内部资料 免费交流

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

数智安全 内生为本

——2023 北京网络安全大会特刊

第31期

2023 年 7 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。

数智时代需要什么样的网络安全?

随着 ChatGPT 为代表的生成式人工智能的兴起，推动喧嚣多年的人工智能进入加速普及的 2.0 阶段，人类社会从而进入数智时代，显著改变信息社会经过 80 年形成的社会生产、生活和治理模式。

在数智时代，数据成为社会运营的基础和驱动力：数产生了智，智又产生了新的数，在螺旋式上升的循环中创造了一个繁荣的数智世界。在数智时代，机构利用人工智能、区块链、机器学习等下一代技术，改善运营并改变游戏规则；机构利用从数据中获取的智能，提供更好的服务、简化流程、更好地利用员工才能，同时创造出新的业务模式。未来，每个行业有可能围绕少数行业智能中心进行重新组织，推动行业的全球整合。

数智时代的网络安全会有何不同？在 7 月初举办的 BCS2023 北京网络安全大会以“数智安全内生为本”为主题，邀请中外嘉宾围绕能源网络安全、金融网络和数据安全、安全运营、AI 大模型安全等主题展开交流，深入探讨如何应对数智时代的安全挑战。

全国政协委员、全国工商联副主席、奇安信集团董事长齐向东认为，安全是数智时代的基础。在数智时代，如果数据被删除或篡改，盲区将变得无穷大，事故的边界将不可控制，社会生产可能停摆。因此，让网络更安全、让数据更安全，将成为数智时代政府、企业和社会组织的主要任务。在数智时代，任何一场重大的网络攻击都有可能造成前所未有的影响，我们似乎越来越输不起。因此，齐向东认为，“数智时代的安全要以‘零事故’为目标。”

面向数智时代的网络安全，需要依靠脚踏实地的实践与摸索，趟出一条真正可行的道路来。

针对数智时代的安全挑战，齐向东认为，“数智安全要以内生为本。”内生安全强调从规划、建设、体系运行保障最终实战结果，再用实战结果评估指导新的规划、建设、体系运行，在螺旋式上升的循环中，保卫数智世界的安全。

中国科学院院士冯登国则从技术创新角度阐释了安全技术发展如何应对现实挑战。他认为，网络空间安全技术呈现出零化、弹性化、匿名化、量子化和智能化五个基本特征，将引领网络安全技术的未来发展。他认为，未来通过充分发挥五个基本特征，将可以应对日益复杂和多样化的网络安全威胁，构建更加安全可靠的网络空间。

BCS2023 北京网络安全大会上，既有来自金融、能源行业专家的安全实践分享，还有针对 AI 大模型安全、安全运营等前沿安全技术等的探讨，更有最新安全技术与方案的发布。希望这期的《网安 26 号院》能帮助您全面了解同行经验和技术前沿。

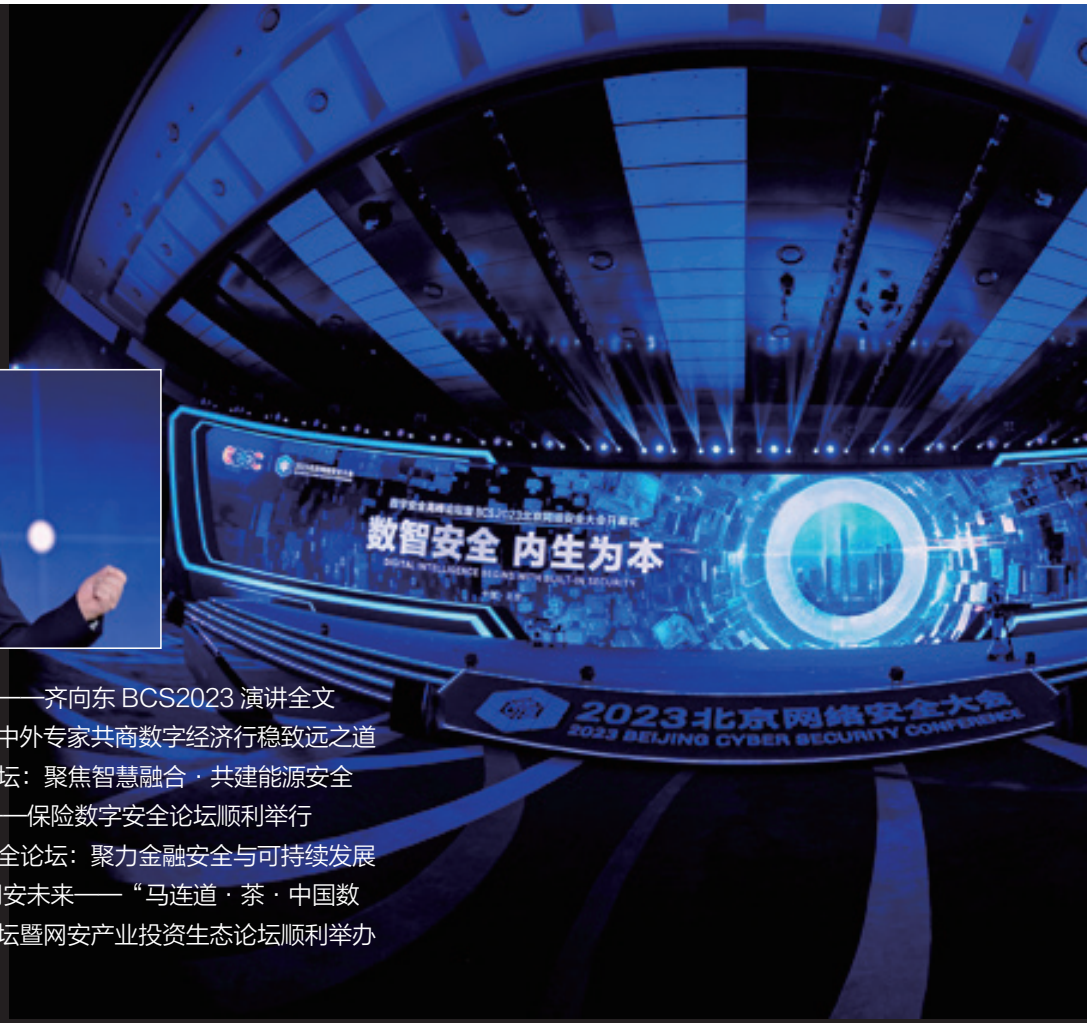
总编辑

李建平

2023 年 7 月 1 日

CONTENTS 目录

产品战略



奇安资讯

技术前沿

安全新品

《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
安全叨客主编：魏开元
奇安资讯主编：陈　冲
报告速递主编：闫　延
专　　栏主编：李建平

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
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
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 7 月 26 日

栏目主编　王彪

政策篇

国内，部分金融机构外包服务商网络安全风险频发，金融监管总局下发《关于加强第三方合作中网络和数据安全管理的通知》；

国际上，美国白宫连发两份文件，从预算制定、实施指引两个层面推动联邦机构落实国家网络安全战略。

国内

工信部、金融监管总局联合印发《关于促进网络安全保险规范健康发展的意见》

7 月 17 日工信部官网消息，工业和信息化部与国家金融监督管理总局联合印发《关于促进网络安全保险规范健康发展的意见》（以下简称《意见》），围绕完善政策标准、创新产品服务、强化技术支持、促进需求释放、培育产业生态等提出了 5 方面 10 条意见。《意见》明确，鼓励保险公司面向不同行业场景的差异化网络安全风险管理需求，开发多元化网络安全保险产品。面向重点行业企业开发网络安全财产损失险、责任险和综合险等，提升企业网络安全风险应对能力。面向信息技术产品开发产品责任险，面向网络安全产品开发网络安全专门保险，为信息网络技术产品提供保险保障。面向网络安全服务开发职业责任险等产品，转移专业技术人员在安全服务过程中因人为操作可能引发的安全风险。

七部门联合公布《生成式人工智能服务管理暂行办法》

7 月 13 日网信办官网消息，国家网信办联合国家发展改革委、教育部、科技部、工业和信息化部、公安部、广电总局公布《生成式人工智能服务管理暂行办法》（以下简称《办法》），自 2023 年 8 月 15 日起施行。《办法》提出，对生成式人工智能服务实行包容审慎和分类分级监管，明确了提供和使用生成式人工智能服务总体要求，提出了促进生成式人工智能技术发展的具体措施，明确了训练数据处理活动和数据标注等要求。规定了生成式人工智能服务规范，明确了生成式人工智能服务提供者应当采取有效措施防范未成年人用户过度依赖或者沉迷生成式人工智能服务，对图片、视频等生成内容进行标识，发现违法内容应当及时采取处置措施等。此外，还规定了安全评估、算法备案、投诉举报等制度，明确了法律责任。

四部门调整《网络关键设备和网络安全专用产品目录》

7 月 3 日网信办官网消息，依据《中华人民共和国网络安全法》，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门更新了《网络关键设备和网络安全专用产品目录》，现予以公布，自印发之日起施行。据悉，新版目录相较 2017 年首版目录，网络关键设备为 4 类，保持不变；网络安全专用产品由此前的 11 类扩大为 34 类，范围由此前的限定性能以上扩大为不限性能的产品功能描述，类别和范围均大幅提升。

《北京市智能网联汽车政策先行区数据分类分级管理细则（试行）》发布

6 月 30 日北京市高级别自动驾驶示范区公众号消息，北京市高级别自动驾驶示范区工作办公室发布《北京市智能网联汽车政策先行区数据分类分级管理细则（试行）》（以下简称《细则》）。《细则》为车路云一体化数据分类分级

提供细化的落地指引，明确数据分类策略，定量数据定级方法并提供实操样本案例，有效推动形成依法规范、协同建设、共享红利的示范区数据安全发展模式。《细则》核心亮点包括构建多维统一的数据层级、落实保护措施贯穿数据流转全生命周期、压实企业数据治理责任。

金融监管总局发布《关于加强第三方合作中网络和数据安全管理的通知》

6 月 27 日中国证券报公众号消息，国家金融监督管理总局发布了《关于加强第三方合作中网络和数据安全管理的通知》（以下简称《通知》）。《通知》指出，近期，部分银行保险机构的外包服务商发生多起安全风险事件，主要涉及企业微信服务风险、科技外包风险两类情况，对银行保险机构的网络和数据安全、业务连续性造成一定影响，暴露出银行保险机构在外包服务管理上存在突出风险问题。《通知》要求，银行保险机构应强化“服务外包、责任不外包”的主体意识。银行保险机构应加强风险评估和尽职调查，加大监控力度和违规问责，加强对外包服务商的监督管理和实地检查，合作结束后必须下线相关系统并删除数据。

美国国家网络总监办公室发布《国家网络安全战略实施计划》

7 月 13 日白宫官网消息，美国国家网络总监办公室公布《国家网络安全战略实施计划》，为实现国家网络安全战略的前瞻性目标提供了一份“路线图”。拜登政府称，该文件有两个首要目标：确保公共和私营部门中“规模最大、能力最强、地位最有优势的实体”承担更多责任，以降低网络风险；出台鼓励投资网络安全的长期激励措施。该文件提出了 69 项举措，如建立全球 SBOM 数据库、更新国家网络事件响应计划、加强预算支持等，为负责实施变革的数十家联邦机构明确分配责任，设定最终期限，推动它们加强网络安全监管、简化监管流程。据悉，该文件预计明年将滚动更新。

欧盟委员会通过“欧盟 – 美国数据隐私框架”的充分性决定

7 月 10 日欧盟委员会官网消息，欧盟委员会通过了关于“欧盟 – 美国数据隐私框架”的充分性决定。该决定认为，根据新框架，从欧盟转移至美国公司的个人数据，美国确保了可以与欧盟相提并论的足够保护水平。基于新的充分性决定，个人数据可以安全地从欧盟流向参与此框架的美国公司，无需实施额外的数据保护措施。新框架包含新的约束性措施，且引入了美国第 14086 号行政命令的内容，以回应欧盟法院在先前裁决中提出的关切，包括限制美国情报机构对欧盟数据的访问、建立数据保护审查法院等。这是继安全港协议、隐私盾协议之后，美欧试图建立稳定的跨大西洋数据流动安排的尝试。

美国 CISA 发布针对云业务应用的扩展可见性参考框架指南

6 月 27 日 CISA 官网消息，美国网络安全与基础设施安全局（CISA）发布《安全云业务应用（SCuBA）扩展可见性参考框架（eVRF）指南》，为组织部署云服务时提供指导，用于识别可见性数据、减轻威胁、了解特定产品和服务提供可见性数据的程度，并确定存在的潜在差距。CISA 负责网络安全的执行助理 Eric Goldstein 表示，“该指南将为包括联邦机构在内的所有组织，改进网络安全和可见性方面的差距，这些差距长期以来阻碍大家充分理解和管理网络风险。”

美国白宫发布《行政部门 2025 财年预算网络安全重点任务》

6 月 27 日白宫官网消息，美国白宫管理和预算办公室（OMB）和国家网络总监办公室（ONCD）联合发布备忘录《行政部门 2025 财年预算网络安全重点任务》（M-23-18），概述了联邦机构编制 2025 财年网络安全预算时，需落实的五大重点任务。备忘录五大重点任务与拜登政府今年 3 月发布的国家网络安全战略五大支柱保持一致，包括：保护关键基础设施、破坏和摧毁威胁行为者、塑造市场力量以推动安全和弹性、投资更有弹性的未来、建立国际伙伴关系以追求共同目标。两大办公室将审查联邦机构提交的预算提案，“确定潜在差距”和“解决这些差距的潜在方案”。

事件篇

全球关键基础设施近期频频曝出网络安全事故。日本最大港口名古屋港因勒索攻击被迫暂停运营；俄罗斯卫星网络被黑后连接持续中断；加拿大石油巨头被黑影响全国加油站支付服务；国内某银行系统遭非法入侵，泄露 1300 余万条储户信息等。

因一低级漏洞，孟加拉国政府网站泄露约 5000 万公民身份数据

7 月 10 日 TechCrunch 消息，孟加拉国出生与死亡登记主管办公室网站存在漏洞，泄露了大量公民个人信息，包括全名、电话号码、电子邮箱地址和国民身份证号码。Bitcrack 网络安全公司研究员 Viktor Markopoulos 在 6 月 27 日意外发现了此次数据泄露，他表示在谷歌搜索一个 SQL 错误时，第二个结果就是这些数据。据他估计，该网站泄露了约 5000 万孟加拉国公民的数据，该国总人口约 1.63 亿。Viktor 联系了孟加拉国电子政务计算机事件响应小组（CIRT），该小组在 7 月 9 日修复了该漏洞。

公安部网安局通报多起重点单位网络攻击入侵窃密事件

7 月 7 日公安部网安局公众号消息，公安部 6 日在京召开维护国家网络和数据安全新闻发布会，公安部网安局相关负责人在会上通报了多起重点单位网络攻击入侵窃密典型案例。2022 年 4 月，四川公安机关破获一起非法侵入控制税务系统案，抓获犯罪嫌疑人 4 人，查明该团伙虚开发票 6231 张，非法牟利 2000 余万。2022 年 4 月，安徽公安机关侦破一起非法控制计算机信息系统案，打掉一个专门从事漏洞扫描、木马植入等违法活动的犯罪团伙，查获木马控制服务器 12 台、被控主机 700 余台、虚拟账号 17 万余组。2022 年 8 月，重庆公安机关侦破一起非法侵入银行系统案，抓获犯罪嫌疑人 10 名，查明该团伙获取储户信息 1300 余万条。此外，北京、江苏、陕西、上海、浙江等地公安机关侦办多起境外黑客组织对我能源、军工、金融、教育等领域重点单位实施的网络攻击入侵窃密事件，迅速查明情况、有效堵塞漏洞、及时消除隐患，确保重点单位网络安全。

英国知名金融科技公司漏洞遭利用，近 1.5 亿元资金失窃

7 月 9 日英国金融时报消息，多位知情人士透露，英国知名金融科技公司 Revolut 的美国支付系统在去年爆出漏洞，网络犯罪分子在数月内盗取了该公司超过 2000 万美元资金（约合人民币 1.44 亿元），直到 Revolut 封堵漏洞才停止。据知情人士透露，该漏洞源自欧美支付系统的差异，当某些交易被拒绝时，Revolut 会错误地向账户退款。这种欺诈行为不会影响顾客账户，而会窃取公司自有资金。由于 Revolut 风控能力不足，该漏洞遭利用了数月之久，直到公司的合作银行发出警告才被发现。

美国供水设施又遭黑：加州一水厂核心系统服务器被破坏

7 月 7 日 SecurityAffairs 消息，美国司法部发布新闻稿称，加州特雷西市居民 Rambler Gallo 被控，对该市愉景湾镇水处理设施发动网络入侵，并蓄意破坏一台计算机。该设施负责全镇 1.5 万居民的饮用水处理和废水处理。Rambler Gallo 在拥有该设施的水处理厂就职期间，故意卸载了水处理厂的主要运行和监控系统，随后关闭了运行这些系统的服务器。该系统保护整个水处理系统各项指标，包括水压、过滤和化学物质水平。Rambler Gallo 面临最高 10 年的监禁和 25 万美元罚款。

日本最大港口名古屋港因勒索攻击被迫暂停运营

7 月 5 日 BleepingComputer 消息，日本最大、最繁忙的港口名古屋港遭受勒索软件攻击，集装箱码头运营受到影响。名古屋港务局 5 日发布了“名古屋港综合终端系统”（NUTS）故障通知。NUTS 系统是控制名古屋港所有集装箱码头的中央系统。通知称，故障原因是当地时间 7 月 4 日上午 6:30 左右发生的一次勒索软件攻击。名古屋港务局正努力恢复 NUTS 系统，后续官方公告显示，港口系统在 6 日上午恢复，运营将在下午晚些时候恢复。运营恢复之前，所有使用拖车的码头的集装箱装卸作业已被取消，给港口造成了巨大的财务损失，严重干扰了往来日本的货物流通。

非法盗取人民大学部分学生信息，嫌疑人已被刑事拘留

7 月 3 日南方都市报消息，据微博 @ 平安北京海淀 消息，针对“中国人民大学部分学生信息被非法获取”的情况，嫌疑人马某某（男，25 岁，该校毕业生）涉嫌非法获取该校部分学生个人信息等违法犯罪行为。目前，马某某已被海淀公安分局依法刑事拘留，案件正在进一步调查中。此前 1 日有网友爆料称，中国人民大学某毕业生在校期间盗取学校内网数据，收集全校学生个人隐私信息，包括照片、姓名、学号、籍贯、生日等，公开发布在网站上进行颜值打分。目前，该网站已无法进入。

台积电遭遇天价数据勒索：硬件供应商被黑，泄露少数内部数据

7 月 1 日 ArsTechnica 消息，全球最大芯片代工企业台积电在 6 月 30 日表示，由于硬件供应商 Kinmax Technology 发生一起“安全事件”，攻击者获取了台积电企业网络中一些服务器的配置文件和设置。Kinmax 声明称测试环境遭遇网络攻击，已关闭受损系统并通知受影响客户。台积电代表表示，此事件未影响公司业务运营，也没有泄露任何客户信息。此消息公布前不久，知名勒索软件团伙 LockBit 在网站上“点名”台积电，威胁索要 7000 万美元赎金，否则将公开窃取的数据。

俄罗斯卫星网络遭黑：连接持续中断 攻击者“声援”瓦格纳集团

6 月 29 日 CyberScoop 消息，有黑客组织于 28 日晚间发布消息称，攻击并瘫痪了俄罗斯重要卫星网络服务 Dozor，窃取了近 700 份文件公之于众，声称为瓦格纳集团“鸣不平”。Dozor 主要为俄罗斯军队、情报、电力、油田等关键行业机构提供服务。互联网观测公司 Kentik 发现，Dozor 的互联网连接至少发生了数小时中断。Dozor 母公司 Amtel-Svyaz 确认云基础设施遭到了攻击，可能需要数周时间才能让网络全面恢复运行。自俄乌战争爆发以来，已发生多次卫星网络攻击事件。

全国 2500 余家企业遭“木马”攻击：企业营销号被控制 用户信息全泄漏

6 月 28 日钱江晚报公众号消息，杭州网警召开新闻发布会通报侦破一起案件，抓获全国各地给企业投放木马病毒的一系列犯罪团伙。据介绍，有些商场的品牌专柜营业员被犯罪嫌疑人以扫一扫二维码换取小礼品的方式所骗，手机里的企业员工营销号被犯罪嫌疑人控制，进一步骗取企业营销号管理员的信任，最终控制了企业的计算机，得以盗取企业的客户数据。杭州网警经线索排摸发现，这是一类网络黑灰产，专门给企业投放木马、从而盗取高净值用户信息、卖到境外。境外的诈骗集团梳理了这些数据以后，再按照客户的特征进行有针对性的精准诈骗。经查，全国涉案的被侵害企业有 2500 余家，涵盖证券投资、医疗保险、科技教育等多个行业领域。

加拿大石油巨头被黑影响全国加油站：支付服务瘫痪 仅支持现金

6 月 26 日 BleepingComputer 消息，国际石油巨头森科能源遭网络攻击，导致子公司加拿大石油公司全国 1500 余家加油站支付服务受到影响，或无法使用信用卡、积分支付油费，只能使用现金。森科能源表示已采取措施应对此次攻击，并通报有关部门。森科能源是全球第 48 大上市公司，也是加拿大最大的合成原油生产商之一，年收入达 310 亿美元。

漏洞篇

近期多款关键软件曝光漏洞，如 Linux Kernel、Apple WebKit、泛微 E-Cology 等基础软件，SonicWall GMS/Analytics、FortiOS、FortiProxy 等安全软件。鉴于上述漏洞影响范围较大，建议用户尽快自查更新。

Linux Kernel 本地权限提升漏洞安全风险通告

7 月 17 日，奇安信 CERT 监测到 Linux Kernel 本地权限提升漏洞 (CVE-2023-31248)，由于 nft_chain_lookup_byid() 函数没有检查链是否处于活动状态，导致 nft_chain_lookup_byid 可以引用已停用的链，导致释放后重用，进一步利用可以将权限提升至 ROOT 权限。目前该漏洞细节及 PoC、EXP 已公开，奇安信 CERT 第一时间复现此漏洞，同时监测到主流厂商、Linux Github 主分支已修复此漏洞。鉴于漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache RocketMQ 远程代码执行漏洞安全风险通告

7 月 14 日，奇安信 CERT 监测到 Apache RocketMQ 远程代码执行漏洞 (CVE-2023-37582) 技术细节及 PoC 已在互联网上公开。此漏洞是由于 CVE-2023-33246 补丁未修复完全，当 RocketMQ 的 NameServer 组件暴露在外网，且缺乏有效的身份认证时，攻击者可以利用更新配置功能，以 RocketMQ 运行的系统用户身份执行任意命令。目前，奇安信 CERT 已分析并复现此漏洞，鉴于此漏洞影响较大，建议客户尽快做好自查及防护。

泛微 E-Cology XML 外部实体注入漏洞安全风险通告

7 月 13 日，奇安信 CERT 监测到泛微官方发布安全补丁更新，修复泛微 E-Cology XML 外部实体注入漏洞 (QVD-2023-16177)。由于后台逻辑对 XXE 漏洞防护存在缺陷，导致远程未授权攻击者可绕过现有防护实现 XML 外部实体注入，最终可能造成敏感信息泄露，且进一步配合其他漏洞可能造成远程命令执行等危害。目前，奇安信 CERT 已分析并复现此漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

SonicWall GMS/Analytics 多个高危漏洞安全风险通告

7 月 13 日，奇安信 CERT 监测到 SonicWall 官方发布的安全风险通告中包括多个高危漏洞，SonicWall GMS/Analytics SQL 注入漏洞 (CVE-2023-34133)、SonicWall GMS/Analytics Web 服务身份认证绕过漏洞 (CVE-2023-34124)、SonicWall GMS/Analytics CAS 身份验证绕过漏洞 (CVE-2023-34137)。未经身份验证的远程攻击者利用这些漏洞可以获取敏感信息或执行危险操作。鉴于这些漏洞影响范围较大，建议用户尽快自查更新。

FortiOS 和 FortiProxy 缓冲区下溢漏洞安全风险通告

7 月 13 日，奇安信 CERT 监测到官方发布了 FortiOS 和 FortiProxy 缓冲区下溢漏洞 (CVE-2023-33308)，在 FortiOS 和 FortiProxy 中存在缓冲区下溢，在代理策略或防火墙策略为 SSL 深度包检测模式情况下，未经身份认证的远程攻击者通过精心设计的数据包利用该漏洞可以执行任意代码或命令。鉴于该漏洞影响范围较大，建议用户尽快自查更新。

Artifex Ghostscript 代码执行漏洞安全风险通告

7 月 13 日，奇安信 CERT 监测到 Artifex Ghostscript 代码执行漏洞 (CVE-2023-36664)，由于 Ghostscript 对管道设备（带有 %pipe% 或 | 管道字符前缀）的权限验证处理不当，未经身份认证的远程攻击者通过特制文件利用该漏洞可以实现代码执行。目前此漏洞的技术细节已在互联网上公开，漏洞的现实威胁进一步上升。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apple WebKit 远程代码执行漏洞安全风险通告

7 月 11 日，奇安信 CERT 监测到 Apple 官方发布 Apple WebKit 远程代码执行漏洞 (CVE-2023-37450)。远程攻击者可以诱骗受害者打开特制网页，成功利用此漏洞可在目标系统上执行任意代码。鉴于此漏洞影响范围较大，且已发现在野利用，建议客户尽快做好自查及防护。

泛微 E-Cology SQL 注入漏洞安全风险通告

7 月 10 日，奇安信 CERT 监测到泛微官方发布安全补丁更新，修复泛微 E-Cology SQL 注入漏洞 (QVD-2023-15672) 在内的多个漏洞。远程未授权攻击者可利用此漏洞获取敏感信息，进一步利用可能获取目标系统权限等。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Smartbi 登录代码逻辑漏洞安全风险通告

7 月 3 日，奇安信 CERT 监测到 Smartbi 官方发布安全更新，修复了 Smartbi 登录代码逻辑漏洞 (QVD-2023-15129)。Smartbi 是广州思迈特软件有限公司旗下的商业智能 BI 和数据分析品牌，为企业客户提供一站式商业智能解决方案。Smartbi 身份验证逻辑中存在缺陷，远程攻击者可利用此漏洞绕过身份认证，进一步结合后台接口利用可最终实现远程代码执行。奇安信 CERT 已复现此漏洞。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Grafana 身份认证绕过漏洞安全风险通告

6 月 25 日，奇安信 CERT 监测到 Grafana 身份认证绕过漏洞 (CVE-2023-3128)，由于 Grafana 和 Azure AD 租户对于电子邮件地址的处理存在差异，未经身份认证的远程攻击者可以构造恶意请求利用该漏洞，成功利用此漏洞可以绕过身份认证接管 Grafana 账户。目前此漏洞的技术细节已在互联网上公开，漏洞的现实威胁进一步上升。鉴于此漏洞影响较大，建议客户尽快做好自查及防护。

Apple 多个产品高危漏洞安全风险通告

6 月 22 日，奇安信 CERT 监测到 Apple 官方发布了多个产品高危漏洞，包括 Apple WebKit 任意代码执行漏洞 (CVE-2023-32439) 和 Apple Kernel 权限提升漏洞 (CVE-2023-32434)。Apple Kernel 存在整数溢出漏洞 CVE-2023-32434，本地应用程序可以利用该漏洞以内核权限执行任意代码；Apple WebKit 中存在类型混淆漏洞 CVE-2023-32439，远程攻击者可以诱骗受害者打开特制网页触发类型混淆错误，成功利用此漏洞可在目标系统上执行任意代码。鉴于这些漏洞影响范围较大，且已发现在野利用，建议客户尽快做好自查及防护。

Linux Kernel 权限提升漏洞安全风险通告

6 月 20 日，奇安信 CERT 监测到 Linux Kernel 权限提升漏洞 (CVE-2023-1829)，Linux 内核流量控制索引过滤器（tcindex）中存在释放后重用漏洞，本地攻击者可以利用此漏洞将其权限提升为 ROOT 权限。目前此漏洞技术细节及 PoC 已在互联网公开，奇安信 CERT 已复现此漏洞 PoC，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

注：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。

对抗篇

国内攻防演习 6 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

2023年6月，奇安信Z-TEAM团队共承接攻防演习服务 30 场，其中省级攻防演习 2 场，地市级攻防演习 6 场，客户自主攻防演习 22 场。

本月承接攻防演习数量与上月对比呈上升趋势（见图 1）。

本月承接的攻防演习涉及政府部委、金融、企业行业较多，此情况与上月承接攻防演习涉及行业范围数据大体相同，部分类型活动数量略有不同（见图 2）。

本月攻防演习成果如表 1 所示：

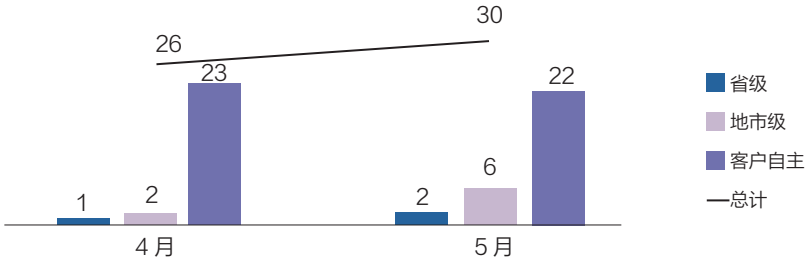


图 1 5-6 月 Z-TEAM 承接攻防演习数量统计

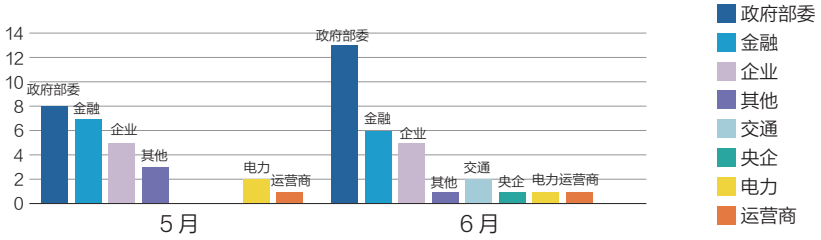


图 2 2023 年攻防演习涉及行业统计图

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	37	59	62	72	55	108	612	2312

表 1

二、本月任务目标特点

本月攻防演习和评估任务行业比较分散，演习目标覆盖面比较广，涵盖了政府部委、金融、电力、运营商、企业及其他行业。随着计算机和网络技术的迅猛发展，企业的业务系统也越来越依赖于互联网和内部网络。然而，随之而来的安全问题也日益严重，黑客和病毒等威胁不断增加，企业信息网络系统面临着越来越大的安全风险。因此，保障企业信息网络系统的安全性，已成为企业信息事业健康发展所必须考虑的重要问题之一。企业行业在本月攻防演习中占比为17%(见图 3) 。

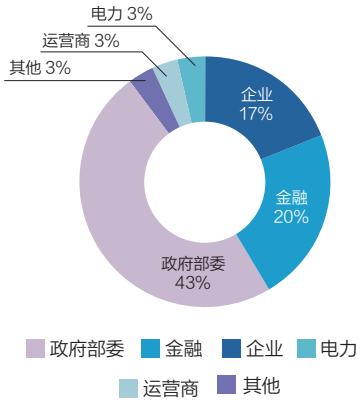


图 3 6 月攻防演习分布图

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果，本月任务中对多个行业的网络目标进行了攻击分析，并总结了不同行业的攻击特点。我们发现政府部委和企业行业的外网安全较弱，容易受到漏洞扫描利用、弱口令等手段的攻击；电力和运营商行业的外网安全防护相对较强，但仍需警惕漏洞扫描、隐秘隧道外联、弱口令等威胁；金融行业的外网安全最高，但也不能忽视漏洞利用、钓鱼攻击和隐秘隧道外联等风险。因此，我们建议各个行业加强外网安全管理，定期检测和修复漏洞，加强口令策略，增强员工安全意识，以防止攻击者利用外网攻击内网。各个行业使用的主要技术手段分布如图 4 所示。

本月攻防演习服务中，攻击队使用攻击手段主要有：漏洞扫描利用、口令爆破、钓鱼攻击、VPN 仿冒接入、内网突破隐秘隧道外联技术等。

整体攻击手段与上月对比，隐秘隧道外联手段利用率基本趋同，钓鱼攻击和 VPN 仿冒接入手段有明显下降趋势，漏洞扫描利用和口令爆破有明显上升趋势（见图 5）。

本月任务中企业行业攻防演习任务占比接近五分之一，通过对该行业的演习数据分析，发现攻击队的外网纵向突破重点是寻找薄弱点，并利用历史漏洞和钓鱼攻击手段结合实现突破。内网横向移动则采用弱口令爆破、VPN 仿冒接入、隐秘隧道外联等攻击手段来实现横向拓展和渗透。在攻防演习中，攻击者通常需要多种攻击手段相互配合才能成功地进行渗透和拓展。

四、典型攻击手段实现案例

随着计算机网络技术的不断发展，其安全性问题变得尤为突出。网络是

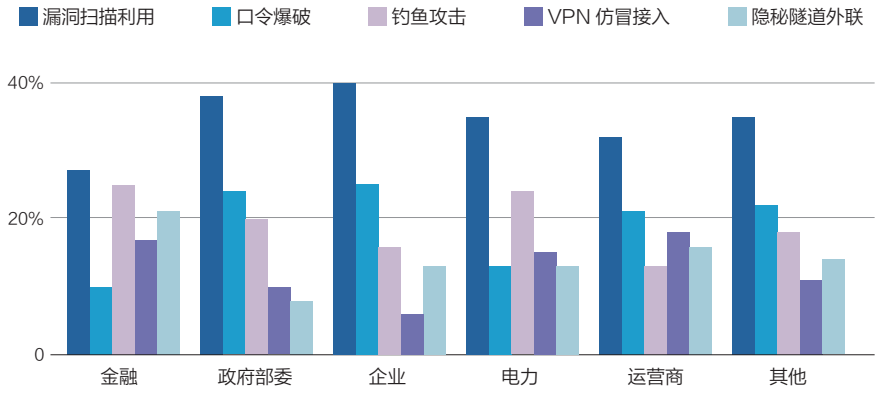


图 4 行业攻击手段分布图

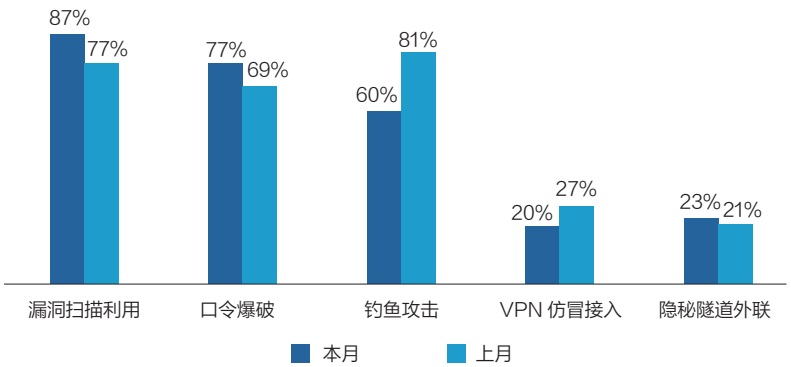


图 5 攻击手段对比图

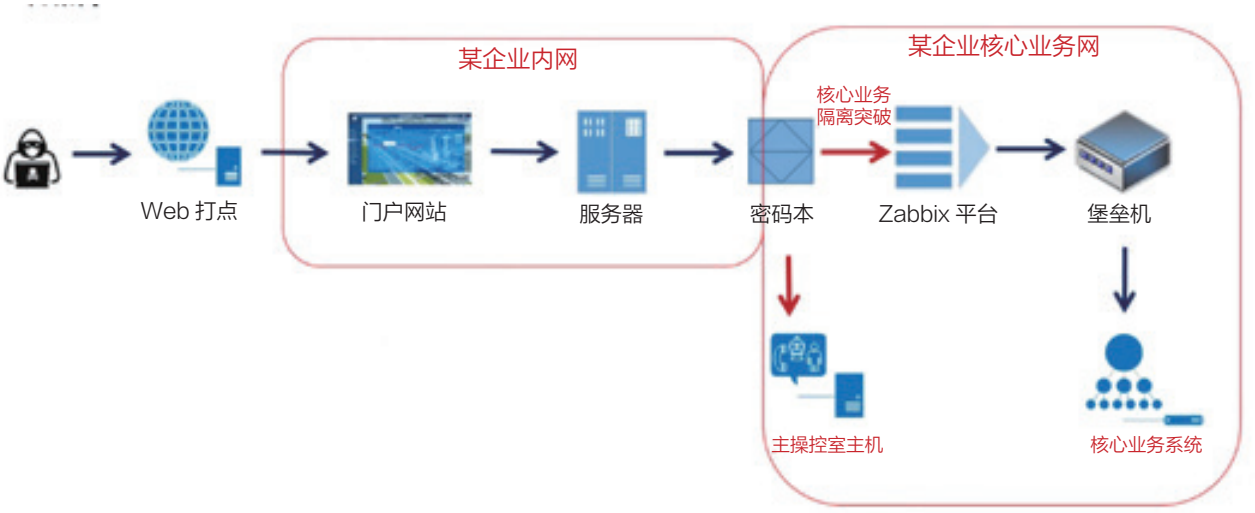


图 6 案例攻击路线图

开放的、系统的，同时也是共享的、复杂的，由于其边界和路径都存在不确定性，所以网络容易受到来自外界的入侵、攻击和破坏，影响数据信息的完整性和保密性。网络技术被广泛应用到企业中，有效地推动了企业的信息化发展，网络技术在企业发展中发挥积极作用的前提是网络技术是安全的，一旦网络被攻破，企业机密的数据、资料可能会被盗取，给企业带来难以预测的损失。因此，企业网络安全的建设必须提上日程，并加以有效防范。

案例：正面突破某企业内网核心业务

在某企业攻防演练中，奇安信攻击队经过前期的情报收集与分析，制定了首先突破办公网，再通过办公网渗透进入核心网的战略部署。

首当其冲，门户网站作为企业互联网的“面子”，成为攻击队优选的突破口，经过多次探索，最终利用 0day 漏洞获取了该门户网站应用及操作系统的管理员权限，进而进入该企业办公内网。

在横向移动过程中，攻击队又发现多个服务系统和服务器，使用已经获得门户网站管理员账号和密码进行撞库攻击，成功登录并控制了内网中的绝大多数服务器。这表明，该企业内网中许多系统服务器使用相同的管理账号和密码。

至此，攻击队突破办公网的第一阶段目标顺利完成，并取得了巨大的战果。接下来，攻击队对已被攻破的服务器系统进行全面排查，发现多台服务器中存储了明文记录的 Excel 密码本，其中包括所有系统用户的账号和密码。此外，服务器上还明文存储了大量机构内部敏感文件，包括企业 IT 部门的组织架构等信息。

攻击队通过密码本储存的 Zabbix 口令获取了某企业生产 Zabbix 平台权限，通过该平台可管控其他 137 台服务器，通过权限绕过获取了堡垒机后台权限，利用堡垒机可管控其他重要核心系统共 211 台，包括某企业集团官网、易创平台、大数据库平台、产投等系统。

同时，攻击队的另一组人马继续摸排受控主机的用途和存储文件。功夫不负有心人，攻击队最终发现一台“生产主操作室”的主机设备，存储有生产专用的文件，其中包括一些涉密文件。一旦被窃取，后果难以想象。

五、安全防护建议

1. 攻击案例剖析

从攻击队利用 0day 漏洞攻陷门户站点进入办公网，到层层突破、扩大战果获取内网大量主机权限和敏感数据，直至进入核心内网获取集权系统和涉密数据，攻击过程中的每个环节都在暴露企业网络系统的防护缺陷和存在的漏洞。

1） 外网门户站点失陷，边界防御被突破：攻击队在使用 0day 漏洞 EXP 攻击系统并获取权限的过程中，网络流量侧和主机端均缺少对提权等异常行为的监测和拦截机制，进而导致主机失陷，自此边界防御被突破。

2） 通过口令撞库获取大量主机权限：攻击方能实现横向移动并探测到大量主机，说明存在网络隔离策略松散的情况。通过对账号口令撞库的方式获取大量主机权限，正是利用了主机系统弱口令和口令同质化的漏洞

隐患，这既是人员安全意识淡薄问题，也是主机安全防护短板问题。

3） 集权系统与重要核心业务系统失陷：失陷主机系统上存储的大量敏感信息，包括 EXCEL 明文密码本，使得攻击队可轻易获取集权系统 Zabbix 权限和堡垒机普通账号，而堡垒机自身存在身份绕过漏洞，被拿到后台权限后导致大量重要核心主机失陷。安全意识薄弱，账号口令信息泄露，对集权系统未做访问限制，是导致多个核心业务系统失陷的主要原因。

4） 生产主机设备失陷，涉密文件泄露：自集权系统和重要核心服务器失陷后，攻击方可基于获取到的权限和敏感数据制定新的攻击战术，开展更为深入的攻击探测，进而发现重要生产主机设备及其存储的涉密文件。由于未对重要核心设备做严格的网络隔离和访问限制，未对涉密文件采取加密存储措施，同时对涉密文件的访问行为也未采取身份鉴别和授权访问限制技术，是导致重要设备失陷和涉密文件泄露的巨大风险隐患。

2. 安全加固策略

基于案例的整个攻击过程分析来看，该企业在网络安全意识和纵深防御能力上存在较多短板，一旦被真实攻击组织攻破利用，将给企业带来极大的风险隐患和难以预测的损失，急需从以下几个维度提升实战化的网络安全防御能力。

1） 提升全网高级威胁监测能力，对攻击行为及 0day 漏洞利用后的恶意行为实现早期的快速发现，对受害目标及攻击源头进行准确定位，做到及时响应和快速阻断，避免边界防御被突破。

2） 建立业务系统主机的安全防御能力，通过在内外网系统主机上部署主机防护软件，实现对攻击行为在端上落地后的行为监测和阻断，如针对攻击方利用 0day 漏洞后的提权、后渗透行为，以及对其他主机发起口令爆破或撞库等攻击行为进行实时防御。

3） 做好分区分域、网络隔离和访问控制策略。采用最小授权、按需申请原则，严格限制不同级别、不相关业务之间的访问通信，做好业务与业务之间的隔离，提升访问控制的细粒度管控水平。

4） 提升全员安全意识，定期开展账号口令安全检查工作，及时整改弱口令和口令同质化问题。禁止在办公终端、运维终端和服务器上存储明文账号口令，统一通过堡垒机来托管运维账号口令。

5） 对重要和集权系统做好访问来源限制，通过网络访问控制和集权系统本地安全策略，建立白名单访问机制，限制外部对运维管理平台、堡垒机和 VPN 等集权系统设备的访问。

6） 对敏感信息和涉密数据采用加密存储方式，对重要数据的访问行为采取身份鉴别、合理授权、行为监测和审计措施。存储敏感信息和涉密数据的重要核心系统需要单独划分区域，限制访问来源，并对异常访问行为及时监测和拦截。安

网络安全学院学生创新资助计划

在中央网信办指导下，中国网络空间安全协会、中国互联网发展基金会、10家一流网络安全学院、奇安信等多家网络安全企业发起“网络安全学院学生创新资助计划”，面向一流网络安全学院的全日制在读本科、硕士、博士学生提供项目资助。

让科技创新“最后一公里”更加顺畅
让科研创新与市场需求“零距离”

十所高校深挖人才“蓄水池”：山东大学、北京邮电大学、北京航空航天大学、西安电子科技大学、东南大学、四川大学、华中科技大学、武汉大学、上海交通大学、中国科学技术大学。
五大科研方向探索新突破：风险检测、识别分析、数据安全、新技术、情报响应。

网络安全学院
学生创新资助计划
项目办公室

安全产业与战略

7 月 6 日，数字安全高峰论坛暨 BCS2023 北京网络安全大会开幕，来自中央网信办、工业和信息化部、公安部和北京市的领导，以及中国电子集团、奇安信集团和国内外相关机构的专家学者，提出推动网络安全行业健康高质量发展的对策建议。

北京市委常委、副市长靳伟在大会上表示，数字安全产业已经成为支撑首都数字经济发展的重要领域之一，为首都高质量发展做出重要贡献。**北京市将持续推动数字安全产业升级，加快抢占技术创新制高点。**

靳伟表示，北京市高度重视数字安全工作，积极承担起创新引领者和产业先行者角色。目前，全市的网络安全产业规模占全国的四成左右，积聚了近千家网络安全企业和全国半数营收规模前十的企业，数量均居全国首位。

靳伟强调，下一步，北京市将持续提升数字安全技术实力，建立数字安全合规技术和产品体系，强化数字安全标准研制，推动制定区块链、隐私计算、关键软件等数字安全核心技术攻关，支持多方安全计算、可信计算等新技术在金融科技、数据流动、安全保护等场景应用，加快抢占技术创新制高点。

“北京市将持续推动数字安全产业升级，以重点产业园区为载体，推动数字安全融入国家网络安全产业园的建设；打通贯穿基础研究、技术研发与产业应用全链条；加快推进数字安全产业规模化和集约化发展，提高产业链和供应链的韧性和自主可控能力，推动数字安全产业的可持续发展。”

靳伟　北京市委常委、副市长

郭涛　中央网信办网络安全协调局副局长、一级巡视员

中央网信办网络安全协调局副局长、一级巡视员郭涛表示，要认真学习贯彻习近平总书记关于网络强国的重要思想，切实把思想和行动统一到党中央对于网信工作的战略部署上，并提出工作要求。

一是全面推进网络安全能力建设。深入贯彻落实《网络安全法》《数据安全法》《个人信息保护法》等有关要求，增强网络安全态势感知能力、网络安全防御能力，切实维护网络安全。

二是强化关键信息基础设施安全保护。集中国家优势资源，加强跨行业、跨部门、跨地区协作协同，建立全域联动、立体高效的联合防御体系。国家已建立国家关基保护的“三层责任”，运营者全面落实安全保护主体责任，保护工作部门落实好监督管理责任，国家网信部门、国家有关职能部门要做好协调、监督、指导及安全保卫等责任。

三是构建教育技术产业融合发展良性生态。要坚持开拓创新，打造国家网络安全人才高地、创新高地、产业集聚区。要持续深化一流网络安全学院建设示范项目建设，培养高校学生自主创新基础能力。要创新人才评价机制，建立以实际能力和贡献为导向的评价标准。要创新企业和高校联合培养机制，大力实施网络安全学院学生创新资助计划。

工业和信息化部网络安全管理局一级巡视员周少清指出，当前，数字经济浪潮正引领全球经济发展新方向，成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。网络安全是护航数字经济发展引擎的关键，是数字时代构筑新优势、领先新赛道的前提。因此，**应当从三个重点方面入手，全面提升网络安全保障能力，护航制造强国、网络强国、数字中国建设。**

一是夯实安全防护，保障新型基础设施建设。贯彻落实《网络安全法》《数据安全法》《关键信息基础设施安全保护条例》等法律法规要求，落实网络安全主体责任，健全网络安全管理制度机制，强化安全保障能力建设，强化新型信息基础设施安全保障。

二是强化创新驱动，推动网络安全技术突破。面向国家战略和产业发展需求，加大科技创新力度，加速内生安全零信任等前沿技术研究，前瞻布局人工智能、区块链等在网络安全领域的融合应用，护航数字化转型发展。

三是加速资源聚集，提升安全产业供给能力。完善网络安全产业发展支撑政策，培育网络安全优质企业，重点行业，企业强化安全需求牵引，发挥龙头企业带动作用，促进产业链上下游协同联动，推动产业高质量发展。

周少清　工业和信息化部网络安全管理局一级巡视员

孔长青　公安部网络安全保卫局二级巡视员

公安部网络安全保卫局二级巡视员孔长青表示，随着数字经济蓬勃发展，数据窃取、侵犯公民个人信息等违法犯罪活动较为突出，重要敏感数据大规模泄露事件时有发生，数据安全风险不断加剧。他认为，数据安全面临的形势越严峻，就越要**强化数据安全保障体系建设**。为此，孔长青提出**三点建议**：

第一，做优做强数字经济，必须统筹发展与安全。网络安全和信息化是一体之两翼、驱动之双轮，而网络安全的核心就是数据安全。要始终统筹发展和安全，以发展促安全、以安全保发展，强化数据安全机制、能力建设，筑牢数据安全坚实底座，护航数字经济健康发展。

第二，推进数据安全技术，必须兼顾创新与实践。创新是数据安全技术发展的第一动力，实践是检验数据安全技术的最佳手段。既要不断加强技术创新，增强数字安全实力，又要通过实践不断检验数据安全技术，优化调整创新方向。

第三，筑牢数据安全屏障，必须坚持可信与可控。可信、可控是保障数据安全的关键基础，一旦缺失，数据安全就是“空中楼阁、海市蜃楼”。要牢固树立风险意识和底线思维，集中优势力量推进数据安全核心技术攻关，切实维护数据安全。

联合国副秘书长李军华指出，**数字化转型伴随的风险可能会使其收益黯然失色。数字化转型之旅需走出一条更全面的通路，增强网络安全保障，尊重个人隐私，保护支撑数字政府和数字经济的关键数字基础设施。**

李军华表示，在许多领域，数字技术已经成为促进创新、提高生产力的重要动力。它同样也推动了数字经济的发展，使其蓬勃发展，促进了制造与服务行业岗位的增加。数字政府则为商业与服务业的繁荣提供了支持框架。不断扩大的数字生态系统在推进各级发展目标方面发挥着关键作用。机器人、人工智能、量子计算、物联网、云和移动计算等在支持人类福祉和可持续发展目标方面具有巨大潜力。

但是，不断发展的数字化转型也伴随着越来越多的风险，这些风险可能会使其带来的好处黯然失色。李军华指出，滥用数字工具已经导致错误信息、虚假信息、仇恨言论、网络犯罪和网络空间军事化等问题增加。

因此，李军华强烈呼吁，必须采取措施，包括通过监管措施等，来解决这些问题，并在网络安全和在线安全之间取得平衡。

李军华　联合国副秘书长

曾毅　中国电子信息产业集团有限公司党组书记、董事长

中国电子信息产业集团有限公司党组书记、董事长曾毅表示，不能把信息系统建完了再做网络安全，要坚持以内生安全为主，把网络安全和信息系统的建设及未来智能化的发展有机融合在一起，推动我国网络安全产业稳步发展。

曾毅表示，中国电子以打造国家网信事业核心战略科技力量为战略目标，构建以网络安全为核心的五个方面重要产业体系，全力推进网信事业的发展。

曾毅介绍了中国电子重点关注的网信事业发展内容，第一点就是技术创新。**“我们的基础技术、前沿技术已经取得了很大的进步，特别是奇安信以技术为依托，构建了十大核心能力，这个在国内，在国际上我认为都是一流的。”**中国电子也将全力支持奇安信，加速核心技术能力的打造。

第二点是推动安全和系统融合发展。中国电子正在打造省级政府平台、数字部委平台，以及央企平台。从顶层设计开始，就考虑如何以内生为主，把网络安全和信息系统的建设和未来智能化的发展有机地融合在一起。

第三点是产业生态融合。当前，网络安全产业发展正处于上升阶段，如何把握住机会，做好产业生态融合，与国内外一流企业实现协同、合作，推动我国网络安全发展，是一个值得深入思考研究的问题。

中国工程院院士、中国电子信息产业集团首席科学家、鹏城实验室方向责任院士方滨兴发表了“模型加工场：一种支持隐私保护的数据使用权交易方法”的主题演讲。

方滨兴表示，**数据需要流通才能发挥最大价值，但隐私保护成为横亘在企业面前的大难题，模型加工场基于分享价值不分享数据的关键技术有望解决这一问题。**他指出，目前国际上已经有一些数据流通交易隐私保护实践。比如，数据厂商 Snowflake 通过数据不动程序动，实现了数据提供方实时安全地共享数据获取数据收益。

基于国际研究和工程实践，方滨兴提出兼顾隐私保护与数据要素流通的模型加工场技术。该技术包含五大要素：核心方法是数据不动程序动，关键技术是分享价值不分享数据，辅助手段是数据可用不可见，应用模式是保留所有权释放使用权，计算环境是算力网互联形成统一数据域。

方滨兴表示，数据不动程序动，是指采取网络靶场技术，构建一个可信计算平台，使得外部程序可以在该平台上进行运行。隐私数据可以以裸数据的形式放在该平台中，由摆渡过来的外部程序利用这些数据来进行模型加工，但人员不能进入该“模型加工场”查看调阅数据。管理员受“云匣子”审计系统控制，防止擅自拖走数据。

方滨兴　中国工程院院士、中国电子信息产业集团首席科学家、鹏城实验室方向责任院士

倪光南　中国工程院院士、中国科学院计算技术研究所研究员

中国工程院院士、中国科学院计算技术研究所研究员倪光南表示，开源软件安全的关键，就在于保障开源供应链安全；即使是自主开发软件，也要重视开源软件供应链安全。7 月 7 日，倪光南在 BCS2023 北京网络安全大会——信创安全论坛上发表《开源软件供应链安全》主题演讲 。

倪光南表示，当前开源已成为商业软件的主要成分，开源成分在各行业代码库中的占比从 46% 至 83%，总计开源成分占到了被审代码库的 70%，且行业越新，比重越大，开源开始引领全球新兴信息技术的创新。

当前国际局势动荡不安，再加上迄今为止大多数开源基金会所支持的开源项目、业界通行的开源许可证和代码托管平台等，往往都被海外学术界和产业界所主导。软件安全涉及网络安全、数据安全、信息安全、供应链安全。与专有软件相比，开源软件的代码受到全世界开发者的共同审视，其应用也得到世界上众多用户的检验，因此开源软件安全的关键，就在于保障开源供应链安全；即使是自主开发软件，也要重视开源软件供应链安全。

如何更好地保护开源软件供应链安全，倪光南介绍了由中科院软件所和中科南京软件研究院联合研发的开源软件供应链基础设施平台“源图”。这是国内首个开源软件采集存储、开发测试、集成发布、运维升级等一体化设施，有效保障了我国软件供应安全、产业创新发展和开源软件供应链安全。

中国科学院冯登国院士指出，当前网络空间安全技术呈现出零化、弹性化、匿名化、量子化和智能化等五个基本特征，将引领网络安全技术的未来发展。

7 月 7 日，中国科学院冯登国院士在 BCS2023 数据安全论坛上，就网络空间安全技术的新特征进行了深入探讨。

零化特征是网络空间安全技术的新标志；零安全技术通过持续验证来建立和维护信任关系。弹性化特征是网络空间安全技术的新潮流，将为网络安全提供更高水平的防护和适应性。匿名化特征是网络空间安全技术的新焦点；机密计算、匿名认证、差分隐私和联邦学习等隐私保护技术，特别是机密计算作为一种保护使用中的数据安全的计算范式，通过可信执行环境提供硬件级的系统隔离，保障数据安全。量子化特征是网络空间安全技术的新动力；抗量子计算密码的研究在数学基础上建立，为应对未来量子计算的安全挑战提供了可行方案。智能化特征是网络空间安全技术的新工具；人工智能技术在自身安全、应用导致的安全问题及防御技术中的应用具有重要意义。

冯登国　中国科学院院士

艾哈迈德·阿卜杜勒·哈菲兹
埃及最高网络安全委员会执行局主席

埃及最高网络安全委员会执行局主席艾哈迈德·阿卜杜勒·哈菲兹表示，**面对网络安全的未来，我们需要改变当前的网络安全安全理念，根据自身业务资产、面临威胁，选择适应自身特点的安全措施与方案。**

在艾哈迈德看来，物联网、云网络、人工智能、5G 等新电信技术、工业 4.0 等新兴技术正在不断发展，并正在以比网络安全措施更快的速度被人们采用，新兴安全威胁成为当今世界每个人面临的真正威胁。当前的网络安全攻防双方陷入此消彼长、循环往复的模式：新引入的软 / 硬件不断曝出安全漏洞，企业不断改进自身的防御措施，以消除安全漏洞。攻击者则不断提升自身的攻击水平和工具。但面对几乎翻倍的网络攻击次数，持续攀升、不可持续网络安全支出，不断引入的新安全工具，网络安全响应水平并未得到提高；相反的是，复杂的安全工具还会产生噪音，导致所谓的“告警疲劳”。

艾哈迈德认为，在网络安全建设上，要理智地思考，做出关于网络安全的正确决策。艾哈迈德建议重点管理好自身风险，这包括摸清自身资产，识别所面临的威胁及攻击方法；同时，根据自身业务目标，确定优先级，建立决策树。

中国电子信息产业发展研究院院长张立分享了我国数字安全产业发展十大趋势，**数据安全将成为数字安全产业发展核心驱动力、数据确权与可信流通将推动数字安全产业健康持续发展、零信任安全创新将进入爆发期等。**

数据成为基础战略资源和新型的生产要素，在数字中国建设如火如荼的推进时，数据安全需求加速释放。张立表示，当前我国数字安全体系已初具雏形，逐渐成为保障数字经济发展和国家安全的新引擎，对此，赛迪研究院总结预测了未来我国数字安全产业发展将呈现的十大趋势，分别是：数字安全政策环境将不断优化；数字安全市场规模将超万亿元；数据安全将成为数字安全产业发展核心驱动力；数据确权与可信流通将推动数字安全产业健康持续发展；“交钥匙”的安全运营将是数字安全新解法；零信任安全创新将进入爆发期；智能化、主动化将成为数字安全产品竞争关键；“融合”与“协同”的安全架构将进一步完善；产学研协作的数字安全生态将加快形成；全链路阶梯型人才培养体系将愈发健全。

张立　中国电子信息产业发展研究院院长

武连峰　IDC 中国副总裁兼首席分析师

IDC 中国副总裁兼首席分析师武连峰表示，**企业数字化发展正在从数字化转型时代进入到数字化业务时代，过去企业的核心是业务的数字化，现在的核心是数据的业务化，**它有着五个明显的特征：第一是国家极为重视数字经济发展和数字化主权；第二是行业为实现转型升级践行数字化优先战略；第三是企业数字化举措由 CEO 和高管支持和推动；第四是绝大多数企业将利用数字技术进行竞争与创新；第五是数字化创新举措可大规模交付业务价值。

武连峰认为，数字业务时代主要存在以下六大安全挑战。

首先是新政策，组织的网络安全建设应当满足相关政策的合规要求；其次是新技术，云计算、大数据、生成式 AI、万物互联等新技术的应用，带来了全新的网络安全挑战；第三是新数据，数据的爆炸式增长及频繁的流动，对现有数据安全保护体系提出了新的要求；第四是新信任，网络边界正在逐渐消失，传统的以内外网为主的信任模型正在受到严重挑战；第五是新价值，数字业务时代，网络安全的内涵和外延不断发展，如何体现新时代的客户价值、社会价值及生态价值，成为不得不考虑的问题；第六是新人才，新技术的发展带来了网络安全的新形态，如 DevSecOps、AI 安全等，如何建设满足要求的人才队伍成为了关键。

华为董事、CIO 陶景文深入解读了华为数据安全建设实践，他表示，**在保障安全的情况下，数据通过流动才能实现价值，基于数据的集成、汇聚和交换实现对业务的增值服务，成为企业高质量发展的核心竞争力。**

华为在全面推进数字化转型战略的过程中，通过重构用户体验、重构作业模式、重构运营模式，实现全联接的智能华为，在追求客户满意的同时，追求效率效益的提升。”陶景文表示，他认为数字化转型存在三个核心。首先，战略是根本，成功的数字化转型都是由战略驱动，而非技术驱动；其次，数据为基础，只有通过对数据的科学治理，数据在企业内部的流动才具有意义，不同维度的数据汇聚在一起，才能创造新的价值；最后，智能是方向，作业数字化、数字平台化、平台智能化、智能实战化，正在实现“小问题”自动决策、自动执行，“大问题”推送分析、辅助决策。

陶景文　华为董事、CIO

顾荣辉　哥伦比亚大学计算机系教授、CertiK 联合创始人

哥伦比亚大学计算机系教授、CertiK 联合创始人顾荣辉从智能分析与审计实践的具体讨论入手，回应 Web3.0 安全领域普遍关注的前沿性问题。

Web3.0 迅猛发展的同时，攻击行为也随之增加。顾荣辉说：“包括智能合约在内的新型创新，也引入了新的漏洞与攻击模式”。**在网络攻击力量远超网络防御的时代，对于参与第三代互联网的人而言，安全风险不容忽视。**

顾荣辉表示，代码开源在为使用者提供便利的同时，也存在着极大的安全风险，一个漏洞就可能导致 1000 万美元的损失。CertiK 将前沿学术成果转化为企业级产品，打造的 CertiKOS 是世界上第一个也是唯一一个经过完全验证的多核操作系统内核，并可为 Web3.0 提供一站式安全解决方案。

新加坡管理大学计算与信息系统学院副院长朱飞达提出了新数字经济时代智能的关键特征：一是多方共同参与的协同智能是大势所趋；二是智能竞争从模型趋向于数据；三是智能和数据的治理日益紧迫。

“在越来越强的 AI 时代，我们用什么样的技术来更好地监管它，使得 AI 能够更好地为我们服务？” 朱飞达认为，AI 越强大就越需要相应的强治理手段。需要重点关注大模型的去中心化和民主化；交易的透明性和可验证性；数据和算力贡献的权益分配；数据溯源和模型计算的可追责性。

朱飞达认为智能数据生态存在诸多瓶颈，所以就引入了 Web3.0 的概念，其主题就是数据绑定，也就是说这个数据如何能够做一个双向身份的绑定，最后使得用户能够真正拥有主权数据的概念。

朱飞达　新加坡管理大学计算与信息系统学院副院长

数智安全，内生为本

——齐向东 BCS2023 演讲全文

7 月 6 日，2023 全球数字经济大会数字安全高峰论坛暨 2023 年北京网络安全大会开幕，全国政协委员、工商联副主席、奇安信董事长齐向东发表题为《数智安全，内生为本》的主题演讲。齐向东表示，我们已经进入数据和实体经济深度结合的数智时代。解决数智时代的安全问题，必须内生为本，以“零事故”为目标。

- 数智时代，让网络更安全、让数据更安全，成为政府、企业和社会组织的主要任务。
- 数智时代，数据发生三大变化:
  - 从“死”到“活”， 在流转中持续创造价值，产生更大风险；
  - 从虚到实，现实世界和网络空间界限越来越模糊，攻击暴露面越来越大；
  - 数据从贱到贵，成为各国争

全国政协委员、 工商联副主席、奇安信董事长齐向东

抢战略资源，黑客攻击的首要目标。

• 数据内生安全要做好以下三件事：从关注 IT 转变成关注业务；从关注设备转变成关注“人”； 从关注建设转变成关注运营。

• 北京冬奥会的实践，证明网络安全“零事故”可以实现。数智安全也应当以“零事故”为目标，这是时代对我们提出的新要求。

以下为奇安信集团董事长齐向东在 BCS2023 大会上的演讲全文：

尊敬的各位领导、来宾，媒体朋友们，大家好！

感谢大家参加 BCS 大会！今年上半年，以 ChatGPT 为代表的生成式人工智能像沉寂多年的火山突然喷发一样，让全社会惊喜。昨天开幕的全球数字经济大会主题是“数据驱动发展、智能引领未来”，我认为这个主题非常贴切目前技术发展阶段：社会已经进入数智时代。

数智时代，是数据和智能的时代。数据时代的标志是数据的爆炸式增长，始于 10 年前的 4G、智能终端、智能识别与控制和云计算技术的成熟，给社会创造了巨大价值；智能时代的标志是大模型通用智能技术的诞生，有赖于算力技术的革命性提升，未来生成式人工智能将改变信息社会经过 80 年形成的社会生产、生活和治理模式。

数智时代和传统时代相比，社会安全生产事故的诱因将完全不同，网络攻击将成为最主要的诱因。让网络更安全、让数据更安全将成为政府、企业和社会组织的主要任务。为了完成这个主要任务，我们要投入超乎想象的资金预算和人力资源。

数智安全，内生为本。我今天的演讲主要分以下三个部分。

第一部分：攻击数智系统是未来战争和犯罪的主要形式。

在传统社会，我们有很多盲区，事故都发生在盲区中。数智系统的普及，解决了很多盲区问题，加速社会发展的同时，也必将减少事故。

比如，煤矿爆炸事故，多数都是因为对瓦斯浓度监测有盲区；煤矿透水，对作业规范监管有盲区；煤矿垮塌，对矿井结构安全性监测有盲区。所以，5G 数字化应用场景中煤矿是重点行业，各种各样的采集器，把数据汇集到大数据中心，进行及时决策，传统矿井变成了数字矿井，盲区没有了，煤矿事故就逐渐被消灭了。

比如，传统政府服务中，老百姓办事跑断腿，就是因为信息孤岛让政府各部门有工作盲区，政府变成数字政府之后，各部门的数据汇集到大数据局，数据共享、一网通办，数据多跑路、群众少跑腿，盲区没了，政府和群众之间的矛盾也就逐渐少了。

比如，社会治安管理中，前一段时间引起巨大反响的唐山烧烤店打人事件，因为遍布城乡每一个角落的摄像头组成的雪亮工程，消除了监管盲区，使得瞬间真相大白于天下，给犯罪分子极大的震慑。

还有智能工厂、智能检验、智能交通、智能驾驶等，都是解决了盲区问题，不仅实现了效率和质量双提升，事故也减少了。

但是，任何事物都有两面性。数智时代解决了旧盲区，也带来了新盲区。试想一下，如果传感器被攻击，将会用假数据产生更大盲区；如果控制器被攻击，将会因为错误的指令导致更大的事故；如果数据被删除和篡改，盲区将变得无穷大，事故的边界将不可控制，社会生产可能停摆。

所以，攻击数智系统将成为未来战争和犯罪的主要形式。我总结，主要有三方面原因：

第一，数智时代，数据发生了三大变化。

第一个变化，数据从“死”到“活”，在复杂流动中产生更大风险。数智时代以前，数据是相对静止、缺少流动的，只是单纯地存储在数据中心、服务器中，价值没有得到充分的利用。

数智时代，数据时刻在流动，并在全生命周期的流转中持续创造价值。以某大型能源国企为例，从勘探生产环节中采集数据的那一刻，数据就作为核心生产要素开始流转，流转环节场景非常复杂，交互极其频繁，每个环节都暗藏风险。比如，数据在云上流动时，存在多个安全“黑洞”，很多企业甚至不清楚自己有没有被安全防护。今年 5 月，英国最大外包公司被爆出他们的亚马逊 AWS 云存储桶因为缺乏安全措施，导致 655G 数据在网上“裸奔”7 年。

数智社会越发展，数据流动越复杂。有媒体评价，数据的流动就像风，既有从“云”上吹来的风，也有从“地”上卷起的风。我们期待它能包容万物、行通天下，也要警惕其中的安全风险。

第二个变化，数据从虚到实，攻击暴露面越来越大。过去，数据主要存在于网络空间，基本不会影响现实世界。数智时代，数据和实体经济深度结合，现实世界和网络空间的界限越来越模糊。最典型的代表就是物联网设备，比如，原来手表只是一个计时工具，现在的智能手表不仅托管着人们的健康数据，还能操控其他的物联网设备。

再如，无人机靠导航数据、目标数据来完成任务，数据就等于实际任务；无人工厂靠数据驱动机器人代替工人生产，数据就等于实际生产力；智能电网、智能水务、智能汽车都是靠数据驱动，数据就等于供电、供水和驾驶。随着数据和各行各业结合得更加紧密，我们将进入真正“数实融合”的世界。

数据从虚到实的过程，是生产业务系统向外打开的过程。这意味着，攻击暴露面被无限放大。根据诺基亚的报告，过去一年，物联网僵尸网络攻击数量激增了五倍，受损的设备从20 万台增加到 100 万台。除了数量倍增，攻击的后果也越来越严重。比如，去年 4 月，哥斯达黎加遭到勒索攻击，支付、关税等系统瘫痪了一个多月，政府宣布进入紧急状态。

第三个变化，数据从贱到贵，价值越来越高，损失也更难承受。越是稀缺的资源，价格就越高。以前的数据，商业价值有限，也不容易进行数据交易。数智时代，数据包含了企业的领域知识、行业经验、科研成果、生产技术等，是驱动企业、社会、国家发展的核心资产。我国多个省份都把建设数据交易所列为了今年的重点任务，去年上海数据交易所累计挂牌数据产品近 1000 个，数据产品交易额超过 1 亿元，今年场内交易额有望突破 10 亿元。

数据不仅是各国争抢的战略资源，也是黑客发起攻击的首要目标。威瑞森发布的报告显示，95% 的数据泄露都是经济利益驱动。数智时代，企业的重要数据被破坏，将意味着生产事故；数据被泄露，意味着失去了竞争壁垒，可能在商业竞争中败北。

数据从死到活、从虚到实、从贱到贵，只有深刻理解这三大变化，我们才能做好数智时代的网络安全工作，才能更好地迎接“风高浪急”，甚至“惊涛骇浪”的重大考验。

第二，数智时代，数据安全出现了三大难题。

第一个难题，数据操作行为真假难辨。数据在流转过程中，包含大量复杂的操作行为，很难分辨是正常业务操作还是网络攻击。比如，黑客会披着合法的外衣做“坏事”，模拟正常业务，采用“蚂蚁搬家”策略盗取数据。

> 数据从死到活、从虚到实、从贱到贵，
> 只有深刻理解这三大变化，
> 我们才能做好数智时代的网络安全工作。

黑客还会篡改、删除、伪造数据。比如，黑客利用 AI 工具仅需 30 秒音频，就能精准捕捉声音特征并进行深度伪造。最近，加拿大一对夫妻就被伪造的音频诈骗了 2 万多美元。黑客还可以利用漏洞，篡改监控系统中的关键数据，隐藏自己的犯罪行为，严重威胁国家安全、社会安全、生产安全、个人安全。

第二个难题，“三员”违规行为难控。威瑞森的统计显示，数据泄露事件，82% 和内部有关。内部人员的风险主要是“三员”，也就是管理员、技术员和操作员。他们往往有较高的数据访问权限，很可能被黑客钓鱼利用。

去年 12 月，媒体曝光某公司前技术员为宣泄不满，远程加密公司服务器，导致业务系统全面瘫痪。

第三个难题，软件供应链漏洞、后门难防。据奇安信统计，仅国内外应用最广泛的 JAVA 编程语言，就有近 1500 万个版本的 JAVA 开源组件，它们当中很多存在漏洞、后门等安全风险，我们对 1780 个开源组件的 1.6 亿行代码进行了检测，共发现安全缺陷 265 万个，每 1000 行代码中就有 16 个安全缺陷，这些缺陷一旦被发现和利用，就变成安全漏洞。

而国产软件对这些开源组件的依赖度是 100%。比如，某国产操作系统，用了超 1000 个开源组件，同时引入了 1000 多个已知漏洞；某国产邮件系统，使用了超过 100 个开源组件，引入了超过 800 个已知漏洞。

第三，数智时代，网络安全“易攻难守”将常态化。

网络防守难，难在不知道黑客从哪里下手攻击，所以要全面防守。全面防守引发了资源危机：首先是兵力分散，其次是体系和设备的薄弱环节难以避免。“千里之堤毁于蚁穴”，就是说防守难。

网络攻击易，易在攻其一点不及其余，更重要的是攻击者永远在暗处，可以集中优势兵力，解决资源不足的问题。攻击之易，还体现在新技术应用初期，软件漏洞易挖、易用。

过去，解决易攻难守难题通常采用网络隔离的方法，比如，把网络划分成物理隔离网、逻辑隔离网、内网、外网等，用减少攻击面解决防守人力不足问题，实现攻防平衡。而数智时代，隔离网络要变成开放网络，“易攻难守”的矛盾更加尖锐。

过去，高水平的黑客只是一小部分，攻击和防守力量基本平衡。而生成式人工智能技术出现以后，不懂代码的普通人也可以编写钓鱼邮件和木马，让黑客数量激增，攻防平衡被打破。比如，今年以来，AI 换脸诈骗在多地发生，福建一位市民 10 分钟内就被骗走了 430 万元。

数智时代，数产生了智，
智又产生了新的数，
在螺旋式上升的循环中创造了一个繁荣的数智世界。

过去，数字化系统都是相对独立的，攻击者需要逐一攻破，耗时耗力。而数智时代，各行各业的系统都依赖数字基础设施，一旦基础设施被攻破，就好比自来水被下毒，一个攻击危害一片，引发“蝴蝶效应”，也造成了网络安全“易攻难守”。

第二部分：数智安全要以内生为本。

奇安信 2019 年就提出了内生安全。过去 4 年里，我们参与了很多国家级的大项目，服务了很多重要客户，不断验证了内生安全理念应对复杂网络攻击的先进性。

数智时代，数产生了智，智又产生了新的数，在螺旋式上升的循环中创造了一个繁荣的数智世界。内生安全也是一样，从规划、建设、体系运行到实战结果，再用实战结果评估指导新的规划、建设、体系运行，在螺旋式上升的循环中，保卫数智世界的安全。内生安全就像人的免疫系统一样，每战胜一次病毒，都增强一次病毒抗体，“吃一堑长一智”“经一事识一人”。所以，解决数智时代的安全问题，必须内生为本，做好以下三件事。

第一件事，从关注 IT 转变成关注业务。过去，我们解决网络数据安全是从 IT 视角出发的，重点解决的是网络边界、网络终端、网络应用的正常运行，安全部门并不关注应用系统中的业务，业务系统和安全系统各自为战。这种状况引发了业务系统最大的安全漏洞，业务异常、访问异常总是被忽略。

内生安全的核心就是业务安全和网络安全合一，确保业务持续稳定。现在，数据从“虚”到“实”，数据和业务的联系越来越紧密，数据安全问题往往会导致业务事故，所以我们解决数据安全问题，必须关注业务。

从生产视角看，我们要从生产的关键环节、关键过程中找出防护重点，比如，在水电大坝的安全防护中，要对开闸放水的控制节点进行重点防护；在工业控制系统中，要把生产业务数据和网络安全数据联合分析，才能及时发现操作异常。而操作异常结果是未知攻击的“狐狸尾巴”。

从研发视角看，我们要对研发人员的研发过程、研发成果、操作行为进行全过程数字化管理，并分类分级实施动态安全防护，比如，对提交和下载研发数据的账号，采取实时监测、严格审计等安全措施。最近，上海一家游戏公司的三名离职员工，盗取了手游源代码，并“换皮”成新游戏上线，获取高额非法利益，为软件研发企业敲响了警钟。

从管理视角看，我们需要建立一把手参与决策的数据安全管理机制，统筹数据在各业务系统之间流转，搞清楚哪些数据是重要数据，并提供相应的合法、合规的安全保护措施；明确哪些部门的角色，可以使用什么样的生产系统，访问什么类型的数据。管理的过程是通过安全能力技术体系，把这些规则和策略落到实处，管理的结果要通过数据驱动来判定是否真的达成，不断整改提升。

第二件事，从关注设备转变成关注“人”。刚刚我提到，数据从死到活，人在使用数据的过程中会产生两个问题：一种是攻击者披着合法人的外衣干坏事，比如，盗取合法的账号和权限，操控设备、窃取数据等；另一种就是合法的人作恶，利用合法身份盗取数据。这提示我们，要解决数据安全问

题要从关注“人”的视角出发，也就是防范“内鬼”视角。

过去，我们对设备信任的基础是账号、IP 地址、主机信息等，设备只要通过认证，就能持续访问数据。数智时代，我们信任的基础不再是单一的、静态的，要从关注“人”的视角出发，采用零信任架构，通过身份分析、环境感知，持续对“人”的行为进行监测分析和控制，确保身份可信、环境可靠、权限可控、行为合规。

过去几年，奇安信通过零信任系统解决了很多问题。比如，有一位客户，被黑客窃取了账号，黑客借用有效的访问凭证，逃过安全检测，长期潜伏在内网，窃取了大量数据。我们通过零信任系统，结合轮换身份验证密钥、终端环境感知、行为检测分析等综合策略，第一时间精准定位出数据窃取行为，成功切断了泄露途径。

第三件事，从关注建设转变成关注运营。刚刚我提到，数据从贱到贵，必然引来国家级力量和顶级黑客组织的攻击，防护难度倍增，因为攻防的“矛”“盾”对抗性，防守方无法准确预测攻击者的武器、方法，使用固有的防护手段以“不变应万变”是不行的。我们必须采用“防守利器”加“运营应变”、以运营为主的策略，也就是“阵型”加“战法”的组合，而“战法”是随机应变的，要靠运营来实现，这样才能提高胜算率，逼近万无一失。

保护的资产价值不一样，需要应对攻击的难度、烈度就不一样。一枚普通的钻戒和一颗价值连城的钻石，防盗策略显然是不一样的。小偷靠技术，战法变化不大，应对起来相对容易；大盗靠谋略，战法千变万化，应对起来要靠综合手段，持续运营。

数智时代的安全运营，要关注几个变化：一是资产的变化，原来的资产是主机、服务和软件，现在的资产还包括数据和 API；二是数据的变化，原来数据集中防护就行了，现在集中防护不利于数据流动，必须对数据进行分类分级防护；三是策略的变化，原来的策略是由网络安全部门制定的，现在的安全策略更多服务于业务，需要业务部门发起，安全部门实现。

第三部分：数智安全要以“零事故”为目标。

电视剧《狂飙》里有句台词“没有人是绝对安全的”，网络安全也没有绝对安全。网络安全本质上是攻防两端的高强度对抗，没有攻不破的网络，没有打不透的墙。但网络安全工程师们始终将“绝对安全”作为奋斗目标，不断创新前进。

奇安信非常有幸成为了北京 2022 冬奥会和冬残奥会网络安全和杀毒软件独家服务商。我们承担起了北京冬奥会“完全的、彻底的、端到端”的安全责任，做出了网络安全“零事故”的承诺。

这份承诺是个艰巨的挑战，因为从伦敦奥运会开始，历届奥运会都发生过或大或小的网络安全事故。比如，2012 年伦敦奥运会，奥林匹克场馆的电力系统遭受了 40 分钟大规模 DDoS 攻击；2014 年俄罗斯索契冬奥会，10 秒倒计时中两块大屏幕黑屏；2016 年里约奥运会，黑客入侵世界反兴奋剂组织服务器，曝光了国际组织默许大量西方发达国家的体育明星使用“禁药”的信息；2018 年平昌冬奥会，黑客攻击导致开幕式直播信号中断；2020 年东京奥运会，官网瘫痪 1 小时，工作人员信息被泄露。可见，奥运会网络安全“零事故”这条路以前没有人走过，但奇安信必须得走通。为了兑现这份承诺，我们一刻不敢松懈，最终创造了奥运史上网络安全“零事故”的世界纪录。

北京冬奥会的实践，证明网络安全“零事故”可以实现。数智安全也应当以“零事故”为目标，这是时代对我们提出的新要求。数智时代，网络安全、数据安全就等于生产安全、国家安全。在传统社会，生产安全和国家安全始终是以“零事故”为目标的，

> 北京冬奥会的实践，
> 证明网络安全“零事故”可以实现。
> 数智安全也应当以“零事故”为目标，
> 这是时代对我们提出的新要求。

随着数智化的深入发展，安全这件事“一着不慎，满盘皆输”，我们必须迎难而上，实现网络安全“零事故”。

具体讲，“零事故”有三条标准：业务不中断、数据不出事、合规不踩线。

先说业务不中断。数智时代，业务不仅变得越来越开放互联，数字化、智能化手段的广泛应用，还让网络暴露面无限扩大。一个智能终端被突破，就可能导致一家大型机构的整个数字化系统陷入瘫痪。比如，今年 5 月，法国一家大型智能电子产品制造商，因为遭遇网络攻击，基础设施被加密，导致旗下三大工厂被迫关闭。

再说数据不出事。数智安全的核心目标，就是要保证数据不出事。一方面，数据作为重要战略资源，穿行在各个生产环节中，本身具有极高的价值；另一方面，人工智能的“智慧”也源于数据的驱动，数据安全事故有可能会导致人工智能“智慧”全无，引发灾难性事故。

最后是合规不踩线。有人认为，合规是目标，但实际上它是“起跑线”。数智时代，只有做到了网络安全、数据安全合规，才有资格谈发展，否则就是埋了一颗“定时炸弹”，一旦爆炸就会直接摧毁企业的根基。这两年，我们能明显感受到“安全红线”越来越多，对数据违法的处罚力度不断加强。今年 3 月，浙江一家企业因为数据泄露，第一责任人被罚款 100 万元。这些事件都在提醒我们，先合规，后发展。

数智时代，真正迎来了一个“万物生长”的时代。每个人的个人数据在生长、企业的数据在生长、社会的数据在生长。这些不断生长的数据，汇成“智慧”的江河湖海，推动人类进步。用老眼光去看新世界，是看不到未来的；用老方法去解新难题，是找不到答案的。

中国有一句俗话，“观念决定思维，思维决定成败”。站在当下，面向未来，多数人的观念都是落后的，先进的思维永远在最先求变的人的手里。

我相信，人类的智慧是无穷无尽的。在大家的共同努力下，我们一定能让技术造福于百姓，造福于人类社会，迎来更加光明繁荣的未来。谢谢大家！

观潮网络空间论坛：中外专家共商数字经济行稳致远之道

7 月 6 日，“北京全球数字经济大会”分论坛——“数字安全国际合作论坛暨第八届观潮网络空间论坛”在国家会议中心隆重举办。本届论坛由全球数字经济大会组委会主办、奇安信集团承办。

论坛以“携手共建开源与流动的数字世界”为主题，就全球化和数字开源时代，如何在基于信任和规则的前提下，促进各相关方探索共同安全机制，促进数据要素合规有序流动，展开开放、坦诚、建设性的战略对话，为维护全球数字空间安全与繁荣献计献策。

美中关系全国委员会会长欧伦斯，联合国经社部公共机构和数字政府司司长朱巨望，全国政协委员、全国工商联副主席、北京网络安全大会主席、奇安信集团董事长齐向东，国务院参事、中科院大数据挖掘与知识管理重点实验室主任石勇，新加坡瑞信德集团主席陈聪发，中美绿色基金董事长、前国家发改委规划司司长徐林，美国派拓网络（Palo Alto Networks）公共部门副总裁约翰 · 戴维斯，以及国家创新与发展战略研究会副会长吕本富等国内外业界领导、专家，以及来自国内各大院校科研机构的资深学者和著名媒体人，共同为数字经济安全高效的全球化发展提供洞见。

齐向东在致辞中介绍，本届观潮论坛主要围绕两方面内容进行了探讨：一方面是探索数字经济全球化发展的开放合作路径；另一方面则是为数据安全的全球化治理提供高效解决方案。

目前受地缘政治和大国竞争等因素的综合影响，数字经济全球产业链与市场布局正经历分裂与动荡，在网络空间凝聚共识和扩大合作，探索各方都易接受的数据治理规则，促进数据资源在全球的合理配置与有序快速流动，进一步激发数字经济开放合作潜能，成为与会专家交流的重点。

新加坡瑞信德集团主席陈聪发分享了新加坡数字经济发展的经验，他

认为国际合作对新加坡数字经济的发展至关重要。“国际合作为新加坡带来知识、技能与最佳实践的分享；国际合作伙伴使新加坡得以利用国际人才资源；协作研发则为新加坡带来产品与服务的创新。”

齐向东在致辞时强调，在数智时代，只有探索符合各方利益的共同安全机制，促进数据要素合规有序流动，才能让数字经济的航船行稳致远。徐林在题为《视野、格局、求实——积极维护全球数字经济的开放属性》的演讲中指出，碎片化的产业格局重塑，必然导致重复建设和效率损失，使已经形成的国际产业分工体系受到严重损害。为此，建议在跨境数据流动和贸易领域，各国要加强数据治理规则的交流，在具有共识和利益交集的领域尽可能形成共同遵守的治理规则，在此基础上推动数据全球化跨境流动配置的便利化和自由化。

石勇认为，数据确权是实现数据在网络空间中安全有序共享、流动、交易的重要前提。开源开放的网络空间需要在不同国家差异化的发展路径下，最终形成包容性的国际标准。为此，倡议尽快建立一个非盈利、非政府的国际数字经济组织，发布国际标准，协助各国数字经济技术合作交流和数据共享。

约翰·戴维斯则认为，应对全球网络威胁为负责任的政府和国际社会提供共同努力实现安全治理的机会，目标是切实减少威胁，实现更可持续的数字经济发展环境。

本届观潮论坛在主旨演讲环节之后，还用更多的时间围绕“守护数字世界活力之源”这一主题，就如何为

数字经济促开放、去梗阻、增活力进行了深入生动的圆桌对话，在联合国经社部公共机构和数字政府司司长朱巨望发表引领性视频致辞后，欧伦斯、徐林、陈柏珲、吕本富、郑剑等中外嘉宾，以及资深时事评论员庚欣先生，在特约专家刘志富主持下，就“如何增进战略互信”“如何打通政策梗阻”“如何维护开源生态”“如何跨越数字鸿沟”四个深层次问题，进行了“穿越四重门”式的集体把脉问诊，触及了全球数字经济发展面临的一系列结构性矛盾，台上、台下嘉宾深度互动，线上、线下受众踊跃参与，在培育互信机制、促进立法沟通、涵养开源环境、实现成果普惠等多个领域，提供了极具理论和实践价值的解锁之匙，激起现场强烈共鸣。

本届论坛得到线下、线上参会嘉宾的一致好评，认为该论坛质量很高，谈得很深入，有思想火花的碰撞。

智慧能源网络安全论坛：聚焦智慧融合 · 共建能源安全

7 月 6 日，2023 北京网络安全大会（BCS 2023）期间，第五届智慧能源网络安全论坛在京成功举办。

本次论坛围绕“聚焦智慧融合 · 共建能源安全”的主题，邀请行业领导、专家学者就如何提升智慧能源网络安全综合保障能力进行交流分享，共同擘画以安全生产为前提的国家现代化能源体系新图景。

中国电机工程学会会士、中国电机工程学会电力信息化专委会副主任委员刘建明主持。

中国电机工程学会会士、中国电机工程学会电力信息化专委会副主任委员 刘建明

没有数智安全，就没有智慧能源安全

中国能源研究会理事长史玉波在致辞中表示，在能源行业网络与数据安全防护形势日益严峻的当下，全面增强能源行业网络与信息安全保障能力，是落实“四个革命、一个合作”能源安全新战略和建设新型能源体系的重要措施。

中国能源研究会理事长 史玉波

中国电机工程学会秘书长王刚在致辞中提到，在“碳达峰、碳中和”目标引领下，我国能源行业进入了构建以新能源为主体的新型电力系统，加快推进能源数字化智能化发展的新阶段，能源行业网络安全已经成为能源安全的本质要求。

中国电机工程学会秘书长 王刚

国家能源局电力安全监管司副司长阎秀文分享了关于能源行业网络安全工作的三点感受：一是要紧密做好国家网络安全有关政策的跟踪落实，积极提高自身网络安全水平；二是要坚持以创新驱动安全发展，持续构建一体化网络安全防护能力；三是加强行业内经验交流分享与总结，建立起共商共建共享的良好产业生态。

国家能源局电力安全监管司副司长 阎秀文

“数智时代，没有数智安全，就没有智慧能源安全。”北京网络安全大会主席、奇安信集团董事长齐向东在致辞中指出，随着社会全面迈入数智时代，智慧能源爆发出了前所未有的生命力，但也面临前所未有的新挑战。智慧能源的网络安全、数据安全建设迎来了三个融合，走向了三个必然。一是能源系统和数智系统加速融合，以“零事故”为目标进行网络安

全建设成为必然。二是能源业务链和数据链加速融合，建设全链条的数据安全保护体系成为必然。三是能源产业和数智产业加速融合，建立覆盖全产业链的网络空间治理体系成为必然。

北京网络安全大会主席、奇安信集团董事长 齐向东

以“零事故”目标构建智慧能源新一代安全体系

论坛主题演讲环节，中国工程院院士、中央网信办专家咨询委员会顾问沈昌祥指出，要构筑主动免疫安全可信网络保障体系，夯实智慧能源网络健康发展支撑底座。此外，还要打造安全可信产业新生态，筑牢工业互联网安全防线，实现自立自强开创可信计算 3.0 时代。

中国工程院院士、中央网信办专家咨询委员会顾问 沈昌祥

国家电网有限公司副总信息师、中国电机工程学会会士、中国电机工程学会电力信息化专委会副主任委员王继业表示，电力行业需要开展新型电力系统网络安全防护研究，防护按照“分区分域、外防内控、核心自主、立体防御”策略，明确新型业务部署原则。

国家电网有限公司副总信息师、中国电机工程学会会士、中国电机工程学会电力信息化专委会副主任委员 王继业

中国电力建设股份有限公司信息化管理部主任、中国电机工程学会会士、中国电机工程学会电力信息化专委会副主任委员吴张建介绍，中国电建在集约化防控防御体系建设实践与探索经验中，明确提出首先坚持正确的网络安全观，做到统一思想、顶层设计、规划先行，统筹资源、突出重点、集中防御的实现网络安全的数字化转型。

“随着数据治理的水平越来越高，数据量越来越大，数据价值越来越大，它的贯通性越来越强，勒索的价值也水涨船高。”中国海洋石油集团有限公司科技与信息化部副总经理陈溯表示，中国海油高度重视网络安全工作，并把数据治理作为近些年的工作重点，加快构建完善网络安全保障体系。

中国电力建设股份有限公司信息化管理部主任、中国电机工程学会会士、中国电机工程学会电力信息化专委会副主任委员 吴张建

中国海洋石油集团有限公司科技与信息化部副总经理 陈溯

奇安信集团副总裁韩永刚分享了以“业务零事故”为目标构建智慧能源新一代安全体系。他表示，需要用系统工程方法体系化构建安全能力。从业务视角出发，面向数字化，进行“规

划—建设—运营”的持续架构管控，做到网络安全“零事故”的目标。

奇安信集团副总裁 韩永刚

强化运营支撑，守护智慧能源安全

中国石油化工集团有限公司信息和数字化管理部副总经理蒋楠介绍，中国石化从管理上以合规为主线，抓严、抓细、抓实网络安全工作，从运营上加强运营体系建设，提升网络安全实战化水平。

中国石油化工集团有限公司信息和数字化管理部副总经理 蒋楠

国家电投集团数字科技有限公司副总经理孙刚表示，国外安全策略 CIE 聚焦设计与操作原则为使用结构化、全面化、流程化的网络安全风险评估，来识别因网络攻击或不当操作导致可能触发严重网络安全突发事件的关键业务、关键系统、关键功能中的脆弱点和漏洞，并通过安全设计、实施和运营手段加以风险控制和安全防护。

国家电投集团数字科技有限公司副总经理 孙刚

中核武汉核电运行技术股份有限公司副总经理戴兵表示，在运营实践中以集约化的模式构建 “两级多节点”的网络安全运营组织体系，建立一级中心为核心、二级中心为支点的网络安全运营组织架构；还要制定自上而下的网络安全管理规范，搭建高效网络安全管控平台。

中核武汉核电运行技术股份有限公司副总经理 戴兵

融合创新 安全使能

——保险数字安全论坛顺利举行

7 月 6 日，2023 北京网络安全大会保险数字安全论坛在北京举行，论坛由人保信息科技有限公司主办，奇安信集团承办，中厚投资（海南）有限公司支持。

论坛以“融合创新 安全使能”为主题，邀请各界领导嘉宾，共同探讨建设网络与数字安全保险市场面临的挑战，研究保险行业如何通过多方深度合作，建立完整的网安险生态体系，完善包括网安险推广展业、风险识别评估、风险监测与预警，应急止损及理赔鉴定等能力链条。

全国政协经济委员会委员、原中国保监会党委副书记、副主席周延礼先生在致辞中表示，随着数据要素的形成，数字资源作为数字经济的核心，对国家经济和社会发展，以及安全发挥着基础性的作用，数据安全也成为关乎国家安全和经济社会发展的重大课题。

网络安全保险方兴未艾

工业和信息化部网络安全管理局网络安全处副处长肖俊芳在致辞中提到，网络安全保险作为具有网络安全风险管理和经济补偿功能的新型网络安全服务，有利于企业加强网络安全风险管理，更有利于加快中小企业数字化转型，对推动网络安全产业高质量发展，护航制造强国、建设网络强国具有重要意义。

“网络安全保险是新兴险种，是企业转移风险的有效工具，能有力推进网络安全的社会化服务。”奇安信集团董事长齐向东在致辞中指出，网络安全保险是数字化转型的必然选择，行业的前景非常广阔。今年 4 月，奇安信发布了“零事故”网络安全保障险，由奇安信提供网络安全防护能力，保险公司提供产品防护能力外的风险兜底，保险科技公司负责风险评估、核保理赔支持，能有效促进我国保险行业和网络安全产业融合发展，为推进我国政企机构的数字化转型起到积极作用。

全国政协经济委员会委员、原中国保监会党委副书记、副主席周延礼

工业和信息化部网络安全管理局网络安全处副处长 肖俊芳

奇安信集团董事长 齐向东

人保信息科技有限公司副总裁王勇在致辞时表示，随着安全保障方案的边界不断被打破，必须从更高的产业生态视角去思考解决问题。这需要数字与网络安全产业链中的安全技术公司、保险公司、保险科技公司等相关方开展深入合作。

人保信息科技有限公司副总裁 王勇

推动网络安全保险健康发展

国家工业信息安全发展研究中心信息政策所副所长冯媛提出了对未来网安险应用路径的建议，要健全完善政策标准体系、强化网络安全保险产品服务创新，推进网络安全保险落地应用，以及发展网络安全保险的生态。

中国人寿财产保险股份有限公司副总裁傅天明表示，针对网络安全保险面临的挑战，要特别聚焦以下几个重点推动保险产品进一步向细分领域拓展、推动保险服务标准化可操作性提升、推动风险量化评估模型建立完善、推动跨行业交流合作。

中国人寿财产保险股份有限公司副总裁 傅天明

中国财产再保险有限责任公司副总经理王忠曜指出，要在政府部门的指导下，开展与网安企业、科技企业的合作，发挥各自优势，共建网络安全保险新生态，加速网络安全保险产业创新升级，为数字经济发展和建设网络强国提供重要支撑。

随后，中国平安财产保险股份有限公司党委委员、首席技术官陈当阳对促进网络安全保险生态健康发展提出建议：进一步做好顶层设计，推动网安险标准化建设；进一步出台相关政策，在政策或补贴层面提供支持；加强整体的风险数据的研究，进行相关数据信息的收集和共享；调动保险公司积极性，鼓励产品创新和研究。

中国平安财产保险股份有限公司党委委员、首席技术官陈当阳

中国人民财产保险股份有限公司风控技术部副总经理帅玉廷认为，要想解决网络安全的问题，需要政府、企业、网络安全专业服务机构、保险公司四方协同发力网络安全治理的生

国家工业信息安全发展研究中心信息政策所副所长 冯媛

中国财产再保险有限责任公司副总经理 王忠曜

中国人民财产保险股份有限公司风控技术部副总经理 帅玉廷

态。

在主题分享的最后，奇安信解决方案专家梁伟分享了奇安信践行“安全技术赋能网络安全保险生态”宗旨的积极探索，如推出“零事故”保障险方案和提供覆盖网安险各服务环节的技术支撑等，并从平台定位、平台五大核心能力、业务逻辑、技术架构等维度，向现场嘉宾介绍了网络安全保险保中监测预警平台。

奇安信解决方案专家 梁伟

中国网安保险市场前景广阔

在以“中国网络安全保险市场发展及国际经验”为主题的圆桌环节中，由中厚投资（海南）有限公司董事长兼总经理于璐巍先生主持，邀请慕尼黑再保险公司大中国区总经理常青、安联保险（全球企业及特殊风险）总经理彭衍滨、中意财产保险有限公司总经理袁颖晖、源堡科技有限公司创始人、总经理韩冰和奇安信集团保险行业总经理邹贵军参与探讨。

谈及中国网安保险市场的发展前景和市场规模，有嘉宾持谨慎乐观态度，虽尚无法准确预测市场发展的“奇点”，但网安险市场存在“真实需求”。

在供给端，再保险公司和保险公司面临的重要挑战之一是，如何解决风险识别、风险量化、风险定价、精准核保及保前中后服务等环节涉及的诸多问题；

谈及政策和监管环境，嘉宾们普遍认为政策环境对市场发展会起到关键作用，在市场发展初期，政策扶持至关重要。

各位嘉宾对市场前景表达了良好预期：中国网络安全保险市场一定会在不远的将来，驶入爆发式增长的快车道。

金融业网络和数据安全论坛：聚力金融安全与可持续发展

BCS2023 北京网络安全大会——金融业网络和数据安全论坛，秉承“国际化、数字化、科技化、可持续”的理念，以“国际可持续发展，金融数据治理与安全”为主题，院士翘楚、专家学者、金融机构代表、产业代表等精英云集，围绕国内外新兴的网络与数据安全监管要求，以及金融数字化转型下的数据安全发展趋势，探讨金融业网络与数据安全的风险应对之策。

内涵外延 构建网络空间大安全

随着数字经济的发展，网络安全的内涵已经从传统的狭义网络安全，扩展到更加广泛的网络空间大安全（Cyberspace Security）。

全国政协委员、全国工商联副主席、奇安信集团董事长齐向东表示，当前，社会已经进入数智时代，即数据和智能的时代。与传统时代相比，网络攻击将成为数智时代安全事故最主要的诱因。让网络更安全、让数据更安全，将成为政府、企业和社会组织的主要任务。

面对网络空间安全的新形势和挑战，齐向东指出，不仅要更新网络安全观念，构建涵盖网络基础设施、信息和数据各个层面的新型网络空间安全体系，还需要把数据安全放在网络空间安全战略的核心位置，不断提升数据安全保障和治理能力。

全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东

齐向东认为，金融行业需要推动以数据安全为核心的内生安全体系建设，实现从关注 IT 转变成关注业务、从关注设备转变成关注“人”、从关注建设转变为关注运营的“三个转变”，在守住安全底线的前提下，以“零事故”为目标，加快完成数字化转型、实现金融业务的升级发展。

融合加速 数据安全与金融安全密不可分

站在金融安全的视角，无论是脱离了数据安全谈业务发展，还是脱离了业务发展谈数据安全，都是片面和局限的。如何让安全保障与业务发展深度交织，让数据安全和金融安全融为一体？本次论坛既邀请了学术界嘉宾，也邀请了工商银行、建设银行、中国银行、北京银行、平安银行等头部金融机构嘉宾，以及网络安全行业专家，他们分别基于行业和业务视角，围绕这一话题进行了深入分享。

中国互联网协会互联网投融资工作委员会主任委员、教育部长江学者讲座教授何佳表示，数字经济的环境下，对于金融机构的监管，在以资本为核心的同时，必须增加对场景的考虑。例如，工业互联网涉及产业、数字、金融三者的融合，Web3 以区块链技术为基础，给数字资产确权，不只是信息流通，更带来价值流通，这些都凸显了数据安全在金融安全中不可缺少的关键作用。

中国互联网协会互联网投融资工作委员会主任委员、教育部长江学者讲座教授 何佳

在新一轮技术革命和产业变革的背景下，维护金融安全，不仅需要技

术创新，也需要制度保障和人才保障，尤其需要对未来金融业务场景有深刻理解、信息技术实力深厚的跨界复合型人才。

清华大学五道口金融学院金融安全研究中心主任、中国互联网金融协会金融消费权益保护与教育培训专业委员会主任委员周道许在论坛上提出，建议设立国家金融安全二级学科，开展金融科技自主创新系列教材的编写工作。“要认识到人才培养不是关在象牙塔里就能完成的任务，需要广泛深入持续的产学研合作，共同打造中国特色的金融科技和金融安全人才培养体系。”

清华大学五道口金融学院金融安全研究中心主任 周道许

工商银行首席信息官吕仲涛介绍，近年来，工商银行不断加大网络安全建设力度，从安全资产保护、安全技术提升、安全平台建设、安全基因融合、安全生态构建五个维度入手，构建了较为完善的网络安全体系。

建设银行首席信息官金磐石指出：“安全工作是一个生态，不是一个部门或者一个银行能够解决的，我们要把包括奇安信在内的所有厂商所有的

工商银行首席信息官 吕仲涛

安全技术，在建设银行这个大的场景中用好，就能够实现高质量数字化转型发展的需要。”

建设银行首席信息官 金磐石

针对银行业数字化转型过程中的数据安全问题，北京银行首席信息官

北京银行首席信息官 龚伟华

龚伟华表示，只有在创新中重视安全，在发展中管控风险，才能在数字化转型浪潮中取得安全与发展的双丰收。在数字化进程中统筹发展与安全，兼顾创新与安全，做强做优银行业核心优势的同时守住安全底线，是银行数字化转型过程中需要破解的关键要点。

如何解决银行里面数据安全谁来负责、谁来牵头、谁来运营的难题，平安银行金融科技部总经理助理宋歌介绍，平安银行的数据安全工作由科技部门牵头，基于全行相关部门的职责和履职方式梳理形成 RACI 矩阵，有效推动整个组织为了管理目标而协作运转；在运营方面，建立了一套机制，把安全要求内嵌到业务流程中，形成与业务、与产品、与研发等相关流程共同的、一致的运营体系。

平安银行金融科技部总经理助理 宋歌

中国银行信息科技部信息安全管理团队主管郑锐分享了中国银行安全运营相关的重点方向和实践。在组织上，实施 24 小时值班制度，设立一、二、三线岗位，分工明确，并采取战备机制应对高级威胁攻击；在人员培养上注重“以干带训”和“以战带训”，通过实干和实战以及与安全专业公司

的深入合作来提升专业安全队伍的能力；在技术平台建设上，以全威胁事件平台安全大脑为核心，统筹各类安全设备与情报资源，通过安全编排实现攻击全流程的自动化响应。通过这些建设，中行的安全运营能力已经迈上新的台阶。

中国银行信息科技部信息安全管理团队主管 郑锐

在北京冬奥网络安全保障过程中，奇安信创造了奥运史上网络“零事故”的世界纪录。北京冬奥网络安全保障总架构师尹智清指出，金融行业要持续保证“零事故”，一定需要持续的运营过程，不断破题深入，通过各种各样标准化、规范化、可量化的操作，

北京冬奥网络安全保障总架构师 尹智清

促进安全架构的更新、促进产品和技术的升级、促进运营的更新，三者相辅相成，激发安全保障与潜能发挥最大化，牢牢守住金融安全底线。

奇安信集团首席战略官、副总裁刘勇也提出，应对网络安全风险需要思维革命。他认为，目前金融行业面临的安全问题集中体现在四个方面：新技术应用不可靠、数据隐私容易泄露、智能攻击难以抵御、深度造假缺乏鉴别手段。为此，需要从责任归属、安全投入力度、组织方式等方面进行思维创新。

奇安信集团首席战略官、副总裁 刘勇

以人为本 数据治理打开可持续发展新格局

对于数据治理的认知，既要理解其中的科学过程，更要考虑人与数据的相互作用。世界银行原首席技术官、DAMA China 主席胡本立认为，所有的数据都是人跟数据互动的结果，所有的数据都是有人参与的。在脑世界数据、自然界的客观世界数据、人产生的表示世界数据这三个数据世界里面，要从整个数据全生命周期来看待

世界银行原首席技术官、DAMA China 主席 胡本立

数据的利用、产生及安全问题。

国际可持续准则理事会（ISSB）主席特别顾问兼北京办公室主任张政伟表示，金融业的数据治理和安全在金融企业可持续信息披露中，已占据了极端重要的地位。“一流的企业要有一流的追求，一流的企业要有自己一流的‘零事故’目标，与之相对应的，一流的企业也要有一流的可持续信息披露。”

国际可持续准则理事会（ISSB）主席特别顾问兼北京办公室主任 张政伟

产学研共建 培育金融科技与安全高质量人才

机密计算为金融行业提供了实现数据价值与数据安全高效兼顾的重要

技术手段，将推动金融业务模式的创新和转型。中国科学院院士冯登国介绍，机密计算是计算效率约束条件下解决使用中的数据安全的重要技术，能够保证海量数据应用场景下数据的可用不可见，提高数据共享流通的安全性。当前，机密计算研究主要集中在信任模型、安全架构、各类安全机制、TEE 构建技术、平台安全服务框架、应用安全等方面。

中国科学院院士 冯登国

随着金融科技的深度应用与融合，金融网络安全形势日益严峻，国家急需培育大批高质量的网络安全实战人才守护金融系统安全。北京航空航天大学网络空间安全学院院长刘建伟表示：中央网信办、教育部的要求是要培养实战性的网安人才。希望银行与校方共同建立金融数据安全联合实验室，开设金融数据安全课程，并编写金融数据安全的教材，切实为金融网络安全事业孵化优质人才。

北京航空航天大学网络空间安全学院院长 刘建伟

北京大学光华管理学院教授、教育部长江学者特聘教授路江涌指出，“网络安全是一个无时无刻不在发生的时间空间概念。我们必须用科学思维、批判思维、主动学习等能力，应对技术发展带来的种种挑战，并在组织内部提升智能效率。”

北京大学光华管理学院教授、教育部长江学者特聘教授 路江涌

麒麟软件董事、北京航空航天大学教授兰雨晴指出，在物联网时代，金融业将大规模使用各类物联网终端和平台，金融网络和数据安全的防护重点应放在操作系统层面，加强底层安全防护。他建议金融机构持续加大对物联网终端和平台操作系统的安全投入，并呼吁在物联网时代重塑新人才。

麒麟软件董事、北京航空航天大学教授兰 雨晴

中科曙光金融事业部总架构师纪钟表示，基于可信执行环境的隐私计算，已经成为当前隐私计算领域的主流技术，可以让金融行业将不同机构或客户的数据进行运算，并确保计算过程的安全性。

中科曙光金融事业部总架构师 纪钟

共话行业发展 共创网安未来

——“马连道 · 茶 · 中国数据街”高质量发展论坛暨网安产业投资生态论坛顺利举办

7 月 6 日，“马连道 · 茶 · 中国数据街”高质量发展论坛暨 2023 北京网络安全大会——网安产业投资生态分论坛 · 共创汇顺利举行。

论坛以“创投智汇西城 · 共创网安未来”为主题，邀请网安领域 100 多家优秀网安创企代表、数十位行业投资人、行业专家与会，共同研讨网络安全行业发展趋势及产业生态建设，赋能网络安全创业者。

中共北京市西城区委常委、副区长 曾林峰

中共北京市西城区委常委、副区长曾林峰在致辞中指出：“随着数字经济的飞速发展，网络安全在经济社会数字化转型发展中的基础性地位、全局性影响愈发突出，西城区高度重视网络安全、数据安全，着力筑牢数字西城的安全底座。”

北京市大数据中心副主任、市经济和信息化局大数据应用与产业处处长唐建国在致辞时讲到：“西城区在数据安全产业方面以奇安信这样的龙头企业为牵引，不断打造产业生态，精心做成区域产业名片，在首都数字经济安全屏障建设中，积极发挥更大作用。”

会上，奇安信集团副总裁陈华平从战略、经营、发展通路等维度，介绍了奇安信集团的企业发展历程、方向和策略。陈华平表示，奇安信通过市场洞察发现，信息化领域从规划建设到运行，网络安全厂商过去主要参与中间的建设阶段，在前后的规划、运行阶段缺位。奇安信通过规划驱动、运行驱动等公司战略，推动扩大产业规模，促进与产品厂商和技术创新厂商的共同发展。

数世咨询创始人李少鹏在演讲时说到，虽然当前数字安全企业的规模扩张和净利润增长处于困境，但是产业整体前景是光明的。随着数字中国

战略推进节奏不断加快，数字安全产业长期向好，未来可期。

企业发展过程中，很多网安企业都面临着招人难的困境。北京网安汇管理咨询有限公司合伙人黄园认为，要规范企业自身的流程保密能力，提高面试效果，简化 offer 审批流程，同时要主动培养自己的招聘能力，并学会用招聘解决业务发展问题。

吉大正元信息技术股份有限公司副总裁田景成与现场嘉宾分享了网安创业的一些心得。网安创业要有刻苦精神，要不断创新不断奔跑，建立企业的优势，同时要保持开放的心态，不能给自己设立边界。

联通资本副总经理程兰介绍了联通资本助力发挥链长融通带动等方面开展的工作，同时呼吁产业资本联合起来，围绕“共同打造产品服务的试验田、当好融合合作平台组织者、共同建立产业资本服务体系”，共同助力网络安全产业高质量发展。

奇安信集团副总裁陈华平

“在信息时代，数据安全产业扮演着保护数字资产和维护社会稳定的关键角色。”奇安信集团数据安全事业部总经理刘洪亮在演讲中，详细阐述了数据安全的特点，以及数据安全从治理到服务的生态，并强调了创新和合作对构建可持续的数据安全生态系统的重要性。

面对网络安全，甲乙方视角是不同的。北京市燃气集团有限责任公司信息档案中心主任王广清从自身企业需求分析，认为网络安全是一项系统化工程，要服务并保障甲方业务的发展和业务的安全，同时在安全合规的主流旋律前提下，做有实效的产品。

北交所金融街服务基地负责人周阳在分享时表示，将进一步发挥国家金融管理中心功能优势，把握资本市场改革重大机遇，修订上市办法，为推动企业的创新发展及企业上市提供更加强大的保障。同时依托金融街优势资源，为基地内企业搭建交流展示平台，拓展业务应用场景。

西城区科技和信息化局、北交所金融街服务基地的代表分别介绍了服务企业发展的政策措施，鼓励支持欢迎优质企业落户西城，互利共赢，共同发展。

在圆桌对话环节，网安赛道的优秀投资人和创业企业代表积极发言，共同探讨了关于网络安全产业投资及网安创企经营发展等问题，真知灼见汇聚，让在场嘉宾收获颇丰。此次论坛的举办，对西城区共建繁荣网安市场，共创良性网安生态起到了重要促进作用。

据悉，“共创汇”是 BCS 安全创客汇的姊妹活动，创客汇侧重优秀创企的比赛选拔，共创汇关注对网安创企的赋能成长，两者将共同打造网安生态体系闭环，共同促进网安产业的繁荣发展。作为 BCS2023 的分论坛之一，本次“共创汇”邀请网安产业领域的大咖做主题分享，以投资人、产品线、行业人力资源、智库、投资银行、运营商、政府、甲方等不同视角，分享各自视角的网安产业趋势和看法，为网安创企进行赋能。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

安全技术与前沿

7 月 7 日，BCS2023 北京网络安全大会进入安全技术交流环节，来自国内外相关机构的安全专家就信创安全、数据安全、威胁情报、安全响应、安全运营等热点安全问题，深入交流前沿技术与应用趋势。

2023 中国网络与数据法治 50 人论坛：

——聚焦数据要素制度创新与国际交流合作

作为 2023 全球数字经济大会专题论坛之一，中国网络与数据法治 50 人论坛于 2023 年 7 月 7 日在北京国家会议中心举行。本次论坛聚焦“创新数据要素制度与强化国际交流合作”，来自联合国科学和技术促进发展委员会、北京市通信管理局、世界银行 (The World Bank)、DAMA China、美国信息产业机构 (USITO)、香港国际金融学会的领导及国内外数据要素领域知名专家学者和企业家参加了本届论坛，共同探讨数据要素制度创新、数据跨境流通交易、数据安全治理等热点话题，助力全球数字经济协同发展。

联合国科学和技术促进发展委员会主席 Peter Major 在致辞中表示，“作为新兴产业，我们必须认识到数字经济的优势及挑战，建立全球数字经济治理机制，关注社会底层，为他们提供更好的数字技术和培训，让所有人都能平等享受到普惠数字服务。同时要加快数字信任建设，实现开放融合，确保安全稳定，不断推动数字经济与可持续发展的紧密结合。只有这样，数字经济才能真正成为人类社会的重要产业，为人类的生活和福祉做出更大的贡献。”

图：联合国科学和技术促进发展委员会主席 Peter Major

北京市通信管理局党组书记、局长 苏少林

北京市通信管理局党组书记、局长苏少林在致辞中表示，公共通信网络作为实施网络强国、数字中国战略的关键基础设施，承担着不可或缺的安全托底重任，所以全行业要勇于承担起这个重任：一是提高站位，秉持为民服务理念；二是健全机制，强化保障体系建设；三是筑牢基础，保障新发展格局，包括筑牢法治保障基础、筑牢产业生态基础、筑牢防护能力基础、筑牢手段建设基础、筑牢人才培育基础等。

全国政协委员、全国工商联副主席、奇安信集团董事长 齐向东

全国政协委员、全国工商联副主

席、奇安信集团董事长齐向东在致辞中表示，“数据作为关键生产要素，只有在流通中才能产生价值。数据要素的安全、高效流通，需要开放合作这个‘金钥匙’。首先，开放合作能助力全球数据跑出‘加速度’；第二，开放合作要以数据要素安全为‘大前提’；第三，开放合作是应对数据安全挑战的‘最优解’。”

世界银行（The World Bank）基础设施副行长 陈广哲

世界银行（The World Bank）基础设施副行长陈广哲在主题演讲时表示，要让人们完全接受数字化，首先需要让他们确信，数字化互动是可靠和安全的，数字安全措施可以更好地保障互联网和数据的使用。因此，我们必须确保提供数据保护、制定网络安全法和建立强有力的机构，以保障开发和实现强大的互联数字系统，从而实现身份验证、快速安全的转移支付，并以负责任的方式交换数据。

美国信息产业机构（USITO）总裁 Christopher Millward 先生就《实现创新的数据治理原则》发表演讲，他谈到，“创新往往是一个非常具有破坏性的过程，是一个挑战现状、挑战规范的过程。因此在创新过程中，风险是很自然的。我们要承担这种风险，并找到管理它的方法，而不能因噎废食、止步

美国信息产业机构（USITO）总裁 Christopher Millward

不前。对于未来，我们将拥有一个多方利益相关者的治理模式，包括公民、社会，包括政府，包括行业，包括你我，数据治理是基于原则和期望的结果，而不是具体原则。只有这样才能推动数字经济健康安全的发展。”

世界银行原首席技术官、DAMA China 主席 胡本立

世界银行原首席技术官、DAMA China 主席胡本立带来了《所有数据是人与数据的数据——我对数据的认识》的演讲，他表示，“数据分为三大过程：实体、概念、表示，这里如果没有人就关联不起来，因此肯定需要通过人，而从实体到概念，从概念到表示，两个过程极为复杂，只有通过人才能表达清楚。”

香港国际金融学会主席、香港中国大学（深圳）高等金融研究院政策

香港国际金融学会主席 肖耿教授

与实践研究所所长、香港特首政策组专家肖耿教授在《数据要素产权的界定、交易与争议解决》主题演讲中表示，“数据要素的产权界定非常重要，它需要基于三个要素：一是界定清晰的数据产权；二是构建有规则和高效的数据交易平台；三是建立数据争议解决机制。面对如此复杂的系统，如何建立数据要素产权基础设施，对于数字经济发展至关重要。”

中国科协网络与数据法治决策咨询首席专家 王春晖教授

中国科协网络与数据法治决策咨询首席专家、联合国世界丝路论坛数字经济研究院院长、浙江大学网络空间安全学院双聘教授，中国网络与数据法治 50 人论坛发起人兼论坛主席王春晖教授发表了题为《数据产权与数据要素制度创新》的主旨演讲。他认为，

“数据产权不是对数据资源占有、使用、收益、处置的权利，而是持有和使用数据资源的权利，主要强调数据资源的社会属性。因此，应强化以数据资源持有权、数据加工使用权和数据产品经营权为核心数据产权制度，淡化数据所有权。”他指出，工业时代形成的生产关系已经不能适应数据生产力时代的需要，所以需要在产业数字化的进程中不断创新数字化生产关系，以适应数据生产力的快速发展，这就是构建数据要素基础制度的底层逻辑。

中国行为法学会副会长 朱小黄

中国行为法学会副会长、中国建设银行原首席风险官副行长、中信银行原行长朱小黄行长在《不确定性与数据重构》主题演讲中表示，为应对数据应用过程中的不确定性，需要有一个全新的数据分类标准，即数据重构，原理就是把原始数据按照不同的分类标准进行重新分类，如按照时间维度分成历史数据、边际数据。从数据产生的源头看，有自然数据、行为数据等。从不确定性来看有必然性数据、偶然性数据，在此基础上对数据进行分类。

有交易，就需要有经纪的存在。在本次论坛上，数交数据经纪（深圳）有限公司首席法律顾问丁振赣先生发布了《数据经纪从业人员评价规范》团体标准。这个标准是由数交数据经纪公司提出，由粤港澳大湾区标准化和质量发展促进会归口，同时有全国近 50 家数据交易场所、数据商、科研院所，还有数据中介机构公投参与来发起的一份专业标准。

《数据经纪从业人员评价规范》团体标准则正式发布

圆桌对话

本次论坛还设置了圆桌对话环节，中国网络与数据法治 50 人论坛发起人兼论坛主席王春晖教授，世界知识产权组织技术与创新支持中心主任、国家“万人计划”领军人才、江苏国际知识产权学院院长戚湧，南京领行科技股份有限公司（T3 出行）CEO 崔大勇，广东财经大学数字经济学院院长，联合国世界丝路论坛数字经济研究院研究员王方方，深圳数据交易所副总经理王冠，奇安信集团副总裁韩永刚等专家，就“创新、合作——创新数据要素制度的求索之路”进行了圆桌对话，围绕数据要素制度创新，数据知识产权创新，企业数据的确权授权与运营，数据跨境流通交易，数据安全治理观点碰撞和交流。

BCS2023 数据安全论坛：共话新趋势新技术新未来

7 月 6 日上午，在 2023 北京网络安全大会（BCS2023）上，由 CCF 计算机安全专委会指导，中国电子数据产业有限公司、奇安信集团、中电数创科技有限公司联合主办，以“构筑数字安全屏障，夯实数字中国建设”为主题的数据安全论坛顺利召开。

论坛邀请全国范围内数据安全领域的顶级专家、学者、领导、企业家，就维护国家数据安全、数据要素赋能实体经济等问题展开深入探讨，为促进数字经济发展红利贡献智慧力量。

中国计算机学会计算机安全专业委员会主任于锐表示，部分数据运营单位的数据安全意识仍然薄弱。因此，数字化转型过程中，数据运营单位要压实责任，依法做好数据安全保护与合规运营，从技术、制度、管理三个方面构建立体化的数据安全合规治理体系；要加强数据安全的态势监测预警平台和应急保障体系的建设，开展攻防演练，以攻促改，以练代战，发现隐患，补足短板。

中国计算机学会计算机安全专业委员会主任 于锐

中国电子信息产业集团有限公司党组成员、副总经理陆志鹏介绍，中国电子正加快打造网信事业核心战略科技力量，推动实现网信事业高水平科技自立自强，自 2020 年开展数据安全与数据要素化工程研究，率先提出以制度、技术、市场三位一体、互为支撑的工程路径。目前已在多地开展实践，积极推进数据要素市场化配置改革，加快建立数据安全全链条防护能力，加速数据要素市场培育与数据要素价值释放，为数字中国建设和数字经济发展筑牢安全底板。

中国电子信息产业集团有限公司党组成员、副总经理 陆志鹏

北京市经济和信息化局副局长苏国斌在致辞中提出做好数据安全工作的三点建议：一是持续完善安全制度体系，贯彻落实数据安全相关立法，重点推进数据分类分级、数据出境管

理、数据安全评估等关键制度的配套制定；二是探索自主创新技术体系，发挥龙头企业的技术人才优势和技术创新主体作用，开展数字安全创新研究和核心技术突破，同时促进交流合作；三是加强安全生态体系建设，继续优化数据安全产业发展政策环境，培育数据安全领军企业，鼓励数据安全关键技术攻关和产品孵化，推动数据安全技术产品的应用落地。

北京市经济和信息化局副局长 苏国斌

中国科学院院士冯登国围绕“网络空间安全技术发展的新特征”发表主题演讲。他介绍，近年来涌现出一大批网络空间安全新技术，零安全技术成为新标志，弹性安全技术成为新潮流，隐私保护技术成为新焦点，量子信息技术成为新动力，人工智能技术成为新工具。特别是以“从来不信任，始终在验证”为核心思想的零信任，近几年受到各国政府和企业界的高度重视。他还提醒，人工智能技术成为新工具，不仅 AI 自身存在安全问题，AI 应用也会导致安全问题，AI 技术会提升网络攻击的精准性、效率和成功率，需要加以重视。

中国科学院院士 冯登国

中科院网络空间地理学实验室主任，公安部网络安全保卫局原副局长、一级巡视员、总工程师郭启全表示，在网络战、国家有组织的网络攻击风险剧增的情况下，网络安全跨进新阶段，主要特征是技术对抗。因此，首先要保护数字化基础要素安全、数据流通安全及数据应用安全，在此基础上保护好由此构成的数字化生态安全。强化数字化生态安全保护，需要大力提升技术对抗能力，还要打造一支攻防兼备的队伍，开展数据资产和数据应用大排查，建立数据分类分级制度，完善数据安全保护制度，将数据安全保护工作落实到位。

中科院网络空间地理学实验室主任，公安部网络安全保卫局原副局长、一级巡视员、总工程师 郭启全

国家信息中心外网办安全管理处处长、正高级工程师罗海宁结合政务外网实践和需求，提出面向数据安全、以密码技术保护为导向的技术机制，面向数据治理，以策略规则为导向的管理机制、面向数据网络以密码网络数据一体化设施为导向的设施支撑机制，即数据安全“三向”防护机制的新思路。

国家信息中心外网办安全管理处处长、正高级工程师 罗海宁

中国电子数据产业有限公司副总经理周崇毅表示，关于数据安全流通目前存在三个基本共识：原始数据无法规模化流通、原始数据的安全与流通之间矛盾无法调和、数据要素化要

中国电子数据产业有限公司副总经理 周崇毅

实现原始数据和数据应用“解耦”。中国电子给出的破题思路是，定义数据元件，实现数据的风险隔离和高效流通；构建数据金库，实现数据的存用分离和安全存储。这将为构建行业安全可信数据空间、促进数据融合共享，提供关键支撑。

奇安信集团数据安全首席科学家刘前伟提出了保障数据要素发展的数据安全体系建设：一是将安全、合规贯穿于数据要素化的全过程，强化市场主体数据全流程合规，确保数据流通来源合法，隐私保护到位、流通和交易规范；二是技术体系要落地实现，以“数据资产”为核心，关注数据流转的全过程，将“事件检测、风险分析、访问控制、策略调整”融为一套完整闭环体系，让数据安全看得清、管得好、防得住；三是充分利用数据交易安全的关键技术是数据交易沙箱、隐私技术等，有助于实现“数据可用不可见”，确保在合规、安全的前提下充分挖掘数据的价值。

奇安信集团数据安全首席科学家 刘前伟

北京国际大数据交易所首席专家郎佩佩介绍了北京国际大数据交易所数据要素市场建设情况：近 3 年，数字经济核心产业新设企业年均增 1 万家。北京国际大数据交易所应运而生，于 2021 年 3 月 31 日正式成立，开创了数据交易 2.0 时代。交易所致力于打造数据要素市场的核心基础设施、创建数字贸易示范区的核心平台、建设国际数据跨境流动的重要枢纽，未来还将争创国家级数据交易所，助力全球数字经济标杆城市建设，实现数据资产价值飞跃。

北京国际大数据交易所首席专家 郎佩佩

BCS 2023数据安全论坛的举办，有助于推动数据安全在创新能力提升、标准体系建设、技术产品推广应用、产业生态构建等方面实现明显进展，充分实现数据要素价值。

信创网络安全论坛：自主可控，安全为先

7 月 7 日，2023 年《网络安全大会——信创网络安全论坛》在京召开，论坛由中国电子科技委指导，中国电子科技委网络安全专委会和奇安信科技集团股份有限公司共同主办，自主可控网络安全技术创新中心具体承办。

论坛以“自主可控，安全为先”为主题，共同探讨新形势下信创网络安全产业能力、应用落地、生态构建、产业创新等话题，通过信创网络安全新理念、新路径护航信创网络安全。论坛定向邀请了主管领导、政企客户、行业专家、院校、从业厂商等相关人员，与会者从各自领域的角度出发，分享了业务需求、科技成果和创新案例等，引发与会者的深入思考和讨论。

中关村高科技产业促进中心副主任 刘研

中关村高科技产业促进中心副主任刘研在致辞中表示，当前，我国大力推进信创工程，着力发展自主可控的网络安全和信息化技术产品；网络安全风险防范能力持续提升，产业生态不断完善；下一步将充分发挥政府组织引导作用，持续构建科技企业全生命周期支持与服务体系，大力培育发展新动能。

中国电子信息产业集团副总经理 周进军

中国电子信息产业集团副总经理

周进军在致辞提到，迈入新时代新征程，我们将以自主可控网络安全技术创新中心为新的起点，联合信创领域、安全领域产学研机构开展自主可控网络安全技术研究与产业推广。

中国工程院院士、中国科学院计算机技术研究所研究员 倪光南

中国工程院院士、中国科学院计算机技术研究所研究员倪光南作了《开源软件供应链安全》主题演讲，他表示，“保障开源软件安全的关键在于保障开源供应链安全，要加强开源软件供应链基础设施平台的建设和运营。”倪光南院士认为，软件安全涉及网络安全、数据安全、信息安全、供应链安全；与专有软件相比，开源软件的代码受到全世界开发者的共同审视，其应用也得到世界上众多用户的检验，所以开源软件安全的关键，就在于保障开源供应链安全，即使是自主开发软件，也要重视开源软件供应链安全。

工业和信息化部电子第五研究所

工业和信息化部电子第五研究所 柴思跃

柴思跃博士作了《信创产业发展中的挑战与机遇》报告。他表示，信创是产业发展的一个被动选择，美国公然提出了供应链的“武器化”，国内在产业管理上首先要去应对国际的风险和挑战，通过政策引导去贯穿整个信创工作；对于关键技术创新体系仍然要不断地去投入、去增加、去完备创新的模式，从产业生态体系要建立自己的自驱性，摆脱我们延续了几十年以来对美国信息技术输入的影响。

北京市西城区科学技术协会 马忠

北京市西城区科学技术协会马忠书记作了《加速信创产品迭代更新 推动政务应用替代升级》报告，他表示，“目前国产化的软件、国产化的硬件，完全能够支持地方政府在日常办公中的应用；信创迭代要更加注重用户体验，希望研发、生产、应用能够建成一个生态体系，要建立更深层次的一些信创应用，包括大数据中心、云设施，特别是在教育、民生、医疗领域，是下一步的重点。

麒麟软件公司副总裁 杨诏钧

麒麟软件公司杨诏钧副总裁作了《建信息安全之基 铸信创防护之盾》报告，分享了麒麟操作系统在安全方面的一些技术成果：随着数据的产业化和未来数字化的需求和趋势，整个操作系统作为底层，它的安全关注点也越来越明晰。麒麟操作系统打造了底层安全体系，在操作系统层面采用“三防护一中心”的思路，建立了纵

深防御和主动防御体系，使操作系统作为底座能够更好地支撑上层的信息化安全。

北京小鱼易连科技有限公司副总裁吕斌

北京小鱼易连科技有限公司吕斌副总裁作了《安全可信云视频助力数字政府建设》报告，他表示，“作为云视频厂商，在应用层面需提供安全可靠的应用。第一，数字化平台及信息化应用必须满足安全、可靠、稳定的要求；第二，打造开放融合的平台，根据业务的发展、国产化、安全化要求，能够不断的迭代、创新，成为真正的数字中台和信息化的底座；第三，在应用层面上，能够随时随地响应视频类服务，提高沟通效率、降低沟通成本。”

奇安信集团保密信创总体部总经理周华涛发表了《信息产业大变局，网络安全新思维》报告，他提出“内生安全”的信创安全建设思路，一是，安全建设必须与信创信息化建设同步规划、同步建设；二是，只有做到了同步规划和同步建设，才能将安全能力与信息系统进入深度结合；三是，新形势下的安全建设仍然要围绕体系化能力展开，形成立体化的防护网络。此外，周华涛还重点强调了人的重要性，他认为，安全实战能力取决于人 + 工具 + 数据 + 流程的有机组合。

奇安信集团保密信创总体部总经理周华涛

论坛期间，自主可控网络安全技术创新中心发布了《自主可控网络安全产业白皮书（2023 版）》。本次论坛的成功举办，为信创行业提供了一个成果展示、经验分享和探讨未来发展方向的平台，共同推动信创网络安全发展。

安全运营论坛：聚焦创新、实战与效果

近日，BCS2023 北京网络安全大会安全运营论坛在北京国家会议中心召开。 赛迪顾问业务总监高丹，京东方集团信息安全中心负责人李楠，中央广播电视总台技术局网络安全管理部主任琚宏伟，江苏警官学院计算机信息与网络安全系主任王群，移动云安全产品架构师严仍义，奇安信技术支援中心总经理龚玉山，安在新媒体创始人张耀疆等嘉宾出席了论坛，共同探索 DT 时代安全新挑战下安全运营的实践之路。

安在新媒体创始人 张耀疆

论坛主持人、安在新媒体创始人张耀疆表示，Gartner 2023 年九大主要网络安全趋势预测中，有两点值得关注：一是网络安全运营正在转变模式；二是网络安全运营越来越寻求价值可验，让客户感知到价值。

面对汹涌而来的数字化转型浪潮，安全运营该如何创新应变？赛迪顾问

赛迪顾问业务总监 高丹

业务总监高丹在《数字经济时代的安全运营新思路》演讲中表示，“未来的安全运营工作不仅仅是一个平台化的过程，而是集管理、平台、服务、流程和团队等于一体化的网络安全运营体系化过程。”她预计，未来随着威胁情报、XDR 等技术，将为安全运营不断赋能，MSS、MDR 等服务模式满足不同客户安全运营需求，安全运营将兼顾常规化、实战化的要求，最终推动安全运营成为综合性、体系化的整体工程。”

京东方集团信息安全中心负责人 李楠

京东方集团信息安全中心负责人李楠就《京东方安全运营的实践》进行了主题分享。李楠表示，京东方很早就开始了安全运营中心的建设，具体可以分为四个阶段：第一阶段是基础平台建设期，搭建了 SOC 平台，实现多平台的互联互通；第二阶段是平台功能完善期，进行资产自动同步，威胁场景分析，优化告警流程，完善溯源链条，以及漏洞全生命周期管理等，以资产为抓手进行数据拉通，构建出安全的中枢大脑；第三阶段为运营优化期，进行业务场景建模分析，以及全集团的风险管理，包括告警降噪提升运营效率、关联规则优化、业务建模等，将业务和安全充分打通；第四阶段为效率提升期，通过 SOC 和 SOAR 无缝联动，实现自动化编排响和体系化运营，大幅度提质增效。下一步，京东方将通过 SCMDB、零信任、安全有效性分析等方面的研究，迈入深度的体系化运营阶段。

中央广播电视总台技术局网络安全管理部主任 琚宏伟

中央广播电视总台技术局网络安全管理部主任琚宏伟结合多年实践，就《网络安全运营中面临的一些问题及思考》进行了分享。他特别指出，不能把安全运营仅仅理解为安全部门的工作，如何发挥系统责任主体的主观能动性是提升安全运营效果和效率的关键。为此，琚宏伟总结了三个方面：赋责、赋才、赋能。中央广播电视总台推行统一监测 + 自主监测，总体安全运营 + 分级安全运营，通过对各个系统运营主体赋责、赋才、赋能的落实，提升整体安全运营的效果。

江苏警官学院计算机信息与网络安全系主任 王群

人才紧缺一直是网络安全运营面临的现状，江苏警官学院计算机信息与网络安全系主任王群就《用新的视角定位网络安全人才培养》发表演讲，他认为，“人才培养需围绕几方面进行创新，首先是坚持学科引领，以学科优化提升人才培养质量；其次是细化人才培养方向，以公安为例，分别包括电子数据取证、网络攻防、舆情管控、工业互联网安全等；第三是加快课程群的建设，整合师资力量，避免单打独斗；第四是要发挥平台在人才培养当中的优势；第五是构建不断学习的工程实践教学体系，提升学生实践能力；最后是加强合作，拓展校企、校局合作，建立教学练战一体化的模式。”

移动云安全产品架构师 严仍义

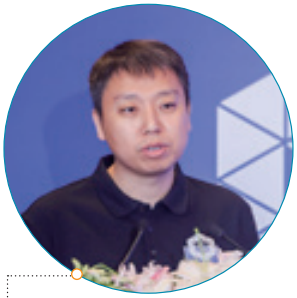
随着业务上云成为大势所趋，云租户的安全建设和运营成为关注焦点。中国移动的专业子公司、移动云安全产品架构师严仍义表示，在安全方面，移动云以‘1+31+N+4’资源布局为基础，围绕合规、技术、运营等几个方面，打造一个可信、可管、可控的云安全体系，从基础的安全防护、集中管理、态势感知等维度，全方位构建平台综合防护能力。以租户安全为例，移动云构建了一个“5+1”全栈云原生安全产品体系，底层是以身份认证或访问控制为内生的能力，上层是云原生安全能力，全面覆盖端、网，应用、云、数据及服务等各个层面，从而为租户提供整体化、体系化的安全保障。

奇安信技术支援中心总经理 龚玉山

攻防实战是检验运营效果的重要标准。奇安信技术支援中心总经理龚玉山在《基于攻防对抗体系的安全运营》分享中表示，随着企业数字化转型的加速，几年之前和现在的攻防已经有很大的区别，三四年前企业都有自己的运营中心，以传统 IT 架构为主，几年来，企业纷纷将架构升级到云原生、微服务系统等，多业务上云打通了各个数据中心，包括运维安全等，这些都对安全运营提出了更高要求。未来安全运营的核心还是依靠人，在人、工具、平台、流程中，最本质的还是人。目前，奇安信已经建立了一套大兵团式、二线支撑的系统，将人的能力融入其中，未来会为客户提供更专业的运营服务。

云原生安全论坛：夯实云原生建设基础

在数字经济和数字化技术的驱动下，企业“上云、用云”进入了全新的阶段，云原生技术体系架构下的容器、微服务等创新技术，让传统的生产和运营效率得到大幅度提升，与此同时，由于云原生下保护对象和安全机制的变化，导致云原生带来大量新型安全风险。7 月 7 日，2023 年北京网络安全大会云原生安全论坛在京召开，以“融合、进化”为主题，汇集了来自云原生领域的众多业界专家学者、甲方客户及安全企业，共同探讨云原生环境下的安全新形态与防御之道，夯实云原生建设基础，护航在数字经济浪潮下的云原生产业健康发展。



奇安信集团副总裁 刘浩

云原生安全成为极具潜力的新赛道

“云原生经过多年发展，核心技术已趋于成熟，产业生态趋于完善，到 2025 年，超过一半的中国 500 强企业将成为软件生产商，超过 90% 的应用程序为云原生应用程序。在对云原生技术应用挑战的调研中，安全性连续三年成为企业用户的最大顾虑，2022 年超七成用户担心，在生产环境中大规模应用云原生技术时的安全

中国信息通信研究院云大所高级业务主管 杜岚

性。”中国信息通信研究院云大所高级业务主管杜岚表示，云原生与安全将双向赋能与融合，并出现防护对象从基础设施向服务交付上移、从单点防护向全流程一体化防护演进等发展趋势，同时，安全与基础设施融合催生新形态的安全能力和交付模式。

云原生安全的应对之道

“运营商行业在利用云原生技术方面走得比较早，率先享受到云原生技术的红利，以中国移动为例，2015年开始采用对容器技术进行探索，经过多年建设，移动的‘磐基’‘磐舟’两大云原生技术平台，支撑了多个大型单位的云上业务。”中国移动信息技术中心运维安全项目总监刘斌说，在云原生的建设过程中，也同样面临镜像的风险、API 风险、运行时的风险和集群风险等安全问题，对此，中国移动参考了 CNAPP 云原生安全保护平台的建设思路，考虑了云原生的特点和需求，体现了安全左移和纵深防御理念，结合研发阶段和应用阶段建设，实现全局的 DevsecOps，除了安全工具，还要有安全机制的保障，如上线前安全需求分析、代码扫描 SAST/ 软件成分分析 SCA、灰盒扫描 IAST、镜像扫描、APP 扫描，提前预防安全风险。上线后持续进行安全防护，定期进行镜像扫描、基线合规检测、运行时通过容器安全与微隔离软件对容器运行实时监测。”

“业务需求与安全监管的博弈抗衡大背景下，真正的 P0 事件往往发生在安全未监管到的最后剩下的 1%，在云原生下同样适用，容器内应用作为暴露互联网初始入侵攻击界面依然存在风险：典型的 (Web 服务、Web 中间件、DB 服务、大数据服务等)RCE 漏洞、弱密码暴力破解、WebSecurity(SQL 注入、XSS、文件上传等) 依然是攻击者典型踩点打法，CoblatStrike,Metaspoit 依然是主流后渗透手法，勒索、挖矿、脱裤等云平台常见威胁影响依然头痛。”火山引擎终端安全攻防研究专家李月锋表示，“攻防战争信息不平衡，攻击者只需点、线突破，防守方必须体、面俱备，客户面临攻击威胁事前、事中、事后全生命周期下核心痛点分析与贴近客户业务视角下优雅解决方案。”

“随着云原生、人工智能和大数据的快速发展，大模型（如 GPT-3）等已经成为了我们生活和工作中不可或缺的一部分。然而，这些大模型在带来便利的同时，也带来了包括数据泄露、恶意攻击等新的安全和隐私挑战，如大模型训练和使用过程中可能产生数据流相关风险。”中科院信工所黄鹤清博士表示，“针对这些新型安全问题，将衍生出 AGI 数据安全防火墙等云原生环境下的新型技术手段。”

中科院信工所 黄鹤清博士

“现在我们看到的云原生风险只是技术应用过程中的一部分，后续随着我们对技术的认知或者技术的迭代，可能会有更多漏洞、更多问题出现，所以我们还是要持续把云原生技术应用的效果发挥出来，同时把它的风险控制在可接受的范围内。”某金融机构安全团队负责人表示，“目前的云原生安全态势需要我们构建一个一体化的、从开发阶段到运行阶段，全生命周期的安全平台，实现闭环管理。”

“现有安全防护体系虽然覆盖了云原生技术架构和全生命周期，但带来的直接结果就是安全工具多、分散，

中国移动信息技术中心运维安全项目总监 刘斌

火山引擎终端安全攻防研究专家 李月锋

某金融机构安全团队负责人

运维和运营成本高；云原生时代开发人员更关注应用的快速上线，没有统一的安全管控流程和基线配置，将导致应用可能带病上线或者推迟上线；云原生时代开源代码和镜像大量，使用，导致供应链问题突出，开发态和运行态资产风险无关联导致安全应急响应慢和风险定位困难。”奇安信云安全首席架构师鲍坤夫表示，奇安信 CNAPP 云原生安全保护平台以“安全左移、原生融合、全生命周期覆盖”为产品理念，以云原生应用为核心保护目标，能力覆盖整个云原生架构，以及云原生应用的全生命周期，纵向从下到上覆盖云原生应用运行的基础设施，横向从左到右覆盖云原生应用的整个生命周期，涵盖开发、部署和运行时阶段的安全风险监测与分析，贯穿一体系（DevOps）、两方向（安全左移与安全右移）、三环节（构建、部署、运行），提供云原生应用全生命周期的风险管理与卡点管控能力。

奇安信云安全首席架构师 鲍坤夫

“随着越来越多的用户上云，对云上的测试有了新的要求。传统的测试仪需要支持虚拟化和容器化才能部署到云上，另外也要根据云原生的特点改造部署和测试流程。”思博伦 Cloud&IP 云和安全产品总监任红波表示，思博伦支持云原生的 pod 到 pod，ingress 负载均衡，混沌测试，性能和安全测试场景，支持 SD-WAN 和 SASE 测试，并和 DevOPS、CI/CD 等开发模式结合来更迅速的满足云及云原生的测试需求。

思博伦 Cloud&IP 云和安全产品总监任红波

安全创客汇总决赛：网络靶场平台厂商软极网络获总冠军

7 月 7 日，由奇安信科技集团股份有限公司、北京网络安全大会（BCS）、中国网络空间新兴技术安全创新论坛（新安盟）、奇安（北京）投资管理有限公司联合主办的 2023 安全创客汇总决赛圆满落幕。

经过激烈角逐，网络靶场平台厂商“软极网络”脱颖而出，获得全国总冠军。犬安科技、众智维科技和云驰未来分别获得最佳技术创新奖、最具商业价值奖和最佳团队奖。

企业占比近 1/5 数据安全成热门赛道

安全创客汇是国内首个聚焦网络安全领域的专业创投平台，也是国内信息安全行业技术创新的风向标。其主要目标就是要打造网络安全创新创业发展的生态平台，推动产业政策落地，共建发展生态和创新环境。

据了解，2023 年安全创客汇是创立以来的第八届比赛，吸引了 100 余家企业报名，经过初赛、复赛的激烈角逐与层层筛选，最终在 BCS2023 上进行了十强总决赛。

今年，安全创客汇热门赛道在紧跟国外先进技术和发展趋势的同时，也体现出我国各行各业对网络安全的需求。比如，在数据安全领域，晋级安全创客汇的 50 强企业当中，数据安全赛道企业占比接近 1/5，充分体现了数字化转型对数据安全的需求剧增，网络安全加速渗透进数字化业务领域的新特点。

此外，今年多数参赛企业较为年轻，大部分成立都在 5 年之内，近三成更是新成立的创业公司。网络安全创业节奏加快，创企的年轻化趋势明显。不少成立时间较长的企业，也在网络安全新赛道上找到了新增长点，焕发出了全新的活力。

把握创新需求 推动网安产业迈上新征程

奇安信集团董事长齐向东在致辞中表示，成功始于创新，更要成于资本，

并现场与奇安投资签订了 2000 万元投资意向书。

据介绍，安全创客汇自 2016 年至今，已经成功举办了八届，吸引了累计上千家企业参与。每年进入决赛前十总计 70 家企业中，赛后均已获得数轮融资，总融资额超过 50 亿元，有效推动了网络安全行业高水平创新、高质量发展。

经过 8 年的发展，创客汇已成为安全行业的大孵化器，对网络安全产业创新发展，做出了积极贡献。“来创客汇参赛的，都是有责任心、有使命感、愿意争强好胜的网络安全工程师，在人才和政策的支持下，持之以恒坚持下去，一定能够取得更好的成绩。”

安全创客汇评委会主任、奇安信集团副总裁陈华平在演讲中表示，当前我国网络安全产业发展迎来了新环境、新挑战和新机遇。一方面网安市场快速发展，增长空间依然广阔，另一方面全球网络冲突加剧，传统网络安全战略已经无法持续。国内网安企业在学习国外先进技术的同时，也要从国内需求侧出发，进行创新驱动，推动网络安全产业迈上新征程。

最终，犬安科技获得最佳技术创新奖，众智维科技获得最具商业价值奖，云驰未来获得最佳团队奖。总得分排名最高的软极网络获得总冠军，

AI 大模型安全论坛：AI 新时代，安全须先行

AI 大模型的安全到底情况如何？未来 AI 安全应该如何保证？AIGC 内容安全该如何保证？7 月 7 日，以“AI 新时代，安全须先行”为主题的 AI 大模型的安全挑战与应对论坛在 2023 北京网络安全大会上召开。五位 AI 领域的专家、学者分享了在人工智能，尤其是大模型安全方面的研究成果。

浙江大学计算机学院教授、博士生导师、可信人工智能研究中心主任纪守领指出，AI 的快速发展给予了攻击者更多的机会，攻击的能力也显著增强。他提到了一些已知的攻击方式，如对抗样本和后门攻击。他认为，面对这些挑战，AI 安全已成为一个热门话题，并且越来越多的研究人员和企业开始思考如何应对这些问题。

纪守领教授提到了数字空间和物理空间中的实际案例，如活体检测、目标识别和恶意软件生成。他指出，这些领域的复杂性和挑战性使其成为引人入胜的研究方向。在演讲中，纪守领教授向观众展示了他们团队开发的一个平台，用于集成现有的检测和生成方法，并应用于对抗攻防研究。这一平台的实验结果令人惊叹，展示了对抗攻防领域的新颖性和挑战性。

浙江大学计算机学院教授、博士生导师、可信人工智能研究中心主任 纪守领

中国科学院信息工程研究所研究员、中国科学家大学教授 / 博士生导师陈恺博士在他的演讲中涵盖了人工智能领域的两个关键方面：攻防和可解释性方法。他介绍了使用人工智能技术来赋能安全领域的研究，并提出了一种利用大型模型来分析安全漏洞、恶意代码和漏洞利用的方法。此外，他还强调了人工智能模型本身的安全性问题，特别是在应对后门、对抗样本和语言模型等方面的挑战。

陈恺博士的研究强调了人工智能在安全领域的重要性，并提供了几种创新的方法来应对攻击和提高模型的可解释性。这些研究为人工智能的安全性和可靠性提供了新的思路和解决方案，对于推动人工智能的发展具有重要意义。

中国科学院信息工程研究所研究员、中国科学家大学教授 / 博士生导师陈恺

作为产业界的代表，百度安全副总裁、主任架构师包沉浮指出，大模型应用面临的安全挑战主要包括模型技术滥用、业务服务和接口滥用、内容滥用和品牌滥用。为了应对这些挑战，需要建立多层次、多环节的安全体系。

大模型应用的安全问题仍在不断发展，提供方和使用方应加强技术风

险预判，关注和控制应用层面的风险，并建立多方协同的安全治理机制，以应对应用的衍生风险。

百度安全副总裁、主任架构师 包沉浮

中国科学技术大学信息与通信工程专业博士、科大讯飞研究院研究员高天介绍，随着技术的突破，语音合成的自然度和应用领域不断提升，但这也带来了合成语音的安全挑战，因此合成语音检测的研究变得至关重要。在解决合成语音检测难题方面，高天博士介绍了一些最新的技术进展。他提到利用预训练模型和说话人自适应的方法来提取更鲁棒（Robust）的高层特征，改善合成语音检测系统的性能。此外，他还介绍了量子机器学习在合成语音检测中的探索，通过量子网络与深度学习相结合，提升检测系统的效果。

中国科学技术大学信息与通信工程专业博士、科大讯飞研究院研究员 高天

斗象科技安全专家杜南表示，在网络安全技术上深度探索，尤其是以基于 AI 技术的智能攻击面管理技术为重要代表之一的集成化、可视化、自动化、数智化的新一代安全解决方案备受企业的青睐。

斗象科技智能攻击面管理平台 APTP 通过资产的生命周期监控和对攻击全链路的刻画，构建了一款面向企业攻击面检测与管理逻辑链路完整的管理安全平台，同时也是一款技术与 AI 的自动化机器渗透测试平台。旨在帮助企业解决多元数字资产的可管理、数字资产的可运营等。智能攻击面管理以更智能、更多维、具备白帽知识的方式侦查和识别企业资产暴露面，以更持久的方式管理攻击面和资产地图，以更自动化、更定向、更接近人工渗透的手段方法，通过机器人节点进行攻击面预测、视图展现、安全预警和常态化安全运营。

斗象科技安全专家 杜南

在最后的圆桌讨论中，专家们就新技术发展与社会安全挑战的平衡问题提出了观点。如何平衡新技术发展和安全挑战？专家们认为技术发展是不可阻挡的，并强调了在技术研究、应用和监管方面取得平衡的重要性。总体而言，他们认为技术发展必须继续，但需要与安全问题的应对相结合，以实现健康发展。

据悉，论坛由中国网络空间安全协会指导、奇安信集团、北京赛博英杰科技有限公司联合主办。赛博英杰创始人 & 董事长谭晓生主持了此次论坛。

威胁检测响应与持续验证论坛：探索数智时代最佳攻防实践

“网络安全被完全看见才安全，网络威胁被快速处置才放心，安全防御的有效性被持续验证，才能够真正提升网络安全防御能力。”7 月 7 日，2023 年北京网络安全大会威胁检测响应与持续验证论坛在京召开。本次论坛，立足攻防视角，以“威胁对抗，防御有道”为主题，共同从实战对抗中探索数字浪潮下不同行业的网络安全防御应对之策。

应对网络攻击，各行各业都有“妙招”

随着数智化在金融、电商、互联网等各行各业的深入，网络安全问题变得越来越突出，企业不得不投入更多的精力，去应对层出不穷的网络攻击。

在金融领域，国家信息技术安全研究中心处长曹岳表示，大规模、有组织的针对金融机构网络安全攻击事件与日俱增，各种新型攻击手段层出不穷，电影中的情节成为现实，给各大银行金融机构的网络与信息安全带来了新的重大挑战。对此，金融机构等关键基础设施运营单位，在网络安全防御中应具备若干要件：首先是全流量检测、分析能力；其次是使用旁路阻断及重定向实现快速处置；第三应借助云蜜罐（配合 HIDS）实现溯源反制。曹岳表示，客户既有的基础设施、威胁情报、安全团队经验等是串联上述要件，实现安全能力整合的重要前提。

国家信息技术安全研究中心处长 曹岳

中国工商银行业务研发中心安全部资深经理叶红认为，人工智能面临基础框架、数据、算法模型和产品服务四方面的安全风险，与传统安全攻击有很大的差异，需要充分评估人工智能及大模型服务接入交易系统引发的安全风险，规范其应用场景，并在

中国工商银行业务研发中心安全部资深经理 叶红

网络安全的本质是攻防两端的动态对抗，如何提前发现尚未发现风险面成为了安全防护的重中之重。对此，京东实战攻防团队蓝军负责人叶猛认为，建设一支成熟的蓝军模拟风险源，并通过实战攻防演习、红蓝对抗、沙盘推演、蓝军评估等手段，提前发现未知风险，在最大程度上起到以攻促防的作用。

京东实战攻防团队蓝军负责人 叶猛

南方电网数字电网集团二级专家邹洪说，能源领域关键信息基础设施已成为网络攻击的重要目标。为此，南方电网按照“全域防御、纵深防御、实战引领、攻防兼备”的整体原则，打破组织与系统壁垒，应用大数据、人工智能等数字化技术赋能网络安全，通过开放架构及核心技术攻关，逐步构建全网一体化的“云盾”平台，打造数字电网安全“中枢”，实现“资

产可视化、业务数字化、研判智能化、处置自动化”，全面支撑公司数字化转型的网络安全保障。

南方电网数字电网集团二级专家 邹洪

探索威胁检测与安全验证前沿力量

对于威胁检测中的新技术、新技巧，安全厂商也是各显其能。

漏洞作为网络空间“兵家必争”的重要战略资源，在威胁检测中具有举足轻重的地位。赛博昆仑攻防实验室负责人戴明强调说，漏洞情报帮助客户筛选出真正能够造成威胁的漏洞，从监测、分析、评估、预警和响应处置进行全生命周期的闭环，并持续运营，既要避免在那些实际危害很小的漏洞中投入过多精力，也要避免忽视那些看起来不起眼但却可能造成大范围蠕虫传播的漏洞。

奇安信观星实验室攻击队负责人袁桢唤表示，被动的威胁检测具有滞后性、误报率，并且依赖特定环境和专业人才，因此需要站在攻击者视角，实现对攻击者的溯源反制。袁桢唤认为，防守方威胁狩猎应当在部署了相应的网络安全防护设备的可观测的环境中，通过一系列诸如日志分析、行为检测等方式进行持续化的监控，以达到对当前环境中存在的异常事件感知，并通过一定的调查分析手段确定为攻击事件后，进而采取应急响应等措施最小化降低攻击的影响，再循环迭代此步骤完成整个威胁检测的闭环。

奇安信观星实验室攻击队负责人 袁桢唤

软极网络副总裁、关键基础设施事业部总经理肖钧分享了软极网络在网络靶场方向的研究成果。他表示，优秀的网络靶场应当具备一栈全面仿真、一键全程导调、一网全量采集、一屏全域评估、一体全局协同等五大关键能力，助力客户建设方案可定义、过程可调度、操作可追踪、结果可回溯、流程可优化的全生命周期测试验证和安全运营五可框架。

“为应对愈演愈烈的网络安全实战攻防对抗要求，安全团队需要明确安全部署和策略是否合理且有效。”奇安信安全攻防 PBU-BAS 产品负责人邢熙悦说，仅凭人力难以对安全防御体系有效性进行验证，且同样难以长期保持一个持续、且处于较高水准的安全状态。客户应当采用 BAS 方案，它可以自动使用各类攻击手法对企业的复杂网络进行模拟攻击，并综合评估企业安全体系及策略的有效性，协助企业提升防御能力，有效地解决防御能力难知晓、投入难量化、有效性难验证等此类影响安全运营闭环的问题。据邢熙悦介绍，奇安信 BAS 具备两大核心优势：其一基于真实攻击，安全评估更有效；其二告警解析更灵活，安全有效性评估更自由。

赛博昆仑攻防实验室负责人 戴明

软极网络副总裁、关键基础设施事业部总经理 肖钧

奇安信安全攻防 PBU-BAS 产品负责人 邢熙悦

威胁情报技术论坛：威胁情报驱动安全运行体系建设

7 月 7 日，2023 年北京网络安全大会威胁情报技术论坛在京召开。本次论坛以“威胁情报驱动的安全运行体系建设”为主题，邀请业内多位专家分享威胁情报的有效利用案例及经验，探索建立一个全方位、多级别、多领域、多渠道的安全运行体系。

威胁情报技术已历经十年的发展，其内涵和外延均已发生了较大的变化，其重要性早已不言而喻。对于用户而言，什么样的威胁情报才是最需要的呢？关于这个话题，中国信息安全测评中心梁智溢在演讲中表示，大量的厂商都宣称可以提供威胁情报服务，但情报的质量却参差不齐，用户采购时好比开“盲盒”。对此，用户应当针对威胁情报构建有针对性的评价方法，持续评估威胁情报质量。作为安全厂商，也应当持续探索，共享合作，为用户持续提供高质量的威胁情报及相关服务。

中国信息安全测评中心 梁智溢

“百分之九十的情报来自开源，另外百分之十来自秘密情报工作，真正的情报英雄是夏洛克 · 福尔摩斯，而不是詹姆斯 · 邦德。”国防科技咨询服务机构蘑菇云创始人王得金引用了一句军事领域的名言，阐述了开源情报的重要性。他认为，相对于闭源情报，开源情报仅需投入 5% 的成本，便可获得 80% 的价值。在开源情报需求旺盛与供给不足同时存在的情况下，情报提供商应当基于开源情报足够的重视，告别过去的手工作坊，逐渐步入工业化生产的时代。

蘑菇云创始人 王得金

盛邦安全副总裁任高峰表示，网络资产是威胁情报的关键要素，缺乏资产基础情报数据的威胁情报是一种“空中楼阁”。而提及网络资产信息，网络空间测绘则是现阶段展示资产态势最行之有效的技术之一。任高峰介绍，威胁情报与网络空间测绘的融合应用，可以帮助客户做到漏洞威胁情报捕获与风险预警、APT 组织情报的标注与识别，实现网络空间的挂图作战。

盛邦安全副总裁 任高峰

“真实攻击者的情报能力可能超出你的想象，比如系统配置信息、供应链信息、登录凭证、0day 漏洞等在他们面前都一览无余。”零零信安创始人 &CEO 王宇从攻击者视角深入分享了扩展威胁情报的应用，显而易见，无论再高明的防守专家，也无法完全保护看不见的东西。王宇认为，“这正是扩展威胁情报的价值所在，能够打破攻防双方情报力量的不平衡状态，具体而言包括三点：其一是泛数字资产暴露面的检测，为收敛提供依据；其二是数据泄露监控，为第一时间进行事件影响评估和处置提供支持；第三是其他安全产品与服务提供数据支持，提升检测效率和准确率。”

零零信安创始人 &CEO 王宇

天际友盟创始人 &CEO 杨大路表示，面对新型数字风险，企业如果没有足够的事前准备和有效的风险防护体系碰到问题时，往往手足无措，会延误甚至错过解决问题的最佳时间窗口。为此，企业应当建设威胁情报和数字风险的协同反馈体系，实现更智能的威胁情报生产、更高效的协同反馈、更大范围的数据采集，以及更多场景的风险扩展。

天际友盟创始人 &CEO 杨大路

为最大化发挥威胁情报的价值，尽可能实现全流量留存成为很多企业想要达成的目标。派网软件 CEO 孙朝晖认为，全流量对于威胁情报检测的支撑主要体现在六个方面，即全量数据留存、元数据提取、关键字检索、文件还原、数据重放及离线分析。但在实践过程中，很多企业低估了威胁情报数量，高估了设备计算资源，导致无法发挥出全部性能。因此，情报源提高精度，控制情报数量成为了破局的关键。

派网软件 CEO 孙朝晖

除此之外，情报对于精准消除漏洞等企业安全风险也有着重要的意义。“第一时间完成所有漏洞的处置工作对于任意一个组织来说，都是一件极其困难的工作。”奇安信威胁情报负责人汪列军强调，“应当基于漏洞实际的危害和自身业务情况，合理安排漏洞处置优先级，确定最优的漏洞修复方案，对于消除威胁才能起到事半功倍的效果。”汪列军认为，基于漏洞情报的新型漏洞管理模式，能够在企业安全运营过程起到收集器、过滤器和富化器的作用，帮助企业摆脱漏洞处理的泥潭，更加高效地进行漏洞处置和管理。

奇安信威胁情报负责人 汪列军

依托“TI INSIDE 计划”诞生的网络安全威胁情报生态联盟（CEATI 联盟），也是本场技术论坛的主办方之一，作为由奇安信威胁情报中心联手国内多个著名安全公司共同发起的共建威胁情报行业生态的联盟机构，已吸纳 50 余家成员单位，能力涵盖情报运营、APT 跟踪、样本对抗、Web 安全、数据安全、大数据分析、云安全、等保合规安全硬件等多方面关键技术。

网络黑灰产治理论坛：共探全面高效的防范、应对与打击策略

7 月 7 日，由奇安信集团和反网络黑灰产联盟共同主办的 BCS2023 网络黑灰产治理论坛在北京顺利召开。北京网神洞鉴科技有限公司司法鉴定所、盘石软件（上海）有限公司计算机司法鉴定所联袂承办此次论坛，同时得到了北京司法鉴定业协会、上海市司法鉴定协会及北京刑事侦查学研究会的全力支持和指导。

在网络技术日益发展的今天，网络黑灰产业链成为了一个令人关注的问题。它不仅侵害了网络安全、公共利益和个人权益，还威胁了国家安全、社会稳定和经济发展。更重要的是，随着技术的进步，网络黑灰产业链的形式愈发复杂和智能化，对治理策略提出了新的挑战。

此次网络黑灰产治理论坛以深入探讨网络黑灰产的治理方法为目标，聚集了来自政府部门、司法机构、高校、企业等各界专家学者，共同探讨和分享对网络黑灰产治理的经验和洞察，寻找行之有效的防范、应对与打击策略。

奇安信集团副总裁 韩争光

奇安信集团副总裁韩争光指出，网络黑灰产是当前网络安全领域面临的一大挑战，需要各方面的共同关注与应对，奇安信集团愿意与各界合作伙伴共同推进网络黑灰产治理，为构建安全、可信、有序的网络空间贡献力量。

华为云安全首席专家 万涛

华为云安全首席专家万涛提出，网络黑灰产需要坚持长效治理、综合治理与生态治理，呼吁相关领域的从业人员加强联合协作，应对黑灰产带来的挑战，共建更安全、健康的网络环境。

演讲嘉宾分别从技术、法律等多个角度，探讨了涉网黑灰产案件的取证技术和挑战，分享了处理相关涉网黑灰产案件的经验与策略，给出了深入而富有洞察力的观点和建议，实现了一场全方位、多维度的对话。

最高检首批全国网络犯罪检察人才白磊

最高检首批全国网络犯罪检察人才白磊分享了他在处理涉及黑灰产刑事案件中的经验，特别是企业在存证和提证过程中的挑战与解决方案。他强调了平台需要培养留证意识，同时也提出了平台应注意提证的三性问题。此外，对于寄生类 APP 的鉴定打击，还提出了一套具有中立性、客观性的鉴定方案。

奇安信数字司法服务事业部总经理段继平

奇安信数字司法服务事业部总经理段继平提出了针对黑灰产产业链上中下游的治理重点和应对策略，并强调了在打击黑灰产案件中，电子证据与司法鉴定的重要性。同时，他呼吁政府与企业各方信息共享，共同治理与打击黑灰产行业。

特邀嘉宾 陈小兵

特邀嘉宾陈小兵从涉网黑灰产案件的取证技术的角度，探讨了涉网黑灰产案件的取证难点和挑战。他指出，涉网案件取证面临着数据加密、数据量大、智能化应用、远程取证等挑战，为了克服这些挑战，需要不断发展取证技术，扩大数据收集范围，并且关注与案件相关的敏感信息。

奇安信数字司法服务事业部鉴定技术总监 谢春磊

奇安信数字司法服务事业部鉴定技术总监谢春磊介绍了奇安信数字司法服务事业部在电子取证鉴定方面的核心能力和优势，以及在不同类型的网络黑灰产案件中提供的专业解决方案。他列举了几个涉及网络黑灰产案件的典型应用场景，如“薅羊毛”、刷流量、流量劫持、数据窃取和考试作弊等，并详细介绍了在这些场景中进行电子取证鉴定的流程、方法和防范措施。

特邀嘉宾 丁健琮

特邀嘉宾丁健琮从降本增效背景下，介绍了企业应重点打击的黑灰产类型，包括付费账号的免费注册与共享、虚假点击 / 虚假流量、盗用大平台 CDN/BOS 服务器等。他通过具体案例，对上述类型进行展开介绍，包括危害性、针对性的防护措施、适用法条与打击策略，帮助企业更好地应对黑灰产的挑战。

网络著作权领域的侵权诉求多样，技术问题和法律问题相互交织，给权

北京知识产权法研究会著作权专委会副秘书长 黄继墨

利人和司法机关带来了挑战。北京知识产权法研究会著作权专委会副秘书长黄继墨针对网络文学黑灰产业链的侵权诉讼进行了精彩的分享。她详细地梳理了资源层（动态代理）、服务层（开源资源与定制工具）和变现层（广告收益）在网络文学黑灰产业链中的作用，阐述了在实际司法实践中遇到的侵权案例及其难点，如网络技术的隐蔽性、线上维权的难度、区块链技术的合法性验证等。

北京师范大学新闻传播学院副教授 姜申

北京师范大学新闻传播学院副教授姜申从视听产业与网络黑灰产的角度，探讨了视听产业尤其是视频流量欺诈的治理问题。他指出，流量造假问题愈发智能，给互联网取证带来了极大的难度，关于识别真假流量，他提出了两个聚焦点：一是围绕账户本身的特征识别；二是围绕账户所发表的评论或信息进行识别。最后，他呼吁政府、行业、协会和视频消费者，共同合作、共同打击此类行为，实现网络视听产业的健康发展。

网络黑灰产的治理需要全社会的共同努力，每个个体和组织都需要肩负起责任，共同维护网络空间的安全稳定。在这个过程中，企业不仅可以积极履行其社会责任，还可以通过提高自身的安全防护能力，保障其业务的持续和稳定发展。安

> 网络黑灰产的治理需要全社会的共同努力，
> 每个个体和组织都需要肩负起责任，
> 共同维护网络空间的安全稳定。

解决数字化工作“三难”，奇安信发布“奇安天信”零信任工作系统

“信息化环境日益复杂，企业安全边界模糊，如何确保数字化工作安全、可信、合规、敏捷的开展？”7 月 7 日，奇安信集团在 2023 全球数字经济大会上正式发布“奇安天信”零信任工作系统（简称“奇安天信”）。奇安信零信任事业部总经理张泽洲表示，数字化浪潮席卷而来，传统的安全手段已无法有效支撑数字业务开展，构建基于零信任构建安全的数字化工作入口势在必行，奇安天信通过“一站式访问、一站式工作、一站式保护”解决数字化过程中的“重、乱、险”等问题，提供简捷、高效、安全的工作体验，实现业务安全与工作效率并举，构建数字化工作新范式。

业务和安全如何共生？企业正面临“三难”

2022 年 4 月，黑客获取英伟达某员工的访问权限，公开叫卖 RTX30 系列显卡的挖矿限制破解算法；

2023 年 6 月，黑客组织入侵了微软某员工的账户， 获取了 Bing、Cortana 等项目共计 37G 的源代码；

……

“网络攻击手段日新月异，针对身份和权限的攻击手段日渐成为主要形式。”张泽洲表示，“传统安全模型基于网络而不是身份制定安全策略，难以应对针对身份、应用和数据的安全威胁。而另一方面，传统的安全基础设施未针对数字化业务进行设计，在进行身份和权限判定时往往流于繁难重，很容易限制业务的开展。奇安信基于多年的安全实践，提炼出数字化工作开展中，政企机构普遍面临的三大难题。”

首先是访问流程太“重”了。企业在数字化过程中，会根据业务需求，快速上线很多应用，并匹配安全方案。然而问题也随之凸显，比如，应用访问入口众多，身份认证烦琐，现有安全方案未针对数字化业务进行设计，导致不同的应用访问缺乏统一入口。完成一项业务审批，就需要若干次登

录、验证，操作烦琐，极易出错，让高管和员工们苦不堪言。

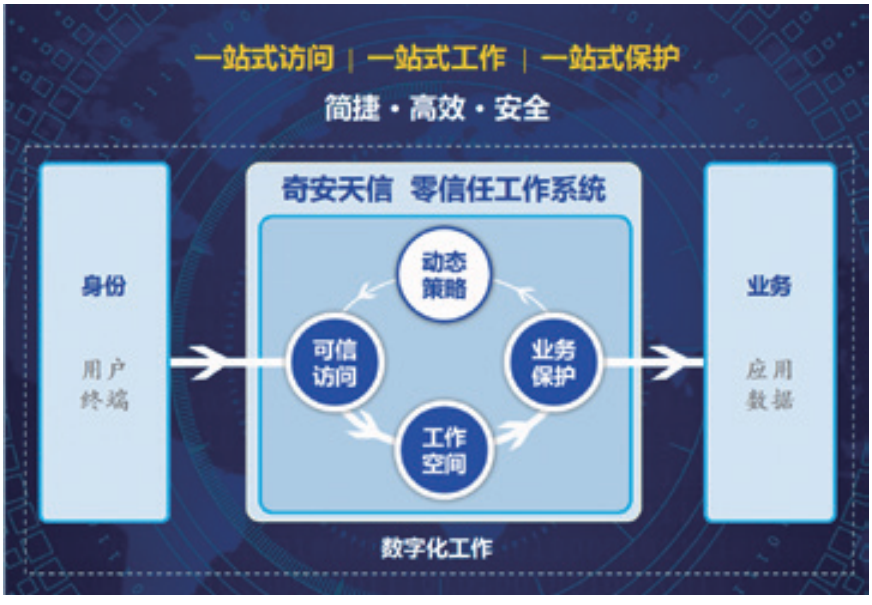
其次是工作协同太“乱”了。伴随着数字化的深入，企业上线了邮件、OA、CRM、ERP、进销存等各类应用，数量烦杂，不仅寻找工作软件浪费时间，业务权限开通烦琐，工作协同冗余低效；而且使用非可信来源工具、应用也屡见不鲜，员工自行下载安装各类工作软件，来源不明，容易导致恶意软件入侵，给企业数据造成极大安全隐患。“凌乱”还造成了信息流转路径繁多，数字化工作环境乱象横生。

最后是数据资产太“险”了。数字化环境复杂，安全边界模糊，数据攻击频繁发生，然而传统安全模型基于边界思维构建，未从业务视角出发，难以应对针对身份、应用和数据的安全威胁。尤其是静态的安全策略、粗颗粒度的管控手段，很难对业务数据进行有效地管控和安全防护，这些都导致企业面临着巨大的数据泄露风险。

内生为本，奇安天信打造一站式零信任工作系统

数字化工作如何安心又简单，将安全和业务实现内生聚合，破解企业普遍遇到的“重、乱、险”三大难题？奇安信给出的答案是：基于零信任构建安全的数字化工作入口。本次发布的奇安天信零信任工作系统，就是一款聚焦数字化工作困境，以安全内生为根本的新一代零信任产品。

张泽洲表示，和过去关注网络和边界的安全产品不同，奇安天信以身份为基石、以数据为中心，通过“可信访问、工作空间、业务保护、动态策略”四大核心能力，打造基于零信任的“一站式”安全工作入口，实现“身份化可信访问、工作开展不受限”“场景化工作空间、工作效率不打折”“体系化业务保护、工作数据不泄露”“一体化动态策略、工作风险不延误”等数字化目标。



在具体实现上，奇安天信通过“一站式”理念，解决企业数字化三大工作难题。

第一是通过一站式访问，告别繁复，拥抱简捷，让访问流程不再“重”。奇安天信以身份为基石，通过先验证后访问，动态最小权限访问，构建起业务安全新边界；通过自适应多维身份认证，确保人员可信；通过安全终端管控，持续环境感知评估，确保设备可信；通过全场景业务流量代理，确保流量可信；通过动态最小权限业务访问，确保访问可信。

第二是通过一站式工作，告别杂乱，拥抱高效，让工作协同不再“乱”。奇安天信基于场景化、集中式工作环境，实现化繁为简；而轻便化、一站式工作体验，让使用者举重若轻；通过统一资源访问门户，实现业务访问简便易用；而轻量化应用商店更让工作软件随手可得。在协同方面，通过对接业务信息流，实现业务协同高效便捷；通过对各类终端、各种操作系统的全面兼容，使得工作体验无缝跨屏，满足远程、移动等各种场景需求……一系列一体化、协同化的设计，让企业的数字化工作拥抱轻简、效率倍增。

第三是通过一站式保护，告别风险，拥抱安全，让数据资产不再“险”。奇安天信在业务保护方面，以数据为中心，围绕工作空间构建隔离、加固、纵深管控的全链条业务安全保护能力。包括通过工作空间环境隔离、工作软件安全加固等方式，实现数据安全存储、来源安全可控。通过精细业务权限管控、数据流转有效保护，实现敏感数据的识别、脱敏和加密。

同时，奇安天信还基于动态策略实

现持续性的风险预警和响应。其中包括通过多属性、多卡点、多手段动态策略管控，快速实现风险闭环，同时满足业务平滑性需求。一旦出现潜在风险，动态策略迅速调整，将业务风险降至最低。这一系列多样化控制手段，能够满足业务平滑开展的需求，并且有效提升风险响应的实时性与有效性。

> 奇安天信通过“一站式访问、工作、保护”，解决数字化过程中的“重、乱、险” 等问题，提供简捷、高效、安全的工作体验。

82% 的组织将向零信任迁移，奇安信处于领先地位

作为现阶段最炙手可热的网络安全防护理念之一，“零信任”已经被全球组织普遍接受。权威调查表明，零信任安全模型能更好地支撑数字化业务的开展，82% 的组织表示正在或即将迁移至零信任安全架构。IDC 的预测数据显示，全球 ZTNA 产品的市场规模将在未来几年保持快速增长，2022 年至 2026 年的年复合增长率将达到 30.3%。在中国，许多行业代表性企业也已将“零信任”作为重要的网络安全体系建设方向，列入企业长远规划。

作为国内零信任安全的首倡者，奇安信于 2018 年率先将零信任安全理念及技术系统介绍到国内。目前，奇安信在零信任领域成果丰硕，广受业内认可，相关产品曾获得第十届吴文俊人工智能科技进步奖（企业技术创新工程项目），也是国内首个零信任国家标准《信息安全技术零信任参考体系架构》的牵头单位。而 IDC 最新报告也显示，奇安信零信任网络访问解决方案在所有六项关键技术能力评估中均取得最优成绩，成为所有入围企业中，唯一获得五个五星、技术评估雷达图最接近正六边形的企业。

可以预见，此次推出的奇安天信，必将打破业务和安全之间长期割裂的状况，将零信任很好地融入到数字化工作场景之中，开启“全场景全终端可信接入、工作环境开箱即用、工作业务一键可达”的数字化工作体验，为数智时代广大企业打造一站式安全工作入口。

奇安信集中发布 9 大新品，解决新业态、新业务、新场景的安全问题

7 月 6 日至 7 月 7 日，以“数智安全，内生为本”为主题的 2023 全球数字经济大会数字安全高峰论坛暨 BCS2023 北京网络安全大会在京成功举行。连续举办 4 届的 BCS 大会今年升级为全球数字经济大会的网络安全板块，展现出在数据驱动和智能引领的数智时代，网络安全保驾护航意义重大。

大会期间，奇安信集中发布 9 大新品，再度提升新一代网络安全体系的防护能力，有效解决新技术产生的新业态、新业务、新场景衍生出的新安全问题，助力政企客户更好地实现网络安全零事故。

全面保护业务访问安全，奇安信安全代理网关 SWG 4.0 携三大硬核功能全新升级

奇安信行为安全产品总监 侯昀

伴随着企业上云和数字化转型的加速，云上 Web 应用资产快速增加，随之而来的是难以管控的安全风险和不间断的黑客攻击，数据泄露、非法访问、勒索病毒攻击等安全事件时有发生，有效保护 Web 应用安全、守住访问入口刻不容缓。

奇安信安全代理网关 SWG 是领先的 Web 访问代理产品，可为企业提供基于应用和网站服务的流量检查解决方案及全面的 Web 安全防护，有效隔离恶意流量，保护企业内网安全。本次推出的“奇安信安全代理网关 SWG 4.0 版”支持信创环境，响应国家“2+8”安全可控体系的信创战略，并新增数字水印、安全脱敏、数据防泄露三大硬核数据安全能力，更全面地保护业务访问安全。

更佳用户体验，奇安信发布椒图云锁服务器安全管理系统 Lite 2.0 版

奇安信服务器安全产品运营总监 亢飞

目前，勒索攻击事件日趋频繁，攻击范围逐渐扩大，勒索技术、反防御技术快速升级，并出现了多平台入侵、双重勒索、多路径攻击，以及复杂编写语言等新型攻击手段，大幅增加了勒索病毒防治的难度。

针对日益严峻的勒索攻击态势，奇安信椒图云锁服务器安全管理系统 Lite 2.0 版再次升级，构建针对勒索病毒的全链路防护策略，从前期的风险暴露面梳理到事中的入侵监测、病毒实时处置，再到事后的攻击溯源，形成统一、有效、场景化的安全闭环，以更低的资源消耗、更有效的风险管控、更细粒度的安全防护和更及时的勒索病毒查杀能力，为客户打造精准、高效、易部署的服务器端勒索病毒防护体系。

集大成者！奇安信发布 CNAPP 云原生安全保护平台

奇安信云安全管理事业部产品总监 范维博

在数字经济和数字化技术的驱动下，企业上云、用云，进入了全新的阶段。基于云原生技术底座的新一波技术创新、应用创新、模式创新即将爆发，同时也带来了严峻的安全挑战，近年来针对关键基础设施的云原生安全攻击频发。为此，奇安信正式推出 CNAPP 云原生安全保护平台，该产品是奇安信在云安全及云原生安全领域深厚技术积累的集大成者，依托业界领先的开发安全能力、运行时安全能力，为云原生应用提供全生命周期安全防护。

奇安信 CNAPP 云原生安全保护平台，以云原生应用为核心保护目标，能力覆盖整个云原生架构及云原生应用的全生命周期。纵向从下到上覆盖云原生应用运行的基础设施，横向从左到右覆盖云原生应用的整个生命周期，涵盖开发、部署和运行时阶段的安全风险监测与分析，贯穿一体系（DevOps）、两方向（安全左移与安全右移）、三环节（构建、部署、运行），提供云原生应用全生命周期的风险管理与卡点管控能力。

笃行致远，奇安信 Q-SASE 2.0 四大升级守护云网访问安全

奇安信 SASE 产品部总经理 王茜

数字经济时代，大型企业并购、应用系统上云、移动远程办公增加，各种新型数字化应用场景层出不穷，企业应用访问的边界模糊，资产暴露面扩大，对企业网络安全提出了更高的要求。

奇安信 Q-SASE 采用安全能力云服务化架构，基于一体化安全管理运营服务平台，实现三种场景下的安全能力全面防护，以及集中的安全管理和统一运营。本次推出的奇安信 Q-SASE 安全访问服务平台 2.0 版，以实践求真、知行合一为理念，实现简化部署、深层服务、易于合作、提升效率四大升级，“笃行致远”，为云网访问全程安全保驾护航。

让资产看的更全、更细、更准，奇安信发布网络资产攻击面管理系统

奇安信系统安全产品市场总监 李传洋

大部分组织在网络资产安全管理方面，仍然采用传统的人工台账、手动报告或依赖单一资产管理系统的工作模式，虽然能对可控资产进行掌握，但对一些影子、无主、僵尸、沉默、幽灵等资产却无从下手，导致逐渐失去对资产的可见和掌控，使未受保护的资产暴露未知攻击面，被攻击者利用造成安全风险。

奇安信网络资产攻击面管理系统

（简称 CAASM）通过 API 的方式获取分散在组织内部各系统中的“资配漏补”相关数据，对来自多源异构的数据进行归一与富化后，描绘出组织内部的全量资产安全关系图谱，并提供攻击面管理、资产管理及漏洞管理能力，让管理者对组织内部的资产及安全情况了如指掌，对应相关部门与责任人一目了然。

CAASM 通过对采集整理后的全量资产安全数据进行持续的碰撞与分析工作，发现资产安全事项，随即触发安全运营流程，持续驱动安全与运维人员消除问题与风险，输出相应运营成果。运营工作流程结束后，新发生的数据变更将为新一轮的数据碰撞分析提供输入，循环往复。CAASM 将以数据的方式持续触发安全运营流程，达到收敛组织网络资产攻击面、有效防护网络攻击路径的目标。

威胁情报新品发布，抓牢企业安全“主动脉”

奇安信合伙人＆威胁情报中心负责人汪列军

奇安信威胁情报中心此次共发布 ALPHA 威胁分析平台国际版、漏洞情报订阅服务、威胁情报 FEED 订阅服务三款产品及服务，继续完善威胁情报产品服务矩阵。

其中，ALPHA 国际版面向港澳市场及国际市场，聚焦以下三项业务：漏洞情报订阅服务，高价值、海量且及时的漏洞数据；威胁情报 FEED 订阅服务，高精准、多维度的威胁情报数据；研判分析查询服务，可直接判定报警真实性，了解攻击团伙 / 软件的意图和能力，进而快速筛选出真实、重要的报警。

漏洞情报订阅服务依托奇安信集团多年来积累的海量网络安全和互联网基础数据资源，通过长期的系统建设和专业团队的持续运营，输出全面的漏洞基本信息，聚焦真正形成威胁的漏洞，提供经过研判后的漏洞情报数据和报告服务。

威胁情报 FEED 订阅服务面向客户提供高精准、多维度的威胁情报数据和丰富的上下文信息，可以用来进行报警研判、攻击定性、黑客画像，以及识别失陷主机、被控终端、钓鱼邮件等。提升客户安全防护体系的基于威胁情报的自动化威胁处置能力，使企业客户可以更快速地分析威胁事件，及时遏制未知高级威胁攻击扩散和核心资产损失等重大风险的发生。

打造安全可控的文件流转通道，奇安信发布跨网文件安全交换管理系统

为解决用户文件流转过程中数据容易泄露、文件流转审计难、权限不好管控等问题，奇安信推出跨网文件安全交换管理系统（简称 FES 文件交换管理系统）。系统能够帮助客户在不同网络、不同安全域之间建立一个安全合规、高效便捷的可管控的数据

奇安信边界安全产品市场总监 刘志明

流转通道，让所有文件数据流转都能实现事前审核、事后审计，还能自动对流转的文件进行病毒检查和敏感信息发现，并根据安全检查结果自动触发不同审批流程，实现文件安全可靠流转，防止敏感数据外泄。系统支持多个隔离网之间的复杂交换规则，可广泛应用于企业、医疗、金融、军工、政法、党政等行业。

助力企业实现混合基础架构全流量可视化，奇安信发布流量解密编排器 2.0

奇安信鲲鹏网络平台总经理 李红光

企业数字化转型过程中，混合云基础架构将成为事实上的标配并长期存在。成熟的网络监控和安全工具专为本地化部署设计，无法适应整个基础设施，将导致企业看不全、看不清网络中正在发生的活动。缺乏统一的全视角和全流量的可视化解决方案，可能阻碍企业数字化转型进程。

针对如上问题，奇安信流量解密编排器 2.0 版本给出了很好的解决方案。

首先，通过各种隧道技术（GRE、VxLAN、IPSec 等），可将混合基础架构下的流量或元数据汇聚到总部数据中心进行集中全面的网络和安全可视化分析，简化企业网络安全管理，提升运营效率。

其次，新增的预处理技术（如去重、截短、去隧道、脱敏等）能够大幅降低混合基础架构下多个数据采集点导致安全工具重复处理无效流量开销，提高整体处理性能，以及避免企业数据隐私泄漏的风险。

此外，2.0 版本还引入了对国密 SM2、SM3 和 SM4 的支持，并可使用多种经过认证的硬件安全模块（HSM）来生成和保护密钥。同时，该版本还支持多种国产化硬件平台，其处理能力可覆盖企业全业务场景。

综上，奇安信流量解密编排器 2.0 版本，通过更多的流量可视化能力，可以提高混合基础架构下的安全和网络管理效率，降低客户安全基础设施总拥有成本。

专为中小企业打造，奇安信发布天擎终端安全管理系统 EDR 先锋版

中小企业虽然终端数量少，安全预算少，但面临的威胁却不少，并有着严格的终端安全管理要求。为此，

奇安信天擎事业部总经理 浦欣

奇安信特别推出了天擎终端安全管理系统 EDR 先锋版（简称“天擎 EDR 先锋版”）。

天擎 EDR 先锋版是专为中小企业打造的轻量化终端安全解决方案，具备全、能、极、简四大特点。

- 能力全面：天擎 EDR 先锋版的防火墙、漏洞补丁、自研 + 三方多引擎病毒查杀、高级威胁防御，对终端提供威胁攻击在事前、事中、事后的全方位防护；软件管理、终端管控功能，助力企业规范终端软件安装、管控终端行为；一体化管理平台，可同时管理 Win/macOS/Linux/ 信创系统的终端安全。
- 高级威胁防御能力：自研高级威胁防御引擎 +EDR 组合拳，防御钓鱼、勒索、APT 等高级威胁能力远超传统杀毒软件，让企业专注业务，无终端安全问题的后顾之忧。
- 性能极致，占用少：运行占用资源少，老旧的低配终端也能安装，不影响终端业务软件运行。
- 部署简单，轻松上手：一键即可部署，部署完即可使用。管理方式自动化，非专业安全管理人员，也能轻松管理。安

2023（第五届）北京网络安全大会于2023年7月6日在北京国家会议中心开幕。本届 BCS 大会将与 2023 全球数字经济大会融合举办，全面升级为国家级会议。

方滨兴、沈昌祥、冯登国、倪光南四位院士出席 BCS2023 并发表主题演讲。

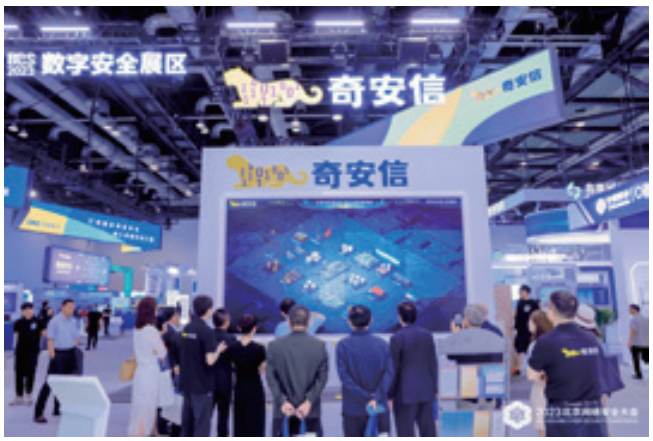

2023北京网络安全大会
2023 BEIJING CYBER SECURITY CONFERENCE
023北京网络安全大会
开幕仪式
23北京网络安全大会
EIJING CYBER SECURITY CONFERENCE


数智时代，是数据和智能的时代


2023北京网络安全大会
2023 BEIJING CYBER SECURITY CONFERENCE
2023北京网络安全大会
2023 BEIJING CYBER SECURITY CONFERENCE
签到处


《加强数字安全建设与保障》倡议

在 7 月 6 日的大会开幕式上，奇安信集团董事长齐向东发表“数智安全 内生为本”主题演讲，提出要以“零事故” 为目标、以“内生安全”为核心，推动数智时代网络安全建设。



大事记

齐向东出席中国互联网大会：数实融合 安全第一

7 月 18 日，在 2023 中国互联网大会上，全国政协委员、全国工商联副主席、奇安信集团董事长齐向东在发表主题演讲时表示，数实融合让数据成了关键生产要素和驱动发展的重要战略资源，要以“零事故”为目标，以“内生安全”为核心，进行网络空间的安全建设。

他表示，我们必须实现网络安全能力的全覆盖，做到无死角的安全防护，才能实现数实融合的万无一失。

北京市委网信办主任张劲林一行莅临奇安信开展主题调研

7 月 10 日，北京市委网信办主任、市委互联网企业工委书记张劲林一行莅临奇安信集团，就网络安全能力建设、网络安全运营能力提升进行主题调研。市委网信办副主任马春玲，网安处、技术处、综合处相关领导参与了本次主题调研。

张劲林一行详细参观了奇安信安全中心展厅、工控实验室、网络安全保障指挥中心及党建室，并听取了奇安信集团安全能力汇报，深入了解奇安信的企业发展沿革、战略规划、安全能力、科研创新等能力情况。

张劲林对奇安信在网络安全领域的建设及发展成果表示充分肯定。一方面，奇安信凭借网络安全领域的前瞻理念、先进技术、成熟能力，有力推动了我国网络安全事业从被动应对转向主动防御，并形成了领先优势；另一方面，在近年来北京市重大活动保障及促进本市产业发展、信息化建设方面，奇安信都做出了重要贡献。

齐向东出席 2023GDEC：用“零事故”标准 迎接数智时代的安全挑战

7 月 5 日，在 2023 全球数字经济大会（2023GEDC）主论坛上，奇安信集团董事长齐向东在发表主题演讲时表示，数智时代，“安全红线”越来越多，安全主体责任不断压实，政府和企业要加快补上数智安全课，以“零事故”标准进行网络安全建设。

补齐安全课，需要了解数智时代的安全态势。齐向东将其总结为三个“常态化”：勒索攻击常态化、数据泄露常态化和私挖滥采常态化。面对频发的网络安全事件和不断加剧

的网络安全事件后果，以“零事故”标准进行网络安全建设成为了大势所趋。基于奇安信圆满完成北京冬奥网络安全保障任务的成功经验，齐向东提出了“零事故”的三条标准：业务不中断、数据不出事、合规不踩线。

齐向东：破解数据安全“三难” 推动网安产业大发展

7 月 3 日，在“马连道 · 茶 · 中国数据街”高质量发展论坛开幕式暨 2023 全球数字经济大会西城区分论坛上，全国政协委员、全国工商联副主席、奇安信集团董事长齐向东在发表主题演讲时表示，数智时代，数据的作用发生了质变，数据安全需求将推动网安产业获得更大发展。

大发展是体现在多个方面的：其一是纵深防御的内生安全体系将获得大发展；其二是动态防控的“零信任”体系将获得大发展；其三是“零事故”的安全运营体系将获得大发展；其四是一体化的数据安全体系将获得大发展；其五是网络安全投入将不断填平补齐，达到 10% 以上。

“随着政企机构增加安全投入，网络安全产业会获得更大发展。”齐向东表示，奇安信也将紧抓安全需求，聚焦西城区重点产业领域的场景创新、产业发展和应用推进等方面，服务好西城区的数字化建设。

为充分整合西城区在金融、文化、商务服务等方面的优势资源，全力打造全球数字经济标杆城市示范区，在活动上，区委副书记、区长刘东伟代表西城区人民政府，与中国电子、北京联通、北京铁塔、中建设计研究院、阿里云、奇安信集团六家龙头企业，就联合打造“数字经济标杆街区”共同签署了战略合作协议。

奇安信完成中国首批人社部电子数据取证分析师认证

全国首批电子数据取证分析师（四级 – 中级工）职业技能等级认定考试于 2023 年 7 月 1 日在奇安信北京总部完成，共有 34 名考生通过前期报名资格审核并参加此次认证考试。

奇安信严格按照国家人社部职业技能等级认定标准及北京市人社局相关规章制度，从考务流程、题库设置、人员分配、质量管理、考核监督等各个环节形成标准体系化运营流程，积极配合人社局外督员考前、考中督导检查，最终圆满完成国家首批电子数据取证分析师认证考核工作。

江苏智慧 CA 获奇安信可信浏览器及八大操作系统联合认证

近日，江苏智慧 CA 加入由奇安信可信浏览器与主流操作系统厂商联合发起的“商用密码证书可信计划”，并通过“商用密码证书可信共同体”联合审核信任，受信根证书也将按计划预置到“商用密码证书可信共同体”的相关产品，包括奇安信可信浏览器、银河麒麟操作系统、统信 UOS 操作系统、openKylin 开源操作系统、欧拉社区、麒麟信安操作系统、方德桌面操作系统、统信 USmart 操作系统、超聚变 FusionOS 操作系统等。

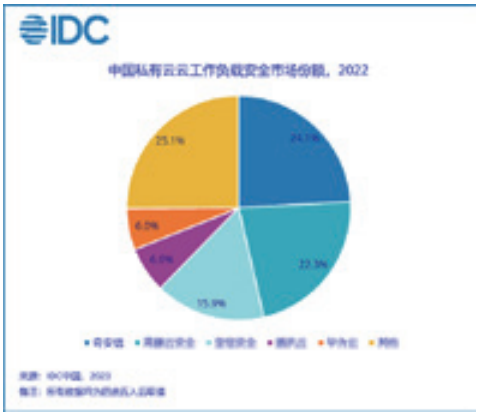
随着江苏智慧 CA 加入，目前已有 20 家 CA 机构加入“商用密码证书可信计划”，与浏览器及操作系统厂商共同推进国产密码证书信任体系落地，筑牢我国网络安全信任基石。

荣誉墙

IDC 报告：奇安信获私有云 CWPP 市场份额第一

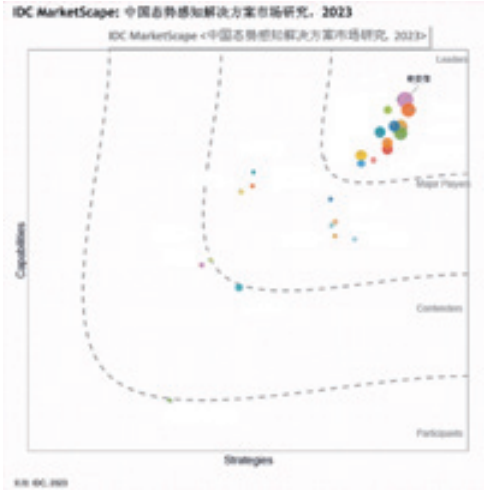
近日，全球领先的 IT 市场研究和咨询公司 IDC 发布了《中国私有云云工作负载安全市场份额，2022：合规为根基，技术为骨干》（下简称《报告》），其中奇安信 2022 年产品体系能覆盖云原生及混合云环境下的云工作负载安全（CWPP）需求，并在政府、金融、运营商、卫生、能源、制造等多个重要行业取得连续突破，营收达到 5290 万美元，以 24.1% 的占有率高居国内市场榜首。这是继去年奇安信获得云工作负载安全市场份额第一之后，在私有云场景下的又一“完美表现”。

依托奇安信集团完善的交付和安全服务体系，有效保障客户云工作负载安全产品的快速部署和调试及问题快速响应。在 2022 年北京冬奥会与冬残奥会重保期间，奇安信实现了冬奥云上 + 云下服务器的跨区域统一安全管理，涵盖赛事管理、运维管理、冬奥场馆等数十个冬奥业务系统。



能力和市场双领先！奇安信连续三次获态势感知“领导者位置”

近日，全球领先的 IT 市场研究和咨询公司 IDC 发布了



《IDC MarketScape: 中国态势感知解决方案市场 2023 年，厂商评估》（下文简称《报告》），对国内态势感知市场趋势、技术发展及国内主要供应商进行了深入分析和评估。

《报告》显示，奇安信凭借技术、服务及市场等多方面的绝对领先优势，再次入选“领导者象限”，这是自 2019 年 IDC 推出该系列报告以来，奇安信连续三次被评为“领导者”，且能力和市场双领先。

筑牢安全访问基石！奇安信斩获信通院双料大奖

7 月 12 日，中国通信标准化协会算网融合产业及标准推进委员会（CCSA TC621）“2023 年算网融合产业发展峰会”在京成功召开。会议期间，奇安信落地项目“基于信创技术的民航领域零信任安全体系”“某市教育城域网智慧安全服务化项目”分获“零信任最佳方案奖”和“SASE 优秀服务奖”。

奇安信在 2023 政法智能化建设技术装备及成果展上斩获殊荣

7 月 10 日至 11 日，2023 政法智能化建设技术装备及成果展在京开展，全面展示政法智能化建设领域新的科技应用和成熟方案。在成果展上，奇安信高效服务客户，运用新技术新理念解决客户难点、痛点的三个案例，获评创新案例。

它们分别是上海市司法局构建基于“人 + 工具 + 流程”的全维度闭环的安全运营能力、贵阳市检察院网络安全运营解决方案、乌拉特后旗政法委政法智慧化项目。

“六全框架”守护数据安全 奇安天盾荣获“数字经济创新引领成果”奖

7 月 7 日，2023 全球数字经济大会正式发布了数字经济新品成果征集评选结果。奇安信自主研发的“奇安天盾数据安全保护系统”（简称“奇安天盾”）凭借“能看清、能管好、能防住”的一体化保护能力脱颖而出，荣获“创新引领成果”奖。

据悉，本届活动自征集发布以来，来自北京、上海、天津、浙江、福建、广东等全国 16 省市地区，近 180 家企业参与其中，共计申报 230 余项新品。经充分的市场调研，以及来自国家工信部、科技部、中关村发展集团、北京邮电大学、中国软件评测中心、中国信息通信研究院、中国互联网投资基金等权威部门组成的专家团评议，奇安天盾最终斩获该项殊荣。

奇安信获得教育部“网络空间安全产学协同育人优秀案例”

7 月 6 日，由教育部高等学校网络空间安全专业教学指导委员会产学合作育人工作组主办、四川大学与华中科技大学共同承办的“第三届网络空间安全产学协同育人优秀案例”评选活动正式公布获奖名单，奇安信分别与清华大学网络科学与网络空间研究院、华中科技大学申报的协同育人案例获得一等奖，与武汉软件工程职业学院共同申报的协同育人案例获得三等奖。

本次优秀案例评选旨在深入贯彻习近平总书记在国家网络安全宣传周作出的关于国家网络安全工作“四个坚持”原则的重要指示精神，落实“要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态”具体工作布置要求，积极探索网络空间安全产学协同育人新模式、新机制。

奇安信虎符战队在 2023 年中国工业互联网安全大赛再获一等奖

7 月 5 日至 6 日，2023 年中国工业互联网安全大赛决赛及闭幕式在重庆国际博览中心举行，奇安信虎符战队在 125 支晋级决赛的队伍中脱颖而出，夺得一等奖。这也是该战队连续两年摘得大赛桂冠后的又一次夺冠。

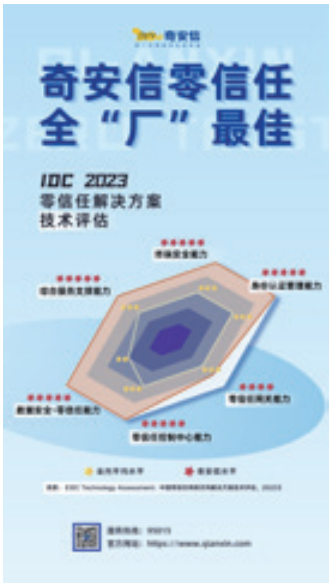
据悉，中国工业互联网安全大赛是中央网信办正式批复、由中国信通院牵头组织举办的国家级网络安全赛事，今年共吸引了来自全国各地区、各行业领域的近 2000 支队伍、6000 余名选手参赛，广泛汇聚电信、互联网、航空航天、能源等各行业领域专业技术人员及高等院校教师、学生。此次夺冠，再次证明了奇安信在安全服务、特别是工业互联网安全建设方面的不俗实力。

奇安信再次入选 2023 Gartner® SOAR 市场指南报告

近日，Gartner 正式发布了 2023 年《Market Guide for Security Orchestration, Automation and Response Solutions》报告。继 2022 年入选报告后，奇安信再次被列为具有代表性的供应商（Representative Vendors）之一。

奇安信 SOAR 具备区别于其他同类产品的 5 大关键能力——安全能力编排化、安全流程自动化、告警响应智能化、案例管理协作化、系统架构开放化。此外，SOAR 的协同作战式功能，还能让安全工程师实时沟通、并内置大量自动化剧本和命令，进一步提升人机协同作战效率。

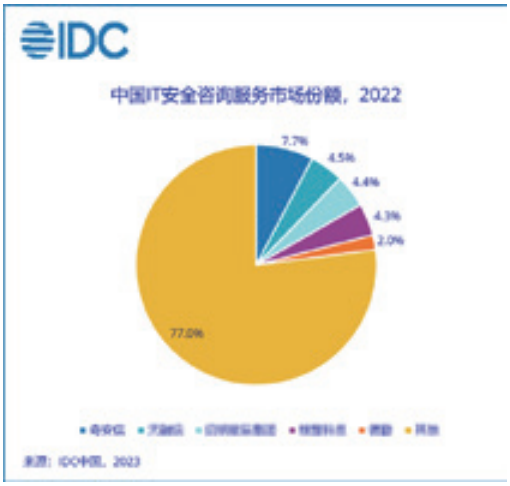
IDC 报告：奇安信零信任解决方案关键技术指标均表现优异



近日，全球领先的 IT 市场研究和咨询公司 IDC 发布了《中国零信任网络访问解决方案技术评估，2023》，对国内主流零信任网络访问（ZTNA）解决方案进行了深入的技术评估。其中，奇安信零信任网络访问解决方案在终端安全能力、身份认证管理能力、零信任网关能力、零信任控制中心能力、数据安全－零信任能力、综合服务支撑能力等所有六项关键技术能力评估中，均取得最优成绩（五个五星，一个四星），成为所有入围企业中，唯一获得五个五星、技术评估雷达图最接近正六边形的企业。

安全咨询服务连续三年第一！奇安信持续领跑安全服务市场

近日，全球领先的 IT 市场研究和咨询公司 IDC 发布了《2022 下半年中国 IT 安全服务市场跟踪报告》（以下简称《报告》）。《报告》显示，2022 年下半年中国 IT 安全服务市场厂商整体收入约为 18.4 亿美元（约合 128.5 亿元人民币），同比上升 4.8%。结合全年数据，2022 全年中国 IT 安全服务市场规模达到 30.7 亿美元，较 2021 年上升 7.2%。其中，2022 年奇安信以 7.7% 的市场份额，连续三年占据安全咨询服务子市场头名。另外，在托管服务市场，奇安信以 10.9% 的份额位居第二。



IDC 认为，随着企业和政府对自身数据安全保护的要求越来越高，不断推进安全运营中心理念和整体方案，安全服务和产品边界也变得模糊。目前，奇安信已经支撑了中央政府部门、金融、运营商、能源、电力、交通和地方企业等大型客户的咨询规划、托管运营，以及全国多个省市的智慧城市安全运营服务。

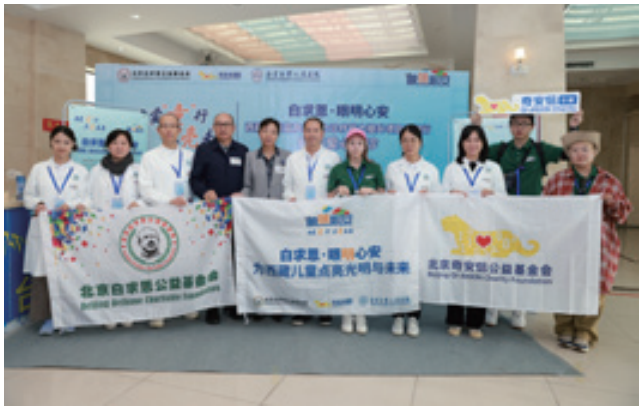
社会责任

白求恩 · 眼明心安—西藏儿童盲及低视力诊疗提升项目光明行活动圆满结束

7 月 12 日—15 日，由北京白求恩公益基金会主办、北京奇安信公益基金会和北京大学人民医院支持的“白求恩 · 眼明心安—西藏儿童盲及低视力诊疗提升项目”光明行活动在西藏自治区拉萨成功举办。

此次活动共邀请到 14 位来自北京大学人民医院、北京大学第三医院、首都医科大学附属北京同仁医院、复旦大学附属儿科医院、深圳市眼科医院、四川大学华西医院的国内顶尖眼科专家。在为期 4 天的活动中，开展了爱心义诊、入户探访、手术带教和诊疗技术培训等活动。“白求恩 · 眼明心安”项目培训基地同期揭牌。

本次“白求恩 · 眼明心安”西藏光明行活动是深入西藏开展儿童眼病防治工作的里程碑。项目响应了国家对西藏等高海拔地区的防盲治盲工作的指示，助力实现《“十四五”全国眼健康规划（2021—2025 年）》目标，将优质的眼科医疗资源带到人才技术匮乏地区，让西藏人民在“白求恩 · 眼明心安”西藏光明行活动中享受到国家推进健康中国建设成就，提升幸福感和满意度。



奇安信基金会与哈工大签署捐赠协议 哈工大 – 奇安信助学基金正式设立

6 月 28 日，北京奇安信公益基金会与哈尔滨工业大学教育发展基金会签署捐赠协议，正式设立“哈工大 – 奇安信助学基金”。基金将为哈工大网络空间安全学院家庭经济困难学生参与社会实践、紧急救助和奖助学金。

“哈工大是奇安信基金会在 2023 年资助的第一所 985 院校。”奇安信基金会秘书长齐子昕表示，哈工大作为我国“工程师的摇篮”，在网络安全专业建设方面也有深厚基础，多年来为我国网络空间安全产业发展培养和输送了一大批优秀学子，希望双方能够以此次捐赠签约为新起点，共同助力教育强国、科技强国、网络强国建设。

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

奇安信连续三年位居
“中国网安产业竞争力50强”
第一名

6月20日，中国网络安全产业联盟（CCIA）
公布“2023年中国网安产业竞争力50强”榜单，
凭借扎实的技术实力和领先的市场表现，
奇安信连续三年高居榜单第一名。

“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	华为技术有限公司
5	天融信科技集团股份有限公司
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	新华三技术有限公司
9	阿里云计算有限公司
10	杭州安恒信息技术股份有限公司
11	三六零数字安全科技集团有限公司
12	亚信安全科技股份有限公司
13	中电科网络安全科技股份有限公司
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