顶象 DING XIANG

CAICT 中国信通院

《业务安全白皮书》

——数字业务风险与安全

北京顶象技术有限公司

中国信息通信研究院云计算与大数据研究所

2022年6月

版权声明

编委成员

编委成员（排名不分前后）

陈树华、袁野、戴义正、卫斌、郭雪、孔松、李忆晨、宋文利、张晓科、张祖凯、史博、王路超、刘越强。

前 言

数字化时代下，数字经济飞速发展，企业数字化转型势在必行，业务愈加开放互联，关键数据、用户信息、基础设施、运营过程等均处于边界模糊且日益开放的环境中，涉及利益流和高附加值的业务面临多样的安全隐患，随时可能遭遇损失，进而影响企业运营和发展。

一方面，业务安全隐患形式多样，在电商、支付、信贷、账户、交互、交易等形态的业务场景中，存在着薅羊毛、刷单炒信、账号盗用、虚假账号、信贷欺诈、刷票刷流量、信用卡套现等欺诈行为；另一方面，欺诈行为日益专业化、产业化，利用自动化、智能化的新兴技术，以大规模牟利为目的网络黑灰产业不断发展，具有团伙性、复杂性、隐蔽性和传染性等特点。

业务安全产业结合各类技术，对用户行为风险、业务逻辑风险、网络攻击风险、数据泄露风险等进行智能评估，通过优质的业务安全产品和服务帮助企业有效抵御业务欺诈威胁，能够解决各个业务环节的安全问题，保证业务稳定和安全运行。

基于此，北京顶象技术有限公司与中国信息通信研究院云计算与大数据研究所联合推出《业务安全白皮书——数字业务风险与安全》，旨在帮助企业梳理数字化转型浪潮下将面临的业务安全风险以及相应的防控技术，为建设更完备的业务安全体系提供策略指导。

本白皮书对业务安全风险的发展态势和关键技术要求进行分析，梳理了重点行业业务安全建设时的关键点以及现阶段重要的政策指导，进一步明确了业务安全体系的建设流程和评估要素，帮助企业构

建更完备高效的业务安全能力体系。

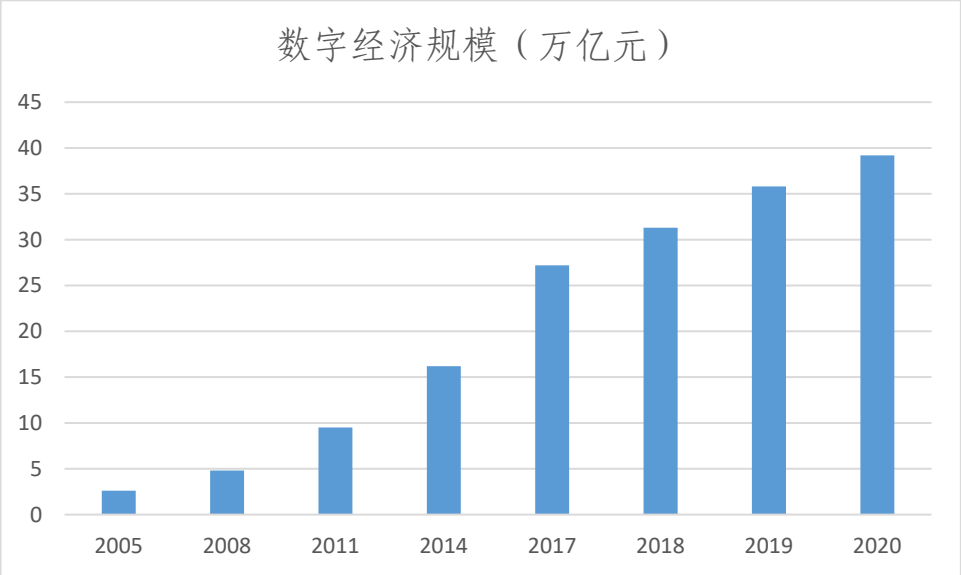
目 录

1、 构筑数字化业务安全防线，推动企业业务健康发展

1.1 数字化进程快速发展，数字经济成为经济高质量发展的重要支撑

随着新一轮科技革命和产业变革深入发展，数字化转型大势所趋。数字经济以数据资源为关键要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要素数字化转型为重要推动力，是数字时代国家综合实力的重要体现，是构建现代化经济体系的重要引擎，发展数字经济是把握新一轮科技革命和产业变革新机遇的战略选择。

一方面，我国数字经济规模发展稳中向好。“十三五”时期，我国深入实施数字经济发展战略，不断完善数字基础设施，加快培育新业态新模式，推进数字产业化和产业数字化取得了积极成效。《中国数字经济发展白皮书（2021）》显示，中国数字经济的规模已经由 2005 年的 2.6 万亿元，增长到 2020 年的 39.2 万亿元，占 GDP 的比重由 14.2%上升至 38.6%，已成为经济高质量发展的重要支撑。“十四五”时期，我国数字经济将转向深化应用、规范发展、普惠共享的新阶段。



数据来源：中国信通院

图 1 中国数字经济规模

另一方面，数字经济推动我国生产方式、生活方式和治理方式深刻变革。大数据、云计算、人工智能等技术加速创新，更快、更好融入网民生活发展全领域全过程，数字经济正在成为重组生产生活要素资源、重塑社会经济结构、改变全球竞争格局的关键力量，主要表现在几个方面：**一是**我国网络能力持续提升，持续深入推进网络提速提质，已建成全球规模最大的光纤和移动宽带网络，光纤化改造全面完成，累计建成 5G 基站 142.5 万个，5G 移动电话用户达到 3.55 亿户；**二是**互联网持续释放普惠效应，远程办公、在线医疗、社区团购等新业态持续发展，有效缓解了区域发展鸿沟问题，让更多人民不断从网络经济、社会和文化中获得利益和满足。中国互联网络信息中心（CNNIC）第 49 次《中国互联网络发展状况统计报告》显示，截至 2021 年 12 月，网络支付用户规模达 9.04 亿，网络购物用户规模达 8.42 亿，网络新闻用户规模达 7.71 亿，网上外卖用户规模达 5.44 亿，在线办公用户规模达 4.69 亿，在线医疗用户规模达 2.98 亿。同时，

数字政府迅速发展，截至 2021 年 12 月，我国互联网政务服务用户规模达 9.21 亿，占网民整体的 89.2%，各省市努力提升公共服务、社会治理等数字化、智能化水平，尤其在数字防疫方面发挥巨大潜在价值。

1.2 数字业务遭遇新风险，业务安全监管逐渐清晰化

1.2.1 数字业务风险多样，黑灰产不断演进

数字经济规模快速扩张，但发展不平衡、不充分、不规范问题较为突出，企业数字风险逐渐凸显。企业核心业务、关键数据、用户信息、基础设施、运营过程等均处于边界模糊且日益开放的环境中，涉及利益流和高附加值的业务面临多样的安全隐患，随时可能遭遇损失，进而影响企业运营和发展，企业迫切需要转变传统发展方式，加快补齐短板弱项，防范数字技术应用风险。

一方面，业务安全隐患形式多样。在电商、支付、信贷、账户、交互、交易等各种形态的业务场景中，存在着形式多样的薅羊毛、刷单炒信、账号盗用、虚假账号、信贷欺诈、刷票刷流量、信用卡套现等欺诈行为，结合自动化、智能化的新兴技术，对购物、金融、社交、出行、教育、游戏等业务造成极大威胁。

另一方面，欺诈行为专业化、产业化，黑灰产不断发展。2021 年出版的数字业务安全图书《攻守道——企业数字业务安全风险与防范》中，将黑灰产定义为：利用计算机、网络等手段，基于各类漏洞，通过恶意程序、木马病毒、网络、电信等形式，以非法盈利为目的规模化、组织化、分工明确的群体组织。黑灰产熟悉业务流程以及防护逻

辑，能够发现业务存在的漏洞，寻找牟利路径；同时，黑灰产能够熟练应用各类新技术，不断开发和优化各类攻击工具。据统计，目前网络黑灰产从业人员近200万之众，每年造成的损失达数千亿元。

1.2.2 国家高度重视业务安全领域发展，业务安全市场监管逐渐加强

随着数字时代经济的快速发展，企业业务面临的安全风险日渐凸显。近年来，各类数据泄漏、数据滥用、个人隐私侵害等安全事件更是层出不穷。如何在保障数字经济高速发展的同时，兼顾企业业务层面的安全性，已经引起了业内广泛的关注。

我国各级政府高度重视业务安全工作，出台众多业务安全方面法规，有效对业务安全领域的技术发展和应用创新提供支撑。业务安全政策的逐步实施，将带动政府、企业在业务安全方面的投入。以下为部分我国业务安全领域发布的重要政策法规：

表 1 我国业务安全领域政策法规汇总

发布时间	监管政策	监管内容
2017年6月1日	《中华人民共和国网络安全法》	第二十五条：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。 第四十二条：网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
2021年9月1日	《中华人民共和国数据安全法》	第二十七条规定：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络

		安全等级保护制度的基础上，履行上述数据安全保护义务。 第二十九条规定：开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。
2021年11月1日	《中华人民共和国个人信息保护法》	第五十一条规定：个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失。 第五十八条规定：提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务： （一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督； （二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务； （三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务； （四）定期发布个人信息保护社会责任报告，接受社会监督。
2020年2月	人民银行JR/T0068-2020《网上银行系统信息安全通用规范》	网上银行的验证码应随机产生，采取图片底纹干扰、颜色变换、设置非连续性及旋转图片字体、变异字体显示样式、交互式认证等有效方式，防止验证码被自动识别。 验证码应具有使用时间限制并仅能使用一次。图形验证码应由服务器生成，客户端源文件中不应包含验证码文本。 客户端程序应采取代码混淆、加壳等安全机制，防止客户端程序被逆向分析，确保客户端的敏感逻辑及数据的机密性、完整性。 客户端程序应保证自身的安全性，避免代码注入、缓冲区溢出、非法提权等漏洞。客户端程序应采取进程保护措施，防止非法程序获取该进程的访问权限，扫描内存中的敏感数据或替换客户端页面等。客户端程序应保证自身的安全性，避免代码注入、缓冲区溢出、非法提权等漏洞。
2020年3月	人民银行《移动金融客户端应用软件安全管理规范》	要求各金融机构加强客户端软件设计、开发、发布、维护等环节的安全管理，构建覆盖全生命周期的管理机制，切实保障客户端软件安全。其中，在身份认证安全中强调，若采用图形验证码作为验证的辅助要素，图形验证码应具有使用时间限制并仅能使用一次，图形验证码应由服务器生成，客户端源文件中不应包含图形验证码文本内容。 客户端抗攻击能力中要求，客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。 客户端应用软件安装、启动、更新时应

		对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。客户端应用软件如使用安全输入控件，该控件应具备抵御一定程度攻击的能力。
2021年8月1日	最高人民法院《最关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》	第二条规定：信息处理者处理人脸信息有下列情形之一的，人民法院应当认定属于侵害自然人人格权益的行为： （一）在宾馆、商场、银行、车站、机场、体育场馆、娱乐场所等经营场所、公共场所违反法律、行政法规的规定使用人脸识别技术进行人脸验证、辨识或者分析； （二）未公开处理人脸信息的规则或者未明示处理的目的、方式、范围； （三）基于个人同意处理人脸信息的，未征得自然人或者其监护人的单独同意，或者未按照法律、行政法规的规定征得自然人或者其监护人的书面同意； （四）违反信息处理者明示或者双方约定的处理人脸信息的目的、方式、范围等； （五）未采取应有的技术措施或者其他必要措施确保其收集、存储的人脸信息安全，致使人脸信息泄露、篡改、丢失； （六）违反法律、行政法规的规定或者双方的约定，向他人提供人脸信息； （七）违背公序良俗处理人脸信息； （八）违反合法、正当、必要原则处理人脸信息的其他情形。

1.3 业务安全有效应对新风险，保障数字产业健康发展

业务的健康稳定不仅是企业营收的重要保障，更是企业信誉和生存发展的决定因素。《IDC创新者：中国业务安全之反欺诈技术，2019》指出，中国数字化转型及数字化原生企业将长期面临业务欺诈的严峻挑战。

业务安全结合各类技术，对用户行为风险、业务逻辑风险、网络攻击风险、数据泄露风险等进行智能评估，抵御企业面临的业务层面风险。通过优质的业务安全产品和服务帮助企业有效抵御业务欺诈威胁，解决各个业务环节的安全问题，为业务的稳定、安全运行保驾护航。

作为安全服务中最贴近业务、最直接面向用户核心价值的安全维度，业务安全涉及基础网络安全、客户端安全、风控、大数据、人工智能等技术，更需要与金融、零售、航旅、能源、供应链、工业制造等行业的具体业务相结合。

2、 业务欺诈与业务安全始终处于博弈发展之中

2.1 业务欺诈特点分析

（1）团伙性

企业面临的数字业务风险越来越有计划、有预谋，业务欺诈分子彼此分工明确、合作紧密、协同作案，形成一条完整的产业链。他们熟悉企业各项业务流程，了解企业的需求、风控规则及业务漏洞，能够娴熟的运用移动互联网、云计算、人工智能等新技术进行业务欺诈操作。相较于个体欺诈，团伙欺诈行为更难侦测和识别，传统的反欺诈工具无法从全局视角洞察欺诈风险。

（2）复杂性

业务风险欺诈不断变化，手段更迭快速，新攻击手段对既有的防控措施进行了调整甚至免疫，传统措施不能及时对新风险进行识别和预警。

（3）隐蔽性

网络黑灰产对移动互联网、云计算、人工智能等新技术利用娴熟，风险欺诈手段日益复杂多变，数字化技术更便于业务风险团伙伪造、

消除源头、路径，让业务风险的源头更加隐蔽，让取证更加困难。

（4）传染性

数字化响应快，覆盖范围广，跨界、跨区域交叉特征明显，风险传播速度快，涉众广，传染性强，且多个业务风险叠加。当某个平台的业务上出现该风险，会被迅速复制到其他业务平台上。以往业务风险传染性以天计算，现在以分钟计算，传染性传播性大增。

2.2 业务欺诈典型技术分析

（1）盗取

利用各种技术和手段，在未经同意使用或批准的前提下窃取并牟利。例如，盗取个人敏感信息、用户账号、个人资金、有版权的图文视频报告等。

（2）伪造

利用各种技术和手段，进行非法制造、编造、变造身份信息、证件文件、数量进行牟利。例如虚假账号、刷量、虚假借贷、薅羊毛等。

（3）破解

利用各种技术和手段，破译并解开软件或设备的安全保护，并对软件或设备进行篡改，植入恶意代码，以实现牟利。例如，账号破解、App 破解、软件破解。

（4）劫持

利用各种技术和手段，修改软件、进程、服务等，将正常服务转移至非法链接，或强制使用者访问某些网站，以谋取利益。例如，人

脸劫持、链路劫持、验证劫持、服务劫持等。

2.3 业务欺诈常见场景分析

（1）薅羊毛

薅羊毛是黑灰产借助技术手段，批量抢夺原本属于用户的优惠和福利，并给平台或主办方带来经济损失。

2018 年 12 月，某品牌发起“注册新人礼”活动。凡通过 App 成功注册新会员，均可获得一份优惠券，凭借此券可以在国内门店免费兑换任意一份礼物。据监测显示，一天内，“羊毛党”就注册了近 40 万个虚假账号去领取该品牌的优惠。按照每张优惠券可以兑换一份 30-35 元的礼物估算，价值千万的特惠券被“羊毛党”们领走。

（2）刷单炒信

刷单炒信为一种不正当的竞争手段。店方通过假扮顾客或使用软件，用虚假违规的购物方式提高网店的排名和销量，为自身填写虚假好评的行为，来增加商品的信用度，从而误导用户购买选择，影响平台和市场管理部门统计与决策。

2017 年，某消费者在某大型电商平台上下单 2000 多人好评的牛肉，收货后却发现商品与宣传严重不符。该网店通过“刷单”制造虚假销量，进而炮制虚假好评，把一些质量不高的商品包装成“爆款”，从而误导消费者购买。

（3）刷量

刷量是利用程序自动化或组织人工等不正当手段制造虚假的数

量，实现重复投票、增加点击率、伪造读者阅读、提升榜单排名的造假行为。这类行为都破坏了公平、公正、公开的“三公”规则，给用户造成误导，影响客户决策，给企业数字业务带来经济损失，也影响企业品牌形象。

2020 年 11 月，某专场直播，某商家缴纳 10 万元开播费后，当天成交 1300 余台，直播后退款 1000 余台，退款率高达 76.4%。直播中出现大批多台退款单的刷单行为，导致店铺收到平台的虚假交易警告。

（4）虚假账号

虚假账号是黑灰产通过技术手段批量注册、并盗用他人信息激活认证的账号。不仅给企业和消费者带来财产损失，甚至给用户带来生命健康威胁。

2020 年 10 月，某粉丝沉溺于某明星账号的视频。此类账号为利用视频剪辑配音等技术手段做出的虚假账号。该账号骗取粉丝信任后，再向粉丝兜售虚假商品、骗取钱财等。

（5）恶意爬虫

恶意网络爬虫是按照一定的规则、自动地抓取网络信息的程序或者脚本。恶意爬虫爬取、盗用、盗取的爬取行为，不仅造成企业直接的经济损失，更消耗了平台服务和带宽资源。

2019 年 10 月，某网站被曝光“数据造假”。该网站的 2100 万条真实点评中，有 1800 万条是通过机器人从其他平台抄袭而来。在该网站上发现了 7454 个抄袭账号。

（6）团伙骗贷

团伙骗贷是指有预谋的一人或多个人，有组织有计划的虚构生产经营项目、交易、大额商品、抵押物，伪造各类资料，向金融机构申请经营贷款、消费贷款、抵押贷款，给金融机构直接带来资金损失。

2018 年 1 月，某派出所接到银行工作人员报警，称某贷款人在银行办理了购车信用贷款，但一直处于断供状态，且该贷款人的工作证明经系伪造。警方调查发现，这是一个专门骗取银行贷款的诈骗团伙。该团伙中，部分负责游说贷款人，让其同意向银行骗取车贷；部分负责伪造贷款材料，指导贷款人申请贷款；部分负责联系买家，快速将新车倒卖套现，共同构建起一条完整的“购车骗贷”犯罪链。

（7）养卡套现

养卡套现是指信用卡的卡持有人利用不法商户或刷卡设备制造虚假刷卡消费交易，以少量的手续费把信用额度全部转化为个人的现金。套现的方式有“他人消费刷自己的卡”，与商家或某些“贷款公司”、“中介公司”合作套现，或者是利用一些网站或公司的服务等套现。

2020 年 6 月，某地警方破获 7 处 POS 机恶意刷卡套现、非法支付结算等经营窝点，抓获 8 名涉案人员，查获 POS 机 157 台，银行卡 1200 余张和大量信用卡账单、POS 机账单。该团伙通过张贴小广告、发送短信、微信群内发布广告等方式向社会宣传信用卡代还、套现等业务。然后为他人刷卡套现、非法支付、结算等违法犯罪活动，收取高额手续费，牟取不正当利益，涉案流水资金高达 3000 余万元。

（8）洗钱

洗钱是一种将非法所得合法化的行为，主要指将违法所得及其产生的收益，通过各种手段掩饰、隐瞒其来源和性质，使其在形式上合法化。洗钱不仅包含将贩毒、走私、诈骗、贪污、贿赂、逃税非法收益通过各种手段使其合法化的过程，也包含将合法资金通过多种方式转变成以达到个人占有、逃避监管、转移到境外等目的。

（9）山寨 App

山寨 App 是指通过盗用制作企业数字业务信息、名称、图标等，诱导用户下载，却并不提供正常的服务，反而窃取用户通讯录、照片等隐私、资金等信息，给用户带来隐私风险与经济损失。

2020 年 6 月，我国在西昌卫星发射中心用长征三号乙运载火箭将最后一颗北斗三号组网卫星成功送入预定轨道。与此同时，多个 App 市场出现了带有“北斗”字样的导航，这些 App 不但功能缺乏，设计粗糙，且要求用户付费。诱骗消费者。

（10）虚假考勤

虚假考勤是破解入侵官方 App，通过屏蔽摄像头影像采集、拦截无线网络检测，并对 GPS 劫持，伪造虚假的 LBS 地理位置，已达到绕过核验、达成验证的目的。

2021 年 12 月，某职员每天无需到公司上班，在家中即可完成每日打卡并拿到全勤奖。分析发现，该职员使用的是一个黑灰产作弊工具。该工具能够屏蔽摄像头影像采集、拦截无线网络检测，并对 GPS 劫持，伪造虚假的 LBS 地理位置。在进行相关设置后，该员工输入自

己的工号，上传自己的照片即完成“考勤打卡”。该类工具在电商平台上也有大量销售，买家只需要花费少量费用即可以购买。

3、 构建数字业务的安全云，满足企业业务安全新需求

3.1 企业业务安全随着数字业务的发展产生新需求

安全是业务不可分割的一部分。数字业务不断发展，安全需要以业务为中心，企业基于业务需求和行业特征构建安全体系。

庞杂的业务需要专业的人才与服务。地域与行业的数字普及率有差异，业务的行业特征明显且差异大；各行业业务场景丰富，应用环境繁杂，安全需求多样。很多企业对业务风险与业务安全的认知不够，针对安全的投入不足、研发力量薄弱，迫使企业优化业务安全管理机制，引入更多拥有安全实战经验的业务安全人才。

通过情报与策略共享应对专业欺诈。黑灰产熟悉各项业务流程及漏洞，能够娴熟的运用各种新技术，而且有计划、有预谋。传统的安全手段主要基于以往的历史经验训练和指导设计，这导致已知的防控手段，难以防控最新的业务风险，无法从全局视角洞察欺诈风险。

单点防御失效亟需全网联防联控。攻防节奏加快、安全事件频发、欺诈手段复杂多变。企业单点防御作战能力无法应对全网随时出现的攻击，传统安全机制和运营思路也不适应新环境下产生的威胁。覆盖全网的联防联控安全机制，能够协调行业企业快速响应，并组建成一张业务安全大网，快速精准有效狙击新威胁。

3.2 构建全网业务安全云，为不同业务场景提供安全防护

基于数字业务的特性和挑战，企业需构建一个提供全流程防护，能够满足不同业务场景，拥有各行业策略且能够基于自身业务特点实现沉淀和更迭演进的业务安全云。业务安全云打通产业链上下游，链接各行业和业务的“信息孤岛”，拥有威胁感知、安全防护、数据沉淀、模型建设、策略共享等安全服务，提供全网迭代、覆盖不同行业和业务场景的策略，以及业务安全情报和风险数据，实现业务安全能力零启动、风险情报和策略持续共享，帮助企业实时响应的联防联控机制。

3.2.1 业务安全云架构体系

业务安全云架构体系主要包含云和端两部分。其中，“云”作为业务安全经验的沉淀和决策依据的大脑，提供实时的业务安全情报、具体业务场景的防御策略、反欺诈相关的风险数据；“端”主要是在全链路多环节的业务交互中，提供安全工具和平台，利用云上的经验，实时识别到业务风险，并及时进行防御和处置。

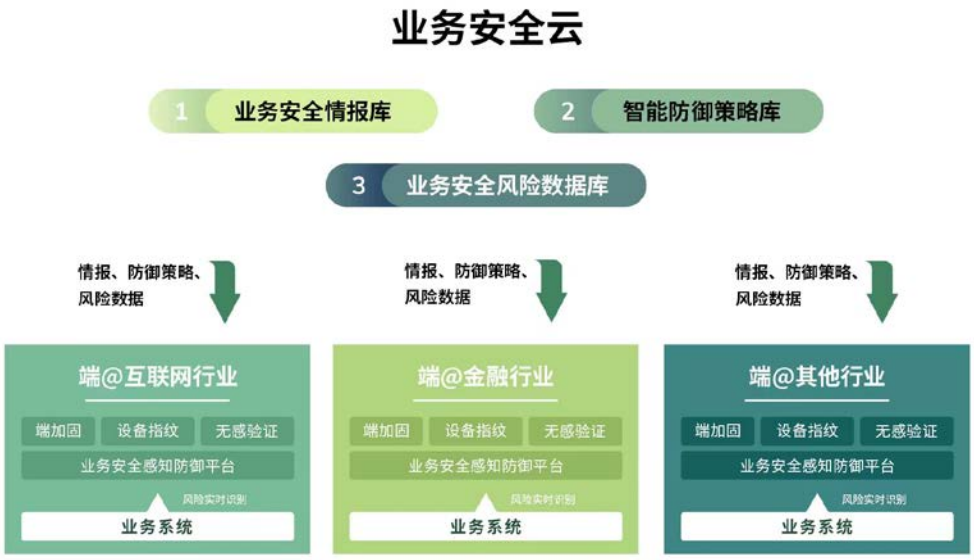


图 2 业务安全云架构体系

3.2.2 业务安全云技术特点

业务安全云应具备以下技术特点，来帮助企业应对日益繁杂的业务层面风险。第一为**行业情报共享，全网风险感知。**汇总行业风险动态，从攻击者的角度分析欺诈分子的手法、技术、流程，通过数据的整理挖掘和专家攻防对抗经验，融合提炼出的行业风险情报，为企业提供安全攻防对抗情报。第二为**丰富防御策略，实时云端迭代更新。**基于攻防实战中打磨的技术和实战经验，并与业务场景深度结合，形成行业通用策略和针对需求定制的专属策略，通过云端机制实现实时的迭代演进。并基于全网的风险态势变化，实现情报、策略和防控的措施联动。第三为**专家审查机制，一体化风险处置。**集成多个轻量化风险处置工具以及重量级业务风险处置能力，覆盖风险识别、防御处置、攻击还原、人工审查、关联分析、数据沉淀，能够为企业提供一体化闭环风险处置能力。第四为**风险数据沉淀，云端实时更新。**基于

风险的闭环管理、行为分析、关联关系挖掘，实现黑样本数据、风险行为特征的沉淀，并通过云端下发各业务安全体系，进一步提升整体风险防控能力。

3.2.3 业务安全云能力要求

设备真伪识别能力。覆盖手机系统版本、手机系统对权限的不断收紧、黑灰产各种对抗和篡改工具，保证一定采集率和采集数据不被篡改，需要具有较好的稳定性和安全性。并且要具有多端支持、风险标签输出、设备画像及关联分析的能力，以及稳定性/唯一性/安全性三个基本能力。

行为验证能力。需要具有行为验证数据采集保护、快速应对攻防、验证监控预警、体验偏好设置等能力。

风险感知能力。需要具有实时感知端上风险、实时防护处置、黑样本数据沉淀、攻击行为还原、风险监控预警等能力。

高性能实时计算能力。需要具有进行实时的风险感知、关联分析计算和处置的能力，并具备高性能的实时计算引擎，以实现低延迟、高并发的计算分析任务，支持多场景下多种实时指标的统计计算的能力。

轻量高效的策略执行能力。实时识别业务风险需要综合结合业务原始字段、衍生字段、实时计算的指标特征、在线模型预测服务和外部风险数据、名单数据等信息，给出最终的风险等级建议，这就要求策略的执行要高效，响应足够快的能力。同时，随着维护的规则、指

标、名单数据等数量增长，要避免对内存等资源的大量占用，在系统架构设计上要足够的轻量。

攻击还原能力。从业务请求到策略执行的整个过程中，涉及多个中间处理环节，需要完整的将执行流程记录下来，还原每一步判断过程和快照，除了决策结果有依据，还可以提升安全运营人员对风险情况查看的管理效率，需要拥有策略执行记录的能力。

3.3 业务安全云的典型应用

顶象防御云基于多年实战经验和技术产品，具有常用的技术工具、数万个安全策略及数百个业务场景解决方案，具有情报、感知、分析、策略、防护、处置的能力，提供模块化配置和弹性扩容，助企业快速、高效、低成本构建自主可控的业务安全防控体系。

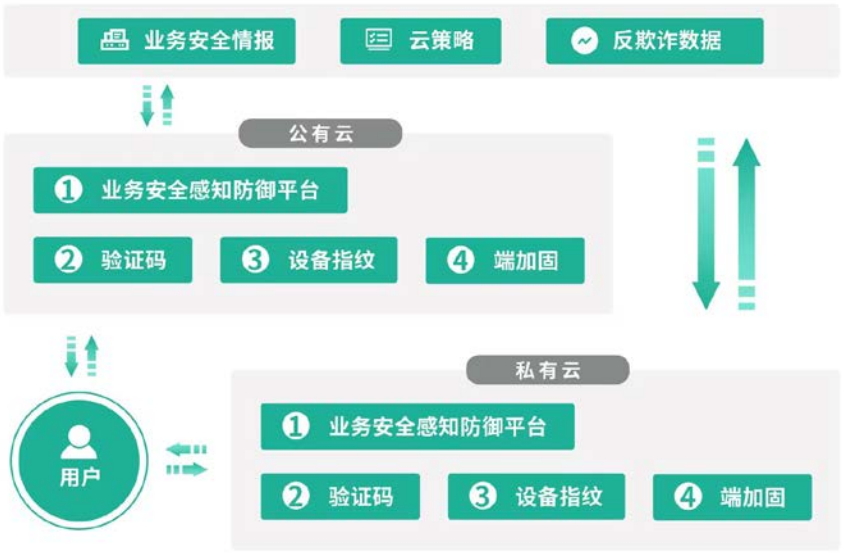


图 3 业务安全云典型应用

业务安全云主要包含 4 个部分，分别是业务感知防御平台、验证码、设备指纹和端加固。

第一部分为业务安全感知防御平台。通过对移动端 100+风险项及异常行为的分析识别，及时发现针对摄像头劫持、设备伪造等风险，并提供从风险识别、预警处置、黑样本沉淀的闭环管理。能够脱离决策引擎单独使用、轻量化、即时性强、数据开放能力高。

第二部分为验证码。无感验证基于设备、时间、访问频率、操作轨迹等信息，智能分析识别操作者的真伪，有效拦截批量撞库扫号、批量注册等机器风险行为，大幅提升使用体验和安全性。提供 13+种不同难度的验证、集成多种攻防对抗配置组合、10 秒内配置 60 秒即生效。

第三部分为设备指纹。设备指纹通过对上网软硬件生成唯一指纹信息，支持安卓、iOS、H5、公众号、小程序，可有效侦测模拟器、刷机改机、ROOT 越狱、劫持注入等风险。100%的唯一性、稳定性大于 99.99%、响应时间小于 0.1 秒、崩溃率小于 1/10000。

第四部分为端加固。端加固基于虚机源码保护专利技术，为安卓、iOS、H5、小程序提供全方位的安全保护，效防御调试、注入、多开、内存 Dump、模拟器、二次打包和日志泄露等攻击威胁。独有“蜜罐”功能、保护 Android 16 种数据和文件，提供 7 种加密形式，率先支持对 iOS 免源码加固。

4、 新形势下数字业务安全发展趋势与展望

4.1 业务安全整体将呈立体化、精细化、智能化、云化发展

（1）立体化

企业的数字业务不仅出现在固定场景，而是出现任何与用户接触的场景中。例如，用户不仅可以在专业的电商平台享受到网购服务，也可以通过银行、旅游、传统企业的网络平台进行网购；银行传统的零售端转向贸易链、供应链，利用线上服务优势将业务边界延伸，扩大了业务范围和服务边界。随着业务的场景化加强，不同场景下业务风险也有差异。

立体化防控就是基于数字业务的特点和属性，综合运用各种技术手段和工具，从多渠道、多角度、全流程进行防控，并与业务的上下游的安全体系形成协同，从而形成立体的防护体系，满足不同场景下业务风险变化，以有效防控数字业务安全。

（2）精细化

数字化业务呈现出个性化、差异化、定制化的态势，这就需要防控体系上更加精细化。针对不同生命周期的用户，同一生命周期的不同场景下提供差异化的防控措施，转变过去一对多的防控模式，精细化防控就是多对多的对应关系。

通过覆盖全流程的、立体防控体系，提供灵活、弹性的差异化防控策略和措施，以应对复杂场景下多变的业务风险，既能有效防范已

知风险和潜在的未知风险，保障业务安全，又不影响用户多元化体验和需求。

（3）智能化

数据的开发与应用是应对风险挑战的关键。企业在生产经营过程中积累了海量的数据金矿。利用大数据、人工智能等技术，切实增强数据应用能力，提升数据洞察能力和基于场景的数据挖掘能力，让数据发挥应用的价值，实现业务全要素、全过程、全方位的风险感知、风险监测，并对业务风险及其防控数据进行智能化分析、精准化预测和可视化管理。

（4）云化

不同业务场景、差异的网络环境、多层次的安全需求却又需要统一安全管理。云化的产品和服务能够多层次安全需求，能够适应不同业务需求弹性扩容、动态调整，更大幅简化用户在产品交付和运维上的工作，具有便捷、简化流程、降低成本等特点。对绝大多数企业而言，以云的方式交付网络安全的构建成为最佳选择。

同时，随着业务安全建设伴随着企业的终身发展，需要长期持续性的投入运营，并需要专业的运维团队保障后续改进升级，云化的服务能够良好满足沉淀、演进、创新的需求。

4.2 新技术与业务防控技术的组合应用助力业务安全创新升级

（1）虹膜识别

人眼虹膜纹理图像包括斑点、条纹、细丝、冠状、隐窝等细节视觉特征，这些特征人各有异、出生一年后几乎终身不变，因此可以采用图像处理和模式识别方法精确鉴定虹膜图像的人员身份。虹膜识别通过对比虹膜图像特征之间的相似性来确定人们的身份，其核心是使用模式识别、图像处理等方法对人眼睛的虹膜特征进行描述和匹配，从而实现自动的个人身份认证。

（2）声纹识别

声音中包含能表征和标识说话人声音特征，以及基于声音特征多建立的语音模型的总称。每个人说话时声音特征（音调、响度、音色）和发音习惯几乎独一无二，通过电声学仪器可测量并分析每个人的声波频谱都不尽相同，声纹是一种可用电声学仪器显示的携带言语信息的声波频谱，而声纹识别就是通过辨识声纹特征识别说话人身份的过程，在注册、登录、交易等，通过即时的比对分析声音，迅速确定操作人的身份，有效的防范业务欺诈等风险。

（3）生物探针

生物探针技术是指基于设备的加速度计、陀螺仪、重力加速度计、磁场传感器计等传感器，收集并记录用户使用设备时的数据，机型汇总分析，并进行画像，校验。通过获取的设备唯一标识，及时发现识

别发现设备的真伪与变化，防范设备存在的风险。

生物探针通过对操作者进行分析，如从某个开始行为事件直到结束事件进行全流程记录和分析的一种方法。了解操作人员操作环境的变化、行为的变化等，并将之作为识别业务交易风险等级的判断维度之一，通过对数据的分析和比对，了解操作者真伪，对海量用户的行为习惯形成精确了解。

（4）区块链

区块链是一种提供分布式数据存储、点对点传输、共识机制、加密算法的一种技术，理论上是一种新型的存储数据库，具有不可伪造、全程留痕、可以追溯、公开透明、集体维护等特征。

区块链能够良好实现风险与数据共享，打破信息不平衡，提供统一、丰富的信息，是核验识别更加精准；防范业务数据信息污染造假，优化数据质量，提高防控能力；让一切操作有记录且可追溯，防范业务数据信息污染造假，优化数据质量，提高风控能力；利用区块链技术，让业务各个环节、各个信息的关键动作上链，实现全流程操作可追溯，尤其是防止内控失去监督，尤其在防范内外勾结的风险欺诈更明显。

（5）机器学习

机器学习是目前大数据、人工智能领域的核心技术，被普遍认为是实现机器智能的主要途径，涉及线性代数、概率论、信息论、数值计算、算法理论等多个领域，通过数据处理、特征工程、模型训练和模型验证等工作程序完成机器学习模型的创建，并在模型成果的实际

应用中持续对其实施训练和调优，以不断提高预测和判断的准确性。

大数据是数字业务的关键因素，机器学习是大数据价值变现的重要工具。机器学习通过对数据的梳理、分析、提炼，并从数据中“学习”到有价值信息，进而辅助进行身份识别、风险校验，风险挖掘，关联关系图谱构建等，在反欺诈、风险监测、身份核验、趋势预测、模型构建等作用明显。通过对复杂多样的数据进行深层次的分析，更高效地利用信息，让业务越来越智能。

（6）人脸识别应用安全

人脸识别作为一种生物识别技术，被广泛运用于生产和生活领域，主要作用是实现在线身份认证，已成为登录、确认、申请、修改等业务环节中重要的验证技术。近年来，频繁出现人脸信息被冒用、人脸信息遭盗用、人脸识别应用遭劫持篡改等若干风险。

通过防范 API 接口被篡改劫持，保证输出效果、生成网络效果的真实；保障发现设备和系统端口、通讯的异常；及时预警，防止灌入虚假人像、混淆真假人像、库内人像信息被篡改；保障人脸数据存储以及传输的完整性、机密性等。此外，企业建立立体的风控体系，增强人脸识别从源头到应用的全链条预警、拦截、防护能力，提升人脸识别应用的安全性。

附录 1　顶象防御云典型行业应用实践

1.1 金融行业

某上市银行遇到了欺诈风险挑战。很多客户的资料被中介进行了包装伪造，银行审批中无法客观掌握该类客户的风险，加上高额中介费导致融资成本激增，发生群体性逾期甚至不良的风险极高。

基于顶象防御云，该银行建设零售业务反欺诈体系。实施后 1 个月内，识别信贷申请高风险客户 56 个，涉及潜在风险金额 231.5 万元；识别在异常资金交易高风险客户 1170 个，涉及潜在风险金额 6200.6 万元；识别信用卡养卡高风险客户 1000 个，涉及潜在风险金额 1700.3 万元。

1.2 电商行业

某电商平台是精选全球优质的商品。每逢平台网购日或商户促销，就有大批羊毛党进行疯抢优惠商品，给商户和用户带来诸多损失。

基于顶象防御云，该电商平台建设一套营销活动反欺诈体系。应用一个月后，90%的薅羊毛请求被精准识别且有效拦截，平台虚假注册降低 85%以上，极大化提升用户体验；发现并定位 5 万多个羊毛党、外挂秒杀、黄牛党账号；营销费用的投入，较体系部署前降低了 95%左右。

1.3 航空行业

某航空公司网站上出现大量虚假查询流量、爬票等，损害乘客合法权益，影响公司正常运营。

基于顶象防御云，该航空公司构建专属的航空专业务安全体系，应用后，B2C 平台上，99%的恶意爬虫请求被直接拦截；正常旅客的访问占比提高至 90%，访问效率提高 10 倍以上，用户体验满意度上升 21%；该航空公司每年向中航信应交查询费减少由 700 万降为 80 万，每年可为公司节省 89%的查询开支。

1.4 保险行业

2021 年底，“考勤打卡神器”刷屏网络。某保险公司员工，利用该工具在家就能实现到公司打卡，能够全额领取全勤奖。不仅破坏公司正常考勤秩序，给正常考勤上班员工带来负面作用，更消耗公司人力成本。

基于顶象防御云，某保险公司构建一套员工考勤反欺诈体系。部署后，当月发现 10000+名代理人通过劫持人脸信息进行虚假考勤打卡，拦截阻止超过 15 万次风险操作，为分公司挽回 500 万元的代理费用。

1.5 出行行业

某出行公司拥有 1 亿多用户，活跃用户超过 1000 万，作为典型的移动互联网公司，在市场拓展和老用户回馈活动中，遭遇到薅羊毛、

垃圾注册等风险，不仅用户合法权益受损，更影响业务正常运营。

基于顶象防御云，该公司建立一套营销拓展反欺诈防控体系。能够有效识别异常用户和违法操作，同时进一步提升 App 安全性，增强黑灰产破解攻击能力。应用后，当周发现并定位 10 万+异常风险设备，拦截 90 多万次异常操作，营销精准率提升 45%，营销成本降低 39%。

附录 2　中国信息通信研究院云计算与大数据研究所简介

中国信息通信研究院（以下简称“中国信通院”）是工业和信息化部直属科研事业单位，以“国家高端专业智库产业创新发展平台”为发展定位，在信息通信行业重大战略、规划、政策标准和测试认证等方面发挥了有力支撑作用。云计算与大数据研究所作为中国信通院设置的核心业务单元，旨在对云计算、大数据、人工智能、区块链等新兴技术展开深入研究，推进相关标准的制定以及生态圈打造，促进 ICT 技术加速与工业、金融、医疗、电力等传统行业的深度融合，助力我国产业互联网和实体经济发展。

云计算与大数据研究所从 2015 年开始开展数字化安全研究，创建“可信安全”品牌，聚焦软件供应链安全、业务安全、零信任、安全防护、数字基础设施安全、安全保险等领域，成为政府支撑、行业规范、用户选型与开发建设的重要参考。

顶象
DING XIANG

CAICT 中国信通院