公司 Positive Technologies 的研究人员也在同一时间发现了影响 Zoom Meeting Connector Controller、Zoom Virtual Room Connector、Zoom Recording Connector 和其他应用程序的漏洞。漏洞将允许攻击者输入命令来执行攻击，从而以最大权限获得服务器访问权限。

配送机器人

酒店送餐机器人被极客轻松攻击成功。在 2021 年 GeekPwn 极客大赛上，有选手通过入侵酒店送餐机器人的系统，将恶意代码植入，能将客人的外卖轻松“调包”。他们首先采用之前准备好的攻击脚本，获取它的远程管理员权限，然后使用手机作为移动终端，与机器人建立联系，修改了送餐的目标房间，成功掉包外卖。选手介绍，更具威胁的场景是，通过控制送餐机器人的运行，黑客将可能使一部电梯瘫痪。

Temi 医疗机器人存在高危漏洞。疫情爆发后，全球医疗机构广泛使用机器人协助医疗工作，其中 Temi 公司就在全球范围内一年售出 10000 多台机器人，供医疗机构使用。2020 年 8 月，网络安全公司 McAfee 找到了入侵 Temi 系统的方法。研究人员在 Temi 系统中发现了四个漏洞，这些漏洞使他们能够远程拦截电话、激活摄像头和麦克风并在房间内驾驶机器人。在某些情况下，这只需一个电话号码即可完成。

智能快递柜

俄罗斯快递柜公司遭黑客袭击 2732 个储物格瞬间全开。2020 年 12 月，一个神秘的俄罗斯黑客，利用网络攻击强行打开了一家快递服务公司 8000 个快递柜当中的 2732 个。虽然警察和小区物业在事件发生后迅速介入，限制人们进入明显出现故障的储物柜，但仍有部分客户反馈快递被冒领、丢失。

直播电商

国内 5000 多家直播平台遭受 DDoS 攻击。2020 年 12 月，南通市公安局对外通报，成功破获一起特大破坏计算机信息系统案，该犯罪团伙为打压竞争对手，设法从网上购买了“3ddos”流量攻击平台会员账号，利用该平台发起流量攻击，先后破坏 20 余个网络直播平台服务器，造成这些平台直播画面卡顿、不流畅，以增加自己平台的用户量。截至案发，该平台已累计向全国 5000 余家网站实施过流量攻击，总次数多达 58451 次。

自助收银

IT 服务供应商遭勒索软件入侵，导致瑞典超市连锁品牌 Coop 关闭旗下 800 家门店。2021 年 7 月，黑客通过袭击 IT 管理软件供应商 Kaseya 公司一个名为 VSA 的工具，向使用该公司技术的管理服务提供商（MSP）进行勒索，同时加密这些提供商客户的文件。20 家管理服务提供商受到威胁，这些公司的超过 1000 家客户成为此次勒索事件的受害者。这些客户的数据已经被黑客加密，只有支付赎金后才能获得。作为其中受影响最大的公司之一，瑞典超

市连锁品牌 Coop 表示关闭了旗下 800 家门店中的绝大部分。Coop 称，其管理服务提供商 Vissma Escom 遭到攻击后，影响了该超市的收银系统和自助收银台。

2.3 | 网络安全风险加剧

诸多实际发生的案例表明，网络安全风险已成为组织不容忽视的重要风险之一。据安联发布的《2022 全球风险晴雨表》 指出，通过调查来自全球 89 个国家和地区的 2650 名专家发现，在 2022 年全球最重要的商业风险 Top10 中，网络事件、业务中断和自然灾害是 2022 年全球面临的三大商业风险。其中，**网络事件（包括网络犯罪、IT 故障 / 停机、数据泄露、罚款和处罚等）被视为最为重要的风险，**持这一观点的受访者占比 44%，相较于 2021 年的 40% 有所提高。在不同场景下，面临的网络安全风险如表 1 所示。

表 1 非接触新经济网络安全风险

非接触场景	网络安全风险隐患
远程办公	1、远程沟通风险：沟通内容安全；文件存储、传输安全；离职员工泄露风险。 2、远程访问应用风险：远程人员身份安全风险；远程访问通道安全风险；越权操作风险。 3、远程开发风险：代码泄露风险；用户身份安全风险；访问通道安全风险。 4、运程运维风险：运维权限控制风险；运维审计风险；远程运维人员身份安全风险。
互联网医疗	1、互联网应用的使用安全风险：PC 端互联网门户网站；移动客户端软件下载渠道。 2、数据安全风险：与保险机构、药企、物流配送等第三方机构进行数据共享存在被窃取、别加密、被滥用的风险。 3、医院内外网交互中的安全风险：内外网边界更加模糊，内外面临的网络入侵和信息泄露风险明显增大。 4、在认证 – 授权 – 审计机制中，审计环节较为薄弱。
在线教育	1、互联网攻击风险：DDoS 攻击致不可用；入侵攻击；系统篡改；安全漏洞利用。 2、运程运维风险：身份安全风险；越权操作风险；高危操作风险。 3、数据安全风险：敏感信息窃取；内部信息泄露。
配送机器人	被恶意攻击者植入恶意代码，获取远程管理员权限，篡改系统配送信息
无人配送车	随着 V2X 技术应用和普及，“车辆”在与网络进行连接过程中，在感知层、通信层、软件层、云端等均存在被入侵的风险，一旦发生自动驾驶系统被入侵，就有可能失去“车辆”控制权，造成严重交通事故。

非接触场景	网络安全风险隐患
虚拟会展	虚拟会议平台可能存在高危漏洞，导致与会者个人敏感信息遭窃取和篡改，漏洞可能允许不法分子执行跨站点脚本攻击、窃取用户 cookie、冒充用户身份或将用户的网络浏览器跳转到不同的位置。
直播电商	1、遭遇 DDoS 攻击导致直播画面卡顿、不流畅。 2、直播间内链接、二维码等跳转服务指向恶意站点。
智能取餐柜	利用系统漏洞攻击后端网关，可能导致柜门自动打开。

2.4 网络安全管理的内部挑战

目前，对组织来讲，普遍存在的根本问题是网络安全意识薄弱，尤其对于中小企业而言，这将严重影响组织内部网络安全预算、资源分配和网络安全实践的有效实施。

1、组织普遍缺乏网络安全意识

在组织中，网络安全并非只涉及 IT 相关人员，而应该是组织文化的一部分，每个人至少应该对网络安全以及他们的态度如何影响整个组织的网络安全态势有基本的认识。例如，员工应该了解鱼叉式网络钓鱼和其他社会工程攻击的工作原理、使用自己的设备访问公司 ICT 环境的规则以及其他基本的网络安全预防措施。但据欧盟网络安全局（ENISA）发布的《中小企业网络安全挑战和建议》调查显示，在接受调查的中小企业中有 45% 实施了新技术以应对疫情，但超过 90% 没有实施任何新的安全措施来确保这些解决方案的安全性。除非网络安全控制作为 IT 解决方案的一部分包含在内，否则许多中小企业并没有意识到网络安全对其业务构成的潜在风险。

2、缺乏网络安全预算

网络安全准备工作需要从各个方面进行投资，包括意识培训、专业岗位培训、部署网络安全技术措施、聘请外部专家等。尽管许多组织已经采用新

的线上方式提供服务，但其中许多并未投资于任何额外的网络安全控制措施。许多组织尤其是中小企业将网络安全视为一种成本，而不是对其业务的投资。因此，中小企业必须更好地了解网络安全问题对其业务构成的风险，并分配适当的预算来投资于所需的控制措施。

3、缺乏网络安全专业人员

目前在很多组织尤其是中小企业中，普遍缺乏网络安全专职人员，甚至连兼职人员都没有。此外，许多网络安全解决方案需要专业的 IT 知识才能正确实施和管理。所有这些问题加在一起，使组织的网络安全管理工作成为一项巨大挑战。随着企业业务的发展和变化，其采用的技术将发生变化，网络威胁格局将不断变化，这要求组织确保其管理网络安全的努力应该是持续和一致的。如果公司不直接雇用具有专业网络安全知识的人员，则需要投资于外部专家。

4、对关键和敏感信息的保护不足

在医疗、教育、办公、消费等众多服务场景中，组织会收集、存储、处理大量的个人敏感信息，然而缺乏特定的数据备份策略、未在所有类型的设备上部署最新的终端反恶意软件解决方案、使用非自动更新的过时或未打补丁的软件，都可能会严重危及组织的关键和敏感信息，使其很容易成为勒索软件或其他网络攻击的目标。

5、影子 IT 和个人设备激增

许多企业允许员工使用个人设备访问公司系统和数据，这一趋势在疫情爆发后得到了加快。此外，员工还会通过从自己的家庭网络访问互联网，来访问公司系统和数据。在大多数情况下，这些家庭网络的安全性较差，没有以安全的方式进行配置。这导致企业的网络范围扩展到其所有员工的家中，带来了安全风险。

PART 3
国内非接触新经济安全监管现状

目前，国家相关行业监管部门在医疗、教育、直播等领域发布了相关政策法规，要求加强网络安全和数据安全防护，保障用户切身利益。

例如在医疗领域，2018 年 7 月，国卫医发〔2018〕25 号《关于印发互联网诊疗管理办法（试行）等 3 个文件的通知》，同步发布了《互联网诊疗管理办法（试行）》《互联网医院管理办法（试行）》《远程医疗服务管理规范（试行）》三个文件，旨在“进一步规范互联网诊疗行为，发挥远程医疗服务积极作用，提高医疗服务效率，保证医疗质量和医疗安全”。三份文件都提出了明确的网络安全要求，如《互联网诊疗管理办法（试行）》第十三条提出，“医疗机构开展互联网诊疗活动，应当具备满足互联网技术要求的设备设施、信息系统、技术人员以及信息安全系统，并实施第三级信息安全等级保护”，《互联网医院管理办法（试行）第十五条》提出，“互联网医院信息系统按照国家有关法律法规和规定，实施第三级信息安全等级保护”。2021 年 10 月，国家卫生健康委医政医管局公布《互联网诊疗监管细则（征求意见稿）》，第二十八条要求“医疗机构建立网络安全、个人信息保护、数据使用管理等制度，并与相关合作方签订协议，明确各方权责关系”，第三十一条要求“省级监管平台和医疗机构用于互联网诊疗平台应当实施第三级及以上信息安全等级保护”。

在教育领域，2019 年 7 月教育部等六部门公布《关于规范校外线上培训的实施意见》，要求校外线上培训落实网络安全等级保护制度、网络安全预警通报制度和用户信息保护制度，具有完善的安全保护技术措施，做好培训对象信息和数据安全防护，防止泄露隐私，不得非法出售或者非法向他人提供培训对象信息。2020 年疫情期间，教育部又连发《关于在疫情防控期间做好普通高等学校在线教学组织与管理工作的指导意见》《关于疫情防控期间以信息化支持教育教学工作的通知》《关于继续组织在线课程平台提供疫情防控期间支持高校开展在线教学的资源和服务方案的通知》三份文件，要求强化网络安全保障。其中《关于继续组织在线课程平台提供疫情防控期间支持高校开展在线教学的资源和服务方案的通知》提出在线课程平台须至少获得国家信息安全等级保护二级认证，要能够保证 24 小时运行，且运行安全稳定畅通。2022 年 3 月，教育部、中央网信办、工信部、公安部、市场监管总局联合发布《关于加强普通高等学校在线开放课程教学管理的若干意见》，第 11 条提出“提供学分课程的平台必须严格落实网络安全等级保护制度，履行安全保护义务，平台安全保护等级不应低于第三级”，第 15 条提出要“严格遵守国家网络安全管理规范，确保意识形态安全、信息内容安全、网络安全、数据安全、运行服务安全，有效防范有害信息传播、在线服务中断、数据篡改和师生个人信息泄露。”

在网络直播领域，2021 年 4 月，国家互联网信息办公室等 7 部门发布《网络直播营销管理办法（试行）》，第六条要求“直播营销平台应当建立健全账号及直播营销功能注册注销、信息安全管理、营销行为规范、未成年人保护、消费者权益保护、个人信息保护、网络和数据安全管理等机制、措施”，第九条要求“直播营销平台应当加强直播间内链接、二维码等跳转服务的信息安全管理，防范信息安全风险”。

综上所述，对于非接触新经济的发展，国家在医疗、教育、直播领域颁布了若干法律法规，从监管层面对相关通过在线方式提供服务的场景提出了明确的网络安全要求，这对于行业加强网络安全防护措施有一定的积极作用。但对于在线办公、无接触配送、虚拟会展等其他非接触在线场景，目前法律法规层面仍较为缺失，无法保障这些服务的安全应用。此外，相应的标准制定也比较欠缺，尤其在互联网医疗、在线教育、虚拟会展、以及消费等领域，标准依然处于空白。

表 2 我国非接触新经济各领域网络安全法规

领域	时间	发布机构	文件名称	网络安全相关需求
互联网医疗	2021.10.26	国家卫生健康委医政医管局	《互联网诊疗监管细则（征求意见稿）》	第二十八条 医疗机构应当建立网络安全、个人信息保护、数据使用管理等制度，并与相关合作方签订协议，明确各方权责关系。 第三十一条 省级监管平台和医疗机构用于互联网诊疗平台应当实施第三级及以上信息安全等级保护。
	2020.2.6	国家卫生健康委医政医管局	《国家卫生健康委办公厅关于在疫情防控中做好互联网诊疗咨询服务工作的通知》	要充分利用省级互联网诊疗服务监管平台，加强对互联网诊疗服务的事前、事中和事后的动态监管，加强医务人员资质、诊疗行为、处方流转、数据安全的监管，保障互联网医疗健康服务规范有序，确保医疗安全和质量，对不合规范的诊疗咨询行为进行预警和跟踪处理，对不良事件和患者投诉进行受理，确保群众健康权益。
	2018.7.17	国家卫生健康委员会、国家中医药管理局	《互联网诊疗管理办法（试行）》	第十三条 医疗机构开展互联网诊疗活动，应当具备满足互联网技术要求的设备设施、信息系统、技术人员以及信息安全系统，并实施第三级信息安全等级保护。 第二十条 医疗机构应当严格执行信息安全和医疗数据保密的有关法律法规，妥善保管患者信息，不得非法买卖、泄露患者信息。
	2018.7.17	国家卫生健康委员会、国家中医药管理局	《互联网医院管理办法（试行）	第十五条 互联网医院信息系统按照国家有关法律法规和规定，实施第三级信息安全等级保护。 第二十三条 互联网医院应当严格执行信息安全和医疗数据保密的有关法律法规，妥善保管患者信息，不得非法买卖、泄露患者信息。

领域	时间	发布机构	文件名称	网络安全相关需求
	2018.7.17	国家卫生健康委员会、国家中医药管理局	《远程医疗服务管理规范（试行）》	参与远程医疗运行各方应当加强信息安全和患者隐私保护，防止数据丢失，建立数据安全管理规程，确保网络安全、操作安全、数据安全、隐私安全。
在线教育	2022.3.10	教育部、中央网信办、工信部、公安部、 市场监管总局	《教育部等五部门关于加强普通高等学校在线开放课程教学管理的若干意见》	11. 提供学分课程的平台必须严格落实网络安全等级保护制度，履行安全保护义务，平台安全保护等级不应低于第三级。 15. 严格遵守国家网络安全管理规范，确保意识形态安全、信息内容安全、网络安全、数据安全、运行服务安全，有效防范有害信息传播、在线服务中断、数据篡改和师生个人信息泄露。
	2020.2.4	教育部应对新型冠状病毒感染肺炎疫情工作领导小组办公室	《关于在疫情防控期间做好普通高等学校在线教学组织与管理工作的指导意见》	确保在线教学安全平稳运行。高校要与课程平台就在线教学组织进行充分沟通，择优选取符合本校实际、与网络环境条件相匹配的方案，保证在线教学平稳运行。要与课程平台密切配合、规范管理，强化对课程内容、教学过程和平台运行监管，采取安全有效手段，防范和制止有害信息传播，保障在线教学运行安全。
	2020.2.6	教育部应对新型冠状病毒感染肺炎疫情工作领导小组办公室	《关于疫情防控期间以信息化支持教育教学工作的通知》	强化网络安全保障。教育部加强对重要信息系统（网站）的网络安全监测通报，组织电信运营商和网络安全服务商为国家体系等重要信息系统（网站）提供重点保障。教育网网络中心应保障教育网安全稳定运行。各地各校要落实网络安全等级保护制度，加强网络安全管理和技术保障能力。重点加强个人信息保护，选用第三方平台和服务的应明确个人信息使用规则，不得借机超范围采集个人信息。
	2020.2.6	教育部高等教育司	《关于继续组织在线课程平台提供疫情防控期间支持高校开展在线教学的资源和服务方案的通知》	要求在线课程平台：须至少获得国家信息安全等级保护二级认证；要能够保证 24 小时运行，且运行安全稳定畅通，平台须配备专业人员进行课程审查、教学服务管理和安全保障，能够采取安全有效手段，防范和制止有害信息传播。
	2019.9.19	教育部等 11 部门	《关于促进在线教育健康发展的指导意见》	（九）建立规范化准入体系。按照包容审慎原则，完善在线教育准入制度，明确准入条件与资质认证流程，建立健全在线教育资源的备案审查制度，切实维护国家安全、社会公共利益和师生个人信息安全。

领域	时间	发布机构	文件名称	网络安全相关需求
在线教育	2019.7.12	教育部等 6 部门	《关于规范校外线上培训的实施意见》	要求校外线上培训应落实网络安全等级保护制度、网络安全预警通报制度和用户信息保护制度，具有完善的安全保护技术措施。做好培训对象信息和数据安全防护，防止泄露隐私，不得非法出售或者非法向他人提供培训对象信息。
	2019.8.15	教育部等 8 部门	《关于引导规范教育移动互联网应用有序健康发展的意见》	提出教育移动应用提供者应当落实网络安全主体责任，采取有效措施，防范应对网络攻击，保障系统的平稳、安全运行。教育移动应用和后台系统应当统一落实网络安全等级保护要求。
	2018.4.18	教育部	《教育信息化 2.0 行动计划》	要求全面提高教育系统网络安全防护能力，全面落实网络安全等级保护制度，深入开展网络安全监测预警，提高网络安全态势感知水平。重点保障数据和信息安全，强化隐私保护。
网络直播	2021.4.23	国家互联网信息办公室等 7 部门	《网络直播营销管理办法（试行）》	第六条 直播营销平台应当建立健全账号及直播营销功能注册注销、信息安全管理、营销行为规范、未成年人保护、消费者权益保护、个人信息保护、网络和数据安全管理等机制、措施。 第九条 直播营销平台应当加强直播间内链接、二维码等跳转服务的信息安全管理，防范信息安全风险。
	2016.11.4	国家互联网信息办公室	《互联网直播服务管理规定》	第十二条 互联网直播服务提供者应当保护互联网直播服务使用者身份信息和隐私，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

表 3 我国非接触新经济各领域网络安全标准

领 域	标准号	标准名称
在线办公	GB/T 35282–2017	《信息安全技术 电子政务移动办公系统安全技术规范》
	/	《网络安全标准实践指南—远程办公安全防护》
互联网医疗	GB/T 39725–2020	《信息安全技术 健康医疗数据安全指南》
配送机器人	GB/T 38244–2019	《机器人安全总则》
无人配送车	GB/T 38628–2020	《信息安全技术 汽车电子系统网络安全指南》
	GB/T 40861–2021	《汽车信息安全通用技术要求》
	GB/T 40857–2021	《汽车网关信息安全技术要求及试验方法》
	YD/T 3594–2019	《基于 LTE 的车联网通信安全技术要求》
	YD/T 3737–2020	《基于公众电信网的联网汽车安全技术要求》
	YD/T 3750–2020	《车联网无线通信安全技术指南》
	YD/T 3752–2020	《车联网信息服务平台安全防护技术要求》
在线教育	无	/
虚拟会展	无	/
电商 / 直播 / 自助收银	无	/

PART 4
非接触新经济安全治理策略

4.1 法规层面

4.1.1 加快法律法规建设

当前，非接触新经济通过新一代信息技术实现人与人、物与物的全面链接，给人们的生产生活带来了更高的智能水平和便利程度，但网络安全却成了往往被忽略的因素。安全并没有被视为技术创新的一个组成部分，这意味着技术的发展很可能很少或根本没有考虑到恶意威胁。这需要国家相关部门进一步加大对产品和服务的监管，将网络安全纳入产品和服务的硬性质控指标，保护用户合法权益。例如针对在线协同办公平台、在线教育技术平台、虚拟会展服务、以及无人配送车、配送机器人、自助收银台等产品和服务，应加强网络安全和数据安全相关法律法规的制定和落地，提升产品和服务提供商的安全风险意识和合规意识，切实保障用户权益。

4.1.2 提供更具可操作性的指南

在加快完善法律法规的同时，相关监管部门和标准化组织应为企业提供具体的、易于使用和清晰的网络安全指南、指引和实践手册，为企业提供实施安全和隐私措施的具体标准、方法和技术，指导企业落实和部署法规要求的管理和技术措施。监管部门、标准化组织可以和行业协会、公共研究机构、网络安全公司等机构进行合作，以更好地制定相应的网络安全指南。

4.2 组织层面

4.2.1 短期关键安全措施

在疫情发生后，许多组织需要快速改变业务运营方式和服务提供方式，缺乏充足的时间建立完备的网络安全管理和技术体系。针对这种情况，组织可重点关注以下几个方面，确保业务快速上线后的数据、服务和系统安全。

（1）确保在线平台的安全性

以非接触的方式提供服务需要依靠软件、应用程序、网站等渠道，组织应确保以安全的方式配置和维护其在线平台，平台上的重要数据和个人信息都应得到适当保护。这需要对网站进行定期安全测试，以识别任何潜在的安全漏洞，并进行定期审查，以确保网站得到正确维护和更新。

（2）保障云安全

采用基于云的补丁管理和基于云的防病毒平台可以为组织在在线场景中提供确保其 IT 基础设施得

到管理和保护的能力。但上云也带来了一定的风险，因此组织应在此过程中关注几下事项：

● 实施多因素身份验证，以确保基于云的帐户被攻击者劫持的风险较小。否则，账户的安全性依赖于密码设置的强弱，并可能遭到网络钓鱼攻击。多因素身份验证可以提供额外的保护层来帮助防止这种情况发生。

● 许多云服务都提供了内置的安全功能，但这些功能通常默认关闭。组织应确保订阅足够的网络安全服务，以保护云上业务的安全。

（3）检查远程访问设备

疫情期间，远程访问需求大大增加，组织部署了不同的方式来实现这个目的，包括安装或升级虚拟专用网络 (VPN)、安装远程桌面管理工具、启用远程桌面协议 (RDP) 等远程连接协议等。组织应检查远程访问设备的安全性，包括：

● 确保所有远程访问软件都安装了最新的补丁，并且持续更新远程访问软件。

● 对远程访问实施强密码，并在可能的情况下启用多因素身份验证。

● 检查远程访问设置以限制访问仅来自受信任位置。

● 确保启用监控和警报，以警告可疑的攻击或异常的可疑活动。

（4）加强移动设备管理

许多组织允许员工使用自己的个人设备开展远程工作，这导致存储在这些个人设备上的数据存在安全风险。组织可采用移动设备管理 (MDM) 解决方案，来实现：控制远程设备的访问；确保设备安装了最新的防病毒软件；确认设备是否安装了最新的软件补丁；判断设备是否加密；强制设备受 PIN 和 / 或密码保护；如果员工设备丢失或被盗，或者员工离职，则远程擦除设备中的企业数据。

（5）开展安全意识培训

虽然技术措施可以最大限度地降低各种威胁带来的风险，但人为因素也是需要不断管理的因素。如果员工没有意识到网络安全威胁，或者员工应该如何应对可疑的安全漏洞，那么发生安全事件的风险就会显著增加。组织应定期向员工提供网络安全意识教育，以确保他们能够识别并妥善处理面临的各种网络安全问题。这些培训活动的目的不是让每个员工都成为网络安全专家，而是提供对实际网络相关风险、对组织的影响以及他们的行为如何影响结果的基本了解。

4.2.2 长期安全保障措施

从长期来看，组织应建立完备的网络安全治理体系，保障线上业务的稳定安全运行。完备的网络安全治理体系包括三个方面，分别为组织机构人员管理、网络安全流程管理和网络安全技术防护措施。

● **组织机构人员管理：包括**领导层面的全面支持、网络安全责任落实、网络安全技能培训、网络安全意识培训、网络安全制度建立、第三方管理等。

● **网络安全流程管理：包括**风险评估流程、安全审计流程、事件响应流程、软件更新流程等。

● **技术防护措施：包括**网络安全、应用安全、终端安全、数据安全、安全管理中心等。

PART 5
安全技术解决方案

5.1 远程办公零信任解决方案

背景：

疫情期间，非接触企业服务和远程办公成为常态，在保障数据和资产安全的同时，基于零信任网络构建内外统一的一体化业务访问平台，打造一个基于零信任网络架构体系的远程办公环境至关重要：在远程办公人员、设备和业务系统之间构建一张虚拟的基于身份的逻辑边界；对访问业务数据资产的各类场景进行梳理，逐步构建一个一体化的零信任动态访问控制体系。随着行业数字化转型的深入，IT基础架构大量引入云计算、移动计算等新兴技术，内外网络物理边界日趋模糊。传统防护思维中，默认内网比外网安全，通过边界部署防火墙等设备，以达到安全保障的目标。在新技术冲击下，防御面急剧膨胀，内外部网络边界交错，边界防护节点难以有效定位。同时，攻击者的技术手段也在日益提升，特别典型的是 APT 组织，他们通常不会正面进攻，而是以钓鱼邮件，或者从防御薄弱的分支机构迂回等多种方式，绕过边界防护进入企业内部。在内网可信的思维指导下，内网安全防御能力普遍不足，一旦边界被突破，攻击者往往能在整个企业内部自由移动，最终达到攻击目的。

痛点：

随着企业的信息化程度、移动化程度不断提高，内部业务系统逐步成为组织的核心资产，随时随地处理内部业务系统的信息变得越来越普遍和重要。企业员工有职场内（公司场所）、职场外（远程）灵活办公的需求。职场内，以防止企业内部威胁为主；职场外，当员工因疫情或其他等原因需在家临时办公，或者长期出差在外，以及外部伙伴因业务合作需要访问企业内部系统，需要确保远程办公访问过程的安全，以减少企业内部系统被从职场外部入侵的风险。同时，如何在保障远程办公安全的同时兼顾效率，也成为一个越来越现实的问题和挑战。

从远程办公的业务需求上来看，主要有以下业务场景：

1）普通办公需求：主要需求是访问公司的OA、审批系统、知识管理系统，以及公司的邮件、即时通讯、视频会议系统等；

2）开发测试需求：主要需求是访问公司的测试环境、代码仓库、持续集成系统等；

3）运维需求：主要需求是能远程登陆运维管理平台、远程服务器登陆维护等。

职场内部，传统安全架构下内部系统完全暴露在企业职场办公网络，一旦员工办公终端设备被植入木马或者未知威胁的恶意代码，攻击者可以直接进行企业内网扫描和横向移动，快速掌握企业内网

的所有数字资产。职场外部，员工所处的网络环境安全无法保障，BYOD 的流行使得员工访问企业内部系统的终端设备不再安全可靠。而传统远程办公，多数企业是采用 VPN 的方案，但 VPN 方案已经越来越无法满足当前安全和效率需求， 并暴露出来一些先天的缺陷，主要体现在以下几个方面：

1）无法判断来源系统环境的安全性，存在以来源终端为跳板攻击企业内网的风险；

2）无法进行精细化、动态化的权限控制；

3）缺乏安全感知能力，只能基于网络流量进行审计；

4）扩展能力较差，无法应对大规模的突发远程办公需求。

方案描述：

零信任架构的核心思想是“从来不信任，始终在校验”。它默认不信任内外部任何人和行为，遵循“先认证用户和设备，后访问业务”的原则，以身份为中心进行访问控制。零信任的安全监控不仅限于准入的过程，在访问过程中也会持续进行监控，及时发现终端是否被入侵控制，用户是否存在异常威胁行为，并实施动态访问控制。这种将安全技术与应用、业务特性相结合，安全技术与安全运营相结合的理念，使得安全体系具备足够的安全弹性和自适应能力，有利于应对 APT 等主流攻击。

零信任安全架构针对远程办公应用场景，不再采用持续强化边界的思维，不区分职场内外网，针对核心业务和数据资产，梳理访问这些应用和资产的各种访问路径和场景，在人员、设备和应用之间构建一张虚拟的、基于身份的逻辑边界，针对各种场景构建一体化的零信任动态访问控制体系。主要包含以下四个优势：

1）构建更安全的远程办公网络

通过实施“从不信任并始终验证”，不同类型用户只能按照预先确定的信任级别，访问预先申请的内部业务应用，未预先申请的内部业务应用将无法被访问。通过零信任技术方案构建了一个可控的资源访问通道，通过身份动态认证牵引业务信任关系。

2）增强对企业内部业务应用和数据的保护

在实施“按需受控访问”的基础上，有效整合数据安全保护相关的传输加密、敏感数据识别、精细化访问控制等技术，保护应用资源、数据在网络中的传输和调用，并优先保护高价值和高敏感数据资产。

3）大面积减少攻击暴露面

用户通过访问认证之前，应用资源对用户是隐身的；即便在用户通过访问身份认证和应用授权后，用户也仅仅获得该授权应用的使用权，并未开放网络使用权。零信任技术方案从根本上降低了资产的暴露面减少被攻击到的概率。

4）降低安全管理成本和潜在建设成本

落地零信任技术方案终结了安全防护手段各自为政的现状，在零信任技术方案实施时，可以通过与现有的安全工具集成，提升一体化安全管理能力，并在远程场景下，减少了 VPN 的潜在建设成本，简化了运营模式，优化了安全管理成本。

通过零信任技术提供统一的业务安全访问通道，取消职场内部终端直连内部业务系统的网络策略，尽可能避免企业内部服务完全暴露在办公网络中的情况。所有的终端访问都需进行用户身份校验和终端 / 系统 / 应用的可信确认，并进行细粒度的权限访问校验，然后通过零信任网关访问具体的业务，这样能极大的减少企业内部资产被非授权访问的行为。

远程办公场景下正确的实施零信任方案后可以带来如下好处：

a）可快速扩容：零信任网关可以通过负载均衡

实现快速的横向扩展，来满足突发的远程办公需求；

b）安全控制能力强：零信任把安全架构延伸到用户终端上，有更强的控制和感知能力；

c）安全攻击面小：零信任远程办公方案中，唯一可被访问的只有零信任应用代理网关，所有内部资源全部被隐藏在网关后，即便资源存在 0day 也难以被攻击到；

d) 用户体验佳: 用户一旦完成认证后，整个使用过程对用户不会有打扰，权限维持一致性，有较好用户体验。

5.2 | 智慧医院解决方案

■ 智慧医院发展中的痛点

1）传统 IT 基础架构难以满足智慧医院业务发展需要

随着智慧医院以集成平台为核心进行建设，医院的数据中心也需要不断升级。现在部分医院信息化建设还在采用传统物理架构与虚拟化技术相结合的方式来构建数据中心，已经无法满足日益增长的业务需求。为了方便患者就医，提高服务质量、工作效率，以及患者满意度，同时加强患者及公众对医院的信任与支持，创建和维护和谐医患关系，需要进一步促进业务和信息资源的整合，提高信息资源的利用率，降低医院信息化总体运维成本，降低网络、服务器与存储系统等信息系统基础设施的管理复杂度，提高应用信息系统部署的时效性。

2）智慧医院面临的信息安全问题愈发突出

通过大数据、人工智能等新技术提升医疗系统的信息化、智能化程度，是当前新型医疗服务运作模式的发展趋势。但在医疗系统信息化水平快速提升的同时，信息安全问题也愈发突出和严重。

医疗行业由于行业的特殊性保存了大量的个人信息、财务信息和健康信息等多种敏感的数据，这些数据具有非常高的价值，受到黑色产业链的觊觎，一旦泄露容易引发严重的后果。

随着互联网 + 医疗的发展，越来越多的医院借助 WEB、APP、第三方医疗服务平台等形式，提供网上预约挂号、网上缴费、网上查询报告等多项线上医疗服务。更便利的是，第三方医疗服务平台还可同时为多家医院提供线上挂号预约、体检预约以及医生咨询等服务，线上医疗服务带来方便的同时也带来了新的漏洞风险和数据泄露风险。

2017 年以来，医疗行业已成为攻击者实施勒索的最主要目标，有 29% 的勒索软件的攻击目标是各类医疗相关机构。除勒索外，医疗业务资源被黑客滥用于挖矿，亦会破坏企业内部 IT 环境、数据中心的正常运行秩序以及关键应用的交付，同样使得业务连续性遭受极大安全威胁。勒索、挖矿已经成为影响医疗业务连续性的主要威胁。

3）医院 IT 人员运维压力大

随着智慧医院的持续推动，IT 系统已经成为智慧医疗的一个重要基石，一旦运维失败，医院正常运转就会出现混乱，轻则造成医患矛盾，重则耽搁最佳治疗时机，危及生命。因此，IT 运维的性质已经发生了巨大变化，绝不再是医院的“边缘”岗位，医院 IT 人员面临非常大的运维压力。

■ 智慧医院“安全之道”

基于智慧医院发展中的痛点，智慧医院应当打造安全、弹性、智能的基础架构，以超融合技术搭建基础架构平台，围绕网络安全、终端安全、数据

安全、应用安全打造安全稳定的智慧医院安全防御检测体系，采用 AI 及大数据技术建设集中安全管理、安全运营、态势感知的安全管理中心。

图 3　智慧医院网络安全防护基础架构

1）超融合构建智慧医院下一代数据中心

超融合系统是面向下一代数据中心的基础架构解决方案，全面集成虚拟化和分布式存储软件，是医疗行业部署云环境的最佳基础架构解决方案，也是部署云平台最简单和快捷的方式，是对以往医疗行业数据中心系统架构的全新升级。实现全数字化医疗的智慧医院，支撑医疗业务模式转型，超融合是必不可少的基础架构，可以为医疗行业的数据中心带来最优的效率、灵活性、规模、成本和数据保护。

2）全面解决智慧医院的安全问题

以等级保护2.0安全标准为安全建设指导方针，结合智慧医院运营中面临的实际安全问题，比如勒索病毒、医疗数据丢失等问题，建设以感知预警、动态防护、安全检测、应急响应为核心的主动安全体系，全面解决智慧医院面临的安全问题。

3）大数据技术打造智慧医院安全运营管理体系

大型三甲医院网络复杂，资产数量多，出现安全问题排查溯源困难，本方案中基于 AI 及大数据技术建设智慧医院安全管理中心，轻松解决智慧医院资产不明、风险不明、安全事件难溯源、安全事件难处理等问题。

■ **解决方案优势：**

1）更灵活的智慧医院数据中心

以超融合架构打造智慧医院数据中心，可实现计算和存储完全的资源整合、统一管理、调配和统一存储功能。智慧医疗新业务上线无需复杂冗长的设备采购流程，只需进行虚拟资源的分配即可实现新业务的快速上线，大幅度缩短了业务上线时间，使得智慧医疗的业务更加灵活。

2）更可靠的智慧医院数据中心

● 超融合架构通过负载均衡、弹性 IP、虚 IP 实现业务高可用

● 服务器虚拟化实现主机高可靠，主机宕机可漂移

● Ceph 分布式存储实现三副本，保障数据不丢失

● 主控选举制度保障平台的平稳运行

3）更安全的智慧医院

从持续监测、威胁发现、智能分析、机器学习等融合入手，通过端到端相互关联的威胁分析系统，协助用户从单一安全事件监控向整体安全态势感知转变，从被动安全事件处理向可持续性安全监测分析转变，从单台设备部署防护策略向整体联动的网络安全架构转变，帮助医院打造安全整体运营能力，建设更安全的智慧医院，保障智慧医疗业务运行无忧。

4）更简单的运维管理

超融合架构简单，大大降低医院基础架构复杂性，降低运维和管理的成本；同时，安全运营自动实现攻击链溯源，提供可视化大屏，客户能够全局观察整个系统的安全态势，让运维管理变得更加简单；提供工单运维处置，协助客户进行安全管理工作的绩效考核，从而达到对安全事件的闭环处置。

5.3 | 在线教育系统安全整体解决方案

在线教育风险来源：

1）互联网攻击风险：来源于黑客对内部服务器发起的攻击，如：DDoS 攻击、入侵攻击、系统篡改、利用漏洞发起的其他攻击。

2）运维风险：来源于公司内外部的运维审计人员的身份认证与操作等风险，如：身份安全风险、越权操作风险、高危操作风险等。

3）数据安全风险：来源于黑客所发起的对内部敏感数据资源的窃取，以及运维人员和第三方造成的明数据泄露。

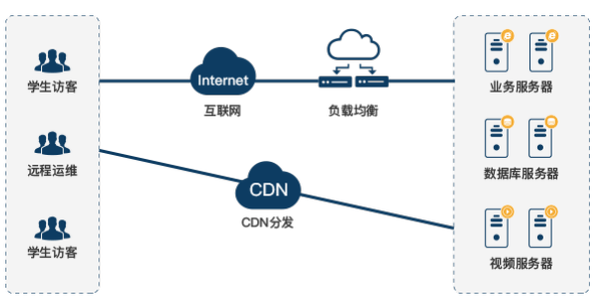

图 4 在线教育网络安全风险来源

在线教育安全整体解决方案：

1）云端安全监测与防护方案

事前使用云监测技术，无需部署任何软硬件，就可以对在线教育系统进行远程漏洞扫描与安全监测，再结合人工渗透测试服务，发现业务系统潜在的主机、WEB 和业务逻辑漏洞，同时通过云监测远程发现隐藏的后门和暗链等事件，确保系统能安全上线。

事中通过高防、云防护系统，用户端零部署零运维，只需将流量引流到云端防护系统，即可对访问流量进行实时检测与防护，保障系统不中断、页面不被黑、数据不被偷，并通过云监测技术实时对系统进行安全事件与可用性监测，发现暗链、黑页、断网等问题。

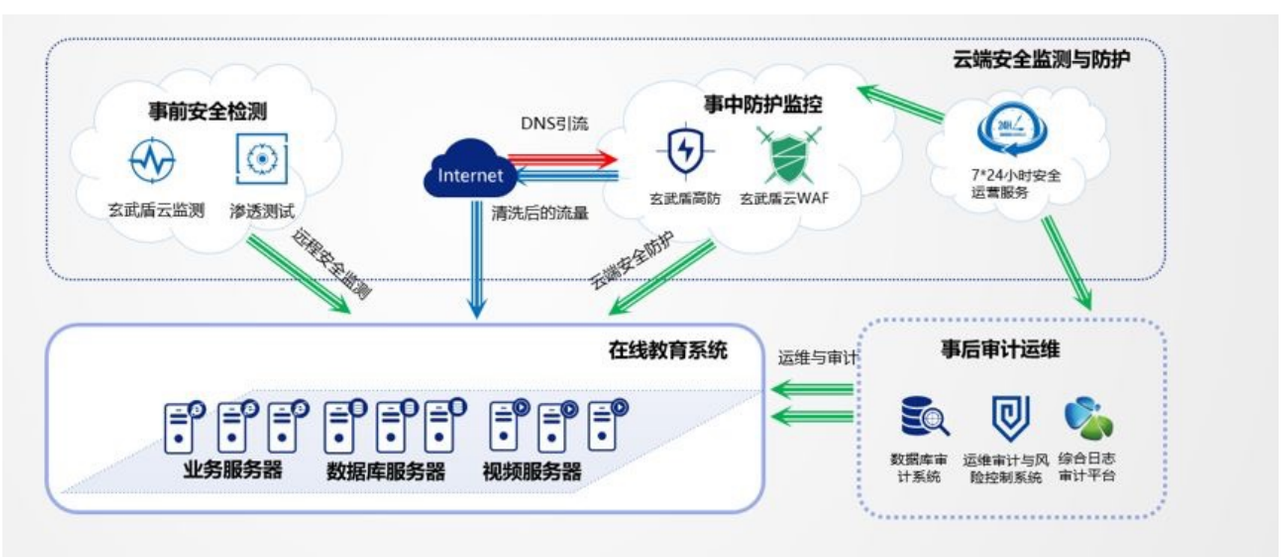

图 5 云端安全监测与防护方案

2）安全运维与审计方案

（1）远程运维系统时，先通过 VPN 登陆到运维审计与风险控制系统进行身份验证后，然后通过运维审计跳板机登陆到服务器进行远程运维，运维过程全程记录，保障运维安全。

（2）通过部署数据库审计系统针对数据库的访问流量进行流量审计，发现师生敏感数据泄露、越权操作等数据库安全风险。

（3）通过综合日志审计平台针对涉及的系统、网络设备、安全设备进行统一日志收集、分析和展示，以满足安全审计要求。

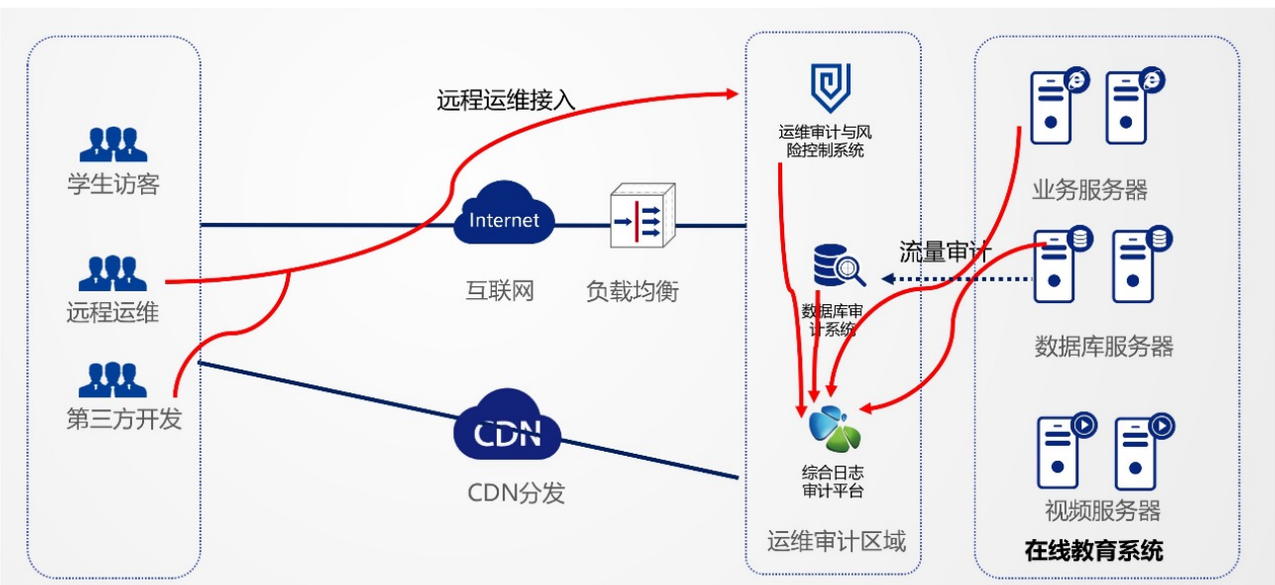

图 6 安全运维与审计方案

5.4 物联网安全解决方案

在非接触经济中，配送机器人、配送无人车、智能取餐柜、自主收银台等智能硬件都需要部署物联网安全解决方案，以实现这些场景的应用安全。

5.4.1 物联网安全感知与管理平台

物联网安全感知与管理平台基于安全传输、异常行为分析、可信身份、威胁分析、安全防护、数据防泄漏等技术，以可感知、可防御、可管控为终极目标，形成安全防护闭环管理，实现整网的安全感知，让安全管理更高效灵活。

图 7 物联网安全感知与管理平台

1）快速资产识别

通过终端自主上报和主被动扫描探测，精准发现和识别终端资产，生成物联网资产安全画像，实时管控全局资产。同时平台拥有自建打分模型，针对单个终端进行动态安全评分，帮助用户盘点全局，对资产做到心中有数。

2）安全隐患探查

从“隐患”视角出发，将原理性扫描和非原理性扫描相结合，事前探查并监测漏洞及弱口令的分布情况与趋势，将安全隐患扼杀在摇篮里。

3）安全事件发现

通过大数据安全分析、威胁建模、数据挖掘等技术实现威胁感知，及时发现非法外联、有害程序攻击、访问异常等威胁事件，真正做到少漏报，低延迟。

4）安全运营闭环

通过安全运营模块实现对隐患、告警弱口令人工精确验证，生成安全事件处置工单供决策建议，支持企业内部的工单协同处理及监管，提升高效管理。

5）定期报表输出

对于多而分散的物联网终端，除了要统一管理之外，定期的报告分析至关重要。平台可生成日报、周报、月报及自定义时间的资产安全报告，利于用户掌握当前资产情况，提供决策依据。

5.4.2 高交互、高仿真物联网蜜罐

1）物联网蜜罐价值

▲诱导攻击者攻击蜜罐，从而保护真实设备；

▲拖延攻击者攻击进程，从而获得采取防御措施的时间；

▲捕获攻击代码，从而促进物联网安全的分析研究；

▲捕获攻击者行为信息，从而对攻击者进行分析定位等。

2）高交互、高仿真物联网蜜罐的优势

用户部署蜜罐之后，能与黑客在网络安全的对抗中获得更大的主动权。高仿真、高交互物联网蜜罐则具备更多的优势来达到集中攻击火力、消耗攻击者精力、捕捉攻击痕迹、保护真实系统的目的。

高仿真的特点表现在它可以引诱攻击者攻击蜜罐，保护真实资产；高交互的特性则使它能诱导攻击者持续攻击，捕获更多攻击行为，并分析溯源得到高精准度的攻击者相关信息，轻松定位攻击者。

3）工作原理

贯彻迷网的易用性，高交互、高仿真物联网蜜罐只需“一键部署”，即可仿真物联网设备。接下来只需利用其高交互、高仿真的特性，静待攻击者“咬钩”。

无论攻击者利用何种攻击手法，都将一一被记录于迷网“攻击行为详情”页面中，安全研究人员用于分析当前攻击者攻击意图、攻击方法，进而进行防范，保护真实资产。

	高交物联网蜜罐	其他物联网蜜罐
仿真能力	仿真程度高 一比一还原整个系统	仿真程度低 基本只仿真登录页面
交互能力	交互能力高 支持登陆后对系统继续进行各种操作	交互能力低 仅支持登录操作
仿真数量	20 余种（高交互）	4 种（低交互）

图 8　物联网蜜罐功能对比

5.5 | 安全托管服务解决方案

安全托管服务（Managed Security Services，简称 MSS 服务）通常是指政企用户为达到降本增效或专注自身业务发展等需要，将部分或全部持续性、专业性较高的网络安全运营工作托付给第三方网络安全服务商，由其提供常态化的网络安全运营工作。

基于云化或远程技术的 MSS 服务通过云端安全运营平台为政企用户提供一系列超便利、高效率、低成本的网络安全服务，有机整合了专家化运营能力、标准化操作流程、智能化运营平台、场景化运营数据等资源，为用户提供常态化的覆盖资产管理、风险检测、威胁监测、事件处置等服务，与用户协同构建持续、主动、闭环的网络安全运营体系。

该解决方案可用于几乎所有的非接触线上场景，助力组织实现安全风险可控和安全能力提升。

MSS 服务体系

MSS 服务体系建设，以提供实战化、体系化、常态化的 MSS 服务为目标，通过多层级运营团队、标准化运营流程和专业运营支撑平台的建设，构建“人员 + 流程 + 平台”三位一体的 MSS 服务支撑体系，基于 IPDRR 框架的识别、防护、检测、响应、恢复五个阶段提供 MSS 服务，协助用户建设可持续的安全运营能力，持续改进和提高信息安全水平。

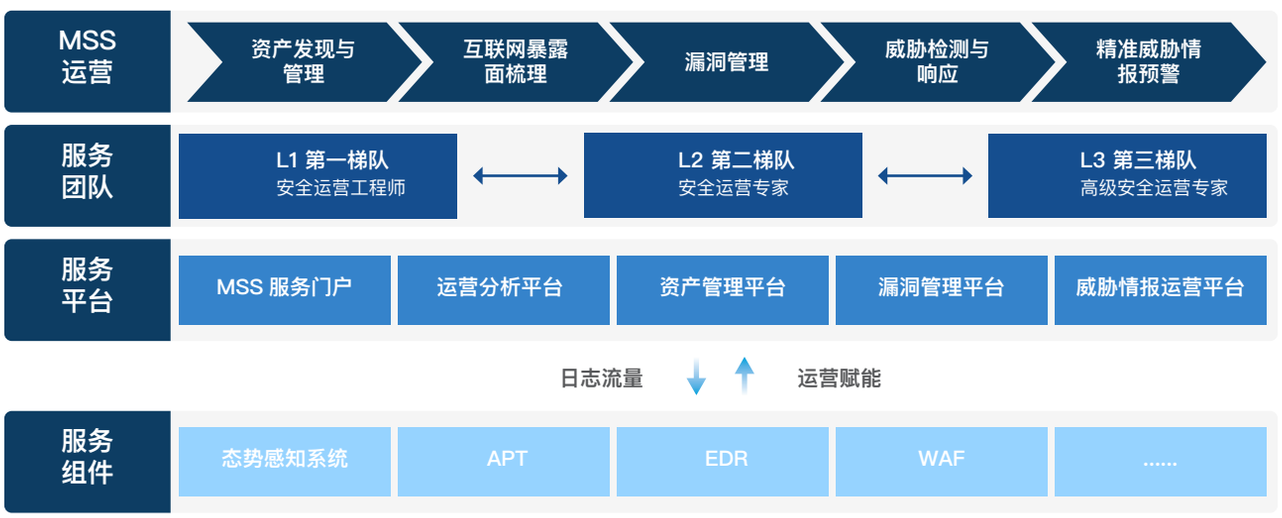

图 9 MSS 服务体系建设框架

1) 运营团队

运营团队是 MSS 服务体系的重要组成部分，需要设计合理的人员支撑架构，确保各个单元各司其职、高效输出，保障 MSS 服务的效率和质量。MSS 服务运营团队主要由第一梯队（L1）、第二梯队（L2）、第三梯队（L3）组成，L1 由安全运营工程师担任，主要负责日常安全运营工作，包括但不限于资产发现、资产梳理、漏洞扫描、安全监测、安全处置；L2 由安全运营专家组成，主要负责向 L1 提供技术支撑，包括但不限于威胁溯源、分析研判、应急响应；L3 由高级安全运营专家组成，主要负责安全研究与赋能，包括但不限于威胁研究、情报收集、威胁建模。

2) 运营流程

MSS 服务是一个多用户、多设备、多数据的复杂服务场景，需要一套统一化、标准化、高效化的运营流程，才能有效落地日常 MSS 服务运营机制。基于 MSS 服务内容，MSS 服务运营流程主要分为资产管理、暴露面管理、漏洞管理、威胁管理、情报运营五类流程，标准化的 MSS 服务运营流程，不仅规范了服务操作环节、步骤、工具和方法，还能提高 MSS 服务提供的工作效率，从而保证服务操作的一致性、服务交付的统一性和服务质量的稳定性。

3) 运营平台

服务的质量和效率不仅和服务的人员和流程有关，和服务工具也有着密不可分的关系。为满足 MSS 服务高效、稳定提供的需求，运营平台主要有服务组件和服务平台，服务组件部署在用户本地侧，为用户提供基础安全防护和威胁检测能力，包括态势感知、APT、EDR、WAF 等；服务平台部署在运营中心云端，用于 MSS 服务运营团队开展运营工作和服务结果交付，包括 MSS 服务门户、运营分析平台、资产管理平台、漏洞管理平台、威胁情报运营平台等。

MSS 服务内容

1）信息资产发现与管理服务

信息资产发现与管理服务，以建立完善信息资产管理体系为目标。一方面，协助建立和完善资产管理的规章制度，将安全管理责任落实到个人，督促资产管理规范化，提高资产安全管理水平；另一方面，协助梳理信息资产情况，对资产、业务系统、资产责任人进行关联，形成完整的资产信息台账，能清晰了解自身资产现状和资产分布。同时，通过周期性的资产稽查，监控资产的上线、变更、转移、下线等状态，及时更新信息资产台账。从而有效管控资产盲区，实现资产统一安全纳管和资产风险的可视、可管、可控。

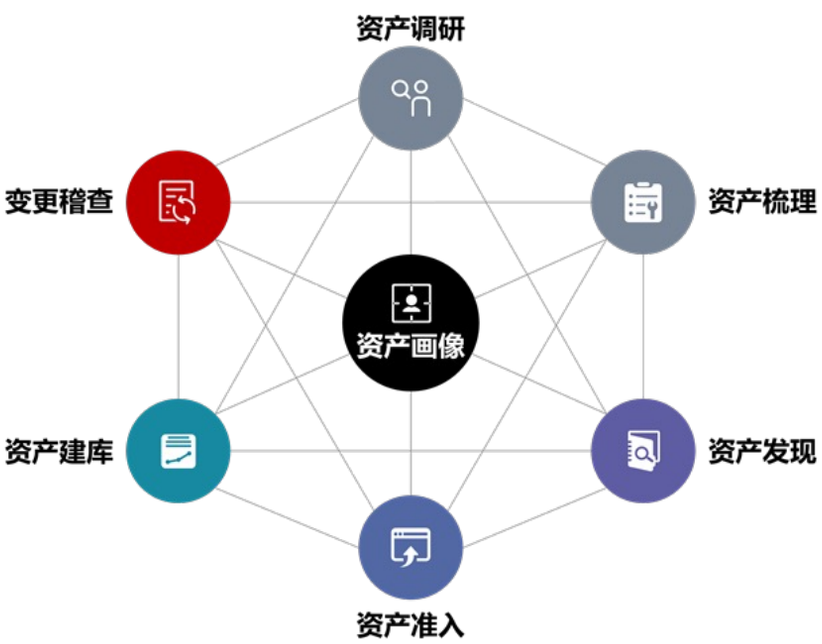

图 10　常态化资产运营管理

2）互联网暴露面梳理服务

基于攻击者视角，MSS 服务运营团队通过云端大数据平台对互联网暴露面进行稽查，与资产、漏洞关联梳理暴露面，基于“最大化收敛，最小化暴露”的原则进行暴露面收敛，减少风险的暴露面。周期性地开展互联网暴露面梳理，动态监控互联网暴露面变化，及时发现和收敛暴露面，降低网络攻击风险。

3）漏洞检测与管理服务

漏洞管理是一项持续性的工作，需要专业的人员和工具，开展漏洞从发现到处置闭环的全过程工作，才能构建覆盖漏洞全生命周期的管理体系，持续不断降低安全风险。漏洞管理服务从漏洞发现、漏洞分析、修复方案、漏洞处置四个阶段进行漏洞闭环管理，结合资产发现与管理服务，周期性开展漏洞管理工作，不断发现和修复系统、设备、应用中的漏洞，有效降低资产被攻陷的风险，实现漏洞的全生命周期闭环运营。

4）威胁检测与响应服务

由 MSS 服务运营团队通过云端运营分析平台，利用关联分析、用户和实体行为分析技术（UEBA）、威胁情报、威胁狩猎等技术，对安全日志、流量进行采集分析，及时发现安全威胁，并结合远端 / 本

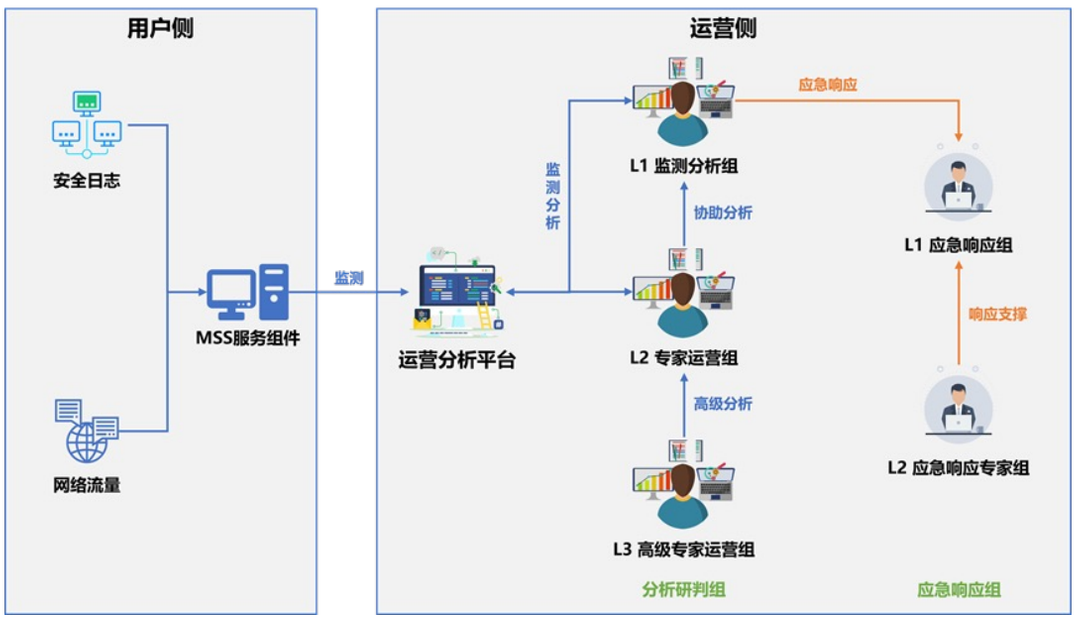

图 11 威胁检测与响应服务

5）精准威胁情报服务

提供威胁情报预警通知，MSS 服务运营团队对安全漏洞、安全事件等情报进行实时跟踪，并结合前期调研结果提供针对性的情报预警通知，包括漏洞和事件的介绍、影响范围、安全建议等情报内容，协助第一时间排查、发现和解除威胁；除此之外，还提供定制化情报推送服务，结合前期调研了解用户所在行业、关注情报类型等需求，通过威胁情报运营平台进行个性化威胁情报推送。

出品方

上海赛博网络安全产业创新研究院

杭州安恒信息技术股份有限公司