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

2022关键词

P27
5 个故事，50 个人，10000+ 字，记录奇安信的 2022

P48
超 10000 台信创终端如何替代?
深圳某区政数局依托准入 NAC 构建安全屏障

第24期
2022 年 12 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。

这一年

2022 年，终于要说再见了。

这一年，现实世界波澜壮阔：从无与伦比的北京冬奥会，到精彩绝伦的卡塔尔世界杯；从世界首个全面网络战，到焦灼反复的新冠疫情；从神舟十四的成功返航，到党的二十大胜利召开……这一年， 有太多历史值得铭记。

这一年，网络世界暗流汹涌：元宇宙不再只是少数人的理论，俄乌冲突将虚拟世界嵌入现实；全域复合战争已经发生，虚拟货币全球崩盘；漏洞超越“核武”成为最强军备，勒索走进企业成为经营常态；数据泄露风波未平，供应链攻击卷土重来……这一年，有太多问题需要面对。

这一年，安全成为全社会的共识。党的二十大报告中，91 次提及安全，29 次提及国家安全。面对百年未有之大变局加速演进，我国国家安全内涵和外延比历史上任何时候都要丰富，时空领域比历史上任何时候都要宽广，内外因素比历史上任何时候都要复杂。

这一年，网络安全已成为发展的先决条件。当传统安全威胁与新型网络安全威胁相互交织，当网络空间对抗成为大国博弈的常态化手段，没有网络安全就没有国家安全，也就没有社会安全，没有人民安全。

这一年，我国加快推进网络安全领域顶层设计。实施了 5 年多的《 网络安全法 》迎来了首次修改， 进一步压实网络安全责任；《 网络安全审查办法 》发布，网络安全风险防范能力不断强化；对网络安全违规事件的审查和处罚力度也不断加强，国家、企业、个人各类网络行为得到规范。

这一年，奇安信作为行业领军企业，在 2022 年创造了冬奥零事故的纪录，推动了销售驱动向技术驱动的转变，开启了国际化新蓝海的航程……

每段过往都会留下记忆，每一段历史时代都会留下痕迹，每个人的背后都有可以留下的故事。如果用几个关键词来体现 2022 这一年，你会选择哪几个？ 每个人的选择不尽相同，惟愿真实的声音激荡时代前行。

本期“2022 关键词”专题，选取体现行业特征的俄乌网络战、安全合规、信创安全、数据泄漏及勒索攻击等关键词，进行深度总结与解析，希望可以留下关于 2022 年的行业记忆。同样是在 2022 年，奇安信也经历军团战略、奥运零事故、国际业务突破、安全运营全面落地等重大事件，体现出行业领军者的技术领先与转型突破。

仅以此记录 2022 这一年。

总编辑

2022 年 12 月 1 日

CONTEN

目录

安全态势

P4 | 蔚来汽车披露数据安全事件：部分数据遭窃取 被勒索 1567 万元
P4 | 俄罗斯黑客组织入侵一美国卫星通信服务商，已在内网驻留数月
P4 | 美国关基保护重大事故！ FBI 关基设施关键联络人数据库泄露
P5 | 多个团伙利用社保公积金系统漏洞，非法获取公民个人信息 2300 万条
P5 | 勒索软件凶猛！比利时最大城市数字服务被迫中断
P5 | 法国巴黎又一医院遭勒索软件攻击，暂停运营并转移患者
P6 | Citrix ADC 和 Citrix Gateway 远程代码执行漏洞安全通告
P6 | ThinkPHP 远程代码执行漏洞安全通告 06
P6 | Snapd 本地权限提升漏洞安全通告 06
P7 | 国内攻防演习 11 月态势：哪些薄弱点最易被利用?
P10 | 国家发布“数据二十条”，构建数据基础制度体系
P10 | 《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》发布
P10 | 工信部印发《工业和信息化领域数据安全管理办法（试行）》
P10 | 国家能源局印发《电力行业网络安全管理办法》
P11 | 网信办等三部门发布互联网信息服务深度合成管理规定
P11 | 日本政府正式发布新版《国家安全保障战略》
P11 | 美国政府发布新版文件，提升关键基础设施运行弹性

行业篇

P13 **俄乌网络战**
高频率、大规模、新战法、新模式，首个全面网络战影响关基防护
P16 **安全合规**
监管加码、罚单频出 “合规”建设迫在眉睫
P18 **信创安全**
“大信创”开启万亿级风口 网络安全迎“最好五年”
P21 **数据泄漏**
勒索软件、网络钓鱼、人为错误……造成平均损失 435 万美元的数据泄露究竟因为什么?
P28 **勒索攻击**
国家进入紧急状态、巨量数据泄露、暗网交易猖獗，一切都拜勒索攻击所赐

月度专题

TS

安全之道

P48

超 10000 台信创终端如何替代?
深圳某区政数局依托准入 NAC
构建安全屏障

安全叨客

P52

想睡觉还真有人送枕头?
程序员们千万当心有人“投毒”

奇安资讯

P56 | 奇安信集团董事长齐向东当选全国工商联副主席
P56 | 奇安信入选 2023 年度工业信息安全监测应急支撑单位
P57 | 齐向东：“三步走”构建数据安全体系 守好数据安全红线
P57 | 奇安信中标某省 2022 年天翼云一城一池安全软件采购项目
P58 | 奇安信亮相香港 PwC HackaDay 2022
P58 | 奇安信中标中国联通某主机安全项目 打造主机威胁检测新范式
P59 | 奇安信被 Gartner 列为 NDR 全球代表性供应商
P60 | 奇安信金融行业零信任方案成功入选 CCIA“2022 年零信任优秀应用案例”

企业篇

P28 **新战略**
故事 1：实现销售驱动向技术驱动转变，22 个亿元军团由他们组成

P32 **新高度**
故事 2：奥运史上的“零事故”世界纪录，由他们创造

P37 **新蓝海**
故事 3：开辟万亿国际化新蓝海，由他们启航

P40 **新风口**
故事 4：迎接未来数据安全风口，由他们布局

P44 **新标杆**
故事 5：标杆项目全国领跑，由他们发力

《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：2022 年 12 月 26 日
发行对象：奇安信集团内部

事件篇

关基安全刻不容缓！我国警方打掉多个利用社保、公积金等系统漏洞非法获取公民个人信息的犯罪团伙，发现各类漏洞 300 余个；美国联邦调查局关基设施关键联络人数据库泄露，还有黑客潜伏其中，与其他组织进行交流。

蔚来汽车披露数据安全事件：部分数据遭窃取 被勒索 1567 万元

12 月 20 日综合消息，蔚来汽车信息安全委员会负责人卢龙在官方社区发布公告，称 12 月 11 日收到数据勒索邮件，对方以泄露数据勒索 225 万美元（约合人民币 1567 万元）等额比特币。经初步调查，被窃取数据为 2021 年 8 月之前的部分用户基本信息和车辆销售信息。蔚来公司称，承诺对因本次事件给用户造成的损失承担责任，并将协同有关执法部门深入调查此次事件，依法坚决打击相关的数据窃取、买卖行为。

俄罗斯黑客组织入侵一美国卫星通信服务商，已在内网驻留数月

据 CyberScoop 12 月 16 日消息，美国网络安全与基础设施安全局（CISA）的事件响应分析师 MJ Emanuel 在上个月的 CYBERWARCON 安全会议上声称，今年早些时候，俄罗斯黑客组织 Fancy Bear（又称 APT28）入侵了一家卫星通信服务商，并在内网驻留了数月之久。据悉，Fancy Bear 利用某个 VPN 设备的未修补漏洞进入内网，并在内部系统进行横向移动。该卫星通信服务商的客户遍布美国关键基础设施领域。

美国关基保护重大事故！ FBI 关基设施关键联络人数据库泄露

据 KrebsOnSecurity 12 月 13 日消息，匿名黑客 @USDoD 在一个网络犯罪交流论坛放出重磅数据，包含 8.7 万名联络人详细信息的 InfraGard 数据库，售价 5 万美元。InfraGard 是美国联邦调查局负责协调关键基础设施物理和网络威胁信息共享伙伴计划的联络人数据库，其中涉及美国各类关键基础设施企业的关键人员。有一名黑客成员甚至伪造了一家金融企业 CEO 的身份注册账号，并与其他成员交流。联邦调查局回应称，已了解此事，正在积极进行调查。

国际乒联服务器出安全问题，马龙、樊振东等运动员信息遭泄漏

据环球网 12 月 13 日消息，由于国际乒联的服务器出现安全问题，包括中国运动员马龙、樊振东在内的数百名职业乒乓球运动员护照、疫苗接种情况等个人信息遭泄漏。国际乒联发言人回应称，目前正对有关问题进行彻底的安全检查和调查。发言人还称，“一位独立技术专家提请我们注意我们服务器上的一个安全问题。国际乒联在得知此事后立即保护了访问权限”，“文件仅在此位置存储了很短的时间，我们没有证据表明，在有关报道出现之前，这些个人信息被人访问过。”

多个团伙利用社保公积金系统漏洞，非法获取公民个人信息 2300 万条

据红星新闻 12 月 7 日消息，四川南充市公安局顺庆区分局侦破一起公安部挂牌督办案件，打掉多个利用社保、公积金等系统漏洞非法获取公民个人信息的犯罪团伙，涉及四川、河南、广东多个省市，抓获犯罪嫌疑人 121 人，查获公民个人信息 2300 余万条，发现国内多地各类信息系统平台漏洞 300 余个，收缴黑客工具 12 套。民警调查发现，犯罪嫌疑人杨某先后通过“Telegram”聊天软件建立“普通查询”和“高级查询”两个聊天群，吸纳群成员 2200 余人，并将其从四川、广东、广西等地信息系统非法获取的 100 余万条公民个人信息和 300 余个系统漏洞发布至群内，用于交易牟利，已形成多个犯罪链条。

勒索软件凶猛！比利时最大城市数字服务被迫中断

据 BleepingComputer 12 月 6 日消息，由于合作的数字供应商遭受网络攻击，西欧国家比利时的安特卫普市的数字服务被迫中断，当地市民、学校、日托中心和警署所使用的服务均受到影响。比利时媒体《德斯坦达德报》报道称，造成事故的元凶正是勒索软件，但攻击者身份尚未确定。且还不清楚安特卫普市的 IT 系统何时才能完全恢复正常。该市市长表示，事件造成的影响可能持续到 12 月底。资料显示，安特卫普市是比利时面积最大、人口最多的城市。

法国巴黎又一医院遭勒索软件攻击，暂停运营并转移患者

据 TheRecord 12 月 5 日消息，法国巴黎综合性医院凡尔赛医院中心遭到勒索软件攻击，被迫叫停医疗手术并转移了 6 名患者。6 名患者中，3 名转移患者来自重症监护室，另外 3 名则来自新生儿病房。法国卫生部表示，凡尔赛医院中心目前已经陷入无计算机系统可用的困境。法国卫生部长弗朗索瓦 · 布劳恩 (Francois Braun) 在推特上表示，“这种以法国民众健康为要挟的行为不可接受……我们正在动员一切专业人员，确保给予患者护理和照料。”今年 8 月，巴黎另一家医院 Center Hospitalier Sud Francilien 也遭到勒索软件攻击，经过数周时间才得以恢复。

因遭遇网络攻击，太平洋岛国瓦努阿图政务网络瘫痪超三周

据纽约时报 11 月 28 日消息，受网络攻击影响，太平洋岛国瓦努阿图政府已经离线约三个星期。有官员告知当地新闻媒体，政府网络、官方网站和在线服务曾在 11 月 6 日遭到“入侵”，当时 Alatoi Ishmael Kalsakau 总理领导的新政府刚刚宣誓就职。政务系统离线后，对居住在几十个岛屿上的 32 万瓦努阿图民众生活造成了极大不便。民众难以获得服务，部分公务员也被迫重新拿起笔纸来办理事务。

印度最大医院遭网络攻击：业务中断超 4 天 只能手动处理工作

据 TechCrunch 11 月 24 日消息，印度最大公共医疗机构之一全印度医学科学研究所（AIIMS）遭遇网络攻击，出现业务中断。此次中断影响到数百位使用基础医疗保健服务的患者和医生，波及患者入院、出院和计费等系统。由于负责记录患者数据的服务器停止工作，该机构只能转为手动操作，包括手写病患记录。中断还导致排队周期延长，应急处置工作也开始出现失误。印度国家信息中心的团队正与印度计算机应急响应小组密切合作，帮助 AIIMS 尽快恢复系统。

漏洞篇

国内知名 PHP 开发框架 ThinkPHP 被曝光远程命令执行漏洞，经分析该漏洞需要开启非默认的多语言功能，有一定利用条件，但仍建议用户尽快升级至安全版本。

Citrix ADC 和 Citrix Gateway 远程代码执行漏洞安全通告

12 月 14 日，奇安信 CERT 监测到 Citrix ADC 和 Citrix Gateway 远程代码执行漏洞（CVE-2022-27518）。由于系统未能在其整个生命周期（创建、使用和释放）保持对资源的控制，致使远程攻击者在未经身份验证的情况下可在目标系统上执行任意代码。鉴于该漏洞影响范围极大，且已监测到在野利用，建议客户尽快做好自查及防护。

ThinkPHP 远程代码执行漏洞安全通告

12 月 9 日，奇安信 CERT 监测到 ThinkPHP 远程代码执行漏洞（无 CVE 编号，QVD-2022-46174）。当 ThinkPHP 开启了多语言功能时，攻击者可以通过 lang 参数和目录穿越实现文件包含，当存在其他扩展模块如 pear 扩展时，攻击者可进一步利用文件包含实现远程代码执行。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。ThinkPHP 是一个开源免费的面向对象的轻量级 PHP 开发框架。

Snapd 本地权限提升漏洞安全通告

12 月 1 日，奇安信 CERT 监测 Qualys 发布 Snapd 本地权限提升漏洞 (CVE-2022-3328) 通告，此漏洞需结合其他漏洞（CVE-2022-41974、CVE-2022-41973）使用。拥有低权限的攻击者可以利用这些漏洞将 /tmp 目录绑定到文件系统中的任意目录，进而将普通用户权限提升至 ROOT 权限。CVE-2022-41974 和 CVE-2022-41973 漏洞仅影响安装了 multipath-tools 的系统。目前，上述漏洞的技术细节均已在互联网上公开，恶意攻击者开发出漏洞利用难度降低，漏洞利用现实威胁上升。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Windows IKE 协议扩展远程代码执行漏洞安全通告

11 月 29 日，奇安信 CERT 监测到 Windows IKE 协议扩展存在远程代码执行漏洞（CVE-2022-34721）。IKEEXT 在处理 IKEv1 数据包时，没有对用户输入进行充分验证，未经身份认证的远程攻击者可通过向受影响的系统发送特制的 IKEv1 数据包触发漏洞，并执行任意代码。目前，此漏洞细节及 PoC 已在互联网公开，且存在在野利用，奇安信 CERT 已复现此漏洞。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

对抗篇

国内攻防演习 11 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 11 月，奇安信 Z-TEAM 团队共承接攻防演习服务 13 场，其中本单位自主攻防演习 13 场。

本月攻防演习成果如下图：

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集中，以政务、金融、军队行业为主，客户存在的安全问题主要涉及互联网侧应用更新不及时、内部人员对钓鱼攻击疏于

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	24	31	41	102	27	58	319	1025

防范、内网功能区域未隔离、弱口令及口令复用等。具体情况如下：

1、 历史漏洞仍是外网主要突破口

本月任务中针对特殊行业目标网络，外网突破中漏洞利用占据了主要部分。被攻陷目标所利用的互联网侧应用漏洞以历史漏洞为主，如外部应用中的 Shiro 组件漏洞、Weblogic 反序列化漏洞、Atlassian Confluence 远程代码执行漏洞等都是由于没有及时升级、更新相关应用或系统造成的。历史漏洞的存在仍是目标网络的重大安全威胁。

2、 钓鱼攻击具有较高突破成功率

本月任务中针对特殊行业目标网络，钓鱼攻击在外网突破中占比有所提升，主要是因为金融、军工、政务等这些目标客户网络较其他行业客户网络具有更高的安全要求，整体网络安全防护相对严密。因此，对其网络安全意识比较薄弱的内部人员开展钓鱼攻击就成为了实现外部突破比较高效的手段。

3、 弱口令是安全防护关键薄弱点

本月任务中口令爆破主要针对弱口令和口令复用，目标网络外部应用认证入口突破通过弱口令爆破实现，内网横向拓展过程中发现弱口令、口令复用问题则较为普遍，主要原因是目标网络缺乏对弱口令和口令复用的统一治理，没有对账号口令的设置和使用进行安全规范要求，如要求有相应的密码复杂度、禁止使用通用账号口令、账号口令定期更新等。

4、 业务网络缺乏纵深防御机制

本月任务中目标网络关键业务安全防护缺乏纵深防御机制，存在互联网侧服务器同核心内网未进行逻辑隔离的问题，内网安全部署缺乏功能域划分、Vlan 隔离等措施，主要表现在从外网突破互联网侧应用后台服务器后，可直接对内网业务进行扫描探测，很容易实现对内网核心业务的拓展渗透。

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，对目标网络的外网突破多通过互联网侧业务系统漏洞利用和钓鱼攻击实现，内网横向拓展则以弱口令、口令复用及内部应用漏洞为主。使用的主要技术手段分布如下：

1、 漏洞扫描利用

本月任务中发现漏洞主要集中在目标应用系统上，包括应用系统未授权访问、反序列化漏洞、弱口令、任意文件上传下载等漏洞。出现漏洞主要原因为客户安全运维人员安全意识不足、缺乏常态化的安全运营机制而导致应用系统版本更新不及时、安全策略设置不严格。

2、 隐蔽隧道外联

本月任务过程中，当遇到攻击动作或流量被察觉、目标内网无法出网的情况，就需要借助隐蔽隧道外连手段实现攻击动作的隐蔽执行和攻击数据的隐蔽通信。最终突破目标网络边界隔离限制，实现外网到内网的跨边界跳转访问控制。

3、 钓鱼攻击

本月任务中钓鱼攻击是在互联网侧直接突破手段受限的情况下开展的，主要以网络安全意识相对薄弱的客服人员、人事人员为目标，采取业务咨询、网络应聘等方式，进行钓鱼攻击突破；当针对管理人员和职能部门人员为目标时，则采取业务申请或报告提交等方式进行钓鱼突破。

4、 口令爆破

本月任务中内网口令爆破主要通过弱口令和口令复用方式实现，是内网横向拓展的主要手段。常见问题为未修改安全应用默认口令、管理员将多台网络节点设置为同一口令等，直接反映出目标网络对弱口令和通用口令缺乏统一监管的问题，尤其是对账号口令复杂度设置

和安全使用缺乏严格要求。

5、VPN 仿冒接入

本月任务中行业目标网络核心业务相对集中，对 VPN 入网范围限制较严，只有少量目标业务网络通过 VPN 仿冒接入实现渗透，利用手段包括外网通过 VPN 网关漏洞利用、内网通过口令复用获取 VPN 认证信息等。

四、典型攻击手段实现案例

攻击手段分布

1、漏洞扫描利用

（1）某目标某品牌办公自动化系统 OA 存在命令执行漏洞，通过漏洞利用获取到 OA 服务器权限，在服务器上抓取本地管理员密码，可进一步通过口令复用登录域控服务器，达到对目标办公域的控制。

（2）某目标财务系统存在 CVE-2022-21445 漏洞，通过该漏洞打入内存马，并成功获取服务器控制权限，可得到服务器中的相关敏感数据。

（3）某目标集中管控平台存在 CVE-2022-24990、CVE-2022-24989 漏洞，通过该漏洞可获得服务器权限并登录控制台，对 PC 下发控制命令，可控终端数量为 680 台。

2、钓鱼攻击

（1）利用某目标单位正在招聘的时机，以应聘的名义对目标 HR 人员进行钓鱼诱骗，最终获取到人事部门成员电脑终端的控制权。

（2）针对某目标内部招投标人员进行钓鱼，控制招投标业务个人终端，进一步获取内网招标服务器权限。

（3）通过某目标招标信息获得联系人手机号码添加微信，向其投递木马文件，获取个人 PC 权限，从而进入某目标内网。

3、口令爆破

（1）某目标巴士系统存在弱口令漏洞，通过此漏洞可获取该系统权限，可查看巴士线路、乘客人数、访客身份证号、电话等信息。

（2）某目标监控系统存在弱口令，通过此漏洞可直接登录该系统，查看大量网络设备和网络架构信息。

（3）某目标 OA 履职平台存在弱口令漏洞，通过该漏洞可查看人力资源系统用户的详细信息。

4、VPN 仿冒接入

（1）通过某目标的 VPN 命令执行漏洞，成功获取某目标 VPN 服务器权限，成功进入目标内网。

政策篇

国内，行业网络安全监管体系正加速构建，《电力行业网络安全管理办法》《工业和信息化领域数据安全管理办法（试行）》等纷纷出台；

国际上，日本政府发布新版《国家安全保障战略》，引入“主动网络防御”，允许在造成严重损害前阻止有害网络活动。

国家发布“数据二十条”，构建数据基础制度体系

12 月 19 日，《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》对外公布，从数据产权、流通交易、收益分配、安全治理四个方面提出二十条政策举措，初步搭建了我国数据基础制度体系。该意见提出，建立保障权益、合规使用的数据产权制度，探索数据产权结构性分置制度，推进实施公共数据确权授权机制，推动建立企业数据确权授权机制，建立健全个人信息数据确权授权机制，建立健全数据要素各参与方合法权益保护制度。

《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》发布

12 月 16 日，全国信息安全标准化技术委员会发布《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》（以下简称《实践指南》）。《实践指南》规定了跨境处理个人信息应遵循的基本原则、个人信息处理者和境外接收方在个人信息跨境处理活动的个人信息保护、个人信息主体权益保障等方面内容。《实践指南》为认证机构对个人信息处理者的个人信息跨境处理活动开展认证提供依据，也为个人信息处理者规范个人信息跨境处理活动提供参考。

工业和信息化部印发《工业和信息化领域数据安全管理办法（试行）》

12 月 13 日，工业和信息化部印发《工业和信息化领域数据安全管理办法（试行）》（以下简称《办法》）。《办法》共八章四十二条，主要内容包括界定工业和信息化领域数据和数据处理者概念，明确监管范围和监管职责；确定数据分类分级管理、重要数据识别与备案相关要求；针对不同级别的数据，围绕数据收集、存储、加工、传输、提供、公开、销毁、出境、转移、委托处理等环节，提出相应安全管理和保护要求等七个方面。《办法》自 2023 年 1 月 1 日起施行。

国家能源局印发《电力行业网络安全管理办法》

12 月 12 日，国家能源局印发《电力行业网络安全管理办法》（以下简称《办法》）。《办法》共五章三十五

条，主要内容包括总则、监督管理职责、电力企业责任义务、监督检查等。《办法》提出，电力行业关键信息基础设施运营者要明确一名领导班子成员作为首席网络安全官，应当优先采购安全可信的网络产品和服务，建立网络安全资金保障制度，确保网络安全投入不低于信息化总投入的 5%。《办法》要求，电力调度机构应制定电力监控系统专用安全产品管理办法，并监督实施。

网信办等三部门发布互联网信息服务深度合成管理规定

12 月 11 日，国家互联网信息办公室、工业和信息化部、公安部联合发布《互联网信息服务深度合成管理规定》（以下简称《规定》）。《规定》要求，深度合成服务提供者应当落实信息安全主体责任，建立健全管理制度和技术保障措施，制定公开管理规则、平台公约，对使用者进行真实身份信息认证，加强深度合成内容管理，建立健全辟谣机制和申诉、投诉、举报机制。《规定》将于 2023 年 1 月 10 日起施行。

国际

日本政府正式发布新版《国家安全保障战略》

12 月 16 日，日本政府发布新版《国家安全保障战略》，为包括网络在内的国家安全政策领域提供了战略指导。新战略提出，日本当前面临着二战以来最严峻的安全形势，尤其是针对关键民用基础设施的跨境网络攻击及通过虚假信息传播的信息战不断发生，从而进一步模糊了应急与和平之间的界限。新战略提出，将通过“提升网络安全领域应对能力”来“加强全方位无缝保护日本的力度”。为保障网络空间的安全稳定使用，特别是国家和关键基础设施安全，网络安全领域的响应能力应达到或超过西方领先国家水平。

美国政府发布新版文件，提升关键基础设施运行弹性

11 月 22 日，美国网络安全与基础设施安全局（CISA）针对全国基础设施发布《基础设施弹性规划框架》更新版指导文件。新版文件可帮助用户探索基础设施系统之间的依赖关系，以更好地了解基础设施风险，制定项目和战略来解决它，并确定资金和实施资源来采取行动。该文件引入了新工具关键基础设施识别数据集，可用于查找关于关键基础设施资产的公开信息。

美国国防部发布零信任战略及实施路线图

11 月 22 日，美国国防部发布《国防部零信任战略》及《国防部零信任能力执行路线图》，概述国防部计划如何在 2027 财年前在国防部范围全面实施零信任网络安全框架。美国国防部首席信息官约翰·谢尔曼在战略中指出，该战略的目的是通过从边界防御模式转变为“从不信任，始终验证”，以应对攻击性网络威胁的“快速增长”。战略概述了四项综合战略目标：零信任文化采纳、保护和捍卫国防部信息系统、技术加速、零信任启动，并详细介绍了实现零信任这一网络安全新范式所需的 100 多项活动、能力和支柱。安

行业篇

5个关键词，5篇深度记述，留下2022的年度记忆

2022年，终于要说再见了。

这一年，现实世界波澜壮阔：从无与伦比的北京冬奥会，到精彩绝伦的卡塔尔世界杯；从全球首个现代化网络战，到焦灼反复的新冠疫情；从神舟十四的成功返航，到党的二十大胜利召开……这一年，有太多历史值得铭记。

这一年，网络世界暗流汹涌：元宇宙不再只是少数人的理论，俄乌冲突将虚拟世界嵌入现实；全域复合战争已经发生，虚拟货币全球崩盘；漏洞超越“核武”成为最强军备，勒索走进企业成为经营常态；数据泄露风波未平，供应链攻击卷土重来……这一年，有太多问题需要面对。

这一年，安全成为全社会的共识。党的二十大报告中，91次提及安全，29次提及国家安全。面对百年未有之大变局加速演进，我国国家安全内涵和外延比历史上任何时候都要丰富，时空领域比历史上任何时候都要宽广，内外因素比历史上任何时候都要复杂。

这一年，网络安全已成为发展的先决条件。当传统安全威胁与新型网络安全威胁相互交织，当网络空间对抗成为大国博弈的常态化手段，没有网络安全就没有国家安全，也就没有社会安全，没有人民安全。

这一年，我国加快推进网络安全领域顶层设计。实施了5年多的《网络安全法》迎来了首次修改，进一步压实网络安全责任；《网络安全审查办法》发布，网络安全风险防范能力不断强化；对网络安全违规事件的审查和处罚力度也不断加强，国家、企业、个人各类网络行为得到规范。

在岁末年起，一起回顾一下，2022年有哪些体现年度特征的关键词。

2022关键词

作者 张少波 魏开元 李建平

2022 关键词

“俄乌网络战”

高频率、大规模、新战法、新模式，首个全面网络战影响关基防护

2022 年 2 月 24 日，俄乌军事冲突爆发，网络攻击战先行，期间发生大规模的网络攻击活动，俄乌双方通过大规模攻击关基设施，实现设施破坏、系统中断、数据窃取、信息战等四种主要目标，以配合军事行动。俄乌网络战被国际智库称为世界首个全面网络战。

一、俄乌网络战整体态势回顾

俄乌军事冲突期间，世界首个全面网络战爆发。知名智库北大西洋理事会认为，俄乌网络战是世界第一次全面网络战争，未来所有军事冲突都将同时发生网络攻击活动。

俄乌网络战呈现高频率、大规模、新战法、新模式特色，深度影响未来关基防护——关基设施安全防护需要具备能够应对大规模攻击的能力。

在网络战期间，俄乌双方利用 DDoS 攻击、钓鱼欺诈、漏洞利用、供应链攻击、恶意数据擦除攻击等多种“网络武器” 发起破坏袭击，威胁关系国计民生的关键基础设施，导致设施破坏、业务中断、通信停服、数据窃取的后果。

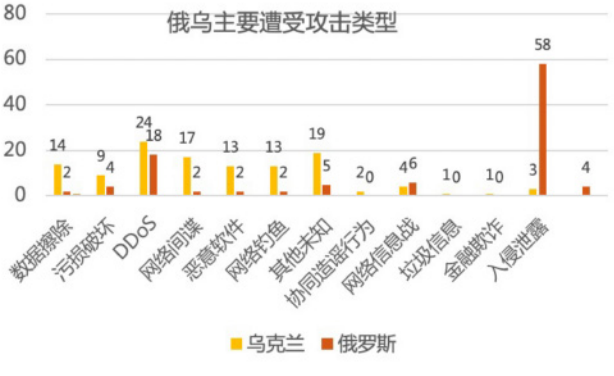
具体来看，网络战期间主要攻击形式包括如下。

（1）设施破坏：半数乌克兰政府遭关停。俄方攻击者利用乌克兰政府网站 CMS 漏洞，破坏乌政府大量网站，发布威胁信息，制造社会混乱。

（2）数据擦除：关键业务被中断。双方使用大量数据擦除软件，对政府、ICT、金融和能源机构进行数据擦除攻击，致使业务瘫痪。

（3）通信中断：影响军事指挥。其中乌电信运营商 Ukrtelecom、卫星互联网公司遭网络攻击，致使全国服务中断，服务能力降至战前的 13%。

（4）数据窃取：大量被窃取利用。俄攻击者窃取 700 万人数据，利用 “机器人农场”向乌士兵发短信，



督促士兵进行破坏和投降。

（5）信息战：直接影响战争走向。俄乌开展信息战，利用各类真实与虚假信息，制造混乱、赢得支持。直接影响舆论走向和战争结局。

二、俄乌网络战主要特点

俄乌网络战是现代首次网络战争，吸引了全球攻击组织与黑客人员参与，西方与俄罗斯网络攻防能力得以全面展示，期间攻防新趋势，对国家安全和关基安全防护建设具有深远影响。概括而言，俄乌网络战是有如下特点：

- **网络战成为现代战争的标配，热战未起网络攻击先行。**

未来的军事冲突都将配合网络攻击活动。根据奇安信的威胁情报分析研判，俄方先于军事行动之前，便爆发了针对乌克兰政府机构等关键部门的大规模分布式拒绝服务攻击和数据擦除恶意软件攻击。在战争开战之前，利用网络战损毁敌对国关键信息系统，窃取军事情报，瘫痪互联网、交通、能源金融等关键基础设施，成为现代战争的首选项。

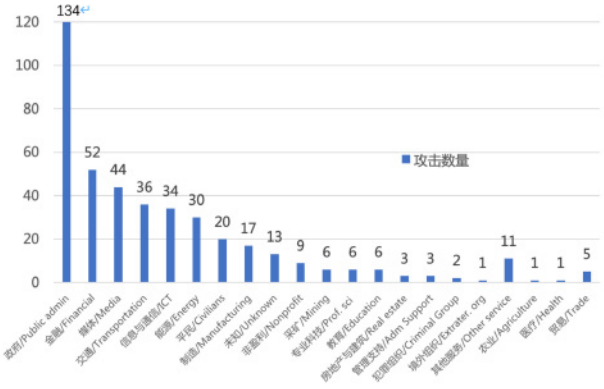
- **网络攻击规模、数量及参与人员达到前所未有的强度。**

主要表现在，参与组织多：全球参与网络战组织达 89 个，为历史最高（截至 7 月 14 日）。参与人员多：全球约 40 万黑客人员参与其中，防护难度空前。攻击行动多：冲突相关网络攻击和行动达 447 多次（截至 2022 年 9 月中，对俄 131、对乌 144），影响 27 个国家。

- **关基行业成为网攻的重点，政府、能源、金融、交通、通信与制造等六行业攻击居前。**

根据截至 9 月的统计，在 447 次行动中，针对政府行业的攻击高达 134 次；战争期间攻击政府机构，中断和瘫痪政务服务，易造成社会混乱。其他依次为金融 52

次，媒体 44 次，交通 36 次，能源 30 次，教育 17 次。



- **网络战出现新战法和新模式**

全球参与攻击组织大量使用各类新攻击手段，出现了大量使用数据擦除软件、首度攻击卫星网络、首度应用深度伪造等新攻击对象和新手法。乌克兰成功尝试 IT 志愿军模式，成功实现安全能力晋级。

三、俄乌网络战对关基防护启示

俄乌利用高级网络武器，对系统漏洞、供应链漏洞、人的漏洞和新技术漏洞开展攻击，令网络战呈现出攻击强度高、手段丰富、目标多样、后果严重的特点，关基行业需要具备抗击未来网络战的风险底线思维，有效防范和面对网络空间的主要安全风险，尤其是需体系化思考，构筑一体化安全体系。

1. 关基设施防护成为重中之重

俄乌网络战关基单位成为首要攻击目标，政府、能源、金融、交通、通信与制造六大行业攻击居前。

2. 新型攻击方式需重点防范

攻击方密集使用数据擦除软件进行攻击，软件供应链攻击、开发关基系统定制木马进行渗透和潜伏。攻击手段越来越难以防范，需要不断更新安全防护能力。其中，供应链风险凸显，成为最难以防范的方式。俄利用内容管理系统攻击，瘫痪数十家政府网站。Notpetya 攻击利用乌财务软件；美国太阳风（SolarWinds）供应链攻击波及 200 家美重要机构。

3. 新攻击面风险需要重点防护

现代数字基础设施加速发展，容器化、SaaS 应用及混合工作环境急速增长，企业面临的攻击面也在随之扩大。

俄乌网络战期间，首次出现对卫星互联网攻击、利用深度伪造发起信息战，展示出新技术的风险。实时更新攻击面，防范新风险。

4. 安全漏洞广泛存在是最大风险

安全漏洞是攻击主要入口。俄利用漏洞部署数据擦除软件，绕过多重身份验证。 47% 的攻击是漏洞利用。1990–2019 Windows 漏洞达 6814 个。主要攻击组织都维护着丰富攻击向量工具箱，可以随时作为攻击的有利武器。

5. 最基础网络攻击依然是重要手段

人是安全链中最薄弱环节。网络钓鱼实现系统突破是重要攻击方式。模拟钓鱼攻击、用户安全意识教育仍是最有效的措施之一。

6. 有效安全运营显著提升防护效果

根据微软公司的分析，俄罗斯对乌克兰的网络攻击成功率仅为 29%。乌通过消减漏洞、降低暴露面、主动威胁狩猎、威胁情报共享、强化安全运营取得了较好防护效果，设法维持绝大多数地区的基本公用事业服务。俄乌网络战期间发生多个终止攻击活动和降低攻击损失的案例。

2022 关键词

“安全合规”

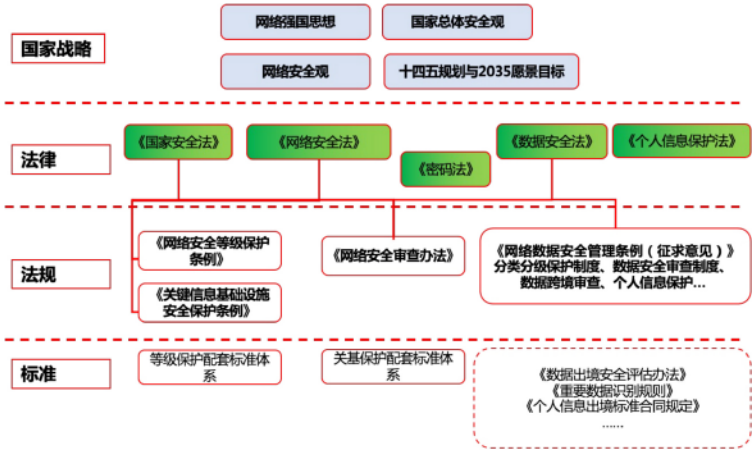
监管加码、罚单频出 “合规”建设迫在眉睫

2022 年，网络安全行业什么话题最热？合规无疑是其中之一。

在这一年，各种法律法规进入全面落实阶段。《网络安全法》迎来正式实施 5 周年，并迎来首次修改；《数据安全法》迎来实施 1 周年，相关的管理认证、监管细则等陆续推出，《数据出境安全评估办法》正式公布；《关基保护条例》《个人信息保护法》先后迎来实施一周年；《网络数据安全管理条例》也正式纳入立法过程。

与此同时，2022 年也是监管加码、罚单频出的一年。滴滴被罚 80.26 亿元；工业和信息化部累计通报、下架违法违规 APP 近 3000 款；《网络安全法》修改意见，对企业罚款从最高 100 万提高到 5000 万或上一年度营业额的 5%。

“不以规矩，不能成方圆”，合规是实现网络安全、保障国家安全的基础，正成为数字经济时代政企机构的首要任务与核心挑战。二十大报告，91 次提及安全，29 次提及国家安全！这足以体现安全在未来国家发展中的地位和影响。对政企机构来说，网络安全合规即发展。



图：国家战略与网络安全法律法规概览

一、内外部形势严峻 网络安全加强合规建设迫在眉睫

网络安全在合规驱动的道路上，至少有国际外部环境、国家战略要求，数字化经济发展、威胁形式变化等多重因素的联合驱动。

首先是国际环境波云诡谲，网络对抗威胁日益严峻。

整个 2022 年，世界百年未有之大变局正在加速演进，和世纪疫情交织叠加，国际环境日趋复杂，网络霸权主义对世界和平与发展构成威胁，网络空间安全面临的形势持续复杂多变。数字化空间的对抗已成为大国交锋的重要战场，网络安全已成为国家安全的重中之重。这也就不难理解我国在平衡安全与发展之间关系时的逻辑。强化安全法律体系构建与合规要求，如何强调其重要性都不为过。

其次是数字化潮流大势所趋，安全底板重要性凸显。

当前，“数字经济”正成为拉动中国经济增长的新引擎，其高速发展离不开国家宏观规划和政策的支撑。2021 年 3 月，“中华人民共和国国民经济和社会发展第十四个五年规划

和 2035 年远景目标纲要”正式发布，其中提出迎接数字时代，激活数据要素潜能，推进网络强国建设，加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革。

2022 年 12 月 19 日，中共中央、国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”），对数据确权、流通、交易、安全等方面做出部署。“数据二十条”明确，数据基础制度建设事关国家发展和安全大局，要维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。

最后，网络空间威胁形势日新月异，影响范围与维度不断扩展，也是网络安全政策法规密集出台的又一大推动因素。

2022 年以来，安全攻击呈现出以下四个新趋势：第一是勒索攻击事件呈现显著上升趋势；第二是数据窃密事件指数级攀升，且每起数据泄露事件带来的平均损失越来越大；第三是有组织的 APT 攻击威胁不减，甚至上升到大国之间的外交博弈；最后，供应链安全已成为网络安全的新战场，之前的安全短板亟待补课。

二、从合规体系完善到实际效果落地尚存在距离

回顾整个 2022 年，面对复杂而严峻的网络安全威胁形式，当前我国各个行业的合规落地实施仍存在诸多软肋和不足，具体表现在以下三个方面。

第一，网络安全的主体责任未压实。

目前网络安全法律法规、规章标准虽然名目繁多，但惩罚措施较为宽松。即便是《网络安全法》正式实施以后，其最高罚款也不超过 100 万元，对于中大型企业尤其是各行业的头部公司而言，相较于复杂的网络安全技术与人才的投入，其处罚力度也远远不够。

这就带来了一个问题，网络安全主体责任并未压实。尤其越是头部的大型企业和政府机构，其发生网络安全事故后导致的后果也越严重，不仅是经济损失，更多时候其造成的国家安全与社会民生影响往往更为严重。这

也是为什么在《关基保护条例》中，特别强调了从关基运营者的主体责任，以及保护工作部门的本行业本领域监测预警与指导任务。

第二，网络安全“能力体系”的亟待完善。

网络安全从法规到落地执行，需要大量的能力支撑，这些能力中包括技术、管理、运行能力，这种综合能力体系的构建，就需要有框架、参考架构、标准、指南作为指导。

近两年来我国网络安全法律法规完善速度非常快，已经走在了全球前列，但在网络安全能力体系的建设上，相比最先进的体系而言，中间这层的能力指引缺失，却在一定程度上阻碍了我国网络安全整体水平的进步。

第三，常态化、实战化的深度运营缺失。

网络安全最终的效果需要从实战化中体现，尽管近年来实战攻防演习的水平越来越高，但有很多问题也隐藏其中。比如，在演习期间防守非常严密，随着演习的结束，所有运营手段都又恢复成“老样子”：对那些高危甚至已经发生在野利用的漏洞视而不见、需要加固的策略无持续优化、安全设备的检测规则也不及时更新……如此一来，原本查漏补缺的目的就并未达到，借演习来提升实战化安全能力、满足合规需求的目标也就随之落空。

三、结束语

总体来看，从无法可依到有法可依，从合规性驱动到合规性和强制性驱动并重，以《网络安全法》《数据安全法》《个人信息保护法》等为代表的网络空间安全法治建设，为维护国家总体安全、抵御网络空间各种风险发挥了重要作用。然而，在当前国际严峻的威胁形势下，网络安全面对的挑战依然严峻，合规建设任重而道远。只有落实体系化建设，实现国家指导、行业保护、网络服务机构支持、运营者落实等多方协同，才能落实相关合规监管要求，筑牢网络安全底板，化解重大风险，为我国数字强国之路保驾护航。

2022 关键词

“信创安全”

“大信创”开启万亿级风口 网络安全迎“最好五年”

党的二十大报告将国家安全和科技自立自强提升到了全新高度，信创（信息技术应用创新产业）作为万亿级热门赛道，成为 2022 年的年度关注焦点。

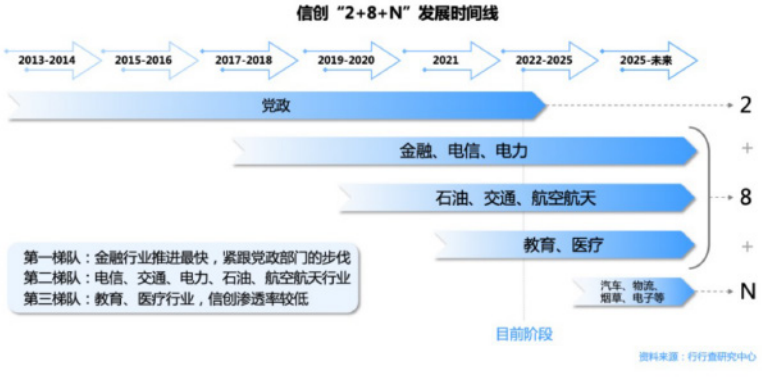
如果说 2020 年是信创元年，2022 年可称为行业信创元年。机构普遍认为，2020—2022 年是党政信创需求爆发的三年，从 2023 年开始至 2027 年，行业信创将接力党政信创，从金融行业、运营商、电力行业，逐渐向教育、医疗等行业扩散。未来五年，从党政到行业，信创“2+8+N”应用体系的需求将全面爆发。据海比研究院统计，到 2025 年，信创市场规模预计突破 2 万亿，2021—2025 年复合增长率为 35.7%。万亿级蓝海市场呼之欲出，“大信创”时代已经到来。

一、信创从党政迈向“2+8+N”重要行业

“大信创”时代，随着信创内涵渐趋丰富、生态日趋成熟，网络安全将迎来爆发式增长的黄金时代。一方面，

信创建设浪潮从党政迈向“2+8+N”重要行业领域，网络安全市场空间将呈指数级攀升；另一方面，信创的数字化也在不断深入和成熟，从早期政务办公到深入行业经营业务，甚至在生产运营系统中，行业的安全需求迎来细分和井喷。可以预见，在产业生态日趋成熟、信创发展日趋市场化的背景下，拥有核心技术实力的安全企业才能够获得领先市场份额。

具体在行业进展上，党政、金融由于起步最早，且有明确政策要求，走在了信创的最前沿。其中，党政作为信创发展的排头兵，目前已基本完成省市级单位电子公文系统的国产化替换。未来会进一步下沉至县级、乡镇级党政单位的电子公文系统替换中。同时，市级以上党政单位的电子政务系统国产替换也会同步进行。金融行业，随着信创一期、二期试点的结束，头部金融机构（银行、保险、证券）基本已完成了OA系统的国产替换，少数已实现了单轨运行。未来将逐步向非核心业务系统（ERP、CRM等）的国产替换演进。在目前进行的第三期信创试点中，信创进程持续推进。



其次，电信行业信创在新一轮的政策引导下，也开始稳步发力。电信行业信创，主要围绕三大运营商进行，目前已基本实

现了底层服务器、整机等硬件的国产替换。同时，各地纷纷建立了相关“信创实验室”，并启动软件迁移适配工作，推动电信行业信创持续落地。

最后，教育、能源、交通等行业的信创，虽尚处发展初期，但一些头部企业和机构已开始进行国产化 IT 设施替换试点。未来随着政策进一步出台，这些行业的信创势必也会全面开展。

二、新场景叠加新威胁 “大信创”赛道催生网安大市场

信创并不意味着安全，甚至可以说，信创更需要安全。因为在信息化的重塑过程中，面临的新场景、新威胁更加复杂，对安全提出了更高的挑战。

首先是信创环境下，安全漏洞和病毒问题更加严峻。由于信创大量基于开源框架复用，面临着软件供应链、信创漏洞研究缺失等问题。根据奇安信《 2021 中国软件供应链安全分析报告 》显示，国内企业软件项目 100% 使用了开源软件；超 8 成软件项目存在已知高危开源软件漏洞。和传统终端环境一样，信创终端同样存在着木马、病毒、恶意软件肆虐，勒索、挖矿病毒横行等情况。

第二是信创安全普遍还是外挂式安全，并没有与数字化深度聚合。目前信创安全普遍与信创重构相脱节，更偏重于生态、适配和业务迁移，缺少了与安全深入融合。随着行业信创的爆发期即将到来，“云大物移智”等数字化新技术在信创环境中不断应用，新的风险、新的攻击手段也不断来临，伴随这些新场景而来的则是一个个巨大的安全问题。

第三是信创安全缺乏全局和前瞻视角，并未实现同步规划、同步建设、同步运营。具体表现在“重替代、轻安全规划”“重功能、轻安全融合”“重单品、轻体系建设”等，面对网络攻击依然停留在事后补救的“补丁式防护”，缺少围绕体系化建设的咨询、规划、评估，其效果可想而知。

可见，在复杂多变的国际环境、层出不穷的新型威胁下，“大信创”面临的安全挑战依然严峻，同时也带来巨大的网络安全需求。

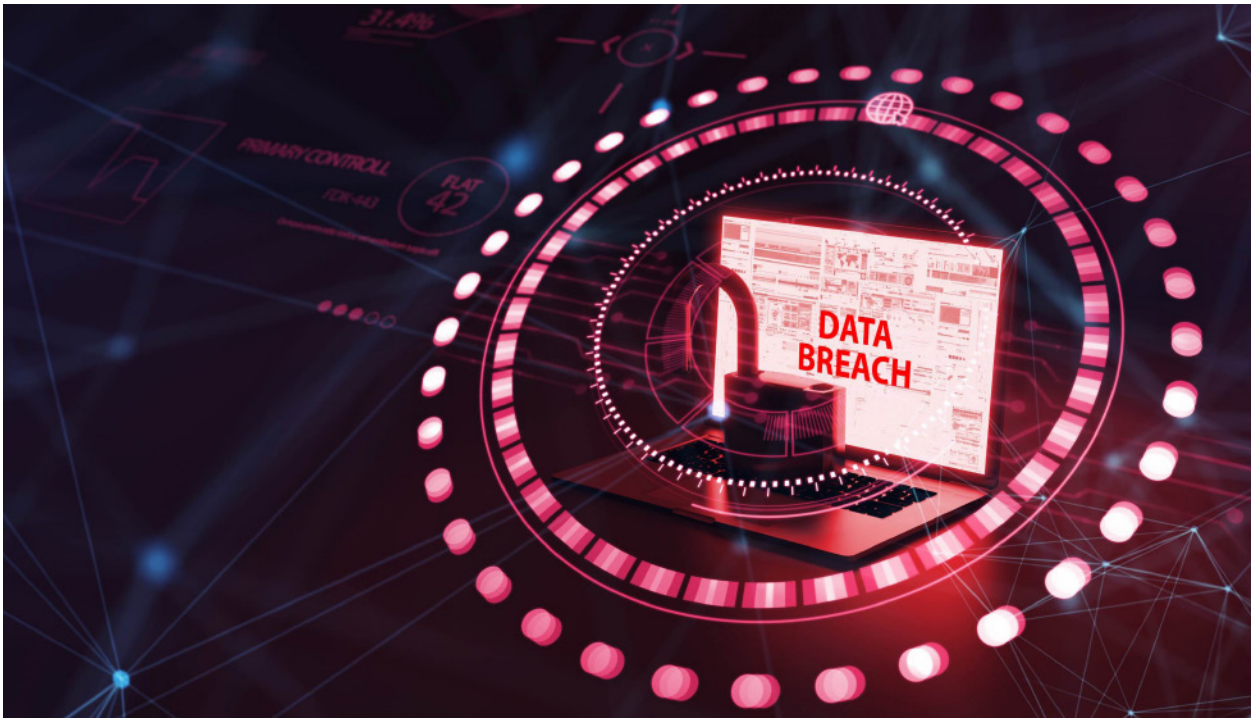
三、政策利好持续加码 信创网安市场将迎井喷

2022 年，信创行业迎来了多重政策利好。二十大报告中多次提到坚持“科技自立自强”，“大信创”在国家战略高度中的基础性、关键性、自主性和安全性特征全方位凸显，未来一段时间预计“信创”有望迎来政策持续加码。

2022 年 5 月，深圳发布了《 关于促进消费持续恢复的若干措施 》，在第五条明确提出了“扩大信创产品市场规模”，并明确要求“对采购 50 万元以上信创产品、符合条件的用户单位，按采购额的 3% 给予补贴。”同时对党政机关、国资国企、新增关键信息基础设施，以及金融、能源、教育、医疗、电信、交通等重点领域的信创产品采购比例进行了规定。研究机构指出，信创核心品类有望继续横向拓宽、纵向下沉，以区县信创为代表的党政事业单位信创有望进一步打开千亿级空间。

据测算，党政信创潜在市场规模 1616 亿元，行业信创潜在需求约 2500 亿元。依据《 网络安全产业高质量发展三年行动计划 (2021—2023 年) 》中规定，电信等重点行业网络安全投入占据信息化投入比例不低于 10% 来计算，信创网络安全市场的潜在市场规模将达 400 亿元以上。预计到 2025 年，中国的信创产业产值将会达到 8000 亿元，如果网络安全能够占到 10%，就能够为网络安全行业带来 800 亿的市场，这无疑是一个巨大风口。

展望 2023 年，行业信创将会爆发，网络安全将围绕着网络、数据、身份、应用、运营等五方面加强建设，数据、身份、安全运营等将是网络安全行业的爆发点。按照网络安全投资占比 5~10% 的比例，万亿级大信创风口将带来数百亿的网络安全市场。在这个过程中，能力全面的头部厂商，竞争优势显然更加明显，容易形成强者愈强的“马太效应”，以奇安信等为代表的综合能力更全面、信创经验更成熟的网络安全厂商，有望在这个黄金赛道上继续扩大领跑优势。



2022 关键词

“数据泄漏”

勒索软件、网络钓鱼、人为错误……造成平均损失 435 万美元的数据泄露究竟因为什么？

在过去的 2022 年里，数据泄露的风波仍在继续，且有愈演愈烈的趋势。有网络安全公司的公开研究显示，仅在第三季度，便有 1.089 亿个账户被侵入而发生数据泄露事件，比上一季度增加了 70%。

与之对应的是，数据泄露给组织造成的损失也在不断增加。

据 IBM Security 的“数据泄露成本报告”显示，2021—2022 年间，数据泄露的全球平均成本从 424 万美元增加至 435 万美元，同比增长 2.6%，创历史新高。虽然数据泄露有关的财务成本较高，但其对于企业的实际影响显然还要更深，甚至涉及到声誉损失、法律责任及消费者的信任损失等。

2022 年全球数据泄露 Top10

综合考量数据泄露数量、影响范围及造成的损失等多方面因素，下面盘点出了 2022 年来全球范围内发生的十起较为严重的数据泄露事件。

No. 10：SuperVPN、GeckoVPN 和 ChatVPN 数据泄露

此次事件涉及几个广泛使用的 Android VPN 服务（SuperVPN、GeckVPN 和 ChatVPN），导致 2100 万用户的信息泄露。这些信息包括用户全名、用户名、国家名称、账单明细、电子邮件地址和随机生成的密码字符串。

No. 9：哥斯达黎加政府数据泄露

在一次备受瞩目的网络攻击中，Conti 勒索软件团伙入侵了哥斯达黎加政府系统，窃取了具有极高价值的数据，并索要 2000 万美元，迫使中美洲政府宣布进入紧急状态。数周后，共有 670GB 的数据（占访问数据的 90%）被发布到泄漏站点。

No. 8：Neopets 数据泄露

今年 7 月，一个包含 Neopets（游戏网站）6900 万用户账户信息的数据库遭公开发售。数据库可用信息包括姓名、电子邮件地址、邮政编码、性别和出生日期等。一项调查显示，攻击者在 2021 年 1 月 3 日—2022 年 7 月 19 日共 18 个月期间，曾多次访问了 Neopets 的 IT 系统。

No. 7：Twitter 数据泄露

年中，Twitter 网站上 540 万个账户的电话号码和电子邮件地址遭泄露。多份报道称，这些数据是在 2021 年 12 月通过漏洞赏金计划中披露的 Twitter API 漏洞收集的，该漏洞允许人们将电话号码和电子邮件地址提交到 API 中检索相关的 Twitter ID。使用这些 ID，黑客得以检索有关账户的公共信息，以创建包含私人和公共信息的用户记录。

No. 6：学习通用户数据疑似被公开售卖

有报道称，大学生学习软件超星学习通的用户信息遭到泄漏被公开售卖，其中泄漏的相关信息高达 1 亿 7273 条。

不少大学生纷纷反映自己的“超星学习通”学习账号疑似被别人使用，账户查看次数大幅增加。此外，不少学生反映，近期接到的诈骗电话可以准确地报出自己的姓名，身份证号及支付宝的相关信息。

不过学习通方面否认了相关数据泄露事件。相关负责人回应，到目前为止还未发现明确的用户信息泄露证据，鉴于事情重大，已经向公安机关报案。

No.5：Twilio 数据泄露

美国通讯巨头 Twilio 今年 8 月证实，网络犯罪分子在一次网络钓鱼攻击后访问了 125 名客户的数据。攻击者伪装成 IT 部门的工作人员，诱骗公司员工交出登录凭证。现任和前任员工最近报告说，他们曾收到自称是来自 IT 部门的短信，称员工的密码已经过期、日程已更改，要求员工登录被攻击者控制的 URL。

Twilio 称，其他公司也曾遭受过类似的攻击，并对如何应对威胁行为者进行了协调，包括与运营商合作停止恶意消息的发送，与注册商和托管提供商合作关闭恶意 URL。

在 27 万余总客户群中的 209 名客户、7500 万总用户中的 93 名 Authy 最终用户的账户受到了此次事件的影响。Twilio 还表示，没有证据表明恶意行为者访问了 Twilio 客户的控制台账户凭据、身份验证令牌或 API 密钥。

No. 4：DoorDash 数据泄露

今年 8 月，外卖巨头 DoorDash 证实其 490 万客户、员工和商家的个人信息遭到泄露。DoorDash 表示，攻击者访问了 DoorDash 客户的姓名、电子邮件地址、送货地址和电话号码。黑客还获取了“一小部分”用户的支付卡信息（包括银行卡类型和卡号后四位数字）。

No. 3：Optus 数据泄露

今年 9 月，拥有 970 万用户的澳大利亚电信公司 Optus 遭遇大规模数据泄露，涉及用户姓名、出生日期、电话号码和电子邮件地址等信息。还有一群客户的实际地址和个人身份信息（如驾驶执照和护照号码）可能已泄露。多份报道称，是由国家支持的黑客或犯罪组织突破了该公司的防火墙，获取了敏感信息。

No. 2：LAUSD 数据泄露

由于美国第二大学区——洛杉矶联合学区 (LAUSD) 未能在 10 月 4 日之前支付赎金，俄语黑客组织 Vice Society 泄露了该学区的 500GB 信息。这些数据包含护

照详细信息、社会安全号码和纳税表格、联系方式、法律文件、包含银行账户信息的财务报告、健康信息、定罪报告和学生的心理评估等个人身份信息。

No. 1：Medibank 数据泄露

澳大利亚最大的健康保险提供商之一 Medibank Private 证实，970 万新老客户（包括 180 万名国际客户）的数据已被未经授权访问。但 Medibank 称不会支付赎金，并表示：“我们认为，通过支付赎金来确保黑客归还、并防止其公布客户数据的可能性非常有限。”

从上述发生的事件来看，造成数据泄露的原因多种多样，主要包括勒索软件攻击、钓鱼邮件及不正确的安全配置等外部和内部因素。

据 Verizon 发布的《2022 年数据泄露调查报告》（DBIR）显示，目前有四个主要途径会威胁到数据资产：凭证窃取、网络钓鱼、漏洞利用和僵尸网络。其中，82% 的违规事件涉及人为因素。无论是凭证丢失、网络钓鱼、误用等简单的错误，人在安全事件和数据漏洞事件中始终扮演着非常重要的角色。

在所有导致数据泄露的入侵行为中，62% 的系统入侵事件是由供应链造成的。与此同时，勒索软件继续保持上升趋势，同比增加了近 13%。这一增长幅度相当于过去五年的总和。

那么，从防守方角度来看，当前数据安全防护面临的四大难题：一是数据资产梳理不清，被盗窃 100M 的数据和被盗窃 1 个 T 的数据概率相同，防线一旦被突破将导致“一失万无”；二是特权账号管理不严，管理员、技术员、操作员三员”安全隐患大；三是 API 接口管控不当，一点被突破，容易造成安全防线全面溃败；四是风险感知不全面，如遇到“蚂蚁搬家式”的盗窃手法，很难及时告警。

数据安全治理三步走战略

基于奇安信今年来数据安全建设的实践，奇安信提出了数据安全系统治理的三步走战略，盘清资产、精准防护、全局管控。

第一步，盘清资产。系统梳理业务系统、应用、数据等，并形成数据资产梳理报告。

第二步，精准防护。一方面，要做好特权账号管理，做到能审查、能告警、能拦截；另一方面，要做好 API 管理，可通过 API 安全卫士及时发现 API 异常行为，提防外部攻击。

第三步，全局管控。以“零信任”策略为核心，实现“权限最小化”，降低被攻击的风险；通过数据安全态势感知，对各类安全日志进行研判，快速响应处置。

2022 关键词

“勒索攻击”

国家进入紧急状态、巨量数据泄露、暗网交易猖獗，一切都拜勒索攻击所赐

2022 年一系列严重网络安全事件背后都离不开勒索犯罪集团的操作。2022 年勒索犯罪集团的活跃度达到国家勒索的新高度，LockBit、Conti 和 Lapsus$ 三大勒索犯罪集团空前活跃，政府、医疗、制造业、金融业等行业饱受勒索软件困扰。

2022 年勒索攻击四大特点：

特点 1. 进入“国家勒索时代”的勒索攻击日益政治化

勒索软件不仅是网络犯罪分子的工具，而且是具有潜在影响力的政治工具，这意味着越来越难以区分，攻击是处于经济动机还是政治动机。

2022 年哥斯达黎加总统罗德里戈 · 查韦斯 · 罗伯斯在就职当日（5 月 8 日）签署了紧急状态法令，宣布哥斯达黎加遭受网络犯罪和网络恐怖分子的侵扰，国家进入“网络安全紧急状态”。 根据报道，从 4 月中旬到 5 月初，27 个政府机构成为第一波攻击活动的目标；5 月底的第二波攻击又使哥斯达黎加的医疗保健系统陷入了漩涡。作为应对，哥斯达黎加总统向勒索软件攻击背后的负责人“宣战”：“我们处于战争状态，这并不夸张。这是一场针对国际恐怖组织的战争。这可能是迄今为止最严重的勒索软件事件。”在勒索软件侵扰下，该国国际贸易陷入停顿状态；超过 3 万次医疗预约被迫重新安排；税务服务也被迫中断。数以百万计的哥斯达黎加人因勒索攻击而损失惨重，受影响机构的工作人员只能转用纸笔来完成工作。

此次勒索攻击狂潮的核心力量是与俄罗斯有关的勒索犯罪集团 Conti。在 Conti 的 1000 多次勒索软件攻击中，针对哥斯达黎加的攻击尤为突出。这种针对哥斯达黎加整个国家的勒索攻击，意味着进入“国家勒索” 的新勒索软件时代，它完全不同于过去针对政府机构的勒索攻击——大多是针对地方市政机构的战术攻击，而不是针对关键政府服务的广泛攻击。

对黑山和阿尔巴尼亚的高度破坏性勒索软件攻击同样具有高度的政治动机。在阿尔巴尼亚，伊朗国家附属团体从 2022 年 7 月开始对该国政府系统实施了一系列破坏性、报复性攻击，被归因于伊朗情报和安全部 (MOIS)。2022 年 8 月导致黑山的政府系统和国家服务关闭的勒索软件攻击，几乎可以肯定也是出于政治原因。

特点 2. 勒索软件即服务（RaaS）渐成主流

回顾今年的勒索软件形势和重大事件，我们发现，勒索即服务（RaaS）愈加成熟，旧的恶意软件变体回归，新的变体不断发展，漏洞愈发武器化，网络勒索生态逐渐工业化。在过去的几年里，勒索软件成为网络罪犯最流行的工具之一。网络勒索犯罪集团的工具包在不断升级，以使数据泄露的过程更快、更轻松。

勒索软件即服务作为一种新兴的商业模式，允许任何几乎没有技术专长的人就可以发动对特定目标的勒索软件攻击，所需要的仅仅是注册 RaaS 平台，并支付相应的服务费用（通常是所收取赎金的一定比例）。

LockBit 团伙是 2022 年全球最猖獗的勒索犯罪集团。LockBit 也被称为 Bitwise Spider，起源于俄罗斯，遵循 RaaS 运营模式，赎金由 LockBit 开发人员团队和发起攻击的会员分配，后者最多可获得 3/4 的赎金，且后期主要采用“双重勒索”策略（文件加密 + 数据披露）来敲诈受害者。LockBit 目前攻击的受害者数量已高达一千多个，约为著名勒索团伙 Revil 的 5 倍，Conti 的 2 倍。此外，网络安全供应商 Digital Shadows 的报告显示，在 2022 年第二季度勒索软件攻击事件中，LockBit 占到了 33%。2022 年 6 月，Unit 42 发布报告称，截至 5 月份，LockBit 占据了 2022 年勒索软件相关攻击事件中的 46%，导致全球 850 多家组织沦为受害者，可见其威胁之大。

特点 3. 勒索软件新技术趋势：跨平台快速加密

越来越多跨平台勒索软件，适应性提高。为了造成尽可能多的损害并提高恢复难度，勒索组织会加密更多的系统，这意味着其勒索软件需要在不同的架构和操作系统中运行。应对方法是用“跨平台编程语言”（如 Rust 或 Go）编写勒索软件，使用跨平台语言还方便将勒索软件移植到其他平台。此外，对分析人员来说，破解跨平台二进制文件比破解普通 C 语言编写的恶意软件更困难。

勒索攻击者正在大量应用间歇性加密来快速加密受害者的文件，这也是 2022 年勒索软件的一个重大的特点。

2022 年度重大勒索事件

	勒索对象	时间	勒索赎金	攻击者
1	哥斯达黎加政府	2022 年 4 月起	2000 万美元	Conti
2	法国巴黎 CHSF 医院	2022 年 8 月	1000 万美元	LockBit3.0
3	黑山政府部门和国家议会	2022 年 9 月	1000 万美元	Cuba
4	律师事务所 Ward Hadaway	2022 年 3 月	价值 600 万美元的比特币	Hacker
5	奥地利卡林西亚州政府	2022 年 5 月	价值 500 万美元的比特币	Black Cat（也被称为 ALPHV）
6	意大利铁路公司 Trenitalia	2022 年 3 月	价值 500 万美元的比特币	Hive
7	美国麦岭市公共市政系统	2022 年 8 月	500 万美元	Black Cat
8	意大利比萨大学	2022 年 6 月	500 万美元	Black Cat
9	罗马尼亚石油公司 Rompetrol	2022 年 3 月	200 万美元	Hive
10	法国服装公司 Damart	2022 年 9 月	200 万美元	Hive
11	美国蒂夫特地区医疗中心	2022 年 7 月	115 万美元	Hive
12	澳洲电信运营商 Optus	2022 年 9 月	价值 100 万美元的加密货币	Hacker
13	美国格伦县教育办公室	2022 年 5 月	100 万美元	Quantum
14	半导体芯片公司英伟达	2022 年 2 月底	100 万美元	Lapsus$

从两方面来看，间歇性加密对勒索软件运营者来说是非常重要的：速度——完全加密是非常耗时的，而时间对攻击者来说是非常重要的，加密速度越快就越能防止被检测与拦截；逃避——防御者可以使用统计分析来检测勒索软件的加密操作，通过评估文件 IO 操作强度或文件修改的相似性可以进行检测。与完全加密相比，间歇加密可以有效规避此类分析。LockFile 勒索软件是首批引入间歇性加密技术的勒索软件家族之一。后来，越来越多的勒索软件都应用了这一技术。

特点 4. 关基设施仍是勒索重点攻击目标

2022 年第三季度，包括能源、医疗保健和制造业在内的关键行业成为勒索软件的高度攻击目标。

2022 年 8 月，我国知名的财务软件公司用友畅捷通 T+ 软件客户遭受勒索病毒攻击，同时广联达、金蝶、管家婆、致远等软件公司用户也被勒索病毒攻击。经确认，来自该勒索病毒的攻击案例已超 2000 余例，且数量仍在不断上涨。此外，我国某知名家电巨头也被传出遭遇勒索攻击。

通过对公开报道的 LockBit 重大勒索事件统计也可以反映出其攻击重点。LockBit 组织的攻击尤其青睐软件和信息技术、制造、政府、网络安全、国防等关键行业。

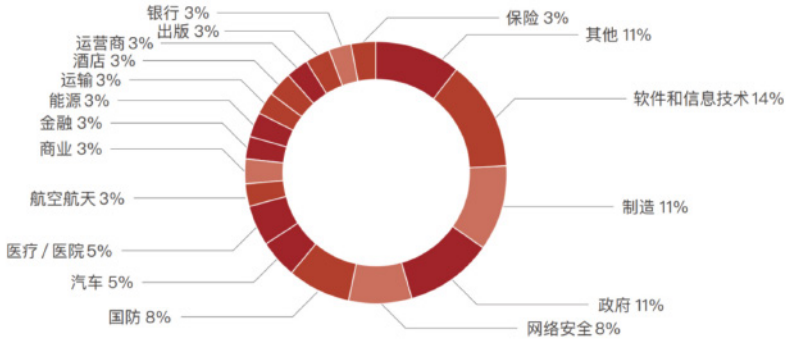
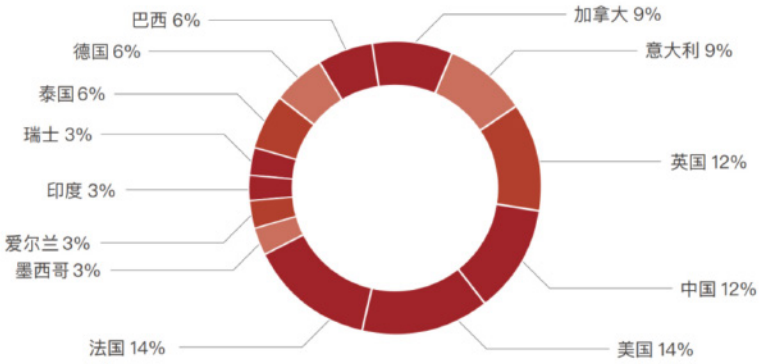


图 2 LockBit 勒索软件攻击的行业分布图

目前，LockBit 勒索软件攻击范围遍及北美、欧洲和亚太地区，似乎并无国界之分。其中，美国、法国、英国、中国等国家为重灾区。



总结

勒索攻击走进新时代，网络罪犯变得越来越专业，也越来越肆无忌惮。其传播方式、攻击目标将突破传统局限性，向多元化、低门槛、广分发等方向传播。

在勒索病毒威胁面前，没有人能够置身事外。与常规战争不同，这场反勒索国际战争没有尽头，应对无国界的网络勒索攻击，需要各国更多的合作和团结一致，加大对网络安全的投入，提高其网络安全弹性，分配更多资源来应对攻击。

此外，面对不断升级的新型攻击技术和勒索方式，传统安全手段已无法有效抵御勒索软件攻击。奇安信安全专家建议政企机构重视常态化安全运营、打造体系化与细粒度的安全防护，加强溯源能力，同时升勒索攻击发生后的快速响应、处置能力，以有效应对勒索攻击的威胁。

2022 关键词

企业篇

5个故事，50人，

致敬不平凡的2022

这一年，奇安信集团的领头人齐向东，作为优秀企业家代表，成功当选了全国工商联副主席，抒写着网安人的荣耀和传奇；这一年，10000+ 奇安信人在顺境中御风而行、乘风破浪，在逆境中迎难而上、奋勇前行，创造了北京冬奥“零事故”的世界纪录，驶入了国际化的万亿蓝海。

站在年终岁末，我们写下5个故事，致敬这不平凡的2022。

2022 关键词

“新战略”

故事 1：实现销售驱动向技术驱动转变，22 个亿元军团由他们组成

“又是一个亿元大单！而且还是海外某国家首都城市网络安全指挥中心建设项目，这是奇安信军团战略落实以来，又一次重大突破！”作为军团总负责人，奇安信集团总裁吴云坤显然对 2022 年军团模式的连战连捷，颇为自信。

在吴云坤看来，2022 年，是奇安信集团实施高质量发展战略的关键一年。从年初成立军团委，面向 22 个重点领域和重点行业组建了 22 个军团，以小切口带动大突破，并构建满足客户复杂需求的一体化生产管理组织，深耕重点领域，由此拉开了营销体系变革的序幕，吹响了加速高质量发展的号角。

图：奇安信集团总裁吴云坤参加 2022 世界互联网大会发表演讲

“效果是显著的，2022 年我们拿下了多个亿元大单，这在以往是难以想象的。尤其是在 2000 万美元的海外项目中，我们集中了最优秀的销售专家、规划设计专家、产品专家和平台专家克服疫情影响，一起出差到客户本地，确保了项目顺利进行，赢得了客户认可。这就是军团模式的优势体现。”

何为军团模式？吴云坤认为，军团的本质是围绕关基领域的重点行业和重点客户，深挖客户的个性需求，从规划网络安全体系建设入手，利用公司冬奥“零事故”的经验优势，打通销售、产品、研发、服务等内部多环节，合理高效地调配资源，同时充分利用研发平台量产的优势，为客户提供全面的、具有攻防能力的个性化网络安全产品和服务，更好地解决客户的痛点和难点，深受行业客户认可。

从供给侧看，军团模式提升了公司满足数字化时代客户对网络安全需求的综合能力。

随着数字化转型的深入，客户对复杂业务场景的安全需求越来越高，之前的标准化的产品和服务已无法满足需求。奇安信充分汲取冬奥项目的“零事故”成功经验，尤其对冬奥这种军团作战模式进行打法升华、复制推广，最终面向 22 个重点行业组建了 22 个军团，大大提升了满足这些行业网络安全需求的综合能力，22 个军团 500 万以上大项目订单数量比 2021 年同期增长了 103%。

从需求侧看，军团模式引导客户从合规导向的标品购买，走向结果导向的体系建设运行。

军团从之前的销售驱动模式向技术驱动型模式转变，通过主动把握和引导客户需求，为客户提供定制方案，帮助客户在体系化建设的同时建立实战化运行体系，使得整个安全系统有效运行起来，发挥应有的价值。比如，抓住客户攻防演习和二十大重保需求，将冬奥保障方案定制形成“小冬奥重保方案”，在 2022 年的攻防演习和二十大重保中，有超过 200 家关基客户选择了奇安信的“小冬奥重保方案”，确保了这些客户圆满完成了演习和保障任务。

吴云坤认为，军团模式不仅极大提升了公司对大型客户的项目实施能力，支撑了公司高质量发展目标的实现，更重要的价值是形成了从客户视角看问题，为公司营销体系变革探索了路径，积累了经验。可以说，军团委全体战士在宏观环境和诸多客观因素影响的同时，为公司乃至整个行业发展模式变革都做出了有益的创新和探索。

对于 ICT 行业而言，军团模式并不是新鲜事物，谷歌、华为和中国联通都已经进行了成功实践，但在网络安全领域奇安信是第一个“吃螃蟹者”。奇安信基于北京冬奥会保障中的军团作战模式和经验基础上，充分吸收和借鉴了谷歌、华为在信息化领域的成功经验，从而形成了满足新时期客户需求的具备网络安全行业特色的奇安信军团模式，为长期落后于信息化发展、“小零同”问题（小规模、零散化、同质化）严重的网络安全行业，探索了一条新发展路径。

陈静

2022 年回顾

2022 年，我很庆幸能成为军团的一员，与军团的战士们并肩奋战、踔厉前行，见证了军团的成长，并带领运营管理部为军团模式高效运行保驾护航。

2023 年展望

2023 年，是挑战和机会并存的一年，我希望基于军团模式运行经验支撑 CBG 组织变革，取得更好成绩，助力公司业绩增长。

2022 年回顾

2022 年，我最有成就感的一件事是带领小团队，超额完成年度任务。团队所销售超额完成业绩，为整体部门的任务达成添砖加瓦。

2023 年展望

2023 年，我立下的小目标是继续超额完成团队指标，人均奖金争取双倍，同时力争 2023 年的金砖。

张晓明

李彪

2022 年回顾

2022 年，有幸加入运营商三大军团，见证了军团业绩在这一年高速增长，完成了几乎不可能完成的任务！印象最深刻的是，入职不到一周时间，受命协调组织并参与了公司顶级的高层技术交流会议，奠定了奇安信在客户心中的核心地位！

2023 年展望

2023 年，希望军团迈向新的高度，个人能够在其中发挥更大的价值，实现新的突破；在军团委及军团长的带领下开启新篇章，书写辉煌！

2022 年回顾

2022 年，我最有成就感的一件事是进入军团，并带领所在军团一起完成了全年财务毛利。
2022 年，最让我印象深刻的一件事是当在大屏幕上展示全年 1.41 亿财务毛利任务的时候。

2023 年展望

2023 年，我立下的小目标是和我的小伙伴们一起把所在军团做成公司的大而强行业部，团队的每个小伙伴在新的挑战中都能独当一面。

穆阳阳

赵娜

2022 年回顾

2022 年，最让我印象深刻的一件事是军团改革，这给我们每个人都带来了机会，同时也带来诸多挑战，在疫情之下竭尽全力完成 100% 任务增长的目标，我深切地体会到一点：要发展，所有人必须跟上脚步！

2023 年展望

2023 年，我希望所在军团能取得从 0 到 1 的突破，创造可持续的盈利模式。践行军团改革思想和原则，打造一支有战斗力的团队，为客户创造价值、为公司创造效益、为行业创造商机，在行业网络安全业务上保持领先地位。

2022 年回顾

2022 年，最有成就感的事情是克服疫情不利影响，带领团队精诚合作，全面完成业绩指标，为明年实现进一步跨越打下坚实基础。

2023 年展望

2023 年，希望在公司管理层的指导支持下，能够为公司做出更多贡献，实现企业价值和个人价值的有机统一。

廖雪琳

徐世枫

2022 年回顾

2022 年，我最有成就感的一件事是能代表军团项目交付部出差海外，顺利完成海外某国家 SD 项目前期集成规划工作。

2023 年展望

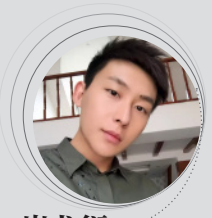
2023 年，我希望在顺利交付海外某国家项目的同时，让国际客户感受到我们集团在网络安全建设方面强大的集成能力。

2022 年回顾

2022 年，感恩集团信任可以让我成为军团的成员，作为军团组建的第一年，压力与挑战并存。在这一年的时光，身边有努力奋斗的队友，有肝胆相照的兄弟，有与“敌人”血战到底的气概，更有完成组织上任务的决心。

2023 年展望

2023 年，疫情收尾，一切规划步入正轨，希望军团模式组织的变革，带来更大的成功与突破。听集团指挥，坚决敢打敢拼的工作作风，打胜仗超额完成任务！



崔戈衍

李东

2022 年回顾

2022 年印象最深刻的事情是客户遭遇勒索，得到消息的第一时间，公司组织了应急人员支持，帮助客户度过难关，证明了公司的能力！客户给奇安信的评价对我印象深刻：“奇安信改变了我对于安全的认知。”很高兴公司能得到客户的高度认可。

2023 年展望

2023 年，我希望在新的一年能够创造更好的成绩，不只是完成目标业绩，而是以更高的要求激励自己。为公司明年更高的目标付出自己的努力。

2022 年回顾

2022 年最让我印象深刻的一件事是随军团的业务发展一起成长，军团 HR 团队在不断的进步，全年每天都是走得最晚的团队，并且和业务、运营管理团队协同配合，最艰难的时候大家一起共同度过！

2023 年展望

2023 年，我希望在新的工作上快速学习和适应，助力业务成功。

张嘉禾

2022 关键词

“新高度”

故事 2：奥运史上的“零事故”世界纪录，由他们创造

提到世界纪录，我们总能联想到赛场上运动健儿们的英姿。比如，创造了 9 秒 58 百米世界纪录的飞人博尔特；再如，28 次打破世界纪录的“撑杆跳女王”伊辛巴耶娃。世界纪录的背后，是“更快、更高、更强、更团结”的奥运精神。

图：奇安信年会迎接开创网络安全“零事故”奥运历史的冬奥将士凯旋

2022 年 3 月 13 日晚，北京冬残奥会落下帷幕，奇安信作为奥运史上首家网络安全官方赞助服务商，交上了北京冬奥会、冬残奥会网络安全保障“零事故”的答卷。3500 多位奇安信安全工程师，800 多天的日夜坚守，他们创造了奥运史上网络安全“零事故”的世界纪录。

“冬奥重保带给公司的最大收获是什么？我认为是在超高风险、超大难度、超强压力条件下，奇安信综合安全保障能力得到了全面实践和检验。”北京冬奥组委技术部高级专家、奇安信集团副总裁张翀斌表示。

超高风险！北京冬奥会面临前所未有的网络攻击威胁。里约奥运会、平昌冬奥会、东京奥运会等历届重大赛事，都发生过网络攻击造成直播故障或数据泄露的情况，而对于万众瞩目的北京冬奥会，一旦攻击得逞，其后果不堪设想。

从冬奥会开始到冬残奥会结束，奇安信累计监测到各类网络攻击超 3.8 亿次（含社会面），发现上千个攻击

者组织、数万起 APT 组织活动事件……尤其是开幕式、闭幕式和重要赛事期间，攻击频次更密、强度更烈。在这样严峻复杂的网络风险中，奇安信人经受住了最严苛的考验。

超大难度！安全保障面对前所未有的复杂度和挑战阻力。跨越百余公里的 3 个赛区、38 个场馆，近百个国家、数千名运动员的交流沟通、场馆协作、需要依赖大量先进的技术。开放式 5G 网络、云计算、物联网、人工智能等技术，200 多项科技应用，使奥运网络系统空前复杂，因此牵涉到的责任相关方非常多，关心问题千差万别。

“赛前会遇到这种情况，别人质疑我们方案，比如要求部分产品异构，即必须引入国外安全设备，尤其是临近比赛前要完成。这需要我们一方面给他们树立信心，更重要的是找到质疑方的担心点，通过技术和管理方案去解决，如借助更多资源、备份机制、应急预案等，办法总比困难多。”

张翀斌特别提到，超大难度还体现在敢于对自己动刀子。“打铁还需自身硬，为了确保万无一失，我们要求所有参与冬奥项目的产品部门，都要用最高标准来挖掘自身漏洞。这是很艰巨的任务，但实践证明，这是‘零事故’的必要保障。”

超强压力！我们作出前所未有的“零事故”承诺。作为奥运史上首家网络安全赞助商，奇安信对冬奥做出了网络安全“零事故”的承诺，承担“完全的、彻底的、端到端”的责任，即“托底责任”。

承诺就是责任，责任就是压力，对于冬奥重保的总带头人张翀斌来说，这是无数个不眠之夜。“假设是一定会丢失某些点，用多长时间发现，多长时间恢复业务，多长时间处置堵漏完毕，越到赛前越是睡不好觉，反复的实战演练和沙盘推演，包括和不同的攻击队进行面对面对弈，发现问题就最快速度解决。”

“技术方案没有经过实践和检验都是空中楼阁；服务是人提供的，背后隐藏着人员能力培养、流程设计、团队组织、指挥调度等多方面工作，如此大规模的保障凸显了作为一家公司的综合作战能力，更为整个行业带来了信心：以‘中国模式’‘中国框架’‘中国服务’‘中国产品’组成的网络安全‘中国方案’，被验证是成功的！”张翀斌如此总结冬奥带给行业的巨大价值。

“实践证明，我们的冬奥网络安保系统经受住了‘实际网络战’的检验。”齐向东表示。整个 2022 年，奇安信陆续展开了数百场冬奥经验交流会，包含金融、通信、水利、电力、医疗等众多重点关基行业，推广冬奥成功经验，众多单位已开始利用冬奥“零事故”的中国方案，完善网络安全建设，向“网络强国”目标迈进。

顾鑫

2022 年回顾

2022 年，最让我印象深刻的一件事：山区、郊区场馆的住宿条件真是太差了，有的地方住的是临时工棚，住宿房间与公共卫生间相邻，散发着难闻的气味，房间温度也无法保障，在屋子里不脱衣服再裹上棉被才能睡着；就是在这样的条件下，奇安信的战友们没有一句怨言，没有一个人因为条件艰苦申请换岗，都义无反顾的坚守在工作岗位，用自己的坚韧和信念完成值守任务。能和这样的一群战友共事，让我倍感荣耀！

2023 年展望

聚是一团火，散是满天星。2023 年，我希望播撒在奇安信各个角落的奥运战士们无论在什么岗位都能发出耀眼的光芒，我们共同用这绚烂光芒，照亮用户的零事故之路！

吴江波

2022 年回顾

2022 年，我最有成就感的一件事是在冬奥网络安全保障工作上，带领奇安信 ZVL 保障团队顺利完成对场馆的网络安全保障工作，为冬奥成功举办贡献了自己的一份力量。

2023 年展望

2023 年，我希望在公司售后技术支持的岗位上，能够继续带领云安全团队做好公司云安全产品的售后技术支持保障工作，完成团队的工作目标。

2022 年回顾

2022 年，我最有成就感的事是实现了北京冬奥网络安全“零事故”。2022 年 3 月 13 日晚上央视闭幕式直播结束的时候，心情感到无比的轻松。

2023 年展望

2023 年我希望在北京冬奥会验证过的网络安全运行方案，能够在更多的单位得到验证并逐渐完善成熟。

尹智清

刘敬群

2022 年回顾

2022 年，印象最深的事情是冬奥结束后，韩主席代表奥组委表达对奇安信的感谢，那一刻无比激动、自豪！

2023 年展望

2023 年，希望公司真正把奥运的沉淀应用于流程及组织变革中，斩获更多市场份额、实现更多客户的“零事故”。

2022 年回顾

2022 年，最让我印象深刻的一件事是冬奥会开幕式当晚，在冬奥技术运行中心值守，虽未亲临鸟巢现场，但通过技术运行中心的大屏看到开幕式表演依然激动万分。

2023 年展望

2023 年，我希望疫情结束，公司业绩大涨，冬奥经验能孵化出更多服务和产品，为更多的用户提供“零事故”的网络安全保障。

仝磊

曾庆

2022 年回顾

2022 年是冬奥项目大考的关键年。期待着冬奥如期、安全的举行；期待着艰苦的三年冬奥项目圆满划上句号；也伤感项目结束后的分离，感谢这段经历，挑战、成长，一段很有温度的其妙旅程。

2023 年展望

2023 年希望冬奥那份激情依旧：工作上能够持续践行结硬寨、打呆仗的冬奥项目精神；生活上能够持续保持乐观、向上的冬奥精神。

2022 年回顾

2022 年，我最有成就感的一件事是在冬奥会开幕式前 1 小时，实时监控大屏上突然出现的大量告警信息，带领团队有序进行分析、快速进行定位、及时进行确认，直至开幕式结束，创造了待处理告警为 0 的佳绩。

2023 年展望

2023 年，我希望在新的一年中，能够发扬冬奥精神，高效做好安全运行标准化的孵化，做到从 0 到 1 的创新，实现从 1 到 100 的复制推广。

徐春雨

王莎莎

2022 年回顾

2022 年，我最有成就感的一件事是成为奇安信坚守在冬奥现场的一名一线战士，回顾整个冬奥会 804 天的建设和保障经历，带给我莫大的行业使命感与自豪感！

2023 年展望

2023 年，希望在公司的布局和带领下，继续向我们的客户传递北京冬奥网络安全保障的成功经验，传承冬奥网络安全“零事故”的精神，继续守卫各行各业的网络安全。

李松鹤

2022 年回顾

2022 年悄然而过，奋战在冬奥安全防线的时光恍如昨日，正是冬奥的洗礼使我以百倍信心迎接着一个又一个挑战。

2023 年展望

在 2023 年，愿以昨日的奋斗作为今日的起点、持续进化，以冬奥标准的安全运行能力为更多客户实现价值。

杨召军

2022 年回顾

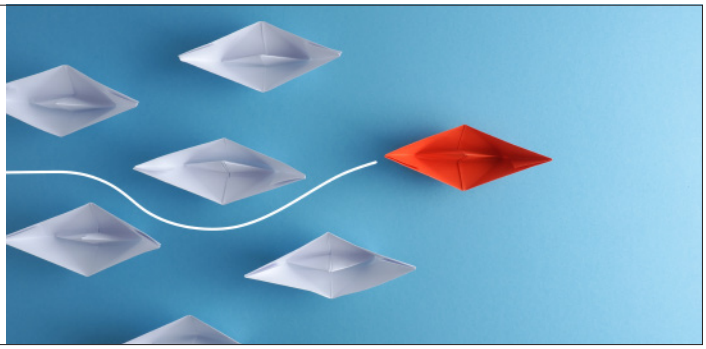
最让我难忘的是成功说服冬奥组委技术部、市场开发部、财务部，大幅采购公司网络安全产品与服务，保障了公司冬奥赞助权益。

2023 年展望

把冬奥营销模式推广复制到保密军团，通过解决方案营销模式，拉通销售、售前、交付、产线、运营团队，为客户、公司创造更大价值。

2022 关键词

“新蓝海”



故事 3：开辟万亿国际化新蓝海，由他们启航

以“让网络更安全，让世界更美好”为使命，以“成为全球第一的网络安全公司”为愿景，在官网、展会活动等无数场合，总能看到奇安信的企业使命与愿景。加快国际化，为世界各国客户提供先进的网络安全产品与服务，成为公司的重要战略之一。

据 IDC 预测，2025 年全球网络安全产业规模将达到 2114 亿美元，折合人民币超 13000 亿。而同期，中国网络安全总体市场规模将超 214 亿美元，约为全球的 1/10。因此，要成为“全球第一”，拓展万亿规模的海外市场，无疑是必经之路。

对于刚当选全国工商联副主席的奇安信集团董事长齐向东来说，身为中国 ICT 行业和民营经济发展的见证者、亲历者、推动者，肩负着“弘扬企业家精神、加快建设世界一流企业”的政治责任感和使命感，需要充分发挥网安龙头企业的标杆带头作用，率先“出海”开疆扩土，履行企业使命和责任。

从社会责任到家国情怀，从带领行业开拓蓝海到寻找企业增长的第二曲线，奇安信从 2019 年开始就将国际化列为公司重要战略。在短短 4 年内，国际化接连奏凯，捷报频传，尤其是 2022 年，奇安信的海外新签订单相比去年同比增长 100%，其中不乏过亿大单。

不过，在国际化业务负责人何瑞看来，订单与成绩只是表象，从更深层次来看，国际化的收获还远不止于此。

第一份收获是通过与国际巨头同台竞技，打出了中国网络安全公司的口碑。

图：国际化团队出征海外某国网络安全大型项目

国际市场是一个强手如林的大舞台，奇安信要取得一席之地，就必须有能与美国、俄罗斯、以色列等国际巨头公司相媲美的产品技术。经过数年短兵相接，奇安信领先的产品技术、集成、交付和服务能力，已获得充分验证。例如，在总额达 1.45 亿的海外某国家首都城市网络安全指挥中心建设项目中，奇安信在与 23 家国际大厂的技术 PK 中最终胜出，一举中标。在亿级总额的海外某国家 Tbps 级超大网络流量威胁检测项目中，奇安历经 11 个月的努力，顺利完成项目交付，赢得客户认可。

第二份收获是充分发挥头雁效应，为中国同行出海树立了标杆典范。

2021 年，奇安信当选北京市第一批“隐形冠军”企业。在 CCIA 发布的“中国网安产业竞争力 50 强”榜单中，奇安信连续 2 年蝉联第一。作为行业龙头企业，奇安信在国际化方面，也在积极发挥“头雁效应”，率先探索和开拓新市场，向世界一流企业迈进。从 2020 年开拓印尼等东南亚市场，到 2021 年深入参与阿尔及利亚、安哥拉、埃塞俄比亚等国家关键基础设施部门、重要政府单位的网络安全建设，再到 2022 年逐渐参与到欧洲和大洋洲个别发达国家的网络安全建设项目中，奇安信为中国同行企业探索出了一条出海之路。

最后，也是最重要的收获，是凝聚和吸引了一批敢打敢冲的小伙伴，淬炼出一支能征惯战的国际化团队。

国际化团队出海征战的 3 年，恰恰是全球疫情蔓延的三年。他们从疫情之初就走出去，脚步一直没有停止，反复转战多个疫情最严重的国家地区，在三年中听令而行、逆行出征，克服困难、从未抱怨。最终，公司越来越多的业务线参与到国际化团队之中，他们用砥砺前行的担当冲破了重重荆棘，用精益求精的专业开疆拓土，书写了中国网络安全龙头企业的出海“传奇”。

黄沙百战穿金甲，不破楼兰终不还。国际化团队用无数个日日夜夜的奋斗，让公司朝着“成为全球第一的网络安全公司”的愿景目标迈近了一大步。

Ryan

2022 年回顾

与 23 家大厂 PK、6 轮商务竞价最终拿下海外某国项目。

团队共 12 人，其中 8 人感染新冠的情况下仍然扛着病痛完成测试任务获得客户高度评价。我为自己曾经与这样一些兄弟并肩战斗过深感荣幸。

2023 年展望

我们见证了奇安信是有能力和国外主流厂商同台竞技并取得胜利的。

希望在海外某国 SD 交付阶段，从项目管理工作角色出发，做好 SD 项目的交付管理工作。并以此项目为原点，深化和推进海外某国的全国网络安全市场的拓展，并辐射周边区域。

2022 年回顾

2022 年，我最有成就感的是一年之中 80% 的时间都在海外沉浸式工作。

2023 年展望

2023 年，我希望有越来越多的同事加入奇安信国际化的大军。

Leo Zhang

Neal Cui

2022 年回顾

最有成就感的一件事是公司第一个海外大型的集成项目顺利按照计划进行了交付，同时客户对我们的产品及服务充分认可，为项目的二期打下坚实的基础，可以支撑我们继续深化拓展形成新的商机。

2023 年展望

希望国际化的业务可以快速成长，在当前国际经济环境颓势的情况下，通过公司各部门的共同努力在国际市场中继续砥砺前行，画下属于公司特有的色彩，实现业绩持续增长，为公司成为全球第一的网络安全公司添砖加瓦。

2022 年回顾

最有成就感的一件事是在海外出差期间，快速将市场由之前单一的内政部客户，横向扩展到了皇家办公室、运营商、大型企业等多个客户。并且多个项目已进入测试阶段，为签单打下良好基础。

Jamila

2023 年展望

2023 年，随着疫情的开放，我相信国际市场必将快速发展，也希望有更多热爱国际事业的小伙伴加入国际部。

Mr. Cao

2022 年回顾

在中东某国项目交付结束后，客户为了表示感谢组织部门人员和我们员工一起旅游。中国人和阿拉伯人其乐融融，不仅仅是客户对我们产品人员的认可，也体现了中阿友谊生生不息。

2023 年展望

帮助公司再赚 0.5 个亿。

2022 年回顾

海外的第一个大项目，在无任何经验积累的情况下，顺利完成项目交付，期间完成了英文版项目，共 39 个文档共 50 万余字的文档整理。

Zhengping. Qin

2023 年展望

希望完成中东某国项目（一期）终验并收到回款，同时能签下项目二期；
希望国际部业务发展越来越好，在海外签更多的合同。

MR. Song

2022 年回顾

来到奇安信收获了新的机遇，信心在伙伴和领导的那句“加油，你可以的”获得新生。

2023 年展望

“不忘初心，莫问归期”，成长为伙伴中有力的帮手，去鼓舞他人，是我的期待。

2022 关键词

“新风口”

故事 4：迎接未来数据安全风口，由他们布局

“尽管今年整个行业面临着前所未有的挑战和压力，但我们依然克服了重重困难，预计可实现整个数据安全板块约 50% 的高速增长，预计主力数据安全产品可取得 100% 的增长。”奇安信集团副总裁、创新 BG 负责人孔德亮表示。

数字时代，风起云涌。数据作为核心生产要素，关乎个人、企业甚至国家安全，数据安全成为数字经济发展的底板工程。加上国家“十四五”规划和 2035 年远景目标纲要政策加码，《数据安全法》等法律法规落地，数据安全迎来了超级风口。

大风口就能带来大市场么？孔德亮认为，数据安全从热闹到热销，还有很长的路。“我们至少遇到两方面的压力，首先宏观层面，在数据安全上升到国家战略高度的情况下，作为‘网安一哥’，如何承担相应的国家

责任和社会责任；其次在落地实施层面，奇安信作为综合的网络安全厂商，面对数据安全的巨大市场，如何拿出相应的解决方案和资源匹配，满足客户对数据安全的多场景细分需求。”

整个 2022 年，孔德亮从年初挂帅数据安全负责人之后，就深刻意识到，要打好这场战役，既需要仰望星空、目光长远、掌控战略主动权，又需要脚踏实地、紧贴客户需求、低调务实。

在他看来，奇安信能在数据安全这个战场上抢占先机，快速确立领先优势，得益于三个方面。

首先在战略层面，集团决策果断、规划得当，兼顾了长远和眼前。

早在 2021 年，奇安信就将数据安全定位为集团战略，举全公司之力来进行全面布局。到 2022 年 3 月，奇安信结合中国广大企业在数据安全的薄弱现状，制定出了“三步走”的数据安全建设整体思路，分别是第一步先理后治，补短固底；第二步系统治理，体系规划；第三步有序建设，持续运营。

孔德亮认为，全行业 85% 以上的客户，都需要从第一步开始，最紧迫的任务是“补短板、防裸奔”，尤其是 2022 年多次曝出的信息泄露事件，如学习通等，充分表明了这一点。

其次是战术层面，通过快速组建数据安全专班，抢占了市场先机。

好的战略离不开强大的执行团队，集团在确立数据安全战略之后的第一件事，就是从战略规划中心等多个业务线抽调专家，形成数据安全专班，助力战略落地。

从结果来看，这个数据安全专班发挥了巨大作用。“从 4 月开始，江苏、上海、广东、北京、重庆……数据安全专班可以说是频繁出差，转战大江南北，和千行百业的客户，以及合作伙伴深入交流，为快速打开局面、拓宽市场立下了汗马功劳。”

最后是全集团高效协同，凸显规模效应和综合实力。

数据安全是一个复杂度高、极其专业的领域，单个产品和技术只能解决某个细分场景的需求。孔德亮认为，

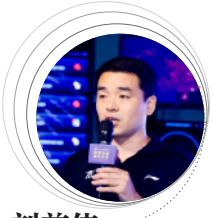
图：奇安信获中国信通院全部七大品类数据安全产品检验证书

奇安信的规模效应和综合实力，在数据安全领域体现得淋漓尽致，并发挥出 1+1+1>3 的效果。

例如，在政策合规、标准制定方面，奇安信积极与国家相关主管部门、监管机构深入合作，率先参与到数据安全法律法规、标准规范等工作。在咨询规划方面，依托集团战略规划研究院的优势，为客户提供全局治理的体系化建设思路，以及更具实操的完整方法和工具。同时，奇安信强大的产品、研发团队，显著加快了产品创新和迭代速度，使得奇安信具备业内最齐全的产品谱系和强大的竞争力。

天道酬勤，在 2022 年 7 月举行的“数据安全峰会 2022”上，奇安信旗下多款数据安全产品通过了中国信通院的七大品类测评认证，成为首家获得全套数据安全产品测评资质证书的网络安全企业，也是迄今为止数量最多、品类最全、覆盖最广的网络安全企业。

“目前数字经济浪潮尚在起步阶段，数据作为核心生产要素的战略价值刚刚凸显，数据安全的项目普遍周期长、复杂度高，急功近利是很难走到最后的。奇安信坚持不赚快钱、赚辛苦钱的长期战略，在这个数据安全新兴市场上，和客户共同成长。”孔德亮这样总结到。



刘前伟

2022 年回顾

2022 年数据安全专班齐心协力，一路披荆斩棘，从产品创新、解决方案、开拓市场、行业影响力等方面均取得不错的成绩，感谢齐总、吴总的指导、孔总和韩总的鞭策及集团其他领导的关心和支持。

2023 年展望

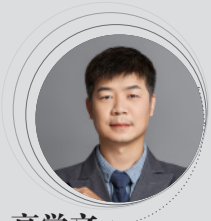
2023 年是数据安全高速发展年，希望更多优秀的同仁投身到数据安全领域，开疆拓土，勇创佳绩。

2022 年回顾

2022 年，在数据安全专班的领导下、兄弟团队的支撑下，数据安全发展进入了快车道。“蓬勃发展的数据安全事业，以及为此拼搏努力的同事”，每每想到此就令我激动不已。

2023 年展望

2023 年是数据安全发展的关键之年。希望在工作中积极践行公司倡导的价值观，与各位优秀的同仁一道，追求“让网络更安全，让世界更美好”的使命。



高学文

王子伟

2022 年回顾

回顾 2022 年，集团数据安全创新领域各项工作逐步走向标准化，越来越多的伙伴参与进来出谋划策，增砖添瓦。

2023 年展望

展望 2023 年，立足今年打下的坚实基础，数据安全必能攻城略地，遍地开花，为集团的市场影响力再填一块金字招牌。

2022 年回顾

2022 年最有成就感的是立足集团平台资源优势，在战推中心领导的带领下，在团队共同努力下，围绕国家政策及集团数据安全业务发展现状和需求，主动思考，多方沟通与谋划，形成了 2022 年助推集团数据安全业务发展专项行动计划，并取得多项优秀成绩，有效推动了数据安全业务的发展。

2023 年展望

2023 年希望继续充分发挥个人主观能动性，提高政策敏感性，提升产品和业务学习主动性，在工作岗位上继续发光发热。

单晓

任文浩

2022 年回顾

回顾 2022 年，支撑的各行业标杆项目的落地，完善了体系框架，沉淀了更多经验，这一年收获颇丰。

2023 年展望

展望 2023 年，面对更多的机遇，发挥经验优势，深度配合市场体系，集团数据安全业绩必将势如破竹。

2022 年回顾

2022 年，我很荣幸从事数据安全解决方案专项工作，实现多个行业数据安全方案的从 0 到 1，为公司数据安全取得佳绩尽最大努力。

2023 年展望

2023 年，结合公司流程变革中强调的“以客户为中心的一条龙服务”，作为众多“一条龙”中的一员，助力公司数据安全业绩更上一层楼。

朱赫

林永强

2022 年回顾

2022 年，我最有成就感的一件事是推出了 API 安全卫士产品，打造了一套持续闭环的 API 安全解决方案。

2023 年展望

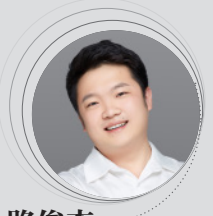
2023 年，我立下的小目标是继续完善 API 安全卫士产品，使更多行业及客户得到广泛的应用。

2022 年回顾

2022 年，我最有成就感的一件事是推出了数据跨境卫士产品，打造了数据出境安全整体的解决方案。

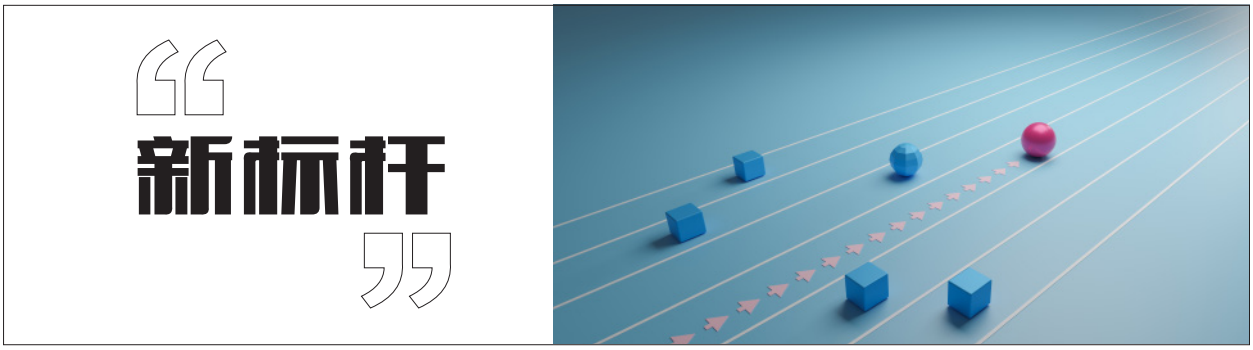
2023 年展望

2023 年，我立下的小目标是全面推广数据跨境卫士产品，使其在监管行业及被监管行业可以得到广泛应用。



路俊杰

2022 关键词



故事 5：标杆项目全国领跑，由他们发力

“2022 年对于区域发展中心是实践的一年、突破的一年、创新的一年。这一年最大的收获，不仅是网络安全‘中国模式’——城市安全运营‘虎安天枢’，企业安全运营中心在各地、各行业实践开花的一年，更是从实践中得到滋养反向补充、丰富、优化我们的运营框架、方法、策略、方案和效果的一年。”奇安信副总裁、区域发展中心负责人张龙这样总结自己的 2022。

“零事故”冬奥网络安全保障的实战经验、技术产品和模式，形成大量的冬奥遗产，对于推动我国网络空间安全保障能够发挥重要作用，更对探索适合中国国情的安全运营模式提供了宏观框架指导。

图：奇安信发布星城平台 2.0 引领城市网络安全运营中心建设

2022 年，区域发展中心传承冬奥经验，深化安全运营三大运营模式，即“城市安全运营”“综合安全运营”“托管安全运营”，为地方政府、大型企业、中小企业等不同类型不同规模的客户，建设体系化、实战化、常态化的网络安全运营体系。

在城市安全运营的落地方面，奇安信结合最新国家政策、数字政府建设指南等要求，梳理、整合、分析城市安全运营当今痛点和核心问题，并结合长沙安全运营成效，于 7 月 21 日正式发布了星城 – 城市网络安全运行平台 2.0（简称星城平台 2.0）。截至目前，星城平台 2.0 已在湖南、北京、广东、湖北、安徽、江苏等多省份得到落地，并得到广泛的应用和推广。

在企业综合安全运营业务方面，奇安信在终端运营服务能力架构方面实现了重大研究与突破。以能源行业为代表，在奇安信终端准入、防病毒、防泄密、桌管、监测、管理制度、运营流程等七方面构建了终端统一化运营能力体系，着力于解决客户资产不清晰、监测能力弱、管理制度不明等方面难题，为 10 万量级且多级管理机构在终端综合运营能力的建设上提供服务标准。

在安全托管业务方面，奇安信持续拓展新模式。为了深耕区域客户，开展了基于奇安信特色的区域运营中心；为了深耕行业客户，与广东电信、澳门天网、山东赛尔等战略合作伙伴开展了联合运营中心模式；为了更

好开展多样化的运营中心业务，奇安信组建安全托管服务教练团队，满足运营中心团队组织搭建、服务流程设计、服务人员培训等工作。

“以前我们经常有一种认知：‘经济不发达地区的客户不重视网络安全’，但这一年我们从南到北走了几十个三四线城市，我们可以看到，这些地方的客户非常清晰的认识到网络安全对于当地数字化经济的重要性。市场机会从来不缺，对我们考验的是对客户需求的洞察，安全运营工作就是要紧贴客户，从客户中来到客户中去，我们的业务才会具备持续的生命力。”

2022 年，奇安信安全运营托管服务屡获国内外研究机构认可，其中包括 Gartner、Forrester、IDC 等权威机构，这也从侧面证明，在安全运营这个赛道上，奇安信继续稳居行业领跑地位。

刘顺

2022 年回顾

2022 年，我最有成就感的一件事是所负责的长沙市城市网络安全运营中心入选“IDC 中国 20 大杰出安全项目”且被评为 IDC 2022 年亚太区智慧城市大奖（中国区）“灾难应对 / 应急管理”类别最佳智慧城市项目。参加省市两级公安与网信 4 次攻防演练均获得优秀防守单位。

2023 年展望

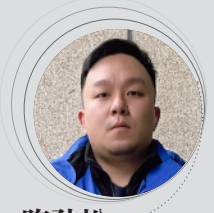
2023 年，我希望：长沙城市网络安全运营中心模式推向全国，实现网络空间安全的高效治理，为城市网络安全提供强有力保障。

2022 年回顾

2022 年，我最有成就感的一件事是经历了半年的出差，依托奇安信城市运营模式，在湖北宜昌合资公司，从团队组建到项目攻关，协助合资公司成功获得了宜昌市政务网络安全运营中心的授牌和相关项目，迈出了整体城市安全运营的第一步。

2023 年展望

2023 年，我希望奇安信城市运营中心模式能在全国遍地开花，构建奇安信的城市安全运营中心版图。



陈劲松

陈泉林

2022 年回顾

2022 年，我最有成就感的一件事是客户有安全运营需求，千里奔赴现场深挖客户运营痛点，对症下方。

2023 年展望

2023 年，我立下的小目标是多向前辈及同事请教经验，自己在工作中少走弯路，同时将自己的工作进行总结，让其他同事少走弯路。

胡心波

2022 年回顾

2022 年，我最有成就感的一件事是安全运营工作的设计得到了用户的认可，以点带面推动了全省安全项目的落地。

2023 年展望

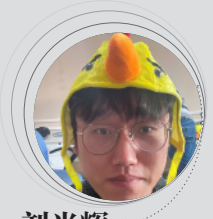
2023 年，我立下的小目标是推动安全运营专项工作，落实安全运营目标，树立行业标杆，成就客户、奇安信价值。

2022 年回顾

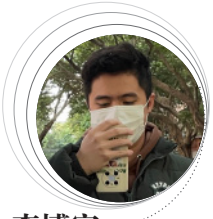
2022 年，我最有成就感的一件事是带领终端运营团队完成了光大银行天擎 V10 推广任务，在一整年 12 次投产保障中完美的完成测试验证以及投产保障工作，使产品达到客户满意效果。

2023 年展望

2023 年，我希望自己可以做好运营经理的工作，协助北区运营服务一组的小伙伴们做好项目工作，并提高每个人的产品和沟通管理能力，为部门增加优秀的一线人才。



刘光辉



李博宏

2022 年回顾

2022 年我最有成就感的一件事是与同事们一起战胜深信服，拿下了美的 MSS 服务订单，仿佛感受到少年时一起打 BOSS 的酣畅，得到胜利时的雀跃。

2023 年展望

2023 年，我希望拥抱变化，找到更多自驱力，继续发光发热，给公司、部门带来价值。

2022 年回顾

2022 年，我最有成就感的一件事是客户现场回访时，客户领导亲自迎接表达对安全托管服务的认可和对服务团队的感谢，那一刻我感觉“千淘万漉虽辛苦，吹尽狂沙始到金”。

2023 年展望

在 2023 年新的一年中，我希望能够让更多的用户都体会到服务的价值，在大家共同努力下，奇安信成为客户最信赖的安全运营服务提供商。

李佩霖

张佳瑶

2022 年回顾

2022 年，中国没有辜负世界的期望，办好了冬残奥会；我没有辜负公司的期望，完成了网络安全“零事故”保障使命。

2023 年展望

2023 年，我将继续摩拳擦掌作战于一线，将中国网络安全代表队的职业精神深耕于踏过的每一寸网络安全阵地。

结束语

回望 2022，奇安信是当之无愧的网安龙头：根据 IDC、赛迪等机构的数据，奇安信在终端安全、云安全、数据安全、态势感知、安全管理、安全服务（含咨询和托管）等多个领域，均保持市场第一的地位。在中国网络安全产业联盟 (CCIA)、安全牛等机构发布的网络安全企业排行榜中，奇安信已连续多年蝉联第一。

展望 2023，后疫情时代，国际环境仍将“风高浪急”，国内发展面临机遇挑战；数字经济或将加速暴发，改革转型必将日益深入……贯彻落实党的二十大精神，统筹发展和安全变得愈发重要。

展望 2023，可以预见，网络威胁、网络战争将进入无常与反常的黑客战国时代，网络安全基础保障成为社会发展的基本前提。

展望 2023，可以预见，网络安全、数据安全将进入合规与合需的双轮驱动时代，网络安全技术自主创新成为行业发展主流趋势。

展望 2023，可以预见，以奇安信等为代表的网络安全企业，既是命运共同体，也是责任共同体，必将践行“网络安全为人民”的使命，以“看得见威胁”“打得赢攻击”为标准，全方位提升安全能力，为建设社会主义现代化国家保驾护航。

踔厉奋发、笃行不怠。2023，属于奇安信的传奇，仍将继续！

超 10000 台信创终端如何替代？深圳某区政数局依托准入 NAC 构建安全屏障

作者 研究员 张少波

“目前，区党政机关电子政务外网的终端和服务器正在全面进行的信创的替代改造。在这个过程中，信创和非信创终端同时并存，终端面临的安全风险更加复杂，包括如何对资产进行识别、仿冒发现？如何确保访问身份和权限安全？如何确保接入安全合规？这些都关系到电子政务的整体防护能力。” 深圳市某区政数局相关负责人这样谈到。

深圳市某区政数局于 2019 年 3 月 15 日正式挂牌成立。其核心职责之一，就是统筹推进全区电子政务建设，负责电子政务外网（含政务办公网和政务服务网）、政务云平台、公共支撑平台、通用应用系统的建设、管理、应用和安全保障等工作，统筹协调各部门业务应用系统建设，指导各街道电子政务建设。

在国产化全面替代的大潮下，该区政数局走在了前列，截至目前，政数局及下辖 6 个街道办的信创替代已经完成了约 90%。同时，该区政数局深知电子政务稳定运行和数据安全的重要性，尤其面对信创和非信创同时存在的复杂环境，探索了“1+6”新一代信创准入安全防御体系。

信创终端替代超 10000 台 安全风险愈加复杂

作为全球电子信息的聚集地之一，深圳近年来积极推动信创产品的替代浪潮。今年 5 月，深圳发布了《关于促进消费持续恢复的若干措施》，明确提出了“扩大信创产品市场规模”。其中包括“对采购 50 万元以上信创产品、符合条件的用户单位，按采购额的 3% 给予补贴。原则上新增办公系统、业务系统中信创产品的采购比例，金融、能源、教育、医疗、电信、交通等重点领域不低于 20%；新增关键信息基础设施中信创产品的采购比例，党政机关、国资国企不低于 40%”。

目前，该区政数局管理的信创终端（含区委机关部门），以及下属的六个街道，信创替换已经达到了 90%，扩容信创终端超过 10000 台。该区信息中心负责人表示，由于大量信创及非信创终端同时存在，加上电子政务外网业务本身的开放性，以及日趋严重的勒索病毒、木马、黑客等攻击，安全风险变得更加复杂。

更具体而言，体现在四个方面：

首先是接入设备的资产识别和仿冒发现。目前包括区政数局及六个街道办，接入各类设备多达数万，其中包括移动终端、哑终端、泛终端、PC 等，如何对这些终端进行及时准确的资产识别和仿冒发现，是保障电子政务外网安全的关键。

其次是访问身份和权限的管理。电子政务外网很多业务对外开放，需要各方人员接入到政务网中。在这个过程中，访问身份和权限是否安全，访问的终端是否合规可信，遇到问题如何做设备定位追踪、接入行为溯源，以及接入安全分析，需要整体的防御体系。

第三是信创 PC 安装率及使用率的保障。国产化替代的过程中，不可避免地存在信创 PC 没有有效落地的情况，安全一方面要保障信创 PC 安装率及使用率，防止非法卸载，另一方面要确保接入安全合规。

最后是不同终端针对性的准入策略配置。由于信创与非信创终端并存，且分布非常分散和混杂，需要进行有效识别，制定针对性策略。

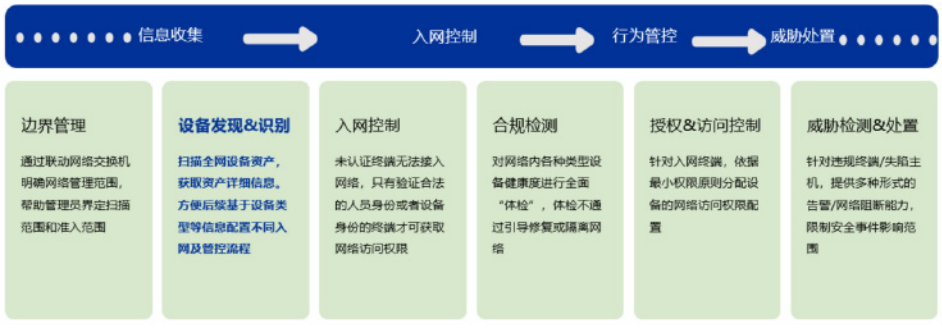
综合以上情况，该区政数局意识到，亟需在区政数局和 6 个街道办各增加部署一套准入系统，实现信创终端、非信创终端的识别与分类管控，保障国产化替代过程中的网络接入安全。

基于“1+6”准入方案 实现统一监管、统一准入

在病毒、木马、蠕虫及黑客等不断威胁并入侵政府内部网络资源的形势下，区政数局深知，终端安全不仅仅局限于恶意代码防范、病毒查杀、漏洞修补等方面，合规保障、接入感知、资产发现、认证授权、安全检查、追溯审计等“一站式”准入安全管理，都是电子政务安全不可缺少的一部分。

为此，该区政数局通过和奇安信的深入研究与探讨，双方在部署天擎终端安全管理基础上，共同制定了“1+6”新一代信创准入（NAC）解决方案，以实现电子政务网整体安全防护能力的全面提升。

据介绍，“1”指区政数局，“6”指下辖的 6 个街道办。项目在建设思路层面，通过政数局及 6 个街道办核心交

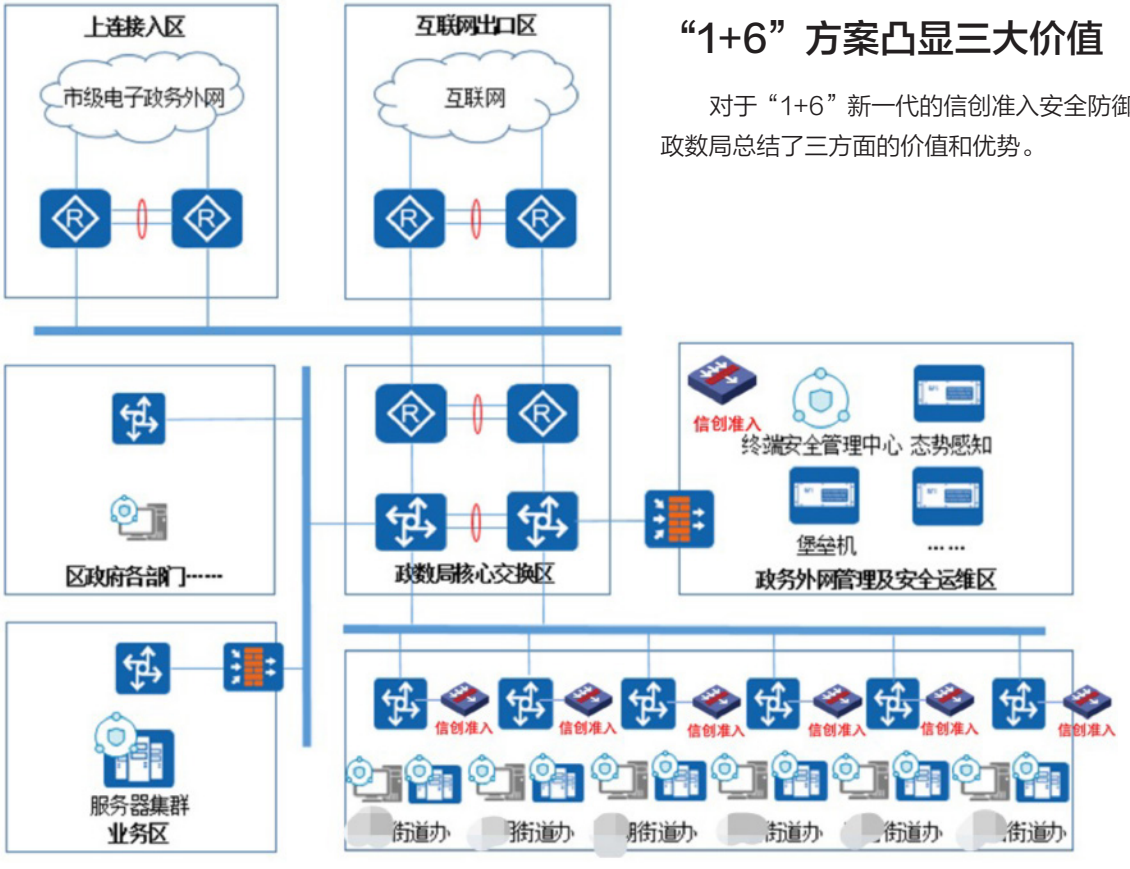


图：网络安全准入系统（NAC）产品功能

换机各旁路部署 1 套信创准入设备，对接入网络的设备实现：发现识别、强制身份认证、合规检查、异常处置、访问控制、入网追溯，终端 / 设备入网流程形成一个闭环，有效控制各阶段的接入安全风险，防止非法用户或设备随意接入网络，保障入网各阶段的安全可信，从而达到合法用户，合规终端的网络安全接入。

而在拓扑建设方面，政数局及 6 个街道办的准入设备采取集群方式部署，各街道办设置二级管控中心自行运维。通过一级管控中心进行集中统一监管，真正做到区政数局及 6 个街道办终端集中管理、整体防护、可视化呈现。具体拓扑建设情况如下：

图：深圳市某区政数局信创准入部署方案



在能力匹配方面，该区政数局根据信创 PC 扩容要求，信创及非信创终端统一安全管控，以及各街道办网络改造及接入资产管控需求，对新部署准入系统提出以下三项能力要求：

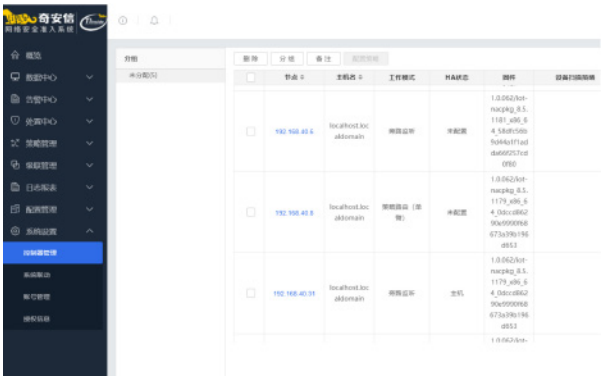
首先是能识别区分非信创及信创终端，实现入网合规基线检查（有没有装防病毒软件、是否存在弱口令、是否自带病毒），并能统一管控；

其次是能做终端资产识别梳理（视频 IP/MAC、设备类型、系统类型、厂商、网络位置、开放端口、流量协议），识别泛终端（如摄像头、打印机、交换机等）、移动终端和 PC，做到绑定终端 IP 和 MAC 地址（防止终端随意修改 IP）；

第三是支持 IPv6 地址。在满足当下电子政务网络的前提下，更好地适应未来互联网升级演进的需求。

“1+6”方案凸显三大价值

对于“1+6”新一代的信创准入安全防御体系，该区政数局总结了三方面的价值和优势。



首先是一体化设计，实现了天擎和准入完美联动。信创准入系统客户端与信创天擎客户端共用，信创准入系统支持与终端安全一体化管理平台联动，通过联动可强制 PC 机安装信创天擎客户端，通过信创准入系统了解该区信创终端资产数量及替换率。一体化管理解决终端杀毒补丁等安全需求的同时，通过合规准入、违规外联等基线策略的检查，有效管控内部资源违规访问和泄露的问题。

据介绍，在过去，安全准入和终端安全软件往往是相互独立的，这给管理和部署带来了一些难题。而奇安信 NAC 可以基于天擎集中统一管理，可在天擎“一体化”平台对引擎设备进行集中策略下发、设备批量升级、设备统一监测、区域分权管理等方式，适应超大规模用户的部署，多种灵活的手段满足大型网络架构下的业务管理需求，解决了传统方式的独立管理、散兵模式的部署难题。

同时，这种一体化管理显著减轻了用户运维人员的工作量。另一方面，由于 NAC 和天擎终端安全进行一体化的联动，使得终端只需打开一个进程，避免多进程对计算资源的消耗。

其次是“1+6” 新一代的信创准入模式，实现分级和统一两者兼得。通过“1+6”信创准入模式，既实现了各街道办分级管理终端，又能汇总全网数据，建立该区党政机关电子政务外网统一的终端安全管控系统。

值得一提的是，奇安信 NAC 方案最显著的优势就是部署更灵活。NAC 可采用旁路部署方式，对网络环境依赖较小，不改变用户网络架构，支持集中和分布式部署方式。而且，该产品支持多种准入技术混合部署模式，可实现核心区域的准入控制、终端层的准入控制、接入层边界的准入控制，满足不同场景下的应用部署需求。

第三是支持信创平滑替换，并全面兼容国产系统。据介绍，为满足国产化替代要求，奇安信网络安全准入系统提供基于 PK（飞腾麒麟）架构的国产化硬件设备，可通过多种手段准确识别网络中的 Windows 终端和信创终端，针对不同终端执行不同入网策略。在 Windows 终端替换为信创终端，以及第三方安全管理软件替换为天擎终端安全管理系统过程中，不关闭原准入策略，不影响待替换 Windows 系统正常使用。

更重要的是，NAC 准入系统完全适用主流国产系统银河麒麟、中标麒麟和专用国产系统银河麒麟、中标麒麟、中科方德操作系统，终端运行对国产系统中办公软件群均无冲突和影响。同台管理 Windows 终端、Windows 服务器、Linux 服务器、国产通用终端、国产通用服务器、国产专用终端、国产专用服务器，在单一平台统一管理多种类型终端，显著减少了管理员的管理成本。

信创替换运行平稳 安全事件实现“零事故”

“网络安全不能抱有侥幸心理，电子政务尤其如此，严格合规始终是我们的红线。”该区负责人反复强调安全的重要性。据介绍，得益于信创准入系统的部署，整个替换过程非常顺利，目前信创和非信创终端均运行平稳，未出现一起安全事故，同时各项业务均在平稳进行。

当前，信创替代浪潮目前已在党政、金融、能源等行业全面展开，并形成了巨大的市场空间。该区政数局联手奇安信打造的“X86 天擎升级 + 信创天擎 + 信创准入”的升级版一体化终端安全防护方案，很好地解决了信创过渡期面临的复杂安全风险、合规准入、统一管控等难题，为同行开辟出了一条值得业界借鉴的道路。安

想睡觉还真有人送枕头？程序员们千万当心有人“投毒”

“兄弟，稳么？”

如果是在别的游戏，你开外挂只会被一众玩家的口水喷到灰溜溜下线，但在某知名横版格斗游戏里，其他玩家只会问你上面这句话，生怕因为队友开挂而自己也惨遭游戏官方封号。

在这款游戏公测后的十多年里，游戏官方出了大大小小无数的关卡副本。但由于部分关卡的难度让普通玩家望而却步，为了追求通关后的奖励，不少玩家冒着被封号的风险，选择使用 F1（外挂秒杀快捷键大多为 F1）或者让使用 F1 的玩家带自己通关。

不过，使用外挂是有一定风险的，除了有可能会被游戏官方惩罚，还有可能“引狼入室”。部分黑产团伙为牟取利益，将木马程序植入到某些外挂工具中，一旦用户下载使用这些外挂，就会感染木马程序，导致自己的游戏账号或者其他虚拟资产被盗。

比如这些：

所以有些人也给出了个人 PC 的防病毒小妙招：不开外挂、不看“小电影”。

但你以为这样就安全了么？那些在普通人眼中拥有高超计算机技术的程序员极客们，即便严格遵守上述“小妙招”，也会有马失前蹄的时候。

一次早有预谋的“供应链投毒”事件

对于大多数程序员而言，MobaXterm 这款工具即便没用过，也或多或少听说过。作为一款功能强大的终端管理工具，能够允许用户远端管理虚拟机，如文件拷贝、执行等。

当然，能够在 SecureCRT、PuTTY、XShell 等一众终端管理软件中脱颖而出并受到广大用户的青睐，MobaXterm 有着自己独到的优势，如支持 SSH、FTP、串口、VNC、XServer 等；支持众多的快捷键和插件，用户体验非常好……

所以在社交平台上，不少用户给出了很高的评价：

不过，这款软件也并非没有缺点，最典型的就是

MobaXterm 虽然有免费版本，但用户界面目前不支持中文，这让不少习惯了汉化界面的用户颇感不爽。

因此，网上有着不少用户寻求汉化资源的声音。当然也有不少技术大拿慷慨解囊，将自己使用的资源分享在某些技术社区里，供其他用户下载。

不过，也并非所有人都那么好心。

11 月 4 日开始，一篇打着推广“MobaXterm 中文版”旗号的文章，出现在了国内某知名技术社区和社交平台网站上，文章里还精心附上了中文版下载链接。

这让不少用户喜出望外，直呼博主“666”、“好人一生平安”，心想可算不用对着一堆看不太明白的英文干活了，这不是想睡觉刚好有人送来了枕头么?

博主似乎也很懂得国内用户的心理，连续在各大社区发表了 7 篇推广中文版资源的文章。如果在搜索引擎搜索“MobaXterm 中文版”，就能在第一条链接找到该博主发布的推广文章（现已删除）。

然而，就在有些人自鸣得意以为找到了汉化资源的同时，奇安信网络安全部却发现了不同寻常的事情。

奇安信网络安全部在日常运营过程中通过天擎 EDR（终端安全检测与响应软件）发现，该中文版资源似乎携带并试图传播木马程序。

这个发现让当事人吃了一惊，如果木马被实锤，那么，这就又是一起典型的利用社会工程学和软件供应链的投毒事件：攻击者利用用户想要汉化版资源的心理，技术社区和社交平台等软件分发渠道，传播木马程序，从而达到不可告人的目的。

为了进一步搞清楚这件事的前因后果，奇安信威胁情报中心旗下红雨滴团队，对该事件进行了进一步的拓展分析。

一次早有预谋的网络攻击就此浮出水面。

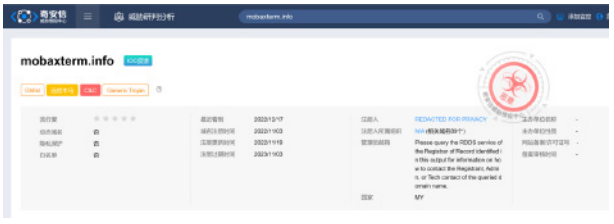
目标窃密，已有多人中招

为了迷惑受害者，攻击者将带毒应用的托管域名，伪装成了和 MobaXterm 官方网站类似的域名。

带毒应用的托管域名：mobaxterm.info

MobaXterm 的官方网站域名：mobaxterm.mobatek.net

而通过 Alpha 威胁分析平台（ti.qianxin.com），红雨滴团队反查到了该域名的注册信息：域名注册时间是 11 月 3 日，恰好就是攻击者发布第一篇带毒应用推广文章的前一天。



与此同时，红雨滴团队还发现了另外一条关键线索：早在攻击者发布第一篇带毒应用的推广文章前的半个月，也就是 10 月 19 日，攻击者在各大社区创建了账号。不过直到账号注销为止，除了推广文章，这些账号从来没有发过其他内容。

根据这两点来判断，说攻击者早有预谋，可一点也没冤枉。

那么，攻击者如此大费周章处心积虑地传播木马程序，究竟是想要干嘛呢?

经过红雨滴云沙箱对木马程序的深度分析，答案就显而易见了：用户下载得到的压缩包中携带恶意载荷，最终会加载 Gh0st 木马，执行远程控制和窃密行为。（具

体细节可关注奇安信威胁情报中心文章：《注意！终端管理工具 MobaXterm 中文版暗藏木马陷阱》）

不幸的是，从域名访问次数来看，域名注册短短一个半月的时间，已经有不少用户可能已经中招。

该域名自注册以来的访问趋势如下：

预防供应链投毒，安全意识是关键

经过红雨滴团队的一通拓展分析，目前，基于奇安信威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼、NGSOC 等，都已支持对此类攻击的精确检测。

需要注意的是，类似的利用供应链进行木马病毒程序传播的网络安全事件，这并不是第一起，当然也不会是最后一起。

巧合的是，从 2020 年开始，每一年的年底都会发生（曝光）一起影响较为严重的供应链安全事件。

比如，2020 年年底曝光的 Solarwinds 后门事件，攻击者通过向其 Orion 软件更新服务器上植入后门程序，从而感染了大量 Solarwinds 用户；

再比如 2021 年底发生的堪称“核弹级”的 Log4j2 漏洞事件，由于使用该组件的应用非常多，攻击者可以利用该漏洞，攻击绝大多数的 Java 应用。

所不同的是，在此次事件中，攻击者并没有选择在软件供应链的源头下手（当然这需要一定的技术实力或者契机），而是在软件的分发渠道上（如技术社区），设置一个带毒的目标，引诱受害者下载，就像西游记中猪八戒偷青牛精的衣服穿，导致被妖怪捉住一样。

预防此类投毒事件，其实方法也很简单。说白了，用户的安全意识才是关键。

奇安信威胁情报中心提醒，近年来，利用付费软件破解版和国外软件汉化版为诱饵的软件投毒事件层出不穷，软件使用者需要加强安全意识，仔细鉴别软件下载地址是否为真实官方地址，不使用网上来历不明的软件，避免成为网络攻击者的猎物。

另外，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行夸张标题的未知文件，不安装非正规途径来源的 APP。做到及时备份重要文件，更新安装补丁。

不过话又说回来，并非所有好用的小工具都能轻易找到官方下载地址，不少极客手里可能都有自己的“私货”，想要把这些东西拿来用又不感染木马程序，除了睁大眼睛仔细辨别，正确使用安全工具就显得非常重要了，如部署安装率先发现木马程序的终端安全产品天擎 EDR。

除了天擎 EDR，还有一款工具非常实用，奇安信威胁情报文件深度分析平台（sandbox.ti.qianxin.com/sandbox/page），它内置多款动静态分析引擎，可对 Windows、安卓平台在内的多种格式文件进行深度分析。

安装运行之前，把软件上传到平台上检测一下，是不是有问题就一目了然了。安

规划快一步

奇安信 | BEIJING 2022

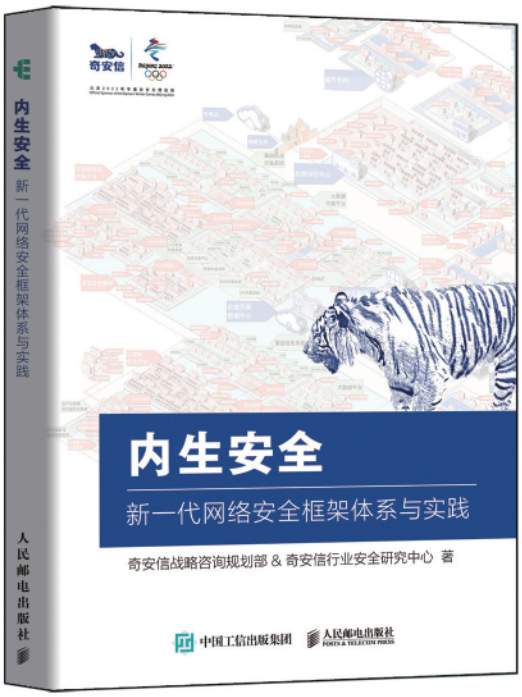
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

大事记

奇安信集团董事长齐向东当选全国工商联副主席

中国工商业联合会第十三次全国代表大会于 12 月 11 日至 12 日在北京举行。大会选举产生了全国工商联新一届领导机构和领导班子，全国政协副主席高云龙再次当选全国工商联主席，中央统战部副部长徐乐江连任常务副主席，奇安信集团党委书记、董事长齐向东等 22 人当选副主席。

奇安信入选 2023 年度工业信息安全监测应急支撑单位

近日，国家工业信息安全发展研究中心公布公示了 2023 年度工业信息安全监测应急支撑单位名单，凭借在工业信息安全领域的长期深耕和技术实力，奇安信集团成功入选。

为进一步落实党的二十大精神，围绕建立大安全大应急框架的战略目标，更好地支撑国家工业信息安全监测预警与应急管理体系建设，国家工业信息安全发展研究中心整合现有的工业信息安全监测网络建设支撑机构、工业信息安全应急服务支撑单位为工业信息安全监测应急支撑单位。此次入选，是对奇安信在工业信息安全领域实力的充分肯定。

深化校企合作 奇安信与南信大共建网络安全英才班

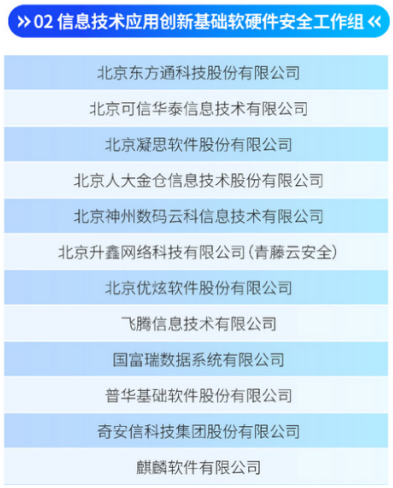
近日，奇安信集团与南京信息工程大学举行共建网络安全英才班暨深化校企合作签约仪式。双方将共建“南信大 – 奇安信数字取证联合研究院”“南信大 – 奇安信网络安全创新创业实验室”，开设奇安信网络安全英才班。同时，双方将共建“数字取证教育部工程研究中心”。

据悉，网络安全英才班主要通过高考优录及全校考核相结合的方式组建而成，以培养满足国家网络空间安全战略及顶尖安全企业的人才需求为导向，面向数字取证、网络安全、司法鉴定等培养方向，双方共同完成全日制授课，通过扎实的理论和丰富的实训案例，有效推进专业人才培养。

奇安信首批入选网络安全技术与产业发展工业和信息化部重点实验室专项工作组

近日，工业和信息化部网络安全产业发展中心公布了网络安全技术与产业发展工业和信息化部重点实验室专项工作组成员单位（第一批）名单。奇安信集团入选信息技术应用创新基础软硬件安全、工业互联网安全、车联网安全三个工作组成员单位。

重点实验室依托工业和信息化部网络安全产业发展



中心（工业和信息化部信息中心）于 2019 年申请并获批。重点实验室聚焦网络安全新模式、新技术、新业态，围绕新一代信息技术与传统产业深度融合，开展信创环境下云安全、大数据应用与安全、人工智能、工业控制安全、密码应用等网络安全新技术在重点领域、重点行业的基础研究、产品开发、方案集成、成果转化及应用推广。

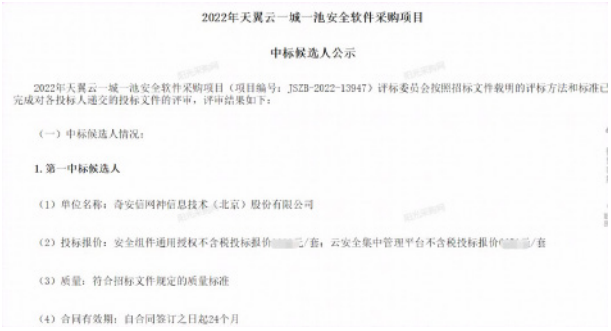
齐向东：“三步走”构建数据安全体系 守好数据安全红线

12 月 2 日，由贵州省委网信办主办的“强化网络安全保障体系 护航数字经济发展创新”论坛在贵阳市举行。奇安信集团董事长齐向东表示，数据强监管时代已经到来，政企机构应通过“盘清资产、精准防护、全局管控”的“三步走”，来破解数据安全防护难题，守好数据安全红线。

奇安信中标某省 2022 年天翼云一城一池安全软件采购项目

近日，中国电信公布了某省 2022 年天翼云一城一池安全软件采购项目中标候选人，奇安信网神信息技术（北京）股份有限公司以第一中标候选人的身份成功中标，中标产品包括云安全集中管理平台、安全组件通用授权等。本次中标，再次彰显了奇安信云安全在运营商行业的领先优势。

得益于云安全领域的产品和技术优势，奇安信与天翼云一直保持紧密的合作。在年初，中国电信天翼云公布的 2021 年云资源池安全产品集中采购中，奇安信集团旗下网神公司以综合排名第一的成绩，成为该项目第一中标候选人。



2022年天翼云一城一池安全软件采购项目

中标候选人公示

2022年天翼云一城一池安全软件采购项目（项目编号：JSZB-2022-13947）评标委员会按照招标文件载明的评标方法和标准已完成对各投标人递交的投标文件的评审，评审结果如下：

（一）中标候选人情况：

1. 第一中标候选人

（1）单位名称：奇安信网神信息技术（北京）股份有限公司

（2）投标报价：安全组件通用授权不含税投标报价[redacted]元/套；云安全集中管理平台不含税投标报价[redacted]/套

（3）质量：符合招标文件规定的质量标准

（4）合同有效期：自合同签订之日起24个月

北京市学习贯彻党的二十大精神宣讲团报告会在奇安信集团举行

11 月 22 日，北京市学习贯彻党的二十大精神宣讲团赴奇安信集团举行宣讲报告会。市宣讲团成员，市委网信办主任、市委互联网企业工委书记韩昱做报告，并与广大党员干部代表座谈交流。

报告会后，韩昱与奇安信集团负责人、高管代表开展深入交流。齐向东强调，奇安信要不断深化党委委员对二十大精神的深入学习，动态调整学习计划。一方面，面向集团高层，建立二十大精神线上学习班，分阶段推进学习；另一方面，针对分布在全国各地的党支部，建立学习专班，反复学习、深刻领会、重点讨论，深入领会二十大报告精神。

奇安信亮相香港 PwC HackaDay 2022

由普华永道在中国香港举办的一年一度的网络安全盛会——PwC HackaDay 2022 在港岛中环大馆召开，奇安信集团受邀参加并由华南区技术总监陈志华发表主题演讲——“2022 北京冬奥网络安全‘零事故’实战化安全体系”。这是冬奥网络安全“中国方案”首次在香港公开分享，受到与会的安全专家、企业代表的极大关注，成为当日观众人数最多的一场演讲。

陈志华表示，接下来，奇安信将及时把成功经验引进香港，为香港地区政企机构提供基于“零事故”标准的产品、技术、服务和方案，守护香港网络安全。

奇安信中标中国联通某主机安全项目 打造主机威胁检测新范式

近日，奇安信中标 2022 年中国联通旗下某单位主机安全项目，中标产品为奇安信旗下主机安全产品椒图，助力该单位打造主机安全领域威胁防御、检测与响应的新范式。

据悉，除该项目外，奇安信还多次中标中国移动、中国联通、中国铁塔等主机安全项目，中国联通的多个重要公众业务系统均由奇安信承担主要安全防护工作，并取得了中国联通相关运营单位的认可。

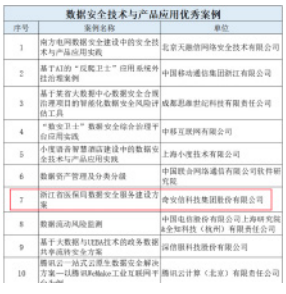
荣誉墙

奇安信斩获“数据安全共同体计划”双料大奖

近日，中国信通院联合 60 余家高校、科研院所、企事业单位共同发起的“数据安全共同体计划”，公布了数据安全“星熠”案例征集活动的入选名单，奇安信申

隐私计算技术应用优秀案例

序号	案例名称	单位
1	基于数据沙箱技术的数据安全流通平台	奇安信科技集团股份有限公司
2	隐私计算赋能政务数据跨域安全共享与融合计算	杭州金智塔科技有限公司
3	星云Clustar隐私计算算力解决方案	深圳致星科技有限公司
4	多源数据共享应用平台	上海同态信息科技有限责任公司
5	小度端云一体数据安全解决方案	上海小度技术有限公司
6	浙江五环市贸联网门户产业互联网平台	北京八分量信息科技有限公司
7	基于隐私计算的债券估值体系建设项目	深圳市洞见智慧科技有限公司
8	企业级机密信息的大数据隐私计算应用案例	腾讯云计算（北京）有限责任公司
9	基于多方安全分析的智能化理赔助力普惠医疗	蚂蚁科技集团股份有限公司



数据安全技术与产品应用优秀案例

序号	案例名称	单位
1	南方电网数据安全建设中的安全技术与产品应用实践	北京天融信网络安全技术有限公司
2	基于AI的“反舰卫士”应用系统外挂治理案例	中国移动通信集团浙江有限公司
3	基于某省大数据中心数据安全合规治理项目的智能化数据安全风险评估工具	成都思维世纪科技有限责任公司
4	“数安卫士”数据安全综合治理平台应用实践	中移互联网有限公司
5	小度语音智慧调研建设中的数据安全技术与产品应用实践	上海小度技术有限公司
6	数据资产管理及分类分级	中国联合网络通信有限公司软件研究院
7	浙江省医保局数据安全服务建设方案	奇安信科技集团股份有限公司
8	数据流动风险监测	中国电信股份有限公司上海研究院&全知科技（杭州）有限责任公司
9	基于大数据与UEBA技术的政务数据共享流转安全方案	深信服科技股份有限公司
10	腾讯云一站式云原生数据安全解决方案—以腾讯Polaris工业互联网平	腾讯云计算（北京）有限责任公司

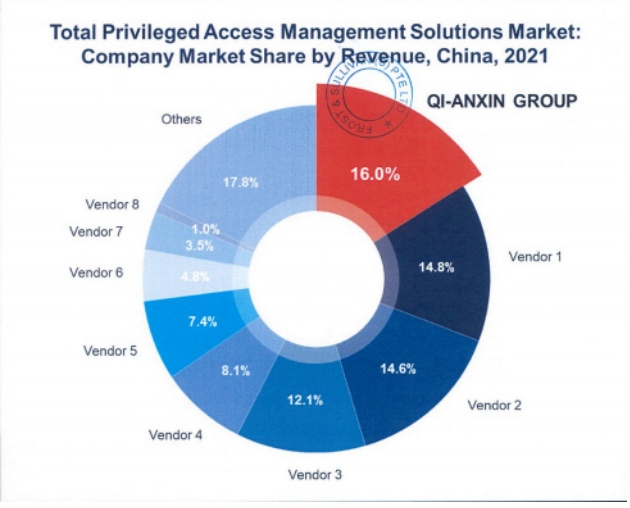
报的“基于数据沙箱技术的数据安全流通平台”“浙江省医保局数据安全服务建设方案”，分别入围“隐私计算技术应用优秀案例”和“数据安全技术与产品应用优秀案例”两大方向，斩获双料大奖。

奇安信被 Gartner 列为 NDR 全球代表性供应商

近日，国际机构 Gartner 发布了 2022 年《网络检测与响应市场指南》，对全球范围内 NDR 市场发展、技术变化、部署建议、代表供应商等进行了详细的剖析。其中，作为国内网络安全领军企业，奇安信凭借旗下天眼新一代安全感知系统（天眼系统），被列为具有代表性的供应商 (Representative Providers) 之一。

中国第一 亚太前二 奇安信 PAM 解决方案入围全球头部阵营

日前，全球企业增长咨询公司 Frost & Sullivan 发布《全球特权访问管理 (PAM) 解决方案增长机会研究报告》，对全球范围内 PAM 市场增长情况、主要供应商等进行了详细的分析。凭借“特权账号生命周期管理流程”的特权访问管理解决方案，奇安信以 16.0% 的市场份额位居中国市场第一，并当选全球范围内主要 PAM 供应商。



2022 全球数商大会首届数据交易节 奇安信获评“年度领军数商企业”

11 月 25 日，上海数据交易所主办，新加坡科技工商协会、西部数据交易中心、深圳数据交易所、安徽大数据交易中心（筹）联合主办的 2022 全球数商大会在上海开幕。大会首次组织了数据交易节，为数字经济和数据交易领域领先的数商企业、交易机构、行业领袖颁发奖项。奇安信集团荣获“年度领军数商企业奖”。

主办方表示，“年度领军数商企业奖”面向全国范围内有影响力的数商企业，依照创新型、引领性、代表性、发展潜力四大维度进行评选。凭借着行业领先的产品技术积累及在数据安全领域的创新实践，奇安信一直领跑数据安全赛道。

同比增长 45.8% 领跑中国数字政府 IT 安全软件市场

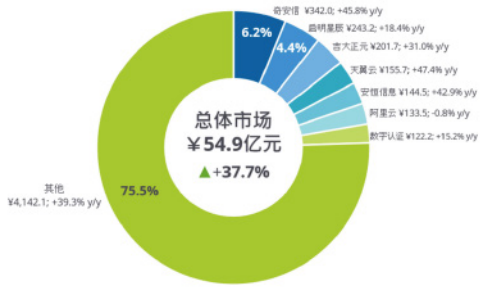
近日，领先的 IT 市场研究和咨询公司 IDC 机构发布了《2021 年中国数字政府 IT 安全软件市场份额报告》。IDC 报告显示，2021 年中国政府 IT 安全软件市场规模达到人民币 54.85 亿元，同比年增长率为 37.7%。

在竞争格局方面，奇安信位居市场领先地位，并保持了 45.8% 的高速增长。

《报告》指出，奇安信自成立以来，持续深耕政务领域网络安全的研究与开发，融合政务业务和研发经验，基于安全大数据、人工智能和安全运营技术，形成了智慧城市安全监管与运营响应、税务数据安全、信创云安全、网络安全等级保护（等保 2.0）服务、保密攻防实训等众多政务网络安全整体解决方案，并已成功应用到中央部委及各级地方政府。

图 1

中国数字政府 IT 安全软件 2021 年市场份额概况



注：2021 年厂商份额（%），收入（¥百万元人民币），增长率（%），总体市场（¥亿元人民币）

来源：IDC, 2022

奇安信金融行业零信任方案成功入选 CCIA“2022 年零信任优秀应用案例”

近日，中国网络安全产业联盟对外公布“2022 零信任优秀应用案例”评选结果。奇安信集团、国信证券联合报送的“面向金融行业的零信任跨网动态授权平台”作为行业标准化典型案例凭借实用性、创新性、先进性，入选 CCIA“2022 年零信任优秀应用案例”，成为本次优秀案例中唯一一项金融行业零信任落地标杆。

“2022 年零信任优秀应用案例”评选结果名单

序号	案例名称	申报单位
1	零信任助力疫情下远程高效办公	北京快手科技有限公司
2	某集团园区网零信任安全	格尔软件股份有限公司
3	零信任安全架构在医疗领域的应用	广东省新黄埔中医药联合创新研究院、北京数字认证股份有限公司
4	基于零信任的移动业务安全防护体系建设实践	上海上讯信息技术股份有限公司、国瑞网信科技（北京）有限公司
5	零信任安全创新应用—构建动态可管可控的安全	中国移动通信集团江西有限公司
6	360 零信任数字工作空间案例	三六零数字安全科技集团有限公司、三六零科技集团有限公司
7	面向金融行业的零信任跨网动态授权平台	奇安信科技集团股份有限公司、国信证券股份有限公司
8	基于零信任框架的下一代 IAM 平台	中国移动通信集团有限公司、中国移动通信集团设计院有限公司
9	云网融合场景下端到端网络安全防护实践	中国移动通信集团公司信息安全管理与运行中心、中移互联网有限公司、中移（杭州）信息技术有限公司
10	江苏移动零信任网络建设项目	亚信科技（成都）有限公司
11	某市大数据局业务系统零信任架构升级	中孚信息股份有限公司

奇安信威胁情报产品和能力进入全球头部阵营

日前，全球企业增长咨询公司 Frost & Sullivan 发布了《2022 全球威胁情报平台雷达图》，奇安信集团凭借战略创新及全面的产品组合入围该报告，被评为中国威胁情报平台（TIP）市场增长最快的网络安全厂商之一，创新力全球领先。

奇安信电力行业 5G 网络安全接入能力建设入选“5G+ 工业互联网”典型案例

2022 中国 5G+ 工业互联网大会上，公布了 2022 中国“5G+ 工业互联网”典型案例。奇安信集团“电力行业 5G 网络安全接入能力建设”解决方案成功入选。

项目负责人表示，由于没有可供参考的案例，整个方案进行了创新性的方案设计。通过项目的部署和成功实施，不仅为电力行业进行 5G 无线通信安全建设提供参考，也使得目前行业的安全能力从少量的“样本规范”转变为可推广、可复用的“解决方案”。该项目为电力行业无线网络安全建设起到了很好的示范作用。

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

网络安全 中国代表队 | 奇安信

2022年北京冬奥会胜利闭幕

“零事故”

奇安信圆满完成冬奥会网络安全保障任务

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。


奇安信科技集团股份有限公司

CCIA 50强

2022年中国网安产业竞争力50强

编号：CCIA-2022JZL-01

中国网络安全产业联盟
2022年6月

“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