SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

“零事故”

打破奥运网安“魔咒” P18

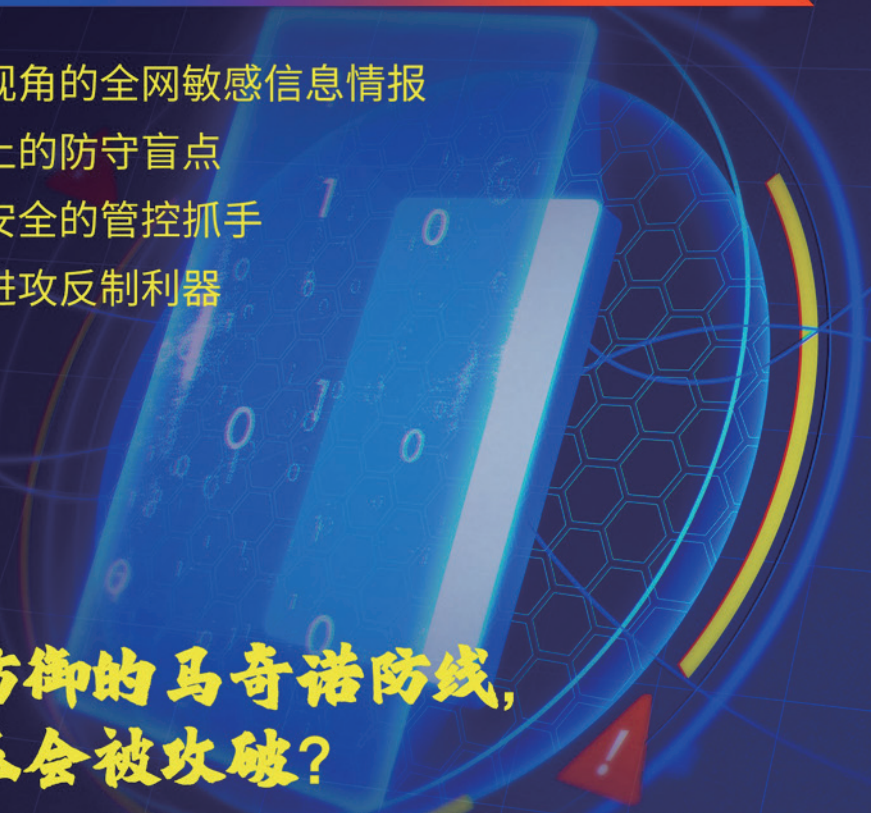
第14期

2022 年 2 月

奇安信

敏感信息泄露情报服务

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



纵深防御的马奇诺防线，为什么会被攻破？

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

服务定位 SERVICE POSITIONING

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

奇安信安服团队

“零事故”只是新的开始

2 月 20 日，北京冬奥会大幕落下，中国代表团创造了参赛史上最好成绩，为我国冰雪运动创下新高度。

在紧张的赛事、光鲜亮丽的数字技术背后，一场隐形的赛场也在悄然进行：一支完整的网络安全保障团队努力确保冬奥会各项系统正常运转。作为奥运会历史上首家第三方网络安全服务商，奇安信最终以“零事故”的成绩交上了 2022 年北京冬奥会的网络安保答卷。

作为世界上观看人数最多的体育赛事之一，冬奥会一直是网络攻击组织的主要目标，从参赛运动员个人信息，到赞助商、赛事系统，冬奥会上充满了令攻击者垂涎的对象。

2012 年伦敦奥运会期间发生约 2.12 亿次攻击。东京奥运会期间这一数字达到两倍多。韩国平昌冬奥会甚至发生世界级网络安全事故，导致互联网和广播系统中断、奥运会网站瘫痪。

2022 年北京冬奥会同样面临严峻的网络安全形势。据了解，跨度百余公里的 3 个赛区、26 个场馆，近百个国家数千名运动员的交流沟通、场馆协作需要依赖于大量先进的技术。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。

据奇安信网络安全保障中心统计，在冬奥重保期间，累计监测到各类网络攻击超过 2.4 亿次（含社会面），跟踪、研判、处置涉奥舆情和威胁事件 105 件。同时累计发现、修复安全漏洞 5782 个，排查风险主机 150 台，发现恶意样本数 54 个。

赛事期间，奇安信成立了 11 支冬奥保障团队，并设置产品指挥组、一线指挥组、漏洞情报组、支撑保障组等 20 个分组，以及由数百名白帽子组成的“冬奥网络安全卫士”，7*24 小时监测、研判、阻断和处置威胁，全方位保护冬奥网络安全。

“零事故”标志着北京冬奥会的网络安全保障能力全面超过往届，也证明了以奇安信为代表的国内安全企业技术实力是世界领先的，树立了行业新标杆。

“零事故”也是新的开始。在这场国际赛事中积累的丰富防护经验，无疑会成为保障国内政企安全的基石。

总编辑

李建平

2022 年 2 月 1 日

CONTEN

目录

安全态势

月度专题

“零事故”

打破奥运网安“魔咒”

—— 奇安信冬奥网络安全保障揭秘

P18

冬奥会全球瞩目，是黑客团伙垂涎的攻击目标。里约奥运会发生奥运相关组织数据泄漏；平昌冬奥会发生世界级网络安全事故，导致互联网和广播系统中断、 奥运会网站瘫痪。作为奥运会历史上首家第三方网络安全服务商，奇安信却创造出北京冬奥会“零事故”的佳绩，这是如何做到的?

TS

奇安资讯

第 14 期

《网安 26 号院》编辑部

主办 奇安信集团

总　　编　　辑：李建平

副　　总　　编：裴智勇

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

奇安资讯主编：陈　冲

安全意识主编：李建平

奇安信集团　虎符智库　安全内参

电子版请访问 www.qianxin.com 阅读或下载

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 2021-L0058 号

印刷数量：45000 本

印刷单位：北京七彩虹印刷有限公司

下载地址：www.qianxin.com

事件篇

国家敏感机构频频遭遇严重网络攻击，英国外交部、美国国防承包商、乌克兰政府、伊朗国家电视台等机构均受影响；勒索软件攻击持续猖獗，航港巨头瑞士空港、欧洲多处港口石油设施等沦为最新受害者。

美政府称国防承包商被俄黑客入侵长达一年，敏感信息失窃

据 CISA 官网 2 月 16 日消息，美国网络安全与基础设施安全局、国家安全局、联邦调查局联合发布咨询称，自 2020 年 1 月以来，俄罗斯黑客组织已经入侵了多个国防承包商网络，在某些情况下，至少持续了六个月，定期窃取数百份文档、电子邮件和其他数据。被入侵的实体包括支持美国陆军、美国空军、美国海军、美国太空部队及国防部和情报计划的国防承包商。这些持续的入侵使攻击者能够获取敏感的、非机密的信息，以及承包商专有的和出口控制的技术。

乌克兰政府和银行网站遭大规模网络攻击被迫关闭

据 The Record 2 月 15 日消息，乌克兰政府和银行遭受大规模 DDoS 网络攻击，导致国防部、外交部、文化部及国内最大的两家国有银行 Privatbank 和 Oschadbank 等机构的网站停止运行，两家银行的 APP 和在线支付都无法使用，部分用户收到虚假消息。乌克兰警察称，虚假消息不包含网络钓鱼链接，显然是为了制造混乱的“信息攻击”。此次攻击正值俄乌边境局势紧张，乌克兰文化和信息政策部暗示，俄罗斯可能是此次事件的幕后黑手。

中欧小国最受欢迎电视台播放中断：因遭受网络攻击

据 The Record 2 月 10 日消息，中欧小国斯洛文尼亚最受欢迎的电视频道 Pop TV 遭受网络攻击，引发运营中断，致使新闻节目、频道与体育赛事直播中断，当地的北京冬奥会直播也受到影响。近几年来，全球发生了多起针对广播电视机构的网络攻击，其大多属于勒索软件攻击，通过攻击电视台后端 IT 基础设施令节目播放受影响，从而实施勒索。

英国外交部遭遇一起严重网络安全事件，细节未知

据路透社 2 月 8 日消息，英国政府网站近日发布的一份招标文件显示，今年早些时候，英国外交部成为了一起严重网络安全事件的目标，但未披露任何事件细节。该文件还显示，外交部被迫请来国内防务巨头贝宜系统旗下子

公司（BAE Systems Applied Intelligence）处理这一事件，并为这项工作支付了46.7万英镑（约人民币402万元）。

葡萄牙全国大面积断网：因沃达丰遭破坏性攻击

据 The Record 2 月 8 日消息，国际电信巨头沃达丰旗下葡萄牙公司披露，由于遭到破坏性网络攻击，导致 4G/5G、固话、电视等网络服务全部持续中断，只有语音和 3G 网络经恢复后勉强可用。沃达丰在葡萄牙拥有超 400 万移动用户、340 万家庭及企业宽带用户，此次攻击造成了大规模不便甚至混乱。网络上有猜测认为是勒索软件所为，官方暂未确认。

网传 B 站企业邮箱发钓鱼链接，致使多员工被骗达 8 万元

据灼燃科技 2 月 7 日消息，微博用户 @ 王落北 爆料称，1 月 5 日凌晨，B 站公司内部邮件发出了全员钓鱼链接，多位同事中招，受骗金额总计 8 万元左右。当天下午 1 点 IT 才把钓鱼邮件删除完。该微博的配图显示，钓鱼邮件为“年终工资补贴通知”相关内容，受害员工成立了“钓鱼邮件受害者”群，已有 72 人加入。

欧洲多处港口石油设施遭黑客攻击，油轮无法靠港

据央视新闻 2 月 5 日消息，当地时间 1 月 29 日开始，因遭到勒索软件的攻击，位于荷兰阿姆斯特丹和鹿特丹及比利时安特卫普的几处港口的石油装卸和转运受阻。截至 2 月 4 日，至少有七艘油轮不得不在安特卫普港外等候，无法靠港。负责从这些港口向内陆城市转运石油的驳船也发生延误。目前受影响公司正聘请网络安全专家进行调查。去年美国的几家石油公司也曾遭遇类似事件。

国际航港巨头遭勒索软件攻击，致使运营受干扰、机场航班延误

据 Bleeping Computer 2 月 4 日消息，全球航港巨头瑞士空港日前披露了一起勒索软件攻击事件，IT 基础设施与服务受到影响，导致运营被干扰。瑞士空港的客户苏黎世机场透露，这波网络攻击发生在 2 月 3 日早上 6 点，并导致当天 22 架次航班发生轻微延误，大约在 3~20 分钟之间。瑞士空港解释道，其地勤服务能在缺少 IT 系统支持的情况下继续保持运作，只是不可避免会发生一定程度的延误。

伊朗国家电视台遭网络入侵，播放“杀死总统”暴恐信息

据美联社 1 月 27 日消息，伊朗国家电视台遭到网络攻击，旗下多个频道被劫持，播放了反对派组织领导人的信息，甚至提到“向 Rajavi（反对派领袖）致敬，让 Khamenei（伊朗最高领导人）去死”等暴恐信息。伊朗国家电视台表示，当局将对此次黑客入侵开展调查，并可能会得到国外势力的帮助。此前 1986 年，伊朗国家电视台也曾出现播放异常内容的情况，有媒体称是美国 CIA 在幕后策划了该起事件。

勒索软件组织声称已入侵法国司法部，要挟支付赎金

据 Politico 1 月 27 日消息，Lockbit 2.0 勒索软件的暗网博客将法国司法部添加到受害者名单当中，要挟必须在 2 月 10 日前支付赎金，否则“所有被盗数据都将被发布至暗网”。法国司法部回应称，已知悉情况并采取措施，包括开展相关检查。Lockbit 2.0 近期攻势非常凶猛，其暗网博客还放出了一系列西欧国家的大型企业名单，威胁索要赎金。

漏洞篇

近期，钉钉、向日葵等国产大众软件被曝高危漏洞，漏洞细节和 PoC 均遭到公开，危害较大，建议用户尽快自查并更新修复。

钉钉 Windows 版远程代码执行漏洞风险通告

2022 年 2 月 17 日，奇安信 CERT 监测到钉钉远程代码执行漏洞 PoC 已在互联网上公开。攻击者可将恶意代码托管在服务器上，诱使受害者使用钉钉打开链接，钉钉即会获取恶意链接指向的网页内容并用内置浏览器渲染，从而触发漏洞，在受害者电脑上远程执行代码。经验证，钉钉 Windows 版 v6.3.15 受到影响。目前，该漏洞已发现在野利用且 PoC 已公开，建议用户尽快自查并更新至新版本进行修复。

向日葵远程控制软件命令执行漏洞风险通告

2022 年 2 月 16 日，奇安信 CERT 监测到互联网上泄露关于向日葵远程控制软件命令执行漏洞的细节。远程攻击者在未授权情况下，可通过构造特殊请求执行任意命令。经验证，在个人版 Windows v11.0.0.33826 中测试成功。目前官方已发布最新版 Windows v12.5.1.44969 修复了漏洞。鉴于该漏洞利用难度极低，危害较大，建议用户尽快自查并更新修复。

Fortinet FortiWeb Web 应用防火墙漏洞预警

2022 年 2 月 8 日，国家信息安全漏洞库收到关于 Fortinet FortiWeb 安全漏洞（CNNVD-202202-129、CVE-2021-43073）情况的报送。成功利用漏洞的攻击者，可向目标设备发送特殊请求，从而远程执行恶意代码。FortiWeb 6.4.1 及其以下版本均受此漏洞影响。目前，Fortinet 官方已发布新版本修复了该漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

Linux Polkit 安全漏洞预警

2022 年 1 月 28 日，国家信息安全漏洞库收到关于 Polkit 安全漏洞（CNNVD-202201-2343、CVE-2021-4034）情况的报送。成功利用此漏洞的攻击者，可在默认配置下提升本地用户权限。Polkit 所有版本均受此漏洞影响。Polkit 是一个在类 Unix 操作系统中控制系统范围权限的组件，存在于所有主流 Linux 发行版的默认配置中。目前，Polkit 官方已发布新版本修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

对抗篇

国内攻防演习 1 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 1 月，奇安信 Z-TEAM 团队共承接攻防演习服务 24 场，其中，行业级攻防演习 1 场，地市级攻防演习 1 场，客户自主攻防演习 22 场。

本月攻防演习成果如下：

本月攻防演习成果：

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	21	44	76	112	18	51	132	855

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，涉及的目标业务以金融、电网、运营商为主，客户存在的安全问题主要涉及互联网侧应用组件存在漏洞缺陷、内部人员对钓鱼攻击防范意识不足、内网口令复用及弱口令普遍、内网访问权限策略设置不严、内网功能区域缺乏安全隔离等。具体情况如下。

1、漏洞利用是主要突破手段

本月任务中发现大部分目标被攻陷是因为互联网侧应用存在漏洞，且可被利用进行突破渗透。漏洞以历史漏洞为主，如log4j2漏洞、sql注入、shiro反序列化漏洞、任意文件上传等，多因外部应用更新不及时导致，这些历史漏洞的存在，成为目标网络的重大安全威胁。

2、钓鱼攻击是实现突破的有力辅助

本月任务中钓鱼攻击主要针对金融和电网目标人员开展，这些行业网络安全体系建设比较完善，防护相对严密，互联网侧系统可利用漏洞和其他突破途径较少。针对安全意识相对薄弱的客服或HR等人员进行钓鱼攻击，成为了攻击者实现外部突破的高效手段之一。

3、内网弱口令和口令复用安全隐患严重

本月任务中目标网络弱口令和口令复用情况依然严重，弱口令和口令复用主要存在于内网。其中，内网安全设备、数据库服务器和系统等存在弱口令和口令复用的情况较多，导致这种情况的原因为人员安全意识薄弱，对此类问题的危害严重性认识不足。

4、访问策略缺陷是严重的安全威胁

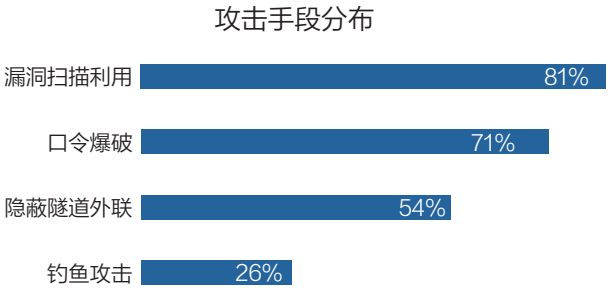
本月多个任务目标业务系统存在未授权访问问题，未授权访问多因对外部接入的安全配置或权限认证相关策略设置存在缺陷。授权页面存在缺陷导致攻击者可以直接访问系统，变更系统权限，造成数据库或网站目录等敏感信息泄露，未授权访问漏洞利用成为了外部突破的重要途径之一。

5、内部业务网络缺乏纵深防御机制

本月任务中发现目标网络缺乏纵深防护机制。主要表现为从外部突破进入目标内网后，内网安全部署缺乏功能域划分、Vlan隔离等措施，尤其是核心业务系统强防护或隔离措施极少。纵深防护机制的缺乏会导致目标核心业务安全防护非常脆弱。

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。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，从而导致应用系统版本更新不及时、安全策略设置不严格等问题。

2、口令爆破

本月任务中因目标外网防护相对严密，互联网侧系统应用弱口令情况很少发现，弱口令或口令复用问题主要存在于内网，常见问题为未修改安全应用默认口令、多台设备管理员账户口令相同。弱口令或口令复用为内网渗透拓展带来极大的便利。

3、隐蔽隧道外联

本月任务中因客户行业特殊，业务内网均无法直接从外网直连访问，需要借助端口转发、隧道技术等手段实现转发通信，对于网络功能区划分严格、核心业务隔离措施完善的内部网络，往往需要借助多层隧道转发才能实现对目标核心业务内网的渗透拓展。

4、钓鱼攻击

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，主要是由于金融、运营商、电网这类目标客户网络相比其他行业具有更高的安全要求，整体网络外部安全防护相对严密，对其内部网络安全意识比较薄弱的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。

四、典型攻击手段实现案例

1、外部漏洞利用突破

（1）某金融目标业务系统存在远程代码执行漏洞，攻击者通过该漏洞利用获取业务系统管理员权限，进入业务系统管理界面，对 28 个项目共计 1133 个 api 接口进行操作，可获取相关项目的敏感数据。

（2）某目标人力资源管理系统存在 CVE-2020-14882 漏洞，通过该漏洞打入内存马，并成功获取到服务器控制权限。

（3）某目标管理系统存在 S2-016 命令执行漏洞，可通过漏洞利用获取 2 个数据库、9 台内网服务器管理权限，其敏感数据达 2 万余条。

2、钓鱼攻击

（1）通过向某目标子公司邮箱发送钓鱼邮件，最终上线 3 台终端，成功进入到办公网，并在终端上发现了大量的账号、密码等信息。

（2）某目标针对客服钓鱼，获取客服业务服务器控制权限，成功进入目标内网。

（3）对某目标网络以业务投诉为理由对其微信客服进行钓鱼攻击，控制目标客服人员主机，从中获取大量内网系统信息。

3、口令爆破

（1）某目标网络内网堡垒机存在弱口令，通过弱口令登录获取该堡垒机控制权限，可直接控制 1 万余台服务器。

（2）某目标培训考试系统存在弱口令，可直接登录该系统，并进一步获取内网办公业务人员姓名、电话、身份证号、地址等敏感信息。

（3）某目标监控系统存在弱口令，可直接登录访问该系统，可查看大量网络设备和网络架构信息。

政策篇

国内，《工业和信息化领域数据安全管理办法（试行）》《互联网信息服务深度合成管理规定》等多个政策文件公开征求意见，网络安全监管进一步细化；

国际上，美国政府零信任战略正式落地，白宫管理和预算办公室、司法部先后发布联邦、部委级推进计划。

《关于进一步规范移动智能终端应用软件预置行为的通告》公开征求意见

2022 年 2 月 18 日，工信部信息通信管理局发布《关于进一步规范移动智能终端应用软件预置行为的通告（征求意见稿）》，公开征求意见。《通告》提出，生产企业应确保除基本功能软件外的预置应用软件均可卸载，并完善移动智能终端权限管理机制，提升操作系统安全性，采取技术措施预防在产品流通环节发生置换操作系统或安装应用软件的行为。

工信部《工业和信息化领域数据安全管理办法（试行）》再次征求意见

2022 年 2 月 10 日，根据数月前《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》收到的公开意见，工信部进行了修改完善，第二次公开征求意见。修改版的条目由原先的八章四十四条缩减为八章四十一条，主要修改包括：强调个人信息保护、扩充数据定义、明晰监管机构职权范围、对分级分类标准进行微调、明确备案机制、严格主体责任等。

国家标准《App 生命周期安全管理指南》公开征集意见

2022 年 2 月 8 日，信安标委发布国家标准《信息安全技术 移动互联网应用程序（App）生命周期安全管理指南（征求意见稿）》，公开征求意见。该标准提出了移动互联网应用程序（App）生命周期安全管理的建议，适用于 App 开发者对 App 的开发、运营，也适用于移动应用分发平台厂商和移动智能终端厂商对 App 的管理，也可作为第三方机构对 App 进行安全检测时的参考。

《广东省公共数据安全管理办法（二次征求意见稿）》公开征集意见

2022 年 2 月 7 日，广东省政务服务数据管理局发布《广东省公共数据安全管理办法（二次征求意见稿）》。征求意见稿分为总则、基础制度体系、全生命周期数据安全管理、数据安全支撑保障、监督与法律责任、附则共计六章三十二条。征求意见稿规定，公共管理和服务机构应当按照国家网络安全等级保护制度、商用密码应用要求，采取数据脱敏、加密保护、安全认证等安全保护措施，保障公共数据安全。这是极少数专门针对公共数据安全起草的地方性规章。

网信办《互联网信息服务深度合成管理规定》公开征求意见

2022 年 1 月 28 日，网信办发布《互联网信息服务深度合成管理规定（征求意见稿）》，公开征求意见。《规定》明确了深度合成服务提供者主体责任，要求建立健全算法机制机理审核、信息内容管理等管理制度，具有与新技术、新应用发展相适应的安全可控的技术保障措施。《规定》还明确了深度合成信息内容标识管理制度，要求服务提供者通过有效技术措施添加不影响用户使用的标识，依法保存日志信息，使深度合成信息内容可被自身识别、追溯。

美国司法部制定零信任发展路线图，将在三年内落地

据 FCW 2 月 16 日消息，在美国联邦零信任战略发布不足一个月内，作为 SolarWinds 事件的重要受害者，美国司法部率先推出了零信任落地三年路线图。司法部副首席信息官 Kevin Cox 称，此次零信任迁移是司法部内部的“重大行动”。这套基于身份的零信任架构计划分为六步实施，预计在 2024 年实现完全部署。

NIST 发布《软件供应链安全指南》

2022 年 2 月 4 日，美国国家标准与技术研究所（NIST）发布了关于确保软件供应链安全的指南文件，以响应拜登政府旨在加强国家网络安全的行政令（EO 14028 第 4e 节）。NIST 建议向美国政府提供 / 销售软件的生产商采取一系列基本的安全措施，包括统一软件供应链报告语言，要求对软件使用和开发方面的安全实践进行证明等。

欧盟提出金融业网络安全事件响应协调框架

2022 年 1 月 27 日，欧洲系统性风险委员会（ESRB）提出了一套新的系统性网络事件协调框架，希望帮助欧盟在应对欧盟金融部门的重大跨境网络安全事件时能够更好地进行协调和响应。ESRB 是一个独立的欧盟机构，负责监督欧盟金融系统，以预防和缓解系统性风险。三大欧洲监管机构（欧洲银行管理局、欧洲保险和职业养老金管理局、欧洲证券和市场监管局）宣布采纳 ESRB 的建议，并呼吁逐步建立泛欧系统性网络安全事件协调框架（EU-SCICF）。

美国正式发布联邦政府零信任战略

2022 年 1 月 26 日，美国白宫管理和预算办公室（OMB）发布备忘录 M-22-09《美国政府全面转向零信任网络安全原则》，作为联邦零信任战略的落地文件。备忘录要求，联邦政府在 2024 财年前满足必要的网络安全标准和目标，以实现零信任安全架构防护体系。零信任战略的核心要素包括：通过强大的多因素身份验证机制改进网络钓鱼防御水平、整合各机构身份系统、加密进出流量、将内网环境视为不受信环境、加强应用程序安全以更好地保护数据内容等。

英国政府发布《国家网络安全战略：2022-2030 年》

2022 年 1 月 25 日，英国政府发布《国家网络安全战略：2022-2030 年》，阐释了应对网络威胁的策略，并描绘了战略愿景，即确保政府核心功能对网络攻击具有韧性，使英国成为一个民主、负责任的网络强国。《网络安全战略》分别从背景、方法、网络安全风险管理、网络攻击防御、网络安全事件检测、网络安全事件影响控制、网络安全知识技能及文化培养、成果评估及战略执行九个方面对战略进行了全面描述。

政策解读

循序渐进：工信部再次征求数据安全管理办法意见

作者 汉坤律师事务所 段志超 蔡克蒙

2022 年 2 月 10 日，根据 2021 年 9 月 30 日公布的《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）（简称《管理办法》）收到的公开意见，工信部对该法规草案进行了修改完善，再次面向社会征求意见，反馈截止时间为 2022 年 2 月 21 日。

2021 年以来，针对如何落实《数据安全法》，以及《个人信息保护法》，工信部和网信办分别出台了具体的实施细则，并侧重于不同领域。

针对工业和信息化领域数据安全管理，工信部出台了上述《管理办法》，对接《数据安全法》等法律法规要求，在工业和信息化领域对国家数据安全管理制度进行细化，明确开展数据分类分级保护、重要数据管理等具体要求，构建工业和信息化领域数据安全监管体系。

针对网络数据，网信办于 2021 年 11 月 14 日，公布了《网络数据安全管理条例（征求意见稿）》（简称《数安条例》）。该条例针对《数据安全法》和《个人信息保护法》中的相关制度设计了实施路径；针对上位法中的相关要求进行细化和明确；并创设增加了一些新的要求，如重要数据处理者备案要求和年度报告要求、数据出境安全管理义务、网络平台责任等。

目前《管理办法》和《数安条例》均处在编写阶段，二者作为数据安全领域的两大主要监管部门工信部和网信办分别出台的实施细则，虽然部分内容存在交叉，但同时也强调了与数据本身属性相关的监管内容，潜在地为工信部和网信办之间的监管范围和路径进行了区别。

修改后的《管理办法》条目由原先的八章四十四条缩减为八章四十一条。

《管理办法》主要修改内容有：

· 强调个人信息单独保护：新增《个人信息保护法》作为目的依据。

· 扩充数据定义：将无线电数据纳入适用范围。

· 明晰监管机构职权范围：明确工信部对地方监管部门的督促指导作用。

· 修改分级分类标准：判定标准和细分标准发生变化。

· 明确备案机制：补充备案申请、审批、变更相关要求。

· 严格主体责任：法定代表人负责制，加强内部管理。

· 更新全生命周期合规要求：取消核心数据不得出境，新增核心数据跨主体处理要求。

· 统筹协调数据安全审查：灵活化安全评估、监督协助等要求。

我们将在下文对比《管理办法》（2021 版）和《管理办法》（2022 版），梳理此次修订的重要内容，并同时提出我们的解读。

一、强调个人信息单独保护：新增《个人信息保护法》作为依据

在《管理办法》（2021 版）的起草说明中曾强调，《管理办法》秉承《数据安全法》将个人信息纳入重要数据目录和核心数据目录进行重点保护的工作理念，将个人信息纳入数据全生命周期安全管理，不再单独提出个人信息保护的要求。因此《管理办法》（2021 版）将《网络安全法》《数据安全法》作为上位法基础，但并未提及《个人信息保护法》。

但在此次最新发布的《管理办法》（2022 版）中，新增了《个人信息保护法》作为目的依据，并且在具体条款中也调整了关于个人信息的规定，例如：

· 在第八条【分级分类方法】的数据分类类别列举中，删除了“个人信息”的表述，保留了原先的管理数据、运维数据、研发数据等非个人信息；

· 在第八章附则中新增第三十七条【个人信息保护】，“开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。”

综上可见，《管理办法》（2022 版）调整了对于个人信息的规制思路，由原先的“纳入重要数据目录和核心数据目录统一管理”到强调个人信息的单独保护。此变化是为了与此前发布的相关法律文件形成统一。

在《管理办法》（2021 版）发布后，2021 年 11 月 14 日《数安条例》公开向社会征求意见，其中明确了重要数据和核心数据的定义，并不包含个人信息。此外，无论是 2021 年 9 月 23 日全国信息安全标准化技术委员会秘书处发布的国家标准《信息安全技术 重要数据识别指南》征求意见稿（简称《指南》）第一版，还是 2022 年 1 月 13 日发布的《指南》修订版，其中，重要数据的定义中，均明确说明“重要数据不包括国家秘密和个人信息，但基于海量个人信息形成的统计数据、衍生数据有可能属于重要数据”。为实现法律规定的统一协调，此次《管理办法》（2022 版）中改变了对于个人信息管理的思路，强调《个人信息保护法》作为个人信息保护基础性法律的作用。

二、扩充数据定义：将无线电数据纳入适用范围

《管理办法》（2022 版）在第三条数据定义中修改了如下表述。

· 明晰了工业和信息化领域数据包括三类：即工业数据、电信数据和无线电数据。

· 删除行业领域的具体列举：在《管理办法》（2021 版）中，对工业和信息化领域进行了列举，如“原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等行业领域”。但是在《管理办法》（2022 版）中，删除了列举表述，而是用“工业和信息化领域”作为统称，此修改更有抽象概括性，避免了无法穷尽列举和实践变化导致的法律不兼容问题。

· 新增无线电数据的定义：即“无线电数据是指在开展无线电业务活动中产生和收集的无线电频率、台（站）等电波参数数据”。《管理办法》（2022 版）在定义条

款中将无线电数据纳入适用范围的同时，还对应修改了配套制度，例如，新增“无线电频率、台（站）使用单位”作为工业和信息化领域数据处理者；新增无线电管理机构作为监管机构之一；将电磁所受影响纳入重要数据与核心数据判定标准。

三、明晰监管机构职权范围：明确工信部对地方监管部门的督促指导作用

《管理办法》（2022版）中对中央和地方主管部门的职权进行了进一步明晰。

· 中央层面：要求工信部的监督管理活动需遵守国家数据安全工作协调机制统筹安排。此前提的补充是为了解决此前数据监管“九龙治水”的局面，强调数据安全工作的统筹协调。

· 地方层面：《管理办法》（2021版）中并未明晰层层监管的架构，尤其是中央层面对地方层面的监督。《管理办法》（2022版）进行了修改，明确了工信部负责督促指导各省、自治区、直辖市及计划单列市、新疆生产建设兵团的地方工业和信息化主管部门、地方通信管理局和地方无线电管理机构；由地方工业和信息化主管部门、地方通信管理局和地方无线电管理机构负责监督本地区的数据处理活动。

· 强调上述行业（领域）监管部门需依照有关法律、行政法规的规定，依法配合有关部门开展的数据安全监管相关工作。

四、修改分级分类标准：判定标准和细分标准发生变化

《管理办法》再次重申了《数据安全法》确立的数据分类分级管理要求，在《管理办法》（2022版）对分级分类工作要求、方法、一般数据、重要数据及核心数据判断标准进行了修改调整。主要体现在以下方面。

· 工作要求：《管理办法》（2022版）中将【分级分类工作要求】提前到第七条；地方工业和信息化主管部门、通信管理局、无线电管理机构新增了重要数据和核心数据具体目录上报更新义务；删除了企业应当坚持先分类后分级的工作方法。

· 分级分类方法：补充新增工业和信息化领域数据处理者可在一般数据、重要数据和核心数据三级基础上细分数据的类别和级别。

· 判定标准：取消“恢复数据或消除负面影响所需付出的代价程度”作为一般数据或重要数据的判定标准；在核心数据判断标准中，新增无线电数据场景。

然而，此次修改并未对“重大影响”“严重影响”“重大损害”等判断因素进行量化，故企业如何在实践中落实重要数据和核心数据的分级分类工作，仍有待主管部门提供更明确的指引。

五、明确备案机制：补充备案申请、审批、变更相关要求

《管理办法》（2022版）在《管理办法》（2021版）的基础上，针对重要数据和核心数据目录备案义务进行了进一步细化和明晰，具体表现如下。

· 备案机构：明确工业和信息化领域数据处理者应当将本单位重要数据和核心数据目录向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）备案。

· 备案内容：调整了语言表述，对原先备案内容进行了更为严谨的整合；并明确备案内容不包括数据内容本身。

· 备案审核时间：要求地方工信部门、通信管理局、无线电管理机构在工业和信息化领域数据处理者提交备案申请的二十个工作日内完成审核工作。

· 审核结果：予以备案应发放备案凭证，同时将备案情况报工信部；不予备案的应当及时反馈备案申请人并说明理由。

· 备案变更要求：重要数据和核心数据的类别或规模变化30%以上的，或者其他备案内容发生重大变化，工业和信息化领域数据处理者应当在发生变化的三个月内履行备案变更手续。

· 更新备案要求：销毁重要数据和核心数据需要向工信部门、通管局、无线电管理机构更新备案。

六、严格主体责任：法定代表人负责制，加强内部管理

《管理办法》（2021 版）中明确了企业落实数据安全管理义务的第一步是建立健全数据安全组织架构，并进一步要求企业党委（党组）或领导班子对数据安全负主体责任、主要负责人是数据安全第一责任人、分管数据安全的负责人是数据安全直接责任人。

而《管理办法》（2022 版）对原来的第十三条【主体责任】、第十四条【工作体系】、第十五条【关键岗位管理】和第十六条【数据收集】进行了整合，修改删减为第十三条【主体责任】。在内容上也进行了相应调整。

· 确定法定代表人负责制：将“本单位党委（党组）或领导班子对数据安全负主体责任”改为“本单位法定代表人或者主要负责人是数据安全第一责任人”。此调整更符合法律责任要求，党委或领导班子是行政上的设计，无法适用于所有的企业，但是法定代表人是公司法制度的核心设计，体现了责任的承担，更适合担任数据安全责任人。

· 严格内部管理制度：针对重要数据和核心数据处理者，新增要求“建立内部登记、审批机制，对重要数据和核心数据的处理活动进行严格管理并留存记录”。

对于可能处理重要数据、核心数据的企业，需要密切关注此项调整，进而重新设计内部组织架构，可能承担责任的法定代表人、主要负责人、直接责任人及关键岗位人员需提高数据合规重视度，积极参与数据安全的各类培训，提升数据治理专业能力。

七、更新全生命周期合规要求：取消核心数据不得出境，新增核心数据跨主体处理要求

《管理办法》（2022 版）针对数据全命周期的不同环节，再次更新了适用各级别数据的通用要求，以及处理重要数据与核心数据应遵守的额外要求。如下合规变化值得企业关注。

· 数据存储：新增存储重要数据和核心数据的，需定期开展数据恢复测试。

· 数据使用加工：删除“未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动”。

· 数据公开：删除“对涉及个人隐私、个人信息、商业秘密、保密商务信息不得公开”。

· 数据销毁：新增“销毁重要数据和核心数据的，应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）更新备案”。

· 数据出境：取消核心数据不得出境的要求，统一核心数据和重要数据出境监管要求，即确需向境外提供时，应当依法依规进行数据出境安全评估。

· 核心数据跨主体处理：新增第二十四条，要求跨主体提供、转移、委托处理核心数据的，应当评估安全风险，采取必要的安全保护措施，并经由地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报工信部。工信部按照有关规定进行审查。

· 用户权利响应：《管理办法》（2021 版）中第二十九条【举报投诉处理】中曾要求“工业和电信数据处理者应当建立用户投诉处理机制，公布电子邮件、电话、传真、在线客服等便捷有效的联系方式，配备受理用户投诉的人员接收数据安全相关投诉，并自接到投诉之日起 15 个工作日内答复投诉人”，此为强制性义务。但是在《管理办法》（2022 版）中删除了该表述，并改为了“鼓励工业和信息化领域数据处理者建立用户投诉处理机制”，减轻了数据处理者应对用户投诉的合规义务。

八、统筹协调数据安全审查：灵活化安全评估、监督协助等要求

根据此前的《管理办法》（2021 版），国家通过数据安全检测、评估、认证，以及监督检查、安全审查，落实数据安全监督管理。企业需要履行开展安全评估、协助监督检查及通过数据安全审查的合规义务。

此次，《管理办法》（2022 版）对第五章【数据安全监测、认证、评估管理】和第六章【监督检查】进行了灵活化调整，主要体现在以下方面。

· 放宽认证机构管理：此前《管理办法》（2021 版）第三十二条明确要求工业和信息化部和地方监管部门建立数据安全检测、评估与认证机构管理制度，制定机构认定标准，开展机构选拔认定、资质授权、日常管理和推荐目录发布等工作。但《管理办法》（2022 版）中删除了由监管部门开展机构选拔及资质授权的要求，改为了“工业和信息化部鼓励、引导具备相应资质的机构，依据相关标准开展行业数据安全检测、认证工作”。

· 取消一般数据处理者的自评估要求：《管理办法》（2021 版）第三十三条鼓励一般数据处理者开展安全自评估，但是在《管理办法》（2022 版）中删除了该表述，仅强调重要数据和核心数据处理者应自行或委托第三方评估机构展开评估。

· 取消预留检查接口要求：《管理办法》（2021 版）第三十四条规定，企业有配合行业监管部门开展监督检查、并预留检查接口的义务。对于企业而言，主管部门可通过检查接口访问并审查的数据范围、接口的技术标准与调用条件，可能是企业最为关心的事项。但在《管理办法》（2022 版）中删除了预留检查接口这项要求，仅为笼统地要求企业配合监管部门检查。

· 统筹协调数据安全审查：《管理办法》（2021 版）第三十五条规定，工信部在国家数据安全工作协调机制指导下，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查。另一方面，2022 年 1 月 4 日，网信办、中国证券监督管理委员会等十三部委正式联合出台了修订后的《网络安全审查办法》，将数据处理活动纳入了审查范围，其中“核心数据、重要数据或者大量个人信息被窃取、泄露、毁损及非法利用、非法出境的风险”是网络安全审查重点评估的因素。可见，若依据《管理办法》（2021 版）则数据处理者会同时面对基于工信部《管理办法》与网信办《网络安全审查办法》的双重审查。此次《管理办法》（2022 版）中删除了“对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查相关工作”的要求，仅强调工信部需在国家数据安全工作协调机制指导下开展数据安全审查工作，对未来工信部和网信办如何统筹协调数据安全审查保留了灵活性。

九、结语

本次《管理办法》（2022 版）修改内容较多，除了以上重要实质合规义务的修改，在语言表述及法律责任承担上也进行了调整（如删除了将数据处理者的安全管理责任纳入信用管理和失信名单的要求）。此次调整体现了《管理办法》与相关法律法规的统筹协调，修正了相关概念表述，灵活调整了监管和合规思路。《管理办法》作为工业和信息化领域数据安全管理的顶层设计，提出了多项新增和细化的合规要求，建议工业和信息化领域数据处理者密切关注。

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

奇安信图书馆

国际经验分享系列

网络安全科普系列

网络安全认证系列

网络安全实战系列

网络安全教育系列

扫码购书

奇安信致力于网络安全科普、教育、认证与实战，基于国内外先进实践及理念，编撰并翻译系列网络安全丛书。

“零事故”打破奥运网安“魔咒”

—— 奇安信冬奥网络安全保障揭秘

冬奥会全球瞩目，是黑客团伙垂涎的攻击目标。里约奥运会发生奥运相关组织数据泄漏；平昌冬奥会发生世界级网络安全事故，导致互联网和广播系统中断、 奥运会网站瘫痪。作为奥运会历史上首家第三方网络安全服务商，奇安信却创造出北京冬奥会“零事故” 的佳绩，这是如何做到的?

齐向东的虎年新年

作者 公关部 庞悦宁 李恩达

在奇安信掌门人齐向东的世界里，这个壬寅虎年春节，注定忙碌而紧张。

不仅是齐向东，对所有奇安信人来讲，这个春节都注定不平凡。作为北京 2022 年冬奥会官方网络安全赞助商，奇安信在这个春节护航冬奥会网络安全。竞技赛场之外，在这个网络安全的“隐形赛场”上，攻防两端的高度对抗弥漫着看不见的硝烟。对齐向东和奇安信来讲，必须赢，是一种责任，更是一场考验。

一、火炬手与开幕式：光荣的冬奥瞬间

2 月 8 日，谷爱凌首秀夺金，全民沸腾，冬奥会各项赛事仍然在火热进行中。对于此时的齐向东而言，奇安信已经至少拥有了两个光荣的、值得被铭记的瞬间，一个是他与其他 7 名奇安信人一起成为火炬手，另一个是冬奥开幕式网络安全保障任务的零事故。

“当接到奥运圣火，手握火炬时，我觉得自己的心也被点燃了。”2 月 2 日，大年初二下午，在北京石景山的冬奥公园中，齐向东身着白底、红黄两色纹样的火炬手制服，高擎“飞扬”火炬奔跑。

圣火象征着光明、团结、友谊、和平与正义。这和网络安全从业者始终追求的最高理想不谋而合。齐向东在火炬传递现场接受采访时表示：“我从事网络安全工作，我想在自己的专业领域弘扬奥运精神，传承中国精神，刻苦努力、勇于创新，用敢想、敢干、敢赢的劲头创造更优秀的成绩，为国家安全建设经济发展贡献一份绵薄之力。”

在传递火炬后，齐向东又回到了奇安信网络安全保

障指挥中心，开始为冬奥会开幕式的网络安保备战，迎接两日后的开幕式大考。

4 日，齐向东早早就来到公司，密切关注各个场馆网络安全一线的工作情况。冬奥开幕式参与人员众多、构成复杂，运用了丰富的科技手段，每个细小环节，都可能带来严重的网络安全隐患。为了保障开幕式，乃至此后比赛的网络安全，作为奇安信冬奥保障团队的总指挥，齐向东必须要对 3 大赛区，近 40 个场馆的排兵布阵、网络安全建设情况了熟于心。近一个月来，他每天晚上 9 点都要和 60 多个冬奥重保任务的分管人员开协调会，直到深夜。

开幕式当晚，奇安信安全中心大楼灯火通明，冬奥网络安全保障指挥中心弥漫着紧张的气氛。奇安信网络安全保障指挥中心，是保卫冬奥网络安全的重要“神经中枢”，也是各种网络安全专业兵种联合作战的参谋部。这里能协同联动冬奥网络安全的各个驻点，24 小时全天候地监测、研判、阻断和处置威胁，全方位保护冬奥赛事场馆和每个关键环节的网络安全，为冬奥筑起牢固的网络安全防线。

齐向东亲自坐镇，他希望能够通过这样的方式让同事们吃下一颗定心丸，迎接即将到来的压力，分布在各地、各岗位的工程师们正全身心投入到安全运维工作中。两个小时内，工程师们不间断将近千套不同设备，万余台终端及操作系统、数据库系统、业务系统等产生的 1.1 亿条日志等信息，实时进行标准归一化、关联分析、行为分析，进行实时动态、可视化的呈现，对所有攻击行为和异常行为进行预警与处理。

伴随着“飞扬”火炬载着奥运的火种来到鸟巢，国家体育场上空再次迎来礼花绽放。当主持人宣布开幕式结束的那一瞬间，奇安信冬奥网络安全保障指挥中心爆发出欢呼。齐向东激动地向大家宣布：“我们做到了！我们实现了冬奥开幕式网络安全保障任务的零事故！”

热烈的掌声、喝彩声萦绕在耳边，齐向东看着大家的一张张笑脸，心里无比自豪。冬奥开幕式圆满结束，这是奇安信完成的第一场，也是极为关键的一场安全大考。但齐向东也深知，尽管冬奥开幕式奇安信打了一场漂亮的胜仗，但考验还远没有结束。

二、承诺与兑现：向“零事故”目标冲锋

“零事故”，是齐向东和奇安信给 2022 年北京冬奥会和冬残奥会，也是向全国人民做出的网络安保的承诺。从成为奥运历史上第一个网络安全官方赞助商起，齐向东和奇安信开始为网络安全“零事故”的目标冲锋。

齐向东带领奇安信为冬奥这场大考准备了两年多，在奥运会筹办期就介入冬奥会重要设施的规划和建设中，全流程参与冬奥软 / 硬件搭建。奇安信专门为冬奥会系统打造了“全层面管控、全网络防护、全领域覆盖、全周期保障、全线索闭环、全兵种协同”的“六全”网络安全保障框架体系，全力提供奥运标准的网络安全保障。

随着奥运周期进入北京时间，奇安信的各种战前准备接踵而至。两次测试赛、两次技术演练检验、十轮次网络安全攻防演习、三场沙盘推演……所有保障人员提前进入了 7*24 战斗模式。

距离冬奥开幕式 42 天，齐向东宣布冬奥历史上首个网络安全保障指挥中心正式建成。北京冬奥会期间，指挥中心将为北京冬奥会及全国奇安信用户提供全天候、全覆盖、高质量网络安全保障。

距离冬奥开幕式 30 天，奇安信举办网络安全中国代表队百地万人誓师大会。11 支冬奥保障团队从齐向东手中接过战旗，并和多个驻场保障团队、全国 64 个分支机构的代表、上万名奇安信员工，一同庄严宣誓：“我们是网络安全中国代表队，我们宣誓：共同守卫北京冬奥，坚决捍卫网络安全；我们必将听从指挥，坚守岗位，争分夺秒，团结协作，为北京举办一届安全的科技冬奥盛会，贡献力量！”

距离冬奥开幕式 15 天，奇安信开通了北京冬奥会网络安全保障指定号码 95015，这也是我国第一个网络安全服务短号。齐向东在启用仪式上表态，95015 将“永久服役”，奇安信会不断提升服务人员的能力水平、加快应急响应服务速度、强化安全技术支撑能力，坚持用奥运标准护航网络安全。

……

一次次冲锋在前、坚守一线，都是齐向东带领奇安信在“零事故”之路上走出的坚实一步。

冬奥开幕式当天，1500 余位奇安信员工参与了网络安保工作，其中，一线投入 634 人，覆盖指挥中心、近 40 个冬奥场馆及远程监控中心；二线投入 807 人，在远端驻地值守。上千人的付出和心血汇聚起来，实现了开幕式“零事故”的初步目标。

开幕式结束后，所有奇安信人又紧锣密鼓地投入到了一场又一场的战斗当中。在各项赛事成功开展的背后，奇安信人守护着转播的网络安全、守护着重要单位的网络安全、守护着关键系统的网络安全。

2 月 20 日晚，北京将冬奥的接力棒成功交接给米兰－科尔蒂纳，冬奥闭幕式取得圆满成功。这标志着奇安信给北京 2022 年冬奥会的网络安保交上了一份“零事故”的满分答卷。

三、创新与坚守：从 1 个人到所有人的努力

“北京冬奥会的网络安全保卫没有前车可鉴，只有不断创新创造、小步快跑、努力尝试，才能实现动态安全。”齐向东在接受采访时表示，网络安全的底气来自创新。

“创新”是齐向东人生的关键词。从下海经商创办 360，开创网络安全免费时代，再到 2014 年创办奇安信，带领奇安信成为网络安全国家队，与中国电子联手打造“PKS”体系，助力中国走科技自立自强之路。不断创新，用科技为国家、社会创造更大价值，早就融入到了齐向东的血脉当中。

为保障北京冬奥会网络安全“零事故”，奇安信将多

年创新技术研发成果应用于网络安全保障工作，首次将“大禹”安全中台应用于国家级态势感知指挥平台，大幅度提升安全建设、安全管理和安全运行的效率；首次利用人工智能安全分析引擎“Sabre”实现对海量数据的精准告警，实现威胁的智能发现及威胁检测方法的优化；首次全面应用基于指令执行序列检测技术的新一代安全引擎“天狗”，第一时间发现 0day 漏洞并进行封堵；首次在特大型重保活动中落地内生安全情报解决方案，实现情报生产、实时检测、分析协同、研判溯源，为威胁的监测和处置提供强大的信息支持。

创新的背后，是数万奇安信人的努力和坚守。两年多来，奇安信累计投入 3500 人，开展奥运史上首次系统性、全局性网络安全规划，统筹部署冬奥网络安全保障工作，完成了身份、终端、场馆网络安全、态势感知等 8 大防护工程的一体化系统性规划设计和建设；赛事期间，成立了 11 支冬奥保障团队，并设置产品指挥组、一线指挥组、漏洞情报组、支撑保障组等 20 个分组，以及由数百名白帽子组成的冬奥网络安全卫士，7*24 小时监测、研判、阻断和处置威胁。

据奇安信网络安全保障中心统计，在冬奥重保期间，累计发现、修复安全漏洞 5782 个，累计监测到各类网络攻击超过 2.4 亿次（含社会面），跟踪、研判、处置涉奥舆情和威胁事件 105 件，排查风险主机 150 台，发现恶意样本数 54 个。

“零事故，标志着北京冬奥会的网络安全保障全面超过往届，达到了前所未有的高度；零事故也充分证明，奇安信的技术实力是世界领先的，树立了行业新标杆；零事故的成绩，凝聚了你们每一个人的汗水与智慧！”齐向东说，“一起向未来，既是冬奥会与冬残奥会的口号，也是我们未来继续做好网络安全保障的目标。”

这个虎年注定不平凡，虎年伊始，齐向东和奇安信人就迎来了北京冬奥网络安全保卫的关键一战。

这个虎年注定光荣。作为奥运历史上第一个网络安全官方赞助商，奇安信将会向中国和世界展现网络安全的创新实力与底气。

这个虎年注定充满希望。3 月 13 日冬残奥会结束后，奇安信还会迎来无数大大小小的网络安全“战役”，但这个人带领的这群人，有信心、有能力，将继续争分夺秒，与网络安全威胁赛跑，为国家和社会筑起坚固的网络安全防线。

一起向未来！
——奇安信冬奥网络安全保障纪实

作者 公关部 陈冲

“奇安信冬奥网络安全保障圆满成功！”随着冬奥火炬的熄灭，2022 年北京冬奥会落下帷幕，这也意味着奇安信的冬奥网络安保工作圆满结束。

“今天，我们兑现了承诺！”零事故，这是作为北京冬奥组委首次选用的第三方网络安全服务商的奇安信，给北京冬奥会做出的承诺。这一路，也见证着奇安信向北京冬奥会和所有热爱奥林匹克的人们，交出了一份充满科技色彩的“安全答卷”。

“0”事故！冬奥网络安保的荣耀时刻

2 月 20 日晚上 8 点，奇安信大楼内部依然灯火通明。从 2022 年北京冬奥会开幕前起，无数奇安信人就开始为北京冬奥会的网络安全保障默默付出。不一样的是，今晚，他们迎来了冬奥会闭幕式的最终大考。

这一晚，对于所有奇安信人来讲，既充满期待，也依然延续着多日的紧张与忙碌。自冬奥以来，奇安信的工程师们进驻了奥运场馆、关键部门、重要企业中值班值守，为北京冬奥编织了一道网络安全之网。作为 2022 年北京冬奥会安保的收官之战，他们不能有丝毫松懈，需要在这个烟火灿烂的夜晚继续守护 100 度的热情；但令他们高兴的是，距离他们完成冬奥安保任务的目标也越来越近了，他们将创造一段具有奇安信印记的冬奥安保历史。

在北京冬奥组委指导下，奇安信作为北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商，也是奥运历史上的首家网络安全服务商，承担了完全的、彻底的、“端到端”的责任，以网络安全“零事故”为目标，进行系统性、全局性、整体性的网络安全保障体系规划、建设和运营。

“零事故！奇安信冬奥网络安全保障工作圆满成功！”当奇安信集团董事长齐向东在奇安信冬奥网络安全保障指挥中心宣布这个消息时，全场沸腾了，掌声与欢笑让空气中都弥漫着轻松与骄傲。

零事故的背后是一组令人骄傲的数据，它们展现出网络安全赛场的激烈对抗，以及奇安信网络安全战士的坚守。据统计，在冬奥重保期间，累计发现、修复安全漏洞 5782 个，累计监测到各类网络攻击超过 2.4 亿次（含社会面），跟踪、研判、处置涉奥舆情和威胁事件 105 件，排查风险主机 150 台，发现恶意样本数 54 个。

这些成绩，来源于 1500 余位参与冬奥会开幕式网络安保工作的奇安信员工的坚守与付出，不论是在指挥中心、近 40 个冬奥场馆及远程监控中心的 634 位一线人员，还是在远端驻地值守的 807 人，这么多天来，每一个数字背后都凝结着他们的心血。

16 天，冬奥网络安保“隐蔽战线”上的角逐

16 天，是北京冬奥会的周期，也是奇安信冬奥安保战线的作战时间。从开幕式取得零事故的佳绩后，保障冬奥赛事期内“零事故”就成为这群人追求的目标。

“零事故”不代表“零风险”，“零事故”的实现依赖于及时敏锐的威胁感知。不仅冬奥赛场有着令人心跳的激烈对抗，在网络安保这条隐蔽的战线上，一幕幕惊心动魄也在上演。

奇安信威胁分析师 Jack 在排查终端告警时发现一台工作主机频繁访问同一未知 IP，根据这个 IP，他发现了一个钓鱼网站。

网站源代码分析结果显示，在冬奥关注热潮和“一墩难求”的背景下，幕后黑手精心伪造了钓鱼页面，诱使受害者访问该网站，一旦受害者填写注册信息，攻击团伙便可通过钓鱼页面窃取用户姓名、身份证号、手机号、验证码等信息，并将窃取的信息传送回攻击者的服务器中。

并且，该网站还嵌入了一个应用下载链接，用户点击即可下载相关软件。

红雨滴云沙箱软件深度分析结果显示，该软件植入了木马模块，一旦受害者启动该应用，便释放恶意代码，同时绑定其他合法进程，实现持久化利用。此后，奇安信冬奥重保指挥中心开始展开进一步排查检测，排除风险。这样，在电光火石间，在工程师迅速敲击代码的短短时间内，一场危机的苗头便被扼住。

对于工程师们来讲，他们需要一面聚精会神高效率地完成安全保障工作，一面克服疫情、气候条件等客观因素带来的困难，牺牲了春节期间与亲友团聚的时光。

“为冬奥会做网络安保是一份荣耀！”“如果不能参加安保将是一份遗憾”……在《冬奥日记》中，诸多岗位的工程师在讲述自己的光荣与梦想。在“零事故”的目标下，在一份家国情怀与职业使命的加持下，他们坚守在这条“隐蔽战线”上蛰伏、角逐。

800 多天，冬奥科技安保军团的“四大安全”

这是一届充满“科技感”的冬奥会。跨度百余公里的 3 个赛区、26 个场馆，近百个国家数千名运动员，数万名媒体记者、志愿者，数十万观众等，都要依靠互联网进行信息交换、数据存储，开展比赛、训练，进行工作、生活和交流。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。

信息系统规模大、结构复杂、风险点多，北京冬奥会面临的网络安全挑战比历届奥运会大得多，而且没有任何经验可以借鉴。但从成为首家奥运会和残奥会官方网络安全服务和杀毒软件赞助商的那天起，800 多天来，技术能力不断提升、安保经验不断累积、安全理念不断升级，最终铸造了“网络安全铁军”。

800 多天里，奇安信打造了全维度管控、全网络防护、全天候运行、全领域覆盖、全兵种协同、全线索闭环的“六全防护体系”，15 项安全解决方案与冬奥全部 15 个比赛分项有机结合对应，部署包括防火墙等各类安全设备近千套。春节前，所有设备就已投入运转，近万名员工春节假期上班，每天处理超过 40 亿条各类网络安全日志。依靠技术创新和实时响应的能力，冬奥网络安保实现了“经营安全”。

更值得一提的是，奇安信提前规划、参与建设，将“内生安全”从一开始就植入冬奥安保中。网络安保团队提前两年多，在奥运会筹办期，就介入冬奥会重要设施的规划和建设，建立安全标准，全流程参与冬奥软 / 硬件搭建，堵住已知的安全漏洞，定制了奥运专属的网络安全服务。

在此基础上，奇安信建立了联动指挥、三级实战的“全域安全”体系，能够迅速捕捉风险信息，并由专家第一时间分析研判。

此外，为了能吸纳更多网络安全人士，进一步加强冬奥网络安全防护力量，500 名“冬奥网络安全卫士”也加入到冬奥网络安全的队伍中，协助查找冬奥会信息

技术系统的防护短板和漏洞。这一创新机制形成了开放平台、协同保障的格局，实现了“过程安全”。

未来的∞天，创新网络安保在路上

冬奥会的结束，对奇安信的网络安保工作来讲，既是一个结束，也是一个开始。

再过半个月的时间，2022 年北京冬残奥会即将开幕，各个战线的网络安保人员将继续奋斗在工作岗位上，为冬残奥会的圆满召开保驾护航。

而在更长远的未来，如何更好地为国家各类重要项目、关键基础设施的网络安全保障，贡献一份来自奇安信的力量？作为行业领军者，如何更好地推动国家网络安全的建设与进步？这些都成为未来需要长期面临的课题。

“一起向未来，既是冬奥会与冬残奥会的口号，也是我们未来继续做好网络安全保障的目标。”奇安信集团董事长齐向东说，“零事故”标志着北京冬奥会的网络安全保障全面超过往届，达到了前所未有的高度，也充分证明奇安信的技术实力是世界领先的，树立了行业新标杆。

他表示，奇安信将认真总结北京冬奥网络安全“零事故”的经验，未来继续为国家各类重要项目、关键基础设施的网络安全保障，贡献来自奇安信的力量。

冬奥视角下的奇安信防护黑科技
——十五项安全防护技术与冬奥运动项目的映射

奇安信以“零事故”的骄人成绩，圆满保障“冬奥会”成功举办。作为奥运会历史上首家第三方网络安全服务商，奇安信在北京冬奥会网络安全保障过程中，展示了自身作为国内网络安全领军企业的综合实力与众多黑科技。

短道速滑 1 主动防御

短道速滑有着复杂的战术体系，是一项综合考察运动员个人素质能力和集体战术配合的运动项目。运动员要时刻关注对手的动作，既要防止对手压制干扰，又要主动出招争取优势。

网络安全同样需要根据形势，进行主动防御。面对日益严峻的网络安全形势，基础网络设备、域名系统等基础网络和关键基础设施同样面临着巨大的安全风险，各行业的安全防御体系正在从被动防御向主动防御模式转变。

2月5日，中国队获得短道速滑项目混合团体接力冠军。新华社记者杨磊摄

主动防御是一种变相的反制型安全措施，是现代网络技术实现的新型网络安全防御方法，核心在于料敌预先，避免被动挨打、事后补救。主动防御综合运用蜜罐、白名单、样本分析、威胁情报、漏洞挖掘、态势感知等技术，在入侵行为对计算机系统造成恶劣影响之前，及时精准预警，实时构建弹性的防御体系，避免、转移、降低系统面临的风险。

奇安信拥有丰富的主动防御经验，以安全大数据为核心，全面布局主动防御的网络安全体系，满足了客户从以往的“被动防御”转向“主动防御”的建设需求。叠加新IT架构场景需求，围绕上层的身份、数据、应用和行为等构建新的主动防御体系，公司时刻紧跟行业发展和攻防技术演进，已推出了零信任、泛终端、新边界、云安全、态势感知等一系列具备攻防实战化效果的产品，在新细分赛道先发优势不断凸显。

根据IDC的统计，奇安信态势感知、终端EDR、安全资源池等新产品国内市占率均排第一，多款产品位居行业前列。日前，在第二十三届中国国际高新技术成果交易会中，奇安信旗下新一代安全感知系统（简称天眼）、全球鹰网络空间测绘系统和开源卫士系统三款产品，凭借领先的产品优势及技术水平，获评“优秀产品奖”。在“网络安全界的奥斯卡”赛可达实验室发布的2021年度赛可达优秀产品奖（SKD AWARDS）获奖名单中，奇安信天擎终端安全管理系统、奇安信OWL反病毒引擎斩获“企业终端安全”和“杀毒引擎”两项大奖。

速度滑冰 ② 态势感知

速度滑冰作为冰上基础大项，有着“冰上田径”之称。速度滑冰运动员需借助冰刀的刀刃切入冰面形成稳固的支撑点，通过两腿轮流蹬冰、收腿等滑进动作，以及全身协调配合向前快速滑行。

这就要求运动员能够全方位、动态地感知场地环境变化、身体运动状态和装备使用情况，在拥有洞察八方、随机应变的能力的同时，还需快人一步，才能在最终比赛中获得理想的名次，甚至夺冠。

中国选手宁忠岩在北京冬奥会速度滑冰男子 1000 米比赛中。新华社记者王建威摄

“态势感知”一词起源于军事，后期逐渐应用于网络安全领域，描述的是一种基于环境的，动态、整体地洞悉网络安全风险的能力。如今，态势感知已成为网络安全行业中最热门的领域之一，从美国、日本，到中国，各网络大国都纷纷将态势感知上升到国家战略高度。

奇安信的网络安全态势感知平台，以大数据平台为基础，通过数据的收集，利用关联分析、机器学习、威胁情报等技术，帮助政企机构构筑全方位、全天候的网络安全态势感知能力，持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，做到网络安全快一步。

根据 IDC 的统计，奇安信态势感知产品国内市占率第一，位居 IDC MarketScape 模型领导者位置，成为深受业界人士信赖的重要选择。这也是继 IDC《中国态势感知解决方案市场 2019 年厂商评估》报告后，奇安信再次位居中国态势感知解决方案领导者位置。

雪橇 ③ 精准防护

雪橇，起源于瑞士，后逐渐在欧洲、北美和亚洲等地流行，是一个以坐姿开始，以卧姿前进的冬奥体育项目，需要运动员通过精准的身体控制，实现雪橇平衡，以最快的速度到达终点。

2 月 9 日，中国选手黄叶波和彭俊越在北京 2022 年冬奥会双人雪橇项目比赛中。新华社记者孙非摄

由于雪橇在运动过程中最高可达到时速 140 千米 / 小时，因此也被称为是最危险、最刺激、最“卷”的冰上项目。在比赛中，雪橇运动既依赖于运动员自身良好的平衡能力以进行快速冲刺，同时在运动过程中如何进行自身防护也尤其重要，否则一旦发生失误就极有可能导致失控翻车，发生危险。

在网络安全领域，随着数字化的逐渐演进与发展，如何对个人数据信息、企业的大批量数字资产进行及时有效的安全防护尤为重要。在此次被称为“科技冬奥”的北京冬奥会上，各个场馆都配备了先进的数字技术，来自各个国家的工作人员、运动员、志愿者所带入的各类终端也将接入冬奥数字系统，在这整个过程中，如何进一步有效保护数字信息与资产，将是一个重点。

为了实现对冬奥会网络安全保障“零事故”的承诺，奇安信安全防护软件（冬奥版）已于 2021 年投入使用，软件支持汉语、英语、法语等多种语言，优先保证给各个国家参加冬奥的工作人员、运动员、志愿者，以及奥运会举办城市的城市志愿者使用。

软件保留了奇安信天擎业界领先的强安全能力，还重点强化了个人终端关注的隐私保护、卡慢追踪、网络连接管理、攻击溯源、无广告打扰等功能，通过前置的数据准备与分析，对个人电脑进行实时精准防护，对应用程序行为进行精准控制，第一时间遏制最新的病毒木马，分析电脑卡慢的原因，确保电脑系统和数据隐私的安全，并让电脑像赛场上的雪橇一样，始终以最快速度平稳运行。

单板滑雪 4 内生安全

单板滑雪，以一块滑雪板为工具，在规定的山坡线路上快速回转滑降，或在特设的“U”形场地内凭借滑坡起跳，在空中完成各种高难度动作，也被称为“雪上冲浪”。

在 2 月 7 日结束的男子单板滑雪坡面障碍技巧决赛中，中国 17 岁小将苏翊鸣以 88.70 分获得银牌，成为了中国男子单板滑雪第一枚冬奥会奖牌获得者，创造历史；而在 2 月 10 日的女子单板滑雪 U 型池场地技巧决赛中，中国运动员蔡雪桐做出了个人最高难度动作，外转 1080 站立成功，向世界展示了中国单板滑雪运动员的实力。

反抗地心引力、依靠势能和动能的转换控制身体和滑雪板在空中翻转、腾挪，并平稳落地，可以说单板滑雪的至高境界是“人板合一”，那么网络安全的至高境界应该是安全能力和信息化建设合一的“内生安全”。

2019 年，奇安信提出“内生安全”，是指在信息化环境下，内置并不断自我生长的安全能力；2020 年，提出“内生安全框架”，是用系统工程方法，把网络安全能力落地成完整的安全防护体系。2020 年乌镇世界互联网大会上，奇安信内生安全框架荣膺“世界互联网领先科技成果”。

在 BCS 2021 上，奇安信集团董事长齐向东提出了“经营安全、安全经营”，组成了政府和企业实施网络安全的“三部曲”：把内生安全理念，用系统工程方法落地成完整的安全防护体系，最后通过经营安全做到对网络安全的动态掌控。

中国选手蔡雪桐在比赛中。新华社记者牟宇摄

目前，“内生安全框架”已经纳入到上百家央企及重要行业客户的“十四五”网络安全规划中，包括能源、金融、航空等多个重点行业，并获得了用户的极高评价。

冰球 5 联防联控

冰球，是极具观赏性的一种冰上运动，它结合了速度滑冰的灵动和曲棍球运动的精准，也是对抗较强的冰上集体项目，需要不同功能角色分工协作，相互配合，进行灵活的战术调整，联防联控，才能最终赢得比赛。

网络安全同样需要联防联控。奇安信态势感知与安全运营平台（简称 NGSOC）如同“司令部”，一旦发现网络攻击事件，立即快速响应，通过数据联动，将网络中的各个安全软件与安全设备协同起来，实现边界、终端、流量、情报等多种安全要素的自动化联动机制，构建统管全局、联防联控的“积极防御”体系，实现网络安全的全面监测与动态防护。

可以说，构建网络安全联防联控体系，可以实现“一处报警，处处设防；一处威胁，处处处置”，提升整体应对网络攻击能力。而态势感知与安全运营平台在其中功不可没。

2 月 12 日，中国队守门员杰瑞米·史密斯在比赛中防守。新华社记者李安摄

目前，奇安信态势感知与安全运营平台已广泛应用于医疗、交通等重点行业，并多次在国家级重大活动的网络安全保障工作中发挥作用。

钢架雪车 6 安全运行

钢架雪车以是雪橇为工具，借助起滑后的惯性从山坡沿专门构筑的冰道快速滑降的一种冬季运动，也是冬奥会上，最为惊险刺激、危险系数最高的比赛项目。

2 月 10 日、11 日，我国运动员闫文港、殷正参加男子钢架雪车比赛，赵丹、黎禹汐参加女子钢架雪车比赛。其中，闫文港发挥出色，以 4 分 01 秒 77 的成绩获得铜牌。值得一提的是，中国钢架雪车国家队于 2015 年才成立，北京冬奥会是四位选手的冬奥首秀。

因其具有高危险性，该项目曾在冬奥会上被取消过两次，直到 2002 年的盐湖城冬奥会才再次出现，并被一直保留到现在。除了速度快，该项目的风险还体现在运动员需要头部朝前以获得更好的视野、更灵活的操作。因此，钢架雪车必须在追求速度的同时，保证自身安全，保持安全运行。

对于网络空间来说，安全运行是指一个整合相关的流程、技术、人员和服务，对企业和组织中网络空间资产的安全要素信息（资产、弱点、威胁、风险、情报等）进行持续地感知、监测、预警、告警、分析和响应、恢复，并不断优化的过程，是安全保障体系的重要组成部分，是安全管理的基础支撑。

奇安信安全运行服务，以威胁发现为基础、以分析处置为核心、以推动提升为目标。发现威胁，正如在钢架雪车比赛中，运动员需要了解自身优势，观察对手；分析处置即为统筹安排滑行策略；推动提升就像比赛中的不断超越和赛后的反思总结。

在对抗中化解风险、在实战中有效运行。奇安信高速、灵活、流畅的安全运行服务，同钢架雪车全速前行、不惧惊险、沉稳坚守的气质不谋而合，是为政务、公共设施及各行业提供集约、高效的安全运行保障。

2021 年 8 月 30 日，奇安信集团正式发布“数据安全运行构想图”（数据安全 ConOps）。数据安全运行构想图采用系统工程的方法，从数据安全运行视角，以新型数据中心的业务场景为依托，基于业务到技术实现的层次化视角，囊括了数据安全应具备的三个状态：治理态、规划态和运行态，细致展现了数据安全治理结果转化到规划设计、技术落地的过程。

为满足全周期全流程的数据安全需求，奇安信将数据安全运行构想图分为四个层次，分别是数据策略中心层、数据流转管控层、数据应用安全能力层和数据中心安全能力层。

这四个层次涵盖了业务规则、资源流转、应用能力、

2 月 11 日，中国选手闫文港在比赛中。新华社记者孙非摄

产品部署，并与能力框架中的各类策略清晰对应。其中，数据策略中心层重点是健全数据安全管理制度，这就像限制选手运动姿势的赛事规则，而数据应用安全能力层，就像比赛时运动员要穿戴头盔和其他护具保护身体安全，它涉及隐私数据访问，保护个人信息。

随着网络空间安全对抗的持续升级，当前企业和组织的安全运行工作在人员组织、告警处置、快速响应、知识沉淀、整合协作五个方面面临的挑战越来越突出，因此安全编排自动化与响应（SOAR）应运而生，安全运行迎来了 SOAR 时代。2021 年 3 月，奇安信 &Gartner 最新白皮书《安全运行迎来 SOAR 时代》已正式发布。

在以“迈向数字文明新时代——携手构建网络空间命运共同体”为主题的 2021 年世界互联网大会乌镇峰会上，奇安信冬奥网络安全运行指挥中心系统向观众展示了形成威胁风险地图的过程，并将如何处置冬奥期间发生的网络攻击更直观地呈现在屏幕上。这也使观众明白了奇安信是如何将小到一个计分设备、大到一个数据库的运行状态“尽收眼底”，如何有保障冬奥会零安全事故的底气。

高山滑雪 7 应急响应

高山滑雪是勇敢者的运动。在比赛中，运动员要将速度与技巧完美结合，在充满急转弯和高耸跳台的蜿蜒赛道上滑行，凭借纯熟的技术和经验，认真完成每一次回转，不能错过任何一个旗门，尽显高山滑雪的魅力。

如同高山滑雪在保证速度的同时，又不能错过每一个旗门，网络安全应急响应，也要求能力全面，不错过每一处细节。

2022 年 1 月 20 日，北京冬奥会开幕前夕，全国第一个网络安全行业服务短号 95015 正式开通。95015 热线，是全国各地重大网络安全事件应急响应的绿色通道，更是全国冬奥网络安全保障工作中的关键一环，为 5G8K、云上科技冬奥，提供坚强扎实的后盾。

奇安信集团董事长齐向东表示，“95015 是我国第一个网络安全服务短号，是北京冬奥会网络安全保障指定

2 月 10 日，中国选手张洋铭在比赛中。新华社记者陈斌摄

号码，赛后，95015 将永久服役。95015 承载着网络安全行业的责任和使命，北京冬奥会期间，将作为网络安全保障工作的重要支撑平台，为网络安全事件的应急响应开辟一条绿色通道。”

据统计，2021 年，奇安信集团安服团队共接到应急服务需求 1097 起。在事件发生的第一时间，奇安信协助政企机构处理安全事故，确保了政企机构门户网站、数据库和重要业务系统的持续安全稳定运行。

同时，“网络安全应急响应关键技术研究与服务能力建设”项目，通过“指挥中心 – 调度平台 – 应急资源”三级体系，该项目首创网络安全领域“120”服务模式，荣获 2021 年度中国电子科技创新奖（民品）科技进步一等奖。

雪车 8 动态可信

雪车也称“有舵雪橇”，是乘坐可操纵方向的雪橇在冰道上滑行的运动项目。雪车起源于瑞士，由雪橇发展而来，1924 年在法国夏蒙尼第一届冬季奥运会中被列为正式比赛项目。

2022 年北京冬奥会雪车项目的比赛在延庆赛区的国家雪车雪橇中心进行。其中，女子单人雪车是北京冬奥会新增项目，首次参赛的中国选手怀明明、应清表现不俗，

2 月 14 日，怀明明在比赛中。新华社记者孙非摄

以总成绩 4:22.58 和 4:23.41 获得第 6 名和第 9 名。

雪车项目，代表着冰雪赛道上的速度与激情。惊险刺激的赛道转弯表演、高速行驶的技巧展示，给观众带来了感官上的冲击。双人雪车项目，更考验了两位运动员之间的默契配合程度。领航员负责方向把控和动态评估，制动员负责让雪车保持动态前进，两者相互配合，才能保证雪车在槽状滑道内高速前进。

动态可信就是综合多种安全标准对网络安全风险进行信任评估。在网络安全领域，多因子认证系统，就像雪车比赛中的领航员，也需要将多种信任度量进行叠加把控。这是网络安全可信访问控制台系统研发中的重大突破。

奇安信多因子认证，运用于奇安信 ID 智能手机令牌、多因子自身加密口令一次性使用及二维码扫描认证、带外确认，帮助多项功能实现了极致的身份认证安全。它通过持续、动态、无感知的风险与信任评估，实现了安全防控与业务平滑运行的完美平衡。

奇安信可信访问控制台是为了解决在企业应用及 API 服务访问场景下的安全问题而推出的一款创新产品。该平台主要针对多个企业应用及 API 服务的访问控制需求，采用了动态授权、身份认证、风险感知、国密算法等多项核心技术，集中解决企业应用访问场景的核心安全问题。可信访问控制台作为奇安信零信任身份安全解决方案中的核心组成部分，是联动各子系统的控制中心。

零信任作为一种以资源保护为核心的网络安全理念，认为主体访问资源时，主体和资源之间的信任关系都需要从零开始，通过持续环境感知与动态信任评估进行构建，从而实施访问控制。

零信任理念自提出以来，在世界范围内得到了广泛认可。

2018 年以来，奇安信集团率先将零信任安全理念及技术系统介绍到国内，并推出了具备“以身份为基石、业务安全访问、持续信任评估、动态访问控制”四大关键能力的零信任安全架构与整体解决方案。

2020 年，由奇安信集团牵头的《信息安全技术零信任参考体系架构》，在全国信息安全标准化技术委员会成功立项，成为零信任标准层面的首个国家标准。

同年，由奇安信集团完成的“支撑零信任安全架构的人工智能信任决策系统”项目，荣获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）。

北欧两项 9 动态防御

北欧两项，由跳台滑雪和越野滑雪两个比赛项目组成，是最古老也是难度最大的雪上项目之一，自 1924 年首届法国夏蒙尼冬季奥运会中被加入了正式比赛，延续至今。2022 北京冬奥会上，北欧两项在张家口赛区的国家跳台滑雪中心“雪如意”和国家越野滑雪中心进行，共设三枚金牌。

北欧两项从远古时代的滑雪狩猎演变而来，是一场又快又远的角逐。由北欧地区的两个传统项目，融合了速度、力量和勇气的跳台滑雪与考验耐力和技术越野滑雪构成，是对运动员综合能力的考验。

在网络安全行业，动态防御，是指结合业务系统的运行状态与外部环境的动态变化，动态调整网络安全的防御策略与具体安全规则，从而使安全运行充满活力，动态应对各种危机。业务运行与外部环境并重、防御策略与安全规则兼备，是动态防御的内在要求，与北欧两项平衡兼顾的要求不谋而合。

在网络安全等级保护制度 2.0 和关键信息基础设施安全保护制度中，对网络安全提出了“三化六防”的要求，

2 月 17 日，中国队选手赵子贺在跳台滑雪比赛中

即“实战化、体系化、常态化”“动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控”，以此构建国家网络安全综合防控系统，深入推进等保和关基保护的积极实践。

威胁情报作为动态防御的核心能力之一，指明了攻击者的攻击策略、方向、技战术手法以及使用的恶意样本、IP 等网络资源，能够指导组织动态调整防护策略，精准检测已失陷主机。

奇安信威胁情报平台（Threat Intelligence Platform，简称 TIP）为企业提供高价值威胁情报，实施科学、合理、快速的动态防御。威胁情报平台使企业可以在安全建设中方便的利用威胁情报增强自身检测、响应及预防能力，做到精准、全面、及时的发现威胁；快速定性、研判事件，对接用户本地安全设备实现联动管理。

2021 年 12 月，在国际权威机构 Gartner 发布的《Market Guide for Security Threat Intelligence Products and Services》（安全威胁情报产品和服务市场指南）报告中，奇安信凭借旗下威胁情报平台（TIP）、威胁分析和研判平台（Alpha）等多项优势能力，入围该报告。

自由式滑雪 10 隐私计算

自由式滑雪是将高山滑雪和空中技巧相结合的一种极具刺激感的滑雪项目，由空中技巧、雪上技巧和雪上芭蕾三个独立的小项组成。其中，空中技巧小项，一直是中国雪上项目的强项。

2 月 8 日，谷爱凌在自由式滑雪女子大跳台决赛中夺冠，这是北京冬奥会中中国队在雪上项目中夺得的首枚金牌。2 月 14 日，在北京冬奥会自由式滑雪空中技巧比赛中，四次征战冬奥会的徐梦桃以 108.61 的高分获得金牌。

在自由式滑雪比赛中，运动员需要完成一系列高难度的规定和自选动作，因此，只有精湛的技艺，才能让身体在空中自由地翱翔。数字时代，数据也需要更加自由的流动空间，但保护用户隐私数据是数据自由流动的基本前提。

2021 年 4 月 25 日，在福州召开的第四届数字中国建设峰会上，奇安信集团董事长齐向东表示，数字经济这艘大船要想行稳致远，必须兼顾数据流动和数据安全，在保障安全的前提下，对数据价值进行充分挖掘利用。

隐私计算，是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一系列信息技术，是一种实现数据可用不可见、分享数据价值而不分享数据本身的数据安全新理念，是解决数据利用和安全性这对矛盾的重要途径。

数据沙箱技术通过构建一个可信计算环境，使外部程序可以在该平台上进行执行。这样，既可以使用外部程序对数据进行加工处理，也可以保障数据的安全。

奇安信数据交易沙箱，基于调试和运行分离的体系结

2 月 18 日，中国队选手谷爱凌在比赛中。新华社记者肖艺九摄

构，突破多项隐私数据保护关键技术，实现了高效、安全的隐私计算，为网络安全增添了一道新的保障。同时，它存储了各个数据源全量数据，在数据需求方部署隐私保护的前提下，对多个数据源的全量数据进行充分分析和挖掘，数据分析师只能带走不含敏感数据的分析模型文件和分析结果，从而确保数据在流动过程的安全性。

2021 年 12 月 21 日“数据安全产业峰会暨可信隐私计算高峰论坛”上，中国信通院正式公布第 5 批“可信隐私计算评测”结果，奇安信自研的隐私计算产品——奇安信数据交易沙箱顺利通过了“区块链辅助隐私计算”权威评测。同时，奇安信数据交易沙箱也通过了中国信通院组织的第 13 批“大数据产品能力评测”，顺利通过了“可信数据流通平台”权威评测。

为保障冬奥期间的网络安全，奇安信推出了第三代安全防护软件冬奥版，将隐私保护作为核心。当用户对办公、学习等重要文件，以及上网历史记录、聊天软件记录、电子邮件等个人重要信息设置成为特别保护模式时，奇安信安全防护将禁止其他应用软件访问，进而提高保护强度，防止隐私泄露。

花样滑冰 11 智能协同

花样滑冰，将运动技巧与舞蹈音乐有机融合在一起，是最具艺术性和观赏性的冰雪运动。该运动起源于 18 世纪的英国，后相继在德国、北美地区国家迅速开展。

2 月 7 日，中国花样滑冰队获得北京冬奥会花样滑冰团体赛第五名，刷新了中国队在该项的冬奥会历史最好成绩。2 月 14 日，在冰上舞蹈自由舞项目中，中国花滑选手“马达引擎”组合王诗玥、柳鑫宇以总分 184.42 排名第 12，这是中国冰舞的历史最好成绩。

冰上舞蹈同双人滑一样，都要求一位男选手和一位女选手相互配合，这考验了每位选手的个人能力，也考验了两人配合的默契程度。

在网络安全领域，奇安信云边协同智能威胁检测系统也实现了两种技术的“默契配合”。它将云计算与边缘计算有机结合，更好地发挥了大数据与机器学习效力，更高效地检测了复杂可疑的情况，获得了强大的联动防御能力。

2 月 7 日，中国选手彭程（上）、金杨在比赛中。新华社记者鞠焕宗摄

云边协同从数据的可视、可管、可控三个维度，做到对敏感数据的识别、发现和分类分级。云边协同通过加密、脱敏、掩码和授权管理等多种技术对重要数据进行有效保护；通过多因素认证、动态持续认证和访问控制等技术确保合法用户对敏感数据具有合理的授权访问；通过数据边界管理和控制让数据在边缘和云端流转时能够实现数据共享安全防泄漏；通过审计分析确保访问行为与内容的合规性。云边协同智能威胁检测系统能够发现高级威胁，自动更新并响应防护策略，帮客户快速构建基于全网数据检测、响应、追溯闭环处置且满足相关合规要求的安全防护模式。

此前，云边协同智能威胁检测系统为十九大、全国两会、国庆、阅兵、一带一路峰会、达沃斯论坛等重要活动提供了安全保障。2020 年 12 月，由奇安信集团、清华大学和云盾智慧联合完成，奇安信集团董事长齐向东作为第一完成人的“基于云边情报协同的智能威胁检测和分析技术攻关及规模应用”项目，荣获 2020 中国通信学会科技奖二等奖。2021 年 10 月，在以“赋能高质量，打造

新动能”为主题的 2021 全球工业互联网大会上，奇安信云边协同智能威胁检测系统，亮相于国家工业互联网创新发展成果综合展区。

冬季两项 12 整体防护

冬季两项是由越野滑雪和射击两种特点不同的竞赛项目结合在一起进行的运动，最早是由斯堪的纳维亚地区的古代滑雪狩猎活动演变而来。本次北京 2022 年冬奥会的冬季两项比赛在张家口赛区的国家冬季两项中心进行，共产生 11 枚金牌。

由于冬季两项是在茫茫野外的越野雪道中进行，不仅需要充沛的体能，更需要在多个时间段冲刺后的精确射击，这就要求运动员同时具有由动转静与由静转动的能力。

网络空间瞬息万变，这就要求网络安全技术同时具有快速反应与及时处置的双重能力。服务器安全防护作为网络安全防线的重中之重，涉及事前梳理风险点与暴露面、攻击对抗中持续检测与响应、事后精准溯源分析，需要多重措施、层层设防。唯有样样精通，才能做到静态守护稳如泰山，动态防护快如疾风奇安信服务器安全体系就犹如冬季两项运动，动静结合，游刃有余，以出色的整体防护能力，形成闭环式立体防御，为关键服务器系统建立稳固防线。

奇安信服务器安全管理系统椒图，可以助力企业在进行服务器安全建设中及时关注安全左移与应用运行时的安全，同时洞察黑客入侵行为，完成资产发现 – 漏洞检测 – 漏洞利用防护的闭环管理，打造服务器事前防御、事中对抗、事后溯源的内生安全能力。

奇安信统一服务器安全管理系统，是面向政企用户的虚拟化、云、数据中心环境，保护其服务器、虚拟机、云主机、容器等 IT 基础设施安全的产品。产品通过微隔离、入侵防御、恶意代码检测、系统加固等防护方式，可以有效抵御恶意扫描、漏洞利用、病毒传播及东西向移动等服务器安全威胁，并提供服务器安全态势感知及可视化平台，为运营商用户提供服务器安全风险的统一管理和分析平台。2021 年 12 月，网神统一服务器安全管理系统成功中标中国电信发布 IT 通用软件（2021 年）集中采购项目 – 服务器防病毒软件（有代理版）（第二次招标）。

冰壶 13 纵深防御

冰壶，又称为“冰上象棋”，是团队协作进行的投掷类竞赛项目，考验参与者的体能与脑力，展现动静之美，取舍之智慧。比赛时，每场由两支球队对抗进行，双方运动员分别投掷冰壶，运用合理技术将对方石壶击打出大本营，使己方石壶处于更接近大本营圆心的有利位置。

中国选手程方明在冬季两项比赛中。新华社记者彭子洋摄


中国队在女子冰壶循环赛中。新华社记者鞠焕宗摄

大年初二晚，北京冬奥会开幕前两天率先展开的冰壶项目混合双人首轮对决中，组队不满三个月的中国组合凌智 / 范苏圆发挥稳健，通过加赛局 7:6 爆冷击败平昌冬奥会亚军瑞士队，为中国冬奥军团打响头炮。

作为一种攻中有防，防中带攻，充满智慧与趣味的运动，在冰壶赛场上多个冰壶掷出之后，或占位、或得分、或阻挡对手，形成立体纵深防御，和网络安全有异曲同工之妙。

纵深防御的目标是通过层层设防，努力增加攻击者达成攻击目标的难度，需要确保每层防护措施，都知道如何在可疑的攻击事件中采取行动，限制恶意破坏或意外破坏的机会，并最大限度地提升安全漏洞的发现机会与修复速度。

如同冰壶中的“防御球”，在建设纵深防御体系里，构建边界防御是最重要的原则之一，企业通常通过部署防火墙、IDS 等安全设备来实现，所有这些都是为了把威胁挡在外面。

作为中国含金量最高的防火墙测试之一，奇安信连续两年参与中国移动硬件防火墙集采测试项目，并表现优异，连续两年成为唯一入围中国移动硬件防火墙集采项目的独立网络安全供应商。

同时，2021 年上半年，奇安信天眼独家中标了中国移动态势感知一期工程全流量监测项目，与奇安信防火墙等产品联动，共同成为中国移动网络安全纵深防御体系中不可或缺的一部分。

可以说，纵深防御体系的本质是多层防御，使得入侵者必须突破层层堡垒才能接触到核心数据资产。防守方建立起纵深防御体系后，攻击方的入侵难度和入侵成本将大幅度提高，通常远未到终点时就会被发现，这就使得防守方有充足的时间响应和处置。

跳台滑雪 14 分析溯源

跳台滑雪，起源于 19 世纪的挪威，要求运动员加速从高台跃下，在快速下滑中积累速度，在高高跃起的一瞬间，完成一系列高难度动作。1924 年，跳台滑雪被列入冬奥会项目，在北京冬奥会期间，跳台滑雪项目在国家跳台滑雪中心“雪如意”举行，共产生 5 枚金牌。

跳台滑雪的基本技术分为 5 个部分：助滑、起跳、空中飞行、着陆、终止区滑行。由于涉及的技巧多样，因此此项运动不仅是对运动员体能及身体力量的考核，更是对运动员在运动中的运行速度、空中技巧，以及快速反应能力的多重考验。

2 月 15 日，中国选手苏翊鸣在单板滑雪男子大跳台中。新华社记者熊琦摄

分析溯源是应对网络攻击的关键技术能力。正如跳台滑雪的关键动作，需要控制速度、考虑风速、调整好姿势；面对网络攻击，唯有利用技术将威胁进行全面关联与全要素分析，找到源头，才能从根本上阻断攻击、捕获攻击者。

奇安信天眼新一代安全感知系统，对威胁发生的所有线索分析溯源。其基于网络流量和终端 EDR 日志，运用威胁情报、规则引擎、文件虚拟执行、机器学习等技术，可以精准发现网络攻击的入侵行为，利用本地大数据平台对流量日志和终端日志进行存储和查询，结合威胁情报和攻击链分析对事件进行分析、研判和回溯，同时结合边界 NDR、终端 EDR 及自动化编排处置，可以及时的阻断威胁，以帮助客户进行有效防护。

天眼作为奇安信拳头产品，一直备受行业肯定。2021 年 4 月，天眼参与申报的“高级持续威胁 /APT 攻击检测与预防”项目，作为 C5 类别中唯一中国项目，

荣获 WSIS Prizes 2021 C5 类建立使用信息通信技术的信心和安全性“Champion Projects（冠军项目）”奖项；5 月，在数说安全发布的《中国网络安全 APT 检测市场顶级供应商评估报告》中，奇安信凭借天眼产品对 APT 攻击高精度的检测能力、响应能力，以及在 APT 防御方面的创新力和影响力，成功入围中国网络安全 APT 检测市场顶级供应商名单；10 月，在国际权威咨询机构 Forrester 发布的《Now Tech：Network Analysis And Visibility (NAV), Q4 2021》报告中，奇安信天眼成功入选；2022 年 1 月，在第二十三届中国国际高新技术成果交易会中，天眼与奇安信其他三项产品，凭借领先的产品优势及技术水平，获评“优秀产品奖”。

越野滑雪 15 移动安全

越野滑雪起源于北欧，又称北欧滑雪，是世界运动史上最古老的运动项目之一，也是冬奥会传统的雪上项目。1924 年越野滑雪被首次列入冬季奥运会比赛项目。本次北京冬奥会的越野滑雪项目将在国家越野滑雪中心举行，预计在 10 个比赛日内共决出 12 个小项的 36 枚奖牌。

越野滑雪中，运动员需要运用登山、转弯、滑降、滑行等基本技术滑行于山丘雪原，这不仅考验运动员的平衡、耐力和技巧，更考验了运动员对复杂地形的判断力和应对能力。

2 月 16 日，中国选手王强在越野滑雪男子团体短距离（传统技术）比赛中。新华社记者邓华摄

5G 时代，大量移动终端的使用，导致传统的网络边界变得模糊不清、复杂多样。通过移动终端连接企业内网、处理移动办公业务、传播企业数据信息等行为增加大量暴露面，一如越野滑雪中的复杂地形，加剧了企业安全风险的引入。

移动安全也因此成为了网络安全中必不可少的一环。奇安信一直以来深耕移动安全领域，拥有品类全面的移动安全产品与解决方案，旗下的盘古实验室长期致力于信息安全漏洞攻防研究，被称为“移动安全领域的引领者”。

奇安信移动安全管理系统，具有终端强管控和终端强安全等特性的移动终端安全管理产品，为企业提供了安全 IM、安全浏览器等安全办公套件；移动应用自防护产品及移动安全解决方案，可以帮助企业精准调整转换状态，以快速适应复杂的移动环境，通过提供工作专属空间，实现了公私数据隔离，同时配合专有的强项杀毒和二次身份验证，确保了业务数据安全不被泄露；云手机安全管理系统，采用全新的 VMI 技术，将云计算技术运用于网络终端服务，实现了企业所有业务数据均不出数据中心，移动应用和数据均不在终端落地，最大程度保障了企事业的安全移动办公。

奇安信盘古实验室，自成立开始就针对移动安全领域进行研究，研究范围覆盖 iOS、Android、HarmonyOS 等主流移动平台，长期保持对最新 iPhone 破解能力，积累了丰富的攻防对抗经验。其在各类主流操作系统和重要应用程序中发现过大量高价值安全漏洞，也多次在极具影响力的工业安全峰会和顶级学术会议发表前沿研究成果。

2021 年 10 月 17 日，在第四届“天府杯”国际网络安全大赛上，来自盘古实验室的白帽黑客 slipper，完成了 iPhone13 手机的全球首次公开远程越狱，取得手机最高控制权限。被主办方评为“最具价值产品破解奖”，斩获了大赛最高单项奖金 30 万美元；同年 12 月，苹果官方推送了 iOS、macOS、tvOS 和 watchOS 的系统更新，盘古实验室在本次系统更新中贡献较大，共计收获苹果官方的 6 次致谢。安

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

奇安信威胁情报中心

中国威胁情报行业领军者

威胁情报中心

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


曲晓东


齐向东


裴智勇


吴云坤


顾鑫


蒋虎


吴亚东

赛场之外的赛场
——直击北京冬奥网络安保的“隐蔽战线”

作者 公关部

2 月 20 日，2022 冬奥会圆满落下了帷幕。赛场之内，中国队气势如虹，摘金夺银，展现出竞技体育的精彩；而在赛场之外，还有一个“隐蔽战线”：包括北京、延庆、张家口三大赛区数十个场馆，还包括保障冬奥的水电燃气、通信、交通等重要民生机构和关键信息基础设施，都依赖于安全、稳定、可靠的网络平台和信息系统，一场黑客病毒和网络安全守卫者的较量，正在悄悄进行。它关乎冬奥会的安全，更关乎每个人的利益，其激烈刺激程度不亚于赛场之内。

两个赛场，两条战线，一样的惊心动魄，一样的巅峰对决。

0.01 秒，都要全力以赴

0.016 秒绝杀！ 2 月 5 日，短道速滑 2000 米混合团体接力赛中国队夺冠！这是中国体育代表团北京冬奥会的首金，为中国体育代表团赢取开门红！

短道速滑尤其是接力赛，虽以用时短取胜，但更多考验的是队友之间的技术和战术配合……不仅要与时间竞赛，还要考虑策略，随时调整速度和线路，不断在无形的对抗中完成超越！

“就在 2 月 5 日当晚，中国队冲击冠军之时，各个直播转播系统流量激增。我们发现了一次对通信运营商

图：中国队在比赛中 人民网记者 胡雪蓉摄

系统的可疑攻击行为，凭借安服团队和天眼安全感知系统的珠联璧合，仅仅用时 13 分钟，就处理了这起安全事件。” 安全服务子公司白永帅表示。

冬奥期间，运营商承担着通信服务、调度指挥、赛事直播等重任，任何安全事件都可能引发严重的后果。上届平昌冬奥会开幕时，黑客攻击就曾导致互联网和广播系统中断、奥运会网站瘫痪数小时、开幕式直播信号中断等后果。保障通信运营商在冬奥期间“万无一失”，是中国网络安全国家代表队——奇安信奥运网络安全保障团队的郑重承诺。

“运营商资产数量庞大，互联网暴露面多，易被恶意人员攻击，因此，对应的告警数量巨大，这对我们的威胁检测、分析处理、研判甄别、溯源追踪等，都是非常大的挑战。”白永帅表示，因此，“客户对我们人员技能水平要求特别高，本次负责值守的 12 位安全工程师都是经过客户考核通过的人员。”

在冬奥保障期间多次立功的天眼，以攻防渗透和数据分析为核心竞争力，聚焦威胁检测和响应，具备“更高的准确率、更低的误报率”“更强的恶意文件检测能力”“更快的响应处置速度”等优势。尤其在 APT 检测和追踪、威胁情报、协同联动、海量数据的运算和检索等方面，天眼均处于行业领先地位。

短道速滑战术千变万化，像风一样疾驰，决胜在秒的千分位。“时间就是命令！平均检测时间 (MTTD) 和平均响应时间 (MTTR) 一直是衡量安全对抗效果的重要评价指标，更是天眼对自身的要求。”奇安信副总裁、安全攻防 BG 负责人张卓这样表示。“冬奥期间，天眼和公司其他产线多举并措、紧密联动，并与前线安服、应急团队环环相扣、无缝协作，将威胁发现、研判分析、溯源处置等时间压缩再压缩，每一分秒，都会全力以赴。”

图：奇安信奥运网络安全保障团队

图：谷爱凌创造历史 为中国夺得第三金

不仅是安服和天眼，天擎、NGSOC、态势感知、智慧防火墙、云与服务器安全……所有团队都像速滑运动员一样，向更快的极限挑战，在刀尖上焊牢网络安全。对于他们而言，听到告警，如同听到发令枪，全力冲刺，和时间赛跑。

为了 100 分 绝不妥协

“我参加比赛不只是为了击败别人，更要挑战自己，向全世界展现自己的能力。”2 月 8 日，首钢滑雪大跳台，中国队选手谷爱凌在最后一跳开始前成绩暂列第三，是选择稳妥的动作保住一枚奖牌，还是挑战高难度动作险中求胜？场内外观众全都屏息以待。

加速滑行、准备起跳、空中翻转，一个几乎完美的偏轴转体两周 1620 度动作，谷爱凌首次完成了女子大跳台比赛中的最高难度动作后平稳落地。94.50 最高分！谷爱凌征服全场，“一战封神”。

“面对复杂场景带来的高难度与动作零失误这两大挑战，谷爱凌向全世界展现出了自己的实力，正如这场比赛一样，终端安全保障工作经常面临着同样的双重挑战：既要极端时间内攻坚克难，又要确保不能出现任何疏漏，否则会在冬奥环境出现影响业务的重大事故。”终端安全 BG 孙诚这样表示。

首先是难度大、时间紧。尽管孙诚和团队早早就做好了冬奥打硬仗的准备，但这次任务的艰巨仍然远超他们的预期。

“身份查验终端环境非常复杂，几百台身份查验设备分散在北京、延庆、张家口几十个场馆。不同于一般终端，身份查验设备是工控机架构，独特的操作系统和专有配置、专用程序都为产品部署与安全策略的适配工作增加了不少难度。身份查验终端如果出现问题，会导致冬奥运动员、工作人员、嘉宾、观众、车辆等无法正常出入场馆，甚至影响比赛顺利进行，这将是重大事故。同时，这批终端临近‘技术封网’不到一周的时间才开

始大规模部署，给产品容错的时间非常有限。因此，终端安全团队肩上的担子非常之重。”

“最难的一关是针对冬奥环境新设计了多种增强安全防护效果的功能，上线时间十分紧迫。按正常开发排期，至少也得是几个月的时间。可从接到任务开始，留给我们的时间只有不到一个月！”

“在冬奥技术中心的交付现场，为了保证新功能的顺利交付，以及在各类终端稳定运行，从九点到次日傍晚六点，连续 30 多个小时‘熬大夜’是经常事儿。我们抽调骨干、不惜人力的提前组建强大的攻坚专项组，完成这项几乎‘不可能完成的任务’。”

谷爱凌不断挑战自我极限，完成了两次完美且高难度的动作，而另一个隐蔽赛场上一样在追求着“零事故”。

为了达成冬奥网络安全“零事故”这一目标，天擎产品团队联合安全能力中心、威胁情报、反病毒等多个团队，统一组织，7×24 小时值守岗位，打破原有运营方法，将以往以天为单位的安全策略更新缩短至小时级别。极致发挥云安全运营与奇安信威胁情报的优势，对终端安全事件的处理，从发现、研判到响应处置，最快可达分钟级。同时，在产品层面重点保障天擎和各类型终端的兼容适配，以及与其他产品的联动和运行稳定。

在这些高质量、高标准的背后，是以奇安信天擎为主的终端安全管理系统，充分发挥了云安全、核心技术引擎和 EDR 三方面的能力优势，并与奇安信天眼、锡安、NGSOC 等多平台联动，对安全事件形成立体式的处置闭环。

“挑战高难度与零事故，我们一样做到了！这类多种安全产品的大规模协同联动与多团队安全运营的协作模式，放眼整个安全行业也是前所未有的。经历过这种极端场景的考验，终端安全防护整体能力将再上一层楼，也为后续的重保工作积累了宝贵经验。” 孙诚感叹道。

图：中国女冰点球五连扑 铁血防守捍卫冰上荣耀

高手过招 实力才是王道

2 月 6 日，当人们的目光都盯在绝杀夺冠的中国女足身上时，冬奥赛场上，中国女冰同样书写着自己的传奇。

巧的是，中国女冰的开局也十分不顺。频繁的身体对抗，使得前锋张梦莹意外受伤，日本队趁机攻入一球。

顽强的中国队并没有放弃追赶，并在常规时间结束之前由胡宝珍强行扳平，最终比赛被拖入残酷的点球大战。

此时，门将周嘉鹰站了出来，连续扑出日本队 5 粒点球，而中国队员米勒在前 3 粒点球被扑的情况下打进致胜一球，逆转击败日本女冰。

素有“冰上曲棍球”之称的冰球，以激烈的身体对抗而闻名，其程度丝毫不亚于足球、篮球、橄榄球等传统球类运动。在电视转播的镜头中，中国女冰捍卫了冰上运动的荣耀。

在另一个激烈对抗的角落，还有一支队伍守护着网络安全的荣耀。

北京冬奥会的成功举办，不仅仅“捧红”了谷爱凌、陈虹伊等一大批冰雪运动员，还捧红了吉祥物——萌萌的冰墩墩。目前冰墩墩已经脱销，可谓是“一墩难求”。但大批热情的粉丝仍然试图寻找各种渠道，买到自己心心念念的吉祥物。

Jack 正是其中之一。作为中国网络安全国家代表队中的一名威胁分析师，他在排查终端告警的时候，无意间发现了一条线索：有一台工作主机近两天频繁访问一个未知的 IP。经验告诉他，这台主机八成是中招了。

经过 Jack 进一步的调查，这个 IP 指向了一个钓鱼网站。网站源代码分析结果显示，幕后黑手精心伪造了钓鱼页面，诱使受害者访问该网站，一旦受害者填写注册信息，攻击团伙便可通过钓鱼页面窃取用户姓名、身份证号、手机号、验证码等信息，并将窃取的信息传送回攻击者的服务器中。

并且，该网站还嵌入了一个应用下载链接。

“我倒要看看这是个什么木马。”说话间，Jack 上报安全事件的同时，将这款应用投入到了红雨滴云沙箱里。对了，红雨滴云沙箱算得上是样本检测的神器，在多款反病毒引擎和威胁情报的加持下，任何恶意伪装都会被一层层揭开。

果不其然，该软件植入了木马模块，一旦受害者启动该应用，便会释放恶意代码，同时绑定其他合法进程，实现持久化利用。

此时，奇安信冬奥重保指挥中心下来了指示：迅速确定影响范围，排查中招主机情况。

于是，威胁情报团队根据网络资源和文件特征，迅速提取了相关情报，下发至天擎 EDR、天眼等设备，进行检测排查。

“威胁情报的对抗是无声的，但同样也是激烈的。你的对手每天都会变换攻击手法，就像冰球一样，你永远无法预测下一秒会发生什么。但如果不抓住机会主动出击，就永远无法摆脱被动挨打的局面。”

其实，封堵钓鱼网站只是安全工作的冰山一角，网络安全正和人民财产安全密不可分。冬奥期间相关的水电气热、交通、通信等民生机构和关键基础设施，奇安信一直在做着保障。

两个不同的赛场 一个共同的目标

“网络安全一直是奥运会主办国、国际奥委会和商业赞助商关注的重要问题。”北京冬奥组委专职副主席、秘书长韩子荣曾多次表示。截至冬奥闭幕，安全团队未发现一起入侵成功事件，各项水电气热、交通、通信等民生机构和关键基础设施均稳定运行。作为中国网络安全国家代表队，奇安信奥运网络安全保障团队依然高度戒备、严防死守，确保北京冬奥网络安全的全程“零事故”。

一个是全球瞩目下的体育竞技赛场，一个是隐蔽的网络攻防战线，虽然赛场不同，但在这一刻，都只有一个目标——“胜利”。一样在和时间赛跑，决胜每分每秒；一样对高难度与零失误的孜孜追求；一样的攻防较量、巅峰对决……都是为了“安全”“简约”“精彩”的冬奥会努力。背后，是实力、是拼搏，更是使命、担当与责任。安

规划快一步

奇安信 | BEIJING 2022

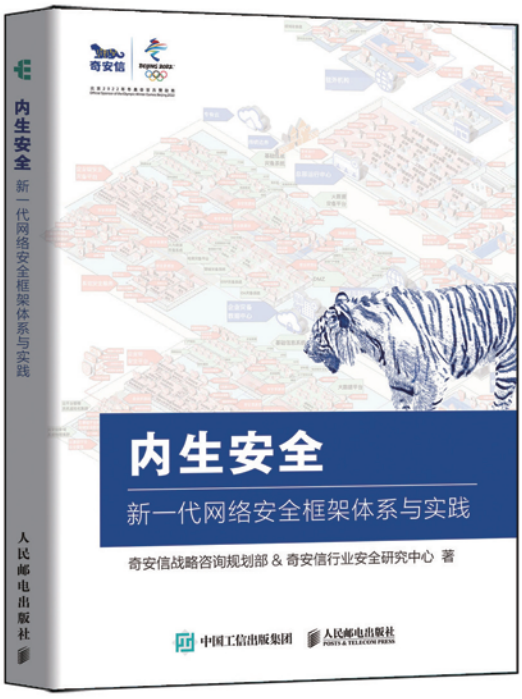
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

知己知彼 严阵以待
——中国电建如何打造网络安全的“眼手脑”

作者 云与服务器安全 BG 李栋

服务器安全建设是个复杂工程，不可能一蹴而就，需要综合考虑服务器自身的环境、应用、业务以及网络等综合环境，也需要对黑客攻击、病毒等安全威胁进行有效预判、监控和防护，由繁入简，通过企业自身的情况有序进行。

“椒图作为一个成熟的服务器安全产品，已经基本满足目前对服务器安全的防护、管理、运维等所需的基本要求，能够对数据、安全性和服务质量得到最有效控制，集安全、管理、运维为一体，管理被防护服务器，进行防护策略配置、安全巡检、防护目标管理、攻击监测日志查看、系统资源监控等。具体使用过程，我们也在和椒图沟通让功能描述更加易懂、最佳实践更加有普适性、从而做到更高级别的服务器防护。”中国石油某一项目组负责人如是说。这是客户与椒图一起打造中国石油服务器安全防线的心路历程，以安全能力为基石，以客户需求为导向，也正是椒图一直信仰的产品哲学。

中国石油天然气集团有限公司（简称“中国石油”，英文缩写：CNPC）是国有重要骨干企业和全球主要的油气生产商和供应商之一，是集国内外油气勘探开发和新能源、炼化销售和新材料、支持和服务、资本和金融等业务于一体的综合性国际能源公司，在国内油气勘探开发中居主导地位，在全球 35 个国家和地区开展油气投资业务。2021 年，中国石油在《财富》杂志全球 500 强排名中位居第四。2020 年，在世界 50 家大石油公司综合排名中位居第三。

作为国家能源行业的支柱企业，中国石油拥有庞大而负载的信息化业务体系，尽管先后部署了多套边界安全方

图：中国石油现代化油田

案，服务器安全风险长期存在：服务器资产不清晰、漏洞补丁更新不及时、系统 & 应用缺乏有效防御、攻击事件不能清晰定位，服务器安全已成为亟待解决的重点、难点问题。通过奇安信网神云锁服务器安全管理系统，实现了对操作系统及应用的安全防护，能有效检测与抵御已知、未知恶意代码和黑客攻击，并融合资产管理、微隔离、攻击溯源、自动化运维、基线检查等强大功能，构建了服务器端的自动化防护体系。

服务器安全痛点明晰

服务器的众多资产无法进行有效收集管控，资产里面的漏洞、配置风险不可知，服务器的口令风险、基线风险不可知，攻击者对服务器发起的攻击不能进行精准溯源分析。针对操作系统不能进行有效加固。具体表现如下。

1. 服务器资产不清晰：由于服务器数量众多，服务器上的应用数量变幻莫测，依靠人工台账统计资产的方式已经不能满足众多的业务需求。

2. 风险隐患无法感知：由于缺乏必要的技术管控措施，中国石油部分服务器的弱口令风险，漏洞风险，基线风险，病毒风险不能得到有效控制，导致黑客攻击的成本很低，而我方却不知黑客是否攻击成功。

3. 内网服务器之间的访问无法得到有效控制：由于服务器之间的访问关系错综复杂，而边界设备只能管控纵向的流量，针对服务器互相访问的情况一无所知，容易造成当黑客攻击进来内网中的任意一台服务器时，轻易就能对同网段内的其他服务器进行横向渗透。

4. 操作系统无法进行加固： 针对比较老旧的操作系统和应用的漏洞，很多厂商早已不支持进行补丁更新，但是黑客可以利用这些漏洞进行恶意攻击。

5. 事件溯源无法精准定位： 对黑客是否攻击成功和黑客的攻击手法操作和路径一无所知，无法进行有效溯源。

对症下药，攻克安全难关

在了解完客户痛点后，解决方案就随之而出，通过部署保护应用系统稳定运行，防止恶意攻击、页面篡改和数据泄密，对操作系统文件、进程、注册表、服务进行保护，还可以对业务系统进行保护，保证系统业务的连续性。通过资产发现与匹配，辅助中国石油快速发现自身系统存在漏洞风险，杜绝被攻击渗透的风险。

1. 服务器资产动态掌握：奇安信网神云锁服务器安全管理系统帮助中国石油自动清点服务器资产状况，快速了解业务系统情况。实时动态掌握服务器资产中存在的各类风险以及暴露的问题，方便中国石油快速检索特定的资产详情或相关风险。

2. 领先的未知威胁响应能力： Rasp 技术：通过 Rasp 技术对应用系统的流量、上下文、行为进行持续监控，识别并防御已知、未知威胁。有效防御 SQL 注入、命令执行、文件上传、任意文件读 / 写、反序列化、Struts2 等基于传统签名方式无法有效防护的应用漏洞。

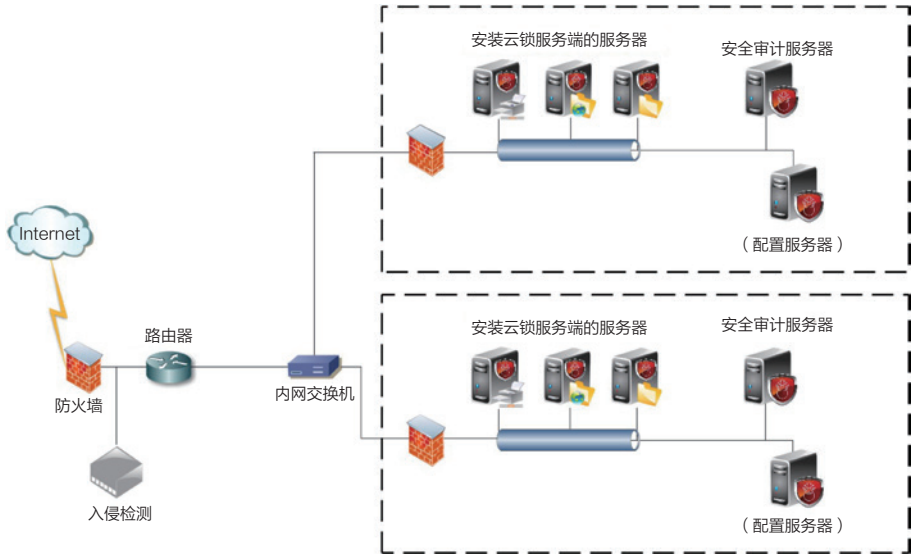
3. 立体化防护：通过持续监控和行为识别为核心，对管理中心平台回传的行为数据进行智能分析，完成对应用攻击的预测、防御、监控和回溯，实现立体化纵深防御体系。

4. 部署方式以及兼容性高：奇安信网神云锁服务器安全管理系统结合客户网络现状，支持外网、内网及混合网络的产品交付。采用业务优先原则，产品以轻量级代理的方式部署到服务器中，占用系统资源少，并支持 Windows Server2003 及以上 Windows 服务器操作系统；支持 centos、Ubuntu、redhat、中标麒麟、红旗 Linux 等超过 280 个 Linux 内核版本。

纵深防御、主动防御，打造能源行业信息安全典范

基于“三化六防中的‘纵深防御、主动防御’”的指导思想，该企业搭建了统一的服务器安全防护体系，实现了从事前资产清点，事中监控 + 防御的纵深监控防御体系，到事后精准溯源。功能通过方便快捷的一体化平台管理。策略通过批量 + 模板 + 单台的下发模式。很大程度提高了安全运营的效率。

技术层面：通过各自集中安装部署 agent, 对中国石油部分关键应用系统的服务器进行集中管控，并通过子账户等权限分配，使各个安全系统管理员可以实时掌握该服



务器的资产变动信息，以及资产是否存在安全隐患等信息，通过动态实时监控管理端服务器的安全事件信息，达到安全运营效率大幅度提供并实时发现服务器发生的可以威胁事件，通过使用 agent 端的操作系统加固等防护能力，大大减少了服务器被入侵的风险。

管理层面： 中国石油将奇安信的服务器安全产品与日志服务器进行联动，统一平台管控，当有安全事件发生时，该日志服务器软件会第一时间发送邮件或者微信给业务部门进行整改，每个月会将整改情况通过邮件发送给主管领导进行公示。

知己知彼，百战不殆

通过奇安信网神云锁服务器安全管理系统为中国石油的服务器监控与防护，更加精准和合理的统计和展现了服务器的事前资产梳理及风险发现，到事中的 Rasp、EDR、操作系统加固和监控等能力，再到事后内核级的事件溯源的处理能力，达到了对服务器端安全管控的重要保障。

1. 资产统一管理： 资产管理功能实现了自动收集服务器上的资产信息包括服务器资产信息、网站资产信息、应用资产信息、数据库资产信息、内核模块信息、环境变量信息、启动服务信息、安装包等信息，帮助中国石油快速了解本应用系统服务器资产情况，同时提供资产搜索能力，方便各项目组快速检索特定的资产详情。资产发现功能帮助各项目组自动扫描所在网络空间未纳入安全管理的服务器，自动排除普通网络设备，保证探测与被探测服务器正常运转。

2. 威胁实时监控： 中国石油部署服务器安全管理系统后，通过威胁监测采用行为学习与监控技术，对恶意扫描、暴力破解、软件后门、Webshell、反弹 shell、本地提权进行实时监测及防护，同时对各类威胁事件的及时处置。此外，提供端口防扫描模式，通过限制单个 IP 单位时间内允许扫描的端口数目，防止了利用端口扫描工具获取服务器敏感信息，当扫描的端口超过设置数目时对 IP 进行锁定。

3. 攻击精准溯源： 当安全事件发生后，系统自动回溯黑客攻击过程、提供攻击过程分析、生成事件分析报告，实现入侵取证。采用行为关联分析方法将访问行为过程中所产生的日志进行综合分析比对，将入侵行为分别以探测、攻击、控制、其他等阶段，并以安全事件的方式发出告警，实时监控记录恶意攻击发生的路径及关键点，利用监控所获取的数据，分析事件完整过程，找出根本原因。日志分析记录当前所有服务器产生的事件日志，并提供筛选的功能和自定义时间段筛选查询，可通过安全日志快速锁定问题服务器，并进行相应处理。

截至 目前，椒图已经完成了中国石油 1、2 两期的服务器安全实施工作，先后对中国石油 3 个重要核心应用系统共计 700 多台服务器进行服务器安全防护，涉及到综合办公系统、桌面安全及门户系统，未来将继续快速推进中国石油的服务器安全建设，为国家能源命脉的信息安全保驾护航。安

奇安信
新一代网络安全领军者

聚焦安全运营，构建智能平台

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

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

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

将平战结合进行落地

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

重大安全事件的威胁预警

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

专业的安全运营服务

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

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一 ——数世咨询认证

用思考，打磨内心的一把“尺”

——奇安信副总裁张庭

作者 公关部 包世玉

“我其实是个追求完美的人，我的眼睛就是尺子。”张庭在聊到一次调整产品界面时，发现其中某个元素偏了一个像素没有对齐，然后硬是让同事改了过来。

但这并不是张庭追求完美主义的唯一体现，在生活中他也同样如此，各类电子产品的数据线都被他用买来的扎带一一缠好，然后分类摆放到收纳盒内。谈起这些生活、工作中的“执念”，张庭说：“其实也不累，把这些弄整齐了，看着舒服。”

若说是这些生活中的点滴小事造就了他这种一丝不苟的性格，那么在工作中，这样的“执念”同样成就了张庭。

2021 年 7 月，张庭在冬奥版软件发布会现场

100 多个版本成就冬奥标准

北京冬奥会在 2 月 4 日开幕，而张庭的“冬奥”则在一年半前就已开始。确切的说，他是在 2020 年 9 月，奇安信上市后接到的第一个任务——打造一款不同于行业现有的具有冬奥标准的网络安全防护软件。

“真的不知道从何入手。我们这个团队已经做了七八年的安全防护软件，闭着眼睛都能把传统的那种防护软件产品图画出来，但这样的产品绝对不是我们想要的，也绝对不是现在新一代客户想要的。”张庭谈起一开始带领团队接手安全防护软件冬奥版项目时，思维的惯性让整个团队都对开发一个颠覆行业对安全防护软件传统认知的产品很迷茫，张庭说：

“这哪里是要做出颠覆行业的产品，这是要颠覆我们自己啊！”

但也正是张庭的团队，在 2021 年成功做出了安全防护软件冬奥版——这个搭载最新技术、具有强烈科技感的产品，成为奇安信在 C 端的创新，也填补了市场中对应产品的空白；现在，这款软件已应用到了所有北京冬奥工作人员、运动员和志愿者的手机上。不过这都是后话。

若让刚刚计算机专业毕业的张庭来想象十几年后的自己在做什么，估计他自己也想象不到。互联网行业龙头不断涌现，网络安全行业形态也有了不小的改变。而张庭也从一开始毕业加入到互联网公司，然后跟着当时的领导进入到 toC 安全行业，再后来转战网络安全领域，自己成为领导带领团队。

这一路走来，从初出茅庐到做出颠覆行业的产品，不知不觉间，学习、升级、迭代、创新，这些其实是他不断颠覆自己思维方式的准备赛，也给张庭在这次带领团队做出冬奥版防护软件，做出了不少认知方式、思维方式以及技术方面的准备。

“一开始确实不太理解，我们一个做 B 端业务做得风生水起的网络安全公司为什么突然要拓展 C 端产品。”张庭坦言，他接到负责冬奥版软件整体研发的任务后，几天都没有想通。但他必须要搞清楚，于是他带着这些问题找到了齐总。

其实仔细想想，传统安全防护软件的痛点不言而喻。时代在发展，网络从 2G 演变到了如今的 5G，手机成为

除电脑外最重要的个人终端，大量的数字资产被各类软件使用，用户对于个人隐私保护的意愿增强；与此同时，捆绑营销早已不适应新一代网民，免费的模式并非真正“免费”，消费者已被这种模式折磨良久；且近些年消费者对于软件付费的习惯也已经被养成，对于能够切实达成效果的软件付费意愿程度很高。

通过这一番沟通与思考，无论是从行业、公司，还是从技术角度出发，张庭都觉得 C 端的安全防护软件行业确实值得颠覆一下。他也相信，无论是自己、团队，还是奇安信，绝对是可以做出行业颠覆的那一个。这样的信念和坚持，在后面也一直支撑着张庭。

奇安信安全防护软件冬奥版界面图

将原因搞清了，下一步就是执行。但就像开头说过的那样，张庭和团队对于安全防护软件有着绝对的经验，但同样，也正是这样绝对的经验困住了他们的手脚。“无论脑子里怎么想象，怎么描画，都还是原来的那一套逻辑、那样的产品。”张庭在最开始和团队沟通时就发现了这个问题，他知道：这样绝对不行。

作为一个产品人，他开始像个产品经理一样思考，如何能够帮助自己和团队跳出以往的思维定式。如果说最终需求是做出一款可以解决目前市场上安全防护软件痛点的产品，那么他们要做的就是找出其中创新的底层逻辑，将需求与最终产品呈现之间的链路打通。

不给自己设限，相信自己的能力，是他那一阵子经常鼓励自己和团队的一句话。最后做出来的时候，整个团队已经大大小小改过 100 多版。“每一版做出来的时候，感觉确实朝着想要的方向进了一步，但好像还是差着一点儿不。只能接着改。”这其中不知道经历过多少次的沟通、磨合、修改。最终一版做出来的时候，张庭一看就知道：

是了，就是它了。

2021 年 4 月，冬奥版软件开始邀请内测，7 月正式发售，北京 2022 年冬奥会期间，已成功交付志愿者等冬奥工作人员使用。

“最终成功兑现了奇安信对冬奥的承诺，我们也兑现了突破自己的承诺。这可能就是我们自己的奥运精神吧！”张庭打趣地说道。

确实，张庭团队在这版软件上充分展现了网络安全的“奥运精神”。

更快——软件提供的“卡慢追踪”功能，可以让用户实时感知应用程序的 CPU、内存、磁盘 IO、数据资产等多维度资源占用情况，通过对比标准数据、历史数据等，找到当前运行卡慢原因，正如奥运选手一样，可以使设备始终保持在最佳状态；

更高——软件同时支持“攻击溯源”功能，详细记录系统和应用软件的行为和事件，有问题可溯源，正如奥运选手在训练中的精准记录，在后续有针对地进行能力提高；

更强——软件在病毒木马查杀的基础上，重点强化了隐私保护能力，并将各类应用的运行和信息收集，以图表可视化的形式呈现给用户；

更团结——软件支持汉语、英语、法语等多种语言，优先保证冬奥的工作人员、运动员、志愿者及奥运会举办城市的城市志愿者使用。在冬奥结束后，也会继续为这些人群提供免费的国际化的冬奥标准服务。

经过不到一年的时间，张庭和他的团队啃下了这根硬骨头——一款拥有超强科技感辨识度、数据透明度高、奥运标准的奇安信安全防护软件被成功打造出来。

他们做到了。

三个月，啃下又一根硬骨头

去年 9 月，在张庭刚刚成功把奇安信安全防护软件冬奥版推行发布之后，又接到了齐总派给他的另一个“难啃的硬骨头”——负责整个天擎的业务。

这又一次难坏了张庭。

如果开发安全防护软件冬奥版是张庭在擅长的领域颠覆自我，那么负责天擎团队这绝对颠覆了张庭一直以来的自我——负责开发冬奥版软件，虽然要颠覆以往的模式，但好在他也有着七八年的经验；又或者说负责另一个产品，作为一个产品人，这些年张庭也是经验颇丰。

但这一次让他接手的，却是天擎整个业务部门，包括业绩。

“刚接到任务时，是 2021 年 9 月，那时天擎 V10 刚推出时间不长，2021 年的业绩完成进度很慢。”从未在奇安信管理过 toB 的业务，也不知道要怎么做，张庭整个人非常焦虑。

但既然接了这个任务，以他追求完美的个性，最终的结果只能是成功。所以接下来的 10 月、11 月、12 月，张庭一心扑在了这个上。

也是那个时候，他发现万事皆可相通。那就还是同一套逻辑：业绩不好，为什么？——先把原因找到。与上次不太相同的是：如果说冬奥版的问题需要向上、向外延寻找，是行业和定位；而这次天擎的问题，则要向内、向根部找寻。

因此张庭带着整个团队先打了 200 多个电话。跟各区域的销售、售前一个个沟通，扎入根部了解需求、了解痛点，挖掘问题到底出在了哪。功夫不负有心人，问题总算被他发现了——

原来在那个时候，天擎 V10 刚刚推出，但很多销售对新产品并不了解，甚至对整个下单的流程都很生疏，所以依然在向客户推荐天擎 V6。再加上大多数交付同事对于 V10 也同样生疏，反馈给销售的意见也是不要推荐 V10。正是这一系列的连锁反应，导致天擎 V10 的销售在一开始就遇到了滑铁卢。

“当时是真的觉得很可惜，天擎 V10 更新换代之后更强，绝对是可以帮助到客户的拳头产品。我们的销售

2021 年，张庭在演讲中

团队一直以来也在勤勤恳恳地努力工作，但仅仅因为新产品推广中间的链路没有打通，才导致了这样的一个结果。”张庭谈起当时的情形非常感慨。

了解到这些之后，他第一时间带领团队前往各区域，与销售、售前进行沟通、培训、讲解。十几场培训下来，确保一线对 V10 有着足够的了解，成果显著。紧接着，天擎 V10 新的营销策略推出，进一步提高了一线销售的动力。随着这一套组合拳下来，一线销售也愿意推、交付也愿意教了。

2021 年年终的这三个月中，张庭带领团队磨下 100 多个成功案例，到年底 100% 达成了业绩目标，最终完成了这个看似不可能完成的任务。

又拿下一根难啃的骨头，张庭的 2021 年充满挑战，但成果也是显著的。

用思考，打磨出内心的那一把尺

对于网络安全行业，张庭也一直在尽自己的努力，向期待的方向靠拢。提起这个，他谈了不少这些年来的观察和思考：“网络安全未来的路很宽很长，我认为我们最重要的使命，就是做那个中间人——在个人和信息使用者之间架起桥梁，但更要架起关隘，通亦要守。”

《个人信息保护法》在 2021 年颁布，张庭作为行业相关方，在法规刚刚颁布时就给出了自己的解读。如果说从他的解读中总结出一个最重要的词，可能就是：透明。

“现在的信息使用太不透明了。很多 App 下载之后都会问你同不同意使用个人数据，但具体同意了什么、同意之后的这些数据将会被如何处置、如果未来不同意以往的数据是否可以被完全撤回——这些都还在飘着。”张庭说了很多，“这也是我们在做冬奥版软件中的目的之一，让数据可视可见，让用户知道自己的数据用在了哪里，这是我们网安人的使命。”

也正是这些思考与实践，让他有了多于常人的积累和沉淀。

如果说张庭的 2021 年可以用惊心动魄来形容，那么 2022 年迎接他的，可能还有更多的挑战——这一次，齐总让张庭接管了整个终端 BG。

“说真的，我最近一直在思考，齐总这次交给我的任务，绝对是对我 2022 年的大考。”张庭望着远方思考，说出了三个词：挑战、压力和探索。

张庭和团队部分成员

其实回看这两年，颠覆、创新——是奇安信的精神内核，是张庭一直以来践行的信念，也是总结张庭工作成果的关键词。而这种种成绩背后的压力、责任与挑战，旁人也同样难以体会。

但张庭以绝对的完美主义要求自己，这样的“执着”也成就了他。无论是颠覆和创新，还是压力和挑战，都帮助张庭不断思考，最终打磨出来他心中的那一把“尺子”。

如果问是谁告诉过张庭，需要改版 100 多次才能成为冬奥版防护软件？

没有。

若说是有谁告诉过张庭要打 200 多个电话才能发现天擎的销售问题？

同样也没有。

而这些问题的答案，可能都来源于张庭内心的那一把“尺子”——来自一个产品人的经验、一位管理者的自信，和一个完美主义者内心的执着和坚持。

行于外，察于内。

这把尺子，不知丈量出多少深夜的思考和颠覆式的自我认知重构。最终，也成功帮张庭丈量出了这些耀眼的成绩。 安

大事记

“零事故”完成北京 2022 年冬奥会开幕式网络安全保障工作

2022 年 2 月 4 日晚，北京 2022 年冬奥会开幕式在万众瞩目中顺利举办。奇安信圆满完成北京 2022 年冬奥会开幕式网络安全保障工作，实现“零事故”承诺。

奇安信集团 1500 余名战士，组成了北京赛区分队、延庆赛区分队、张家口赛区分队等十余组保障中心分队，出色完成了开幕式保障任务，接下来将认真总结北京 2022 年冬奥会开幕式网络安全保障经验，以高标准、严要求做好冬奥会后续各项网络安全保障工作。

奇安信八名火炬手传递光荣与梦想

2 月 2 日，奇安信集团董事长齐向东作为火炬手，在北京冬奥公园参与了北京冬奥会火炬接力。

本次共有八名员工入选冬奥火炬手，火炬手齐向东、吴云坤、曲晓东、蒋虎、齐子昕、吴亚东、顾鑫、裴智勇，分别在北京冬奥公园、张家口、延庆参与奥运圣火传递。

北京西城区领导莅临奇安信等中关村西城园企业调研检查冬奥会服务保障相关工作

2 月 12 日上午，北京西城区区委书记孙军民，区委副书记、区长孙硕到奇安信集团调研检查 2022 北京冬奥会和冬残奥会服务保障相关工作。

调研检查中，区领导通过视频连线形式，向坚守冬奥会网络安全保障一线的工作人员送去诚挚问候，对大家全力护航冬奥会网络安全的辛勤付出表示衷心感谢。区领导聂杰英、王波、桑硼飞和区委办主任夏淑敏、西城园管委会常务副主任袁文一同参加。

在视频连线中，孙军民详细询问一线保障团队人员的工作、生活情况，向他们送去诚挚问候和新春祝福，并对大家全力护航冬奥会网络安全的辛勤付出表示衷心感谢，勉励工作人员展现网络安全国家队的担当，为护航奥运盛会贡献力量，完成光荣任务。区领导还通过红色云展厅、网神洞鉴等项目，了解企业发展和科研攻关情况，鼓励企业继续加大研发投入，推出更多优质网络安全产品和服务。

中国电子芮晓武一行到访奇安信安全中心调研冬奥网络安全保障工作

1 月 30 日，中国电子党组书记、董事长芮晓武，党组成员、副总经理靳宏荣，来到奇安信安全中心的冬奥保障指挥中心，调研北京冬奥会网络安全保障准备情况。

芮晓武一行亲切慰问了坚守在各冬奥场馆及监控保障中心的驻场网络安全保障团队和闭环管理中的一线值守人员，向大家致以节日的问候和新春祝福。

全国第一个网络安全行业服务短号 95015 正式开通

1 月 20 日，全国第一个网络安全行业服务短号 95015 正式开通。95015 是为全国各地政府、企业、相关机构提供网络安全应急响应、合作与咨询服务的电话专线。

奇安信集团董事长齐向东表示，“95015 是我国第一个网络安全服务短号，是北京冬奥会网络安全保障指定号码，赛后，95015 将永久服役。95015 承载着网络安全行业的责任和使命，北京冬奥会期间，将作为网络安全保障工作的重要支撑平台，为网络安全事件的应急响应开辟一条绿色通道。全国的政企机构遇到任何网络安全问题，都可以拨打 95015，奇安信将提供 24 小时

冬奥标准的应急响应服务。”

荣誉墙

奇安信可信浏览器首家获得密码二级认证

奇安信可信浏览器正式获得了由国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》，成为国内首家获得密码二级产品认证的浏览器产品。

此前，奇安信可信浏览器首批获得《商用密码产品认证证书》一级认证，此次认证升级，不仅代表着技术实力上再次得到权威认证，可为用户提供更加安全可靠的


商用密码产品认证证书

证书编号：GM001112220210301

委托人名称及所在地
网神信息技术（北京）股份有限公司
北京市西城区西直门外南路 26 号院 1 号楼 2 层

生产者（制造商）名称及所在地
网神信息技术（北京）股份有限公司
北京市西城区西直门外南路 26 号院 1 号楼 2 层

生产企业名称及所在地
网神信息技术（北京）股份有限公司
北京市西城区西直门外南路 26 号院 1 号楼 2 层

产品名称和型号、版本
奇安信可信浏览器软件（密码模块）

产品标准和技术要求
GM/T 0028《密码模块安全技术要求》第二级要求

上述产品符合商用密码产品认证规则的要求，特此发证。

颁发日期：2021 年 8 月 24 日　　有效期至：2026 年 8 月 23 日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

牛路宏

国家密码管理局商用密码检测中心

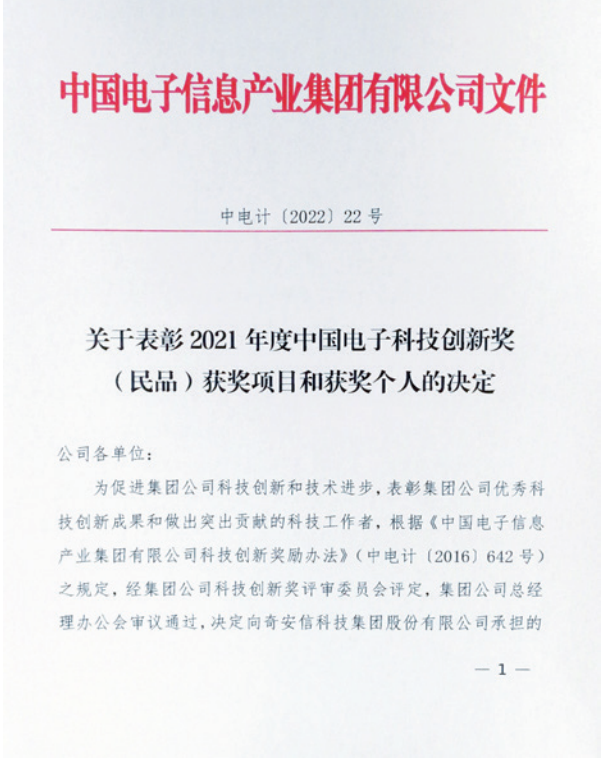
仅用于参考使用，他用无效

工作支撑平台，也将为我国商用密码算法相关产品的研发与落地，起到良好的示范作用。

奇安信荣获中国电子 2021 年度科技进步奖一、二等奖

中国电子集团公司年度工作会上，奇安信集团荣获中国电子科技进步奖 2 项、科技人才奖 1 项。

其中，“网络安全应急响应关键技术研究与服务能力建设”项目荣获科技进步一等奖，“开源软件供应链安全检测关键技术研究及产业化应用”项目荣获科技进步二等奖，集团副总裁张聪荣获“中国电子集团 2021 年度科技人才奖”。



中国电子信息产业集团有限公司文件

中电计〔2022〕22 号

关于表彰 2021 年度中国电子科技创新奖（民品）获奖项目和获奖个人的决定

公司各单位：

为促进集团公司科技创新和技术进步，表彰集团公司优秀科技创新成果和做出突出贡献的科技工作者，根据《中国电子信息产业集团有限公司科技创新奖励办法》（中电计〔2016〕642 号）之规定，经集团公司科技创新奖评审委员会评定，集团公司总经理办公会审议通过，决定向奇安信科技集团股份有限公司承担的

— 1 —

奇安信蝉联赛可达实验室企业终端安全和杀毒引擎两项大奖

2022 年 1 月，国际知名第三方网络安全检测服务机构赛可达实验室发布 2021 年度赛可达优秀产品奖（SKD AWARDS）获奖名单，来自 11 家网络安全企业的 24 款网络安全产品入选此名单。其中，奇安信天擎终端安全管理系统、奇安信 OWL 反病毒引擎凭借强大的技术创新能力，从国内外众多优秀的产品中脱颖而出，斩获赛可达实验室“企业终端安全”和“杀毒引擎”两项大奖。

值得注意的是，自 2020 年率先通过赛可达实验室威胁检测能力测试之后，2021 年 9 月，奇安信天擎 EDR 再度通过该项测试，并以 ATT&CK 框架攻击技术覆盖面 164 个、勒索病毒查杀率 100% 的佳绩再创同类产品新高。

网神信息技术（北京）股份有限公司
奇安信天擎终端安全管理系统
荣 获
2021年度
赛可达优秀产品奖
SKD AWARDS
赛可达实验室 skd labs

网神信息技术（北京）股份有限公司
奇安信 OWL 反病毒引擎（QOWL）
荣 获
2021年度
赛可达优秀产品奖
SKD AWARDS
赛可达实验室 skd labs

奇安信位居“2021年中国网安产业竞争力50强”第一名

6月16日，中国网络安全产业联盟（CCIA）揭晓
“2021年中国网安产业竞争力50强”。
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，
奇安信位居第一名。

“2021年中国网安产业竞争力50强”榜单

TOP15	公司名称	公司简称
1	**奇安信科技集团股份有限公司**	**奇安信**
2	深信服科技股份有限公司	深信服
3	启明星辰信息技术集团股份有限公司	启明星辰
4	华为技术有限公司	华为
5	天融信科技集团股份有限公司	天融信
6	腾讯科技(深圳)有限公司	腾讯
7	阿里云计算有限公司	阿里云
8	新华三技术有限公司	新华三
9	绿盟科技集团股份有限公司	绿盟科技
10	杭州安恒信息技术股份有限公司	安恒信息
11	三六零安全科技股份有限公司	三六零
12	亚信安全科技股份有限公司	亚信安全
13	中孚信息股份有限公司	中孚信息
14	杭州迪普科技股份有限公司	迪普科技
15	山石网科通信技术股份有限公司	山石网科

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