内部发行 免费赠阅

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

把脉2023

第25期
2023 年 1 月

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

两种模式
模式随心选择

- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

多种形态
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现

- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享

首创“云地结合”模式

打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导

专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

2023 年最大胆的预测

网络安全行业习惯在岁末年初进行预测。在众多安全企业、媒体与研究机构的预测中，知名安全媒体 Dark Reading 编辑给出了最为大胆的预测：黑客针对关键基础设施的攻击可能引发一场世界大战。

国家资助、精心策划，针对国家电网、证券交易所的网络攻击，会不会如奥匈帝国王储弗朗茨·斐迪南大公被刺一样，成为第三次世界战争的导火索？这听起来似乎有些耸人听闻，一方面网络攻击者唯利是图居多，而攻击溯源也是难以达成一致的难题。但在全球地缘政治日趋紧张和出现分裂趋势的环境下，以网络攻击为借口对国家实施全面制裁，导致国家关系日趋恶化，进而引发战争，却并非不可能。

网络安全领域的人士在担心全面网络战争之时，来自网络保险机构的变化令人不得不担心日益恶化的安全态势：英国伦敦保险巨头劳合社 (Lloyd's) 发布公告，从 2023 年 3 月起，其网络保险产品将不再涵盖国家之间“网络战争”造成的损失。这意味着国家资助网络攻击的行为将日趋频繁，造成的危害也日趋严重，严重到网络保险公司无法承受的程度。

安全专家预测，2023 年可能是整个世界被勒索的一年。勒索攻击组织越来越大胆，他们不仅盯上为社会提供关键价值的大型组织，还有国家基础设施。2023 年网络攻击者可能会利用流行操作系统中的漏洞，对全球使用的软件进行供应链攻击，瞄准关键的国家基础设施。2023 年网络攻击不仅变得更加普遍，还会攻击云服务，甚至会入侵处于萌芽中的元宇宙，成为网络攻击者勒索赎金的目标。

也正是在这样的背景下，在全球经济遭遇困难的年份，网络安全的支出不减反增，出乎很多人的意料。根据 ESG 机构的研究，网络安全预计将成为明年企业 IT 支出的最大驱动力。随着网络攻击的日益普遍且损失严重，网络安全支出已成为所有市场条件下的必需品，改善网络安全状况成为证明技术投资价值的首要指标。

总编辑

李建平

2023 年 1 月 1 日

CONTENTS

目录

安全态势

月度专题

奇安资讯

《网安 26 号院》编辑部
主办 奇安信集团

总　编　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
攻防一线主编：魏开元
安全之道主编：张少波
奇安信人主编：孙丽芳
安全叨客主编：王梦琪
奇安资讯主编：陈　冲
研究报告主编：包世玉

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2122-L0058 号
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2023 年 1 月 26 日
发行对象：奇安信集团内部

政策篇

国内，行业网络安全政策标准不断完善，《直播类在线教学平台安全保障要求》《证券公司网络和信息安全三年提升计划（2023-2025）》《电力行业关键信息基础设施安全保护要求》陆续发布和征求意见；

国际上，美国又签署通过一项网络安全法案，名为《退伍军人事务部网络安全增强法案》，2022 年已累计通过近十项。

国内

工业和信息化部等十六部门发布《关于促进数据安全产业发展的指导意见》

1 月 13 日，工业和信息化部等十六部门发布《关于促进数据安全产业发展的指导意见》（以下简称《指导意见》）。《指导意见》提出，到 2025 年，数据安全产业基础能力和综合实力明显增强。数据安全产业规模超过 1500 亿元，年复合增长率超过 30%；建成 5 个省部级及以上数据安全重点实验室，攻关一批数据安全重点技术和产品；培育若干具有国际竞争力的龙头骨干企业、单项冠军企业和专精特新“小巨人”企业。到 2035 年，数据安全产业进入繁荣成熟期，大幅提升对数字中国建设和数字经济发展的支撑作用。

住房和城乡建设部发布《关于加快住房公积金数字化发展的指导意见》

1 月 10 日，住房和城乡建设部发布《关于加快住房公积金数字化发展的指导意见》（以下简称《指导意见》）。《指导意见》提出，到 2025 年，将基本形成全系统业务协同、全方位数据赋能、全业务线上服务、全链条智能监管的住房公积金数字化发展新模式，服务事项“网上办、掌上办、就近办、一次办”更加好办、易办。《指导意见》要求，全面落实安全管理责任，切实保障数据和网络安全，着力规范信息系统建设。其中特别指出，住房公积金信息系统的基础设施、应用系统、安全防护等建设内容，不得由同一企业全部承建。

中国证券业协会就《证券公司网络和信息安全三年提升计划》征求行业意见

1 月 6 日，中国证券业协会公布《证券公司网络和信息安全三年提升计划（2023-2025）（征求意见稿）》（以下简称《安全提升计划》），开始征求行业意见。《安全提升计划》从科技治理能力、科技投入机制等六个方面明确了提升方向和要求，并要求券商从组织领导、人才培养等六个方面建立保障机制。《安全提升计划》鼓励有条件的公司 2023 年至 2025 年三个年度，信息科技平均投入金额不少于上述三个年度平均净利润的 8% 或平均营业收入的 6%，其中网络和信息安全投入不低于信息科技投入总额的 7%。

电力信息化专业标委会就《电力行业关键信息基础设施安全保护要求》征求意见

1 月 4 日，中国电机工程学会电力信息化专业标委会公布《电力行业关键信息基础设施安全保护要求（征求意见稿）》，开始征求意见。该文件给出了电力行业关键信息基础设施安全防护总体原则，规定了风险识别、防护、监测预警、应急处置等主要防护环节的保护要求，适用于电力生产、电力传输、电力配送等相关企业。该文件提出，电力行业关键信息基础设施安全保护框架以顶层设计、整体防控、动态防护、协同联防、能力整合、智能运营为安全保护基础原则。

教育部发布《直播类在线教育平台安全保障要求》行业标准

2022 年 12 月 30 日，教育部发布《直播类在线教学平台安全保障要求》教育行业标准。该文件共分为六部分，给出了适用范围、规范性引用文件、术语和定义，规定了直播教学平台安全合规要求、直播教学模式安全功能要求及直播教学平台数据安全要求。该文件提出，直播类在线教学平台安全合规应符合网络安全等级保护、APP 安全认证、信息安全风险评估、商用密码安全性评估等要求。

反间谍法修订草案二审稿增加有关网络间谍的规定

2022 年 12 月 28 日，十三届全国人大常委会第三十八次会议对反间谍法修订草案二审稿进行分组审议。有意见提出，网络窃密、攻击、破坏是间谍行为新形态，建议增加有关网络间谍的规定。修订草案二审稿将为间谍组织及其代理人提供针对关键信息基础设施的网络安全漏洞等信息的行为规定为间谍行为。委员们认为，修订草案二审稿已比较成熟，建议尽快出台实施。

国际

美国国家档案与记录管理局更新联邦政府网络安全日志留存规定

1 月 11 日，美国国家档案与记录管理局发布 GRS Transmittal 33 文件，更新了联邦政府一般记录时间表（GRS）对网络安全日志留存的规定。新规则要求，全流量数据包（PCAP）至少留存 3 天，安全事件日志至少留存 30 个月，获商业授权还可留存更长时间。该规定是对美国第 14028 号总统行政令、M-21-31 备忘录的进一步细化。一般记录时间表（GRS）是联邦政府机构存留数据的实施文件，其在 2014 年首次对网络安全日志进行了规定。

NIST 发布《应用网络安全框架：太空运营地面部分》

2022 年 12 月 31 日，美国国家标准与技术研究院（NIST）发布了 NIST IR 8401《卫星地面部分：应用网络安全框架以确保卫星指挥和控制》文件。该文件为卫星指挥、控制和有效载荷系统的系统、过程和组件的分类提供了指导，以确定网络安全风险态势并解决空间部分管理和控制中的残余风险。其还为卫星指挥、控制和有效载荷系统的系统、过程和组件定义了理想的网络安全状态，并建立了明确且可重复的风险管理方法，以将实际网络安全状态提升到理想的网络安全状态。

美国总统拜登签署《2023 财年综合拨款法案》

2022 年 12 月 29 日，美国总统拜登签署《2023 财年综合拨款法案》（以下简称《法案》），涉及了一系列重要的网络安全项目。《法案》提出，为网络安全与基础设施安全局拨款 29 亿美元，较前一财年高出 3 亿美元，金额创下纪录。《法案》还提出，禁止政府手机上使用 TikTok，加强医疗设备网络安全，报告外国勒索软件攻击及其他网络攻击活动等。

美国总统拜登签署《退伍军人事务部网络安全增强法案》

2022 年 12 月 27 日，美国总统拜登签署《退伍军人事务部网络安全增强法案》（以下简称《法案》），要求退伍军人事务部对其关键信息系统进行独立的网络安全评估。《法案》提出，退伍军人事务部应制定时间表和预算清单，以解决评估期间发现的任何安全缺陷。退伍军人事务部秘书应在评估后的 120 天内向国会提交详细的报告与实施计划。2022 年期间，美国已通过近十项网络安全法案，包括《关键基础设施网络事件报告法》《优化网络犯罪度量法》《国家网络安全防范联盟法案》《联邦网络劳动力轮岗计划法》《州和地方政府网络安全法》《量子计算网络安全防范法》等。 安

栏目主编　王彪

事件篇

网络攻击已逐渐影响现实世界运行。澳大利亚地方消防局遭网络攻击，近百个消防站断网工作多天；加拿大最大儿童医院遭勒索攻击，系统一周多仍未恢复，医患人员工作与就诊受影响；英国邮政巨头因网络攻击临时中断国际寄件服务。

国内仿冒电子邮箱发起钓鱼邮件攻击事件频发！工业和信息化部发布预警

据工业和信息化部网站 1 月 11 日消息，工业和信息化部网络安全威胁和漏洞信息共享平台监测发现，近期利用仿冒电子邮箱发起的钓鱼邮件攻击事件频发。攻击者伪装成家人朋友、工作同事、合作伙伴等，发送特定主题的电子邮件，降低用户防备心理，诱使用户点击邮件中的恶意链接或者恶意程序，可能导致计算机、手机等终端设备被窃取信息或远程控制。为降低网络安全风险，工业和信息化部网络安全管理局提醒相关单位和公众用户提高网络安全风险意识，并给出了一系列防范措施建议。

网络攻击致使英国邮政巨头中断国际寄件服务

据 BleepingComputer 1 月 11 日消息，因“网络事件”导致的“严重服务中断”，英国邮件递送服务巨头皇家邮政（Royal Mail）宣布暂停国际运输服务。皇家邮政暂时无法将邮件发往境外目的地，已经寄出的国际邮件递送也面临延迟或取消。英国国家网络安全中心的发言人表示，“已知悉此次影响皇家邮政公司的事件，正在与该公司及国家犯罪局合作，以充分了解其影响。”

我国公安机关网安部门 2022 年共侦破 8.3 万起案件

据公安部网安局 1 月 9 日消息，2022 年，全国公安机关网安部门深入推进“净网 2022”专项行动，对严重危害网络秩序和群众权益的突出违法犯罪和网络乱象发起凌厉攻势。截至 2022 年 12 月底，共侦办案件 8.3 万起，其中网络诈骗赌博相关支撑黑产案件 3.1 万起、侵犯公民个人信息案件 1.6 万余起、网络黑号打码接码相关案件 1.1 万起、网络攻击案件 1300 余起、“网络水军”案件 550 余起、窃听窃照偷拍等案件 340 余起，抓获一大批犯罪嫌疑人，以实际行动维护了网络空间安全和网上良好秩序。

旧金山湾区地铁遭勒索攻击，轨交业已成黑客攻击重灾区

据 The Record 1 月 9 日消息，美国排名第五繁忙的重轨快速交通系统——旧金山湾区城轨交通系统（BART），在 1 月 6 日被 Vice Society 勒索软件团伙列入其官网“已勒索”名单。BART 首席通讯官 Alicia Trost 表示，他们正在调查该团伙窃取和发布的数据。她还说，“ BART 的服务或内部业务系统并未受到影响。”近年来，轨道交通行业已成网络攻击重灾区，全球出现了数起重大安全事件。

外媒披露：俄罗斯“冷河”黑客组织攻击美国核实验室

据路透社 1 月 6 日消息，俄罗斯黑客组织“冷河”（Cold River）曾在 2022 年 8~9 月攻击了 3 个美国核研究实验室 BNL、Argonne 和 LLNL。“冷河”组织通过钓鱼攻击为每个实验室创建虚假的登录页面，并向核科学家发送电子邮件以诱使他们泄露密码。研究人员无法确定攻击者为何针对这三个实验室，以及他们的攻击是否成功。多家安全公司采访显示，安全专家在 2016 年针对英国外交部的网络攻击中

首次发现“冷河”组织，此后陆续发现其还参与了数十起知名黑客事件。

华为鸿蒙系统去年修复近 300 个漏洞，超 3 成是高危漏洞

据 SecurityWeek 1 月 3 日消息，SecurityWeek 基于华为公司发布的月度安全公告统计显示，鸿蒙系统在 2022 年修复了 290 多个漏洞，其中有近 100 个影响第三方库的安全漏洞，20 余个“严重”级别漏洞，94 个“高”等级漏洞。这些漏洞可被用于实施拒绝服务攻击、远程代码执行、信息获取和权限提升等活动。根据 CVE Details 公布的数据，Android 系统在 2022 年修复了约 800 个漏洞，相比之下数量高出近两倍。当然，Android 系统的应用范围远高于鸿蒙系统，受到的安全研究和检查也更多。

加拿大铜山矿业因遭遇勒索软件攻击被迫关停矿场

据 BleepingComputer 2022 年 12 月 30 日消息，加拿大铜山矿业公司（CMMC）公布，因遭受勒索软件攻击，业务运营受到影响。此次勒索软件攻击发生在 2022 年 12 月 27 日晚，铜山矿业 IT 团队已通过预定义的风险管理系统及协议迅速做出响应。为了遏制此次事件，铜山矿业隔离了受感染系统并将其余部分关闭，并关停矿场预防影响进一步扩大，其余流程则转为手动操作。工控安全公司 Dragos 统计数据显示，2022 年针对工业系统的勒索软件攻击频繁发生。

加拿大最大儿童医院遭勒索攻击，一周仍未恢复系统

据 The Record 2022 年 12 月 27 日消息，加拿大规模最大的儿童医院多伦多病童医院（The Hospital for Sick Children）在 2022 年 12 月 18 日（星期日）遭遇勒索软件攻击。这家医院最初表示，攻击事件只影响到几个网络系统，对病患的正常护理仍在继续。但随后更新称，这是一起勒索软件攻击，部分临床和业务系统受到影响，已启动停机措施，所有系统需要数周时间才能恢复正常。此次攻击导致医生无法正常访问实验室和成像资料，病患的待诊时间也随之延长，处方的发放流程也受到了影响。

关基保护重要警示！能源巨头因遭受勒索攻击影响信用评级

据 SC Media 2022 年 12 月 22 日消息，南美洲国家哥伦比亚的能源巨头 Empresas Publicas de Medellin（简称 EPM）日前遭到勒索软件攻击，导致公司网站、移动应用、支付网关及内网运营中断。穆迪评级称，这起事件可能影响其信用水平。穆迪合作伙伴 BitSight 对 EPM 的最新网络防御实践评级为“C”。该事件为关键基础设施行业敲响警钟，提醒相关企业应制定行之有效的缓解措施与漏洞管理计划。

俄罗斯黑客劫持美国机场出租车调度系统搞黑产

据 BleepingComputer 2022 年 12 月 21 日消息，美国司法部日前公布的未密封起诉书显示，两名美国男子在俄罗斯黑客的协助下，于 2019 年 9 月至 2021 年 9 月期间入侵了肯尼迪机场的出租车调度系统。黑客们利用未经授权的访问权限创建了一项付费服务，能够将停留在肯尼迪机场的特定出租车添加至队列最前端，迅速为其派单。参与该计划的出租车司机需要向黑客们支付 10 美元，愿意向同行们推销这项服务的司机则能获得优惠，可以免费享受“插队”待遇。两名美国男子已被捕。

澳大利亚地方消防局遭网络攻击，近百个消防站断网工作多天

据 The Record 2022 年 12 月 16 日消息，澳大利亚维多利亚州消防与救援服务局发布声明称，由于遭受“外部第三方”的网络攻击，已关闭其运营网络并转为手动操作。此次网络攻击导致了“大范围 IT 中断”，影响到电子邮件、电话与紧急调度系统，消防部门关闭了整个网络以防止进一步蔓延。该州 85 个消防分站目前仍在照常工作，只是被迫使用无线电、寻呼机和手机来响应当地 000 报警呼叫。消防与救援服务局局长 Gavin Freeman 表示，预计系统关闭可能持续达四天。

漏洞篇

国产开源项目管理软件禅道被曝光远程命令执行漏洞，该漏洞技术细节已公开，经奇安信 CERT 研判其利用难度较低，建议客户尽快做好自查及防护。

禅道项目管理系统远程命令执行漏洞安全通告

1 月 13 日，奇安信 CERT 监测到互联网上公开禅道项目管理系统远程命令执行漏洞技术细节，未经授权的远程攻击者可利用身份认证绕过漏洞获取系统管理员权限，进一步组合后台命令执行漏洞最终可在目标服务器上注入任意命令，实现未授权接管服务器。目前，此漏洞技术细节已公开，奇安信 CERT 已复现此漏洞。经研判，此漏洞利用难度较低，远程攻击者可未授权接管服务器。鉴于此漏洞影响较大，建议客户尽快做好自查及防护。

Windows Backup Service 权限提升漏洞安全通告

1 月 12 日，奇安信 CERT 监测到 Windows Backup Service 权限提升漏洞 (CVE-2023-21752) PoC 及 EXP 已在互联网公开，经过身份认证的攻击者可利用此漏洞提升至 SYSTEM 权限。奇安信 CERT 已第一时间复现此漏洞。鉴于此漏洞影响较大，且 PoC 及 EXP 已公开，漏洞的现实威胁进一步提升，建议客户尽快做好自查，及时更新至最新版本。Windows Backup Service 提供 Windows 设备上的备份和还原功能。

PowerShell 远程代码执行漏洞安全通告

1 月 10 日，奇安信 CERT 监测到互联网上公开 PowerShell 远程代码执行漏洞 (CVE-2022-41076) 技术细节，并将此漏洞命名为“TabShell”。经过身份认证的远程攻击者，可利用此漏洞绕过沙箱限制，在目标机器上执行任意代码。目前，此漏洞技术细节、POC 及 EXP 已公开，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache Kylin 多个命令注入漏洞安全风险通告

1 月 3 日，奇安信 CERT 监测到 Apache Kylin 命令注入漏洞 (CVE-2022-43396) 和 Apache Kylin 命令注入漏洞 (CVE-2022-44621)。其中 CVE-2022-43396 是历史漏洞 CVE-2022-24697 的黑名单修复绕过，攻击者通过控制目标服务器 conf 的 kylin.engine.spark-cmd 参数来控制命令。CVE-2022-44621 是由于系统 Controller 未验证参数，攻击者可以通过 HTTP 请求进行命令注入攻击。鉴于这些漏洞影响范围较大，建议客户尽快做好自查，及时更新至最新版本。

Fortinet FortiOS 安全漏洞通报

2022 年 12 月 23 日，国家信息安全漏洞库（CNNVD）收到关于 Fortinet FortiOS 安全漏洞（CVE-2022-42475）情况的报送。成功利用漏洞的攻击者，可向目标设备发送特殊请求，从而远程执行恶意代码。FortiOS 多个版本均受此漏洞影响。目前，Fortinet 官方已发布新版本修复了此漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

对抗篇

国内攻防演习 12 月态势：哪些薄弱点最易被利用？

作者 | 奇安信安服团队

一、本月演习整体情况

2022 年 12 月，奇安信 Z-TEAM 团队共承接攻防演习服务 16 场，其中本单位自主攻防演习 16 场。

本月共承接攻防演习数量与上月对比呈上升趋势，与本年每月平均承接的攻防演习数量对比呈下降趋势（图 1）。

本月承接的攻防演习涉及金融行业、政府部委较多，此情况与本

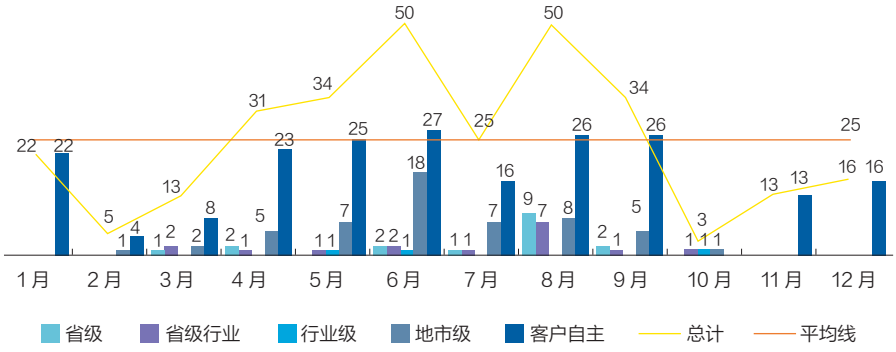


图 1：2022 年 Z-TEAM 承接攻防演习数量统计

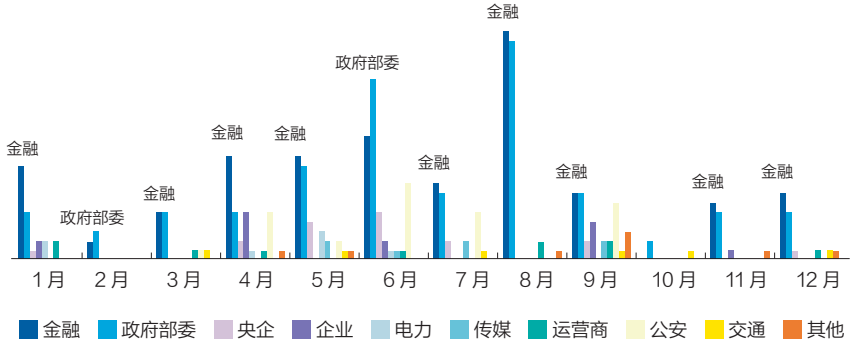


图 2：2022 年攻防演习涉及行业统计图

年承接攻防演习行业数据特征基本一致（图 2）。

本月攻防演习成果如（表 1）：

二、本月任务目标特点

本月攻防演习和评估任务覆盖行业比较分散，涉及目标包括政府部委、央企、交通、运营商、金融等行业。目前金融行业目标的安全形势较为严峻，在本月攻防演习中占比最高，为 44%（图 3）。

金融企业是不法分子关注的重点攻击目标，因此其对安全的要求也非常严格。关键行业属性，加上政策合规、业务保障、技术发展等因素，决定了金融行业攻防安全验证的必要性。网络攻防演练通过对金融行业的网络平台和信息系统进行全方位渗透测试，以发现可造成数据泄露、资产受损、系统篡改等风险的漏洞，帮助客户提早发现网络空间中的安全隐患，未雨绸缪。

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果分析，对不同的行业目标使用不同攻击手段，如交通行业外网突破的主要手段包括口令爆破和漏洞扫描利用等；政府部委行业主要是漏洞扫描利用和隐秘隧道外联等；金融行业外网突破的主要手段包括漏洞利用、钓鱼攻击和口令爆破等。各个行业使用的主要技术手段分布如图 4：

本月攻防演习服务中，攻击队使用的攻击手段主要有：漏洞扫描利用、钓鱼攻击、认证口令爆破、弱口令扫描、内网突破隐秘隧道外联技术等。

首先，漏洞利用主要集中在互联网侧业务系统和门户网站，以敏感信息泄露、未授权访问、组件反序列化、文件上传执行等漏洞扫描利用为主。

其次，对可利用漏洞入侵成功率较小的目标，采取钓鱼攻击进行迂回突破。目标内网则用口令爆破、VPN 仿冒接入、隐蔽隧道技术等手段实现内网横向拓展。

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	14	32	41	67	18	52	134	573

表 1：12 月攻防演习成果

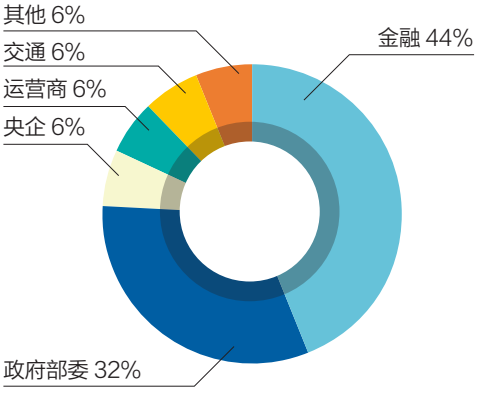


图 3：12 月攻防演习行业分布图

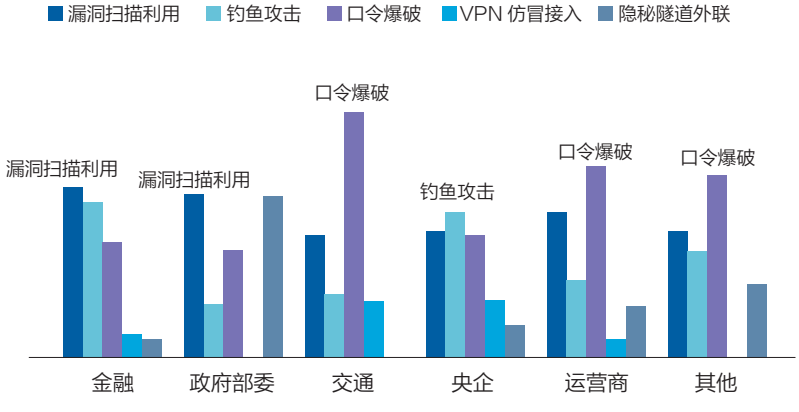


图 4：行业攻击手段分布图

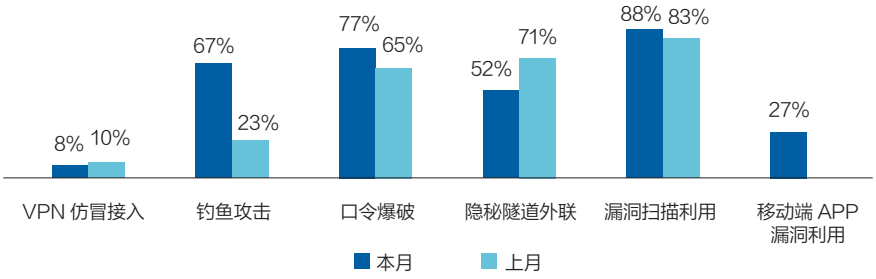


图 5：攻击手段对比图

整体攻击手段与上月对比，VPN 仿冒介入和漏洞扫描手段利用率基本趋同，隐秘隧道外联有明显下降趋势，钓鱼攻击和口令爆破有明显上升趋势。

因本月任务中金融行业攻防演习任务占比近半，通过此行业的演习数据分析发现，针对手机 APP 的漏洞扫描利用已成为非常高效的进攻手段。

这些漏洞之所以存在，主要是因为 APP 软件在开发过程隐藏了大量安全漏洞，如弱口令、权限绕过、注入漏洞等，以及 APP 使用了大量的存在安全风险的开源组件等。

攻击队可以通过手机 APP 作为“入口”，获取手机 APP 后台服务器访问权限，然后再开展内部横向移动攻击。使用的主要技术手段分布如图5。

四、典型攻击手段实现案例

众所周知，金融行业具备较强的互联网侧安全防护能力，通过传统 WEB 攻击方式已经很难取得正面突破。攻击方愈发重视社工钓鱼、供应链攻击及对移动 APP、公众号、微信小程序等的攻击。

结合奇安信攻击队攻防演练实战经验，本月攻击队以 APP 典型案例为主题，列举 2 个通过手机 APP 攻击取得突破口的攻击案例，并结合案例给出对应防护策略。

1、 案例 1：利用 APP 后台组件漏洞突破目标外网

孙子兵法有云：知己知彼，百战不殆。奇安信攻击队在对 A 银行的攻防演练中，每个攻击队员分工合作，充分利用自己的优势，将“知己”发挥到极致，并通过各种各样的方法尽可能多地搜集该银行暴露的资产信息和敏感信息等，以达到“知彼”的目的，为制定出更全面、更有效的攻击战略提供信息基础，获得先机。

从收集到的信息中筛选出可进行攻击的网站、系统、APP 等清单，攻击队员敏锐地发现，该银行的 APP 更新不久，存在多个版本，预计旧版本的砸壳成功率很高，于是将 APP 作为首要攻击入口。为了验证这一入口是否可行，攻击队迅速从应用商店获取了该银行的手机 APP 程序，考虑到最新版本 APP 的安全性，攻击队以旧版本的 APP 作为入口尝试进行突破。

攻击队从应用商店下载了多个版本的 APP，由于 APP 都是加密后的文件，逆向 APP 就得先砸壳。攻击队通过利用常见的砸壳工具对选中的 APP 进行自动化砸壳。果然如攻击队所料，旧版本的 APP 很快砸壳成功。对于砸壳成功的 APP，攻击队进行脱壳反编译代码操作，希望从代码中获得蛛丝马迹。经过对代码的审计研究后发现，在 com.cqtk.creditforload.sdk.a 类中找到如下 2 个接口地址：

http://x.x.x.x:18082/sdk-managerment

http://x.x.x.x:9501/SDKManagerment

攻击队对上面的接口进行调试后，发现后台使用了版本较低的 Struts2.0 组件，极有可能存在 Struts2 的历史漏洞。经过验证，漏洞存在，攻击路径可行。最终，攻击队成功利用 Struts2 反序列化漏洞突破该目标外网，越过防火墙，获取到手机 APP 后台组件管理服务器的控制权限，以服务器为通道暗度陈仓进入内网，进行横向渗透，不出所料，攻击队拿下目标靶机。

2、 案例 2：利用 APP 漏洞组合攻击潜入目标内网

在攻防演练中，资产的控制权始终是攻防双方的争夺焦点，互联网暴露面作为流量的入口，是攻击方重要

图 6：案例 1 攻击路线图

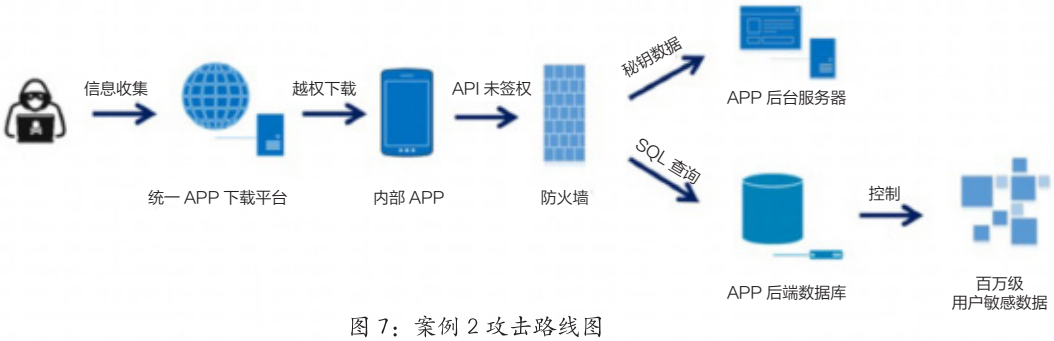


图 7：案例 2 攻击路线图

的攻击突破点。奇安信攻击队在对 B 银行的攻防演练中，决定兵分两路，第一小队以 VPN 为入口尝试进行正面进攻，第二小队以 APP 为入口尝试进行突破。

前期第一小队通过利用 OA 漏洞，获取到某位用户的 VPN 账号密码，但登录时发现还需要 APP 上的动态口令。于是，攻击队尝试绕过动态口令或对口令进行爆破，却发现 APP 的首次绑定需要验证在办公 IM 下发的验证码且不允许暴破，无法获得验证码，并且没有获取到该用户的硬件信息，不能伪造硬件特征码。最后，第一小队正面进攻失败。

而第二小队通过信息收集，发现该目标公网 APP 统一下载平台使用了不合理的校验规则，由此导致该平台存在越权漏洞，这意味着任意用户输入任意密码即可绕过鉴权，非法下载内部 APP。该发现使攻击队为之一振，立即以该平台作为突破口制定多种攻击路线。

路线制定后，经过攻击队员多次验证，选出其中最高效的攻击路线。首先攻击队利用某浏览器模拟手机下载多个内部 APP 进行本地逆向分析，逆向分析是信息安全行业的重要基础技术，攻击队员的经验越丰富，可发现的信息越多。

经过攻击队员的缜密研究，从数万行 APP 源代码中发现了多个堡垒机的内部接口，且部分 API 接口存在未鉴权漏洞。众多周知，未鉴权漏洞的危害可大可小，通常是由于系统配置不当、无认证或无健全的认证机制导致。攻击队测试发现，该漏洞允许任意用户调用 API 接口获取内部敏感数据，包括大量业务文档、密钥信息、员工领导个人敏感数据，其中涉及身份证号、姓名、住址、手机号、人脸等个人隐私信息。

大量的敏感信息为攻击队进入内部网络和开展攻击提供了便利。攻击队通过挖掘内部业务文档信息发现了关键内容，并利用所获取的密钥数据，突破防火墙的防护，最终获取 APP 后台服务器和内网多个业务服务器控制权限，进而可获取百万数量级的用户数据。

五、防守加固建议
——面向 APP 攻击的安全防护策略

1、案例剖析

互联网上存有多个版本 APP，不同版本 APP 在安全架构、组件安全、接口安全等相关技术管控措施上，呈现出版本越早的客户端 APP 相关配置暴露安全脆弱点的概率越大的特点；案例中攻击者利用新型攻击手段可对较早版本 APP 进行脆弱点识别及后续利用，成功迂回拿下现有系统的相关权限。

案例暴露问题：市场已发布的 APP 在版本管理、组件管理、API 接口管理上存在安全隐患。

2、防护策略

结合案例暴露出的安全隐患，需从管理、技术两方面提升 APP 安全能力。

管理上，要建立和完善 APP 版本管理体系，包括制定 APP 发布管理流程、版本市场留存管理流程、APP 安全检测管理要求等；

技术上，借助平台 + 人工，开展 APP 安全风险评估检测，包括但不限于：

- 梳理发布在互联网各类市场上的所有版本 APP；
- 管控下载通道，与软件市场协商对历史版本、二次打包 APP 下架；
- 检测通过工具 + 人工安全检测评估，全面发现 APP 自有发布平台、客户端、服务器及 API 接口等各层面漏洞和隐私合规风险，并提出整改建议使流程完整闭环。

不同行业、不同体量、不同安全能力阶段的客户，面临的 APP 安全威胁和隐患不同，需结合 APP 所处业务场景、监管要求等特点，定制更具体详细、更贴合实际、更满足监管、更符合实战对抗的 APP 安全解决方案。安

奇安信
新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结
从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

从法律法规、产业发展、技术趋势、安全威胁，
多角度预测 2023 发展趋势。

把脉 2023

产业回顾与展望：体系化创新引领网安产业发展

作者 | 奇安信集团产业发展研究中心

2022 年是网络安全产业在大环境的剧烈波动中不断发展的一年。我们从宏观环境、网安产业和细分赛道三个方面对网络安全产业 2022 年的表现进行了分析，并对未来进行了展望。

网络安全宏观环境具备长期向好的基本面。诸多不确定因素作用于网络空间，全球网络安全事件不断表明网络安全形势的不确定性，但安全需求及投入的增长的基本面是确定的。网络安全是国家安全的一部分，当前安全与斗争成为时代强音，网络安全防护对象越来越聚焦到数字经济的核心部分，产业趋向集中化发展。

网安产业发展具备足够的韧性。全球网安市场短期波动，增速放缓但仍好于其他多数行业，五年复合增速依然超 10%。中国网安产业布局完整，市场增速领先全球，增长潜力大，市场机会多点爆发，投融资 2022 年受宏观环境影响大，但创新依然活跃。

细分赛道体现创新活力。全球创新厂商聚焦热门创新赛道，着重核心技术与产品研发，填补头部厂商生态体系，我国网安创企赛道分布相对更为广泛，创业方向更加多样化，体现了我国产业特色与广泛的需求面。

2023 年预期网络安全产业将更加注重体系化创新，保障国家重大网络安全项目和工程的建设。国资和资本市场将进一步加大网络安全投入，持续助推网安产业发展。网络安全与产业应用的深度融合发展将成为带动未来网络安全产业的关键增长点。

1. 宏观环境：变局环境下的网络安全新格局

2022 年是国际形势格外动荡的一年，诸多因素反映在网络空间，引入了不确定因素。这些因素对网安行业的影响叠加对冲，行业总体保持平稳发展。二十大的胜利召开为我国网安产业长期稳定发展指明了方向，我国网络安全产业将走上中国式现代化之路。

（1）网络安全产业受国际局势的影响叠加对冲，总体保持平稳发展

全球政治、经济、军事、民生全方位的不确定性，使得安全需求急剧增加。俄乌冲突带来全球和平发展的不确定性，货币政策重大调整反映经济的不确定性，日本前首相遇刺折射社会治理的不确定性，防控政策重大调整疫情走向仍有不确定性。诸多不确定因素作用于网络空间，全球网络

安全事件不断表明网络安全形势的不确定性。

国际局势的不稳定对网络安全的影响是双方面的。一方面，安全形势不稳定对数字产业造成重大影响，使得可用于数字化乃至网络安全的资金捉襟见肘，相应的产业投资也急速萎缩。另一方面，全球政治、经济、军事、民生全方位的不确定性使得安全需求急剧增加，各国建设网络安全防护能力的需求更加迫切。两方面的影响产生对冲，使得网络安全产业在剧烈波动中总体保持了较为平稳的发展

安全是网安行业的根本逻辑。这是俄乌网络战给我们的启示。2022 年 2 月以来，俄罗斯对乌克兰开展特别军事行动，网络战首次成为军事行动的一部分，并进行了激烈较量，网络战与传统武装行动相互交织的“混合战”正日益成为国际冲突的常态。网络安全是国家安全的一部分，其安全属性高于网络属性的网络战时代已经来临，攻防能力是关键。网络战新模式下必须建立国家级的应对网络战的攻防能力，保卫网络空间国家主权、保护关键基础设施安全运行、保障数字化产业健康发展。

（2）二十大的胜利召开为我国网安产业长期稳定发展指明了方向

当前国际、国内形势风云变幻，安全与斗争成为时代强音。通过二十大报告关键词，对比十九大我们可以看出：安全、斗争、科技均有大幅度的增长；创新、经济、改革和市场则有不同幅度的下降；网络安全是国家安全的重要组成部分，也是数字化时代斗争的前沿和焦点；在传统热战不会轻易爆发的现代社会，通过网络进行试探、对抗和打击已经成为趋势；在现代战争中，网络攻防同样伴随着军事行动广泛开展。

经济建设全局统筹，网络安全趋向集中化发展。未来十年我国经济建设呈现全局统筹的格局：着力振兴实体经济，推动制造业高质量发展，促进数字经济和实体经济融合发展，加快建设现代化基础设施体系。网络安全服务于经济建设，将呈现集中化发展的趋势：网络安全防护对象越来越聚焦到数字经济的核心部分，即关键基础设施和其承载的数字化业务；数字化业务数十万亿的产业规模，和对重大网络安全事故零容忍的要求，在网络安全领域呈现高对抗性的趋势下产生极大的潜在需求，这种需求将长期持续释放，驱动网络安全产业继续实现高增长；网络安全产业的集中化发展并不违背国际产业发展规律，全球网络安全产业也呈现集中化发展的趋势。Momentum 的数据显示，2022 上半年全球网安市场并购总金额为 1026 亿美元，同比增长 160.41%；网络安全产业集中化发展有利于协同创新，网络安全是全球独角兽创企最为密集的领域之一。但是受宏观环境负面影响，2022 年中国网安行业一级市场总共有 92 家网安企业发生 109 笔融资（不含 ipo、二级市场等），融资金额为 66 亿元人民币。

机构调整：中央成立委员会统筹管理网信工作。领导小组一般是议事

> 网络战与传统武装行动相互交织的“混合战”正日益成为国际冲突的常态。
> 网络安全是国家安全的一部分，其安全属性高于网络属性网络战时代已经来临，攻防能力是关键。

协调机构，属于一种“阶段性工作机制”，非严格意义上的实体性组织；委员会一般是成建制的固定机构，是为完成一定的任务而设立的专门组织；中央网络安全和信息化委员会成立，职能更加全面、机构更加规范，运行更加稳定，网信工作组织更加健全。中央网信领导小组上升到委员会标志着网信工作的长期性、稳定性：设立委员会有利于整合资源，实现全覆盖，避免出现盲区和空白；领导小组变委员会，意味着网信工作定位为新时期涉及党和国家事业全局的重大工作；体现在“统一部署”上更有层次和力度，在“执行力”上更加有序和高效。

合规合法驱动：网安法规体系快速细化，逐步落地。2022 年我国快速推进《网络安全法》《数据安全法》等法律落地。为配合国家战略，2022 年我国制定了 190 余项配套措施：政策法规 49 项，行业规章 33 项，地方政策 48 项，技术标准 34 项，产业报告 27 项。2023 年网络安全领域将基本形成较为完善的法律法规落地执行体系，行业驱动作用日益显著。

体系化创新：全国一体化政务大数据体系打造数据安全样板。全国一体化政务大数据体系包括三类平台，三类平台为“1+32+N”框架结构：“1”是指国家政务大数据平台，“32”是指 31 个省（自治区、直辖市）和新疆生产建设兵团，“N”是指国务院有关部门的政务数据平台。体系建设需要管理机制、标准规范、安全保障三大支撑。数据治理与数据安全业务机会包括多个方面，数据目录能力：数据资源盘点服务；数据目录系统建设。数据治理能力：数据质量咨询服务及系统建设。管理机制及标准规范能力：数据权责咨询服务及系统建设；数据标准管理咨询服务及系统建设。安全保障能力：数据安全治理咨询，分类分级咨询；数据安全分类分级系统、监测系统、数据安全保护系统（脱敏、防泄漏、加密、隐私计算）等。

> 未来十年我国经济建设呈现全局统筹的格局：
> 着力振兴实体经济，推动制造业高质量发展，
> 促进数字经济和实体经济融合发展，
> 加快建设现代化基础设施体系。
> 网络安全服务于经济建设，
> 将呈现集中化发展的趋势。

（3）未来道路：我国网络安全产业将走上中国式现代化之路

中国式现代化的重要特征和本质要求：中国式现代化，是中国共产党领导的社会主义现代化，既有各国现代化的共同特征，更有基于自己国情的中国特色。我国将从构建新发展格局与高质量发展、科教兴国、全过程人民民主、全面依法治国、文化自信自强、民生福祉、绿色发展、国家安全、国防军队建设、“一国两制”与祖国统一、构建人类命运共同体、全面从严治党等 12 个方面，全面推进中国式现代化。

我国网络安全产业服务于我国政治、经济建设和产业发展需要，随着网络安全工作的逐步深入和细化，紧跟国际趋势的同时呈现自身特色：龙头企业做大做强，带领网安产业走向中国式现代化：中国网络安全企业的营收规模快速增长，龙头企业奇安信已经跻身全球前十之列。与 2020 年相比，中国厂商营收排名有了较大提升，取代传统美国头部网安厂商的位置。网络安全生态走向中国式现代化之路：我国以基础设施和行业应用为核心的网络安全需求更为复杂和碎片化，需要深耕行业，深入了解行业业务内在的安全需求，由此也推动我国网络安全产业向行业纵深发展，具备更广阔的市场空间。网络安全创新走向中国式现代化之路：我国长期跟随美国等发达国家开展网络安全建设，产业细分领域多且主要热点细分领域与国外基本一致。随着产业发展，我国网安创新方向更为多样化，符合我国产业特色的网络安全创新方向和创新企业大量出现，为产业持续高速增长注入新的动力。

2. 网安产业：短期波动不影响长期向好的基本面

全球网安市场短期波动，但基本面没有改变。在新冠疫情、俄乌冲突、高通胀压力等不利因素的冲击下，2022 年全球经济普遍面临严重的下行风险，经济增速放缓程度高于预期。国际货币基金组织（IMF）在其发布的《世界经济展望》中预计：2022 年经济增长率将由 2021 年的 6% 下降到 2.3%，2023 年则将进一步放缓至 2.7%。受全球宏观经济负面影响，2022 年全

球网络安全市场的预期增速也将降至2020年以来最低点，但是维持了高于7%的增长水平。根据Gartner今年三季度末公布的数据：2021年全球网络安全市场规模达1577.5亿美元，同比增长14.25%；2022年，全球网络安全市场规模预计增长至1691.56亿美元，但是增速同比放缓到7.23%；2023年后将进入复苏期，到2026年市场规模将达到2617.37亿美元，五年复合增速（2021-2026）为10.7%。

（1）全球网安产业碎片化明显，呈现竞争型市场态势

美国Momentum Cyber发布的2022年全球网络安全行业全景图显示：行业一级安全分类有18个，二级安全子分类有39个。Statista的数据显示，在2020年第一季度，全球网络安全市场占有率前4的厂商共计拥有28.2%的市场份额，依照美国经济学家贝恩和日本通产省对产业集中度的划分标准，全球网络安全行业CR4为28.2%，属于竞争型市场。碎片化的特征降低了网络安全行业的市场集中度，从而限制了网络安全厂商成长的空间，因此目前无论是国际网络安全市场，还是中国网络安全市场都没有绝对强势的行业巨头，创业公司有机会脱颖而出。

产业格局：中国网安产业布局完整，技术覆盖与美国接近。中美网安产业布局基本接近，中国在细分领域安全厂商精细化不够。美国网安厂商更多是专注核心技术打磨，而在中国由于2B市场的特点，国内网安厂商为了提供整体安全方案，追求布局完整安全产品线，通常走自研+OEM路线。中美热门领域相对一致：云安全、数据安全与隐私保护、物联网安全、应用安全、威胁检测与防御、自动化模拟攻击等领域。中美网安企业在细分领域的分布数量存在差异；美国安全企业在云安全领域分布数量很多，但在车联网、智慧交运领域（航空、铁路、航海）布局的安全公司数量不多。中美网安企业在商业模式上存在差异：美国领先网安厂商积极拥抱基于SaaS的服务订阅模式，持续为业务收入增长提供驱动力，而国内网安企业仍处于服务化转型探索和客户习惯培养阶段，我国网络安全服务市场仍有较大的发展空间。

产业布局：2022年我国网安产业布局进一步细化。根据CCIA产业联盟发布的《中国网络安全产业分析报告（2022年）》显示，2021年中国网络安全行业的CR4是28.07%，与国际市场相同也属于竞争型市场。安全牛2022年中国网络安全全景图将行业一级赛道划分为14条，二级赛道细分为94条；其中二级细分赛道共计收录2609项，较去年发布的第八版增加486项。

（2）中国网络安全市场增速持续领先全球，企业营收较为稳定

中国网络安全市场五年复合增长率超过 20%，2021 年全球网络安全市场规模为 1354 亿美元，到 2025 年达到 2233 亿美元，其中，美国市场 1031 亿美元，中国市场 215 亿美元。美联邦政府一直保持高强度网络安全投入，将网络安全认定为数字化发展的“命门”；美国白宫公布的 2021 财年预算，其 IT 总预算为 922 亿美元，其中网络安全产业预算为188亿美元，占 IT 总预算 20.4%，比 2020 财年高出 14 亿美元；根据 IDC 统计数据，我国网络安全投入占信息化的比重仅为 1.87%，比例不及美国水平十分之一，也低于全球 3.74% 的平均水平，增长潜力巨大。

2022 年网安头部企业市值受宏观环境影响较大，但营收依然实现较为稳定和快速的增长。从营收方面看，2022 年上半年中国网络安全头部 10 家厂商营收总体增长，营收达到 100 亿元。奇安信、安恒、山石网科等头部厂商营收保持了较快的增长势头，5 家企业增速超 30%；奇安信进入全球前 10，另有 3 家企业进入前 20。从市值方面看，2023 年首个交易日相比 2022 年多数呈现下降，资本寒冬尚未过去。

潜力巨大：中国网络安全产业增长潜力超美国。中国 2021 年 GDP：114 万亿元（17.5 万亿美元）。数字经济：46 万亿元（40.7%）7.1 万亿美元。网络安全：（0.13%），600+ 亿元（典型）/2000 亿元（广义）。美国 2021 年 GDP：23 万亿美元，数字经济：13.6 万亿美元（59%），网络安全：600+ 亿美元（0.44%）。广义网络安全产业包括典型网络安全产业，垂直行业、运营商、云服务企业等主体的网络安全业务，以及区块链、密码，车联网等网络安全融合创新业务。2021 年中国网络安全产业规模与美国相差 1 个人民币与美元汇率，在数字经济中占比不足美国的 1/3。中国网络安全服务于数字产业与基础设施，这些领域有更高的网络安全需求，增长潜力超美国。

> 中国网络安全市场五年复合增长率超过 20%，
> 2021 年全球网络安全市场规模为 1354 亿美元，
> 到 2025 年达到 2233 亿美元，
> 其中：美国市场 1031 亿美元，
> 中国市场 215 亿美元。

（3）投融资总体向好，2022 年受宏观环境影响较大

2022 年中国网安行业一级市场投融资受新冠疫情冲击和宏观经济负面影响，2022 年中国网络安全非上市投融资金额和事件出现明显下降。根据我们从公开信息的不完全统计，2022 年国内网络安全非上市企业披露的融资事件有 109 起，同比下降 26.85%，总金额为 66.23 亿元，同比下降 62.64%，共涉及 92 家网络安全企业。整体来看，2018-2022 年中国网络安全非上市投融资金额总计达 477.51 亿元，除了 2022 年受宏观环境负面影响较为强烈，2018-2021 年中国网安行业非上市投融资金额始终保持高速增长，平均增速约为 55.37%。

2022 年投融资融资热门赛道相对集中，创新领域多且活跃。从细分赛道来看，我国网安创新热门赛道较多，16 个赛道均保持较高的融资热度。从热门赛道看，数据安全（含隐私计算）、威胁对抗与管理、工控安全、云安全、

软件供应链安全、身份与访问安全、密码安全、安全管理与运营、物联网安全、业务与应用安全一级市场投融资活跃度较高。

2022 年投融资分布呈现集中化态势。阶段分布集中化：2022 年投资机构对网络安全一级市场的早中期项目关注度较高，早中期项目占比超过 67%。时间分布集中化：2022 年网安一级市场上半年融资热度较高，总计有融资事件 68 起，约占全年的 57.80%，其中，3 月融资事件最多。地域分布集中化：2022 年中国网安一级市场融资事件共有 109 起，其中北京地区有 51 起，占总样本的 46.79%，北京作为网络安全产业龙头，优势依旧明显；深圳、上海、杭州和南京在网络安全行业的区域影响力也在逐步增强。企业成立时间集中化：2022 年融资的网安非上市企业成立年限区间位于 1999-2022，其中 2015 年以后成立的企业（含 2015）有 75 家，占总样本容量的 81.52%。92 家网安企业的平均成立年限为 6 年，而成立超过 10 年的企业仅有 11 家，行业不断涌入新兴力量。

2022 年投融资热门赛道相对集中，创新领域多且活跃。从细分赛道来看，我国网安创新热门赛道较多，16 个赛道均保持较高的融资热度。从热门赛道看，数据安全（含隐私计算）、威胁对抗与管理、工控安全、云安全、软件供应链安全、身份与访问安全、密码安全、安全管理与运营、物联网安全、业务与应用安全一级市场投融资活跃度较高。

3. 网安细分赛道：方向更加多样化，热点趋于集中

2022 年网络安全产业创新活力依然强劲，方向更加多样化，热点趋于集中。国外优秀创企聚焦热点赛道，技术产品不断演进；我国网安创企紧跟国际先进趋势，结合国情持续创新。

（1）国外优秀创企聚焦热点赛道，技术产品不断演进

创新沙盒十强赛道分布更趋集中，纵观近五年创新沙盒 10 强企业赛道，网安热门细分领域主要包括：云安全 12 家，数据安全 9 家，身份安全 8 家，供应链安全 8 家。其中云安全占比 24%，数据安全占比 18%，软件供应链安全占比 16%，身份安全占比 16%。5 年 50 家 10 强企业中，四个热门赛道创企共 37 家，占比达 74%；其中云安全是最热门的赛道，占比达 24%，其次是数据安全，占比 18%。

国外优秀创企聚焦热门赛道、填补生态位。创新厂商聚焦热门创新赛道：主要集中在云安全、数据安全、身份安全和软件供应链安全领域，与头部企业热门领域基本一致；创新厂商着重核心技术与产品研发：与头部厂商形成良好互动，填补头部厂商生态体系，并有大量创新企业被头部厂商收购。

国外优秀创企网安创新的演进线路稳中有进，影响创新路线的因素主要包括热门应用、热点事件、创新趋势等。2018 年身份安全热度最高，随着零信任架构的广泛认可和应用，身

份安全有了新的发展。基于零信任的身份认证、边界控制、访问控制等技术有了全新的突破，从而成为年度热点。2019 年云安全热度最高，随着公有云的行业应用在美国市场大规模普及，云安全再度成为热点。此时的云安全不仅仅是云基础设施的安全，更包括云上业务、数据、身份和供应链的整体安全，以及基于云的订阅服务等。2020 年软件供应链安全最为热门，随着数字化产业发展，软件供应链越加复杂，基于供应链传导的网络攻击成为新的严重威胁。此外疫情导致的网络办公击破了传统的软件供应链业务模式，新的安全需求急剧增长。2021 年数据与隐私安全最热，如同新冠疫情、贸易战对全球社会和经济带来的重大风险一样，当前全球网络风险正在向着多样化、复杂化且难以预判的方向发展。网络安全防护的重点从抵御攻击转变为保障业务，数据与隐私安全成为重中之重。2022 年云安全再度归来，但演进到云原生安全。云安全是创新沙盒长期以来的热点赛道，但每年在不断演进。从云基础设施安全，到云应用安全，再到基于云原生的业务安全。数字化业务全面上云的时代，基于云原生的安全能力正在快速的扩充和完善，具有广阔的空间。

（2）我国网安创企紧跟国际先进趋势，结合国情持续创新

从 2022 年安全创客汇 50 强企业取样来看，中国网安创企赛道分布特点：①创新赛道多：50 家企业分布在 22 个细分赛道，反应网络安全行业已经进入赛道细分的时代，创新企业专注于一个或几个细分赛道更容易做出好的成果。②热点赛道与国外基本一致：软件供应链安全、数据与隐私安全、SASE 与零信任等是本次创客汇聚焦的创新赛道，共有 19 家企业，占比达到 38%，热点赛道方向与 RSAC 等体现出的国外创企方向基本一致。③我国产业特色逐渐显现：网络安全服务于数字产业，我国数字产业的蓬勃发展催生了具有我国产业特色的网络安全创新领域，如 5G 安全、汽车安全、工业互联网安全等。

我国安全创客汇 50 强企业成长性也有一定特色：①从成立时间看，50 强企业分布的高峰有两个：第一个高峰是 2021 年，新成立的创新企业崭露头角，冲劲十足；第二个高峰是 2018 年，经过三年多的时间，创新企业取得了一定的成长，在业界具有了一定的知名度。②从团队人数看，50~100 人是最常见规模：在 50 强企业中，50 人规模的团队是最多的，占到参赛企业半数；100 人规模的团队也达到了 15 家，这样的规模具备了承担 1~2 个核心产品开发及业务运行的能力；得益于先进的产业模式，一些人数只有 20 人左右的小团队表现不俗，取得了可以比拟 50~100 人团队的业绩。③从销售收入看，3000 万左右的收入是最多的：在 50 强企业中，2021 年销售收入在 3000 万元左右的企业是最多的，占总数的 40%。这也一定程度上反映了网络安全行业的特点，突破 3000 万元是一个挑战，需要企业在产品业务模式上作出一定的调整。

通过 2022 创新沙盒与创客汇赛道对比分析，我们看到：①热点赛道相似：创新沙盒的热点赛道跟创客汇

> 中国网络安全市场增速领先全球，
> 头部企业市值受宏观环境影响较大，
> 但营收依然实现较为稳定和快速的增长；
> 中国网络安全产业增长潜力超美国，
> 市场机会多点爆发，具有旺盛的需求和广泛的行业覆盖度。

较为相似，其中软件供应链安全、数据安全、身份安全都是热点赛道，唯一不同的是创新沙盒云安全赛道热度最高，而创客汇云安全相对较少，而工业安全、IOT 安全相对更多。②创客汇赛道更为多样化：创新沙盒热点赛道更为聚焦，4 大热点赛道汇集了 74% 的厂商。而创客汇排名前四的热点赛道则汇集了 46% 的厂商，分布相对更为广泛，创业方向更加多样化。

从 5 年创新沙盒与安全创客汇年度热门分析看，创客汇热门赛道与创新沙盒基本接近，但具体到每年的热门赛道则稍有不同。创新沙盒热门赛道更具有持续性 从5年的发展历程看，创新沙盒热门赛道始终聚焦在云、数据、身份、软件供应链，但每年都会有一定的演进。例如，云安全从基础设施到平台到应用，再到云原生的业务安全。创客汇热门赛道在紧跟国际趋势的同时更体现出我国行业需求特点：千行百业的安全需求使我国网安行业创新方向更多、更加与业务相结合，网络攻防、安全运营、SOAR 等具实战化的技术与产品方向更受欢迎，数据安全一直是热点，符合我国行业对网络安全的需求。

我国网安产业有足够的成长与创新空间，“十四五”网络安全市场空间预计超 6000 亿。热点赛道规模快速增长，成为网安产业发展的新动力。

4. 总结与展望：网安产业在波动中前行，期待新的突破

过去的 2022 年网安产业在波动中前行，宏观环境具备长期向好的基本面，产业发展具备足够的韧性，细分赛道体现创新活力。2023 年开年迎来重大利好政策密集发布，网络安全体系化创新、融合发展成为趋势，七大重点领域将成为新增长点。期待资本市场整合资源加大投入，推动网安产业实现新的突破。

（1）2022 年网安产业在波动中前行，保持了增长势头

宏观环境具备长期向好的基本面。诸多不确定因素作用于网络空间，全球网络安全事件不断表明网络安全形势的不确定性，但安全需求及投入的增长的基本面是确定的。网络安全是国家安全的一部分，安全是网安行业根本逻辑，行业发展更趋向于在网络空间践行国家总体安全战略。安全与斗争成为时代强音，网络战时代已经来临，攻防能力是关键。经济建设全局统筹，网络安全防护对象越来越聚焦到数字经济的核心部分，产业趋向集中化发展。中央成立委员会统筹管理网信工作，网信工作具备长期性、稳定性，网安法规体系加快细化落地，全国一体化政务大数据体系打造数据安全样板。

产业发展具备足够的韧性。全球网安市场短期波动，增速放缓但仍好于其他多数行业，五年复合增速依然超 10%；全球网安产业碎片化明显，没有绝对强势的行业巨头，创业公司有机会脱颖而出；中国网安产业布局完整，技术趋势与美国接近，应用则结合国情布局进一步细化，发展路线较为清晰。中国网络安全市场增速领先全球，头部企业市值受宏观环境影响较大，但营收依然实现较为稳定和快速的增长；中国网络安全产业增长潜力超美国，市场机会多点爆发，具有旺盛的需求和广泛的行业覆盖度。投融资 2022 年受宏观环境影响大，热门赛道更加集中，创新领域多且活跃。

细分赛道体现创新活力。全球创新厂商聚焦热门创新赛道，着重核心技术与产品研发，填补头部厂商生态体系，并有大量创新企业被头部厂商收购。全球网安行业创新的演进线路稳中有进，热门应用、热点事件、创新趋势带动创新企业不断提升技术能力。全球网安创新赛道更为聚焦，4 大热点赛道汇集了大部分创新厂商。我国网安创企赛道分布相对更为广泛，创业方向更加多样化，体现了我国产业特色与广泛的需求面，热点赛道与国外基本一致。我国网安产业十四五

期间预计超 6000 亿，有足够的成长与创新空间。热点赛道规模快速增长，将为网安产业发展注入新动力。

（2）2023 年网安产业迎来好的开局，期望取得新的突破

1）重大利好政策密集发布，2023 网安产业迎来好开局

二十大之后，网信领域重大利好政策密集发布，2023 年网络安全产业迎来好的开局。

全国一体化政务大数据体系建设启动数据安全体系化建设时代。2022 年 10 月 28 日国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知。全国一体化政务大数据体系包括三类平台和三大支撑：三类平台为“1+32+N”框架结构。“1”是指国家政务大数据平台，“32”是指 31 个省（自治区、直辖市）和新疆生产建设兵团统筹建设的省级政务数据平台，“N”是指国务院有关部门的政务数据平台。三大支撑包括管理机制、标准规范、安全保障三个方面。全国一体化政务大数据体系建设带来数据治理与数据安全业务机遇，包括数据资源盘点及目录系统建设，数据质量咨询服务及系统建设，数据管理、数据安全治理、数据安全保护系统建设及合规服务。

“数据二十条”推动数据要素活起来、动起来、用起来。中共中央、国务院在 2022 年 12 月 19 日正式发布《关于构建数据基础制度更好发挥数据要素作用的意见》，从数据产权、流通交易、收益分配、安全治理四个方面初步搭建我国数据基础制度体系提出二十条政策举措。①数据产权方面，淡化所有权、强调使用权，加强数据分类分级管理；②流通交易方面，数据交易和数据流通监管体系逐步完善，有效市场和有为政府相结合协同发展；③收益分配方面，基于数据溯源进行价值分层，助力科学优化数据要素共享收益分配机制；④安全治理方面，守住数据要素流通合规底线，建设合规高效的数据安全体系。

国资委央企新一轮改革提升，统筹发展和安全、防范化解重大风险。2023 年 1 月 5 日，国资委召开中央企业负责人会议，全面贯彻落实党的二十大精神和中央经济工作会议部署。2023 年组织开展新一轮国企改革深化提升行动：①分层分类深化混合所有制改革，促进国企民企协同发展，进一步发挥国有企业引领带动作用。②聚焦战略安全、产业引领、国计民生、公共服务等功能；加快打造现代产业链链长，积极开拓新领域新赛道，培育壮大战略性新兴产业，在建设现代化产业体系上发挥领头羊作用。③更好统筹发展和安全，有效防范化解重大风险，压实企业主体责任，增强风险处置精准性、有效性，切实提升企业安全生产水平。

证券行业网络和信息安全三年提升计划启动。2023 年 1 月，中证协下发《网络和信息安全三年提升计划（2023-2025）》征求意见稿，提出六大方面、33 项任务清单：①持续提升科技治理水平，制定全方位的网络和信息科技战略发展规划，完善并定期开展供应商评估工作；②建立科学合理的科技投入机制，网络和信息安全投入不低于信息科技投入总额的 7%；③增强信息系统架构规划掌控能力，技术架构转型云计算平台承载及运行的信息系统比例不低于 60%；④强化系统研发测试管理能力，代码审计 100% 覆盖并对第三方系统开展全方位的安全检测监控；⑤夯实系统运行保障能力，建设统一的告警平台，建立数据防丢、防删的权限管控机制和技术手段；⑥健全网络和信息安全防护体系，完善的漏洞管理制度，加强 APP 安全检测认证。

2）2023 年网络安全体系化创新、融合发展成为趋势

未来体系化创新是主要创新模式，为保障国家重大网络安全项目和工程的建设，需要新模式、新架构、新产品和新服务：新模式 – 层级化网络安全态势指挥体系，统一指挥，协同一致，通过体系化优势发挥出最大能力。新架构 – 面对国家大型网络安全体系，全局性、系统性开展规划建设运行。新产品 – 自主研发新一代网络安全产品，形成上下一体、互为支撑的安全产品体系。新服务 – 全天候、全方位、全周期开展演练、运行和应急服务，提升针面向关键信息基础设施的安全服务能力、服务支撑能力、系统建设能力和服务保障能力。

网络安全服务于数字产业，我国产业门类多、企业数量多，推进网络安全与产业应用的深度融合发展是未来网络安全产业的关键增长点。数字化企业对网络安全的感知将进一步提高，实战化攻防演练广泛开展，合规性检查与测评更为常态化。网络安全规划、建设和运营三同步将进一步落地，以业务视角开展网络安全体系规划，开展网络安全能力的模块化建设，广泛使用第三方安全服务，使得企业快速具备安全运营能力。政府层面重点关注网络安全的整体态势感知、安全监管与攻防反制能力建设，企业层面解决自身的安全防护、管理等问题，

未来体系化创新是主要创新模式，
为保障国家重大网络安全项目和工程的建设，
需要新模式、新架构、新产品和新服务。

国家与企业互相支撑，形成国家整体的强壮的安全能力。

3）整合资源加大资本市场投入，八大重点领域将成为新增长点

国资和资本市场将进一步加大网络安全投入，持续助推网安产业发展。国资的投入和整合是支持网络安全产业发展的重要途经，美国中央情报局设立的 In-Q-Tel 公司将网络安全作为重要投资领域，孵化出 FireEye、Palantir 等知名网络安全企业。我国国资已开始进入网络安全领域，未来将进一步形成合力，打通创新链、产业链和价值链，更好释放各类主体的创新活力。在资本市场上，网络安全一直是受资本青睐的热门赛道，一级市场和二级市场均有良好的表现。近段时间受宏观环境负面影响，但仍是投资热点。网安企业稳定增长的趋势，在充满不确定性的国际政治经济形势下，将会为投资方带来持续的高回报。

综合市场吸引力和公司资源与能力因素，结合竞争分析，我们认为 2023 年关基市场、数字化产业市场、数据安全市场、云原生安全市场、合规市场、信创市场、国家安全市场和海外业务市场为 2023 年八大热门市场：①关基市场：随着全球网络安全形势的恶化，对关键信息基础设施的攻防对抗成为热点，同时受法律政策驱动的影响，关基市场逐渐实现重点行业全覆盖，安全投入占比高，在网安整体市场的位置更加重要。②数字化产业市场：我国政企机构业务数字化转型驱动，覆盖速度很快，在网安整体市场占比快速提升接近与传统网安市场规模。③数据安全市场：数据安全监管要求和数字化业务数据保护驱动数据安全市场快速发展，2022 年市场规模已超百亿增速持续加快。④云原生安全市场：云原生安全是 2022 年国际网安市场热点，随着我国东数西算战略的部署，国家与地方政务云和企业云建设加快，数字化业务往云上迁移的步伐也在加快，云原生安全需求正在快速增长。⑤合规市场：国家战略与法律驱动，等保、关保、分保、密评等，在网安整体市场占比迅速提升；⑥信创市场：覆盖重要党政机构、重要行业和央企国企，当前占比较低但市场空间广阔。⑦国家安全市场：保卫国家安全和网络国防能力建设，未来具有很大的市场空间。⑧海外业务市场：国家扩大国际影响力，以及海外利益保护的要求，带来巨大的市场空间。

2023 年网络安全市场机会多点爆发。从行业应用维度看，党政、公安、交通、教育、卫生、银行等行业热度最高，安全需求旺盛。从安全需求维度看，等保密评、政企数字化升级、信息化业务升级、行业安全服务具有广泛的行业覆盖度。

本研究报告作者

奇安信集团产业发展研究中心是奇安信集团的产业研究团队。专注网络安全领域，跟踪国内外产业发展现状与趋势，深入调研网络安全各细分领域，包括产品技术、市场、投融资和产业生态，为网络安全从业人员提供新视角，为企业决策提供依据，推动网络安全产业发展。

陈华平：奇安信集团副总裁，产业发展研究中心负责人。

乔思远：产业发展研究中心研究员，主要负责宏观分析和产品技术研究。

万鹏：产业发展研究中心研究员，主要负责产业生态研究。

尹文鹏：产业发展研究中心研究员，主要负责投融资和市场研究。

法规回顾与前瞻：未来更多部门规章将承担行业数据监管责任

作者 | 陈际红

“无边落木萧萧下，不尽长江滚滚来”，我们很难用一种确切的感受形容即将过去的 2022 年，但该前行的还是在前行。在网络安全和数据保护领域，2022 年是在“三驾马车”法律架构下细化落地监管措施，并大力促进数据要素释放红利的一年，以三套数据跨境传输机制、算法规制、网络安全审查、数字化转型和数据要素化政策等为代表。2022 年虽看似重要，立法没有 2021 年密集，但昔日花今日果，回顾一年来的实践情况，2022 年企业所面临的数据合规实施压力可能更大。

一．立法篇

“数据跨境传输三件套”逐次落地

数据跨境传输涉及国家安全、公共利益及个体权益，一直是立法和监管的重点。自 2017 年实施的《网络安全法》确立数据跨境传输安全评估制度以来，网信办就着手制定个人信息与重要数据的出境安全评估规则，在经历了个人信息与重要数据评估规则的“合－分－合”过程，尤其是去年《个人信息保护法》在立法层面明确了个人信息跨境传输的法律规定后，规则制定明显加快。

在安全评估制度方面，网信办于 2022 年 7 月 7 日公布《数据出境安全评估办法》，并于 9 月 1 日正式实施；此外，网信办于 2022 年 8 月 31 日发布《数据出境安全评估申报指南（第一版）》，提供了开展安全评估的指引，之后各地网信部门相继开通接受安全评估申报的窗口，安全评估申报开闸。

在保护认证方面，信安标委秘书处于 2022 年 6 月 24 日发布《个人信息跨境处理活动安全认证规范》，并进而在 12 月 6 日发布了《个人信息跨境处理活动安全认证规范 v2.0》，第二版认证规范吸收了《数据出境安全评估办法》及《个人信息出境标准合同规定（征求意见稿）》的内容，在数据跨境传输协议、个人信息保护影响评估要求上与之保持一致，新增个人信息主体在权益受损时的赔偿请求权，并试图将认证的适用情形从之前的股权关联拓宽至业务关联，明确要求境外接收方对该规范中列明的个人信息主体权利予以承认。11 月 4 日，

2022 年是在“三驾马车”法律架构下细化落地监管措施，并大力促进数据要素释放红利的一年，以三套数据跨境传输机制、算法规制、网络安全审查、数字化转型和数据要素化政策等为代表。

市监总局和网信办发布《个人信息保护认证实施规则》，建立了认证实施的程序规则，一旦认证机构名单经过批准后发布，认证活动就可以正式开展。

在标准合同方面，自 2022 年 6 月 30 日网信办公布《个人信息出境标准合同规定（征求意见稿）》后，即引发一些争议，比如，GDPR 的新版跨境传输 SCCs 划分了四类个人数据跨境传输场景（C-C/C-P/P-C/P-P），分别对应不同的合同模块。而目前中国版的标准合同仅限于境内为个人信息处理者的情形（即 C-C 或 C-P），此框架能否涵盖真实的出境场景需求？以及，对境外再传输的场景，是否可以加入对接条款（docking clause），使第三方后续以数据传输方或接收方的身份加入 SCCs？据悉，网信部门也在不断地征求各个方面的意见，但按照原来的预期，在年底前发布正式版本实有一定难度。

新《网络安全审查办法》生效，中概股国外上市前景渐明

以某知名互联网出行平台在外国上市引发网络安全审查为契机，修订后的《网络安全审查办法》于 2022 年 2 月 15 日起正式施行。与 2020 年的版本相比，新版《网络安全审查办法》一是将平台企业的数据处理活动纳入到网络安全审查制度的监管范围，二是对于掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，要求必须先行申报网络安全审查。关于修订办法对中概股企业的境外上市影响，我们有以下观察：

- 2021 年美国 SEC 宣布通过法规修正案，完善了《外国公司问责法案》（“HFCAA”）相关的信息披露实施细则，要求外国上市公司的审计机构必须接受美国公众公司会计监督委员会（PCAOB）的审查。今年 3 月 8 日以来，美国 SEC 根据 HFCAA，先后将约 150 家不符合美国 PCAOB 审计监管要求的中概股公司纳入“确定识别名单”，使其面临从美股退市的风险；

- 2022 年 4 月 2 日，证监会发布就《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定》公开征求意见的通知，对规范审计工作底稿信息安全管理提出明确要求，进一步落实上市公司信息安全的主体责任；

- 证监会和财政部于 2022 年 8 月 26 日与 PCAOB 签署审计监管合作协议，于近期启动相关合作，中概股从美股集体退市的风险出现转机；

- 据报道，自 2022 年 2 月 15 日《网络安全审查办法》修订施行以来，已有 20 余家拟赴国外上市企业向国家网络安全审查办公室进行了申报。

据此，中美关于中概股的审计监管基本达成短期的合作规则，网络安全审查制度也逐步开始运转，看似为中概股赴美上市理清了通途。但是，考虑到数据跨境日益强监管，关基运营者、掌握核心数据或重要数据的数据处理者、或处理大量个人信息的平台企业在选择上市地时，港股或境内 A 股或许是更安全的选择。

于 2022 年 2 月 15 日起正式施行。与 2020 年的版本相比，新版《网络安全审查办法》一是将平台企业的数据处理活动纳入到网络安全审查制度的监管范围，二是对于掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，要求必须先行申报网络安全审查。

算法备案正式实施

之前我们在《网络空间治理的升级：从数据治理迈向算法治理》一文中认为，“数据治理”以保障数据安全、保护个人、组织的合法权益为主要目标，而“算法治理”重点指向的则是数据应用的内在逻辑和产生的效果，平台通过算法应用数据来实施其行为，具有权力化的趋势。基于此，我们认为，算法治理会成为未来的治理和监管焦点。2022 年 3 月 1 日，《互联网信息服务算法推荐管理规定》正式生效，网信办并于 2 月 28 日发布了《关于互联网信息服务算法备案系统上线的通告》，算法备案系统正式上线。在 2022 年 8 月，网信办发布算法备案信息，涉微博热搜、百度检索等。综合来看，已经备案公示的算法有以下几个特点。

- 算法分类分级治理：同一款 APP，如存在多款需要备案的算法，

需要分别申请备案；使用算法相同的不同产品或者同一产品的不同端，如微博（APP、网站、小程序）均可在一个申请中进行备案；

- 重点关注内容个性化推荐：个性化推送类算法中的内容推荐类，在首批算法备案名单中，数量最多，体现行业应用和监管关注的重点；
- 大多数备案的算法未经公示，体现出商业秘密保护的考量，但会通过算法逻辑强调算法公平性。

其他重要立法活动

互联网内容治理规则进一步网格化。在 2022 年，监管部门对互联网内容治理和生态治理进一步细化，深化互联网内容合规的红线要求。11 月 25 日，网信办等三部门联合发布《互联网信息服务深度合成管理规定》，对深度学习、虚拟现实等人工智能技术应用于生成新型互联网内容划定“底线”和“红线”；8月1日，新修订的《移动互联网应用程序信息服务管理规定》施行，要求应用程序提供者和应用程序分发平台应当履行信息内容管理主体责任，建立健全信息内容安全管理、信息内容生态治理、数据安全和个人信息保护、未成年人保护等管理制度，确保网络安全，维护良好网络生态。之外，新修订的《互联网跟帖评论服务管理规定》自12月15日起施行，《互联网弹窗信息推送服务管理规定》自 9 月 30 日施行，《互联网用户账号信息管理规定》自 8 月 1 日施行。互联网内容治理手段进一步细化和网格化。

《反电信网络诈骗法》自 2022 年 12 月 1 日起施行，针对电信网络诈骗犯罪之顽疾，该部法律立足各环节、全链条防范治理电信网络诈骗，精准发力，为反电信网络诈骗工作提供有力法律支撑。对于电信、互联网和金融企业而言，需要建立防范个人信息被用于电信网络诈骗的机制，主动建立监测识别和处置机制，履行禁止为电信网络诈骗活动提供支持或者帮助的义务（重点防范与帮助信息网络犯罪活动罪的结合适用）。同时，企业

应准确把握好数据共享义务与个人信息保护义务及消费者权益保护的关系。

“三驾马车”架构中的**《网络安全法》实施五年后亦开始修订**工作，一是加强了对违法行为的处罚力度，让《网络安全法》的“牙齿”更为锋利。修订稿调整了行政处罚幅度并加入了从业禁止等措施，比如，“处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款”及“可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作”等规定。二是解决对现有法律的衔接问题，以转致性规定的形式，加强《网络安全法》同《数据安全法》《个人信息保护法》等的关联适用，预示着其在个人信息和重要数据保护方面将可能让位于另外两部法。

2022 年 9 月 8 日，网信办就**《网信部门行政执法程序规定（征求意见稿）》**公开征求意见，并将取代之前的《互联网信息内容管理行政执法程序规定》，网信部门的行政执法案件类型也明确拓展至网络信息内容、网络安全、数据安全、个人信息保护等，赋予执法部门的调查取证手段也更为丰富，同时还规定了听证和约谈程序。

工业和信息化部于 12 月 8 日印发《工业和信息化领域数据安全管理办法（试行）》，自 2023 年 1 月 1 日起施行。值得关注的是，该办法规定了对工业和电信数据进行一般数据、重要数据和核心数据分级的“三分法”，并在法规层面首次明确核心数据的范围。该办法明确了重要数据和核心数据目录备案义务，如涉及处理相关数据，则应向本地区行业监管部门备案本单位重要数据和核心数据目录。该办法的发布也是工业和电信数据迈向全面行业监管的起始。

二．执法篇

个人信息保护纠纷案件

《个人信息保护法》第四十四条至四十八条赋予了个人信息主体各种权利，并通过第五十条和第六十九条进一步确认了个人信息主体的诉权，2021 年 11 月至 2022 年 12 月 5 日，基于威科先行法律数据库的案例统计，可以检索到的以“个人信息保护纠纷案由”的案例已有 127 件。在 2022 年，借《个人信息保护法》一周年的东风，有些地方法院发布了典型案例。比如，杭州互联网法院发布“个人信息保护十大典型案例”；广州互联网法院发布五个“个人信息保护典型案例”，涵盖算法错误关联个人信息、商家擅自公布消费者个人信息、手机 APP 未经同意收集个人信息、平台泄露投诉举报信息等内容；广东省高级人民法院亦发布了一批个人信息保护典型案例。

在杭州互联网法院审理的**“杜某诉网络公司个人信息保护纠纷案”**中，杜某以个人信息知情权、决定权受电商平台侵害为由，提起诉讼。法院认为，《个人信息保护法》第五十条第二款规定的诉权以“个人信息处理者拒绝个人行使权利的请求”为前提，个人信息主体应先向个人信息处理者请求行使具体权利，只有在个人信息处理者无正当理由拒绝履行义务或一定期限内不予以处理，或者个人信息处理者提供的申请受理机制失效的情况下，个人方可向法院提起诉讼以获得救济。

当然，此判决对于有效使用司法资源，形成个人信息多元治理模式具有裨益，对个人信息主体单纯行使程序性权利的情形是恰当的。同时我们认为，个人信息主体受到的权益侵害可能是程序性权利受到阻碍时带来的侵害，亦可能是违法处理其个人信息所带来的实质性侵害。《个人信息保护法》第五十条和第六十九条则分别规定了这两种侵害对应的请求权。《个人信息保护法》第四章赋予个人信息主体的各种权利不仅具有程序性，也可能兼具有实体性。本案中，原告主张“知情权、决定权”的背后是被告未向其告知且未经其同意即公开其个人信息，实质上是由于个人信息处理者违法处理其个人信息，导致实体上损害了原告的个人信息权利，已超出

一是加强了对违法行为的处罚力度，让《网络安全法》的“牙齿”更为锋利。修订稿调整了行政处罚幅度并加入了从业禁止等措施，是解决对现有法律的衔接问题，以转致性规定的形式，加强《网络安全法》同《数据安全法》《个人信息保护法》等的关联适用，预示着其在个人信息和重要数据保护方面将可能让位于另外两部法。

“程序性”范畴。如果法院绝对化地以“个人信息处理者拒绝个人行使权利的请求”为前提来处理个人信息主体的诉权，可能会限缩个人因损害行为而获得司法救济的权利。不过，本案对企业而言，意味着其在构建响应个人信息主体行权处理机制的同时，应留存个人信息主体行权处理记录，可将之作为可能的应诉证据使用。

个人信息保护公益诉讼

《个人信息保护法》第七十条专设公益诉讼条款，明确将个人信息保护纳入公益诉讼的范围。根据公开数据，2021 年全国检察机关共立案个人信息保护领域公益诉讼案件 2276 件，2022 年 1 月至 10 月立案 3936 件。依照最高检《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》，个人信息保护公益诉讼主要聚焦在五类个人信息的保护：敏感个人信息、特殊群体个人信息、重点领域处理的个人信息、100 万人以上的大规模个人信息，以及对因时间、空间等联结形成的特定对象的个人信息。我们预判，在未来几年内，个人信息保护公益诉讼的数量还会快速增长，考虑其由国家公权力机关提起，且具备公益属性，案件一般会引发广泛的社会关注，给企业带来经济和商誉上的双重损害，平台型企业应当尤其关注公益诉讼风险。

在“杭州市余杭区人民检察院诉某短视频平台未成年人保护民事公益诉讼案”中，涉案公司在开发运营 APP 过程中，未以显著、清晰的方式告知并征得儿童监护人有效明示同意，允许注册儿童账户收集、存储儿童个人信息；在未再次征得儿童监护人有效明示同意的情况下，向用户直接推送含有儿童个人信息的短视频。诉讼期间，检察机关积极推动该公司立行立改，对其运营的 APP 提出 34 项整改措施。该公司积极配合整改，双方依法达成和解。

本案系全国首例儿童个人信息、网络安全保护民事公益诉讼。《个人信息保护法》第二十八、三十一条明确规定十四周岁以下未成年人的个人信息属于敏感个人信息，处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则，并取得未成年人的父母或者其他监护人的同意。具体而言，企业除应单独制定《儿童个人信息 / 隐私保护政策》和《儿童个人用户协议》，采取合理措施通知监护人并征得监护人有效单独同意外，还可采取如下措施：①对儿童个人信息建立专门保护池，采取加密存储等安全措施；②基于算法自动化决策进行推送的场景下，需获得儿童监护人单独授权同意；③应强制为儿童开启陌生人关注限制功能、隐藏儿童用户位置等功能。企业需要注意，目前我国法律对未成年人个人信息权益予以特殊、优先保护，不特定儿童用户的个人信息权益保护具有公益属性，企业如侵害该等用户个人信息权益，或将被提起公益诉讼。

个人信息刑事案件与合规不起诉制度

2018 年至今，全国检察机关以侵犯公民个人信息罪批捕 16459 人、起诉 33417 人，其中，2022 年 1 月份至 9 月份即批捕 1199 人、起诉 6223 人。从今年批捕的人数看，数量明显减少，我们认为这是一种刑事司法角色的正常回归。犹记 2017 年开始的以“大数据爬虫”为主要抓手的执法风暴，此次行动源于监管部门的现金贷溯源性整肃，以及公安机关在全国范围开展的扫黑除恶行动，即打掉“套路贷”和暴力催收的数据源头。这次执法风暴某种程度上严重影响了国内“大数据风控”的业务体系，使得大数据业内谈爬虫色变。得益于从业者个人信息保护意识的提高和合规能力的提升，以及专项执法行动的结束，个人信息刑事案件数量得到控制。我们认为，一方面，在个人信息保护领域，刑事手段应用要秉持谦抑原则，让行政执法和民事司法保护占据更加主导的地位，让数据有关的从业者对法律风险具有更好的管控性；另一方面，与数据有关的企业仍应当把数据刑事风险

我们预判，在未来几年内，个人信息保护公益诉讼的数量还会快速增长，考虑其由国家公权力机关提起，且具备公益属性，案件一般会引发广泛的社会关注，给企业带来经济和商誉上的双重损害，平台型企业应当尤其关注公益诉讼风险。

防范当成一道重要的经营红线，唯此，才能做到基业长青。

数据领域合规不起诉制度的逐步确立。2022 年 5 月，上海市普陀区检察院公布我国首起数据合规不起诉案件办理情况，本案作为数据合规治理与合规不起诉制度的首次交集，意味着我国合规不起诉制度将正式适用于数据合规领域。2021 年 4 月，最高人民检察院下发《关于开展企业合规改革试点工作方案》，“合规不起诉”制度得以确立，即当涉案企业作出合规承诺并积极整改落实后，对特定类型的案件检察机关可作出不批准逮捕、不起诉决定或提出轻缓量刑建议。本案 Z 公司因违法使用爬虫技术而触发刑事责任，其在案发后即向检察院提出了合规不起诉申请，检察院经审查认定可依法启动涉案企业合规考察，进而启动相应合规不起诉程序。Z 公司在整改开始之际即聘请法律顾问团队，在整改期内顺利根据承诺推进对涉案数据合规问题的整改。本案的教训亦可成为企业积极建设数据合规体系的动力：一方面，企业可通过提前部署数据合规工具，设定数据合规管理架构，建立数据合规制度，从而提前防范刑事风险；另一方面，如确已进入刑事程序，可通过“合规不起诉”制度配合检察机关积极开展数据合规整改，继而扭转局势，使企业得以转危为安，延续经营生命。

其他执法行动

备受关注的**某网络出行平台网络安全审查案件**在 2022 年尘埃落定，也是一场全民网络安全教育的案例。该公司依法被处罚款 80 余亿元，公司两位管理层人员各自被处罚款人民币 100 万元。此案可以关注三点，一是执法的域外效力，由于该公司对境内各业务线重大事项具有最高决策权，制定的企业内部制度规范对境内各业务线全部适用，且对落实情况负监督管理责任，据此，本案违法行为主体认定为该网络出行平台公司；二是顶格处罚，《个人信息保护法》规定了

“五千万元以下或者上一年度营业额百分之五以下罚款的”的罚则，而该公司 2021 年全年总营收额为 1700 余亿人民币；三是一案双罚，除了处罚公司，还对直接负责主管人员处 100 万罚款。

APP 治理：从“双清单”到 SDK。去年工业和信息化部印发《关于开展信息通信服务感知提升行动的通知》，推动建立个人信息保护“双清单”制度，今年工业和信息化部又在 APP 违法通报中首次将内嵌第三方软件开发工具包（SDK）违规收集用户设备信息的行为纳入监管视野，并开展了 APP 侵害用户权益整治“回头看”行动。工业和信息化部 2022 年对 APP 的治理工作重点突出关键责任链监管，对应用商店、SDK、终端企业、重点互联网企业等实现监管全覆盖，打造更为安全的信息通信消费环境。网信办则更加聚焦 APP 的生态治理，于 12 月部署开展“清朗 · 移动互联网应用程序领域乱象整治”专项行动，将加强 APP 全链条管理，全面规范移动应用程序在搜索、下载、使用等环节的运营行为，督促应用程序分发平台落实好各项任务，整治各个环节存在的问题。

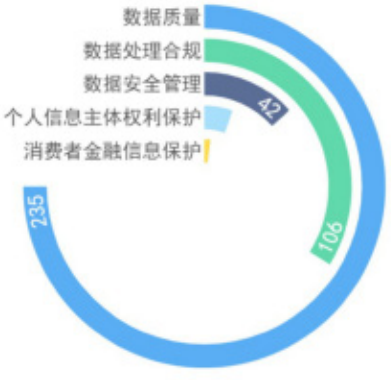


图 1

行业执法。在以网信办、工信部、公安部为代表的综合性网络安全与数据保护执法之外，各个行业主管部门也在不断推进行业监管和执法。以金融行业为例，作为数据密集型领域，金融领域数据合规也愈发受到监管部门关注。根据一行两会所公布的涉及数据监管相关行政处罚数据不完全统计，金融机构所涉违法违规事由关键词可总结为数据质量、数据处理合规、数据安全管理、个人信息主体权利保护四大方面。（见图 1）

三 . 焦点篇

汽车行业监管

2021 年《汽车数据安全管理若干规定》（以下简称“《若干规定》”）生效，确立了汽车数据的强监管趋势，今年更进一步深化了监管规则和监管手段。2022 年，延续去年的汽车年报要求，各地网信办陆续发布通知，要求本省内汽车数据处理者开展 2022 年度汽车数据安全管理情况的年度报送工作。结合数据跨境等新法规的要求，细化了年报要求。在标准方面，信安标委于 10 月 19 日发布《信息安全技术 汽车数据处理安全要求》（以下简称“《汽车数据要求》”），首次从国标层面针对汽车数据处理者如何落实《若干规定》提出了全方位的要求。对《若干规定》一些规则的理解也曾引发业内的诸多讨论，例如，何谓“增强行车安全的目的”，如何理解“无法征得同意”“向车外提供车外个人信息”及“匿名化处理”的顺序和逻辑，成为实务中困扰车企的难题。《汽车数据要求》针对由《若干规定》引发的实务难题一一展开回应，为车企落实《若干规定》提供重要参考和指引。此外，《汽车数据要求》与各省近期

数据出境落地方案：七步法

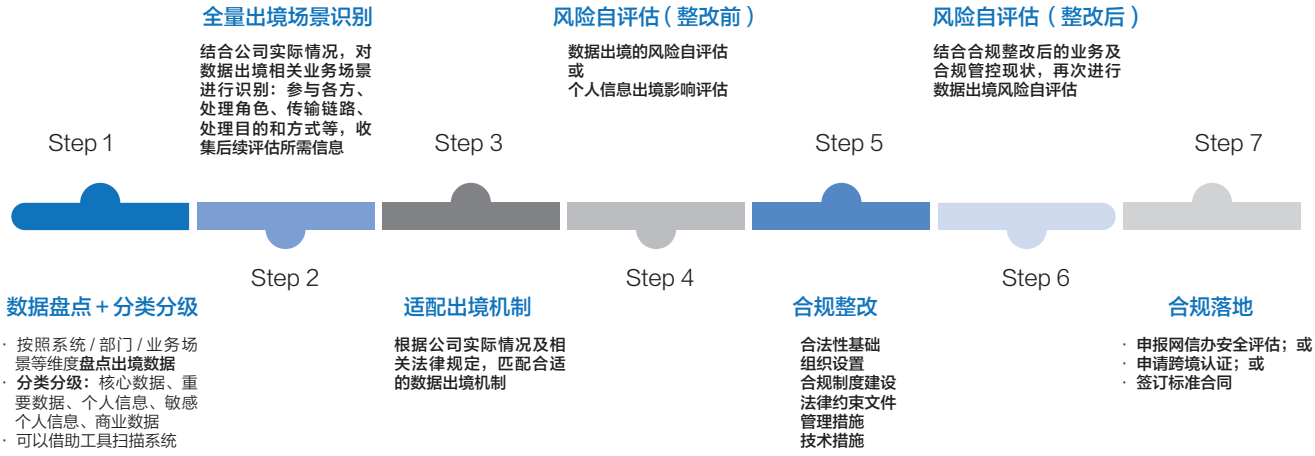


图 2

发布的汽车数据安全管理情况报告模板的结构存在高度相似性，可以理解，《汽车数据要求》也是监管部门开展监管工作的重要参考。

2022 年 4 月 15 日，工信部装备工业发展中心发布《关于开展汽车软件在线升级备案的通知》，明确汽车 OTA 升级备案管理相关事项。2020 年 11 月以来，我国对汽车 OTA 监管不断加码，政策也逐步落地，本次升级备案的落地意味着我国正式进入 OTA 监管时代。工信部于 2022 年 3 月发布的《2022 年汽车标准化工作要点》中，明确提及 2022 年工信部将开展汽车 OTA 升级管理试点，OTA 相关强制性国家标准也将陆续出台。

2022 年 8 月 30 日，自然资源部发布《自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知》，明确智能网联汽车安装或集成了卫星导航定位接收模块、惯性测量单元、摄像头、激光雷达等传感器后，在运行、服务和道路测试过程中对车辆及周边道路设施空间坐标、影像、点云及其属性信息等测绘地理信息数据进行采集、存储、传输和处理的行为，属于测绘活动，纳入测绘监管。企业存在向境外传输相关空间坐标、影像、点云及其属性信息等测绘地理信息数据行为或计划的，要依法履行对外提供审批或地图审核程序等，在此之前应停止数据境外传输行为。相关企业应尽快申办导航电子地图制作等测绘资质，或委托具有相应测绘资质的单位开展。

数据出境项目的管理

2022 年，在很多企业的合规任务清单中，跨境数据合规落地应该是排在最优先级。对于数据出境安全自评估和申报工作，既具有法律性也具有技术性，申报时限紧张，企业要组织法律、合规、技术和业务等部门共同参与，需要协同境内和境外的资源，具有很大的挑战性。有效管理数据出境合规项目是项目成功的关键，我们根据实务经验总结了“七步法”来实施出境项目，如上图。（图 2）

针对自评估工作，我们建议遵循“四流程”的方法具体展开，具体如图。（见图 3）

构建数据基础制度，激发数据要素红利

全球数字化转型的步伐浩浩汤汤，数字技术的进步一日千里。2022 年 6 月 22 日，中央全面深化改革委员会第二十六次会议审议通过《关于构建数据基础制度更好发挥数据要素作用的意见》，提出四个方面的要求：一是要建立数据产权制度，健全数据要素权益保护制度；二是要建立合规高效的数据要素流通和交易制度，完善数据全流程合规和监管规则体系，建设规范的数据交易市场；三是要完善数据要素市场化配置机制，更好地发挥政府在数据要素收益分配中的引导调节作用，建立体现效率、促进公平的数据要素收益分配制度；四是要把安全贯穿数据治理全过程，明确监管红线。国务院于 6 月 23 日发布了《关于加强数字政府建设的指导意见》，提出构建开放共享的数据资源体系、以数字政府建设全面引领驱动数字化发展等意见。中共中央和国务院于 12 月 19 日正式发布《中共中央 国务院关于构建数据基础制度更好发挥数据要

数据出境风险自评估：四个流程

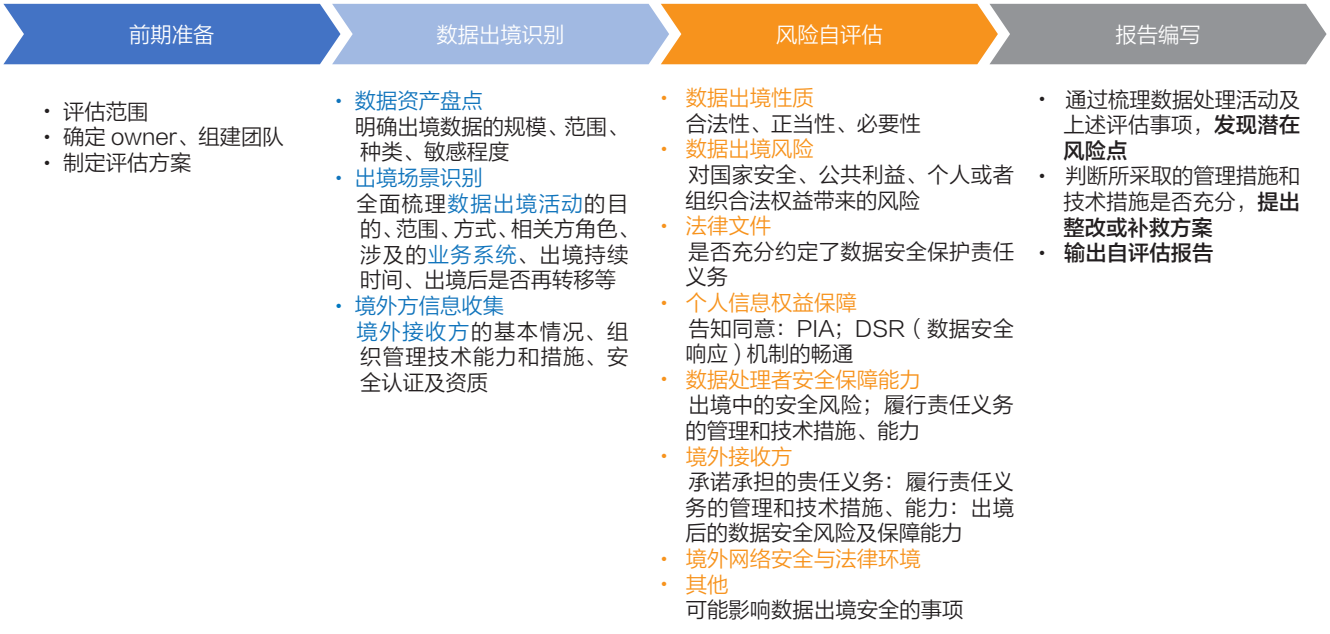


图 3

素作用的意见》（以下简称“《数据二十条》”）。《数据二十条》所确立的数据基础制度的“四梁八柱”，即数据产权制度、数据要素流动和交易制度、数据要素的收益分配制度和治理制度，就是为了解决数据要素化进程中的现实困境。

数据要素化政策暖风频吹，但数据确权是数据资产化的前提，也是数据商业性流动的基石。我国当前数据确权制度仍不清晰，主要体现在数据权利主体及权益分配的界定上。目前数据产权制度建设的基本推进思路是分类确权，推进公共数据、企业数据、个人数据的分类分级确权授权使用；回避传统法律体系中的物权、所有权或知识产权概念，建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制，健全数据要素权益保护制度。

在数据要素流通和交易制度建设方面，2022 年 4 月发布的《中共中央国务院关于加快建设全国统一大市场的意见》提到，要加快培育数据要素市场。国家工业信息安全发展研究中心发布的《2022 年数据交易平台发展白皮书》显示，截至 2022 年 8 月，全国已成立 44 家数据交易机构，此后又有苏州、广州、深圳等地的数据交易所相继揭牌，全国掀起了新一轮的数据交易市场建设浪潮。

数据安全认证体系建设加快

数据安全认证业已成为一个被普遍接受的国际实践，第三方认证机构按照认证标准对数据处理者进行技术验证、现场核查和获证后监督，从而证明数据处理者的安全能力达到特定的标准，认证具有权威、中立和长效的优势。2022 年 11 月 4 日，市监总局、网信办发布《关于实施个人信息保护认证的公告》及《个人信息保护认证实施规则》，将个人信息保护认证分为不含跨境处理活动认证及包含跨境处理活动的认证两类。一旦发布认证机构名单，个人信息保护认证工作就可以正式开展。之前于 6 月 9 日，市监总局、网信办发布《关于开展数据安全管理认证工作的公告》及《数据安全管理认证实施规则》，决定开展数据安全管理认证（“DSM”）工作，鼓励网络运营者通过认证方式规范网络数据处理活动，取得 DSM 认证在一定程度上可作为企业数据安全合规管理工作的证明。加上 2019 年市场监管总局、中央网信办决定开展的 APP 安全认证工作，至此，数据安全三个认证已经成型。（见图 4）

四 .2023 年前瞻

在立法方面，《国务院 2022 年度立法工作计划》将**《网络数据安全管理条例》（网信办组织起草）和《未**

数据安全三个认证概要

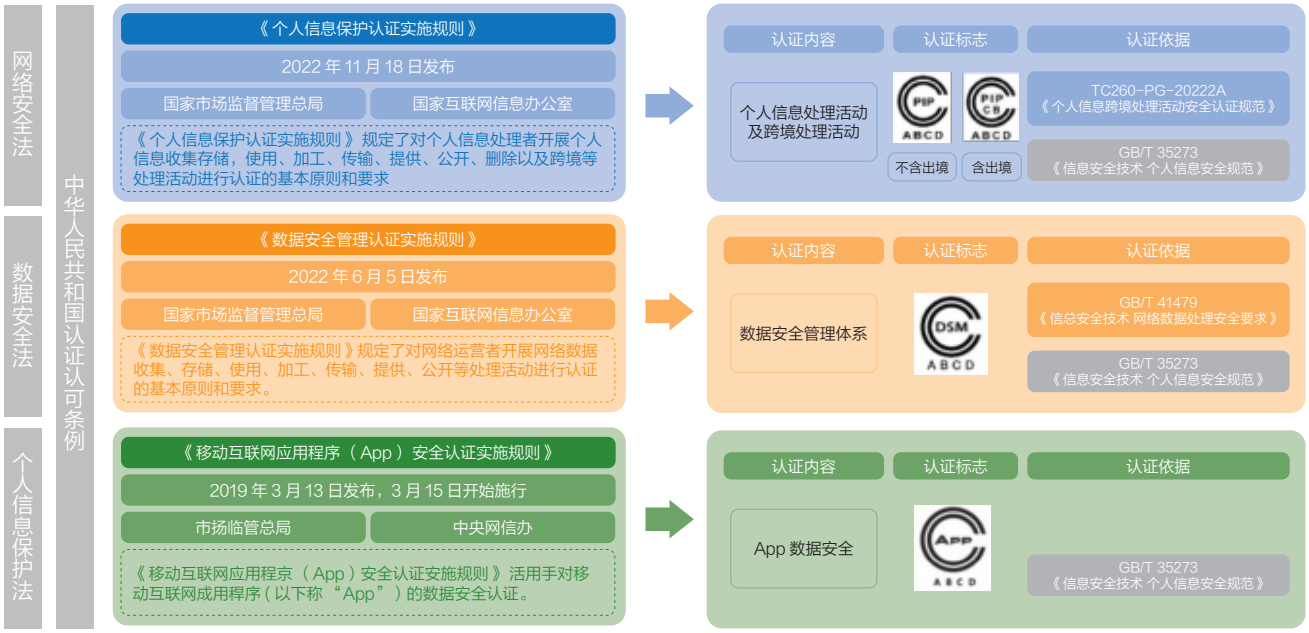


图 4

成年人网络保护条例》（网信办起草）列入年度立法计划。我们认为，考虑到日益加强未成人保护的大环境，《未成年人网络保护条例》于 2023 年出台是大概率事件。而对于《网络数据安全管理条例》，由于条例包含内容非常广泛，有些新设定的监管制度尚存在一定的争议，立法难度相对会更大一些。《工业和信息化领域数据安全管理办法（试行）》在 2022 年底前发布，也给了一个预示，在三部大法框架之下，越来越多的行业数据监管将由部门规章来承担。

数据出境监管机制完全落地实施。《数据出境安全评估办法》已在 2022 年正式实施，2023 年 3 月 1 日该办法所设定的整改宽限期到期，会逐步成为一种常态化的出境监管机制。《个人信息出境标准合同规定》预计会在 2023 年早期公布，作为基础性的个人信息出境合规路径，企业将会更多地采用标准合同来实施跨境数据传输，而对应的个人信息保护影响评估及备案程序，将是企业的挑战。《个人信息保护认证实施规则》公布后，认证活动即将正式开展，可能会成为跨国企业或集团企业的偏爱。监管部门为了促进数据跨境传输监管措施的落地，在 2023 年就严重的违规数据跨境传输行为进行执法处罚，也是顺理成章。

重要数据的识别。重要数据的识别一直是一个困扰业界的问题，可能属于强监管领域中的最大不确定之一，今年开展的数据出境安全评估工作又一次把这个话题拉入视野。我们预计，未来重要数据的识别规范会沿着两个路径徐徐展开。一方面，国家统一的识别规则，比如，《网络数据安全管理条例》和国标《重要数据识别规则》，会确定重要数据的定义、范围、识别原则与识别流程；另一方面，行业重

要数据清单则会通过行业的规章或标准来更加清晰地界定。

与数据有关的国家标准。根据信安标委发布的《2022 年网络安全国家标准立项项目清单》，2023 年值得关注的国家标准制定有《重要数据处理安全要求》、《敏感个人信息处理安全要求》、《个人信息跨境传输认证要求》和《大型互联网企业内设个人信息保护监督机构要求》等。

追逐数据要素化红利。预计在 2023 年随着数据产权制度的逐步建立及确权授权使用规则的清晰，数据要素化政策将进一步推进，各地数据交易机构亦将在数据产品设计和交易方式上日趋活跃。掌握数据资源的企业可以考虑追逐政策和市场红利，盘活数据资产，置身于数据要素化的大潮。12 月举办的中央经济工作会议指出，我国要大力发展数字经济，提升常态化监管水平，支持平台企业在引领发展、创造就业、国际竞争中大显身手。这是一个积极复苏和大力促进数字产业的明显信号，2023 年可以期待有更多的对数字经济的温暖政策。

域外数据风险。2020 年 Schrems II 案的判决，正式宣布欧盟－美国有关个人数据的隐私盾协议无效，但美欧也在今年达成了《跨大西洋数据隐私框架》，欧盟委员会并在今年年底启动了通过欧盟－美国数据隐私框架充分性决定的程序，这将解决跨大西洋数据流动的不确定性。Schrems II 案后，欧盟数据保护委员会（EDPB）明确要求在依据 SCCs 作为数据跨境传输保障机制时应进行数据跨境传输评估（TIA），尤其强调要评估第三国的数据保护法律或实践，以保证数据接收方可以达到与传输方所在国家 / 地区的同等保护水平。目前中国企业广泛采用 SCCs 作为涉欧数据传输的保障机制，而在域外所开展的 TIA 实践中，往往对中国法律环境产生一些误解误读，导致中国企业实施数据传输的成本提升。另外，考虑到国际关系的急剧变化，某些国际关系因素会投射到企业数据跨境风险上，我们要警惕所谓的“数据脱钩”。总之，中国企业将域外数据向境内的传输行为可能会遇到越来越多的法律或非法律的挑战。

作者简介：

陈际红，中伦律师事务所权益合伙人

主要执业领域是网络安全、数据合规、知识产权和 TMT 业务，担任全国律协网络与高新技术委员会副主任、北京市律师协会科技与大数据委员会主任、中国互联网协会法治工作委员会顾问、中国网络与信息法学研究会常务理事、中国计算机行业协会数据安全专业委员会委员、国家市场监管总局发展研究中心新零售和直播电商专家委员会委员和 International Cybersecurity Law Review (ICLR) 编委会委员等职务。

产品技术预测：安全主管 2023 年需把握网络安全十大趋势

过去的 2022 年，网络安全继续成为全社会的关注焦点。网络战在俄乌冲突中风头尽出；勒索攻击给企业造成的损失触目惊心；数据泄露事件愈发频繁、甚至威胁社会安全；供应链攻击无处不在……网络安全已经成为发展的先决条件。

2023 年是贯彻党的二十大精神的开局之年，也是“十四五”规划承上启下之年。1 月 13 日，工信部、国家发改委等十六部门出台《关于促进数据安全产业发展的指导意见》，提出到 2025 年数据安全产业规模超过 1500 亿元。可以预见，2023 年随着国际环境愈加复杂，数字化转型不断深入，网络安全面临的形势将更加严峻，新场景、新威胁势必将驱动网络安全新技术、新产品和新模式的复合创新，进而推动整个行业迈上新的台阶。

作为网络安全的领军企业，奇安信对 2023 年网络安全行业进行了十大趋势预测，一起洞察行业未来的发展脉搏。

趋势一：数据安全成焦点需求 特权账号管理、分级分类紧迫性提升

近年来，数据安全已上升到国家战略高度，《中华人民共和国数据安全法》《个人信息保护法》颁布实施，配套的《数据出境安全评估办法》《网络数据安全管理条例（征求意见稿）》接连发布；国家网信办连续发布了对多家互联网公司实施的数据安全相关审查公告；基础电信、政务、金融、工业等行业陆续制定数据安全管理办法和考核评估规范。

随着数字化转型加速，数据的流存节点和区域变得繁杂、流动量呈现指数级增长、使用方式也不断多样化，政企机构的数据安全防护面临应用场景变化、保护对象变化、管理体系变化的挑战，新环境下滞后的安全建设将造成巨大风险敞口。大量的数据资产攻击、泄漏等事件为政企机构敲醒警钟，Ponemon 和 IBM Security 联合发布的《2022 年数据泄露成本报告》显示，2022 年全球数据泄露规模和平均成本均创下历史新高，数据泄露事件的平均成本高达 435 万美元。

在被动满足合规和自主安全防护双向驱动下，预计未来数据安全建设将持续作为政企机构安全方向的焦点需求。为将数据安全与大数据基础设施和业务应用深度融合，更多政企机构将按“先理后治、补短固底”–“系统治理、体系规划”–“有序建设、持续运营”分

阶段开展体系化的数据安全建设，并在每一个阶段应用相应的产品技术为支撑。其中，特权账号管理技术方案将成为高紧迫、高收益性建设项目。而数据分类分级技术应用也将加速落地，为健全以“数据”为中心的安全保护体系打通“第一道关卡”。

趋势二：寻找中国云原生安全出路刻不容缓

云原生安全是近年来全球网安市场热点，随着我国东数西算战略的部署，国家与地方政务云和企业云建设加快，数字化业务往云上迁移的步伐也在加快，云原生安全需求正在快速增长。

中国信通院在其《云计算白皮书（2022 年）》提出，云原生正通过改进企业的 IT 技术和基础设施，持续加速企业 IT 要素的变革，成为企业用云的新范式。对云原生安全的担忧，正成为企业应用云原生技术的“拦路虎”。中国信通院《2022 中国云原生安全用户调查报告》显示，安全已连续三年成为企业对应用云原生技术的最大担忧。针对微服务、容器和镜像的攻击屡见不鲜。究其原因，近 6 成企业认为技术门槛过高、人才储备不足，仅不到 1 成企业有独立安全部门应对云原生安全事件。

云原生安全应用防护体系建设，需充分考虑制衡和内生。云原生安全是保护云原生应用的安全，涉及企业开发、运维、安全等多个部门。“责任共担”与“能力内生”是云原生安全的两大关键。责任共担不仅是企业内部，还有云服务商和安全厂商之间，这已成为正式行标和关键共识。能力内生则是数字化时代做到统筹发展与安全，做到安全与新技术应用实现“三同步”的基本保障。

预计 2022 年，包括容器安全、云工作负载保护、云安全态势管理、API 安全等安全能力及云原生应用保护平台产品，将为国内所有主流云服

务商的云原生环境，提供稳定可靠的支持。

趋势三：零信任的全面落地将是2023年重点

无论是技术、产品实现，还是用户、资本市场表现，2022年都可以被看作是零信任高速发展的一年。

从国际视野来看，零信任架构已然进入全面落地推广阶段。美国国防、国土安全、情报机构、联邦政府等层面仅在2022年就先后出台十余项政策、规范、标准、参考指南等，全面拥抱零信任架构作为其网络安全战略。在商业层面，无论是全球知名科技公司如微软、谷歌、思科、IBM，还是国际第三方市场机构如Gartner、Forrester、CSA、Deloitte（德勤），也都在积极推出结合自身优势的零信任咨询、产品、解决方案、培训等相关服务。数据上也同样证明了这一点。

根据IBM《2022年数据泄漏成本报告》显示，没有部署零信任的企业其数据泄漏的平均成本为510万美元，而部署了零信任的企业此项成本为415万美元。部署了零信任的企业数据泄漏成本平均降低近百万美元。

反观国内市场，零信任也持续热度高涨。一方面，以远程办公接入为主流场景的ZTNA（零信任网络访问）已然成为2022年国内最热的一个零信任细分赛道，技术、产品、市场、资本均快速入局；另一方面，还是可以看到一些大型政企组织不再满足于单点安全产品的采购，更倾向于选择一家能够真正了解其业务需求、安全痛点、方案适配性强的安全厂商作为其零信任落地合作伙伴，一同构建其自适用其自身的零信任。

2023年，零信任及其在多业务场景的全面落地仍将是每个组织企业的重点工作。零信任的价值毋庸置疑，但如何选择正确的工具、产品和供应商作为零信任战略合作伙伴，以实现预期的业务成果，成功打破安全与业务团队之间的孤岛，将显得愈发重要。仅能解决单点的远程办公安全问题从来不是零信任的初衷；经历过大浪淘沙后，零信任也将逐渐回归其本源，即通过以数据资源保护为核心，遵循最小权限原则，基于身份进行细粒度的权限设置与判定，构建端到端的网络安全体系，旨在移除隐式信任，实现主体身份可信、行为操作合规、计算环境与数据实体有效防护。

趋势四：软件供应链安全的关注度依然炽热

数字化时代，软件无处不在。软件已经成为支撑社会正常运转的最基本元素之一，随着软件产业的快速发展，软件的供应关系也越发复杂多元，近年来，针对软件供应链的安全攻击事件一直呈快速增长态势，造成的危害也越来越严重，特别是由开源软件引发的安全问题更加突出。

奇安信代码安全实验室发布的《2022中国软件供应链安全分析报告》显示，开源软件漏洞的增长速度、安全缺陷和高危安全缺陷的密度，以及典型缺陷的检出率均呈现出增长的趋势；国内企业开发的软件项目100%使用了开源软件，存在已知开源软件漏洞的项目占比86.4%，平均每个项目存在69个已知开源软件漏洞，十几年前的古老开源软件漏洞依然存在于多个项目中，并且通过实例分析也证实了“老漏洞”攻破最新主流产品的软件供应链攻击场景的存在；此外，报告还指出在开源生态系统中，Log4j2之类的关键基础开源软件大量存在，它们一旦爆发漏洞，影响范围和危害可能会非常巨大。

因企业对第三方来源软件，特别是开源软件的检测、管控、治理的不足，可能会带来多种多样的潜在威胁，包括漏洞、后门、恶意代码植入和欺骗、恶意依赖项、编译器破坏、依赖混淆、包完整性篡改、上游源代码删除、开源软件组件停止修复、未按时修复漏洞、包管理器恶意代码上传等，从造成的结果来看，包括数据泄露、勒索病毒、隐私泄露、恶意攻击、恶意挖

矿等。

随着 2023 年我国《软件供应链安全要求（送审稿）》《关键信息基础设施信息技术产品供应链安全要求（报批稿）》《软件产品开源代码安全评价方法》等国家标准的编制或发布，国内企业对软件供应链安全的关注度将进一步提升，在这一方面的工作也会有更多的依据，特别是第三方软件的安全分析和开源软件治理将成为企业保障软件供应链安全的重要任务。

趋势五：合规之后，多云安全防护与托管运营是云安全建设重点

云安全资源池是中国云安全发展当前阶段符合国情及市场需求的必然产物。这一产品形态的价值也开始被全球咨询机构重视。Gartner 在其首个《中国云安全资源池创新洞察》报告中提出，随着数字化和上云用云进程的不断深入，政企寻求以更灵活、敏捷的方式在云上部署安全能力。无论是私有云还是公有云，云服务商往往不会提供企业所需的全部安全能力。云安全资源池支持多云的统一管理、监测和自动化编排，可较好满足“等保”等合规性要求。这一集成型产品可较好的帮助政企缓解其责任之内的云上安全风险。

这点在中国政务云云安全市场，表现尤为明显。IDC 在《中国政务云云安全市场分析》报告中提出，政务云作为关键信息基础设施，当前云安全建设仍以合规驱动为主；基于云安全资源池构建服务化安全能力，是租户安全建设的重要方面。多云安全的统一管理和托管安全运营服务，特别是对信创云的支持，是未来政务云云安全建设要考虑的重点。

云安全管理平台（CSMP）、云安全运营中心（CSC）和云安全托管运营服务（CMSS）的组合方案，将是契合这一发展方向的最佳选择之一。此外，Gartner 融合网络和安全即服务能力的 SASE（安全访问服务边缘）架构，是从访问场景切入，云安全的另一种发展思路。Gartner 在《2022 中国 ICT 技术成熟度曲线》报告中提出，SASE 是数字化转型的关键赋能者，能够有效提升整体的敏捷性、可见性、韧性和安全性。

趋势六：工业关基保护成为工业安全防护重点

工业领域的关键信息基础设施主要包括能源、交通、水利、石油石化和国防科技工业等重要行业，据统计，在关基领域占比超 70%。近年来，对工业领域的关键信息基础设施的网络攻击在全球各地不断出现。仅 2022 年就有欧洲近 6000 台风力发电机组遭网络攻击失去远程控制服务、伊朗国有钢铁公司遭受网络攻击后被迫停止生产、意大利铁路系统遭黑客攻击，致多地车站受影响，越来越多的网络安全事件突显了工业关基网络威胁的严重性。

随着技术的进步，5G、云计算、大数据和人工智能的赋能，使得工业关基的数字化转型提速，其工业控制网络也向着分布式、智能化的方向迅速发展，在提升生产效率的同时，也打破了原本相对封闭可信的环境，网络攻击面随之扩大，网络安全面临严峻挑战。

尤其是《关键信息基础设施安全保护条例》《关键信息基础设施安全保护要求》实施力度和工业关基的内控与合规要求的不断增强，在做好分析识别、安全防护、检测评估、监测预警、主动防御和事件处置 6 个方面

的安全建设的同时，也对工业关基安全衍生了更多需求，如工业资产分级分类管理需求、风险可视化需求、能力聚合需求、运营能力提升和攻防实战演习的需求，这些都成为了工业关基安全建设接下来的重点。基于此，工业关基保护将成为 2023 年工业安全防护重点。

趋势七：攻击检测类产品走向服务化

近年来，中国作为世界第二大经济体稳步崛起，随之而来的境外势力针对我国大型企业、政府等所属相关系统发动愈演愈烈的网络攻击。这其中，工具化、有组织的 APT 攻击更有抬头的趋势，为应对新形势下攻击手段更加隐蔽的特点，弥补传统的基于特征检测的安全设备检测能力的不足，基于威胁情报且可精准实时发现隐藏行为的攻击检测类设备应运而生。

攻击检测类设备通常需收集流量、主机、终端、系统日志数据进行分析，并提供可供分析的告警数据和攻击源，大部分客户在面对这些价值极高但技术门槛也较高的数据时会有无能为力的感觉，为将检测数据的效用最大化，基于攻击检测产品开发（NDR、EDR、CWPP）的服务产品应运而生，并被证明在实战攻防类场景中可发挥巨大的作用，绝大部分企事业单位对这种服务模式普遍认可并在安全建设中持续投入资源。

业界基于攻击检测产品的服务化能力均在普遍提升，在达成业界共识的基础上，预估 2023 年融合产品检测能力和服务人员专业能力的产品，会更多的以服务运营模式推向市场。在此基础上也会进一步推进攻击检测类产品的精耕细作，检测平台之间逐步实现技术融合，从单一检测产品的威胁分析服务升级至多产品跨平台的综合性威胁检测服务。

趋势八：云上实战化安全运营迎来持续关注

新的行业生态不断涌现，企业 IT 系统已经变得愈发复杂。应用和数据已经从核心 IT 环境延伸到了云（包括公有云、行业云、边缘云、私有云），并正在加速延伸到包括物联网、移动设备在内的边缘环境。在边缘创造和处理的数据量正在呈指数级增长。当下及未来的 IT 环境中，办公网、数据中心、多云环境、远程办公等场景将交织在一起。面对愈发复杂的 IT 系统，企业应对数据安全问题需要有体系化的建设思路，不能头痛医头脚痛医脚，必须要依据企业业务发展状况，统筹规划、分布实施。

然而，多数用户在后期运维过程中，还是难以有效应对安全产品的策略调优、网络攻击等工作。在数字经济的今天及未来，安全托管服务（MSS）是弥补客户安全人才短缺无法高效应对网络安全相关问题的首要选择。正如再高档的汽车都离不开 4S 店的维修保养服务一样，网络安全建设后的运维工作同样离不开托管安全服务。在中国，网络安全市场有着自身的特殊性，相当一部分企业的复杂的 IT 系统仍采用本地化或混合 IT 架构方式部署，缺少基础的安全能力，与公有云架构相比，安全建设需要从头做起。因此，很多企业还是希望能够进一步获得技术层面耦合度更高的安全服务，高效

地获得更新的安全能力，以及专业安全人才及时的支持。

随着国际形势的恶化与护网的发展，客户对安全的要求不止合规，逐渐向攻防实战化演进。基于云上的实战化会迎来企业的持续关注。

趋势九：安全运行受到更多重视

长期的网络安全建设投入了大量的设备和人力，各类网络安全产品自身能力发挥不足，安全策略有效性不够。网络安全运行管理和 IT 运行、业务运行管理不融合，各类安全产品产生大量的日志无法及时有效分析，快速准确发现网络攻击事件，事件处置不及时，事件处理效率低下，同时新业务、新技术不断发展，网络攻击隐蔽、多变且持续不断，整体来看，网络安全建设投资难以发挥真正的效能。

随着网络安全的发展，安全运营中心已逐渐成为网络安全建设的标配，但运营中心成熟度普遍不高。相关报告显示，88.6% 的受访企业已经建立了专门的安全运营中心，但总体来看，处于一、二较低成熟度级别的受访单位占比仍然高达 65.5%，大多数单位的安全运营中心的成熟度还比较低。网络安全建设投资是否发挥能效，安全运行是否能切实保障业务，是否具备“能对抗”的实战化安全能力，逐渐成为客户关心的重点。而实战化、常态化、体系化的网络安全运行，将成为安全运行未来的发展趋势。

趋势十：XDR 渐入主流，ASM、BAS 初露锋芒

随着网络攻击日益隐蔽和复杂，攻防对抗从原来的技术之争逐步演变为速度之争。传统的单点安全防护设备无法有效应对安全运营的问题。而 XDR(拓展检测 & 响应) 通过集成威胁检测、分析，响应中不同的产品 & 工具，通过关联分析、事件聚合、威胁情报、自动响应等技术手段形成整体检测和响应策略，从而看见威胁，消除孤岛，提升效率。XDR 的落地价值也正在被主流客户认可。Gartner 预测到 2027 年 XDR 的渗透率将会达到 40%。

由于数字化转型的深入，疫情催生下的远程办公，复杂的数字供应链等导致企业的数字资产暴露面隐患日益增长。而 ASM(攻击面管理) 通过客户的资漏配补数据的融合分析，从攻击者视角帮助安全团队掌握资产安全姿态、收敛资产暴露面、防护网络攻击路径。全面资产可视提升客户安全运营及 IT 运维能力，也是多数客户评估攻击面管理的起始点。

安全防护系统、安全设备的有效性评估一直是困扰着安全主管和安全团队的问题。而 BAS 也是试图解决这个问题。BAS 通过非侵入性的模拟攻击，BAS 评估安全设备的检测有效性，验证安全产品的配置，从而进一步评估安全体系和架构。近两年 BAS 的能力边界也在拓展，覆盖渗透、暴露面验证、红蓝对抗等攻防场景。成为安全团队喜爱的 “瑞士军刀”。

安全产品的平台化、集约化是大势所趋，即不同的安全能力组件在统一的平台架构一下彼此协同和打通。我们也看到越来越多的 XDR、ASM、BAS 彼此集成整合的应用场景。而这些最终给我们的平台最终使用者——安全分析团队带来收益。

安全威胁与技术预测：24 家行业顶级机构看未来

过去一年，海量数据泄露频发，勒索软件攻击日益政治化，进入“国家勒索时代”；俄罗斯与乌克兰爆发冲突，首个大规模现代网络战直接影响关基防护。2023 年网络安全会有什么趋势与变化?

与过去一样，网络安全行业头部公司对新一年的网络安全趋势进行了预测。不过，对 2023 年的预测比以往任何一年都多——网络安全影响日益广泛，已触及社会生活的几乎每个领域，成为各界关注的问题。

现在政府与企业都须快速应对不断变化的网络威胁和数字风险。2023 年，网络安全世界会发生什么? 什么技术会受追捧? 这就是本年度安全预测所试图回答的问题，24 家全球顶级网络安全机构从各自的角度给出了答案。

2023 年安全预测

- 基于乌克兰网络战的经验，未来会发生更多的国家背景网络攻击。
- 多因素身份验证 (MFA) 攻击带来的危害不断增长。
- 2023 年将出现针对太空飞行器和无人机的新攻击。
- 社交媒体攻击激增，尤其是利用深度伪造技术的攻击。
- 伴随公有云普及和数字化转型，网络威胁不断增长。
- 网络攻击导致国外安全保险公司提高门槛，很多机构将失去保险资格。
- 2023 年将出现更多影响社会的关键基础设施攻击事件。
- 黑客攻击将进入元宇宙等新领域，制造更大的问题。
- 企业从端点解决方案转向平台，以降低安全复杂性。
- 勒索软件将卷土重来，出现新的攻击手段，混合攻击流行，制造更多危害。
- 2023 年将出现更多针对非传统技术的攻击，从汽车、智能玩具到智慧城市。

1 趋势科技

- 勒索软件商业模式将发生改变，带来更多数据盗窃和勒索攻击事件。
- 随着云计算应用的不断普及，不同云技术的不一致性以及错误配置将给企业带来安全威胁。
- 用户更加接受混合的工作环境，企业网络边界将扩展到家庭。
- 社会工程成为常青树型的网络威胁——商业邮件欺诈和深度伪造出现新形式。
- 围绕数字藏品和元宇宙等数字新事物的炒作将会减弱，但其背后的区块链技术将会得到真正的发展。
- 攻击者将进一步通过漏洞变现，利用开源软件等被忽视的攻击面进行攻击。
- 工业企业安全技术栈不断提升，但难以满足人员短缺和行业垂直监管的需求。
- 企业在网络安全领域将逐步从单点解决方案转向平台化。

2 奇安信

- 2023 年，全球网安市场短期波动不影响行业长期向好的基本面，产业数字化、数据广泛应用、信创等千行百业的安全需求持续增长，为网络安全产业发展注入持续的动能与活力。
- 针对大型企业机构、结合数据加密和泄露的定向勒索攻击将继续大行其道，保持上升趋势。
- 融合一体化是一直以来的技术趋势，2023 年将看到 IT、OT、IOT 相关安全能力融合的产品或方案。
- 云原生安全与安全运营驱动云安全进入新阶段。

3 卡巴斯基

kaspersky

- 地缘冲突加剧，2023 年将出现创纪录的破坏性攻击，影响政府与关键行业。
- 2023 年邮件服务器成为攻击的优先目标，主流邮件软将曝出 0day 漏洞。
- 重大网络病毒爆发周期 6 ~ 7 年，2023 年将爆发永恒之蓝级别的安全事件。
- APT 攻击者日益关注针对卫星技术的操纵和干扰，卫星技术、生产商和运营商成为 APT 组织攻击目标。
- 新型混合攻击出现，入侵目标并发布内部文件的攻击将会出现更多事件。
- 更多 APT 组织将从 CobaltStrike 转移到其他替代方案。
- 2023 年将出现针对无人机的黑客攻击。
- SIGINT 投递恶意软件攻击行动将会再次出现。

4 Mandiant

MANDIANT

- 更多的攻击由非国家或黑客组织背景的攻击者发起，攻击的目标更多是炫技而不是实际的经济利益。
- 2023 年将爆发更多的勒索攻击事件，欧洲将超过美国成为勒索软件的最大目标。
- 2023 年将出现更多来自俄罗斯、伊朗和朝鲜的破坏性攻击、信息操纵和其他网络攻击行动。

5 Fortinet

FORTINET

- 新型的犯罪即服务产品将会出现。
- 洗钱与机器学习相遇，洗钱即服务 (LaaS) 将出现。
- 虚拟城市将会迎接新一波网络犯罪。
- 数据擦除恶意软件将会激增。
- Web3 面临狂野西部一样的安全威胁。
- 未来需要为量子计算威胁做好准备。

6 Splunk

splunk

- 随着 IT 运营与安全工具、数据的融合，CISO 将在网络弹性方面承担更多责任。
- 勒索软件攻击持续增加，不加密的直接勒索升温。
- 网络犯罪即服务经济将提升网络攻击的数量和有效性。
- 网络战技术将用于商业网络犯罪领域。关键基础设施将很快被武器化，以扰乱政治混乱。
- 企业信息操纵攻击将逐渐成为真正的大问题。
- 供应链攻击将会继续，资金和资源不足的开源将带来严重漏洞。SBOM 将成为强制性补救工具。

- 安全人才危机的两种解决方案：自动化、具有不同背景的多元人才。

7 IBM (X-Force)

- 全球经济衰退临近，2023 年勒索软件攻击激增。
- 网络犯罪即服务生态系统膨胀，全球经济衰退临近，受雇黑客人数将会激增。
- 未来一年社会工程将攻击目标转向 ICS 系统。
- 攻击者发展新型攻击技术，规避 MFA 、EDR 等新安全防护技术。
- 2023 年安全团队加速部署零信任模式，零信任将面临大量实施问题。
- 网络安全通才将是应对人才挑战和能力危机的有效方式。

8 AT&T

- 关键基础设施和公共部门继续成为有吸引力的攻击目标。
- OT 攻击模式将变得更普遍，制造和关基领域面临比数据泄漏更严重的威胁。
- 隐私在美国将受到更多关注，将有更多州通过以隐私相关法规。
- 实现弹性和建设安全文化，需要关注长期目标而不是短期利益至关重要。

- 预算紧缩、IT 和安全人才缺乏，网络安全即服务将继续增长，成为许多公司的最佳解决方案。
- 加强安全基础建设成为重点，漏洞与补丁管理、风险降低及托管扩展检测和响应 (MXDR) 产品成为建设重点。

9 Check Point

- 恶意软件和黑客攻击激增，网络犯罪分子将扩大目标：利用网络钓鱼漏洞攻击 Slack、Teams、OneDrive 和 Google Drive 等商业协作工具。
- 黑客攻击和深度造假不断演进：国家背景的黑客攻击继续增长；深度造假武器化。
- 安全整合：安全团队推动整合 IT 和安全基础架构，以降低复杂性以降低风险，提高防御能力并减少工作量，从而可以实现领先于威胁。

10 Gartner

- 隐私权：到 2023 年底，现代数据隐私法将涵盖全球 50 亿居民、70% 全球 GDP。
- 安全整合加速：到 2024 年，采用网络安全网络架构的组织将能够将安全事件的财务成本平均降低 90%；30% 的企业将部署来自同一供应商的基于云的安全 Web 网关 (SWG)、云访问安全代理 (CASB)、零信任网络访问 (ZTNA) 和防火墙即服务 (FWaaS)。2025 年，80% 的企业将采用一种策略，从单一供应商的 SSE 平台统一 Web、云服务和私有应用程序访问。
- 第三方风险：到 2025 年，60% 的机构将把网络安全风险作为进行第三方交易和业务关系的主要决定因素。
- 勒索立法：到 2025 年，30% 的国家将通过立法，对勒索的赎金支付、罚款和谈判进行监管。
- OT 武器化：到 2025 年，网络攻击者成功地将运营技术 (OT) 武器化，并可能造成人员伤亡。

11 BAE Systems

- 2023 年全球将面临更多勒索软件攻击：从利用流行操作系统的漏洞，到全球软件供应链攻击、以及针对国际关键基础设施攻击。
- 对抗性人工智能达到成为现实威胁的临界点：对抗性 AI 可能会从研究性问题变成真正现实威胁。预计犯罪分子将尝试培训数据投毒和混淆 AI 系统的攻击。
- 网络保险将不再承担国家背景网络攻击的损失，企业将被迫更多采用安全应急响应服务。
- 应对网络安全技能匮乏，未来行业将会有更多安全培训计划。

- 未来将会出现更多产业协作，以弥补政府安全能力的不足。
- 5G 和新型能源网络将会扩大网络攻击面和安全漏洞，安全错误配置将可能影响 5G 网络。

12 Proofpoint

- 全球压力将加剧系统性风险，经济衰退和物理冲突将产生连锁反应：日益复杂、相互关联的数字生态系统加剧现有担忧，引发对系统风险的忧虑，其中任何要素的脆弱性都会威胁整个系统。全球动荡使得我们很难全面了解数字生态系统面临的威胁。系统性风险需要得到持续关注。
- 黑客工具的暗网商业化令网络犯罪不断增长：过去数年，用于实施勒索攻击的黑客工具包成为网络犯罪分子的商品。勒索软件即服务发展成为利润丰厚的暗网经济，导致勒索软件攻击激增。

13 AWS

- 安全将融入组织的所有业务，从而实现持续安全与合规，更容易创造作出正确安全决策的环境。
- 多样性有助于解决持续存在的安全人才缺口：通过推动多样背景的人才投资，以及超越专业技术级别与证书，招聘其他形式才能与技能的人才。
- AI/ML 推动的自动化将带来更强的安全性：AI/ML 给云安全增加关键的自动化能力，实现持续的安全提升。
- 数据保护投资将持续增加：数据安全是客户关心的首要问题，预计 2023 年会出现更多数据保护立法，更多数据保护相关投资，以及自动化技术采用。
- 更高级形式的多因素身份验证将日益普及：随着未来更多转向生物与多模验证方式，多因素验证将会更加易用的同时带来更高安全性。
- 量子计算将令安全受益：后量子时代安全性将会显著提升，当前组织需要确保采用最新的加密技术。

14 Presidio

- 2023 年勒索软件攻击将会持续呈指数级增长。
- 随着组织面临经济下行风暴，将看到更多内部威胁 / 不满离职员工的攻击。
- 身份是网络安全最佳实践的基石。任何框架都是从确保身份保护开始。帐户接管 (ATO)、金融欺诈计划和东 / 西流量移动到提升特权、网络钓鱼 / 深度伪造，一切攻击都始于身份。
- 预计 2023 年将会出现针对云基础设施的集中攻击。这将推动云安全态势评估 (CSPA) 的部署。

- 2023 年的安全计划将根据其对零信任模型的贡献程度来衡量。
- 2023 年安全 PKI 架构的重要性将成为关注焦点，不安全的 PKI 环境会带来被广泛利用的漏洞。

15 Forrester

- 2023 年将有企业高管将因监控员工而被解雇。
- 至少一家全球 500 强企业将因网络安全团队的精疲力尽而被曝光。
- 至少三个网络保险提供商将收购托管检测和响应 (MDR) 提供商。

16 ARMIS

- 公共事业部门的数字攻击面将继续增加，2023 年针对 OT 系统的攻击将迅速扩大。
- 零信任架构部署将提升到新的水平，2023 年将扩展到医疗环境、OT 和 IOT 资产。
- 供应链信任更加受到关注，公共事业部门须要求集成商和供应商具有相同的审慎性。目前美国国防部工业合作伙伴的网络安全成熟度模型认证 (CMMC) 可被民用机构采用。
- 针对关基设施的攻击将会升级，并与国家背景黑客组织的攻击相结合。迫切需要为关键系统部署基本的网络安全功能，重点是部署速度和实现资产可见性。

17 JupiterOne

- 惊人的安全事件与数据泄漏事件将会持续不断发生。
- 安全访问服务边缘 (SASE) 采用不断增长。
- 产品安全兴起和 CISO 控制的总体安全预算下降。产品安全承担更多以前分配给安全团队的职责，公司预算可能会发生变化。

18 思科

- 首席信息安全官需要意识到来自企业内部的压力。高层管理人员将会更加关注风险管理，这有利于首席信息安全官计算网络安全的风险，为降低风险的计划获得更多支持。
- 网络边界已不复存在，网络安全已超出首席信息安全官的组织职权范围。理解第三方安全，并与之协作的能力将日益成为对CISO的要求。
- 大多数机构将采用零信任模式，将其作为安全的起点。首席信息安全官意识到零信任不仅仅是技术问题，现在正逐步解决零信任成功所需的组织和文化变革。

19 源讯

- 多重勒索攻击呈上升趋势。
- 网络弹性将降低攻击恢复的成本。
- 供应链安全将是重中之重。
- 网络安全合规计划将会得到加强。
- 人的因素成为安全战略的核心。

20 Sentinel One

- 吸取惨痛教训：网络安全行业过度热衷关注高级威胁和复杂技术，最严重的威胁并非来自先进攻击技术。2022 年的教训提醒业界关注年久失修的网络架构。
- 网络安全产品只有在“正常工作”时才有效：客户需要整合安全产品和不同安全供应商的协作，而不是无穷无尽的单点解决方案。
- 2023 年没有人可以选择退出网络安全：随着安全预算的减少，成本将成为网络安全规划的主要考虑因素。未来攻击更严重，更多关键基础设施将受到影响。我们正在进入社会工程学的黄金时代，网络钓鱼将继续成为危害身份的主要因素。
- 安全颠覆者就在这里，不会消失：计算能力和人工智能的进步将改变社会工程、欺诈和主动措施（信息 / 影响行动）的有效性。

21 McAfee

- 人工智能成为主流，虚假信息传播增加。
- 新年将出现新骗局（包括加密货币、投资骗局、虚假贷款和元宇宙骗局。）
- ChromeOS 用户增长，未来威胁将显着增加。
- Web3 兴起扩大攻击向量，攻击者利用投资者害怕错失良机的心理发起的威胁持续增长。

22 WatchGuard Technologies

- 网络攻击令保险公司损失惨重，受攻击影响最多行业将面临保险公司更高要求。
- 网络安全评估和验证成为选择供应商和合作伙伴的首要考虑因素，以应对供应链攻击激增问题。
- 首个影响企业的元宇宙黑客攻击将通过企业新生产力功能的漏洞，如远程桌面、用于企业的最新一代 VR/MR 耳机。
- 多因素验证（MFA）的采用推动社会工程攻击的激增。
- 针对新兴自动驾驶汽车服务的攻击有望出现。
- AI 编码工具为新开发项目引入严重漏洞。

23 Security Magazine

- 2023 年需要回归安全基础，提升网络安全基线。远程办公和云化转型意味着需要通过多因素身份验证、密码管理和持续验证来支持强大的访问管理策略，以降低安全风险。
- 网络安全卫生和安全意识将成为 2023 年的重中之重。除了实施更好的访问安全控制，组织还需要赋予员工更好的网络安全意识。这意味着持续的培训和教育，以确保随着威胁的演变，员工准备好成为网络战略的有力捍卫者。

24 微软

- 2023 年网络安全行业将通过更多合作，以统一联合方式解决重大安全问题，包括采用端到端的安全解决方案，以减低安全复杂性。
- 安全数据使用将出现新突破，数据驱动的安全情报将提升云生态的安全性。
- 攻击者将采用人工智能，提升针对关基设施勒索攻击的速度与准确性。
- 攻击者新勒索策略给客户增加赎金支付压力，将助长勒索策略和商业模式创新。
- 网络空间冲突激增，关基设施网络攻击将进一步增长，关键基础设施日益转向云端。安

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

两种模式
模式随心选择

- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

多种形态
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现

- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享

首创“云地结合”模式

打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导

专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

勒索攻击？NO！
实战化服务器安全闭环？YES！

创新技术的应用推动着企业数字化进程的加速，与之相伴的是前所未有的安全威胁和更多未知的安全风险，勒索病毒、0day 漏洞、僵尸木马、恶意攻击扑面而来，网络攻击手段越来越多，无处不存在漏洞，无处不是攻击入口。万物互联使得虚拟世界与物理世界之间的边界正在逐渐打通，一次通过基础物联网设备发起的攻击将直接触达系统的核心。

对企业而言，服务器既是承载公司业务及内部运转的底层平台，也是承载企业数据和创新服务的核心，其稳定、安全的运行是公司正常运转的前提保障，如何解决其安全隐患尤为关键。

勒索攻击泛滥 实战化要求提升

如果说什么最能直观展现服务器安全的重要性，最近几年没有什么比勒索软件攻击更有代表性。最近几年媒体频繁报道可以看到，勒索软件攻击事件特别频繁，且事件发生之后影响也极其严重。

美国石油管道受勒索软件攻击事件就是一件常被安全企业拿来说教客户的一次严重的勒索软件攻击。针对一国政府关键基础设施的网络攻击，直接导致北美十几个州出现能源供应问题。

另外两起勒索软件攻击事件也引起了不小的轰动，其一是针对法国知名军工生产企业泰雷兹的攻击，其二是针对亚洲航空集团的攻击。其中前者不仅在军工领域颇具盛名，其安全防务业务最近几年也在拓展网络安全领域。

这两起勒索软件攻击为企业带来的最大问题在于可怕的数据泄露问题，即数字时代，企业存储在服务器上的数据的安全性至关重要，前者已有 9.5GB 关键资料被勒索组织泄露至公网，后者则有 500 万客户资料存在安全隐患。

勒索软件攻击的威胁代表性是显见且直接的，这种黑客攻击威胁与过去的破坏型电脑病毒完全不同，它更具目的性。也就是说，针对服务器的勒索软件攻击经济目的性是明确的，且在不断发展，从加密数据到窃取数据，再到威胁泄露数据，都是其典型目的性的勒索特征。

鉴于勒索软件攻击威胁的真实性，以及明确的指向性，在李栋看来，这

针对服务器的勒索软件攻击经济目的性是明确的，
且在不断发展，从加密数据到窃取数据，
再到威胁泄露数据，
都是其典型目的性的勒索特征。

也是企业为什么一定要在服务器端做好安全防护工作，因为一旦失守，随着企业所属行业的不同，所要承担的损失将是不可承受的，甚至要高于安全投入的千倍万倍。

“尽管以勒索攻击为代表的服务器安全形势日益严峻，国内依然存在大量组织对安全重视不够，遇到安全问题处置相对混乱。”奇安信资深服务器安全专家李栋说。

不过，近年来以实战为先的情况正在不断向好，大规模的实战演练不仅要求政企单位看得见，更要防得住。“这要求政企单位不仅要有网络安全方面的威胁感知能力，更要针对 IT 资产各级负载实施严密防护，受此驱动，一些头部安全厂商也迎来了业务爆发。”

李栋认为，以下两点是趋势上直观展现的服务器安全重要性的两大因素，其一是勒索软件攻击对服务器端威胁的真实性和广泛性，其二是攻防演练工作要求正转向以防得住实战化为前提。

除此之外，信创国产化将在 2023 年进一步的全面提升应用，覆盖度从试点到全覆盖，信创环境的安全性也需要全面评估和检测。即信创生态当中，第三方安全也将是这个生态的重要组成部分。

服务器安全应以客户视角实战为前提主动求变

作为一名互联网及信息安全老兵，李栋见证了整个服务器安全的发展，从最初的托管服务商拔网线式的“保安全不要业务”粗暴处置，来干预商业因素的恶意攻击，到政策上的合规要求，服务器端开始出现各种形态的安全产品。

> 李栋认为，
> 服务器安全需要用一个相对比较简单的产品，
> 去满足客户更多的需求。

服务器安全的发展，也是人类开掘现代社会经济动作基本方式的一个缩影，从信息化到现在的数字化，都是基于发展不断变化的基础设施服务运作形式。从云的出现，到云的加速普及应用，服务器安全也从过去的简单定义，到精细化定义。

“服务器安全不能像传统模式那样，我只要把流行的病毒防住并杀掉就够了，在服务器端这远远不够。”从云的出现，以及云所承载的时代上的变迁，服务器的安全问题才正式被企业所重视，并且随着云的普及应用，服务器安全也才被正式统一。

调研机构对于云工作负载保护平台（Cloud Workload Protection Platform, 简称 CWPP）技术的定义，在于李栋看来，是服务器安全发展的里程碑事件。因为 CWPP 统一了服务器安全的产品形态，从底层的运维习惯，到系统的防护、应用的防护等，如今安全市场上的服务器安全产品，也大多采用这一系统架构来设计。

从趋势来看，李栋认为服务器安全需要用一个相对比较简单的产品，去满足客户更多的需求。需求的变化，也决定了产品的防护面，以及进一步安全方法论的升级。

比如，服务器安全同样适用现在非常火的安全运营方向——攻击面管理，这项技术理解起来就是不断缩减黑客攻防上的信息差，站在黑客的角度来看自身的薄弱点，在其没有攻击之前，提前收敛系统漏洞。

“黑客如果能够入侵到你的服务器，实际上就是你的攻击面没有做好。”李栋认为，将攻击面管理技术应用到服务器安全领域，可以进一步强调以实战出发的防御效果。

攻击面管理技术加持的服务器安全产品，可以帮助企业迅速摸清旗下 IT 资产情况。比如，企业现在有多少台服务器，这些服务器有哪些漏洞没有修复，开放了哪些危险端口，是否存在弱口令等。

如果企业管理的服务器数量较少，这一工作对于技术应用可能并没有深刻感知，但云时代的特点，以及现在还有更多的企业开始拥抱云原生架构，企业的 IT 资产管理就一定不会再像以前那样简单。

“在以前的数据中心业务当中，客户一次上个 100 台机器，那绝对算得上是大客户了。现在，从虚拟机到容器，企业管理的服务器资产动辄几千几万，在一些重点行业业务场景下，以及规模较大的集团公司当中，甚至要达到几十万、几百万业务主机，要把这么多资产全面的保护起来，实际

上对于企业自身来说也很难。”

而从攻击面管理的角度来理解服务器安全，在一些真实的案例当中，受攻击的一方初始黑入点可能不会是核心的业务系统，而是一些影子资产，因为核心业务通常会有“重兵把守”。攻击面管理技术在于企业的 IT 管理人员精力难以兼顾影子资产，能够实现全面的且及时的隐患排查，攻击面缩减。

摸清资产是服务器安全的第一个入脚点，这项工作要想做好，还要收集更多的攻击面信息，再根据情报，自动化地实现脆弱面修复。从另外一个角度理解的话，攻击面管理其实就是从黑客视角对自身业务系统的全面体检，从而降低入侵风险。

当然，仅仅把攻击面管理做好，将自身暴露面、脆弱面收敛得足够好，只能阻止一部分黑客攻击，却无法阻止高阶黑客的 APT 攻击。再回到 CWPP 系统架构，李栋指出，攻击面管理可对应 CWPP 架构下的 Dev 开发环境检测，而要获得一致的可视性和可控性，面向高阶攻击的 Ops 运行时保护，则是另外一部分同样重要的组成部分。

服务器安全需要拥抱创新

从奇安信椒图服务器安全管理系统来看，这是一款遵循 CWPP 架构开发的一套服务器安全系统，产品搭建了 Dev 开发环境检测与 Ops 运行时保护全链路安全检测，对应前文解释的攻击面管理技术概念的应用，该创新技术应用于实践时可降低服务器 80% 以上的受攻击情况，剩余部分则用于高阶的运行时保护予以解决。

作为一家扎根于安全圈多年的安全厂商，奇安信椒图在攻击面管理技术实践上的理解同样不亚于攻击面管理专业赛道上的那些创新公司，其多维度资产清点，可实现 18 大类，400 多项核心资产上的摸底排查。攻击面管理技术的应用，相较过去，其“事前”的检测能力已经提升了 20%。

“服务器安全产品不能把自己定义成服务器端的漏扫或者防病毒工具，更要为客户交付一种能力闭环。”李栋说。

把资产全面摸清之后，最关键的问题是解决可能存在的漏洞，对于面向生产经营环境的重要角色服务器来说，业内广泛采用虚拟补丁技术，来实现免重启防护。据李栋分享，奇安信椒图在过去一年时间内，在虚拟补丁方面又有明显提升，其中仅数量方面已经接近了 1 万条，数量提升了一倍有余，可面向全行业实现“资产 – 漏洞发现 – 实体补丁 – 虚拟补丁”的闭环管理。

虚拟补丁技术是应用场景上的技术，类似的技术奇安信椒图也在不断地输送给客户，比如，新版本椒图为客户服务器的恶意代码攻击检测方面，提供了两套智能切换方案，在场景应用资源较充沛的前提达成下，可由工作负载本地查杀，反之，则可利用管理中心远程查杀的方式适配客户业务。

在运行时保护方面，奇安信椒图通过遵循 CWPP 架构，搭建了基于服务器深层次防御模型，实现对业务运行时的有效防护，为基于客户的业务实现不同抗体的注入，从而对抗未知威胁，实现安全能力的无限进化。

奇安信椒图通过内置 IN-APP WAF，实现安全内生，该 WAF 具有误报较低不无频繁策略调整等优势，且可实现对加密流量的检测和过滤，其原理是通过代理 HTTP 请求来匹配 WAF 规则，可以有效防御已知 Web 攻击。在云原生的容器化时代，该技术的应用将更加匹配企业业务快速上线需求，将最大化避免业务上线但安全滞后的情况发生。

WAF 也是存在天花板的，其主要问题是基于规则的防护，所以应对未知威胁，仅靠规则还不够。奇安信椒图还引入了新型检测引擎——RASP，用以捕捉未知攻击。RASP 应用运行时自我保护技术通过监控应用脚本的行为及函数调用信息，及时发现恶意代码和漏洞利用行为。

“攻击后背对应着同级的非法操作，非法操作一定会触发一些危险行为。RASP 就是对应攻击行为实现安全的一种对应方式，在于基于规则检测之外的未知攻击能力的补足，其对抗

0day 攻击方面非常有效。”

椒图是国内服务器安全领域内最早引入 RASP 的服务器安全产品之一，在此之外，奇安信椒图通过在服务器系统应用中插入探针，可以实时监控无文件攻击检测。在更多的差异化能力方面，奇安信椒图的运行时防护方面的系统防护能力进一步细化，通过以安全视角下的系统加固进一步提升系统安全能力。

李栋指出，在操作系统安全方面，国内走的是两条路线，一个是重建国产化的操作系统，另一个就是对系统进行底层的驱动层安全加固。椒图属于后者，且有着多年的独立的安全基因和经验，其服务器安全产品也直接移植了这套方案，所以在国内具有极高的领先性。

奇安信椒图服务器安全产品还加入了人的力量。在监控方面，安服团队的加入将产品服务化，也是他们的优势之一。“安服团队的参与，为客户提供了进一步的实战化攻防经验。”其重点解决的是避免纸上谈兵、避免误报等问题。

误报是安全监测类产品常见的弊端问题，但如果存在着大量误报问题，在任何企业应用来看，都是接受不了的。“所以我们这两年，除了不断提升产品性能，也努力地去降低我们的误报。因为海量的误报，对客户来讲是一个很大的负担。”而椒图现在能将误报率控制在非常低的水平，在业界领先。

除了单点技术优势，奇安信椒图的最大优势体现在“整体作战”上。“保护服务器的战斗从来不是单兵作战，而是需要广泛的协同。”李栋强调，作为国内头部的综合类网络安全厂商，奇安信拥有全面、成熟安全产品体系。如此一来，其椒图所在的服务器安全领域，还可以调用其他内部安全模块的能力，所以单从产品方面的协防联动方面，其椒图在交付给客户之后也是无其他竞品能与之匹敌。

如此前奇安信为冬奥做的网络安全防护方案中，就部署了自身 9 大类 55 款的安全产品。在整个方案中，这些安全产品通过协同联动，支撑了从安全运营、感知、研判、防护、处置的全面闭环安全能力。也就是说，客户在应用椒图之后，不仅能获得行业领先的服务器安全能力，还可以将其作为跳板，随时补足其他方面的联动能力。

优化安全场景应用 持续提升产品安全能力

在谈到奇安信椒图未来能力提升方面，李栋从大量的用户基础应用调研总结认为，在不同负载所要求的不同场景下，其能力也不仅仅要求“大而全”，也要有“小而精”的准备。

所以椒图在未来一方面还要不断优化服务器安全管理产品的综合能力，同时也会推出一些“小而精”的产品，这种产品最大的优势，在于可以减小客户平台的资源占用，再针对不同客户的需求，去定制专门的版本。

李栋也强调，能力拆分是基于客户需求为前提的，但能力拆分不会影响椒图整体能力的持续提升，他们也将保证主版本椒图能力持续提升。然后再根据不同的客户使用场景，不同的客户需求去定制专门的版本。

在主版本的能力提升方面，李栋也指出，随着企业拥抱云原生方面的速度加快，服务器安全也需要不断调整，以应对未来趋势应用。主机安全的早期阶段可能只是杀杀毒，到过渡阶段单品泛滥，再到现在成熟阶段的标准化阶段，而随着云原生的应用，CWPP 模型也将会被 CNAPP 模型所替代，安全厂商要做的工作就是不断向前挺进，不断满足客户基于场景应用下的安全需要。

“不仅是互联网厂商在做云原生改造，现在央国企也同样在做大规模的云原生改造，趋势上已势不可挡。”趋势定义威胁，调研机构定义的云原生应用程序保护平台（Cloud-Native Application Protection Platform,CNAPP）将成为服务器安全的未来发展趋势。

在李栋看来，此前业内对于 CNAPP 的认定还处于未来可能，但现在，“可能”二字可以去掉了，他就是未来。安

安全，永远在路上

——中国电子重构网络安全体系探索之路

“央企的网络安全普遍会面临这样的问题：集团太庞大了，组织机构非常分散和复杂，安全短板和漏洞防不胜防；国产化、上云和移动办公等在稳步推进，传统安全体系已经难以胜任；数字化转型加速，安全和业务发展之间难以平衡矛盾，更无法相辅相成、协同并进……”中国电子信息产业集团有限公司（以下简称“中国电子”）运营管理部副主任唐路表示，央企的数字化转型正在全面展开，但网络威胁随之与日俱增，构建适合央企的网络安全防护体系迫在眉睫。

中国电子是国有独资特大型集团公司，主要业务涵盖先进计算、网络安全、集成电路、高新电子、数据治理等战略性、基础性、先导性电子信息产业领域，已成为国内网络安全和信息化领域产业链布局完整的中央企业，员工总数近 20 万，目前拥有包括 17 家上市公司在内的 600 多家所属企业。从 2020 年开始，中国电子基于安全为先、全面上云、融入移动三大原则推动“数字 CEC”战略。在安全方面，中国电子秉承自主化使命、系统化设计、工程化实践、项目化落地、服务化运营的理念，携手安全龙头奇安信，为央企网络安全探索一条可供借鉴的建设之路。

安全为先 构筑一套基于 PKS 体系的数字化底座

网络安全圈经常有这样的比喻，数字化建设如同建高楼大厦一样，在打地基时，沙子做地基；图纸设计时没有考虑安全抗震；建造时安全措施没有同步施工，建成后再补救，无论投入再多成本，也很难坚固牢靠。

同样，中国电子全集团的网络安全也遇到了类似情况，因为安全总是滞后于信息化，导致出现“散、乱、弱、虚”等问题。具体包括：集团过于庞大和分散，所属企业超 600 家，遍布 31 个国家和地区，很难形成统

一的安全防护；海量 IT 资产部署杂乱，梳理难度极大；弱口令、初始口令、被钓鱼、开发代码漏洞等薄弱环节广泛存在；同时，国内安全生态尚不成熟，防护体系仍需完善等。

要解决这些问题，中国电子深刻意识到，数字化建设如同建高楼大厦一样，在图纸设计、打地基、建造等各个环节，就需要提前将安全考虑在内，要始终坚持安全和信息化“同步规划、同步建设、同步运行”。

不过，“同步规划”对于中国电子这类信息化建设相对成熟的央企来说，并不是一件简单的事情。恰好这个时候，即 2020 年，中国电子启动“数字 CEC”战略。（见图 1）

据介绍，中国电子将“数字 CEC”定义为一场管理变革，提出“提升能力，提升效率，控制成本，控制风险”建设目标，希望将“数字 CEC”打造成为数字治理“样板间”、信创生态“试验田”和网信人才“练兵场”。（见图 2）

> 中国电子深刻意识到，
> 数字化建设如同建高楼大厦一样，
> 在图纸设计、打地基、建造等各个环节，
> 就需要提前将安全考虑在内，
> 始终坚持安全和信息化
> “同步规划、同步建设、同步运行”。

“安全为先”是数字 CEC 建设的首要原则。一方面，数字化转型为重构网络安全体系提供了机会，安全能力能够内置到数字化环境中，实现内生安全；另一方面，数字化转型带来了组织管理变革升级的机会，为安全为先、体系化规划提供了多重保障，具体表现在以下几个方面。

图 1：数字 CEC 的战略定位

图 2：数字 CEC 的三坚持两聚焦两关注

首先在组织机制层面进行了保障。数字 CEC 具有良好健全的组织体系，确立了集团董事长亲自来抓的“一把手”责任制，确保让决策贯彻到全集团上上下下。而在执行层面，数字化和网络安全紧密协同、融为一体，打破了沟通隔阂。（见图 3）

其次是为安全规划赋予空前重要的地位。过去安全往往滞后于信息化建设，无法在之前就进行系统性设计和全局规划，数字 CEC 基于国产化平台的全新体系，网络安全可以在规划阶段就实现同步，真正落实了“安全为先”的理念。

最后是构建国产化底座，全面支撑网络安全体系建设。习近平总书记曾指出，“不掌握核心技术，我们就会被卡脖子、牵鼻子……网络强国建设就会成为空中楼阁，成为沙滩上的

图 3：“数字 CEC”技术架构

城堡，经不起半点风浪”。因此，数字化转型最重要的是数字底座的安全，中国电子作为唯一一家以“网络安全和信息化”为核心主业的中央企业，坚持自主与联合创新，积极探索基于 PKS 体系全链条生态产品，实现了从 CPU、内存、操作系统，到信创云的虚拟化资源、容器安全、微隔离，以及移动办公等各个环节的安全融入，全面支撑了集团从底层架构到应用环境的网络安全体系建设。

“安全并不是买两套设备，雇俩人就安全了。而是把整个安全和信息化运维一体化的考虑，从体系规划、系统设计、软件架构之初就融入安全。在开发过程中要融入安全，在上线过程中要融入安全，在运行过程中，整个全生命周期要考虑怎么去安全的运营它。”这就是数字 CEC 中“安全为先”的核心内涵。

从秦长城汲取灵感搭建一张覆盖 600 家分支机构的安全大网

中国电子拥有超过 600 家企业、20 万员工遍布世界各地，互联网出口和信息系统数量更是十分庞大，漏洞、风险可能“潜伏”在集团的任何一个角落。因此，网络安全建设的第一件事，就是统一互联网出口、收敛暴露面、统一防护，避免太多的木桶短板直接暴露在攻击者面前。

在这个时候，安全访问服务边缘（SASE）出现在中国电子的视野。根据 Gartner 的定义，SASE 可将广域网与网络安全结合起来，对移动用户、PC 用户、云资源、数据中心资源、总部资源、分支资源等进行统一管理，并实现网络安全和信息化的深度融合和全面覆盖。在此基础上，

图 4：统一收口的 SASE 体系

中国电子联合奇安信为部署 SASE 做了如下三点规划：

第一是网络安全与信息化的深度融合与全面覆盖，在总部 – 所属企业互联互通的同时，实现统一安全管控。

第二是使所属企业和移动办公的用户能够高效和安全的接入安全资源池的服务节点。

第三是对互联网应用、公有云应用、内部应用进行分级分类的安全运营。

“这就好比秦始皇修长城。”唐路解释说，“战国时期各个国家所筑的长城之间有必然存在很多的间隙，这就给了北方游牧民族大量入侵的机会。所以秦始皇在统一六国之后，在原有的秦、赵、燕三国长城基础上，将长城连成了一片，并派出大将蒙恬统一驻防，这样就避免了遍地烽烟、顾首不顾尾的防守困境。”（见图 4）

对于中国电子而言，SASE 就如同为集团构建了统一安全边界的万里长城，它将网络和安全的功能融合为统一服务模式，从而使企业人员、移动办公员工能够高效安全的接入安全资源池服务节点，实现访问互联网应用、公有云应用、企业内部应用等的统一安全防护和安全运营。（见图 5）

基于SASE的互联网收口安全，仅仅是中国电子“工程化实践”的项目之一。据介绍，包括安全软件国产化适配、零信任身份安全、系统安全、供应链安全、密码专项等 14 个网络安全专项，都在有条不紊的推进，真正从过去局部整改为主的外挂式建设模式，走向深度融合的体系化建设模式。

平战结合
成立一套覆盖 19 万员工的安全运营中心

不过，网络安全不是建设完就可以高枕无忧了。安全日志得有人分析、安全事件得有人处置、安全策略也得有人执行，这是一条永无止境的安全运营之路。

于是，中国电子安全运营中心成立了。

“在安全运营中心，我们建设了集团统一的安全防护运营团队，在平时执行 5×8 小时、战时执行 7×24 小时的监控，通过端口的收敛，集约化保护网络安全。”唐路说，“在 SASE 架构的基础上，安全运营中心为集团量身打造了安全运营的‘三驾马车’。”

第一驾马车是统一的安全运营分析平台，引入冬奥重保模式，确保流量日志“应接尽接”，威胁告警秒级处置。据统计，集团每日接入安全运营中心的日志数量可达十亿级，在实战攻防演习期间会更高，这就需要基于统一的安全分析平台对海量日志进行关联分析，找出其中隐藏的攻击行为。

中国电子通过引入奇安信冬奥重保模式，在冬奥 NGSOC（态势感知与安全运营平台）1000 多条策略规则不断优化和补充，通过“精准规则建模与自动告警处置”，该集团 10 亿级的海量日志及告警，转变为日均千余条可处置的告警，配合自动化响应设备 SOAR，实现秒级的自动化处置，达到“零误封”、减少人员成本，提高防守体系的处置效率。

第二驾马车是平战融合的安全运行机制。针对平时的“管理态”，安全运营中心能够配合业务部门，做好日常的资产、策略、配置、权限、漏洞等相关工作，一旦发现问题，能够精准定位并及时修复，实现平战融合及快速转换。

与此同时，安全运营中心还会定

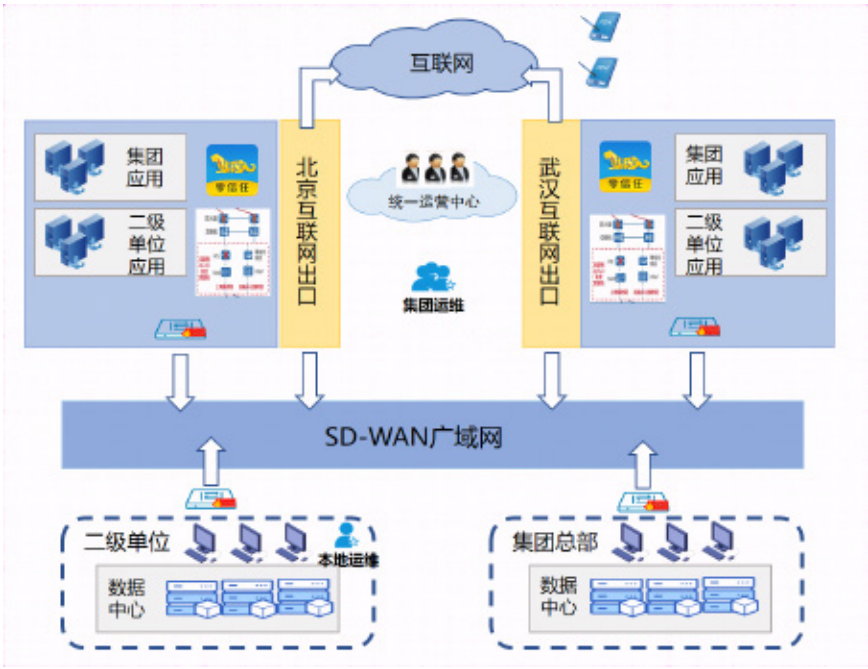


图 5：统一互联网出口安全策略

期组织实战攻防演练，一旦进入战时的“运行态”，就需要基于统一的安全运营分析平台，结合各类安全引擎、威胁情报、漏洞情报等技术手段，在平时资配漏补系统安全的基础上，快速修复漏洞、高危配置等安全风险，并且实现对入侵行为的精准定位、快速响应和全面溯源分析。

第三驾马车是构建专业的安全运营团队。网络安全本质是人与人的对抗，网安工作不只是战时保障，更是日常的持续运营。基于集团网络安全的监控分析及运营需求，在奇安信协同下，安全运营中心设置 8 类岗位、首批成立了 22 人的团队，在中心负责人、监控主管、运维主管的带领下，基于网络安全技术手段，开展常态化安全运营，持续监控分析与处置。（见图 6）

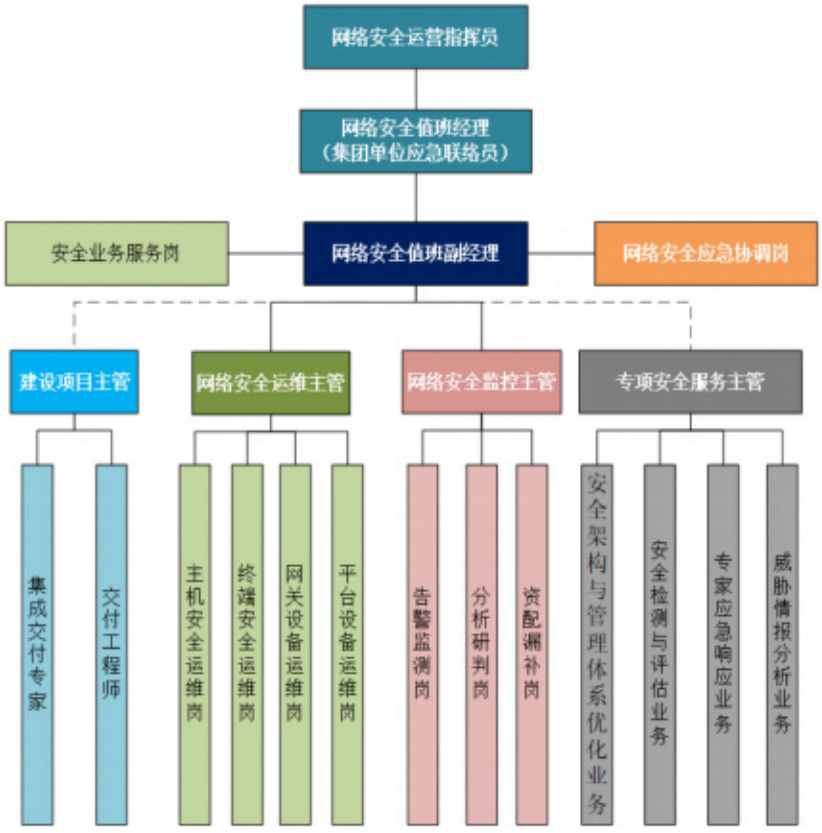


图 6：网络安全运行组织和岗位能力设计

得益于安全运营中心的稳定运转，最终中国电子形成了事件可预警、态势可感知、攻击可追溯、安全内生化、运营一体化、风险可控化的信创环境下的安全效果。

拥抱变化 中国电子网络安全建设的进阶密码

实战是检验效果的最好标准。从 2020 年以来参与实战攻防演练活动结果看，中国电子完成了安全能力进阶的三级跳。尤其是在 2022 年，集团在确保业务应留尽留、平稳运行、基本不受影响的前提下，实现了重要目标“零失陷”。

同时，中国电子还经受了多次极端条件下的严苛考验。在 2021 年年底，集团总部南迁深圳中，网络安全确保了“零中断”“零故障”，满足了“不掉线一秒”要求。

《周易》曰，“上下无常，刚柔相易，不可为典要，唯变所适”。世界上唯一不变的是变化本身，网络攻防尤其如此。如何面对一次次变化带来的冲击和考验？中国电子给出的答案是，拥抱。其中，包括拥抱国产化、自主化趋势，拥抱 SASE、零信任等新技术理念，拥抱龙头企业如奇安信等作为合作伙伴……正是有这种不断拥抱新事物的探索精神，才推动“数字 CEC”建设在坚持安全为先、全面上云、融入移动三大原则下不断深化，为广大央企打造了高标准、可参考借鉴的网络安全体系建设“样板间”。安

规划快一步

奇安信 | BEIJING 2022

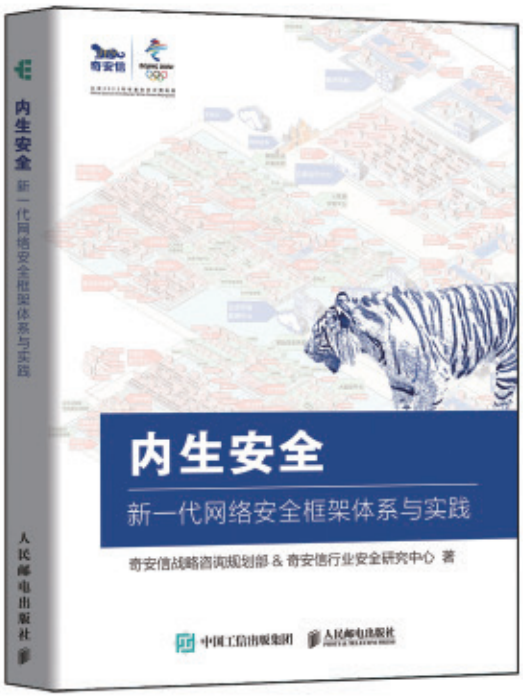
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

新书发布

内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍



- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

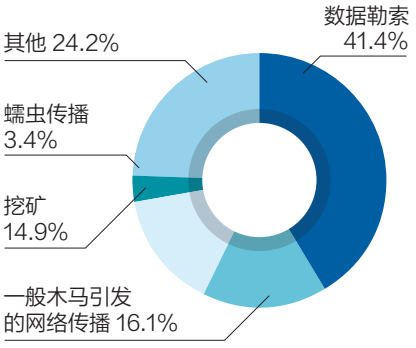
报告：勒索是工业网络威胁最大来源

2022 年 11 月，工业控制系统安全国家地方联合工程实验室、奇安信行业安全中心共同发布了《2022 工业数据勒索形势分析报告》（以下简称《报告》），结合奇安信集团安服团队应急处置案例，对 2022 年工业数据勒索形势进行了深入的分析。

数据勒索是工业网络攻击最大来源

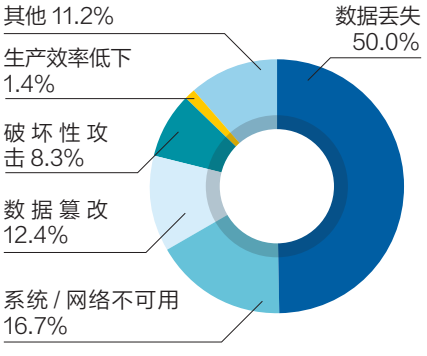
本报告中将因为勒索病毒攻击导致工业企业数据被加密、窃取等事件定义为工业数据勒索事件。《报告》显示，拥有丰富数据、数据勒索损失巨大的工业企业生产系统成为被勒索攻击的首要目标。最近频繁曝出针对大型工业企业的勒索事件，根据国家工信安全中心统计，2021 年公开发布的工业领域勒索事件比 2020 年增长了约 51.5%。

数据勒索也成为数量排名第一的工业网络攻击威胁源，2022 年 1~9 月，奇安信集团安全服务中心共参与和处置了全国范围内 174 起工业网络安全应急响应事件，其中与工业数据勒索相关的安全事件 72 起，占到工业安全应急响应事件的 41.4%。



2022 年 1~9 月
工业数据勒索应急响应事件分布

2022 年 1~9 月，从工业企业遭受数据勒索攻击产生的影响来看，攻击者对系统的攻击所产生的影响主要表现为数据丢失和系统 / 网络不可用



工业企业遭受数据勒索攻击类型
统计分析

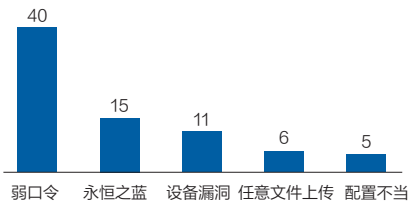
《报告》显示，
拥有丰富数据、数据勒索损失巨大的
工业企业生产系统
成为被勒索攻击的首要目标

等。下图为工业企业遭受攻击后的影响分布。

攻击者将数据进行窃取和加密，导致数据丢失。在上述数据中，有 36 起数据勒索应急响应事件导致工业企业数据丢失，占比 50%。有 12 起应急响应事件导致系统 / 网络不可用，占比 16.7%，攻击者对系统重要数据库进行攻击，严重影响系统和业务的正常运行。

弱口令、历史漏洞是导致数据勒索的最大因素

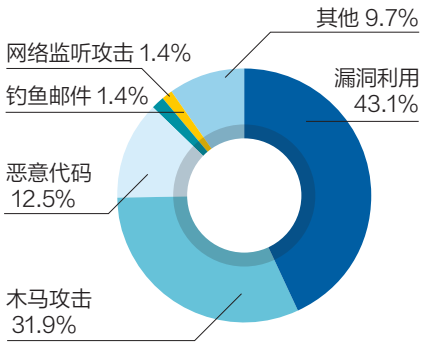
从导致被勒索的原因来看，在 2022 年 1~9 月工业数据勒索应急响应事件中，弱口令是工业企业遭受数据勒索失陷的重要原因，占比 55.6%。



工业企业遭受数据勒索失陷方式

由于弱口令账号的低攻击成本和高命中效果，通过盗取弱口令账号以横向渗透获得特权账号，进而破坏或泄露重要数据资源的攻击行为，给数据安全管理带来很大挑战。

除弱口令外，未修复的历史漏洞也是导致黑客攻击的重要原因。通过对 2022 年 1~9 月工业数据勒索安全事件攻击类型进行分析，漏洞利用攻击手段占比最高，达到 43.1%。



工业企业遭受数据勒索攻击影响统计分析

不过在所有攻击者利用的漏洞中，仅有少数是未公开的 0day 漏洞，多以历史漏洞为主，历史漏洞基本都是由于没有及时升级、更新应用造成的。这也直接反映出客户网络运维人员对下辖网络资产动态跟踪不及时、网络运维缺乏常态巡检机制、对存在的漏洞及安全威胁缺乏应对等问题。

补短固底，做好基础安全防护是当务之急

面对复杂的安全形势，奇安信建议工业企业应先做好基础安全防护，补短固底，在有限资源条件下抵御大部分中低强度网络攻击，在此基础上落实工业数据分类分级，体系规划安全防护体系，有序建设，持续运营。

具体包括以下四点：

第一，补短固底，做好基础安全防护是当务之急。梳理业务，识别重要数据集；做好基础网络安全防护；加强运维和账号安全防护；落实数据实体防护；做好 API 接口安全防护。

第二，结合具体业务场景，做好工业数据分类分级工作。在补齐短板后，工业企业要尽快识别出要重点保护的数据。工业数据本身具有行业差异大、数据类型多的特点，应根据实际业务场景，识别重要和敏感数据资产，形成数据保护目录，对数据进行分类分级，做到“摸清家底，识别关键，分清主次”。

第三，系统治理，体系规划新型数据安全防护体系。工业企业应以数据分类分级为基础落实数据安全治理。通过数据安全治理，摸清现有管理、技术防护措施和执行情况，结合政策法规、行业规范以及业务和信息化战略，做好数据安全组织和制度建设。

第四，数据安全能力有序建设，持续运营。有序建设是在体系规划的基础上，将工业企业数据安全工程任务进行归纳，从紧急程度、技术成熟度、实施难度和预期效果等方面制定量化规则，明确建设优先级、实施周期和投入，完成工业企业数据安全场景建设管控。安

大事记

市政协委员齐向东：筑牢安全底板 打造全球新型智慧城市标杆

1 月 14 日，北京市政协十四届一次会议开幕。来自科学技术界别的市政协委员、奇安信集团董事长齐向东提出，北京应从构建智慧城市安全体系、培育隐形冠军企业两个方面入手，打造模板案例，建设“全球标杆”。为此，齐向东带来了《关于加快将北京打造成智慧城市标杆的提案》《关于加快培育隐形冠军优化北京创新生态的提案》两份提案。

奇安信集团总裁吴云坤当选重庆市第六届政协委员

1 月 12 日，中国人民政治协商会议重庆市第六届委员会第一次会议在重庆开幕。奇安信集团总裁吴云坤当选第六届委员会委员，并出席会议。他此次带来了四份提案：“完善重庆市数字经济安全制度”“建设重庆市网络空间安全‘双能力’保障体系”“加强隐私保护和加大对网络诈骗打击力度”“提高网络安全投入占比”。

奇安信“投资生态 · 2023 共创汇”在京举行

1 月 11 日，奇安信集团“投资生态 · 2023 共创汇”在奇安信安全中心举行。本次共创汇以“聚势汇能，共创共赢”为主题，邀请普华永道、数世咨询、华泰联合证券等集团内外部产业专家成立导师团，并邀请奇安投资、元起资本、中电智慧基金、基石创投、航行资本、中信建投等一众关注网安行业的活跃投资人共同参会。

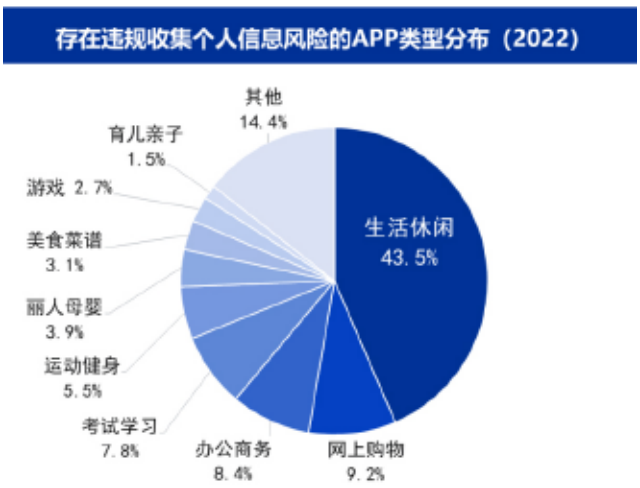
作为 2022 年首届共创汇之后的延续和深化，2023 共创汇共有 50 家网安创企高管、20 位内外部专家顾问、20 位网安赛道投资人出席，嘉宾级别和人数均再创新高，也为奇安信投资生态圈的各家企业在发展的不同阶段提供帮助，建立良性、健康的泛网络安全生态圈，协助网安创业企业发展壮大。

《2022 年度 APP 收集个人信息检测报告》：超 1/4 APP 存在违规

2023 年 1 月 11 日，奇安信对外发布《2022 年度 APP

收集个人信息检测报告》（以下简称《报告》）。

《报告》显示，2022 年度违规 APP 的数量占到了检测 APP 数量的 25.3%，其中类型占比最高的是生活休闲类。检测还发现，违规的 APP 中有 78.8% 都包含了第三方 SDK 违规收集的行为，部分违规 APP 在 100 秒中对个人信息至少收集了 2 次，高频次收集个人信息现象较为严峻。



战略投资软极网络 开启靶场赛道全面战略合作

近日，奇安信完成了对软极网络技术（北京）有限公司的战略投资。本轮融资过后，双方将进一步开启在网络靶场细分赛道的全面战略合作。

谈及与软极的战略合作，陈华平表示双方将开启全面战略合作实现优势互补，奇安信看好软极网络的产品技术、商业模式和未来渠道能力，同时为软极赋能构建更为强大的靶场平台及生态建设能力，满足更多场景下不同客户的需求。

奇安信独家中标天翼云“一城一池”某市信创云安全项目

近日，中国电信公布了 2022 年中国电信天翼云“一城一池”西北某市节点建设工程信创安全产品采购项目中标结果，奇安信网神信息技术（北京）股份有限公司独家中标该项目，中标产品包括云安全管理平台、新一代智慧防火墙、堡垒机等。

该项目不仅是天翼云“一城一池”信创云首个省公司落单项目，更是截止目前运营商落单规模最大的信创项目，为奇安信在信创云安全领域打造了新的标杆。

首届奇安信合作伙伴技术大比武圆满落幕

2022 年 12 月 27 日，奇安信第一届合作伙伴技术大比武总决赛，在湖南长沙奇安星城网络安全运营服务中心举行，入围决赛的 80 名渠道合作伙伴选手通过“网络安全解决方案”“网络安全应急响应”两大赛道进行比拼，最终各决选出冠亚季军一名。

据悉，第一届奇安信合作伙伴技术大比武由奇安信集团渠道管理部联合奇安信解决方案中心、奇安信安全服务子公司共同打造，设置网络安全解决方案与网络安全应急响应两大赛道，面向售前技术人员、售后及安服技术人员展开。

奇安信成为工业和信息化部商用密码应用推进标准工作组首批成员单位

12 月 27 日，工业和信息化部商用密码应用推进标准工作组公布首批成员单位名单，奇安信集团入选。

据悉，工业和信息化部商用密码应用推进标准工作组是

经工业和信息化部批准，统筹开展工业和信息化领域密码应用标准化工作的专业标准化体系，开展标准制修订、技术归口和管理工作。首批成员单位经综合评判企业资信能力、技术水平等多方面因素，遴选出装备制造、电子信息、信息通信、网络安全、密码产品和服务等领域的159家优质企事业单位、科研机构和行业组织。

奇安信获批建设北京市首批网络安全技术创新中心

近日，由奇安信集团牵头建设的“自主可控网络安全技术创新中心”正式获得北京市科学技术委员会、中关村科技园区管理委员会批准，成为北京市首批网络安全领域的技术创新中心。

奇安信集团项目负责人介绍，技术创新中心将从基础技术、应用技术和支撑技术三个层面开展技术攻关，实现安全与计算深度融合，打造领先的专项网络安全能力，为国家全面推进信创工程提供可靠的能力支撑，促进北京市网络安全产业大发展。

奇安信集团董事长齐向东获评首届安全可信创业领军人物

近日，由中关村可信计算产业联盟主办的首届“中国可信计算创新发展三十年成果评选表彰”活动揭晓。

经过5场专家评审会和1场媒体评审会的严格评审后，奇安信集团董事长齐向东获评“2022年度首届安全可信创业领军人物”，奇安信“金融行业信创过渡期终端安全建设方案”获评“安全可信优秀解决方案”。

网安行业唯一！奇安信成为中国联通数字化软件开发者联盟首批成员

12月21日，2022年中国联通合作伙伴大会企业数字化转型论坛线上召开。在论坛上，中国联通数字化软件开发者联盟宣布正式成立，奇安信作为唯一的网络安全行业代表厂商，成为首批数字化软件开发者联盟成员单位。

奇安信集团副总裁李志鹏受邀线上出席会议，并共同参与了中国联通数字化软件开发者联盟启动仪式。

荣誉墙

奇安信获评2022年度信创政务产品安全漏洞专业库优秀技术支撑单位

1月10日，在2022年中国工业信息安全大会“信创安全专题论坛”上，国家工业信息安全发展研究中心公布了

2022 年度信创政务产品安全漏洞专业库优秀技术支撑单位名单，奇安信入选，并获得国家工业信息安全发展研究中心致信感谢。

2022 年中国工业信息安全大会：奇安信连获两大奖项

1 月 9 日，由国家工业信息安全发展研究中心、工业信息安全产业发展联盟联合主办的 2022 年中国工业信息安全大会在北京成功举办。会上进行了工业信息安全产业发展联盟年度系列表彰，奇安信集团连获两大奖项。

凭借在工业信息安全领域长期积累的技术和经验优势，奇安信连续两年获评工业信息安全产业发展联盟“年度优秀成员单位”。

由奇安信集团为多氟多新材料股份有限公司打造的“多氟多化工行业工控网络安全防护建设”，此次获得“工业信息安全优秀应用案例”奖，自 2018 年以来，奇安信集团连续 5 年荣获“工业信息安全优秀应用案例”奖，先后涉及钢铁、化工、制造、管道等多个行业。

Q-SASE 荣获 2022 云安全创新产品奖

近日，2022 年第十七届中国企业年终评选榜单正式揭晓。在产品与技术维度的评选中，奇安信网神边缘安全接入运营平台（Q-SASE）凭借专业成熟的运营服务和助力客户以相对轻量的投入等众多优势，荣获“2022 云安全创新产品奖”。

作为国内首个在超大央企完整落地的 SASE 方案，奇安信 Q-SASE 2.0 以更简易的部署、更全面的服务、更广泛的合作及更高效的运营，迎来了全方位的能力升级。作为奇安信在云安全领域的重要创新成果，Q-SASE 在央国企、运营商、教育等领域有众多客户。

奇安信集团旗下北京网神洞鉴司法鉴定所通过 CMA 认定

近日，北京市市场监督管理局专家评审组对奇安信集团北京网神洞鉴科技有限公司司法鉴定所的质量体系运行情况和技术能力进行了全面审核，顺利通过 CMA 现场评审并取得检验检测机构资质认定证书。

本次 CMA 资质认定范围覆盖声像资料大类别电子数据鉴

定类别中的 4 项检测项目，包括电子数据功能性鉴定、电子数据存在性鉴定、电子数据相似性鉴定和电子数据真实性鉴定。奇安信司法鉴定业务能力、检验质量控制和规范化管理水平获得重要标志性成果。

奇安信入选北京软件和信息服务业综合实力百强企业

12 月 28 日，北京软件和信息服务业协会第十届会员代表大会第三次会议上发布了《2022 北京软件和信息技术服务企业综合实力报告》《2022 北京软件企业核心竞争力评价报告》《北京软件和信息服务业社会责任建设白皮书》。

奇安信集团入选“北京软件和信息服务业综合实力百强企业”“2022 北京软件核心竞争力企业（规模型）”两大榜单。“奇安信网安卫士志愿行动”公益项目入选《白皮书》。

附：2022 北京软件和信息技术服务业综合实力前百家企业名单

序号	企业名称
1	北京百度网讯科技有飛公司
2	小米集团
3	北京京东世纪贸易有限公司
4	航天信息股份有限公司
5	联通数字科技有限公司
6	中软国际有眼公司
7	北京达佳互联信息技术有限公司
8	软通动力信息技术（集团）股份有限公司
9	腾讯科技（北京）有限公司
10	亚信科技（中国）有限公司
11	北京千方科技股份有限公司
12	用友网络科技股份有限公司
13	北京车之家信息技术有限公司
14	东华软件股份公司
15	中国软件与技术服务股份有服公司
16	广联达科技股份有服公司
17	利亚德光电股份有限公司
18	北京全路通信信号研究设计院集团有限公司
19	奇安信科技集团股份有眼公司
20	启明星辰信息技术集团股份有限公司

北京企业 100 强榜单发布 奇安信实力入选四大榜单

12 月 22 日，北京企业联合会、北京市企业家协会在京召开 2022 年度北京企业 100 强工作新闻发布会，发布北京企业 100 强名单及《北京企业 100 强发展报告》。奇安信集团入围“北京企业 100 强”“北京市数字经济企业百强”“北京高精尖企业百强”“北京服务业企业百强”四大榜单。

齐向东荣获 2022 年度 ICT 产业 · 十大影响力人物奖

12 月 21 日，“2022 ICT 企业家大会”隆重召开，会上揭晓了 2022 年度 ICT 产业人物奖、企业奖、产品及解决方案奖榜单。奇安信集团董事长齐向东荣获 2022 年度 ICT 产业 · 十大影响力人物奖。

本届 ICT 产业的年终评选，以“树标杆、促创新、求突破、助发展”为初心，以榜样的力量促进产业链供应链企业互鉴、协作，助推产业高质量发展。主要面向 5G、物联网、工业互联网、人工智能、云计算、大数据、区块链、数据中心、网络与信息安全等 ICT 领域企业及机构组织，针对人物、企业、产品、解决方案等进行评选与表彰。安

奇安信

奇安信威胁情报中心

中国威胁情报行业领军者

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁情报中心

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位，政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

奇安信

新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一 ——数世咨询认证

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器

纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

奇安信蝉联“中国网安产业竞争力50强”第一名

6月23日，中国网络安全产业联盟（CCIA）
揭晓“2022年中国网安产业竞争力50强”榜单。
凭借在网络安全领域领先的技术实力以及突出的市场表现，
奇安信蝉联第一名。

“2022年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	深信服科技股份有限公司
3	启明星辰信息技术集团股份有限公司
4	天融信科技集团股份有限公司
5	华为技术有限公司
6	绿盟科技集团股份有限公司
7	腾讯云计算（北京）有限责任公司
8	阿里云计算有限公司
9	新华三技术有限公司
10	杭州安恒信息技术股份有限公司
11	360政企安全集团
12	亚信安全科技股份有限公司
13	成都卫士通信息产业股份有限公司
14	杭州迪普科技股份有限公司
15	山石网科通信技术股份有限公司