在线新经济系列报告

非接触新经济安全治理报告

GOVERNANCE OF
SECURITY ON TOUCHLESS 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

出品方：

上海赛博网络安全产业创新研究院

技术支持单位：

杭州安恒信息技术股份有限公司

编写组成员：

上海赛博网络安全产业创新研究院：惠志斌、鲁传颖、李宁、王新刚、唐巧盈、石英村、贺佳瀛；

杭州安恒信息技术股份有限公司：周俊、樊兴悦、王程程、罗剑东、夏先宁、毛润华、王辉、叶鹏。

COMPANY PROFILE | 公司简介

上海赛博网络安全产业创新研究院

上海赛博网络安全产业创新研究院是上海市经济和信息化委员会与上海市民政局指导下的民办非企业单位，由国内知名高校、研究机构和知名网信企业共同发起成立。赛博研究院面向全球数字化转型，专注数字经济、网络安全、数据治理、人工智能等领域的政策和产业研究，通过提供研究报告、决策咨询、产业规划、论坛会议、投资分析、数据服务等专业智库产品，助力政府和企业共建美好数字未来。

现已成功举办 2018/2019 世界人工智能安全高端对话、2019CIS 大会、网络安全产业创新论坛等重要活动；发布《人工智能时代的国家安全：风险与治理》《人工智能赋能网络空间安全：模式与实践》《人工智能时代数字内容治理的机遇与挑战》《全球网络安全企业竞争力研究报告》《全球网络安全产业投融资研究报告》《全球数据跨境流动政策与中国战略》《数据安全治理白皮书》《云平台安全责任与治理》等专业报告。

SICSI
CYBER RESEARCH INSTITUTE
赛 博 研 究 院

杭州安恒信息技术股份有限公司

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于 2007 年，科创板股票代码：688023。自成立以来一直专注于网络信息安全领域，公司秉承“助力安全中国、助推数字经济”的企业使命，以“诚信正直、成就客户，责任至上，开放创新，以人为本，共同成长”作为企业的价值观。

公司主营业务为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务。产品与服务涉及应用安全、大数据安全、云安全、物联网安全、工业控制安全及工业互联网安全、SaaS 云安全服务、智慧城市安全运营等领域，覆盖网络信息安全生命全周期的产品体系，能够为客户提供从安全规划、安全设计、安全建设到安全运营的一站式专业安全服务、重大保障服务、可信众测以及产学研用一体化人才培养服务。多次被评为全球网络安全创新 500 强，参与了众多国家与行业标准的制定，成为“2018 年度国家地方联合工程研究中心”依托单位。

安恒信息
DAS-security 安全中国

ABSTRACT | 内容摘要

2020 年新冠肺炎疫情全球爆发，习近平总书记指出，“越是面对复杂局面，越要善于化危为机，看到疫情对产业发展既是挑战也是机遇”。在新冠疫情全球蔓延、世界经济受到重大冲击的局面下，以非接触新经济为代表的新业态新模式逆势而起，在生产方式、消费模式、管理范式等多个方面塑造了数字经济发展的新范式，满足了生产生活升级需求和技术场景赋能产业转型，促进我国经济加速实现质量变革、效率变革、动力变革。

新冠疫情期间，非接触经济借助互联网、云计算、大数据、人工智能、5G 等信息技术，与现代生产制造、商务金融、文娱消费、教育健康和流通出行等深度融合，实现产业链条的更加高效、智能化运转，商业服务的更加便捷与广覆盖。远程办公、在线教育、远程医疗、非接触配送、无人工厂、在线金融、直播电商、在线会议、云旅游、云看展等在线智能交互的新业态新模式迸发出新的活力。

然而，随着非接触新经济的高速发展，网络空间与物理空间的深度融合，网络安全边界逐渐模糊，网络攻击面大大增加，网络安全事件频发，并在云基础设施、网络接入、终端、智能硬件以及数据传输和访问层面都存在一定的脆弱性，易被黑客攻击导致经济损失和数据泄露风险。可以看到，安全挑战成为非接触新经济发展关键掣肘。

在此背景下，本报告提出，应加快建立“法律法规监管 - 企业管理制度 - 技术保障措施”一体化的风险治理体系；并选取远程医疗、远程办公、在线教育、无人工厂等典型场景，在科学研判网络安全风险的基础上构建新的解决方案，护航和赋能非接触新经济安全健康发展。报告认为，在后疫情时代，非接触新经济发展浪潮带来了新的安全挑战和安全需求。一方面，新业态新模式将定义新的安全边界，数据安全和个人隐私保护将更受关注，终端安全与云安全需求将进一步增强。另一方面，这也为网络安全产业带来广阔的市场前景和市场机遇，驱动安全产品和服务模式转型。非接触式的远程安全服务将加快普及，面向企业的线上安全运营服务或将迎来重大发展。

CONTENTS | 目录

PART 1

非接触新经济加速产业业态变革

1.1 | 疫情催生非接触新经济异军突起

新冠疫情全球范围快速蔓延，全球经济遭受重创。三四月份，疫情在全球范围内爆发，各国企业被迫大规模停工停产，大批商店停业，生产端和消费端陷入停滞，导致全球经济遭受巨大损失，对全球范围内的资本市场、进出口贸易、产业供应链和跨国投资造成重大影响。据国际货币基金组织（IMF）最新发布的全球经济展望报告[1]显示，2020 年全球经济将出现 3% 的衰退，比金融危机期间更加糟糕。摩根大通预计到 2021 年底，全球产值损失将达到 5.5 万亿美元，相当于全球 GDP 的 8% 左右，仅发达经济体的损失就能与 2008-2009 年以及 1974-1975 年衰退时相提并论。另据联合国贸发会预测，疫情会降低 2020 年全球外商直接投资 5% 至 15%，世贸组织预测 2020 年全球贸易将缩水 13% 至 32%。我国国家统计局最新数据[2]显示，我国一季度 GDP 同比下降 6.8%。同时，疫情正在全球范围内对就业产生前所未有的深远影响，国际劳工组织估计全球近 27 亿就业者受到疫情防控措施的影响，超过 10 亿就业者面临减薪或失业的高风险。彼得森国际经济研究所预测数据显示，受疫情影响美国失业率或将一度升至 20% 以上。

相比传统线下经济遭受的重大损失，疫情倒逼“非接触新经济”异军突起。“非接触新经济”，即人与人、人与物之间不通过接触就可以实现各类生产生活需求的新型经济活动或模式，它借助互联网、云计算、大数据、人工智能、5G、VR/AR、物联网等信息技术，与现代生产制造、商务金融、文娱消费、教育健康和流通出行等深度融合，依托传统经济的全面线上化、数字化、智能化转型，实现产业链条的更加高效、智能化运转，商业服务的更加便捷与广覆盖，全面变革经济运转模式，极大提升经济柔韧性，是具有在线、智能、交互特征的新业态新模式。在国内疫情高峰期，民众虽居家不宜外出，但复工、复学、消费、娱乐等需求仍然旺盛，为满足用户特殊时期的特殊需求，各类企业顺势推出众多非接触式服务，满足了全民各种生活办公需求，如腾讯、阿里、今日头条等企业推出远程办公服务；京东、美团等电商外卖平台推出非接触配送服务；叮咚买菜、盒马鲜生等生活电商为用户提供生活保障；众多教育机构推出在线教育服务，全国各地组织开展“线上教学”；微医、平安医生及各地大型医院推出远程医疗、在线问诊服务。此外，传统行业纷纷推陈出新，云健身、云旅游、云看展、VR 看房等各类新型服务层出不穷，满足了疫情期间公众各类需求，也催生了新产品、新业态和新型经济模式。同样，国外在疫情高发期也大大促进了远程办公、远程医疗、远程教育等新业态新模式发展，Slack、Zoom、微软 Teams 等远程办公工具用户量大幅增加，谷歌课堂等在线教育平台用户量翻倍，在线点餐、网购等线上交易量快速增长，网络虚拟健身课程、网络虚拟体育赛事等新型娱乐模式不断涌现。

数据显示，疫情期间各类非接触经济形式获得长足发展。我国国家统计局 2020 年 1-2 月份数据显示，全国规模以上工业增加值同比下降 13.5%，而智能手表和智能手环则分别逆势增长 119.7% 和 45.15%；

服务业生产指数同比下降 13.0%，而信息传输、软件和信息技术服务业则实现增长 3.8%；社会消费品零售总额同比下降 20.5%，而实物商品网上零售额则同比增长 3.0%。这一系列对照数据表明，以数字经济、在线经济为代表的新动能在对冲不确定性方面展现出巨大的发展潜力。其中，生活电商领域，疫情期间盒马鲜生网上订单数量相较去年同期激增 220%；今年除夕叮咚买菜订单量月环比增长 300%，春节前后整体订单量增加约 80%；除夕至初四，每日优鲜实收交易额同比增长 321%，春节 7 天总销量突破 4000 万件。远程办公领域，腾讯会议自去年 12 月底发布后，40 天更新 14 个版本，8 天紧急扩容超过 10 万台云主机，投入的计算资源超 100 万核，截至 3 月 20 日，腾讯会议国际版已经在超过 100 个国家和地区上线，日活跃账户数超 1000 万；国外视频协作平台 Zoom，在三个月时间里活跃用户从 1000 万人增长到 2 亿人。远程医疗领域，平安好医生在疫情期间平台访问人次达 11.1 亿，APP 新注册用户量增长 10 倍，APP 新增用户日均问诊量是平时的 9 倍。VR 看房领域，贝壳研究院数据显示，春节假期期间，活跃用户数同比增长超 50%，VR 带看量同比增长约 7 倍；春节后两周内 VR 带看量共计 300 余万次，环比增长超 9 倍。

1.2 | 非接触新经济打造人、物、产业链条全社会链接

疫情期间“非接触”刚需催生的经济形态首先实现的是人与人之间的全面链接。例如企业员工之间、合作伙伴之间、医生与患者之间、商家与消费者之间、中介机构与客户之间、教师与学生之间，等等。非接触新经济使得疫情期间人们的生活消费需求仍被得到满足，人们的顺畅沟通没有被阻断，企业的业务开展没有被停滞。同时，非接触新经济更是开启了一个人们生产生活的新型广阔空间、学习交流的新型互动方式、商家开展业务的新型业务模式、以及产业经济运行的新型商业渠道，解决人们需求的同时，甚至收获了意想不到的更高水平的便捷度、高效率以及高收益。例如疫情期间火爆的直播卖货为线下商家在 2-3 个小时内就带来了以往线下经营几个月的客流量和收益。

非接触新经济促使“物的链接”更加深入地融入各类场景，实现更高水平的智能程度。非接触新经济的实现在众多场景中强烈依托机器人、无人车等智能硬件，例如服务于非接触式餐厅、非接触式酒店的智能机器人；服务于医疗机构的消毒机器人、手术机器人、送药机器人；服务于外卖、快速配送的配送机器人、无人车、无人机；服务于智能工厂的生产机器人；服务于仓储的货物分拣机器人；以及服务于智能楼宇的智能电梯；等等。物的智能升级依托物联网技术的快速发展，在特殊时期通过实现对人的替代，在非接触新经济中发挥了极其重要的作用，同时也降低了人力成本，提高了工作效率。

非接触新经济通过在产品生命周期以及产销各环节之间建立全链接，使得产业互联网时代加速到来。个性化定制、柔性生产是未来制造业的发展趋势，疫情倒逼生产各环节全链路线上化，产品设计、制造等各工序环节之间的协同更加紧密智能高效，消费者与生产端的距离被大幅缩短。例如疫情期间一些服装制造企业利用工业协作平台，将大量工序线上化，实现各类工种人员之间的对接，不仅解决了疫情期间人员无法复工导致生产停滞的问题，还降低了业务对接的时间成本。此外，通过传感器、边缘计算、智能制造等技术手段，掌握一个工位、一条产线乃至一个工厂的生产数据，可以实时了解疫情期间工厂的产能，为工厂、客户、供应商提供决策参考。由此看来，非接触新经济的爆发，是传统产业数字化转型的加速器，将推动产业互联网加速发展。

1.3 | 非接触新经济推动新一代信息技术创新应用全面提速

非接触新经济的本质是传统行业的线上化、网络化、数字化和智能化转型。疫情推动下，传统经济形态线上化迁移、非接触经济形态的瞬时大批涌现，造就了各个场景下的用户全链接，和众多服务的更加高效与智能。非接触新经济的本质是传统行业的在线化、网络化、数字化和智能化转型，这背后是云计算、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的快速发展与融合应用。依托信息技术的快速发展，在疫情倒逼下，“互联网经济”进入新一轮发展阶段，“互联网 +”在医疗、教育、消费、制造等传统领域的渗透进入更深层次。

非接触新经济带来的是新一代信息技术在各个垂直领域的加速落地应用。疫情期间，受益于远程办公、远程教育、远程医疗等线上新业务刚需，云计算、通信业、软件业等信息技术服务业

迎来加速发展。在云办公和 IDC 板块，金山办公、光环新网、数据港等企业的市值在 2 月初从最低点上涨约 50%。金山办公市值巅峰破千亿，成为第一批新纳入 MSCI 的科创板股票，浪潮的股价也在 3 月中旬创下新高，主要原因是其为云计算厂商提供服务器和配套部件。疫情驱动下非接触新经济的崛起，是应对不确定性突发事件的技术提速，带来的是各个传统领域的加速信息化和新一代信息技术在各个垂直领域的加速落地应用。

1.4 | 后疫情时代非接触新经济成为经济发展新力量

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。提质增效是传统产业的广泛需求，便捷智能是人们美好生活的普遍追求。随着新一代信息技术的高速发展，各行各业的数字化和智能化转型是大势所趋。非接触式的生产生活方式虽然是在疫情严峻形势下的不得已之举，疫情过后非接触的需求也会部分消失，但由此引爆的非接触在线新经济潜移默化中培养了用户的生活、办公、消费、就医等习惯，在线服务提供商在疫情期间高效完成了产品和服务推广和市场培育，线上服务的个人认知被迅速构建，人们的生产生活方式被迅速变革，对产业而言是重大发展机遇。后疫情时代，在线服务的需求将持续存在，受疫情推动得以迅猛发展的非接触新经济，将依托需求与政策的双轮驱动，与传统线下“接触经济”互补发展，满足人们的个性化和多样化需求，线上与线下的“双轨运营”模式将加速颠覆传统经济形态。

后疫情时代，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。此次疫情凸显我国医疗、制造、教育、商贸、物流等行业信息化、数字化严重不足，以传统产业为代表的旧动能在应对外生冲击时表现出明显的无能为力。例如受疫情影响，制造业被迫停工无法复产，严重影响生产进程，此时数字化水平高的无人工厂、智能车间则能不依赖工人复工，保持不间断生产。传统商贸更是如此，线下消费大幅锐减，数字化转型需求迫切。疫情期间，传统行业的数字化转型需求被全面激发，数字化进程被按下快进键，疫情过后，传统行业数字化转型将全面加速，同时推动非接触新经济在后疫情时代蓬勃发展。

后疫情时代，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。疫情催生的非接触新经济包含众多新兴产业、新业态和新模式，如远程办公、远程医疗、直播电商、云看展等等，是新一代信息技术集成创新的融合应用，是新技术与传统产业的深度融合，代表着数字经济的发展前景，是产业发展的新动能、新力量和新增长点，将加速我国经济供给侧结构性改革，推动我国经济转型升级和高质量发展。

PART 2

非接触新经济与生产生活加速融合

2.1 | 非接触式办公

我国在线办公市场空间广阔。根据《2018 中国智能移动办公行业趋势报告》，2017 年中国移动办公市场规模达 194 亿元，2012-2017 年复合增长率超过 25%，预计 2020 年市场规模有望达近 500 亿元。虽然国内远程办公市场刚刚起步，但市场需求旺盛。在远程办公市场中，视频通讯领域发展较为迅速，根据 Frost & Sullivan 发布的数据显示，2018 年我国视频会议市场规模约 156 亿，预计至 2022 年，我国视频会议市场规模将达到 446 亿元[3]。

新冠疫情催生在线办公新发展，行业巨头争相入场布局。国内互联网巨头先后布局远程办公市场，特别在今年疫情期间，企业微信、腾讯会议、阿里钉钉、华为云 WeLink、金山软件先后发布了远程办公指南，字节跳动旗下办公套件“飞书”也及时上线了“线上办公室功能”，提供远程办公配套服务。随着疫情在全球蔓延，国外各国众多企业也纷纷要求员工在家远程办公，苹果、谷歌、微软、Facebook 等大型科技企业先后开启居家办公模式。远程办公需求激增导致各大在线办公应用和平台用户量暴涨。截至 3 月 18 日微软的 Teams 聊天和会议应用共计拥有 4400 万用户，较 11 月报告的 2000 万日活跃用户增加一倍多；视频会议平台 Zoom 也因需求大大增加正在扩充服务器，并招聘新员工。

新冠疫情或将逐步培育远程办公习惯。远程办公概念并不陌生，很多大中型企业 OA 系统本身也有相应的远程办公功能模块，但是用户缺乏使用意识及系统培训等导致渗透率偏低；疫情冲击背景倒逼个人用户使用、企业客户统一培训，疫情所提供时间窗口期带来极佳的市场培育机会。同时腾讯、华为、金山办公等相关产品推出的一定时长免费举措可加速用户习惯培养，加速在线办公在国内市场的渗透。

疫情催生招聘活动向线上迁移。2 月 6 日，人社部发布《关于做好新型冠状病毒感染的肺炎疫情防控期间人力资源市场管理有关工作的通知》，要求暂停现场招聘会、跨地区劳务协作、人力资源培训等聚集性活动。同时，鼓励线下招聘转线上，借助“互联网 +”、云平台，通过视频、电话、邮件等开展远程笔试面试。各地也相继出台相关政策举措，加快推进线上招聘，一方面可解决因疫情和延迟复工造成的线下招聘暂停问题，另一方面也能通过线上招聘方式降低企业招聘成本，比如招聘场地租赁费、现场招聘物料准备、交通费等，线上招聘相对能更快速地满足企业的即时用工需求。截至 3 月底，智联招聘已经上线了 547 场空中双选会，其中已举办 231 场，10 万余家企业参与，共发布约 36 万个职位，超过 82 万人报名，投递简历 279 万人次。据智联招聘大数据，随着复工复产的推进，视频面试的使用量逐周增幅约为 123%。

2.2 | 非接触式医疗

我国在线医疗渗透率较低，行业前景广阔。据 Mob 研究院发布的《2019 互联网医疗行业洞察》显示，我国互联网医疗用户规模为 4500 万，同比增长 59.9%，渗透率为 6.6%；预计 2020 年用户规模达到 5900 万，渗透率达 7.9%。当下正处在线医疗行业快速增长阶段，疫情将使在线医疗产品的占据用户时长得到较大提升，群众对各种在线医疗产品的关注度和使用频率预期会创下新记录。根据 Frost & Sullivan 的数据显示，2018 年在线医疗行业中国市场规模达到 491 亿元，2020 年预计接近千亿，保守预测 2026 年达到 2000 亿元，远程医疗方面，2018 年我国远程医疗市场规模 130 亿元，未来五年复合增长率约为 27.63%，2022 年将达到 345 亿元。

疫情成为在线医疗大规模应用的“练兵场”，行业巨头市值飙升。疫情爆发以后，由于医疗资源分配、交通限制等问题，各地纷纷采取远程医疗的方式进行防疫会诊：贵州省人民医院与德江县民族中医院开启远程医疗会诊，判定患者感染情况及下一步诊疗方案；江苏多家医院开设“线上发热门诊”，为线下发热门诊分流，效果显著；河大附院启用远程医疗平台救治发热隔离患者；3 月中旬武汉雷神山医院、中国医师协会和清华大学组织武汉、北京、上海以及美国的呼吸科和危重症治疗方面的专家，为一位 64 岁的新冠肺炎重症患者举行远程会诊。此外，互联网医院线上问诊也成为缓解医疗资源紧缺，防止疫情扩散的重要工具。阿里健康、百度、微医、平安好医生以及各地省市级医院纷纷上线在线问诊服务。疫情期间，平安好医生平台累计访问人次达 11.1 亿次，App 新注册用户量增长 10 倍，App 新增用户日均问诊量是平时的 9 倍。春节期间，好大夫在线全平台每天的新增注册用户数，比 12 月增长了 350%；每天用户提交在线问诊的需求量，比去年 12 月日均增长了 648%。同时，疫情推动行业巨头市场表现强势。截至 2 月 14 日，行业龙头阿里健康、平安好医生，卫宁健康年初以来的涨幅分别达 55.11%，30.52%、46.46%，自 1 月以来阿里健康总市值在 30 个交易日内暴增约 600 亿港元，平安好医生总市值增长 168 亿港元，卫宁健康总市值增长 102 亿元。

在国外，随着疫情在全球爆发，远程医疗在患者初步筛查、咨询、救治等方面也正发挥重大作用，国际间远程会诊等医疗支援活动也借助远程医疗技术和手段大大提升了沟通效率。疫情成为远程医疗发展的重要转折点，远程医疗正在被重新认识和完善，产业将迎来快速发展期。

再迎政策利好，在线医疗有望获得快速发展。为贯彻落实党中央、国务院关于加强新型冠状病毒肺炎疫情防控工作的决策部署，在疫情防控工作中充分利用“互联网 + 医疗”的优势作用，为人民群众提供优质便捷的诊疗咨询服务，2 月 7 日国家卫健委就做好互联网诊疗咨询服务工作发布《通知》，强调要充分发挥互联网医疗服务优势，大力开展互联网诊疗服务，科学组织互联网诊疗咨询服务工作。稍早时候，2 月 4 日，国家卫健委发布《关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知》，要求充分发挥各省份远程医疗平台作用，鼓励包括省级定点救治医院在内的各大医院提供远程会诊、防治指导等服务；要求充分发挥互联网医院、互联网诊疗的独特优势，鼓励在线开展部分常见病、慢性病复诊及药品配送服务，降低其他患者线下就诊交叉感染风险。

2.3 | 非接触式教育

我国在线教育行业规模稳步增长。据中国互联网络信息中心第 44 次《中国互联网络发展状况统计报告》数据，截至 2019 年 6 月，我国在线教育用户规模达 2.32 亿，较 2018 年底增长约 3122 万，占网民整体的 27.20%。预计 2020 年我国在线教育用户规模将达到 3.05 亿人。在市场规模方面，iiMedia Research 数据[4]显示，2019 年中国在线教育市场规模突破 4000 亿元，较 2018 年增长 15.5%，受疫情影响，2020 年在线教育市场规模将达到 4538 亿元。

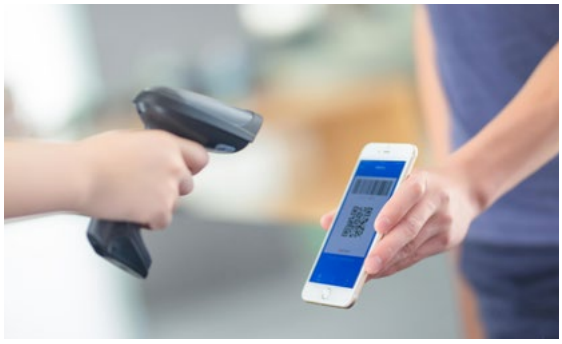
疫情成为在线教育行业发展的助推剂。疫情期间，在线教育需求爆发。为避免人群聚集，我国在教育部“停课不停学，停课不停教”的号召下，全国大中小学、课外机构都把课堂搬到了线上，大大加速国内在线教育的发展。疫情期间，包括新东方在线、学而思网校、猿辅导、作业帮、流利说等在内的多个在线教育平台，均推出了优惠及推广措施。此外，期间还有多家视频平台以“免费上课”的名号宣布入局。抖音、西瓜视频、今日头条等联合 50 家教育机构，邀请名校名师为全国中小学生提供免费上课服务；2 月份，优酷

的“在家上课计划”吸引了全国约 500 万学生参与；爱奇艺知识联合 40 余家教育机构发起“停课不停学”计划，推出各年级、各学科近 2000 场共计 80000 分钟的免费直播课。2020 年 2 月份，我国在线教育企业流量激增，用户活跃度大大提升，猿辅导的周活从 1 月份的 60 万猛增至近 400 万。在国外，随着疫情在全球蔓延，各国纷纷宣布学校停课，在校教育成为学生接受教育的主要方式，如美国各地大中小学停课后纷纷采用线上教学方式，通过谷歌教室、Zoom 等软件进行线上教学。从全球范围来看，所有受疫情影响的国家都成为在线教育的大型试验场。

2.4 | 非接触式金融

疫情促使支付行为转至线上。新冠疫情的传播方式促使人们在支付活动中倾向于选择在线支付。在国内，众多线下消费场景不接受现金，只接近移动扫码支付，为此，支付宝在上海开启“无接触式生活”，推出扫码付款、扫码缴税、扫码加油等业务。在澳洲墨尔本和悉尼，越来越多商店表示只接受信用卡或其他形式的电子支付。在澳洲的一个加油站，过去两周内，使用现金付款的比率已减少至约 15%，而使用触碰支付、Google Pay 和 Apple Pay 的人数逐增。香港八达通卡公司表示，今年 1 至 3 月的交易额比去年同期增长 30%，同一期间虚拟预付卡 O!ePay 和 Mastercard 的交易量也跃增约 60%。印尼电子钱包公司 Dana 则表示，疫情期间其线上交易额大幅增长 11%。

疫情加速在线金融各类新业态创新。疫情期间，各银行保险机构积极推广线上业务，强化网络银行、手机银行、小程序等电子渠道服务管理和保障，优化丰富“非接触式服务”渠道。2 月 18 日起，工行、农行在内的 30 家金融机构将近百支爆款存款、基金产品等搬上了支付宝“理财周”，用户打开支付宝就能在线选择。同期各大公司的明星基金经理、理财大咖们还推出一系列



在线直播与互动。自 2 月 4 日后，支付宝上基金申购交易日均增长 400% 左右。目前支付宝已经与超过 300 家基金、银行、证券等金融机构展开合作，除了接入存款、养老险、银行理财等全资管品类外，还搭建丰富的服务场景，用户在理财的任何阶段都能够获得专业机构、理财专家、社区内容等提供的针对性服务。浦发银行则通过“官网便捷服务通道 + 快递必要材料”的申请模式，在业内率先实现工资代发业务全线上办理，并支持在线提交批量开户申请，免去收集纸质材料的困扰。上海银行以“在线小微快贷”“在线电子票据融资”“在线开立保函”“上行 e 链在线供应链融资”“在线账户管理”等一系列在线服务，保障防疫安全、提升服务效率。疫情加速金融行业全面数字化转型升级，将大大促进金融科技产业快速发展。

2.5 | 非接触式生产

无人智能工厂可大大缓解疫情期间复工延迟对生产活动造成的影响。受复工延迟影响，疫情期间劳动密集型生产企业受到重大冲击，而基于人工智能、大数据、物联网、云计算等技术支持下的智能化工厂则受冲击相对小很多。例如，在上海宝钢，200 米长的生产线上只需 2 名工人流动检视，个位数的员工通过远程操控系统可控制 12 个智能机器人完成所有“危脏难”工作，无人值守的吊机每天可完成 10 万吨的成品钢卷的调运。新凤鸣集团通过提升产线智能化水平，采用 800 台机器人代替了原本严重依赖人工的生产环节，不仅提高了生产效率，也大幅降低了人员短缺对产能的影响。山东翼

菲自动化公司以高速并联机器人为核心，结合传送带跟踪及视觉识别技术，实现了口罩自动化高效包装，单套系统可替代工人 4-6 人，生产效率提高一倍以上。

疫情将加速传统制造业数字化转型。疫情期间，无人工厂与智能化工厂的优势凸显，也显示出传统制造行业的应急生产能力严重不足。疫情将促使制造行业更清晰地认识到产业数字化、智能化带来的好处，加速生产制造流程的数字化转型升级，数字化转型将成为企业应对外部不确定

性的关键策略。伴随着人工智能、大数据、物联网、5G 等新兴信息技术的发展与应用，后疫情时代，无人工厂、智能工厂的普及程度有望获得较大提升。

2.6 | 非接触式配送

疫情催生外卖自提新模式，智能快递柜行业迎来新机遇。疫情爆发起来，京东、美团、阿里蜂巢、饿了么等电商、外卖平台纷纷推出非接触配送服务，减少人员接触带来的交叉感染风险。美团外卖在此前率先推出“无接触配送“的基础上，与各地政府部门先行先试，在全国分批投放 1000 台外卖智能取餐柜。首批外卖智能取餐柜目前已在上海、北京、广州部分核心写字楼、社区卫生中心、医院落地试运营。位于上海的悠饭是一家团餐供应链平台，在疫情爆发前，悠饭在上海共投放了 110 个保温柜，而在企业开始大规模复工 1 个月内，他们收到的合作需求明显增多，目前已根据市场需求新投放 50 个保温柜，3 月还要增加 40 个。顺丰旗下丰巢柜支持快递员免费派件，鼓励快递自助收寄，通过丰巢柜进行物品交接，减少人员接触带来的风险。随着国务院办公厅一号文明确指出“明确智能快件箱、快递末端综合服务场所的公共属性，为专业化、公共化、平台化、集约化的快递末端网点提供用地保障等配套政策”，之前受困于盈利模式不清晰而导致行业发展困难的智能快递柜行业有望迎来新发展。

疫情或推动无人配送模式大规模落地应用。配送机器人、配送无人机等并非新物种，但鉴于技术、成本、基础配套等服务，尚未大规模应用落地。疫情期间，为避免人群聚集和过密接触，配送机器人、配送无人机等迎来一展身手的机会。杭州市第一人民医院使用机器人从病毒洁净区承载餐食或物资出发，自动前往各个隔离区房间进行配送，通过机器人自动化免接触配送的方式，阻断“人传人”的病毒传染链条。北京创新企业九号机器人自主研发的Segway配送机器人S2，可实现自主导航、越过闸机、自主坐电梯、绕开动态障碍物，将餐食及时从办公楼的负一层送达楼上指定地点后，再通过电话、短信的方式通知用户取餐，用户可扫描机器人屏幕上的二维码完成身份验证与开箱，全程做到零接触取餐。在疫情防控期间，迅蚁送吧公司以无人机 RA3 和 TR7S 以及无人站 RH1 作为飞行运输方案，解决了新昌县人民医院与新昌县疾控中心之间的检验检疫物资的运送。相较普通道路运输，无人机的飞行时效能够提升百分之五十左右，为疫情防控提供了高效的运输手段。美国新冠疫情爆发后，对非接触式配送服务的需求增加，谷歌母公司Alphabet旗下Wing公司使用其Wing无人机运送食物和药品，在 3 月底疫情爆发期的两周内已完成了超过 1000 次送货服务。据悉亚马逊、UPS 和许多规模较小的公司也在测试无人机配送模式。

2.7 | 非接触式消费

疫情大大提升网购普及度，加速直播电商发展。新冠疫情导致线下消费大幅降低，线上电商渗透率大大增加，生鲜电商、小程序和社区团购在这场疫情下，解决了居民的菜篮子、米袋子、盐罐子等基本生活需求，其用户群已经从 80、90 年龄段的主流群体延伸到 60、70 后。京东大数据研究院 1 月 30 日公布的数据显示：2020 年春节期间，居家消费全面增长，其中母婴类下单金额增长 164%，家纺、家庭清洁、家居日用等品类增长 110%，食品饮料、酒、生鲜类增长达 106%。部分一直在困境中挣扎的生鲜电商在春节期间打了个翻身仗，如盒马鲜生、每日优鲜、叮咚买菜、美团买菜等均出现蔬菜肉类供不应求或配送延迟的情况。同时，疫情大大加快了直播电商的发展，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。数据显示，今年 2 月以来，新入驻电商及直播平台的主播较 1 月同期增长了 10 倍。

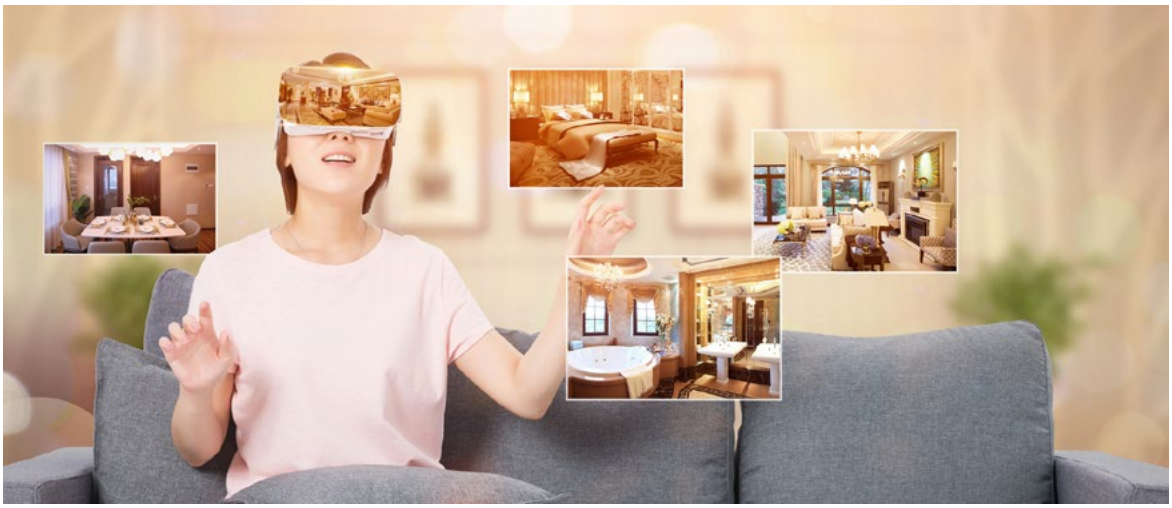
疫情催生“云健身”新模式。疫情期间，网络直播、社交平台成为居家隔离的健身爱好者的“发声器”，阳台马拉松、客厅广场舞、居家体育课等创意不断，“云健身”的旺盛需求，推动越来越多的健身爱好者加入，线上运动逐渐成为一种新时尚。许多健身机构也相继在线上推出直

播合集、直播授课、居家防疫健身指南等多种服务，收获了可观的流量。B 站数据显示，疫情期间 B 站健身运动视频累计播放量达 6.6 亿次，较去年同期增长近 200%，用户总观看时长同比增长了 164%，健身运动 UP 主新增粉丝总数同比增长超 240%。小红书平台数据显示，疫情爆发后，健身内容笔记发布量增加 2.01 倍，其中健身视频播放量上涨 2.09 倍。2020 年 2 月，运动健身 APP 行业活跃用户规模快速上涨至 8928 万，同比增长了 93.3%，健康管理 APP 月活用户突破 2405 万，同比增长 152.8%。

疫情加速“VR 看房”新业态发展。受疫情影响，人员流动停滞、多数居民小区封闭化管理、售楼处关停，严重依赖线下销售网络的房地产行业也转战线上，纷纷通过自建或与线上直播平台合作，搭建“云售楼处”，依托互联网与 VR 等新兴信息技术，推出 VR 在线带看服务，大量线下销售人员化身网络“主播”，房地产业诞生“线上售房”新模式。疫情期间，覆盖客户群体广、跨越时间与空间、节约成本、内容丰富、展现形式多样的“线上售房”战绩不俗，例如，恒大得益于在全国范围的线上布局和全民热议的“75”折等优惠活动，实现了网上认购总套数 99141 套，实现 2 月单月全口径销售金额 470 亿元。

疫情期间“云旅游”异军突起。数字文旅消费在疫情期间异军突起、逆势上扬，已成为新的热点和趋势。云赏樱、云看展、云看动物、云踏青等新的文旅方式，既让消费者足不出户感受春意，也为旅游商家回暖复苏积蓄力量。截至 3 月 8 日，国内已有至少 20 个城市、1000 多家景区开通线上游览服务。2 月以来，阿里巴巴旗下旅游平台飞猪已连续推出约 7500 场直播，观看人次超 3000 万，直播内容覆盖全球 30 多个国家和地区。3 月 1 日，布达拉宫进行了史上首次直播，还在直播中展示了以往不开放的金顶群以及馆藏经书，直播开通仅一小时，观看的网友数就达到了 92 万，相当于以往近一年的游客量。

疫情激发“无人超市”活力。受疫情影响，无接触操作、24 小时不间断服务的无人超市再度走入人们视野。2 月 2 日，在火神山医院正式交付使用之际，一家特殊的疫区 24 小时无人超市也正式营业。火神山医院内启用的无人超市没有店员、没有收银员，买完东西扫码即走。自助收银后也不会产生小票，最大可能地减少人与人之间的接触，并且实现了 24 小时不间断服务，营业首日，超市就接待了 200 多位客人。



2.8 | 非接触式会展

疫情推动各类峰会论坛活动转至线上，开启在线会议新模式。受疫情影响，原定于 2020 年度 2-4 月份的会展、会议纷纷取消或延期。鉴于全球疫情防控的不确定性，诸多国际会议转至线上。深度学习领域顶级会议——国际表征学习大会（ICLR）日前宣布，原定于 4 月 25 日至 4 月 30 日举行的学术会议 ICLR2020 将取消线下实体会议，改为完全虚拟会议。ICLR 认为，这一不幸事件将使其有机会创新远程会议的有效举办方式。2 月 13 日，小米 10 系列新品发布会采用纯线上形式举办。3 月 12 日，世界经济论坛“人工智能在金融服务领域的未来”会议以网络研讨会形式在线上召开。3 月 26 日，G20 领导人应对新冠肺炎特别峰会也首次以远程视频方式在线举行。此外，2020 年度的国际万维网大会要求与会人员采取远程报告的方式参加大会；原定于 3 月 7 日在墨西哥坎昆举行的 ICANN 公开会议也将通过远程参与的方式进行。线上会议形式或将开启会议论坛活动新模式。

“云演出”突破空间限制，覆盖广泛人群，成为娱乐业探索新渠道的一次尝试。传统的线下演出，通常为了能够尽可能的覆盖粉丝群，表演者需要在较长的时间范围内举办多场演出，例如很多明星均会举办巡回演唱会。但这种方式受限于场地大小、运营成本等因素仍然无法满足需求。基于互联网技术的“云演出”，不仅可以解决空间受限、覆盖面不足等问题，更可以降低运营和获客成本。此次疫情期间，各大卫视纷纷采用互联网连线直播方式录制节目，网络平台也纷纷跟进，推出“云演出”、“云相声”。突破空间限制的“云演出”，或将成为娱乐业发展的新渠道。

PART 3

安全挑战成非接触新经济发展关键掣肘

3.1 | 非接触新经济领域网络安全事件频发

网络安全风险成为新冠疫情爆发期间另一重大挑战，严重影响疫情防控工作和民众正常的生产生活。新冠疫情期间，全球范围内网络攻击事件频发，尤其针对中国、日本、意大利等疫情重灾区，黑客利用疫情热点信息作为诱饵发起大规模的网络钓鱼攻击，对网络用户的信息及资产安全构成重大威胁。同时，疫情催生的远程医疗、远程教育、远程办公等非接触在线经济，在成为人们办公、学习、娱乐、就医的重要方式后，由于自身安全防护不到位等原因，遭到了众多网络攻击及信息泄露事件。

疫情期间，互联网医疗行业成为网络攻击的重点领域。疫情期间医疗机构遭到大量网络钓鱼攻击，严重威胁医疗信息系统的安全，还影响了某些国家的疫情防治工作。例如，3 月中旬捷克共和国布尔诺大学医院遭到网络攻击，导致所有手术被迫取消，医院还被迫关闭了整个 IT 网络，作为捷克新冠病毒测试的核心医院之一，网络攻击使得疫情防治工作受到影响。3 月 20 日，美国卫生和公共服务部也遭受了严重的网络攻击，不得不暂停服务数个小时。此外，医疗服务认证暴力破解攻击态势持续严峻，数据显示，黑客曾对我国医疗行业的暴力破解攻击达到了单日 80 万次的高峰[5]。同时，医疗 APP 等应用程序存在大量的网络安全漏洞，攻击者可利用这些漏洞进行 App 仿冒、植入恶意程序、窃取用户敏感信息、攻击服务等，对远程医疗服务构成严重安全威胁。

远程办公同样成为黑客攻击的重要目标之一。例如，疫情期间，英国大量公众选择在家远程办公，使得全国网络需求大幅增加，而相应的网络安全保障工作没有跟上，导致了大规模断网事件。这不仅影响了疫情防控工作，也加剧了公众的恐慌情绪。我国某互联网公司也在疫情期间发生网络安全事件，该公司一位业务主管分享到内部工作群的远程办公工具及电子表格文件被发现感染病毒，导致部门 200 多名员工电脑被感染，该公司系统业务安全受到威胁。此外，疫情期间在全球用户量暴增的视频会议软件 Zoom 被曝存在重大安全漏洞，导致数以万计的私人视频被上传

至公开网页，严重威胁用户数据安全。Zoom 的安全问题并非孤例，多家远程办公类软件均曾被曝发现零日漏洞或被黑客入侵、摄像头劫持等。

疫情期间，在线教育遭到众多网络犯罪和恶意行为攻击。疫情导致全球多个国家的学校无法正常开课，在线课堂成为学校授课的替代方式，但由于在线教育平台安全性不足，导致发生多起网络攻击恶意行为。例如，当地时间 3 月 31 日，美国 FBI 波士顿办公室发布的一则通告称，3 月底，在一所马萨诸塞州高中的 Zoom 网课上，有身份不明的网友进入了网络教室并大声骂脏话，甚至喊出这节课主持老师的家庭住址。另一所该州的学校也报告了网络课堂遭不明身份的人“闯入”的事件，此人还在摄像头前展示了纳粹标志的纹身。前 FBI 探员表示，网络犯罪正在持续攻击像 Zoom 这样的平台，尤其是在新冠肺炎疫情期间，一般来说，犯罪分子会创建一些冒充 Zoom 的域名，达到偷窃个人信息的目的。

3.2 | 非接触新经济面临多重网络安全挑战

非接触新经济依赖人工智能、大数据、云计算、物联网、VR/AR 等多种信息技术的融合应用，其在云基础设施、网络接入、终端、智能硬件以及数据传输和访问层面都存在一定的脆弱性，易被黑客攻击导致经济损失和数据泄露风险。

（1）云基础设施安全

非接触在线新经济的背后是包括网络、存储、软硬件等要素在内的信息通信技术，无论是远程办公、远程教育、远程医疗还是无人工厂，都离不开上游作为基础计算资源的云计算服务的支撑。疫情期间下游各类“云经济”的爆发，也带动云计算行业的需求激增，包括上游 IDC 与服务器行业。例如，由于在线办公需求暴涨，从 2020 年 1 月 29 日开始到 2 月 6 日，腾讯会议每天都在进行资源扩容，日均扩容云主机接近 1.5 万台，8 天总共扩容超过 10 万台云主机，共涉及超百万核的计算资源投入。阿里云也在 2 月初紧急扩充 1 万台云服务器，以确保视频会议、群组直播、办公协作等功能的稳定运行。

云基础设施需求倍增的同时，其网络安全防护水平成为非接触新经济应对网络安全挑战的重要一环。由于云平台接入了大量网络应用和企业服务，一旦出现故障，影响范围甚广，会导致众多网站无法访问、手机 APP 不能使用，严重影响各行各业的在线系统运行。当前，云基础设施的安全性已有一定保障，但仍存在不少挑战。在云计算的复杂生态环境下，暴露的攻击面和攻击路径远远多于传统的网络环境部署。云服务提供商不仅掌握着物理机、内存、CPU 等硬件和底层固件、母机 OS 等资源，还管理着虚拟主机、云储存、虚拟网络等资源，提供各类云服务。因此，云基础设施除面临传统的漏洞管理、权限控制等方面的安全威胁，还面临虚拟化存储、虚拟化网络、虚拟化管理等方面的虚拟化安全威胁。攻击者可通过裸金属服务器管理接口、租户虚拟机逃逸、独立租户 VPC 实例模式的容器和微服务网络攻击、SaaS 服务共享集群模式攻击等多种攻击路径实现对云平台的底层资源、管理软件、管理界面、服务器集群等的网络攻击[6]。

（2）网络接入安全

远程办公、远程教育、远程医疗、无人工厂、无接触配送等非接触在线经济场景中存在大量远程接入内网需求，如大量员工需远程接入企业内网开展远程办公、工厂大量工业设备需接入内网进行生产活动、无接触配送需要送货机器人、送餐机器人、无人机、无人车等智能设施接入控制平台。在终端、设备网络接入需求倍增的同时，也带来了广泛的安全风险。如在远程办公场景中，若缺乏足够的身份认证、访问控制、安全监测、安全审计等安全防护手段，则存在账户被盗、身份冒用、越权操作等各类安全风险，黑客可能会冒用身份侵入内部系统，内部员工也存在越权操作的潜在风险。

（3）数据安全与隐私保护

非接触新经济通过线上的模式完成线下的各类需求，必然涉及大量的数据传输、存储、访问等需求，这些数据涉及企业重要数据、个人隐私等各类数据，一旦被窃取造成数据泄露或数据丢失，将对企业及用户产生不可估量的损失。例如在远程办公场景中，涉及大量商业合同、财务数据、研发数据等企业重要数据的在线传输，也可能通过视频会议的形式沟通企业重要事项、展示企业重要数据，同时也会通过远程接入的方式访问企业内网数据库，这些场景都对数据安全防护提出极高要求。此外，在远程医疗场景中，涉及大量患者病历数据、检测数据等敏感数据，在无人工厂场景中，涉及大量工业生产数据、工艺参数等重要数据，若无充足的安全防护手段，都存在被非法窃取、泄露、公开、共享的高危风险，危及企业利益和用户个人隐私。

（4）终端安全

终端设备的安全水平是非接触在线新经济应对安全挑战的重要一环。在远程办公、远程医疗、无人工厂等具体场景中，都存在大量暴露在互联网环境中的计算机终端或移动终端，面临被黑客攻击的安全风险。例如在远程办公场景中，大量员工个人持有的终端设备需接入企业内网，但由于远程接入的个人终端暴露在互联网上，很容易成为黑客攻击的目标。个人终端可能因未安装或及时更新安全防护软件，未启用适当的安全策略，被植入恶意软件、感染木马病毒，传播至企业内部，甚至成为攻击企业网络的突破口。因此，对外部访问设备做好安全检测，保障接入设备的安全至关重要。

（5）智能硬件安全

非接触经济的实现在大量场景中需要利用智能硬件设备，例如无人工厂中的工业机器人、仓储机器人；非接触配送中用到的智能取货柜、保温外卖柜、配送无人车、无人机等；医疗领域使用的手术机器人、消杀机器人、康复机器人等。这些智能硬件设备也是关键的风险点，存在着严峻的网络安全风险。例如当前工业领域使用的工业机器人的网络安全防护能力普遍较为脆弱，存在重大安全隐患，包括存在通信不安全、欠缺身份认证和授权、使用开源软件、默认设置和软件更新不及时等问题。网络安全公司 IOActive 2017 年曾对市面上十多款来自多家知名制造商的智能机器人进行安全测试，安全人员最终从这些机器人中发现了 50 多个漏洞，攻击者可借此通过机器人的麦克风和摄像头实施监控，窃取数据，甚至造成严重的物理伤害。具体而言，恶意攻击者可利用远程命令执行漏洞修改机器人的默认操作，禁用管理功能，监控视频 / 音频，并将此类数据发送至命令与控制服务器。攻击者同样可利用该漏洞提权，修改 SSH 设置，修改根密码禁用远程访问，并破坏工厂重置机制防止用户恢复系统或隔离勒索软件。

3.3 | 非接触新经济安全治理策略

综上所述，随着非接触新经济推动网络空间与物理空间加速融合，以及数字、智能技术的不断发展与普及应用，网络攻击面和安全风险日益扩大，网络安全形势愈发严峻，安全挑战已成为非接触新经济蓬勃发展的重要限制因素，若不能得到有效治理，将严重阻碍非接触新经济的创新发展。因此，针对非接触新经济的网络安全风险治理具有极强的紧迫性和必要性。综合来看，需借助由法律、管理和技术三重治理手段构成的保障体系加以有效应对。

图 1 非接触新经济安全治理策略

3.3.1 | 法律法规监管

疫情期间针对各类信息服务的网络安全事件频发，引起国内外监管机构高度重视。我国工信部发布《工业和信息化部办公厅关于做好疫情防控期间信息通信行业网络安全保障工作的通知》，要求做好医疗救助、远程办公、教育教学和人民群众生产生活的网络安全保障工作，加强数字基础设施安全防护和网络安全威胁监测处置。教育部、卫健委、民政部等主管部门在各领域信息化建设和信息服务发展促进文件中，均明确要求强化网络安全保障和个人信息保护，同时加强信息服务平台网络安全认证工作，例如教育部要求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，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。在国外，Zoom 安全事件影响到全球用户，美国、德国、新加坡等国家相关机构都对 Zoom 发布禁令，禁止其员工或学校教师使用 Zoom 应用程序。美国参议院还要求美国联邦贸易委员会对 Zoom 安全事件进行干预，并为在线会议服务应用制定全面的规则指南。我国信息安全标准化技术委员会已针对远程办公安全问题，发布《网络安全标准实践指南—远程办公安全防护》，指导远程办公用户建立网络安全保障体系。

细化和落实法律监管是实现对非接触新经济安全风险有效治理和保障其健康发展的关键措施。当前医疗、教育、金融、工业等各个领域加速运用新一代信息技术实现更高效、便捷、智能化的运营，新业态新模式不断涌现，虽然已有对某些行业“互联网 +”业态进行网络安全监管的法规政策或技术标准指南，例如针对互联网诊疗、在线教育等场景（表 2），但相关法规标准对场景的覆盖度远远不够，已涌现的新兴业态仍没有相应的配套监管措施，法规制定的滞后性明显，重大安全事件仍是当前法规标准制定的主要驱动力，法律前置化功能没有充分实现。同时，很多法规仍停留在原则性要求的阶段，没有配套的惩治规定，难以真正落实。**因此，各行业主管部门应加快开展针对各个领域利用数字化手段开展业务的网络安全监管工作，加快制定和细化相关法律法规，运用综合治理手段加强行业监管，并配套针对性的技术规范和指南，提升企业主体安全风险意识和合规意识，切实保障用户权益。**

表 1 疫情期间我国针对非接触新经济安全风险的相关监管措施列表

发布时间	发布机构	法规政策名称	网络安全相关规定
2020.2.3	国家卫生健康委办公厅	《关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知》	加强网络信息安全工作，以防攻击、防病毒、防篡改、防瘫痪、防泄密为重点，保障数据规范使用，切实保护个人隐私安全，防范网络安全突发事件。
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。

表 1 疫情期间我国针对非接触新经济安全风险的相关监管措施列表

发布时间	发布机构	法规政策名称	网络安全相关规定
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。
2020.2.18	工信部	工业和信息化部办公厅关于做好疫情防控期间信息通信行业网络安全保障工作的通知》	要求切实做好疫情防控和经济社会运行的网络安全支撑保障工作，确保疫情防控期间网络基础设施安全，防止发生重大网络安全事件。
2020.3.2	民政部办公厅、中央网信办秘书局、工业和信息化部办公厅、国家卫生健康委办公厅	《新冠肺炎疫情社区防控工作信息化建设和应用指引》	要求做好社区防控信息化产品（服务）系统安全和隐私保护。应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件；具有数据加密、脱敏和防爬取能力，保障数据安全。社区防控信息化产品（服务）提供者应参照等级保护三级以上要求进行安全防护，应当为其产品（服务）持续提供安全维护，在规定或与产品（服务）使用者约定的期限内，不得终止提供安全维护。
2020.3.18	工信部	《中小企业数字化赋能专项行动方案》	加强网络和数据安全保障。推动中小企业落实《网络安全法》等法律法规和技术标准的要求，强化网络与数据安全保障措施。建设工业互联网安全公共服务平台，面向广大中小企业提供网络和数据安全技术支持服务。鼓励安全服务商创新安全服务模式，提升安全服务供给能力，为中小企业量身定制全天候、全方位、立体化的安全解决方案。
2020.3.20	工业和信息化部办公厅	《关于推动工业互联网加快发展的通知》	加快健全安全保障体系：建立企业分级安全管理制度；完善安全技术监测体系；健全安全工作机制；加强安全技术产品创新。
2020.3.23	全国信息安全标准化技术委员会秘书处	《网络安全标准实践指南—远程办公安全防护》	针对远程办公系统的使用方和用户，分别给出了安全控制措施建议。其中，使用方应在管理和技术两方面开展安全防护，健全远程办公管理制度，加强运维管理，强化安全措施。用户应提高自身安全意识，重点针对设备、数据、环境等方面的安全风险进行防护。

表 2 我国部分细分行业网络安全监管措施列表

细分行业	发布时间	发布机构	法规政策名称	网络安全相关规定
医疗	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）》	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。 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）》	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。 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。
	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。
	2018.12.26	全国信息安全标准化技术委员会	《信息安全技术健康医疗信息安全指南》	给出了健康医疗信息控制者在保护健康医疗信息时可采取的管理和技术措施。
教育	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。
	2019.7.12	教育部等六部门	《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	教育部等八部门	《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。
金融	2015.1	全国信息安全标准化技术委员会	《信息安全技术 电子支付系统安全保护框架》	为公共类电子支付系统的信息安全提供了一个公共框架，主要包括安全问题定义、安全目的、安全功能需求和安全保障需求。
	2019.10	中国人民银行	《个人金融信息（数据）保护试行办法》	重点涉及完善征信机制体制建设，将对金融机构与第三方之间征信业务活动等进一步作出明确规定，加大对违规采集、使用个人征信信息的惩处力度。
	2020.2.13	中国人民银行	《个人金融信息保护技术规范》	将个人金融信息按敏感程度、泄露后造成的危害程度，从高到低分为 C3、C2、C1 三个类别；同时，规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。

3.3.2 | 企业管理制度

随着以非接触新经济为代表的数字经济迎来新一轮加速发展，作为新型信息服务模式、以及新型信息技术应用的实施者、运营者的企业主体，应全面构建企业内部安全管理架构，提升安全风险管理能力，落实相关法规标准，实现自身安全稳定运营及用户权益的安全保障。企业主体不仅包括信息系统建设方、运行方（例如开展在线服务的医疗、教育、金融等机构），还包括提供在线服务的信息技术服务提供方（例如远程办公、在线视频会议等应用程序提供方）。完整的安全管理架构应包括：网络安全组织建设、网络安全风险管理、网络安全策略与制度体系建设、网络安全事件管理、网络安全技术措施等。

（1）网络安全组织建设

企业主体应设立负责网络安全工作的组织部门和专职人员，确定网络安全责任人，进行明确的职责分配。网络安全管理部门应负责制定组织内部的网络安全策略和制度规范，负责网络安全风险管理、网络安全合规管理、网络安全标准管理、网络安全事件管理等工作，并对组织内部的网络安全制度和规程执行情况进行指导和监督。

（2）网络安全风险管理

企业应建立科学的网络安全风险管理方法，对网络资产进行风险评估和风险处置，将网络资产的安全风险控制在可接受的水平，为网络安全管理提供依据。风险管理内容包括建立网络安全风险评估方法及实施流程，根据信息系统脆弱性确定网络安全风险等级以及安全事件可能造成的损失及后果。信息系统建设和运营方应对其网络资产进行全面网络安全风险评估，并对新扩展的在线业务进行补充风险评估，信息技术服务提供方也应对其提供的应用程序的网络安全和用户数据泄露风险进行全面风险评估。

（3）网络安全策略与制度体系

企业主体应制定应对各类网络安全风险的安全制度体系，包括网络安全方针、安全策略、安全管理制度、安全技术规范以及安全操作流程等。安全管理策略应确定安全管理的总体目标、对象、范围、原则和安全框架，构建安全管理体系和安全技术体系。安全管理制度应根据安全管理策略规定的安全各个方面所应遵守的原则方法和指导性策略，针对企业网络资产管理、通信安全管理、访问控制管理、操作安全管理、人员安全管理、数据安全管理、个人隐私保护、人员安全管理、安全培训等建立合理和可操作的管理规范和实施办法，对管理人员或操作人员执行的日常管理操作建立标准化、规范化、流程化的操作规程。技术标准和规范应包括各个安全等级区域网络设备、主机操作系统和主要应用程序应遵守的安全配置和管理的技术标准和规范。

（4）网络安全事件管理

企业主体应制定网络安全事件管理规范，明确网络安全事件发生后的事件报告、通知、处置、恢复、责任追溯、影响评估、改进措施等方面的流程，根据网络安全事件的危害程序、影响范围建立网络安全事件分类分级制度及不同的处置流程。

3.3.3 | 技术保障措施

企业主体应根据制定的网络安全策略通过技术手段建立相应的网络安全保障体系，包括在终端安全、网络安全、应用安全、数据安全、智能硬件安全等各个方面部署安全技术措施，并通过综合安全管理平台利用大数据技术实现威胁态势感知与安全管控。

终端安全：在终端层面，通过部署终端安全防护和管理系统，实施终端安全防护、终端安全监控和终端安全响应，实现终端恶意代码检测与防护、流量画像、漏洞管理、性能监控、登录防护、进程防护、勒索病毒防护、挖矿防、终端环境监控等安全目标。

网络安全：在网络接入层面，通过 VPN 安全接入、运维审计、下一代防火墙等技术手段，依托身份认证、权限控制、行为审计、传输安全、病毒防护、入侵防护等技术措施，实现网络安全接入与安全管控。

应用安全：在应用层面，通过构建应用安全生命周期解决方案，让安全贯穿整个业务生命周期（从开发到运营）的各个环节，包括技术开发、测试、上线及运营等各个阶段，并通过安全监测（包括安全漏洞监测和安全事件监测）进行监管。

数据安全：通过部署数据库防火墙、数据库审计、数据脱敏、数据流动追溯等技术手段，实现数据库的安全访问、行为监控、敏感数据发现、数据脱敏、数据泄露预警等数据保护目标；通过加密技术实现数据的安全传输。

智能硬件安全：通过部署智能终端设备安全防护系统、安全监测平台、威胁感知系统和准入控制系统，实现针对智能终端设备的内核防护、网络防护、漏洞加固、权限管理、非法攻击检测等安全防护目标。

安全管理中心：建立安全管理中心，通过运维审计、APT 攻击检测、综合日志审计以及大数据智能分析，实现全面的漏洞检测、运维操作审计、威胁深度检测，并且结合最新威胁情报，针对全网数据进行安全分析，及时发现安全风险，同时为顶层安全决策提供直观的可视化视图及有效的数据支撑。

PART 4
非接触典型场景安全技术解决方案

4.1 | 远程办公

受新冠肺炎疫情影响，多地政府、企事业单位号召员工实行远程办公。对于大多数企业而言，当前使用的远程办公能力是临时搭建的，安全能力相对薄弱且不完整。后疫情时代，如何保障远程办公软件的稳定性、安全性，多角度加固网络安全体系，赋能企业的数字化转型、提质增效，是企业需要重点考虑的问题。目前，企业普遍采用的远程办公方式主要包括：

（1）通过虚拟专用网（VPN）：在公用网络中建立一个临时的、安全的连接，形成一条穿过混乱的公用网络的安全、稳定的隧道，为员工日常办公需求，包括获取公司内部邮件、访问局域网中的文件服务器、内部数据库、CRM、ERP 等等。

（2）远程控制办公：主要通过远程控制技术，或远程控制软件，对远程电脑进行操作办公，实现非本地办公，如在家办公、异地办公、移动办公等远程办公模式。

（3）远程会议 / 社交：主要通过社交软件进行远程视频会议的方式进行工作安排、讨论、汇报等。

4.1.1 | 安全风险

与在公司有专业的网络管理员不同，员工在家办公的网络和工具要更开放、更多样，因此产生的安全问题也往往更容易被忽略，由此给企业带来的安全风险愈加严峻。存储在计算机中的重要文件、数据库中的重要数据等信息都存在着安全隐患，尤其是研发内网中的相关数据，一旦丢失、损坏或泄露、不能及时送达，都会给企业造成很大的损失。如果涉及到商业机密信息，则给企业造成的损失会更大甚至影响到企业的生存和发展。

此外，在长期的公司办公环境影响下，主流的安全防护措施均针对公司内部的网络实施匹配的安全策略。在变更为远程办公的场景后，通过传统的地址映射等手段直接将内部网络资产暴露在互联网中，将带来被恶意攻击者攻击的风险，如恶意扫描、暴力破解、拒绝服务攻击、漏洞攻击等。

具体而言，远程办公场景中存在的网络安全风险包括：

（1）数据安全威胁

远程沟通过程中，可能涉及聊天内容、产品设计资料、内部营销规划、招投标书文件、合同协议等重要数据。这些敏感数据在钉钉、企业微信等办公即时通信软件中存储、传输过程中，存在被窃取和泄露的安全风险。

同时，企业数据纷纷上云，在云平台中计算与存储，实现数据托管服务。数据的所有权与管理权相分离，企业对自身数据的把控性低，数据存在一定的安全风险。外部黑客攻击、权限盗用等会造成数据泄露，数据在任意传输节点都有可能被截获，如传输数据链路被明文截取、通道加密被破解等。

（2）远程访问内网及远程运维安全威胁

当前常见远程办公方式主要是采用 VPN+Windows 远程桌面和使用 Teamviewer 或向日葵等远程工具，均存在明显安全风险。通过 VPN 进入内网后，直接访问办公 PC 或者运维服

务器，这种方式权限控制不足，存在越权操作风险；文件传输无法控制，存在数据泄露风险；运维操作无审计，事后难以追溯。其次，企业采用 VPN 技术为员工建立与内部网络的链接，对企业的账号管理规范、人员管理规范带来调整，会涉及一系列的账号盗用、业务违规等安全隐患。此外，针对企业的信息资产、数字资产采用远程控制维护，增加了企业核心资产的暴露面，被攻击导致数据泄露、资产破坏的风险增加，同时，远程控制也会带来企业资产被恶意远控的安全隐患。

（3）终端安全威胁

远程办公需要用到员工自有的电脑、手机等终端，这些终端暴露在互联网上，很容易成为黑客攻击的目标。员工在远程接入所使用的终端如果不具有合理的安全保障措施，存在将远程病毒带入企业内网的安全隐患。

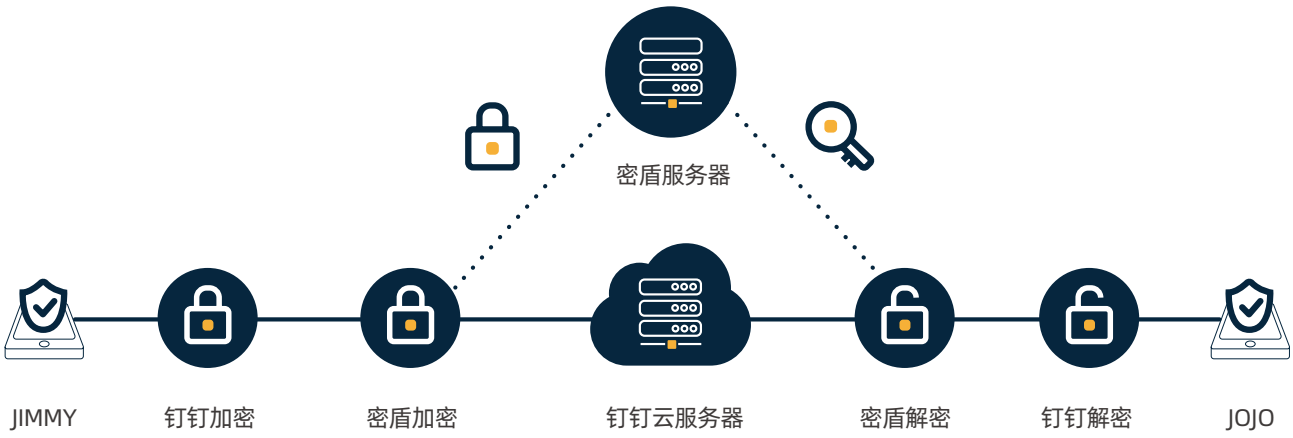
4.1.2 | 解决方案

1、远程办公数据安全场景

（1）信息沟通安全

远程沟通往往需要借助钉钉、微信、邮箱等平台，信息沟通中包含文字、文件、语音、图片、视频等内容，涉及企业的核心数据，因此应对信息进行全生命周期的保护，保障信息在存储、传输过程中的安全。采用第三方加密产品或方案，可有效解决信息传输安全隐患。

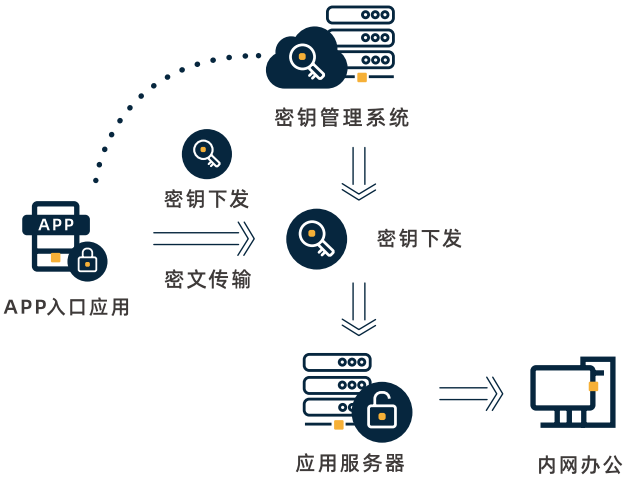
以钉钉为例，通过钉钉 + 第三方加密，对远程办公时即时通讯端的信息进行独立第三方的二次加密，可实现敏感信息保护“双保险”，无论是钉钉还是第三方加密厂家都无法单独打开敏感信息。通过在钉钉客户端中内嵌加（解）密模块，实现用户在客户端请求数据时，可在客户端通过加（解）密模块进行加（解）密，通过密文传输，密文存储到钉钉服务器上。当服务器端返回数据时，密文传输到客户端，客户端通过加（解）密模块进行解密，反馈给客户可识别的信息。



同时，通过第三方加密产品或方案，可实现对离职人员进行有效管理，员工离职后，将无法获得密钥，无法查看在职期间信息。另外，针对数据特别敏感的企业可以采用独立部署密钥管理服务器，自主更新密钥，实现数据由自己掌控。

（2）Web/H5 系统加密

随着智能办公应用的普及，众多组织 / 单位依托钉钉 / 微信作为平台入口，在移动终端上开发适配自身业务的相应功能。与此同时，工作中敏感数据将不可避免地在互联网中传输和存储，这些重要数据存在被非法用户偷窥和窃取的可能。因此，非常有必要采取措施防止重要数据的泄露。可采用云加密解决方案保证内网办公系统向外网迁移过程中的数据传输安全。



（3）视频加密

现有视频信息系统中，视频信息大多以明文方式存储和传输，存在较大的安全风险。为保证设备和控制信令的真实性，以及从信息源头上视频数据的真实性和保密性，可通过视频加密系统，防止视频数据被伪造篡改、非法传播扩散等情况的发生。

（4）存储加密

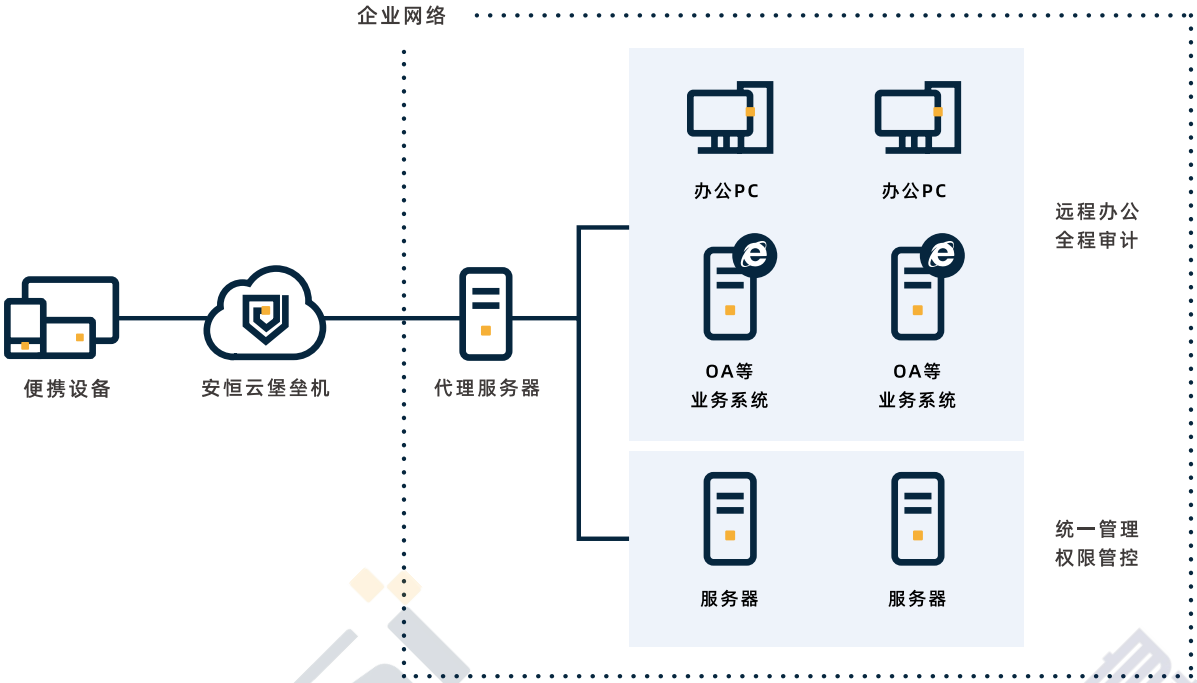
有条件的单位建议通过“云桌面”的方式远程办公，保障企业敏感数据不落地存储，防止数据被拷贝，当数据被导出时可追踪审计。同时，可考虑通过部署云数据库审计、云监测和云防护 SaaS 服务，控制安全准入，防止高危操作、越权行为，对远程办公数据进行实时加密与安全监控，并建立基于操作录像、流量、日志、数据库语句等的审计措施。

2、远程办公 IT 运维安全场景

远程办公模式需要将前期内网的访问权限，开放到互联网。访问通道的开放，也增加了远程安全运维的风险，可能存在权限控制不足、运维链路不安全、无审计不合规等风险。此时，建立安全的传输通道和运维通道非常关键，可通过本地部署或混合云部署具备身份认证、权限控制、文件单向传输和审计、行为审计等功能的远程运维解决方案实现远程运维安全。

本地部署解决方案：采用集成 SSL VPN 功能模块的堡垒机，将 VPN 服务端口映射互联网，即可实现远程 IT 运维，可保障远程运维的接入安全性，同时通过堡垒机单点登录服务器进行远程运维操作，既可解决外网接入的链路安全，同时可保证运维过程的权限控制、操作审计及合规要求。

混合云部署解决方案：云上部署云堡垒机，通过在企业内部局域网中配置一台 Proxy 代理服务器，与云堡垒机服务网络互通，即可实现远程 IT 运维使用。



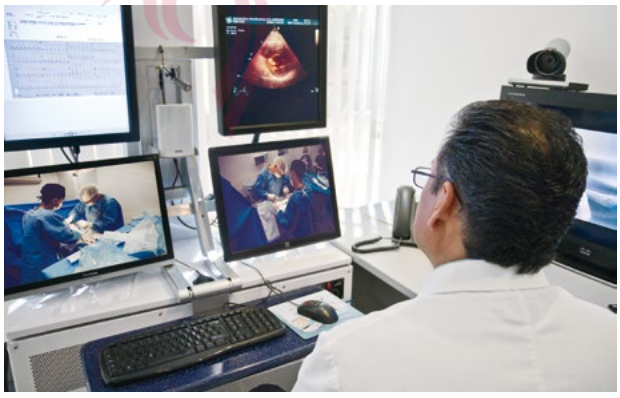
3、远程办公终端安全场景

针对终端安全问题，可通过部署具备勒索专防专杀、补丁修复、外设管控、文件审计、违规外联检测与阻断等安全能力的 EDR 等安全终端防护软件，降低终端数据泄露风险。

4.2 | 远程医疗

4.2.1 | 安全风险

当前，互联网医疗火热的背后，医疗领域网络安全问题如影随形。医院通过应用互联网技术，提供基于网站、微信、App 等医疗服务的同时，相应的网络安全方面的建设还没有呈现配套建设的趋势。然而随着互联网医疗的发展，医院原来相对独立的网络环境已向互联网打开了通路，医院网络安全已经不再是单一的局域网安全，必须要做到局域网与互联网的全面管理。近年来，针对医院的勒索、挖矿、医疗信息泄露等医疗行业的网络安全事件层出不穷，医院信息系统已经成为不法黑客的重点攻击对象之一。一旦网络瘫痪或者数据丢失，不



仅对医院的正常业务造成严重影响，也对医院的形象和服务质量造成不可估量的损失。

（1）外部攻击风险

由于医院等机构的特殊性，黑客可能会通过钓鱼、挂马等社工攻击的方式，实现对医院办公电脑的控制或数据洗劫，从而获取进入内网的入口信息（帐号、密码等），或者直接对有价值的办公网系统实施勒索等破坏

性攻击。患者预约信息、检查检验信息、就诊信息、医学数据等医疗信息都属于需要紧急使用的信息，一旦这些数据被加密勒索，会造成很大的影响，医院也将花费大量时间与资源进行数据恢复。

而外网资产的安全关乎到内网的安全。黑客一般通过攻击外网服务器和办公网电脑系统实现对内网的攻击和数据的窃取。通过攻击外网服务器获取外网服务器的权限，继而利用成功入侵的外网服务器作为跳板，攻击内网其他服务器。以美国互联网黑市的信息售价为参考，数据丰富的医疗信息的价值是信用卡信息的 10 倍。欺诈者利用这些精准信息可以进行电信诈骗、虚假医疗广告营销等违法活动。

（2）应用安全脆弱性风险

随着互联网 + 医疗的发展，越来越多的医院借助 WEB、患者 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、在线问诊、在线处方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。虽然这种更为便利的医疗方式给民众生活带来了极大便利，但随之而来的医疗网络与互联网连接等手段也带来了新的漏洞风险和数据泄露风险。

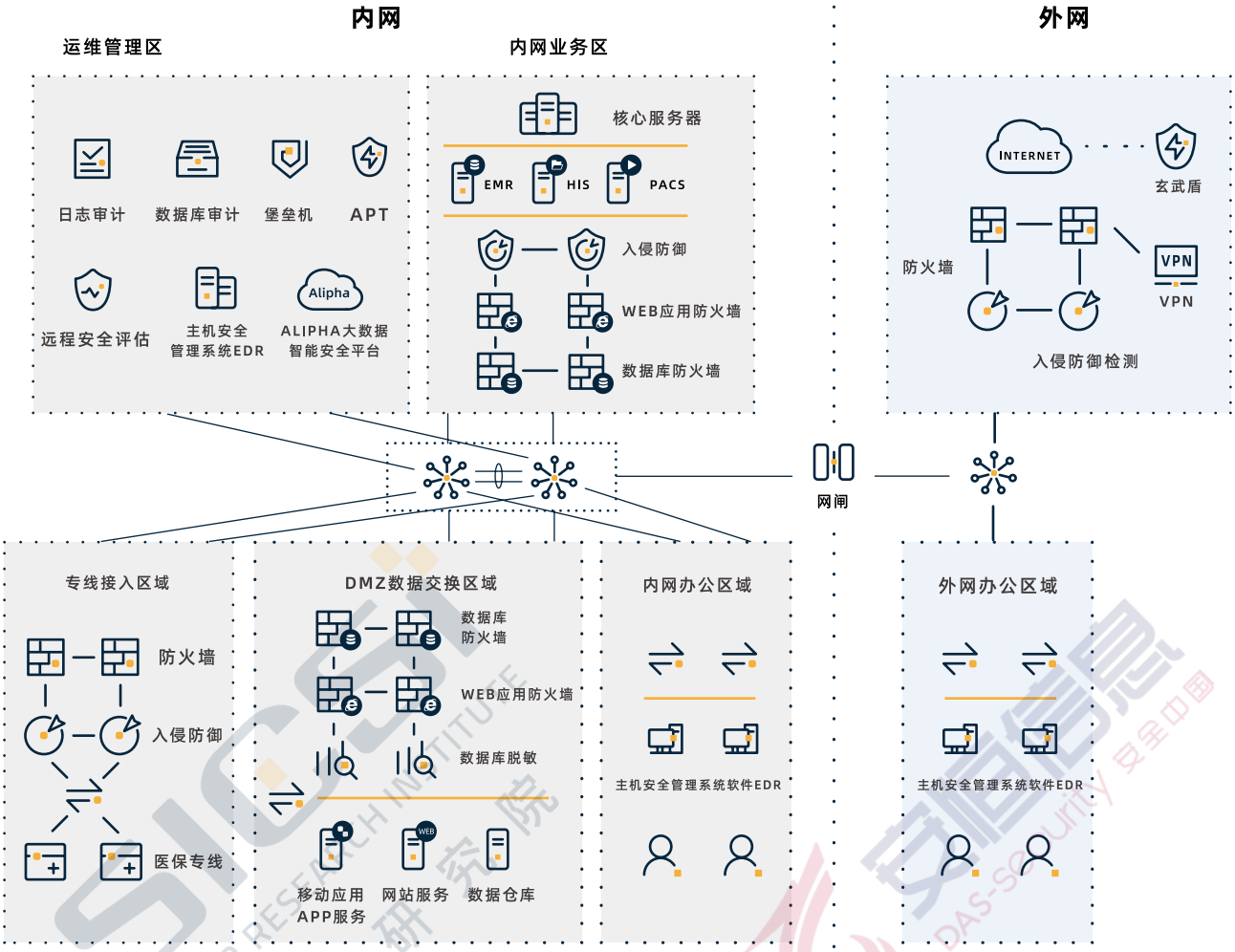
疫情防控期间，安恒信息风暴中心曾抽取医疗卫生行业 1500 余个网站进行实时分析，发现在 1500 余家医疗网络系统中，存在网络安全风险漏洞的网站占比约 10%，高危漏洞占比最高，约 67.94%。同时，在 1500 余家医疗网络 / 系统中，存在高危安全事件 105 起。

（3）内部威胁风险

随着互联网医院信息化的不断发展，安全风险来源、威胁方式逐年变化，来自内部的恶意威胁往往经常被忽视。针对此前发生的大部分医疗数据泄露事件，有很大的一部分责任是内部人员所导致。医疗机构多种不同的系统几乎都是同时运行，其中一个出了问题也会影响其他系统运作。而医院内部人员对医院的系统和业务流程更加熟悉，这为有针对性的攻击活动提供了便利。此外，内部人员不需要花费时间绕过外部安全防护，大大提高了攻击的成功率。大量被发现的攻击表明，内部攻击只需要一些简单的手法而不需要大量的或特殊的技能。

4.2.2 | 解决方案

DMZ 区部署数据库防火墙、数据库脱敏及 WAF，对互联网医院的互联网应用 APP、网站、微信服务等提供数据及数据库安全保护；网络出口处部署 NGFW（下一代防火墙）、入侵防火墙进行安全防护；外网接入部署 VPN 解决远程接入安全问题，接入 SAAS 服务监测网站可用性同时防护外部攻击；内网业务区配置数据库防火墙、WAF、入侵防护设备保护内部业务系统数据安全；安全管理区集中部署安全检测、审计、分析等安全产品，在安全管理区除传统的安全设备外，还可利用大数据分析平台，针对全网数据进行安全分析，及时发现安全风险，同时为顶层安全决策提供直观的可视化视图及有效的数据支撑。办公终端部署终端安全防护 EDR 产品解决终端主机安全问题。



（1）终端安全

互联网医院通过部署全院覆盖的终端安全管理代理、终端安全管理中心与准入控制系统对医院可交互终端（医生 / 护士 / 收费工作站、行政人员办公 PC、应用服务器、自助服务终端、网络媒体发布终端等）与哑终端进行集中式的安全与网络准入管理，并自动根据安全策略进行违规或威胁处置响应。

①终端安全防护：建设互联网医院终端安全防护能力，对终端网络流量实时监测和控制，保护终端网络安全；通过终端安全的基线核查、安全加固、补丁管理等手段，为终端操作系统提供安全防护，防止因操作系统脆弱性而引发的攻击行为；通过安全基础设施的恶意代码检测服务，检测识别病毒、蠕虫、木马、僵尸网络、勒索软件等恶意代码，降低恶意代码活动所带来的系统破坏、数据窃取、资源耗用等的影响，防止终端病毒发起的网络攻击；通过密码管理、补丁管理等手段，对终端应用和数据进行实时监测控制，保护终端应用及数据的安全。

②终端安全监控：建设互联网医院对于自身终端安全的监控能力，实时监控终端网络、系统运行以及应用、数据的使用情况，及时发现终端环境异常，确保终端运行环境安全；通过采集、分析终端用户行为数据，发现存在风险和威胁的终端及其使用人。

③终端安全响应：终端安全响应能力可以实现在管理员或者运营运维平台对终端的安全级别和管控措施需要调整的时候，对其管控指令做出响应，管控能力包含安全基线、病毒查杀、行为管控、网络管控等措施。针对内部终端被动泄密的问题，多数因为终端的安全策

略配置不够严谨或者计算机本身存在安全漏洞。通过终端安全管理系统主动探测和一键修复功能，对入网计算机终端的安全测试进行检查和评分，对存在安全隐患的计算机终端强制禁止入网，并提供一键策略修复技术，解决终端可能存在的不安全隐患，实现全网终端的统一安全管理效果。

（2）接入安全

① VPN 安全接入：

传输安全：VPN 的本质是需要保证数据在公网上传输的安全性，达到虚拟专用网的效果。传输的安全性强度往往需要依靠 VPN 数据所采用的加密算法。通过 AES、DES、3DES、RSA、RC4、签名算法等多种国际主流加密算法对数据进行强加密，可以保证数据传输的高安全。

身份认证：可通过 LDAP/AD 、Radius、CA 等第三方认证联动，及 USB KEY 、硬件特征码、短信认证（短信猫和短信网关）、动态令牌卡等加强认证方式来保障VPN登陆用户的身份确认性。针对需要远程登陆访问互联网医院内网的相关终端，为了解决因用户帐号意外泄漏、帐号盗用导致的数据泄露问题，可对登录终端进行绑定。通过终端的硬件特征码绑定实现硬件终端的唯一标识。通过获取客户端的不可改变的硬件信息，如 CPU、硬盘、网卡等信息生成数字证书，并对证书和用户进行绑定实现用户身份的唯一性控制。

数据沙盒：医院内网的数据极为重要且敏感，在客户端登陆 VPN 后，可在客户端自动使用虚拟技术生成与原有默认桌面完全一样一个封闭式的安全桌面（沙盒），用户在通过 SSL VPN 访问启用了安全桌面的应用时，终端与服务器端所有交互的应用数据将仅会保存在该沙盒之中，并进行高强度的加密。在该沙盒中的数据，无法通过拷贝到本机默认桌面、拷贝到外设、与局域网通信、与外网通信等任何方式将数据传送到沙盒之外。当用户退出 SSL VPN 之后，沙盒中的所有数据都进行清除， 所有的操作将会被重定向。即使是断电导致的安全桌面崩溃，沙盒中的数据也是通过高强度加密保证安全性。下一次 SSL VPN 登录启动时，安装桌面会自动检测之前的遗留痕迹并进行清除。

权限控制：通过 IP、端口、服务、URL 等方式对内网应用以“资源”的方式进行定义，并基于“角色”将特定用户 / 用户组与相应的资源进行对应绑定，实现指定用户只能访问指定的应用的权限划分。

安全审计：VPN 将记录完成的用户日志：用户访问日志（登录 IP、访问资源、时间、认证方式）、用户活跃程度、用户 / 用户组流量排行及查询、用户 / 用户组流速趋势及查询。同时也针对异常信息进行记录：告警日志（暴破登录攻击记录、CPU 长时间占用过高记录、设备内存不足）、用户爆破登录、主从用户名非法访问记录等。

②运维审计：针对医院的远程办公这类特殊场景，在远程接入安全中重点在于如何保障数据

的只进不出，访问登陆及操作行为“可控、可视、可溯”。VPN 实现了登陆办公外网的访问登陆行为“可控、可视、可溯”，而针对医院则需要通过运维审计系统实现远程登陆医院的登陆及操作行为“可控、可视、可溯”。同时通过运维审计联动桌面云（在桌面云终端中的数据，无法通过拷贝到本机、拷贝到外设、与局域网通信、与外网通信等任何方式将数据传送到桌面云终端之外），运维审计账号用户有且仅有对应桌面云的访问权限，保障数据的只进不出。

③下一代防火墙：通过部署下一代防火墙，对重要节点和网段进行边界保护，可以对所有流经防火墙的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，防范各类攻击行为，杜绝越权访问，防止非法攻击。通过合理布局，形成多级的纵深防御体系。

（3）应用安全

① SaaS 安全防护（防护 + 监测）：事前采用云监测对网站进行漏洞监测，事中采用零部署云防护方案，云 WAF 对 SQL 注入、跨站脚本、Webshell 上传、WEB 组件漏洞等安全风险进行防护，事后采用大数据分析形成可视化报告和统计分析报表。

② WEB 应用防火墙：部署 WAF 可有效缓解网站及 Web 应用系统面临如 OWASP Top10 中定义的常见威胁，快速应对恶意攻击者对 Web 业务带来的冲击，对网站进行有效的安全加固。WAF 与云端威胁情报实时联动，可主动发现扫描 IP、僵尸 IP、C&C、代理 IP 等恶意 IP 对 WEB 业务的访问行为，针对恶意的访问行为记录告警日志并及时通知运维管理人员对恶意 IP 的访问行为进行拦截。同时，通过语义分析技术有效识别 SQL 注入、XSS 攻击，结合特征攻击引擎双重判断机制，可更加准确地防护 SQL 注入、XSS 攻击。通过机器学习形成正常和异常访问基线，可采用智能评分机制判定高度可疑的攻击行为，并进行有效防护。

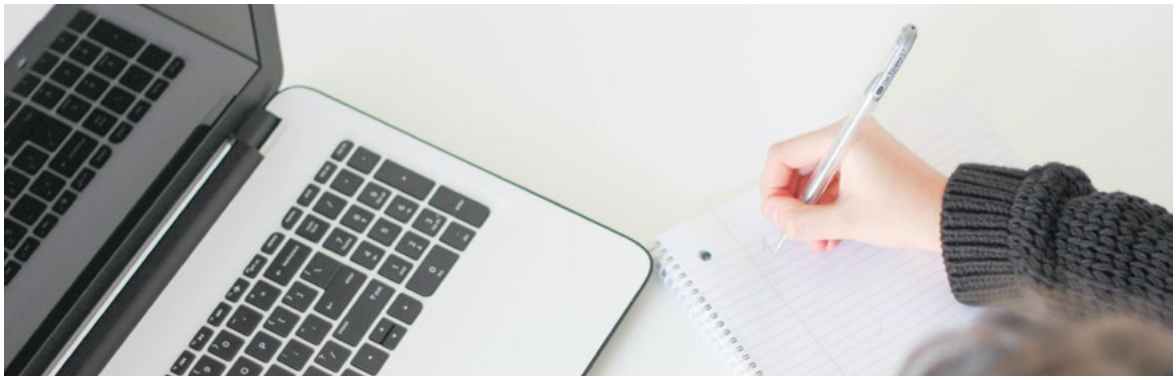
（4）数据安全

①数据库防火墙：数据库防火墙能够对进出核心数据库的双向访问流量进行高效精准的解析、访问控制和攻击特征检测，根据内置的各种漏洞攻击特征策略以及自定义策略实时地对数据库的请求进行精准处理判断，一旦引擎识别到访问请求属于违规访问或者攻击行为将实时告警阻断，让数据库的安全以可视化直观的方式将所有的访问都呈现在管理者的面前，数据库不再处于不可知、不可控的情况，数据威胁将被迅速发现和响应。

②数据库审计：数据库审计与风险控制系统可对进出核心数据库的访问流量进行数据报文字段级的解析操作，完全还原出操作的细节，并给出详尽的操作返回结果。数据库审计能够将所有的访问都呈现在管理者的面前，让数据库不再处于不可知、不可控的情况，数据威胁将被迅速发现和响应。

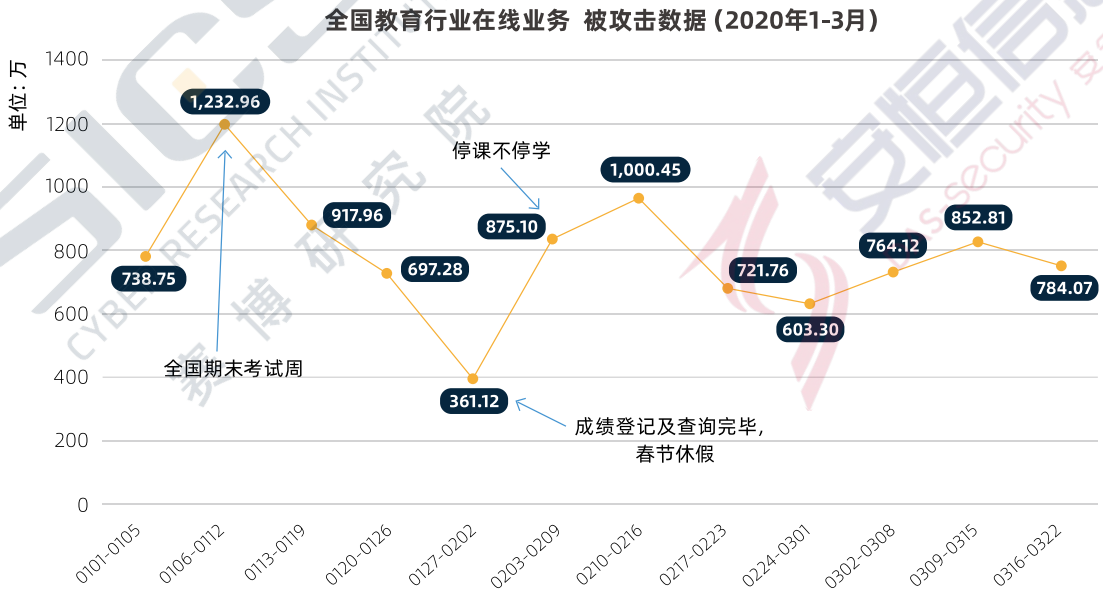
③数据脱敏：数据脱敏系统具有敏感数据发现、脱敏能力的敏感数据管理系统，敏感数据是数据脱敏系统处理的核心，将给用户带来敏感数据的发现、管控能力。

4.3 | 在线教育



4.3.1 | 安全风险

今年 2 月 10 日 -3 月 22 日疫情期间，尤其在全国开展线上教学期间，全国教育行业在线网站 / 系统平均访问流量为 5.8 亿次 / 周、8281 万次 / 天，较之前大幅增加。同时，2020 年 1 月 1 日 -3 月 22 日，全国教育行业在线网站 / 系统累计遭受 9600 多万次网络攻击，说明教育系统的网络安全问题非常严峻。



2020年1月1日-3月22日，全国教育行业在线网站/系统总计遭受9,600多万次网络攻击

在线教育系统存在的网络安全风险包括：

（1）DDoS 攻击导致在线教育系统瘫痪

在线教育系统面向学生提供课程和教学视频，其可用性要求十分之高，一旦遭遇大流量 DDoS 攻击，对业务系统可用性将造成极大的影响，甚至导致在线教育系统瘫痪。

（2）系统篡改

在线教育系统由于网站具备高访问量、高可信度及较高的网络与系统资源，能够为暗链网站带来更多、更持久的访问流量与更高的访问排名，使其获得更多广告经济利益，所以可能会成为黑客组织的重点目标。黑页（黑客入侵篡改首页）、反共页面也成为我国教育网站已检出安全事件的重要类型。

（3）信息泄露

在线教育系统存储了大量的学生与教师信息，如姓名、身份证号码、手机号等敏感信息，此类信息的泄露会给学生及老师带来严重的安全隐患。

（4）0day 攻击

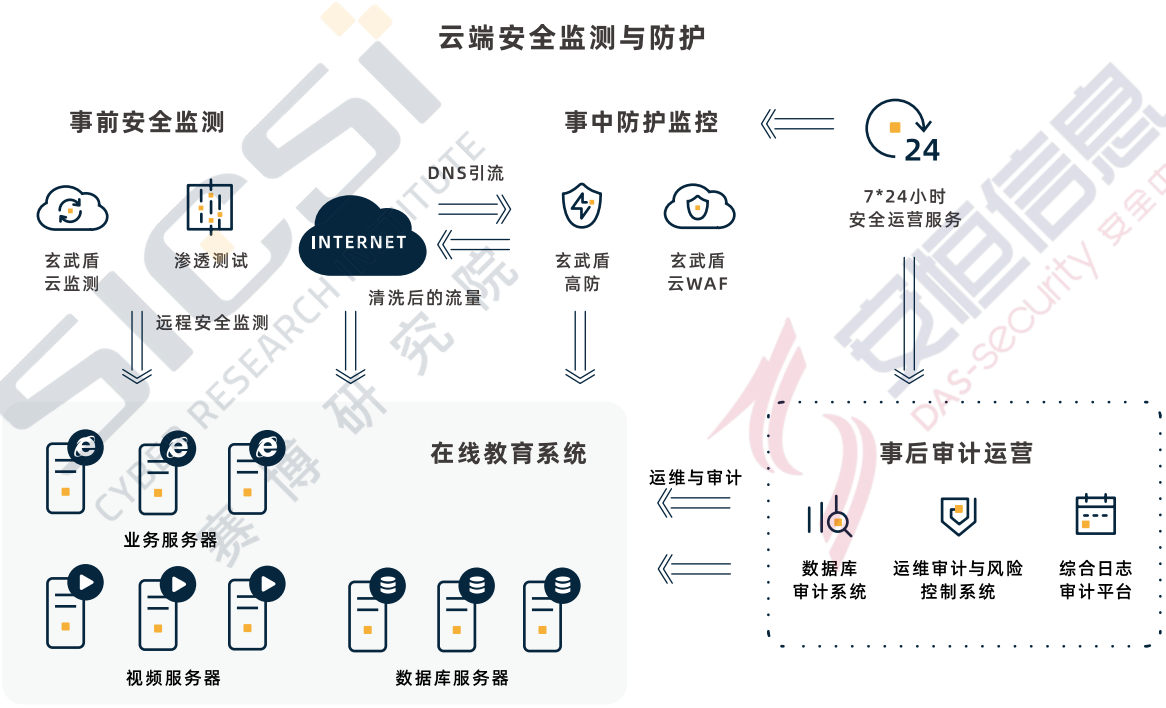
黑客利用 0day 对在线教育系统进行攻击，从而达到控制主机、篡改网站、窃取数据等一系列攻击目的。

（5）运维安全

系统管理员、第三方运维人员、研发人员通过远程运维，会带来新的运维层面安全，会面临越权、运维过程是否记录、操作是否记录等运维安全问题。

4.3.2 | 解决方案

可通过事前安全检测、事中防护监控及事后审计运营等一体化解决方案，保障在线教育系统安全运行。



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。

事后通过在本地部署综合日志审计平台、数据库审计系统、运维审计与风险控制系统对在线教育系统进行审计与分析，确保运维可控，操作可查，结合 7*24 小时安全运营服务快速处置与应急响应。

4.4 | 无人工厂

4.4.1 | 安全风险

智慧工厂物联网的核心技术通常具有以下几个特点: 可跟踪、可监控、可连接,尤其是监控设备、在线物联网设备等智能设备，这些特性决定了其通常具有分散化、规模庞大、边界模糊等特点，极易受到黑客攻击和利用。其安全风险包括:

（1）运行状态异常导致失效

物联网的设备通常数量非常庞大，同时部署位置也很分散化，可能会有断网、设备故障、状态异常等情况，因此，需要实时地对这些物联网设备状态进行实时的监控，及时发现异常的设备并进行预警。

（2）系统漏洞被恶意利用

物联网的设备通常都已经智能化，这些设备大多都有自己的操作系统，可能会存在系统漏洞未修复的情况。因此，需要实时的监测这些未修复的漏洞，并进行及时修复。尤其是智能硬件的设备往往疏于管理，可能存在弱口令等问题，一旦被黑客利用后果极为严重。因此，需要实时地监控系统存在的弱口令，并对其中存在问题的设备进行强化。

（3）身份伪造产生内部威胁

智能硬件的设备可能部署在室外，会被恶意攻击利用，遭到替换设备并伪造身份，被利用作为攻击源，进而对整体物联网造成安全威胁。

（4）非法接入造成内部异常

智能硬件物联网的设备类型多样，可能会面临非法接入导致内部异常，需要对这些设备进行及时的监控，发现其中仿冒的或非法的物联网设备类型。

（5）内部数据被非法窃取

大量的物联网终端产生各种数据，通过专网 / 互联网传播，一旦内网被攻击，可能会出现数据被非法窃取的风险。

（6）终端被恶意控制损坏基础设施

物联网存在各种类型的物联网终端，其中一部分部署位于一区(生产区),比如机器人、传感器、摄像头等,一旦这些物联网终端被恶意程序控制，会影响正常的基础设施监控，同时还可能导致基础设施被恶意攻击而无法正常工作。

4.4.2 | 解决方案

1、需求分析

从需求角度分析，无人工厂的安全方案建设需要全面采集各类物联网终端多重维度的安全数据，包括终端系统层面、终端网络层面、终端流量层面、威胁层面等数据，进行数据统一处理、建模分析。进行全网终端安全风险预警、态势感知。

（1）建立面向物联网终端的实时安全监控防护能力

对物联网资产置入安全模块,进行自身安全加固，对物联网设备进行签名认证，感知周边安全，通过加密技术对数据进行安全加密。

（2）建设统一物联网安全态势感知与管控平台

建立物联网络态势感知平台，对物联网设备的安全状态实时监控，运用大数据分析技术、动态预警技术、泛系统漏洞检测技术等多项关键技术，对范围内的物联网络设备进行安全漏洞威胁主动巡检，及时

感知海量物联网设备的安全状态、漏洞及风险情况，实现物联网设备的安全态势感知和通报预警，最终达到及时感知物联网络风险所在的目的。

（3）形成周期性的物联网安全监测评估机制

为物联网资产进行安全监测，智能感知物联网终端安全状态信息，从物联网终端的资产出发，关注物联网终端资产状态、弱口令、系统漏洞等威胁信息，结合多角度、多维度分析物联网终端的安全事件，为对物联网终端安全管控构建管 理平台。

（4）形成物联网网络安全综合评价体

通过面向物联网的数据治理和分析挖掘技术，对获取的多源异构数据进行数据标准化处理，并结合不同业务需求和场景模型，将各类安全事件进行集中管理 和关联分析，及时有效发现系统中存在的安全威胁，加强对入侵攻击的识别能力、 关联分析能力和攻击趋势预测能力。同时能够预测近一段时间的安全威胁、攻击方式等，进行一系列安全趋势分析，最后从不同的维度对全网进行综合安全指数量化，形成对全网网络安全的综合评价。

（5）实现物联网安全事件预警和响应机制

当发现物联网漏洞、隐患、恶意木马病毒传播时，有针对性的发出预警，对可能受到影响的系统进行提醒。并在事件确认同时启动相应机制，采取有效的安全防护技术手段，对安全事件进行控制和防护。

2、架构设计

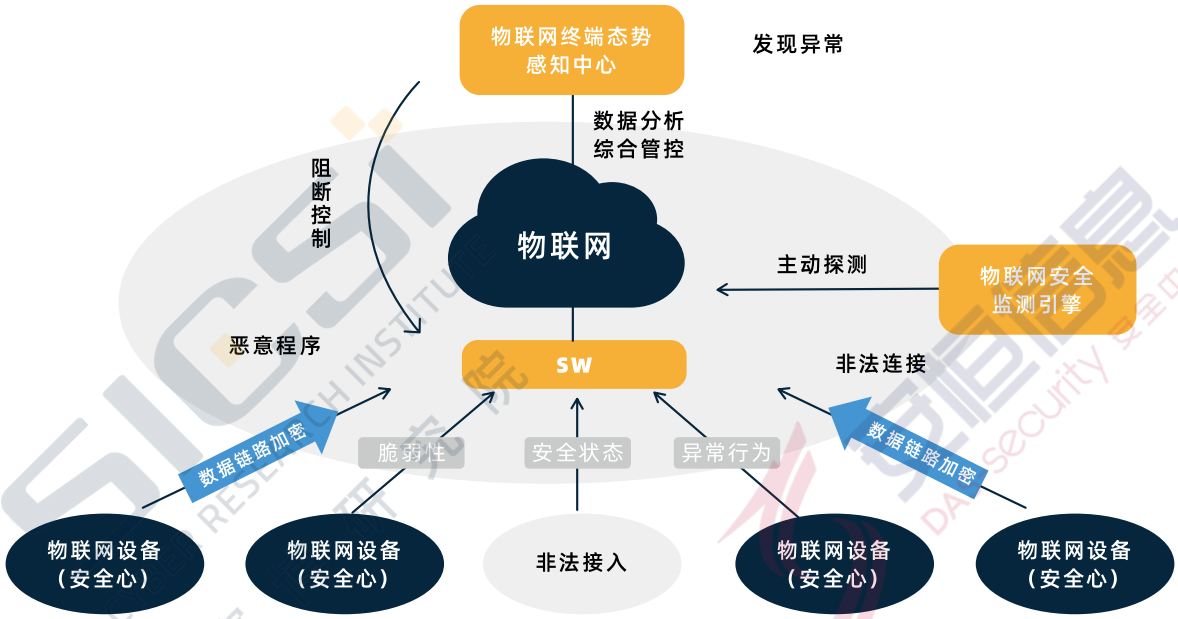
基于以上需求，在安全架构方面，采取可实现防护、分析、响应和预测的自适应安全防护技术，采用基于安全模块的可信计算平台，通过异常威胁的快速发现，实现控制指令正确下发，达到智能终端设备的可信安全管控的目的。

整体系统技术架构图

3、“云＋端”的联动式防护架构

进一步在安全防护架构方面，采用“云＋端”的联动式防护架构，依托内核级进程文件防护技术、大数据安全分析技术、自适应安全防护技术和区域安全态势分析技术等多项关键技术，对海量物联网终端进行安全监控、传输加密和接入管控，建立物联网终端的区域安全态势分析和威胁感知评估方法，及时对物联网应用的物联网终端进行安全防护、数据加密、异常分析和态势感知。

通过对物联网终端嵌入安全心，结合物联网态势感知与管控中心，实现资产管理、威胁分析、秘钥管理、安全审计，为物联网网络提供安全防护、数据加密、 威胁感知和可信管控能力。



4、方案终端防护能力

在终端防护方面，基于嵌入式安全自防护与云端态势感知智能分析结合的防护技术，为物联网终端建立系统监控和防护，通过内核级系统网络、进程和文件监控防护以及专用的数据加密算法，为端到端的数据传输提供高强度的加密和验证服务。

内核防护：结合驱动层的进程防护，建立进程分析模型，发现异常病毒感染、恶意威胁等。

网络防护：通过网络通信防护，快速对异常网络通信和开放端口进行限制。

漏洞修复：对各个物联网设备指纹进行分析，发现存在漏洞，及时采取修复措施。

权限管理：完备的权限管理能力，对异常替换、非授权接入、未知登录事件进行阻断。

数据加密：针对物联网设备建立完整的加密体系，保证数据交换传输的安全。

5、方案安全感知管控能力

（1）安全监测评估

通过部署物联网安全监测平台设备，实时或周期性对物联网进行安全摸底检查，从网络资产快速摸底、设备弱口令及漏洞检测以及网络边界检测等几个方面，对网络进行快速的扫描检测，及时发现存在的各类安全隐患，比如系统漏洞、弱口令、敏感服务端口等安全弱点,摸清物联网安全现状,排查并督促整改重要网络安全隐患、风险和突出问题。

（2）非法接入管控

针对物联网终端接入物联网网络，进行严密准入管控，确保仅有授权的、合法的终端接入网络。以此来保障只有认证通过的合法授权终端，授权允许的协议流量才能通过该设备，其他流量全部阻断。

（3）异常威胁分析

针对海量物联网终端产生的异常威胁，同时可以部署威胁感知流量检测系统，支持多种协议解析并监测物联网设备异常流量威胁事件，能够详细清晰的记录系统发现的异常安全威胁日志。系统采用旁路部署模式，监听异常流量，不会对现有业务产生任何影响，且支持大规模网络流量分析检测。通过对僵尸网络、远程控制、DDOS 攻击等异常威胁的识别，可以对攻击源进行追溯，进一步定位攻击源类型，以便确认受恶意程序感染控制的终端，从而对受控终端进行处置和对源头进行处置。

（4）安全态势感知

针对物联网终端系统进行内核防护、数据加密和实时审计，通过物联网态势感知与管控中心进行智能分析，实现物联网终端的安全态势感知与可信管控。

采用面向区域网络大规模资产横向对比分析和态势分析的技术，利用资产原始数据各要素的依赖关系，基于机器学习的异常威胁分析与事件预警技术，针对海量物联网终端行为数据建立机器学习算法模型，通过训练多维原始数据样本分类聚类、实时挖据分析海量安全数据等关键方法，识别异常威胁和风险行为，快速发现物联网应用的异常威胁和告警。

PART 5

非接触新经济对网络安全产业影响展望

（1）非接触新经济蓬勃发展带来广阔安全市场前景

非接触新经济加速传统产业数字化转型，带动数字经济快速发展，推动经济模式全面线上化、网络化、智能化的同时，必将导致网络安全风险面加速扩大，带动网络安全需求持续提升，为网络安全产业带来新的市场机遇。同时，新冠疫情凸显我国国家治理现代化水平不足，后疫情时代，我国智慧城市建设、政务数字化、城市治理数字化等建设进程将全面加快，大幅提升公共服务、社会治理现代化水平，也必将带来更大的网络安全需求。此外，数字经济与智慧城市的加快发展将带动 5G、数据中心、工业互联网等新基建加速发展，安全作为信息化建设的刚需，将给网络安全产业带来广阔的市场机会。

（2）非接触新经济带来新的安全挑战和安全需求

新型业务模式、办公模式、服务模式、运营模式的发展需要新的信息系统架构支撑、新的网络接入方式，并重新定义了新的安全边界，在对安全性提出全新挑战的同时，也对安全产业提出了新的产品和服务需求，带来了新的业务机会。例如在远程办公场景中，IT 的边界变得非常模糊化，远程办公的终端和应用都不在传统的企业常规的安全保护模型的范围之内，导致无法执行企业的统一安全策略，同时不得不允许远程用户访问原来仅允许内部用户访问的应用，这将大大增加网络的攻击面和安全风险等级，因此亟需新的安全应对策略。此外，其他非接触线上化和智能化服务场景都产生了新型安全风险评估、安全防护和安全监测的各类需求，安全企业应借此机会深入挖掘各类新型安全需求，抓住新的业务机会，提升自身技术能力。

（3）非接触新经济浪潮驱动安全产品和服务模式转型

此次新冠疫情不仅催生远程办公、远程教育、远程医疗等在线式非接触新经济蓬勃发展，对于网络安全行业，由于安全人员无法到达现场，也催生了非接触的远程安全服务模式的发展。例如，疫情期间国内多家网络安全企业推出远程的网络安全云监测与响应服务，保障用户的网络安全需求。

在目前全球网络安全人才严重短缺的情况下，远程网络安全云服务是提高人员使用效率、提高综合服务水平的必由之路。远程安全运营服务具有免部署免运维、快速接入的优势，可提供事前安全监测与体检、事中安全防护与监控、事后安全运维与响应等一站式安全托管服务，还可结合数据大脑威胁情报，提炼出安全预警、安全漏洞和攻击态势等信息，周期性地为用户提供情报共享和展示，有助于安全决策。目前我国网络安全服务发展水平与美国相比差距较大，此次疫情或是一个推动网络安全行业商业模式变革的机会，可能会让国内客户更快发现远程安全运营服务的优势和价值，提升对在线服务的接受度，面向企业的线上安全运营服务或将迎来重大发展机遇。

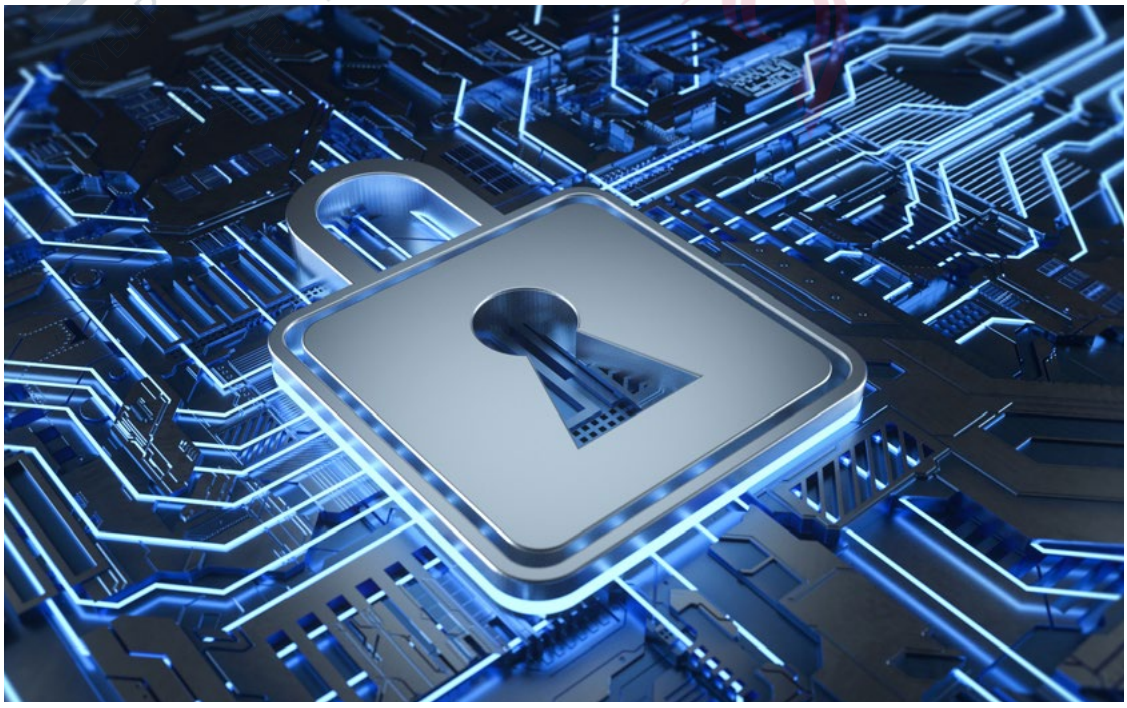
（4）后疫情时代数据安全和个人隐私保护将更受关注

疫情期间大数据技术广泛用于疫情防控，引

发社会对大数据滥用与用户隐私保护的担忧。同时，远程办公、远程教育、远程医疗、在线金融等非接触线上服务场景都使数据安全和隐私保护面临重大挑战，各类企业重要数据和用户个人信息面临遭黑客攻击导致数据泄露的严峻风险，内部威胁也成为数据遭窃取、损毁的重要风险来源，同时由于疫情期间各项信息服务上线较为紧急，安全措施不到位，导致数据安全形势更加严峻。后疫情时代，大量线上化需求将使数据安全和个人隐私保护获得更多关注，同时随着 2020 年《数据安全法》《个人信息保护法》等立法工作提上日程，数据安全将成为安全合规的重要需求方向，安全企业应加快提升数据安全技术能力，满足企业用户的数据安全需求。

（5）终端安全与云安全需求将进一步增强

远程办公场景中大量员工个人终端设备需接入企业内网访问企业内部资源及数据，无人机、无人车等非接触式配送使得物联网终端的安全需求激增，医疗机器人、服务机器人、无人工厂智能设备等终端大量暴露在互联网中，也面临网络攻击风险，这都使得对终端安全防护、监测与响应产品和服务的需求进一步增强。同时，线上服务和智能交互对云服务的需求激增，众多的业务系统被迁移上云，处于私有云、公有云甚至是混合云的复杂环境中。云内部署有众多的核心业务系统和敏感数据，倘若云内系统缺乏必要的安全性，将会存在重大的安全隐患和脆弱点。因此，非接触新经济的蓬勃发展对云安全提出更高的要求，将带来云安全领域的更多安全需求。



PART 6
参考文献

1、IMF. World Economic Outlook, April 2020[EB/OL]. https://www.imf.org/en/Publications/WEO/Issues/2020/04/14/weo-april-2020 — 02

2、国家统计局 . 2020 年一季度国内生产总值（GDP）初步核算结果 [EB/OL]. http://www.stats.gov.cn/tjsj/zxfb/202004/t20200417_1739602.html — 02

3、Frost & Sullivan. 中国视频通信行业概览 [EB/OL]. http://www.frostchina.com/wp-content/uploads/2019/05/shipintongxunhangyegailan.pdf — 06

4、艾媒咨询 .2019 上半年中国 K12 在线教育行业研究报告 [EB/OL]. https://www.iimedia.cn/c400/65829.html — 08

5、中国信通院 .2020 数字医疗：疫情防控期间网络安全风险研究报告 [EB/OL]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202003/P020200316481943325476.pdf — 14

6、腾讯安全、GeekPwn.2019 云安全威胁报告 [EB/OL]. https://baijiahao.baidu.com/s?id=1654084215802843 86&wfr=spider&for=pc — 15

出品方：

上海赛博网络安全产业创新研究院

技术支持单位：

杭州安恒信息技术股份有限公司