出版物准印证号：京内资准字 2021- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

平台化的安全未来

P18

第17期
2022 年 5 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

为何 1+1>2

古希腊哲学家亚里士多德有句名言，“整体大于部分之和”，也就是“1+1>2”。这句来自亚里士多德的《形而上学》中的名句，往往用于解释协同作用的重要性。

在网络安全行业，我们正在经历“1”过多，但总和却不高的困境。

在多数的数字化项目中，基于效率的目标，网络安全往往是事后补救式的建设。为此，我们为了应对各种细分的需求，开发和部署了数量众多的安全设备，用于解决不同的问题、保护不同的系统，以及分布在不同位置的数据。

究其原因，是整体安全架构落后于信息化或数字化发展的进度，导致网络安全建设缺乏统一、全盘的考虑，与 ERP 等成熟的企业信息化方案相比，安全架构依然是点状式建设，造成了分散建设、没法联通，关键时刻还达不到预期效果，这是当前整体安全建设的困难和现状。

越来越多的用户渴望构建统一的安全平台，让这些孤立的安全设备可以实现协同，实现“1+1>2”的效果。奇安信集团副总裁、大禹平台负责人左文建介绍，近一年来，他曾遇到很多客户，无论是大型客户，如北京冬奥、南方电网、城市运营中心等，还是重要行业，如公安、网信、能源、工业、工信、运营商等，都对大型安全系统建设有着强烈的需求。

目前在国际上，头部安全厂商也经开始了统一安全平台的建设，以简化安全、降低成本，同时提高检测和应对安全威胁的能力。

在国内，奇安信从 2020 年启动了平台化战略，确立了三步走的目标。2022 年实现研发平台化，完成了第一步，取得人效比提升的成果，将帮助公司实现盈利。未来奇安信将继续致力于构建具有开放生态的安全平台，帮助大型客户改进威胁预防，提升威胁检测和事件响应能力。

正如上世纪 90 年代，企业通过部署 ERP 软件、取代部门级应用，实现流程再造，取得决策改善、收入提高的效果一样，安全平台的建设必将为用户带来“1+1>2”的收效。

总编辑

李建平

2022 年 5 月 1 日

CONTEN

目录

安全态势

月度专题

平台化安全的未来 P18

面对安全设施日益复杂、安全响应压力不断增大的挑战，平台化正成为安全的未来发展方向。

TS

奇安资讯

《网安 26 号院》编辑部

主办 奇安信集团

总　编　辑：李建平
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
安全叨客主编：王梦琪
奇安资讯主编：陈　冲

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：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 5 月 26 日
下载地址：www.qianxin.com

事件篇

勒索软件持续肆掠，对政务民生、国防、能源、民航等多个关键行业造成重大伤害，特别是针对哥斯达黎加政府的攻击，已经影响到国家稳定；俄乌冲突引发的网空风险外溢至全球，黑客组织高调活动，欧洲多国政府受到较大影响。

勒索软件攻击已造成国家危机！哥斯达黎加宣布进入紧急模式

综合消息，自 4 月 17 日 Conti 勒索软件攻击爆发以来，北美国家哥斯达黎加至少有 27 个政府机构受到影响，其中财政部等 9 个机构受到严重影响，如征税工作受阻碍、公务员工资发放金额错乱等。哥斯达黎加新任总统 Rodrigo Chaves 在 5 月 8 日上任后，马上宣布进入全国紧急状态。Chaves 称，有证据显示，国内有内鬼配合勒索软件团伙敲诈政府，这场危机是政府多年未投资网络安全的苦果。

“8220”挖矿团伙持续传播僵尸网络程序：重点攻击北上广等城市

据 CNCERT 5 月 19 日消息，CNCERT 近期监测跟踪发现，“8220”挖矿团伙近期持续传播 Tsunami 僵尸网络程序。抽样监测发现，近期该团伙单日对上千台主机成功实施漏洞攻击，并下载挖矿、僵尸网络程序等恶意样本。上述团伙传播目标 IP 所在地域主要集中在北京、广东、上海等省份城市。目前捕获的“8220”攻击团伙的 IP 类型的攻击资源，主要分布于美国、乌克兰等国家。CNCERT 建议，对暴露在公网上的应用服务使用高强度口令及认证机制，定期对服务器进行加固，修复相关高危漏洞。

俄黑客组织宣布对美欧十国政府发动网络战，意大利政府网站已瘫痪

据观察者网 5 月 17 日消息，俄罗斯黑客组织“Killnet”在社交软件 Telegram 上发布视频，宣布向美、英、德等十国政府发起网络战。“Killnet”称，普通民众在这次网络战中不会有危险，而这些“支持纳粹和恐俄症”国家的政府会被清算。此外，“Killnet”还否认了意大利警方对该组织攻击欧洲歌唱大赛投票系统的指控，并且宣称已经攻陷意大利国家警察官网长达 30 个小时。

加拿大空军关键供应商遭勒索攻击，疑泄露 44GB 内部数据

据 The Record 5 月 11 日消息，加拿大、德国军方的独家战机培训供应商顶级王牌（Top Aces）披露，已遭到 LockBit 勒索软件攻击。LockBit 团伙的官方网站放出了要求，如不支付赎金将公布窃取的 44GB 内部数据。安全专家称，针对国防相关企业的攻击令人担忧，因为无从得知被盗数据最终会落入哪里，很有可能流入对手国家。LockBit 是目前最流行的勒索软件即服务平台之一，据统计今年已攻击了至少 650 个目标组织。

俄罗斯电视台在胜利阅兵日被黑，显示“恐吓式”反战信息

据华盛顿邮报 5 月 9 日消息，在俄罗斯举行胜利日阅兵的重要时刻，该国用户的智能电视显示画面遭到篡改，展示了许多血淋淋的反战标语信息。俄罗斯多个主要电视频道、最大搜索网站 Yandex、最大视频网站 RuTube 均受到网络攻击的影响。俄罗斯政府近期通过一项法律，任何抹黑俄罗斯军队及其在乌克兰作战行动的企图都是违法的，上述信息在俄罗斯国内会遭到禁止。

农业机械巨头爱科遭勒索攻击，美国种植季拖拉机供应受影响

据路透社 5 月 6 日消息，美国农业机械巨头爱科（AGCO）遭到勒索软件攻击，部分生产设施运营受到影响，官方网站无法访问，影响可能持续了多天。有经销商表示，这导致拖拉机销售在美国最重要的种植季节停滞不前。近一年来，多家农业供应链企业遭到攻击，农业逐渐成为勒索攻击重点目标，美国联邦调查局近一年已发布过两次行业预警。

汽车租赁巨头 Sixt 遭网络攻击，全球系统中断致使业务陷入混乱

据 SecurityWeek 5 月 3 日消息，国际汽车租赁巨头 Sixt 遭到网络攻击，部分业务系统被迫中断，运营出现大量技术问题。公司的客户服务中心和部分分支机构受影响较大，大多数汽车预定都是通过笔和纸进行的，服务热线短时离线后恢复，业务陷入混乱。据猜测，此次攻击可能属于勒索软件攻击，目前暂时没有相关组织表示负责。

北京健康宝遭受境外网络攻击：源头来自境外 已有效处置

据北京青年报 4 月 28 日消息，北京市第 318 场新冠病毒肺炎疫情防控工作新闻发布会召开。北京市委宣传部对外新闻处副处长隗斌在会上表示，当天北京健康宝使用高峰期遭受网络攻击。经初步分析，网络攻击源头来自境外。北京健康宝保障团队进行了及时有效的应对，受攻击期间，北京健康宝相关服务未受影响。在北京冬奥会冬残奥会期间，北京健康宝也遭受过类似网络攻击，均得到有效处置。

地缘政治引发欧洲风电安全危机！已有三家公司遭遇网络袭击

据华尔街日报 4 月 25 日消息，4 月中旬，德国风力涡轮机维护公司 Deutsche Windtechnik AG 遭遇勒索软件攻击，约 2000 台风力涡轮机的远程控制系统瘫痪了一天左右。这是自俄乌冲突全面爆发以来，欧洲第三家风能公司遭到网络攻击。此前涡轮机制造商 Enercon GmbH、Nordex SE 先后沦为网络攻击的受害者。有专家认为，欧美制裁俄罗斯能源入口使得风电行业受益，站队俄罗斯的黑客组织试图在这一行业制造混乱。

加拿大老牌航司遭网络攻击，导致航班严重延误近一周

据 CityNews 4 月 21 日消息，因供应商系统遭受网络攻击，加拿大老牌航空公司阳翼航空（Sunwing Airlines）的重要系统中断服务，致使航班严重延误近一周时间。此次事件导致至少 188 个航班发生延误，许多乘客因此被困在机场，有乘客表示已经滞留在机场超过 3 天。为减少服务中断，阳翼航空表示会尽量以手动方式处理航班业务。

漏洞篇

5 月初，F5 发布旗下 BIG-IP 严重漏洞的修复补丁，漏洞披露不久便遭到积极利用，攻击者试图实施数据擦除攻击。中国等多国 CERT 机构纷纷发布安全预警。

OpenSSL 命令注入漏洞安全风险通告

5 月 19 日，奇安信 CERT 监测到 OpenSSL 官方发布 OpenSSL 命令注入漏洞（CVE-2022-1292）通告。该漏洞是由于 c_rehash 脚本未对外部可控数据进行有效过滤，导致可操作 /etc/ssl/certs/ 目录的攻击者注入恶意命令，从而以该脚本的权限执行任意命令。OpenSSL 1.0.2、1.1.1、3.x 版本均受到影响。目前，官方已发布更新版本，建议客户尽快做好自查，及时更新至最新版本。

Active Directory Domain Services 权限提升漏洞风险通告

5 月 13 日，奇安信 CERT 监测到 Active Directory Domain Services 权限提升漏洞（CVE-2022-26963）细节及 PoC 已在互联网公开。当 Active Directory 证书服务在域上运行时，经过身份验证的攻击者可以在证书请求中包含特制的数据，然后从 Active Directory 证书服务中获取允许提升权限的证书，并将域中普通用户权限提升为域管理员权限。经研判，此漏洞 PoC 有效，漏洞现实威胁进一步上升。鉴于此漏洞影响较大，建议客户尽快自查修复，升级至安全版本。

Netatalk 远程命令执行漏洞安全风险通告

5 月 12 日，奇安信 CERT 监测到开源文件服务器软件 Netatalk 的远程命令执行漏洞（CVE-2022-23121）细节及部分 PoC 公开。未经身份验证的远程攻击者利用此漏洞，可在受影响的 Netatalk 服务上以 root 权限执行任意命令。奇安信 CERT 已复现此漏洞，鉴于已有细节及部分 PoC 公开，攻击者可通过已有信息开发出利用代码，漏洞现实威胁上升，建议客户尽快做好自查，及时更新至最新版本。

F5 BIG-IP iControl REST 身份认证绕过漏洞安全公告

5 月 7 日，国家信息安全漏洞共享平台（CNVD）收录了 F5 BIG-IP iControl REST 身份认证绕过漏洞（CVE-2022-1388）。F5 BIG-IP 是美国 F5 公司一款集成网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。攻击者利用该漏洞，可在未授权的情况下执行任意系统命令，创建或删除文件及禁用服务。目前，漏洞利用细节已公开，厂商已发布补丁完成修复。

对抗篇

国内攻防演习 4 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 4 月，奇安信 Z-TEAM 团队共承接攻防演习服务 31 场，其中行业级攻防演习 2 场，省级攻防演习 2 场，省级行业攻防演习 1 场，地市级攻防演习 4 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	48	43	57	72	41	67	186	1221

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，以专项任务、政务和金融为主，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、内网功能区域缺乏安全隔离、内网访问权限策略设置不严格、内网口令复用及弱口令普遍等。具体情况如下：

1、漏洞利用依旧是外网成功突破的主要手段

本月任务数据显示漏洞利用依旧是外网成功突破的主要手段。利用漏洞以平台组件历史漏洞为主，如未授权访问、Spring 组件漏洞、Shiro 反序列化、任意文件上传漏洞等，多因外部应用及系统组件缺乏日常安全巡检机制、对爆出的漏洞组件未及时升级更新造成的，这些漏洞的存在使得目标网络有随时被入侵的严重安全风险。

2、弱口令和口令复用问题在内网比较突出

本月任务中目标内网弱口令和口令复用问题依旧比较突出。在互联网应用系统，内网应用系统、服务器、数据库等信息设备中普遍存在弱口令，这导致信息设备可被攻击者轻易攻陷。同时多台设备使用相同密码、密码长期未修改等问题也比较常见，这些问题致使信息系统面临严重安全风险。

3、钓鱼攻击是实现外部突破的有力辅助

本月任务中针对特殊行业目标系统网络，钓鱼攻击成为外部突破的主要使用手段，由于金融、航空、电力这类目标业务具有较大的开放性，并且内部客服人员网络安全意识不强，因此具有较高的成功率。钓鱼攻击已成为攻击者实现外部突破的高效手段之一。

4、安全意识薄弱导致敏感信息泄露

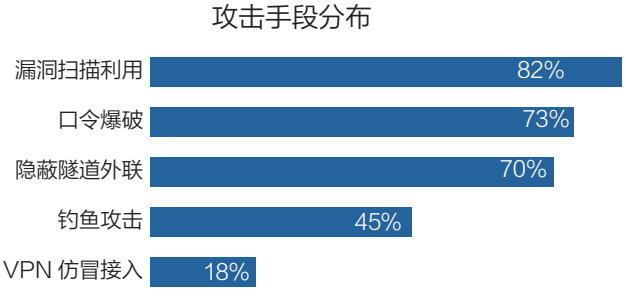
本月任务中目标网络敏感信息泄露较为严重，包括目录文件信息、业务系统、应用开发平台及后台登录地址、内网 IP 地址、接口、安全认证信息在内的敏感源码泄露等，这些敏感信息泄露原因多为安全配置疏漏、平台审核不严，此类敏感信息常常被用来实现针对性的快速突破及渗透。

5、内部网络纵深防护机制不够健全

本月任务中发现目标网络缺乏纵深防护机制。较多客户网络边界隔离不够清晰，一旦突破外网进入内网后，即可横向攻击大量系统、服务器、数据库等内网资产。部分客户在互联网边界安全防护、网络区域边界安全隔离、服务器安全纵深防护等方面未形成纵深防御体系。

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手段实现，内网横向拓展以弱口令、口令复用和内部应用漏洞利用等手段为主。使用的主要技术手段分布如下：



1、漏洞扫描利用

本月任务中漏洞扫描利用主要集中在互联网侧业务系统和门户网站，主要以 SQL 注入、未授权访问、组件反序列化、文件上传执行等漏洞为主。这些漏洞主要是由于系统组件更新不及时、安全策略设置缺陷引起的，直接反映出客户网络运维人员对下辖网络资产动态跟踪不及时、网络运维缺乏常态巡检机制、对存在的漏洞及安全威胁应对不够高效等问题。

2、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、管理员为多台网络节点设置同一口令等，直接反映出目标网络对弱口令和通用口令缺乏统一监管，尤其是对账号口令复杂度设置和安全使用缺乏严格要求。

3、隐蔽隧道外联

本月任务中因大部分目标内网无法通过外网直接访问，需要借助端口转发、隐蔽隧道技术等手段实现转发通信。尤其是对于网络功能区域划分严格、核心业务内网隔离措施完善的攻击目标单位，甚至需要两到三层以上通道转发才能实现对目标核心内网的稳定控制。

4、钓鱼攻击

本月任务中针对网络安全防护相对严密，外网系统难以直接突破的目标，钓鱼攻击成为实现外部突破的高效手段。外网钓鱼攻击主要针对安全意识相对薄弱的客服、人事等人员进行，内网则通过水坑攻击对网络运维、平台研发及核心业务人员等目标进行钓鱼攻击，实现重点突破。

5、VPN 仿冒接入

本月任务中VPN仿冒接入主要针对金融行业目标，因为金融业务性质特殊，分散机构多采用远程 VPN 接入业务网络，测试任务也充分利用目标网络的VPN资源，实现对目标业务内网的隐蔽接入渗透。VPN 仿冒接入认证信息主要通过 VPN 网关服务器漏洞利用、口令复用手段获取。

四、典型攻击手段实现案例

1、外部漏洞利用突破

（1）某金融目标在线点播系统存在 Struts2 漏洞，利用此漏洞可获取目标广播网服务器控制权限，直接突破逻辑内网隔离。

（2）某目标电子文档系统存在 CNVD-2021-26058 漏洞，通过此漏洞利用获取该系统后台服务器控制权限。

（3）某目标外网 OA 系统存在 0day 漏洞，可通过远程命令执行控制 OA 服务器。

（4）某目标管理平台系统存在 Weblogic 反序列化漏洞，可通过漏洞利用获取该管理系统权限，实现网络隔离突破。

（5）某目标互联网业务管理系统存在 Apache Struts2 远程代码执行（s2-005）漏洞，通过漏洞利用获取该管理系统权限。

2、钓鱼攻击

（1）某目标内网对管理员进行钓鱼攻击，在控制目标 ideal 系统后，通过 ideal 注册账号找到管理员邮箱，对该邮箱发送钓鱼邮件并成功上线。

（2）某目标通过电话客服获得某系统运维经理电话，对运维经理进行钓鱼攻击，并成功获取其所运维系统得控制权限。

（3）以招聘内推为由，添加某目标招聘业务人员为好友，对其进行钓鱼攻击，获取内网系统服务器权限。

（4）向某目标官网邮箱投稿钓鱼邮件，通过钓鱼攻击获取主机终端权限。

3、口令爆破

（1）某目标业务系统存在弱口令，可通过口令爆破直接登录该系统管理后台，对系统进行任意操作，获取系统后台中的敏感信息。

（2）某目标外网业务工作培训平台存在弱口令，可通过口令爆破登录业务后台，并进一步拓展控制平台服务器。

（3）某目标 OA 系统存在弱口令，可通过口令爆破直接登录 OA，并进一步获取内网办公业务人员电话、地址等敏感信息。

（4）某目标堡垒机存在弱口令漏洞，通过该漏洞获得内网系统后台管理员权限两个，内网可管控主机 732 台。

4、VPN 仿冒接入

（1）某目标业务网络 VPN 网关存在注入漏洞，通过漏洞利用获取接入目标业务内网的接入口令，最终实现仿冒接入及渗透。

政策篇

国内，全国人大常委会发布《2022 年度立法工作计划》，《反电信网络诈骗法》有望在年内制定推出；

国际上，美国司法部发布司法解释，不再对白帽黑客行为追究责任。司法部副部长称：“计算机安全研究是提升网络安全的关键驱动力。”

国内

国家药监局印发《药品监管网络安全与信息化建设“十四五”规划》

5 月 11 日，国家药监局印发《药品监管网络安全与信息化建设“十四五”规划》。《规划》要求健全和完善网络安全体系，夯实网络安全综合保障能力。具体包括加强网络安全保障管理、推进数据安全保障建设、升级安全管理运维平台。《规划》还提出了两项网络安全任务，完善药监云网络安全信任体系，完善国家局安全管理运维中心。

2022 年将制定反电信网络诈骗法，预备审议网络犯罪防治法

5 月 6 日，全国人大常委会发布《2022 年度立法工作计划》。《工作计划》提出，围绕维护国家安全，促进社会和谐稳定，将制定反电信网络诈骗法（6 月继续审议）等。预备审议电信法、网络犯罪防治法等项目，开展调研和起草工作，视情安排审议。另据《工业和信息化部 2022 年规章制定工作计划》，今年将起草《电信和互联网用户个人信息保护规定（修订）》。

证监会就《证券期货业网络安全管理办法（征求意见稿）》公开征求意见

4 月 29 日，证监会发布《证券期货业网络安全管理办法（征求意见稿）》公开征求意见。《征求意见》稿对证券期货业网络安全监督管理体系、网络安全运行、数据安全统筹管理、网络安全应急处置、关键信息基础设施网络安全、网络安全促进与发展、监督管理与法律责任等方面提出了要求。《征求意见》稿规定，核心机构和经营机构应当依法履行网络安全保护义务，对本机构网络安全负责，相关责任不因其他机构提供产品或者服务进行转移或者减轻。

国家发展改革委发布《电力可靠性管理办法（暂行）》

4 月 25 日，国家发展和改革委员会发布《电力可靠性管理办法（暂行）》。《办法》共十一章，其中第七章为网络安全。《办法》规定，电力网络安全坚持积极防御、综合防范的方针，坚持安全分区、网络专用、横向隔离、纵向认证的原则。《办法》提出，加强网络安

全审查、容灾备份、监测审计、态势感知、纵深防御、信任体系建设、供应链管理等工作，开展网络安全监测、风险评估和隐患排查治理，提高网络安全监测分析与应急处置能力。

《政务网站系统安全指南》等 10 项网络安全国家标准获批发布

4 月 24 日，全国信息安全标准化技术委员会归口的 10 项国家标准正式发布。具体包括智能家居通用安全规范、可信执行环境 基本安全规范、SM9 密码算法使用规范、移动互联网应用程序（App）收集个人信息基本要求、工业控制系统信息安全防护能力成熟度模型、网络数据处理安全要求、信息安全风险评估方法、可信计算密码支撑平台功能与接口规范、信息安全服务 分类与代码、政务网站系统安全指南。

美国司法部发布司法解释，不再对白帽黑客行为追究责任

5 月 19 日，美国司法部发布针对《计算机欺诈与滥用法》（CFAA）的政策执行修订（类似司法解释），首次提出不应对善意网络安全研究追究责任。善意研究是指：仅出于善意测试、调查和 / 或修正安全缺陷或漏洞的目的访问目标计算机。这类活动是以旨在避免对个人或公众造成任何伤害的方式进行的，并且从该活动中获得的信息主要用于促进被访问设备 / 机器 / 在线服务 / 人员的安全或保障。美国司法部副部长 Lisa O. Monaco 表示，“计算机安全研究是提升网络安全的关键驱动力，此举旨在为善意研究人员提供明确规定。”

欧盟商定 NIS2 指令，加强关键领域安全保护

5 月 13 日，欧洲理事会和欧洲议会就 NIS2 指令达成临时协议，商定了在整个欧盟范围实现高水平网络安全的措施，以进一步提高公私部门及整个欧盟的网络弹性和事件响应能力。NIS2 指令为涵盖的关键领域制定了网络安全风险管理措施和事件报告义务的基线，旨在消除不同成员国的要求和实践差异，并要求成立欧洲网络危机联络组织 EU-CyCLONe，执行大规模网络安全事件的协调管理。

美国众议院通过《促进数字隐私技术法案》：大力发展隐私增强技术

5 月 11 日，美国众议院正式通过《促进数字隐私技术法案》，将由参议院进行下一步审议。《法案》是一项支持隐私增强技术研究和促进负责任数据使用的拟议法案。《法案》围绕隐私增强技术的基础研究、劳动力、市场发展、联邦政府采用、最佳实践等方面进行布局。隐私增强技术作为一种广泛的技术，允许组织收集、共享和使用数据，同时减轻这些活动产生的隐私风险。

美国 NIST 发布《网络安全供应链风险管理框架指南》

5 月 5 日，美国国家标准技术研究院（NIST）发布《网络安全供应链风险管理框架指南》项目，这一指南遵循拜登于 2021 年 5 月发布的“改善国家网络安全”行政命令（EO 14028），要求政府机构采取措施“提高软件供应链的安全性和完整性，优先解决关键软件问题。”该指南概述了组织在识别、评估和响应供应链不同阶段的风险时，应采用的主要安全控制措施和做法，以帮助组织识别、评估和响应整个供应链中的网络安全风险，同时还分享了与供应链攻击相关的趋势和最佳实践。

政策解读

工信部《APP 收集使用个人信息最小必要评估规范》征集意见，检测清单需进一步更新

作者 北京德和衡律师事务所 周杨 梁天翔

2022 年 5 月 7 日，工信部发布《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第 1 部分：总则》等 4 项行业标准（详见第 4 节）报批公示稿。公示截止时间为 2022 年 6 月 7 日。该标准适用于 APP 提供者遵循最小必要原则规范其对用户个人信息的处理活动，对于企业有较强的参考价值。

（一）体系定位

本次公示的 4 项行业标准（**总则、位置信息、图片信息、短信信息**）为《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》系列行业标准的组成部分。该系列标准旨在对移动互联网行业收集使用人脸、通讯录、短信、位置、图片等敏感个人信息进行规范，落实最小、必要的原则。

该系列行业标准共由 16 个部分构成：**总则、位置信息、图片信息、终端通讯录、设备信息、软件列表、人脸信息、录像信息、录音信息、通话记录、短信信息、好友列表、传感器信息、应用日志信息、身份信息、剪切板信息。**

（二）与《APP 收集使用个人信息最小必要评估规范》团体标准的关系

本次由工信部发布的评估规范属于行业标准，其与电信终端产业协会于 2020 年起陆续发布的 17 项《APP 收集使用个人信息最小必要评估规范》团体标准密切相关。根据《中华人民共和国标准化法》的规定，标准包括国家标准、行业标准、地方标准和团体标准、企业标准。（T/TAF 077.X-2020）《APP 收集使用个人信息最小必要评估规范》团体标准是在缺少相关行业标准的情况下，由电信终端产业协会相关团体于 2020 年起自主发布，并由社会自愿采用的标准。而（YD/T 4177.X-2022）《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》行业标准是由工信部主导制定的。区别于上述团体标准，该行业标准是对国家标准的补充，**适用于整个通信行业，且指标低于该行业标准的团体标准为无效标准。因此，通常情况下应优先选用该行业标准，并在本系列其他行业标准文件未颁布之前参照相应团体标准。**

此外，虽然无论行业标准还是团体标准都不具备法律强制力，但《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》作为《个人信息保护法》所明确“最小必要原则”的细化落实，及其“主管监管部门、第三方评估机构等组织对移动互联网应用程序收集图片信息行为进行监督、管理和评估”的适用范围，企业仍应将该系列行业标准作为 APP 合规的重要参考，并在其他部分行业标准出台之前了解既有团体标准内容，从严落实标准要求。

（三）适用范围

移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》系列行业标准适用于移动互联网应用程序（APP）提供者规范用户个人信息的处理活动，也适用于第三方评估机构等组织对移动应用软件收集使用个人信息行为进行监督、管理和评估。个别条款不适用于特殊行业、专业应用，其他终端也可参考使用。

· 移动智能终端

能够接入移动通信网，具有能够提供应用程序开发接口的操作系统，并且具有安装、加载和运行应用软件能力的终端。

· 移动互联网应用程序

可安装在移动智能终端内，能够利用移动智能终端操作系统提供的公开开发接口，实现某项或某几项特定任务的计算机软件，包含移动**智能终端预置应用软件，小程序、快应用及互联网信息服务提供者**提供的可以通过**网站、应用商店**等移动应用分发平台**下载、安装、升级**的应用软件。

（四）主要内容

标准编号	标准名称	标准主要内容
YD/T 4177.1-2022	移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第 1 部分：总则	本文件规定了 APP 收集使用个人信息的最小必要基本原则、评估要求、评估方法及评估流程
YD/T 4177.2-2022	移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第 2 部分：位置信息	本文件规定了移动互联网应用程序（APP）在处理涉及用户个人信息（位置信息）的告知同意、收集、存储、使用、传输、删除等活动中的最小必要评估规范，并通过设备信息在处理活动中的典型应用场景来说明如何落实最小必要原则
YD/T 4177.3-2022	移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第 3 部分：图片信息	本文件规定了移动应用软件在处理涉及个人信息主体个人信息相关图片信息的收集、存储、使用、删除等活动中的最小必要信息规范和评估方法，并通过对在个人信息处理活动中的典型应用场景来说明如何落实最小必要原则
YD/T 4177.11—2022	移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第 11 部分：短信信息	本文件是 APP 收集使用个人信息最小必要评估规范系列标准中的短信信息部分，旨在贯彻个人信息收集使用的最小必要的原则，针对 APP 访问、收集、存储、使用、删除用户手机短信（含彩信、5G 消息等多媒体方式）信息等各环节提出相应的最小必要性符合度评估项，并结合典型场景，对 APP 最小必要处理短信信息进行规定

（五）基本原则——最小必要

APP 个人信息的处理应遵循最小必要原则，即处理个人信息应当具有明确、合理的目的，应与处理目的直接相关，采取对个人权益影响最小的方式。**当 APP 提供的业务功能不在《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》系列标准内，同样应满足最小必要要求。**

（六）《总则》明确的最小必要评估基本要求

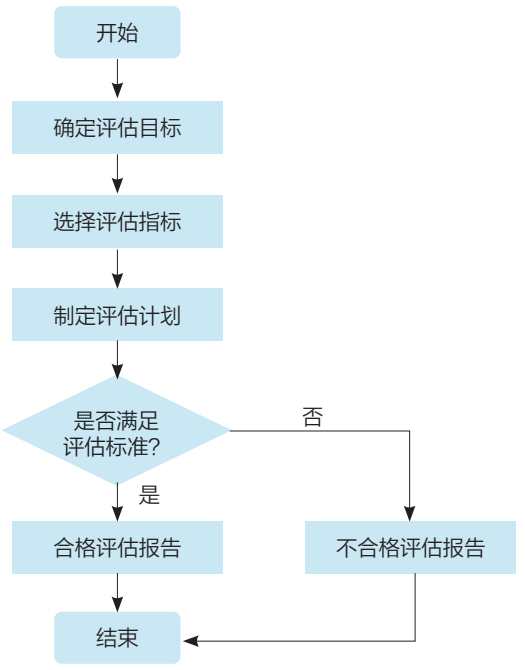
《APP 收集使用个人信息最小必要评估规范 第 1 部分：总则》规定了 APP 收集使用个人信息的最小必要原则的评估要求，其从权限、告知同意、收集、存储等维度全方位地对 APP 个人信息处理环节进行了规定，详见下表：

评估维度	要求
权限	权限申请和使用应遵循最小必要原则，要求如下： · 权限申请和使用的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。 · APP 应申请与业务功能相关的权限，**不应过度申请权限。**如 APP 的业务功能中，不包含录音相关场景，则不应申请录音权限。 · APP 申请敏感权限时，应**同步告知**权限使用的目的和用途。 · APP 宜优先**采用系统自身功能，代替调用相关敏感权限。**如 APP 需要拨打电话功能时，可优先选择调用系统的电话界面，而不是申请电话权限。 · 不得以改善服务质量、提升使用体验和实施风险控制等为由，**强迫**个人信息主体授予权限。 · APP 申请权限时需要在使用对应业务功能时申请，不应一揽子申请多个权限，不得默认、捆绑或使用其他手段变相欺骗、误导、强迫个人信息主体授予权限。 · 对于**第三方 SDK** 等外部代码的引用，APP 应要求 SDK 其相关权限的申请同样满足最小必要原则，不得过度申请权限。
告知同意	告知同意应遵循最小必要原则，要求如下： · 告知同意应遵循最小必要原则，即 APP 所提供产品或服务涉及多项业务功能的，处理个人信息时，宜按业务功能**单项或分项**获得个人信息主体同意，不应采用捆绑方式强迫个人信息主体一次性同意多种业务功能收集的个人信息。个人信息主体拒绝同意时，仅影响与所拒绝个人信息相关的业务功能的正常使用。 · 告知同意的时机及频率，宜在收集使用之前或收集使用之时的**适当时机**告知，增进个人信息主体对告知与所处理收集的个人信息之间关联性的理解。
收集	收集个人信息应遵循最小必要原则，要求如下： · 收集个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。 · APP 被授予权限后，权限使用应遵循最小必要原则，即应合理使用申请的权限，不应滥用权限，超频次、超范围、超精度收集个人信息。
存储	个人信息的存储包含本地存储和服务器远端存储，均应遵循最小必要原则，要求如下： · 存储个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。 · 存储个人信息的类型及数量应遵循最小必要原则，不应超出业务功能的实际需要。 · 存储个人信息的时间应遵循最小必要原则，即存储个人信息的时间，**应当为实现处理目的所必要的最短时间，**在超出上述期限后，应对个人信息进行**删除或匿名化处理。**（注：对于保存在端侧的个人信息，只需对业务运行过程中产生的包含个人信息的临时文件，或过程文件指定删除时间，其他个人信息由用户自己管理和控制） · 收集个人信息后，宜**立即进行去标识化处理，**并将可用于恢复识别个人的信息与去标识化后的信息**分开存储。** · APP 如需在终端本地存储个人信息，则应将个人信息存储在**受保护的文件区域，**防止其他 APP 非授权访问。 · 个人生物识别信息应在本地进行加密存储。如因业务需要确需传出终端的，应使用**单向不可逆摘要算法**进行摘要处理或使用高强度加密算法进行加密处理，且**单独明确告知，用户选择同意**后，方能传出终端。

使用	使用个人信息应遵循最小必要原则，要求如下： · 使用个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要，法律法规另有规定的除外。 · 使用个人信息时，除目的所必需外，应**消除明确身份指向性**，避免精确定位到特定个人。 · 使用个人信息进行定向推送应遵循最小必要原则，不应超出业务功能的实际需要。 · 若 APP 定向推送功能使用了第三方的个人信息来源，应以**个人信息处理规则**等形式向个人信息主体**明示业务功能使用第三方的个人信息进行定向推送**，并向个人信息主体明示第三方的个人信息来源。 · 使用个人信息进行定向推送应显著**区分个性化展示和非个性化展示**，显著区分的方式包括但不限于：标明“推荐”、“猜你喜欢”等字样，或通过不同的栏目、版块、页面分别展示等。 · 使用个人信息进行定向推送应当同时提供**关闭个性化展示**的选项。此外，APP 宜建立个性化展示所依赖的个人信息（如标签、画像维度等）的**自主控制机制**，保障个人信息主体调控定向推送展示相关性程度的能力。
加工	加工个人信息应遵循最小必要原则，要求如下： · 加工个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。 · 间接获取个人信息后，进行加工处理形成新的个人信息并用于其他目的，需要告知，并**再次征得个人信息主体的同意**。
传输	传输个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。
提供	提供个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。
公开	公开个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。
删除	删除个人信息应遵循最小必要原则，超出存储期限后，应对个人信息进行删除或匿名化处理。

（七）《总则》确认的基本评估流程

APP 收集使用个人信息最小必要评估流程应包括确定评估目标、选择评估指标、制定评估计划、实施评估及得出评估结论五个活动。



1. 确定评估目标

被评估方可为 APP 或者 APP 中某项某类功能。

评估方可为 APP 提供者、开发者和运营者，也可为第三方实验室。

2. 选择评估指标

评估方根据被评估方提供的技术说明文档、被评估 APP 样品等材料：确定初步的方案审核，发现涉及的个人信息类型，选择对应的评估规范标准，并由此定义后续的评估的计划和评估项例。

3. 制定评估计划

评估方应根据评估目标，本着公平、公正、公开原

则开展评估工作。

评估准则内容应至少包括评估对象和范围、评估依据、评估环境、评估工具。

评估准则中应明确评估通过 / 不通过准则。

4. 实施评估

依据对应的评估规范标准开展实施评估活动。

通过各部分实施评估工作可顺序开展也可并行开展，无完整的顺序关系。

各部分最小必要评估结果均应以评估报告的形式进行输出，其内容至少应包括开展最小必要信息类型、评估所选择的评估指标及针对评估指标的评估结果。

5. 得出评估结论

针对开展评估的个人信息类别进行评估，APP 收集使用最小必要未见异常并通过评估，否则未通过评估。

在最小必要评估报告中，应包含评估的环境、评估基本要素和每一项评估的结果，同时还应具体描述评估过程中的步骤，如包含未通过项则评估报告中应包含未通过原因的具体描述。

（八）本次公布的其他评估规范中的重点要求

《APP 收集使用个人信息最小必要评估规范》系列行业标准除总则外，此次公开的其他三份标准文件针对**位置信息、图片信息、短信信息三类敏感个人信息处理活动，就其最小必要性符合度评估项进行了特别规定。**针对每一类数据，相应评估规范均针对不同的处理活动期间，如收集、存储、使用等阶段给出了相应的是否满足“最小化”的评估要求。**由于规范规定的颗粒度非常细，且具有很强的实践操作性，为避免遗漏，本文不再做提炼总结，建议直接阅读相应评估规范。**

值得一提的是，针对每一类数据，各评估规范都对相关信息进行了分类，并列明了典型应用场景，对于受众准确和深入理解工信部监管思路具有很大帮助。有关三类信息的具体分类和典型应用场景我们试总结如下：

信息类型	信息分类	典型应用场景
位置信息	根据 APP 业务场景，APP 可收集的位置信息数据分类包括： · 终端定位信息（卫星定位信息、无线网络信息、移动通信基站定位、传感器、IP 地址等）； · 用户填写的位置信息； · 图片、录像数据中的位置信息	· 地图服务 · 广告服务 · 调度服务 · 资产管理服务 · 搜索服务 · 推荐服务 · 画像服务 · 风控服务
图片信息	图片可以通过拍照、屏幕截图及对图片的再加工的方式生成。**根据图片信息中包含的内容，**可将图片信息分为以下三类。 · 图片基本信息：指图片的基本特征信息，包括图片内容信息（原始的和编码后的二进制码）、图片格式、大小、分辨率； · 图片附加信息：拍照时间、拍照设备、拍照参数、图片名称等可关联出个人的图片信息； · 图片位置信息：指拍摄图片时的精准定位信息。如安卓系统可通过 GpsLocationProvider 来获取精确位置信息	· **社交类：**个人信息主体通过 APP 发送固定数量的图片到明确的一个或多个好友或朋友圈限定范围的场景。 · **媒体发布类：**个人信息主体出于图片公开的目的将图片通过 APP 发布到媒体平台的场景。 · **图片加工类：**个人信息主体通过 APP 对图片进行编辑生成新的图片的场景。 · **图像识别类：**个人信息主体通过 APP 对图片或扫一扫生成的缓存图片进行识别的场景。 · **云盘备份类：**通过 APP 将本地图片备份到云盘的场景。 · **客服 / 售后类：**个人信息主体在 APP 中因某种诉求发送图片到客服或售后的场景

短信信息	文件将短信信息包含的信息类型划分为如下类型。 · **本机用户标识：**用于识别或区分短信、彩信信息所在移动终端设备用户的标识信息，可包括发送者的手机号等；依据短信信息的发送方，本机用户标识可以是短信信息的发送者标识，也可以是短信信息的接收者标识。 · **对端标识：**用于识别或区分短信、彩信信息所在移动终端设备用户的短信通信对端标识信息，包括接收者的手机号等。 · **短信内容：**为短信发送者编辑并发送给接收者的各种格式的内容。单一的短信内容是否包含个人信息、包含的个人信息的类目数量及包含的具体个人信息类型取决于每个短信内容的本身。 · **时间：**移动终端设备用户接收或发送该条短信的时间	· **短信云备份：**以数据备份为目的，APP 将用户终端上的短信信息传输至远端服务器上存储的场景。 · **验证码便捷获取：**以协助用户完成登录或支付等操作为目的，APP 识别短信中的验证码并提示用户的场景。 · **便捷短信查询与服务订阅：**以方便用户操作为目的，APP 帮助用户发送特定短信指令至特定号码，查询相关信息或订阅服务的场景，如流量余额查询。 · **短信优化编辑与发送：**以协助用户编辑并发送短信为目的，APP 提供短信编辑功能并发送短信至用户指定号码的场景。 · **短信功能体验增强：**以增强用户短信功能体验为目的，APP 为用户提供如短信发送商户识别和图形化展示等增强短信功能的场景。 · **手机间数据互传：**以在用户不同手机间传输数据为目的，将用户一部手机中的短信信息传输至用户另一部手机的场景，如换机。 · **骚扰拦截：**以帮助用户拦截、屏蔽诈骗、广告等用户不期望接收的短信信息为目的，APP 识别、展示并处置相关短信信息的场景。 · **服务智能化：**以改善服务智能化程度或用户体验为目的，APP 访问用户短信信息的场景。 · **已关联设备的配套应用：**通过此类应用用户可将移动设备与已关联设备（如智能手表、汽车、智能家居设备等）连接起来，还能够收发短信。 · **跨设备同步或转移短信：**在多个设备上（如手机和笔记本电脑之间）同步短信信息。 · **设备自动化：**用户可让设备根据其设置的一个或多个条件（触发条件），在操作系统的多个区域自动执行重复性操作。 · **企业存档及设备管理：**企业存档、客户关系管理 CRM 和 / 或设备管理，如运营商通过短信上报设备信息与驻网状态。 · **车载免提使用和投影显示：**与驾驶 / 出行的核心功能（如导航）直接相关的 APPs，尤其是在用户与设备的物理互动受到限制的情况下。 · **呼救短信：**可在发生人身安全或紧急状况时发送报警短信。 · **用户数据本地备份与还原：**用户的事务性备份和还原及企业的归档（限时 / 非连续）

（九）合规建议

我们理解，**企业应当重点关注、优先适用新发布的行业标准，从数据全生命周期出发规范 APP 的个人信息处理活动以此落实最小必要原则，并持续监测该系列其他行业标准的发布。**同时，考虑到该系列行业标准整体为团体标准的优化、提升，我们也建议企业了解既有团体标准内容，提前做好部署。

目前阶段可供采取的具体行动包括：

（1） 梳理现有 APP 位置信息、图片信息和短信信息，并将其根据《评估规范》进行基本分类。

（2） 根据《评估规范》要求，按照信息类别排查其数据处理活动是否符合最小必要原则，并作出必要整改，对于无法整改的（如定推服务中对与第三方来源信息的披露），应当考虑适当的风险规避措施。

（3） 修订相应的《隐私政策》。安

平台化
安全的未来

面对安全设施日益复杂、安全响应压力不断增大的挑战，平台化正成为安全的未来发展方向。

平台化成为共同选择

4月19日，奇安信集团举办的研发平台战略发布会，奇安信董事长齐向东发表“研发平台化 网络安全的未来之路”的主题演讲，首度阐释集团的平台化战略。数日后，趋势科技发布统一网络安全平台 Trend Micro One。Gartner 的最新研究称，安全产品整合是未来的潮流。

网络安全平台以降低网络安全的成本和复杂性，提高响应能力和效率为目标，正在成为头部网络安全企业的共同选择。

网络安全世界正发生巨变

网络安全世界正在发生巨大变化，变化之快之大，使其面临与过去的情况完全不同的网络安全格局。

数字转型逐步深入，企业越来越多普遍地部署数字平台、云计算、物联网 (IoT) 和移动技术，由此产生了更多需要管理的端点、更多需要保护的网络和更多需要保护的数据。作为连接企业所有网络资产的攻击面正在迅速扩大。

与不断采用的新技术相比，网络安全则是另一回事：实际上，近 80% 的机构引入创新技术速度超过了保护自身免受网络攻击的能力。安全多是事后考虑并临时部署，由此部署的解决方案会带来更多的复杂性。

长期以来，企业习惯于头痛医头的安全策略，习惯于添加孤立的安全工具来应对单一的安全问题。根据 ESG 研究集团的调查，近 2/3 的大型企业（ 5000 名以上员工的机构 ）至少有 25 种网络安全产品在使用中。波耐蒙研究所(Ponemon Institute)在全球的调查则显示，企业在其网络上部署了 45 种网络安全相关工具。

企业部署的网络安全工具越多，其防御的效率却并没有提高。管理成本高昂的零散工具拼凑在一起，给有效和快速的威胁检测造成阻碍。

过多网络安全工具导致机构无法及时检测和打击网络攻击：根据 IBM 的网络弹性报告，部署超过 50 多种网络安全工具的企业，其检测威胁的能力降低了 8%，防御能力降低了 7%。同时，大多数机构无法配备足够多的安全运营人员来管理增多的工具和处理频出的告警。

与此形成对照的是，攻击者的网络攻击技术与手段却不断精进，频繁利用各种攻击面的安全漏洞，实施勒索与数据窃取活动。

彼此孤立、随意增长的安全工具与危险的威胁形势、不断增长的攻击面越来越不能匹配。

平台化成为共同选择

ESG 在 2019 年的研究表明，许多机构已经受够了这种日益复杂、数量众多的安全设施：大量的安全工具令企业“不堪重负”。ESG 的网络风险管理研究项目显示，从多家安全厂商购买产品与技术会增加复杂性和成本。Gartner 在 2021 年底的研究也显示，目前用户对于集成与整合安全系统的需求不断增长。

研究人员建议，企业应与经验丰富的网络安全专家合作，构建能够动态扩展的网络安全平台，以最大限度地减少不断增长的攻击面，从而可以保障数据安全和业务稳定。

因此，为了提高安全效率、降低复杂性，企业需要从使用多个不同且孤立的安全工具转为使用高性能的网络安全平台，以保护分布在边缘环境、用户、系统、设备和关键应用中的数据。

作为单点工具的替代品，紧密耦合的安全平台将安

全能力整合到单一集成平台中，可以覆盖端点、网络和云，提供高级威胁防护与集中管理，无疑成为应对当前安全挑战的最优选择。

正如 20 世纪 90 年代，许多组织放弃了部门应用，转而采用为企业业务流程和规模设计的集成 ERP 软件。尽管转变并不容易，但将应用和数据整合到统一平台，带来了新的业务流程、改善了决策制定，实现了更高的收入和更低的成本。

在网络安全背景下，通过集成和整合实现的平台化，可以实现从整个基础设施——端点、电子邮件、云工作负载和应用、网络，收集和管理数据，无疑会改进威胁预防，加速威胁检测和事件响应。

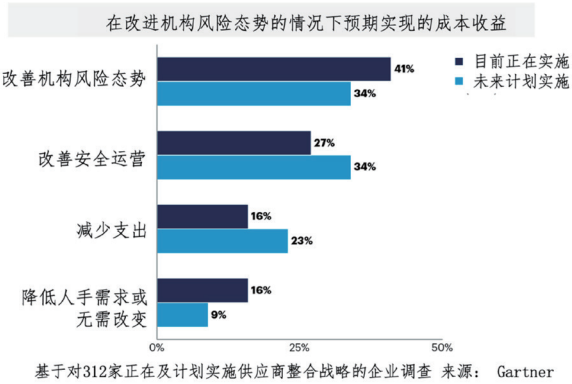
从产品集成到供应商整合

与建设安全平台相对应，越来越多的机构在推进安全供应商整合战略——寻找具有集成技术平台的网络安全战略合作伙伴，在简化安全运营的同时提升安全能力。

Gartner 预计，到 2025 年，3/4 的大型机构将积极推行供应商整合战略，目前这一比例约为 1/4。ESG 的研究则显示，有高达 91% 的企业正积极整合或考虑整合网络安全供应商。

整合网络安全供应商可以带来诸多收益。根据 Gartner 的调查，供应商整合可以改善风险态势、改进安全运营，以及降低成本等收益。

供应商整合战略的主要收益



基于对312家正在及计划实施供应商整合战略的企业调查 来源： Gartner

因此，研究人员建议，为了保护安全投资和提升灵活性，企业安全负责人应部署具有开放架构、开发人员支持和合作伙伴生态系统的平台，可以实现现有的第三方系统的集成。

目前，国内外的安全厂商正逐步分为集成平台厂商和产品组合厂商，前者集成安全工具，实现1+1>2的效果；后者几乎没有集成。

据奇安信集团董事长齐向东介绍，平台化一直是奇安信长期的战略。从 2020 年启动平台化战略，到目前已经完成了第一步，即研发平台化。研发平台化可以提升人效比，帮助公司盈利。未来要实现第二步，即产品平台化，真正地实现安全产品协同与数据统一管理。最终实现第三步，即到 2025 年实现能力平台化。未来，齐安信将在合适的时间向生态伙伴开放其研发平台。

安全研发平台 破解数字化产业五大魔咒

在 4 月 19 日举办的奇安信研发平台战略发布会上，奇安信集团董事长齐向东发表“研发平台化 网络安全的未来之路”的主题演讲，首度阐释集团的平台化战略。

以下为演讲全文。

第一部分 数字化产业蓬勃发展需要专业网络安全力量

最近几年，互联网产业利空不断，已经出现了见顶信号，互联网产业进入成熟后期，未来数字化产业将蓬勃发展。

过去 20 多年，消费端，也就是常说的 C 端，是推动互联网产业发展的动力。但是到 2013 年前后，随着 4G 的普及，移动互联网替代 PC 互联网成为市场主角，消费互联网渗透进人们生活的各个领域。互联网产业的竞争格局发生了巨大变化，大量的细分行业的互联网市场经历了洗牌，逐渐被巨头占领，巨头企业的领先地位得到巩固。行业集中度提升，最终形成垄断，形成赢家

通吃。

这也就意味着，在竞争力上创新不再起作用，规模和实力决定胜负，消费互联网走向成熟后期。在这个时期，因为垄断，互联网平台企业从受到积极鼓励的市场力量，转化为频繁受到严厉监管制约的市场力量。比如，2021 年，阿里巴巴因“二选一”垄断行为被罚 182 亿元、腾讯被责令解除网络音乐独家版权、虎牙和斗鱼合并被叫停、美团因“二选一”被罚 34 亿元。平台企业为了谋求发展，提高价格购买用户，导致流量成本直线上升，价格高居不下，这也严重地打击了互联网创新企业的成长。互联网红利消失。

同时，曾经被互联网行业视为利好的互联网 + 的政府行动计划，实际上推动了政府和企业全面数字化。比如，数字政府、数字工厂、智慧医院等，它们都不仅仅是单纯的网络办事、网络销售、网络服务和网络看病，而是要把政府内部、工厂生产线、医院内部的门诊和诊断工作数字化。在这个过程中，形成了海量的有价值的大数据，这些数据成为互联网 + 的核心内容。

最终，全面数字化，让互联网这个代理平台的存在价值变得越来越小。政府、企业、医院都变成了直接面向市场、提供服务和产品的数字化主体。最终的结局是，全面数字化大大削弱了互联网产业的价值。

我国数字化产业和发达国家相比，还有很大差距，比如，2020 年美国数字化产业占 GDP 总量是 65%，而中国同期占比是 38%。但是全球数字经济增速为 3%，而中国数字经济同比增长 9.6%，我国数字化产业增速全球第一。

数字化产业包含两部分：产业经济数字化和数字技术产业化。先说产业经济数字化，是指用数字化手段提高传统产业效率，是数字技术与实体经济的融合，比如智慧交通、智能制造等。数字技术产业化，是指为产业数字化提供数字技术、产品、服务、基础设施和解决方案，如数字产品制造业、数字产品服务业、数字技术应用业和数字要素驱动业，是数字经济的核心产业和发展基础。

数字化产业需要专业的网络安全力量。我国的网络安全产业经历了四个时期：1995–2002 为初级阶段，年增长率低于 5%，产业规模不足 100 亿元；2003–2013 是产业成长期，年增长率 7% 左右，产业规模接近 300 亿元；2014–2019 是产业加速期，年增长率超 15%，产业规模接近 600 亿元；目前正处在产业爆发期，年均增长率预计超 20%，产业规模到 2025 年增长至超过 3400 亿元。

今年爆发的俄乌战争是人类历史上首次公开、大规模的网络战。军事冲突开始前，网络战就已经打响，直接影响战争形势和国家安全。双方针对敌方军政、金融、能源等关键领域，发起持续性 DDoS 攻击、APT 攻击、恶意软件攻击，产生了严重后果。比如，2 月 25 日俄罗斯网站被攻击长达 5.77 小时，2 月 26 日乌克兰网站被攻击长达 16.42 小时。

3 月 24 日，北约特别峰会决定，将网络安全技术装备与传统武器装备并列，同时作为重点援乌事项。这表明，网安技术装备成为影响战争走向的重要军备物资，网络安全产业将再次扩容。

第二部分 数字化产业面临五大魔咒

在数字化浪潮下，以 B 端为代表的数字化产业加速发展，C 端与 B 端新老赛道碰撞，原本跑马圈地、人海战术、照搬国外等解题思路，无法适用新的产业模式。数字化产业发展面临五大魔咒。

第一大魔咒是圈地魔咒。无论互联网产业还是数字化产业，获客都是发展的根本目标。跑马圈地式的发展手段曾经是互联网产业崛起的杀手锏，但是数字化产业的获客成本高，试错代价大，完全效仿互联网产业跑马圈地是行不通的。

互联网产业的获客成本是以 10 元计。因此，互联网产业偏好跑马圈地，注重扩规模、抢地盘。现在，流量红利见底，获客、留存难度加大，互联网产业逐渐向精细化运营转变。同时，互联网产业试错成本低，

很容易补偿客户损失。企业可以“先开枪，再瞄准”，先发布产品跑马圈地，再在使用过程中完善。即使产品出现问题，只要能够及时修复，使其恢复运转，就能消除客户的不满。

数字化产业的获客成本是以 10 万元计。通过跑马圈地、让利等方式获客，市场投入巨大，成本太高，难以维继。同时，数字化产业试错成本高，难以补偿客户损失。比如，客户 100 万的数字化技术的投入可能要支撑 1000 万以上的数字经济产出，相当于给损失加上了 10 倍的杠杆，如果提供的产品服务质量差，客户损失惨重，还可能干扰社会正常运转。

第二大魔咒是人效比魔咒。人口红利曾经是互联网产业引以为傲的优势，但人口红利带来的客户边际成本优势不适用于数字化产业。

互联网产业中，一个产品面对的是海量用户，一旦产品研发成功就是“一本万利”。随着用户规模不断扩大，边际成本优势也更凸显。因此，早期成功的互联网企业，普遍都拥有人口红利带来的很好的“人效比”增长曲线。当前人口红利见底，获客成本激增、内部高度内卷，外部监管收紧，人效比大幅下降，互联网产业掀起裁员潮。

数字化产业中，服务是重头戏。而服务无法在同一时间做到“一对多”，这意味着服务的客户越多，会推动企业规模扩大，但有可能陷入人效比“死亡陷阱”。数字化产业是木桶思维，产品、销售、服务一个都不能少，数字化产业公司拼的都是组织能力。组织能力能让人效比提升。

第三大魔咒是舶来魔咒。互联网产业都是从“舶来”模式发展起来的，数字化产业不适合“舶来模式”，照搬国外模式“水土不服”。

互联网产业中，每个成功的互联网企业，都或多或少“复制”学习了国外的成功模式，甚至有一部分国内企业实现了“青出于蓝而胜于蓝”的效果。比如我国互联网社交、搜索、电商、短视频、网约车等领域都取得了世界领先的发展成果。随着市场逐渐成熟，消费者水平、需求也变的更高，“舶来”模式遇到了瓶颈。

数字化产业中，以网络安全为例：美国政企客户数字化程度较高，对网络安全理解较深，网络安全需求贯穿企业发展之中，标品、SASE、服务、订阅等付费模式是市场主流。我国政企客户以项目建设型投入为主，网络安全需求仍然处于自上而下的阶段，对规划、咨询需求旺盛。因此希望靠“舶来”模式发展的部分企业，没有循序渐进，发展受阻。

第四大魔咒是标品化魔咒。互联网产业是靠标品化发家的，数字化产业的客户需求全面、复杂、多元，很难实现“标品化”。

互联网产业中，传统的互联网门户时代，用户获取信息往往通过编辑推荐、首页展示，用户习惯“千人一面”的信息获取方式。通过对用户行为大数据的采集和挖掘，用标品化的方式，实现“千人千面”的信息推送，获得新的发展机会。但是，遇到政府对大数据杀熟、个人信息过度收集、隐私信息泄露的强监管，这条路不好走了。

数字化产业中，客户业务复杂，个性化强，很难实现“标品化”。为满足不同企业的不同功能需求，服务提供商要对产品进行定制改动，研发周期一般是半年以上，这就造成一款产品的定制难、复用难。“标品化魔咒”既困扰客户，也让服务商付出巨大的人力和时间成本，吞噬毛利。

第五大魔咒是升级魔咒。互联网产业，后台升级是利器，而数字化产业，产品升级是难题。

互联网产业中，如果产品需要升级迭代，企业只需要服务提供端统一操作，后续则是用户对产品进行升级、安装、卸载的个人行为。不论是对企业还是对用户，升级迭代都很容易。现在由于强监管，互联网企业对产品进行更新升级时，必须对每一位用户进行告知、并获得同意，不再能后台静默升级。

数字化产业中，客户的网络结构、信息系统非常复杂，扩展、更换、新增产品或功能都比较繁琐，涉及到数据迁移、网络变更、算力扩容等多个环节。只要其中一个环节出现问题，就可能对业务带来极大影响。这种客观条件下，企业客户倾向于保持现状，除非现有

系统出现致命问题，否则不会贸然升级或启用新系统。产品升级的创新技术成为客户迫切需求。

第三部分 研发平台化——奇安信解开五大魔咒的钥匙

第一，研发平台化，能提性能、降成本，实现低成本获客，解开圈地魔咒。优质的产品和服务，是赢得 TOB 市场的根本途径。但优质是有代价的，它要求技术创新、性能稳定、差错减少，而研发平台化，能够以较低的代价，实现优质。比如，鲲鹏平台实现了性价比倍增。在提性能方面，鲲鹏平台集合了多种网络安全产品和功能，比如，防火墙、IPS、WAF、VPN 等，它打通各个网络操作系统，结束以往每个产品各自为战的局面，大幅提升产品性能。在降成本方面，鲲鹏平台有强大的适用性，能给国内外很多常见的 CPU、网络芯片提供支持，实现同规格硬件成本下降 50% 以上。

第二，研发平台化，能减少重复造轮子，激发组织活力，解开人效比魔咒。研发平台通过将核心安全共性需求标准化，把很多人从重复造轮子的现状中解放出来，让更多人聚焦更有价值的业务需求，推动产品和服务创新，从而大幅提升人效比。比如，鲲鹏平台的量产，相关产线 2021 年人均创收达到 410 万，同比增长 39.8%。相当于网络安全行业头部厂商的 2~3 倍！

第三，研发平台化，能紧贴中国国情，满足中国需求，解开舶来魔咒。以国际流行的 SASE 服务为例，在美国，客户业务普遍上公有云，SASE 服务节点也主要部署在公有云。但是在中国，简单引进国外流行的新技术，一定水土不服。SASE 服务是云服务，它的技术架构和实现比较复杂，很难本地化。就像我们很多互联网平台公司，有很强的技术系统，但它们无法复制给政府和企业。

奇安信的大禹平台，它具备了多种复杂数据的采集和存储，以及大数据分析和多种安全能力，又能搭载多种安全产品，能够把安全公司的云端 SASE 能力本地化，也就是公有的安全云变成私有的安全云。Q-SASE 就是基于大禹研发平台，实现了安全资源池中的各类安全组件（如 SWG、NGFW、WAF、流量探针等）的告警日志的采集、富化以及基于规则进行归并分析的功能。同时实现了和态势感知、运营平台的一体化。

第四，研发平台化，能用标品化生产，实现个性化需求，解开标品化魔咒。研发平台化的标品生产，就像乐高积木，用标准化的模块，能拼插出千变万化的造型。奇安信从 2020 开始，推动研发平台化、组件化、模块化、函数化，用函数搭建模块，用模块搭建组件，用组件搭建平台，用平台搭建产品，能快速推出满足客户个性化需求的产品。比如，态势感知，用定制化生产需要 9 个月，用大禹平台标品化生产，只要 3 个月，交付效率提升了 300%。

第五，研发平台化，具备强大的弹性架构，能让升级稳定、简单，解开升级魔咒。产品升级的技术创新，是解开升级魔咒的关键。只有帮助客户解决产品升级、更新带来的后顾之忧，才能增强客户粘性。奇安信的研发平台拥有分布式、弹性架构，能帮助客户实现平滑升级，解决以前不敢升、不愿升的难题。比如，大禹平台作为一个强大的安全中台，提供了丰富的接口，可以无缝集成进入原有企业网络中，与其他安全产品实现协同联动。同时其开放的扩展能力，使得能力更为丰富，应用更为快捷。

奇安信从 2020 年启动平台化战略，到今天已经完成了第一步，也就是研发平台化，可以提升人效比，帮助公司盈利。

未来，第二步是要实现产品平台化，真正实现安全产品协同与数据统一管理，全面提升产品竞争力，保持高增长速度。最终到 2025 年，实现能力平台化，适应安全行业整合化趋势，带领行业走向集中化，向全球第一迈进。

未来，奇安信将在合适的时间，向生态伙伴开放研发平台，让更多合作伙伴利用研发平台实现提性能、降成本，并以分布式、弹性架构，助力客户实现平滑升级。

实战大考 安全研发平台高分过关

大禹平台为代表的奇安信研发平台，经受冬奥“零 事故”实战考验，实现好、快、 省、多。

大禹平台解开圈地、标品化魔咒

“近一年来，我们遇到很多客户，无论是大型客户，如北京冬奥、南方电网、城市运营中心等，还是重要行业，如公安、网信、能源、工业、工信、运营商等，都对大型安全系统建设有着强烈需求，然而这样的方案在市场上面却迟迟没有出现。大禹平台就肩负着这样的使命。”奇安信集团副总裁、大禹平台负责人左文建表示。

图：奇安信集团副总裁、大禹平台负责人左文建解读大禹平台

大型安全系统普遍建设难 搭建中枢系统势在必行

为什么大型安全系统建设难？左文建总结了几个方面：首先是客户需求庞杂，安全系统会涵盖攻防、运营、监管等各类功能，非常复杂；其次是客户环境差异非常大，业务系统千差万别；第三是整合成本非常高，包括数据整合、能力整合等；最后是缺少整体性，经常是局部建设，导致系统经常推倒重来，造成极大的浪费。

更深层的原因，是整体安全架构落后于信息化或数字化发展的进度。“企业的信息化方案如 ERP、SAP、CRM、HRS 等都非常成熟，与之对应的是，安全架构依然是点状式建设，造成了分散建设、没法联通，关键时候还达不到预期效果，这是当前整体安全建设的困局和现状。”

如何破题？左文建举了一个形象的例子，“应该借鉴人体的神经系统，神经系统帮助人感知外部威胁，调动身体机能响应外部威胁。安全系统也是如此，我们应该构建独立的安全网络，并且建立强健的中枢安全系统。”

然而，人的神经系统是数亿年大自然进化的成果，要搭建安全网络的中枢安全系统，并非一件简单的事情。仅仅在技术上，就有海量数据、数据种类繁多、噪音很大等挑战，直接把互联网平台技术引入到企业中，势必会遇到方案小型化、高可维护性、成本难以承受等问题，而大禹平台的问世，就是要打造适合安全系统的中枢神经体系，解决这些复杂难题。

经受冬奥“零事故”实战考验 大禹平台实现好、快、 省、多

2019 年，大禹平台关键组件开发启动；2020 年，大禹整体研发正式启动；2021 年 7 月，大禹实验局正式

系统上线；今年 2 月，大禹平台在冬奥实战中获得了全面验证。

“大禹不是孤立的平台，它集成了公司多项关键能力，包括猛禽大数据存储分析引擎，海龙安全设备控制器，赛博威关联分析引擎，诺亚数据接口 ETL、玄机数据资源管理系统。通过这些组件集成，大禹平台的能力得到了极大的发展和提升，可以归纳为好、快、 省、多四个方面。”

首先是项目效果更好、更出色。以冬奥安全系统为例，它构建了运营中心、态势感知和指挥平台的三级架构，基于大禹平台，奇安信仅用 4 个月时间就完成了新增两个节点的建设和开发工作。而在奇安星城项目中，对于高度复杂的多级结构，大禹平台设计了就近数据进行分析计算、合理分解安全级层职责、集约化建设减少投入成本等三大特点。实际来看，基于“大禹”构建的中枢安全系统是经得住考验的，并具有伸缩性、通用性、可配置性等优势，堪称一个“好方案”。

其次是项目开发速度得到快速提升。在冬奥网络安全保障中，奇安信团队依托大禹平台，在冬奥项目组的紧急需求下，以及中国工程院院士方滨兴的指导下，仅用10天时间，实现了蜜点分析、高频攻击分析等功能开发，且自动化生成委外的研判数据，减少了上百人的研判成本。“如果不基于安全中台模式，开发至少需要 100 天以上。”

第三是大禹平台可以显著节省研发成本。左文建表示，此前构建一个大数据安全产品时要花 9 个月，但有“大禹”之后，态势的大禹版本、安全数据感知平台、API 安全感知平台、Q-SASE、TSOC 他们研发第一个版本的时间都从 9 个月下降到 3~4 个月，整体效率就提升了 2~3 倍，对应的研发成本和时间成本，得到了大大的节省。

最后大禹平台具有更强的开放性，可支持更多能力和应用。大禹基于开放架构，通过能力接口支持集成行业的安全能力，通过数据接口支持扩展新的功能特性。未来把整个“大禹”平台开放出去，就能够在上面有更多的应用被更多地开发出来。

大禹构建中枢安全系统 解开圈地魔咒、标品化魔咒

在奇安信研发平台战略发布会上，董事长齐向东指出，数字化产业存在获客成本高、试错成本高的“圈地魔咒”，以及标准化产品无法满足个性化需求的“标品化魔咒”。事实上，大型安全系统建设市场需求非常大，不仅要体系化视角、系统工程思维，还具有随时调整、随时变化的实战需求，大禹平台构建的中枢安全系统，堪称解开两个魔咒的最佳钥匙。

“构建安全未来是大禹平台的愿景，我们下一步将持续研发，不断提升安全能力、质量和效果，以大禹安全中台为客户建立中枢安全系统，以大禹为基座加速新领域的安全产品研发，助力整个网络安全行业的发展。”左文建表示。

川陀平台打破“快好省”不 可能三角

“奇安信拥有多达 30 多款的终端产品舰队，业内遥遥领先，我们基于川陀平台的统一式量产，在保障高质量、低 bug 的前提下，成本下降了 2/3，打破了产品研发中‘好、快、省’的‘不可能三角’。”奇安信川陀平台技术负责人刘浏表示，基于川陀平台可以又快又好又省的批量生产各种终端安全类产品，并且成功兑现了北京冬奥会网络安全“零事故”的承诺。

刘浏表示，终端安全历经多年发展，已经形成包含终端反病毒、终端准入、终端检测与响应、补丁管理、服务器安全、工业主机安全、移动安全、物联网安全、国产化终端安全等多项细分领域的“大家族”，并且其内涵和外延仍在不断发展，市场需求极广。IDC 数据显示，2022 年全球企业级终端安全市场规模将超过 92 亿美元，年复合增长率 8.6%。

与此同时，作为国内终端安全领域老牌供应商之一，奇安信拥有一支由终端安全管理系统、终端安全响应系统（EDR）、安全 U 盘、网络安全准入系统（NAC）、移动安全管理系统（TrustSpace）等 30 款产品组成的庞大“产品舰队”。根据 IDC 最新发布的数据，奇安信从 2018 年到 2021 年，连续四年领跑终端安全软件市场。

“起初，奇安信各类终端安全产品的研发工作，分布在多个独立的部门。”刘浏说到，但很快问题出现了，尽管每款新产品都被期望能又快又好又低成本的开发出来，但“快好省”的三角始终难以兼顾，出现了快 + 好 = 贵、好 + 省 = 慢、快 + 省 = 差的窘境，这就导致了人均产出无法提升、定制化开发周期长的“人效比魔咒”和“标品化魔咒”。然而面对庞大的终端安全“舰队”和越来越细分的终端安全需求，需要一个统一的平台支撑，可以又快又好又省的批量生产各种终

图 奇安信川 陀平台技术负责人刘浏

端安全产品。

于是，川陀平台应运而生。

据刘浏介绍，川陀平台面向终端管控类业务提供一套可复用、可扩展、高性能的终端管控平台，满足终端管理、终端分组管理、用户分组管理、任务管理、策略管理、级联管理、系统设置管理等多项管控类业务开发需求。

川陀平台为终端安全产品的研发提供了三大“秘密武器”。

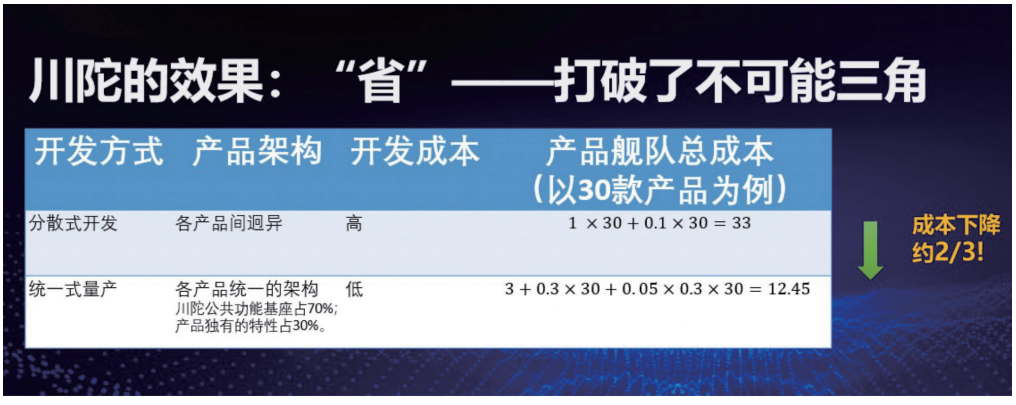
第一，是一套需求抽象方法论。川陀平台已将终端安全产品开发所需绝大部分的共性功能抽象成模块化组件，工程师只需专注于当前产品特有功能需求的研发，从而大大降低了重复造轮子的现象。

第二， 对功能模块的深耕。川陀平台整合了任务管理、策略管理、级联管理、系统设置管理等终端管控的全部共性能力，并且每项能力都达到了行业领先水平。

第三，高效的反馈回路。川陀平台搭建了包括客户反馈系统、问题回报系统在内的多途径的高效自动化的反馈回路，以软件交付常见的“兼容性问题”为例，这套系统可以自动化的收集、分析和处理各种产品问题，一旦问题被转换成“产品经验”，会自动利用平台化优势快速复制到其他各产品。这一反馈系统，为产品快速迭代改进插上了效率的翅膀。

据介绍，基于川陀平台，奇安信终端安全产品的研发实现了“快好省”的统一。在“快”方面，以“云安全管理平台”这款产品为例，基于川陀平台，该产品仅用三周时间就重构完成了旧版本耗时一年开发的功能点。一线工程师反馈基于平台化研发就像拼乐高积木；在“好”方面，川陀平台生产的产品，整体 Bug 数量会下降超过 90%，优秀的产品质量直接推动了旗下天擎终端安全管理系统 V10 在一年内装机量达到千万级；在“省”的方面，终端安全类产品研发成本平均降幅达到了 70%。

“目前，川陀平台投入期已提前结束，并进入量产阶段。”刘浏强调，很快奇安信全线终端安全类产品都将基于川陀平台进行研发，预计将实现 100% 以上的研发效率提升和研发成本的显著下降，真正打破困扰网络安全行业的“人效比魔咒”和“标品化魔咒”。



鲲鹏平台打破人效比魔咒

“鲲鹏平台 2021 年量产后，相关产研的人均创收达 410 万元，达到网络安全行业头部厂商的 2-3 倍；人均创造毛利 266 万元，大幅领先于行业平均水平。”奇安信集团副总裁、首席架构师兼鲲鹏平台负责人吴亚东日前表示。

图：奇安信集团副总裁吴亚东解读鲲鹏如何打破“人效比魔咒”

作为平台化战略的重要一环，鲲鹏平台已然成为破解“人效比魔咒”的密码。

增收不增利不增效 “人效比魔咒”成为行业痼疾

众所周知，以防火墙、上网行为管理等产品为代表的网络边界安全领域，是国内网络安全中历史最悠久、客户需求最大、市场竞争最激烈的细分领域之一，市场成熟度较高。根据方正证券研究所综合 IDC、安全牛等第三方机构的数据估算，网络边界安全的规模将超过 250 亿元，是网络安全行业中最大的细分赛道。

然而，随着网络安全形势的日益严峻，为满足客户日益增长和多样化的网络安全需求，大部分网络安全企业不得不投入更多人力，导致营收虽然稳步增长，但人均创收和利润并没有明显变化，使企业陷入了“人效比魔咒”的怪圈，为快速发展蒙上了一层阴影。

“以边界安全市场为例，其空间巨大的同时也面临着诸多挑战，例如产品同质化严重、质量参差不齐、市场需求迭代慢、人海战术背道而驰等等，这也导致企业经常增收不增利、增收不增效，人效比普遍不高。”吴亚东表示，寻找破解密码，已成为了网络安全企业的当务之急。

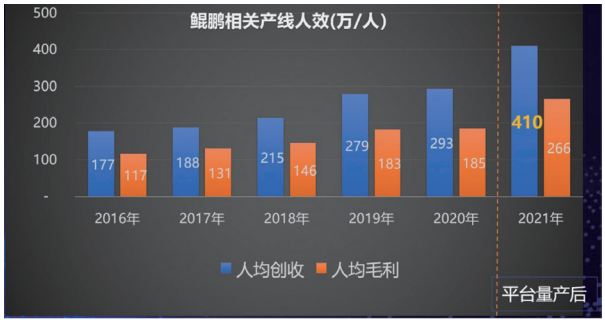
“鲲鹏平台能减少重复造轮子，激发组织活力，显著提升人效比。”吴亚东介绍，作为业界领先的边界安全产品专用网络操作系统，鲲鹏平台具备一体化的安全引擎、开放的软件定义安全架构、全功能的高性能用户态协议栈、网络功能虚拟化等多项优势，能够为网络边界安全设备提供数据通信和应用安全相结合、虚拟化安全网元的管理和流量编排以及网络安全的资源池化等能力，可使产品具备开放式架构，便于快速、按需部署，以及能低成本扩展出不同的安全功能，消除了对细分专用安全设备的依赖。

人均创收 410 万元 2~3 倍于行业头部厂商

依托于鲲鹏平台硬件解耦的软件架构，面对市场各类国产化硬件平台，奇安信边界安全产品的适配速度可提升 90%，能够轻松应对客户侧复杂的 IT 架构和网

络安全需求，降低对人员的依赖，带来人效比的大幅提升，从而取得市场先机。基于鲲鹏平台，奇安信连续 2 年中标中国移动防火墙集采以及中国联通防火墙集采项目，同时 2021 年入围了中国银行信创防火墙集采项目。

数据统计显示，鲲鹏平台 2021 年量产后，产研人员的人均创收超过 410 万元，同比激增约 40%，达到网络安全行业头部厂商的 2-3 倍，同时人均创造毛利 266 万元，同比增速更达 43.5%。另一方面，边界安全等相关产线的研发效率（创收 / 研发投入）在 2021 年达到了 9.5，较量产前同比提升 40%，较未使用研发平台时提升更是达到 70%。



除了打破“人效比魔咒”，鲲鹏平台还帮助相关产线提性能降成本，实现低成本获客，解开获客难的“圈地魔咒”。“通过鲲鹏平台的量产应用，同等规格性能下成本降低一半，让边界安全系列产品的性价比实现了倍增，边界安全产线 2021 年营收同比增长 47.4%，三倍于 15.8% 的网络安全行业平均增速（中国信通院数据）。而毛利同比增长 51.2%，实现了‘增收更增利’。”

值得关注的是，鲲鹏平台还实现了持续引领网络安全技术创新，极大降低试错成本，实现低成本获客和留存。例如面对各类安全产品解密性能不理想的现状，鲲鹏平台基于高性能硬件解密 + 异步调用技术，将解密效率提升了 10.6 倍，同时通过高性能 SSL 服务链编排技术，实现平台一次解密、多次编排，可将解密后的流量自动分发给其他安全设备进行后续处理，从而进一步提升整个纵深防御体系的流量防护能力。据了解，此项技术已在此次北京冬奥会网络安全保障工作中，取得了良好的实践效果。也正因如此，基于鲲鹏平台，奇安信也快速孵化了边界安全栈等新一代网络边界安全产品，并赢得了大量客户的青睐。

“成为支撑集团网关类产品发展方向的专用的高性能和多业务融合的网络操作系统平台，并且达到国际领先水平是鲲鹏平台一直以来不懈努力的方向。”吴亚东强调，未来鲲鹏平台要能促进高性能 SSL 服务链技术、国产化和高性能 SoC 等硬件平台的产品化和规模化应用，实现国内领先水平，并持续协助产品线提高技术竞争力和产品交付能力，构建成熟交付复用体系。

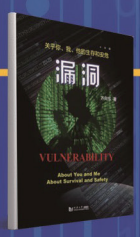
据悉，伴随着奇安信网络安全能力平台化战略发展，鲲鹏平台及其他研发平台还会适时向生态伙伴全面开放，适应安全行业整合化趋势，带领行业走向集中化，改变“小零同”（小规模、零散化、同质化）的现状。 安

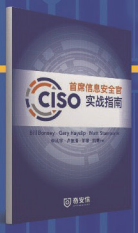
奇安信

BEIJING 2022

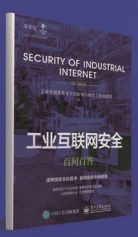
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

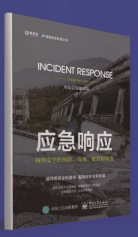
奇安信图书馆





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。

上千亿条冬奥相关日志，赛博威不仅仅是“已阅”

作者 魏开元

作为世界上规模最大、影响最广、竞技水平最高的冬季综合性体育赛事，冬奥会的吸引力似乎已不再局限于冰雪运动员及爱好者。随着数字化技术的日益普及，无论是组织严密的黑客团伙还是民间网络犯罪分子，都试图寻求对奥运会进行网络攻击。比如在平昌冬奥会在开幕式当天，包括冬奥会网站、电视服务在内均遭到黑客攻击，导致部分业务中断。

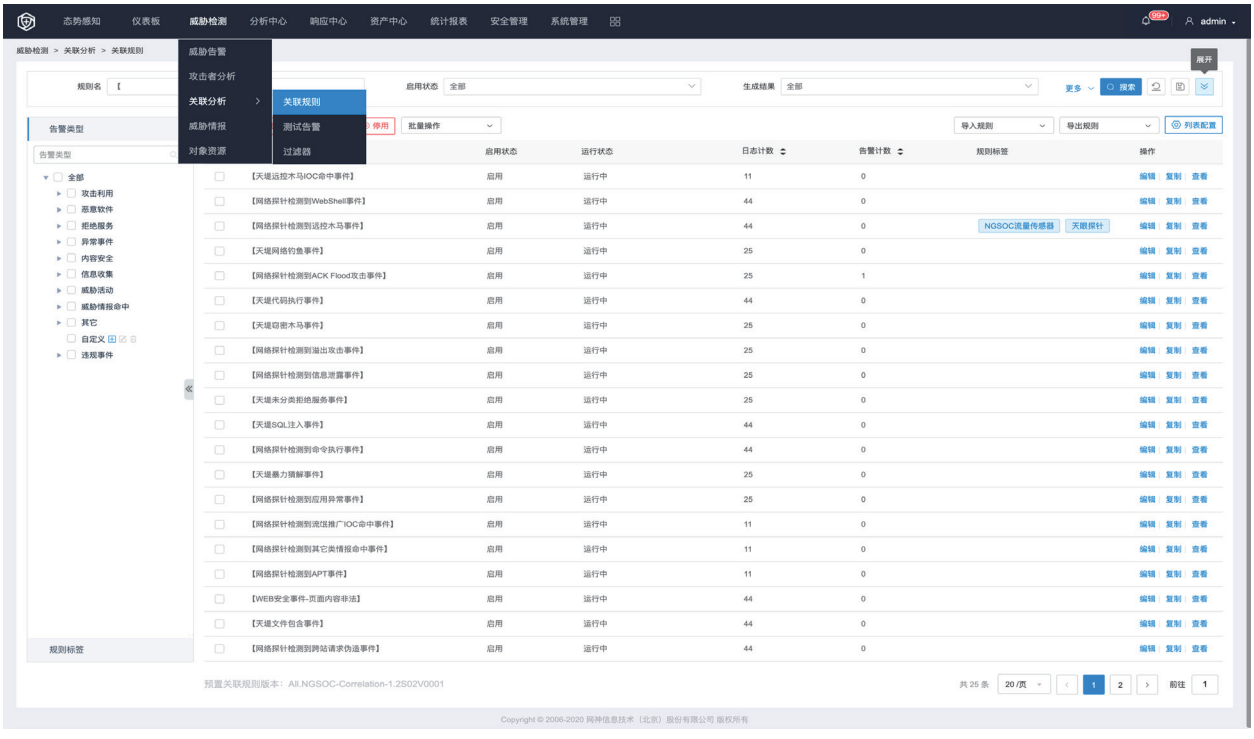
面对网络攻击的压力，在北京冬奥会，奇安信首创了冬奥会系统安全体系，实现了网络安全的“零事故”。而在零事故的背后，其中一项关键性技术就是奇安信集团自研的大数据实时关联分析技术 -Sabre（赛博威）引擎，它支撑起对冬奥 26 个场馆、上千亿条日志的实时监控与安全分析，累计监测数亿次网络攻击，跟踪和研判上百起涉奥威胁事件。

冬奥是一个实时关联分析技术的非常典型的应用场景，具备完整要素。

多源异构数据的采集

毋庸置疑的是，安全运营是落实网络安全防护的最重要手段之一，而安全运营的核心是安全分析，安全分析的核心目标是找出异常事件，并判断这些异常事件是不是由网络攻击造成的。

在这里，事件是 IT 系统中某一活动产生的一组数据，体现的是一个对象，它是有特定的属性和对应的属性值组成。比如一个防火墙事件可能包括源 IP 、包括



目的 IP、目的端口等信息，而这些数据都被以日志的形式记录了下来。

所以想要找出异常事件，安全分析的第一步，就是把日志数据都采集起来，并以事件流的方式输入到安全分析引擎中。

“冬奥期间的日志数据来自于 18 类、共计 1000+ 数据源。”奇安信实时安全分析引擎负责人覃永靖介绍，冬奥期间，所有 IT 系统和网络设备的日志都要汇聚在实时数据平台，不仅仅包括奇安信部署的自有防火墙、SD-WAN、天擎等 55 款 813 台各类安全设备，还包括终端、服务器、网络设备、应用系统、业务系统等所有各类 IT 资产。

这些数据源分布在各个场馆、网络中心、数据中心以及云上系统，它们所产生的日志会被源源不断地送到实时安全分析引擎中进行关联分析。

这其中就产生了三个要特别注意的问题。

第一是尽可能采集所有安全相关日志，不遗漏相关数据。全量日志数据是不发生漏报的最基本条件。网络攻击尤其是 APT 攻击的发现往往取决于看到细节的能力，部分数据漏掉后就很容易产生“漏网之鱼”。比如一次突然的异地登录或者一个未知域名的访问，这些都有可能是已经被入侵的信号。如果采集的数据不全，这些信号就可能会被错过了。

第二是需要将采集的数据尽可能快的发送到安全分析平台，日志在源源不断的生产，后面分析引擎处于一刻不停的自动分析过程中，采集到的数据需要确保一定的时间线，即前后的时间差需要在一个窗口之内，时间相差太大的日志会影响分析的资源和结果产生影响，因此在整条数据流水线上需要保证一定的实时性。

第三是要能够对各类不同的安全日志进行标准化采集、传输解析和处理。数据源不只有奇安信自有的安全设备，还有多个不同供应商的各类应用，这其中不只有网络安全厂商，还包括网络设备提供商、云计算提供商、应用软件提供商甚至包括大大小小的开源组件等等，所以对于多源异构数据的支持也非常重要。这个过程叫做归一化，不同类型但相同含义的字段需要统一类型和名称，为后面的实时安全分析做好准备。

实时安全分析

日志收集起来后，仅仅是“已阅”是不行的，实时分析引擎的核心应该是“判”。

安全分析方法主要包括两种；第一种是延迟计算，即数据收集和安全分析分离；第二种是实时计算，也就是数据收集和安全分析同步进行。

显而易见的是，在每天能够产生超过 40 亿条日志、峰值可以达到近 10 万条每秒的冬奥网络环境下，实时计算更加合适。

否则安全事故没准已经发生了，计算还没开始，这还谈何零事故。

奇安信的实时安全分析引擎分为三层。底层是大数据集群，主要用于日志数据的采集、存储和预处理。大数据集群为实时安全分析提供了强大的算力支持，否则面对如此海量的多源异构数据就该“罢工”了。

中间层主要进行安全分析，它基于目前最流行的开源实时计算框架 Flink 构建，负责利用各种技术手段，同时结合威胁情报、漏洞情报、资产等知识数据，对日志进行安全分析。

最上层则是应用层，负责与用户进行交互，输出分析结果和向安全分析引擎传输用户指令。

众所周知，安全分析的关键要素就是时间，即要求能在最短的时间内发现网络攻击行为、响应安全事件，并且在发现新型攻击行为之后，能够第一时间上线针对性的安全检测方法。

显然，快速完成安全分析是零事故的另一个关键保证，它能够将网络攻击控制在最小范围内。

好在 Flink 最重要的特点是允许以数据并行和流水线方式执行任意流数据程序，并且具备高吞吐低延迟的能力。这就意味着，在充足算力的支持下，即便冬奥期间的日志量再大一些，奇安信安全分析引擎依然能够平稳运行，保证日志分析的速度和准确度。

但安全分析的目的是要找出异常事件，因此用户需

要快速实现威胁建模，并在特定模型下将计算结果与外部输入的检测规则、威胁情报、漏洞情报等知识库进行匹配。

所以，安全分析引擎不仅仅要求极快的计算速度，还要使用起来非常便捷，这样才能最大化提升安全分析的效率。

对于后者，原生 Flink 框架的支持力度是远远不够的。

“所以我们提供了一种针对安全分析场景进行特定优化的安全分析语言。”覃永靖说，它满足了以下几个特点：

第一，简单易用，学习成本低，易上手，能够满足一个没有研发背景的人，也能经过简单学习之后就能上手使用。

第二，支持丰富的数据类型，这些数据不仅要包含文件读写、网络访问等基础数据类型，还要包含大量的安全数据比如 IP，各类时间、资产、漏洞、威胁情报、地理位置等，用户可以不做任何定制就能直接对这些数据进行关联分析，因为这些数据能够为安全分析提供大量的直接证据。比如恶意软件感染发生的时间，感染的主机类型、数量、与外部发生通信的 IP 地址、使用的漏洞、攻击载荷等等。

第三，提供丰富的语义，尤其对安全分析语义进行增强和定制以及扩展。安全分析的场景是复杂、多变的，没有丰富的语义很难满足所有安全分析的需求。但即便是这样，不同的网络环境依然会面临无对应语义的情况，这就需要有经验的分析师进行个性化扩展。攻击手法的变化非常频繁，对于安全分析来说，总会遇到一些安全语义无法判断和解释的行为，尤其是冬奥场景，这对于国内安全厂商来说都是头一回，很难保证不出现什么意料之外的局面。

行为分析与复杂事件关联

如果分析结果能够与已知的规则、威胁情报进行匹配，比如 URL、IP 地址、文件 MD5 等，那自然是网络安全问题无疑，但还有一些时候并不是这样。

举个典型的例子，比如内网某主机的流量经常会明显高于其他同类型主机。

这当然有可能是该主机已经被攻陷，被植入了一些特殊的木马导致流量异常增高。攻击者使用了全新的特种木马和基础设施，导致终端安全软件并没有检测出来。

但如果是仅凭流量偏高这个条件，分析人员很难判定它是异常，因为分析工具并没有一个基线标准能够进行比对，有可能就是有一些特殊业务或者特殊时间段，导致流量偏高。

针对这种事件，行为分析是一个非常有用的安全分析方法，它通过学习待分析对象的历史数据生成安全基线，来检测异常行为。比如今天这个主机的流量不仅比同类型其他主机高，也比历史平均水平和流量峰值高出许多，那基本可以判定是异常行为，需要进一步检查。

从中能够看出，安全基线是判定异常行为的核心。

安全基线分为三类，第一类是统计类安全基线，包含常见的时长、大小、频率、空间、范围等多种形式；第二是序列类，比如指数平滑类和周期类安全基线，具备明显的时间先后顺序或者周期规律；第三是机器学习类的安全基线。（基线详情可参考《当你不知道孰是孰非的时候，总有一个引擎在默默制定判断标准》）

在冬奥场景中，基线检测的应用范围会更加广泛。作为一个全新搭建起来的复杂信息系统，不论是人还是安全设备，都会感到非常“陌生”。因此，历史数据的学习，对于检测异常行为而言十分必要。

除了行为分析以为，关联分析也是必不可少的一项手段，它主要适用于两个场景：第一，单一事件无明显异常，但多个相关事件进行关联则表现出明显异常；其二，单一数据源无法反应攻击全貌，需要综合终端、流量、服务器等多个数据源进行全局关联分析，还原完整攻击链条。

再举两个例子。日志显示，多个高危端口短时间内被多次扫描并尝试登录；内网某服务器发现非法访问行为。

这些事件可能独立发生，也可能会同时发生，之间可能有关联也可能没有关联。如果结合前文中的例子，那么完整的事件就有可能是攻击者攻陷了某内网终端，并利用该终端通过高危端口访问某服务器。

这就是关联分析的重要意义。

“关联分析是一个常用的安全分析方法，比如当发现某个安全事件后需要将攻击者信息进行全局关联，来发现是否还有其它攻击行为。”覃永靖说，这就像拼图游戏，缺少一块是永远拼不完整的。

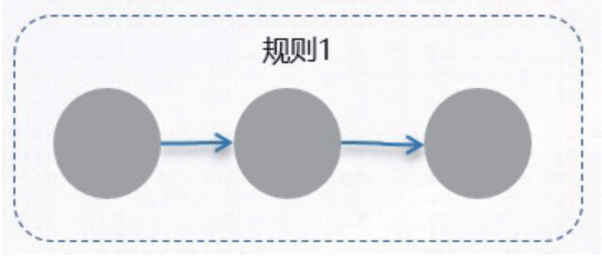
性能优化与状态监控

需要注意的是，对于冬奥这种全球瞩目的大型体育赛事，对于业务的连续性要求是近乎严苛的。大到全球的电视转播，小到一个记分牌或者计时牌，都不能中断。

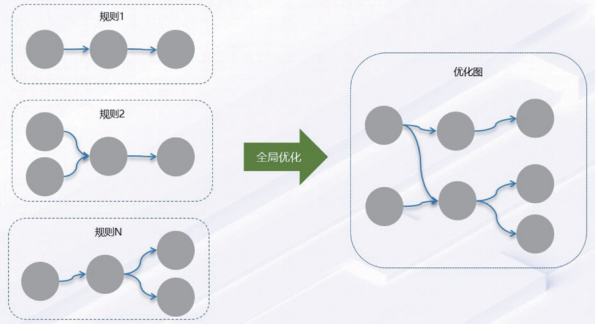
这也就是说，网络安全事故是决不能出现的，但同时也绝对不能出现“网络攻击没把网络搞瘫，‘安检’却把它搞瘫了”的现象。

这就需要对性能和资源使用进行优化，防止占用过多硬件资源。

对于实时分析引擎而言，每条检测规则可抽象为一个逻辑子图，用于表达检测流程，就像下图这样：



然而一个安全检测集通常包含上千条规则，如果同时运行这么多规则，必定会消耗大量的资源，因此需要在全局层面进行优化，将分散的子图转换为一个执行图，以此大幅降低计算复杂度，大致过程如下图：



另外一个需要重点优化的就是外部数据的匹配。在冬奥期间，奇安信累计投入生产了超过 25000 条高质量的威胁情报，如果再加上 10000+ 台终端信息、漏洞情报信息以及各种黑名单、白名单，这个数据量是相当大的。如果每次事件都进行一一匹配，就相当于挨个“打招呼”，不仅需要大量时间，还会造成性能损耗。因此分析引擎需要支持一些数据匹配和存储的优化计数，包含精确、范围和模糊匹配的方法，来提升匹配速度。

比如威胁情报、资产、漏洞、各种白黑名单等，对于超大规模数据表的匹配会带来一些很大的挑战，比如大规模串正则匹配问题等，比如超大规模串正则匹配引擎（100w+），hash 匹配、大规模 IP 匹配计数，包含精确、范围和模糊匹配，以及大规模知识库存储和匹配的优化方法。

万事俱备，然而当引擎真正运转起来之后，作为使用者，还得关心它运行的好不好，如果某些组件资源占用过多，就得对其采取下线、隔离或者限制资源使用等措施了，防止影响其他规则甚至业务的正常运行。

当然，有时候也不能过快了。

实时分析引擎的下游业务可能是一些处理能力比较慢的流程，这时候就需流量控制，防止较快的处理流程向较慢的处理流程输入过多的数据而引起资源过度消耗和卡顿。流量控制需要支持主动流量控制、被动流量控制以及时间窗口相关的流量控制，通过用户配置或自动处理来解决前后处理性能不一引起的数据丢失和系统不稳定问题。

粗算起来，冬奥期间经过实时分析引擎的日志数量就超过了 1000 亿条，产生的告警数量也是极为庞大的。这样的爆肝能力搭载在奇安信 NGSOC 上，难怪会让奇安信冬奥重保奇安信冬奥保障总架构师尹智清直呼“爱了爱了”。

不过，保证冬奥零事故也不是就靠一个实时分析引擎就能完成的，而是人 + 工具 + 流程 + 数据的交互结合，并且不断完善的动态体系。

而奇安信冬奥期间实时安全分析所累积的经验，也将为整个中国乃至全球的网络安全服务。 安

灵魂四问，看奇安信如何保障上万冬奥终端“零事故”？

作者 研究员 王梦琪

“终端是数据和应用的重要载体，具有数量多、弱点杂、易利用的特点，又能深入内网，一直以来都是黑客攻击的重点目标。”

2019 年 12 月，奇安信正式成为北京 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，承担完全的、彻底的、端到端的安全责任。在短短两年的时间里，北京冬奥业务和网络安全从“0”开始建设，面对北京冬奥系统建设周期短、生命周期短的艰巨挑战，面对涉及 306 个场馆及服务设施、62 个业务系统、37 家开发商、10000+ 台终端的复杂形势，奇安信最终圆满完成网络安全保障工作，实现冬奥“零事故”。

那么，作为冬奥网络安全最重要的一环，奇安信又是如何在有限资源和时间内保障上万终端“零事故”的呢？接下来，我们可以从以下问题中一步步找到答案。

三个一定，北京冬奥终端安全形势有多严峻？

2020 年日本东京夏季奥运会、2018 年韩国平昌冬季奥运会、2016 年巴西里约热内卢夏季奥运会……历届奥运会都是网络攻击的目标，无论是以经济利益为目的的黑客组织还是国家级黑客，都会利用各种手段发起攻击。2022 年北京冬季奥运会也不例外。而北京冬奥涉及的终端包括办公终端、运维终端、赛事终端、IoT 终端、打印终端和证件查验等多种类型，总计 10000 多台，对黑客而言就是 10000 多个暴露面。因此，终端一定会被攻击。

每台冬奥终端都发挥着重要作用，例如，办公终端承载着整个冬奥的办公业务系统，运维终端负责各类后台业务系统的维护，证件查验终端负责处理人、车顺利通行，包括 OVR 终端、解说员终端、信息查询终端等专用终端在内的赛事终端则关系到比赛的正常进行和全球直播。因此，攻破一定出事故！

冬奥终端分散在 5 张大网、90 多张小网的 306 个场馆及服务设施，一旦出现事故，就不可能是悄无声息的，也不会有足够的时间去慢慢解决。如 OVR 终端承载着现场成绩处理系统，面向全球直播，所有比赛的比分进展、状态进展都在这个系统里做呈现，如果被攻破，比分可能被篡改，比赛可能会终止。因此，出事一定捂不住。

迎接实战，北京冬奥终端安全保障有多困难?

“要想把分散在 306 个地点的 10000 多台不同类型的冬奥终端真正保护起来，并不是件容易的事，对防御能力和运营保障有着极为严苛的要求。”谈到冬奥终端安全保障，奇安信冬奥保障总架构师尹智清深有感触。

冬奥是全球热点，必然会遭遇多类威胁攻击，甚至是外部攻击与内部威胁并存，再加上北京冬奥的特色又是“科技冬奥”，人工智能、物联网、5G、云计算、大数据等新技术大量应用，网络环境更加开放，也更追求数据集中与共享，实现了多国、多地、多机构、多业务系统、多架构连接。因此，任何一台终端没有保护到位，任何一类威胁没有防御到位，任何一种隐患没有排查到位，任何一个策略没有执行到位，都可能导致冬奥终端被攻破。

由于冬奥终端数量多、类型杂、分布广、连续性要求高，一旦出事必须做到分钟级响应，因此，有 200 多名终端安全运营人员，分别在云端、冬奥技术运行中心、各个冬奥场馆等处进行值守，他们各司其职，共同对终端安全负责。然而，这些运营人员的知识背景和实战能力各不相同，遇到的问题也是千差万别，对同一安全问题的分析和处置能力也不可能完全相同。因此，如果提高不了终端安全运营工作本身的效率和效果，降低不了运营过程对个人经验的过度依赖和人为失误的产生几率，完成不了安全事件的高效闭环处置，冬奥终端安全依然无法得到有效保障。

多重挑战，奇安信如何实现终端“零事故”？

面对冬奥整体环境复杂、严峻、困难的挑战，终端安全仍然做到了安全“零事故”和服务“零事故”。安全“零事故”的背后，是多达 5847 次恶意软件、423 次恶意 DNS、326 次非法终端接入等各类攻击被成功防御；服务“零事故”的背后，是 200 多名运营人员对 6600 多次事件反馈的高效处理。综合整体冬奥实践来看，奇安信在冬奥项目中所应用的终端安全新思路，是行之有效且能够切实解决终端安全问题的。

在近期举行的奇安信冬奥“零事故”终端安全经验分享会上，奇安信集团副总裁、奇安信冬奥终端安全保障负责人张庭为大家分享了终端“零事故”背后的成功

经验——“体系化防御，数字化运营”。这是奇安信倡导的终端安全新思路，以确保各类终端“可信、合规、安全”为核心目标，通过“体系化防御”健全终端安全能力，运用“数字化运营”保障终端安全效果，从而确保终端安全能力的持续有效和稳步提升。

在冬奥终端安全保障中，“体系化防御”由注重实效的一体化终端安全解决方案奇安信天擎 V10 进行实现，在安全能力全覆盖、安全管理全统一、安全响应全协同的基础上，支撑起冬奥终端安全四层防御体系：第一层集成了 QCE 云查引擎、OWL 特征引擎、QDE AI 引擎等多款防病毒引擎，能够有效检测与清理已知恶意代码；第二层基于六合引擎实现高级威胁精准防御；第三层利用天擎 EDR，完成行为采集、威胁检测响应与溯源；第四层则利用第三代安全引擎天狗实现 0day 漏洞防护。

在“数字化运营”方面，数字化终端安全运营支撑平台奇安信 ESOP 则是重要支撑。基于冬奥自身的业务特点和严苛的安全需求，奇安信梳理了 1000+ 任务和 100+ 流程，并通过奇安信 ESOP 进行了落实，在基础数据集中化、运营目标数字化、运营过程标准化、运营效果可视化的基础上，实现了安全状况可衡量、安全责任可分配、安全效果可呈现。

“体系化的防御、数字化的运营是终端安全的未来，冬奥‘零事故’则充分证明了这一点，在新思路的指导下，奇安信终端安全防御系统面对多重挑战交出了满分答卷，整体能力再上了一个新台阶。”张庭总结到。

创新引领，终端安全下个时代在哪里？

冬奥“零事故”，彰显着以奇安信为代表的网络安全龙头企业综合实力和竞争力，让行业有了新的认知，引发对终端安全未来的思考。在此前的奇安信冬奥“零事故”终端安全经验分享会上，赛迪顾问业务总监高丹认为：“终端安全产品从最早期满足合规的防病毒产品，已经演变成包含管理、监测分析、响应处置等功能于一体的体系化防御阶段。”

“未来终端安全市场发展趋势，正随着安全风险的持续性变化，终端安全防护也需要向持续化运营的方向转变。在终端资产管理的过程中就有必要加入运营的思路，满足合规化部署与持续化管控的双方面需求；应用持续检测和响应的手段，来构建快速迅捷的主动防御；与平台化产品形成联动，提供持续化的安全运营服务。”

经过实战检验，奇安信终端安全新思路“体系化防御，数字化运营”在冬奥这样极端的复杂环境和严苛的安全要求下依然交了“零事故”的完美答卷，未来还将持续完善、落地，为更多政企客户解决各类终端安全问题。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

要快、要好、还要省？小孩子才做选择，成年人全都要！

作者 研究员 张少波

产品经理：“开发的兄弟们，咱们这个新版发布时间，能不能再提前几周？”

交付主管：“客户希望这版性能要好、bug 要少，还要稳定可靠……”

HR：“对不起，HC 已经锁了，其他部门也抽不来人了。”

……

“少小不努力，长大敲代码”。话说每一位程序猿、攻城狮，上辈子都是折翼的天使。他们经常要加班加点，没完没了的写代码，满足各种需求变更，争抢工期，保障质量。尤其是，他们经常要同时满足三个不同的愿望：

愿望 1：产品经理希望开发更快

愿望 2：销售、交付们希望质量更好

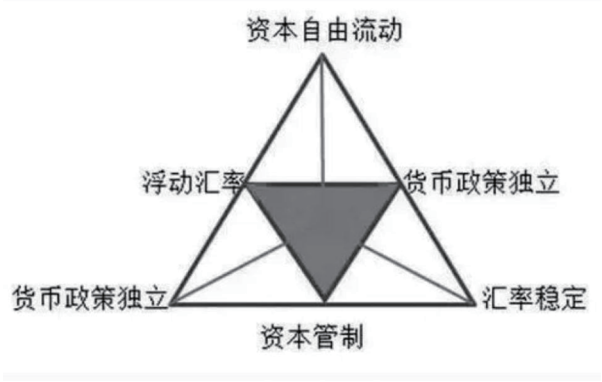
愿望 3：HR 需要更高的人效比，即控制好人力成本

说实话，满足其中两个需求，通常就需要使出洪荒之力了，如果要实现三个，即便是将阿拉丁神灯召唤出来，也未必能够得偿所愿。

引用奇安信川陀平台技术负责人刘浏（人称：刘大爷）的话，对于每一位具有匠心的产品经理来说，都期望每款新产品能又快、又好、又低成本的开发出来，但真正在做一款产品时，必定会在“不可能三角”中艰难取舍。

为什么同时满足三个需求，就非常难呢？这里要普及一下“不可能三角”的概念。

不可能三角（Impossible trinity），原本出自于经济学领域，主要指经济社会和财政金融政策目标选择面临诸多困境，难以同时获得三个方面的目标。在金融政策方面，资本自由流动、固定汇率和货币政策独立性三者也不可能兼得。



“不可能三角”虽然起源于经济学领域，但实际上在我们生活中，可以说是无处不在。比如说找工作，“钱多、事少、离家近”，就是常见的不可能三角。爱情中也存在“不可能三角”，女生选择男生的标准，则不可能同时高帅、专一、有钱；男生选择女生，“不可能三角”就变成了漂亮、温柔、独立。还有选择餐馆的“不可能三角”：好吃、便宜、人少。

这个三者难以兼得、最多选二的规律，就叫“不可能三角”。

那么，传说中的“不可能三角”真的无法打破么？是否有一种钥匙，能让我们放弃取舍，实现三者兼得呢？

答案是肯定的。

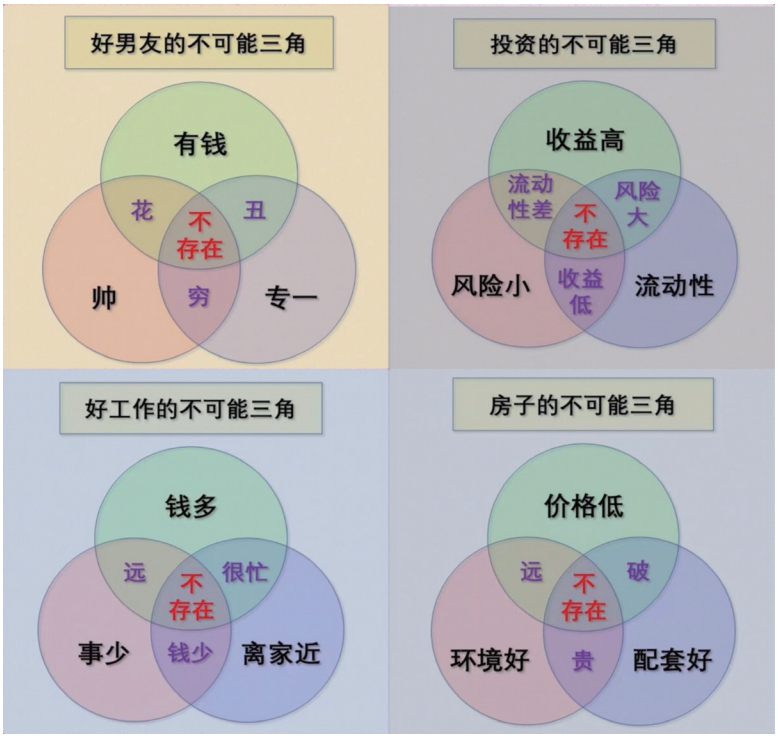
有句话说的好：小孩子才做选择，成年人全都要。

对于一个优秀的研发团队来说，就是需要解锁出“三头六臂”的必杀技，同时满足“快”“好”“省”的各种需求。

奇安信推出的研发平台，就是在探索能实现“高效率、高品质、节省成本”的三全之道。

奇安信集团董事长齐向东曾说过：数字化产业中，经常会遇到两个魔咒：第一个是人员增速超过营收增速的“人效比魔咒”，就是服务客户越多，工作量越大、开发周期越长，相匹配的人员就越多，导致人力成本也越多。

第二个是标准化产品无法满足个性化需求的“标品化魔咒”。数字化产业中企业客户业务复杂，个性化强，很难实现“标品化”。为满足不同企业的不同功能需求，服务提供商要对产品进行定制开发，研发周期一般是 9 个月，这就造成一款产品的定制难、复用难。



研发平台是如何解决的呢?

首先拿“快”这一维度来说。奇安信集团副总裁、大禹平台负责人左文建给出的钥匙是：“依托大禹平台，奇安信在监管态势感知、SASE、TSOC、工业安全等多个领域的首版本发布时间，从同类产品 9 个月缩短至 3 个月，研发效率提升了 300%。冬奥研判分析体系的开发周期，在冬奥组委的极限需求下，更从传统的 100 天缩短至 10 天，堪称定制开发的‘新基建狂魔’。” 刘浏也以“云安全管理平台”这款产品为例，“基于川陀平台，该产品仅用三周时间就重构完成了旧版本耗时一年开发的功能点。”

再拿“好”来说。性能好，是提高产品竞争力的核心武器。奇安信集团副总裁、首席架构师兼鲲鹏平台负责人吴亚东表示，鲲鹏平台作为电信级网络操作系统，堪称网络和安全完美融合的用户态协议栈，它具备全功能、高性能、高可靠三大优势，从而助力产品连续 2 年中标中国移动防火墙集采及中标中国联通防火墙集采等项目。最终实现 2021 年鲲鹏平台产研人员人均创收超过 410 万元，同比激增约 40%，达到网络安全行业头部厂商的 2~3 倍，同时人均创造毛利 266 万元，同比增速更达 43.5%。

第三是“省”的维度。困扰网络安全行业最大的痼疾，就是“增收不增利”，而研发平台在降本增效方面效果明显。奇安信拥有多达 30 余款产品的庞大终端舰队，在业内遥遥领先，通过基于川陀平台的统一式量产，在保障高质量、低 bug 的前提下，成本下降达 2/3，“省”优势不言而喻。同样，通过鲲鹏平台的量产应用，同等规格性能下成本降低一半，让边界安全系列产品的性价比实现了倍增。使得边界安全产线 2021 年营收同比增长 47.4%，三倍于 15.8% 的网络安全行业平均增速（中国信通院数据）。而毛利同比增长 51.2%，实现了“增收更增利”。

面对“快”“好”“省”的“不可能三角”，奇安信以大禹、鲲鹏、川陀等代表的研发平台，努力实现三者兼顾。其最终目标，就是将研发工程师从重复造轮子的投入中解放出来，用更高效的乐高模式，开发出更优秀的产品，进而推动行业的发展和进步。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

红海深处辟蓝海

——走近奇安信副总裁、边界安全 BG 负责人吴亚东

作者 公关部 孙丽芳

“女怕嫁错郎，男怕入错行。”

2003 年，在厦门某大型外贸公司做了 5 年业务员的吴亚东心头常萦绕着这句话。

其实，学经济的干外贸算是专业对口，但吴亚东却志不在此，并且觉得自己有些内向的个性不是很适合，思量再三，决定改行。

也正是在这个阶段，中国迎来了计算机普及的第三次高潮。得益于计算机硬件的成本降低，个人电脑开始走进千家万户。吴亚东打算转去的，正是计算机行业。

底气来自于上学时的兴趣，以及工作后自学了一段时间的防火墙知识，也来自于当时在天融信工作的哥哥。哥哥的支持很直接，他把弟弟引荐进了天融信。

这只是一个开始，在那之后，平凡的外贸业务员“小吴”消失了，替代的是防火墙工程师“小吴”，并最终成为边界安全领域的大牛——“东哥”。

“下”红海

沉静内敛、专注好学、善于思考、逻辑思维能力强，这些特质让吴亚东在防火墙技术领域进步神速。当 2004 年天融信重写自己防火墙架构的时候，吴亚东已经独当一面，负责协议栈部分。之后，吴亚东又加盟过安启华、韦伯森斯、山石网科等网络安全公司。

平台虽然变更，但吴亚东一直很专注。

“这些年间，防火墙所有的软件和硬件架构的变革，我基本上都参与了。”

防火墙是相对成熟的安全市场之一，其中不乏主流的供应商和竞争者。安全威胁不断变化，企业的移动性、虚拟化、云计算等已经对防火墙的功能提出了更高的要求。逐渐的，“下一代”这个关键字频频被安全厂商和业界所提及。

2011 年，占据防火墙、安全管理平台、安全服务市场领先地位的老牌厂商网神正在着力开发下一代防火墙。彼时加盟的吴亚东，凭借自己的视野和经验，开始了这一工作。

2014 年，网络安全行业经历了标志性的一年，“心脏滴血”漏洞、破壳漏洞先后曝光，有超过三分之二的互联网软件、网站等不能保证用户通过互联网传递、存储信息的安全。奇安信在这样的背景下诞生了。在一定规模的信息安全厂商中，奇安信是成立最晚，但发展速度最快的公司。市场疑惑传统网络安全行业门槛较低，持续涌入新的高成长玩家。但实际上，奇安信并不是从 0 开始，公司收购和参股了较多的信息安全厂商，其中就包括网神。

边界安全产品负责人吴亚东也就此走进了更广阔的平台。

奇安信将网神收至麾下，获得了其边界安全产品线。但众所周知，边界安全领域是国内网络安全中历史最悠久、规模最大、市场竞争最激烈的细分领域之一，早已是一片红海。而奇安信的目标不仅仅是保持网神原有的优势，而是要扩大优势。

“规模大，导致这是兵家必争之地，你有什么产品我也一定要有。历史悠久代表了相应的技术积累多，我们如果新开发一个功能影响面就很大，这导致市场需求迭代慢。但随着网络安全形势的日益严峻，客户的网络安全需求呈现多样化，大部分网络安全企业不得不投入更多人力，导致营收虽然稳步增长，但是增收不增利、增收不增效，人效比普遍不高。” 吴亚东觉得，寻找破解密码，是所有网络安全企业也包括奇安信的当务之急。

“铸”平台

市场的压力，会让一部分人失去方向和重心。但同时，也会让一部分人找到机遇。

吴亚东和公司管理层一起对边界安全产品线及公司其他相关产线的现状进行了深入分析。奇安信的公司级网关类产品线众多，而各产品线从系统、框架和功能组件均存在一定程度的交集和通用性。例如，路由模块，网关产品线使用率极高的基本模块，同一个功能模块，不同的网关产品线都在研发，从而导致研发投入“重复造轮子”，研发资源巨大浪费，最为关键的是造出的“轮子”质量参差不齐，影响了产品的质量和用户的满意度。

“为避免研发资源重复投入，提升产品质量，我们整合了核心研发人员，成立了鲲鹏网络平台研发部，向公司级各产品线输出业内最具竞争力的网络产品底层软硬件平台及组件，致力于打造网安行业最具竞争力的网络操作系统。”

鲲鱼是传说中北海里一条几千里长的大鱼，能幻化成巨大的鹏鸟，所以又名鲲鹏。这个源于想象的雄奇物种，现在被寓意网络操作系统覆盖面广、可扩展性强。鲲鹏由吴亚东亲自掌舵。在他的带领下，两年时间，鲲鹏平台被打造成为业界领先的边界安全产品专用网络操作系统。

“依托于鲲鹏平台硬件解耦的软件架构，产线可以彻底从底层系统中解放出来，将不用再关心底层软 / 硬件平台的变化，只需专注自身安全业务，从而极大提高了对客户侧不断变化的领域内安全需求的响应速度。更为关键的是，产品质量和产品交付能力可获得翻倍提升。比如，面对信创市场各类国产化硬件平台和多个操作系统要求时，采用鲲鹏平台，产品线适配速度可由原来的几个月缩短为几周。”

2019 年，公司将鲲鹏平台和边界安全产线进行了整合，组建成为边界安全 BG。吴亚东开始了平台和产线两手抓。

“鲲鹏不是一个纯粹的底层技术平台，它本身就带着很多网关的业务功能，一体化的安全引擎、开放的软件定义安全架构、全功能的高性能用户态协议栈、网络功能虚拟化等。所以二者合起来的作用很明显，平台跟产线对齐了。比如，要做某个核心能力的时候，可能有一些是来自产线针对市场的需求，还有一些是平台根据自己的长远规划和技术发展趋势看到的。二者可以融合在一起统一做规划。”

在吴亚东的带领下，融合后的鲲鹏和边界安全产线，

发生了巨大的化学反应。

“2020 年我们参加中国移动集采就是平台跟产线一起做的。移动集采侧重的都是防火墙的硬功夫，如防火墙的性能、稳定性、数通的接入能力等，这很大一部分都是落在平台这边的，然后产线也进行了相应的开发。这就类似于是硬功夫的比拼，没有取巧的地方。最终我们的防火墙入围了。这代表了鲲鹏的能力，也是对我们防火墙产品各方面实力的肯定。”

基于鲲鹏平台，奇安信连续两年中标中国移动防火墙集采及中标中国联通防火墙集采项目，同时 2021 年入围了中国银行信创防火墙集采项目。

“鲲鹏和产线合了三年，公司边界安全产品线的高速发展也正是这三年。”

2021 年鲲鹏平台实现量产，全面应用到了奇安信的边界安全系列产品中，这让边界安全产线 2021 年营收同比增长 47.4%，三倍于 15.8% 的网络安全行业平均增速（中国信通院数据）。而毛利同比增长 51.2%，实现了“增收更增利”。相关产研的人均创收达 410 万元，达到网络安全行业头部厂商的 2~3 倍；人均创造毛利 266 万元，大幅领先于行业平均水平。

吴亚东在奇安信研发平台战略发布会上解读鲲鹏如何打破人效比魔咒

与此同时，鲲鹏平台的能力正在输出给工控、探针等公司其他产线。重复造“轮子”，不如共享一个超级大的“轮子”。各产线可以“按单点菜”式地选用“鲲鹏”提供的各项技术和服务，从而能更集中各自优势资源，打造自己的核心竞争力，获取更加优异的市场表现。

“重”创新

在鲲鹏平台的支持下，边界安全 BG 的技术创新脚步也从未停止。

“事实上，我们的创新方向并不多，但是我们持之以恒。”搞技术创新，吴亚东有自己的逻辑。

2021 年，全球供应链紧张，对于以生产硬件为主的边界安全产品线来说影响巨大。“主要是网卡芯片非常短缺。边界安全产品在安全设备里面偏向于数通设备，就像路由器交换机一样，设备上面有非常多的接口，每年需要使用大量的网卡芯片，网卡芯片的成本占比很高。”刚需遇上短缺，成本陡然上升，整个边界安全行业感受到了巨大的压力。但奇安信的边界安全产线是个例外。原因在于，从 2019 年开始，吴亚东就带着平台和产线研发一种不用网卡而用交换芯片来扩展接口的方案。

“当时我们没有想到网卡芯片会紧张，只是想着这种方式能降低成本。因为我们这一块在整个公司里，出货量是最大的，金额收入也是最大的，但毛利率也是最低的，所以成本对我们来说特别重要。2021 年的时候用了新方案后，不仅把成本大约降低了 30~50%，也大大缓解了紧张。今年网卡芯片比去年还要紧张。我们这边最经常做的事情就是换各种料件，比如说 Intel 的网卡没有了，换国产的网卡。以前数通厂商有采取这种做法的，因为他们受到成本的压力比我们的还大。但是以前专业安全厂商几乎没有这么做的，现在大家也都在朝着这个方向去走，但有的型号离我们差的还比较远，特别是采用这种 SoC 硬件平台加交换芯片的方案，现在安全厂商里面基本上就我们一家。”

除了从成本角度做创新，在客户场景下的创新也是吴亚东团队的创新方向。

“之前有家客户提了一个需求，这个需求其实比较简陋，就是要在一个框式的设备里，插上好多张板，比如防火墙、ICG、IPS，当成一个统一的东西来管理。于

是我们就做了这样一个东西。卖掉一些之后，我就想，现在是插这些实体的板子，那能不能把它们做成虚拟化的形式，放到我们的网关设备里呢？然后我们就做了这样一款产品，这就是边界安全栈。去年我们就卖了 3000 万，毛利特别高，超过 80%，今年的销量还会更多。”

创新有的源自市场上用户的需求，有的则源自技术发展的趋势。

“对加密流量进行解密就是一个技术趋势。现在大家都看到加密的流量越来越多是吧？你现在上个网站可能都没有明文的网站了，不管是内网还是外网，都是加密流量了。安全上，如果没法对加密流量进行检查，有效性一定是有问题的。但以前大家对加密流量基本上没有太多办法，因为解密非常耗资源。今年我们的防火墙主线要推出的就是 SSL 解密的服务链编排。我们把加密的流量解成明文，然后再根据用户定义的策略，把明文流量给到在线设备（如 IPS WAF），以及旁路设备（如探针），实现一次解密，多次检测，从而进一步提升整个纵深防御体系的流量防护能力。”

据了解，目前国内只有个别友商现在也在往这个方向走。但从目前的公开数据看，对方产品对流量解密的完整度对比奇安信的产品还有些差距。吴亚东带领的团队顺应了技术趋势，也又一次引领了行业。

“我们的创新方向上不多，是因为我们选方向会比较谨慎，一旦选定，我们会照着这个方向做上很长的时间。速度可能比较慢，但是质量可靠。不成熟的产品，我们绝不会给客户使用。我们宁可上线慢，但不要返工，要确保客户能用、好用。有的时候，慢就是快。持之以恒还有一个好处是我们能做得很深，一开头可能是在分支上做，后来我们都会慢慢地进行合并。比如，现在 SD-WAN 跟防火墙就已经合在一起了。”

“轻”管理

极端专注的个性、二十余年的从业经历，早已把吴亚东打磨成顶级技术专家，但是做管理又是另一回事。而且是既要管研发，又要管产线，按说这并不容易。

吴亚东却是大家眼中是最不像高管的高管。

“东哥是领域里的技术领袖，儒雅内敛，对产品和技术精益求精”。鲲鹏平台负责人李红光的感受，代表了吴亚东留给大家的印象。

绝大多数的时候，吴亚东和风细雨、平易近人、举重若轻。

“我们团队一直采用的是‘轻管理’的模式，就是基本没有为了管理做专门的流程，团队非常的扁平化，没有那么多复杂的层级，整体氛围很好。大家都是专注于一线的工作，包括写代码、对前端的支持等。所有的 leader 都要在一线直接干活，不仅仅是分任务，要指导大家去完成任务。我本人主要是抓重点、盯进度，以及日常复核重要的代码，有问题的，我会提出修改意见。大家如果碰到问题也是直接来找我，当面沟通解决。”

“核心代码的每一行，东哥都要亲自过几遍，反复斟酌。从内存泄漏，到安全风险、性能提升等，事无巨细。工作如此方能打造出如此高品质的产品！”网闸负责人杨威由衷地感叹。

儒雅的吴亚东也不是没有脾气，在某次集采入围做测试的时候，团队因为某项内容考虑不周，丢了不该丢的分数。吴亚东发了大脾气。“这种错误无法容忍，从我开始，全部要深刻反省，绝不能再犯。”

负责人深厚的技术能力和身先士卒的做法令团队信服，也收到了很好的示范效果。整个团队和吴亚东本人的风格很像：业绩出众，人狠话不多！

“至于研发和产品两条线的问题，事实上，鲲鹏最早就是从边界安全产线里分出来的，有天然的合作基础，后来合在一起，契合度就很高。比如说我们这边有一个叫大项目的保姆式支持，针对大的市场机会或者项目。从前期跟客户的需求交流，到产品的定制、备货、交付，我们会有一个团队进行全程支持。但这实际上是一个虚拟团队，也就是说不是专职的，是由产线负责人、行销负责人，产线开发人员，平台开发人员共同组成。”

除了紧密合作，边界安全 BG 各线负责人的研发功底都很深厚，且各具特点。吴亚东根据业务发展情况和大家各自的特点，在部门内部灵活调配，实现人尽其才。

“网关产品的负责人王起立，产品经验和市场经验都很丰富，保姆式的市场支持就是他提出来的。杨威是

边界安全 BG 团建合影

网闸的负责人，技术和市场一起抓，如果单算人效，网闸应该是整个公司最高的事业部了。鲲鹏平台负责人是李红光，红光可能跟我有点像，偏内敛型，既专注又认真负责，对平台创新充满热情。网关研发负责人樊俊诚一路打磨出来 SD-WAN 这个创新产品，这两年的销量有了迅猛的增长，现在又在负责高性能 SSL 解密这个很高门槛的技术方向。鲲鹏平台原测试负责人龙艺，现在任边界安全 BG 的行销负责人。我们把对产品技术很了解的同学往一线输送，大大缩短了前后场的距离。”

在最难的赛道上，跑出了最好的成绩，营收、毛利增速、单人创收三倍于同行，如今，边界安全 BG 已经是公司的“产粮大户”。而吴亚东的生活并没有什么大变化，每天两点一线，夏天穿格子衬衫，冬天在格子衬衫外面套一件羽绒服。

2022 年 2 月 4 日，冬奥火炬手吴亚东在火炬传递中

“我其实挺开心的。因为在这里我能发挥自己真正的长处，而且周围有一群志同道合的战友。下阶段除了在之前的技术方向上继续发力，我们还在研发框式的网关，相较以往的产品，性能更高，而且性能可以线性扩展。这是我们现在相比华为、新华三等数通厂商唯一的短板。这块突破了以后，希望能把奇安信的边界安全产品带进中国前三。”

红海深处辟蓝海，一条赛道，20 余年光阴。

尽管鬓角有些斑白，吴亚东看起来比同龄人更精神焕发，也还保留着少年人般的执着。

感谢这份执着，它让中国少了一个平凡的外贸业务员，多了一个边界安全领域的领军人物。安

规划快一步

奇安信

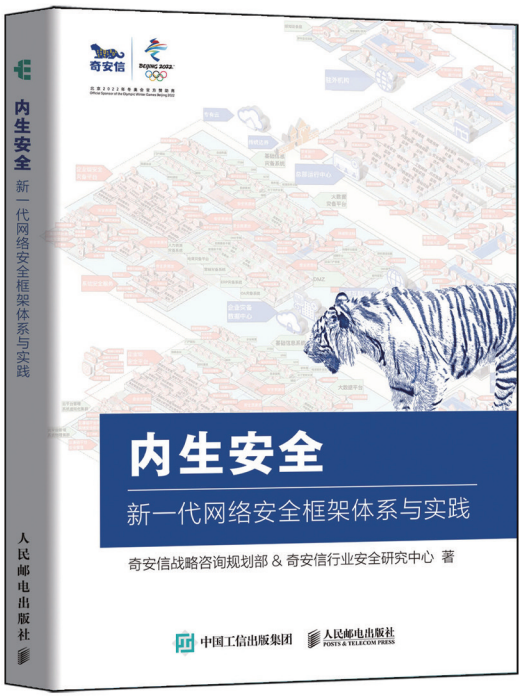
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

奇安信抗疫行动

2022年3月，福建信息职业技术学院抗疫捐赠

▲ 2022年3月，福州大学抗疫捐赠

▲ 2022年4月，福建船政交通职业学院抗疫捐赠

▲ 2022年5月，北京光彩公益基金会捐赠证明

▲ 2022年4月，福州外语外贸学院抗疫捐赠

▲ 2022 年 5 月，奇安信集团组织核酸检测，齐向东董事长亲自担任现场志愿者。

2022 年 3 月，闽江学院抗疫捐赠

▲ 2022 年 5 月，万明园社区志愿工作

荣誉证书

兹有 奇安信科技集团有限公司 向长春理工大学教育基金会捐赠420箱泉阳泉矿泉水。助力学校防疫抗疫，特颁此证，以示谢忱！

长春理工大学
教育基金会
二〇二二年三月二十二日

▲ 2022 年 3 月，长春理工大学捐赠证明

▲ 2022 年 3 月，援港抗疫捐赠

▲ 2022 年 3 月，吉大抗疫捐赠

大事记

BCS2022 冬奥网络安全“零事故”宣传周首日峰会 公开解密“中国模式”

5 月 20 日，2022 北京网络安全大会（BCS2022）冬奥网络安全“零事故”宣传周暨网络安全优秀产品推介会首日峰会开幕，首次公开解密冬奥网络安全保障创新的“中国模式”，同时还正式对外发布了在冬奥期间发挥重要作用的奇安信态势感知研判系统。

齐向东为冬奥网络安全“零事故”总结了未来将发挥的三大重要建设性作用：首先，冬奥“零事故”将助力政企机构的网络安全防御能力实现新飞跃；其次，冬奥“零事故”将加快网络安全行业的创新步伐；第三，冬奥“零事故”将带动网络安全行业进入实战化时代。

奇安信集团与澳门科技大学达成战略合作 打造网安人才培养新生态

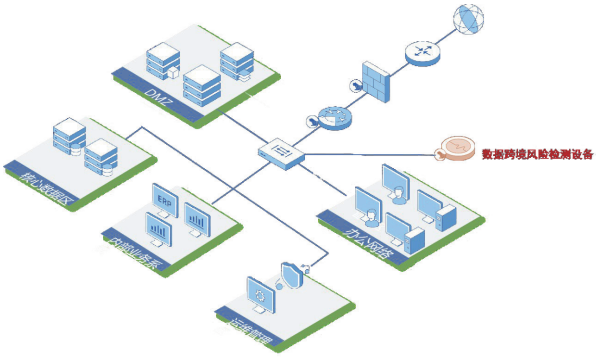
5 月 19 日，奇安信集团与澳门科技大学签署战略合作协议，双方将围绕网络安全人才培养、共建网络安全教学及科研实践基地、优化网络安全人才培养体系、网络安全技术研究合作等方面进行深入合作。

根据协议，双方将整合校企双方资源，在多方面进行深入合作：在人才培养方面，双方将以培养高水平网络安全人才为目标，形成长效合作机制，并针对网络安全产业实际需求，共同开展相关项目技术研究，达成产学研深度合作；在科研方面，双方将共建网络安全联合实验室，为网络安全技术研究和人才培养提供更好的平台和更多资源。

企业数据跨境流动面临合规大考 奇安信发布数据跨境卫士

5 月 18 日，奇安信对外发布数据跨境卫士，帮助企业满足数据跨境传输、流转时面临的合规和合法监管需求，并为企业开展跨境业务、管理境外分支机构、境外上市、跨境数据流动等提供专业的安全保障。

奇安信数据跨境卫士具有四方面功能，首先是保障合规，即帮助企业满足数据安全法、个人信息保护法、数据跨境监管相关条例等合规要求；其次是可查可检，



满足企业正常业务开展的同时，清晰掌握业务数据、重要数据、个人信息等敏感数据跨境流动详情；第三是及时止损，可以帮助企业避免名誉受损、经济受损，同时避免被通报处罚；最后是看清流向，可以全面了解 WHO（什么人）、WHEN（什么时间）、WHERE（什么地点）、HOW（什么方式）、WHAT（什么数据）等整个数据跨境流转的整个过程，实现全局掌控。

奇安信召开北京冬奥网络安全“零事故”经验线上分享会

2022 年 5 月，奇安信举行多次冬奥网络安全“零事故”经验线上分享会。5 月 13 日，与兴业银行举办北京、上海、福州三地的冬奥网络安全“零事故”经验线上分享会；5 月 17 日，与浙商银行举办北京、杭州两地的冬奥网络安全“零事故”经验线上分享会，并进一步针对银行金融领域网络安全建设和安全运营经验进行了深入的交流和讨论。

奇安信冬奥网络安全“零事故”经验宣讲团于 2022 年 3 月 16 日正式成立。宣讲团总结了北京冬奥网络安全“零事故”经验，并将在涉及全球的、复杂的实战化网络安全场景中搭建起的“中国方案”，打造成为可复制、可落地、可借鉴的成熟的“冬奥遗产”，旨在为我国关键信息基础设施、重要活动的网络安全保障工作打造模范样本，并提供成熟的、已通过国际化实战检验的有力技术支撑与保障。

打造通信安全运营服务新生态 奇安信与嘉环科技达成战略合作

5 月 17 日，奇安信集团与嘉环科技股份有限公司签署战略合作协议，双方将积极推进通信行业网络安全运维与运营能力建设，形成联合解决方案，共同打造通信行业安全运营服务新生态。

根据协议，双方将整合自身优势资源，提升信息化服务业务品质：在行业安全服务方面，携手完成符合行业客户需求的场景化解决方案，打造服务型标杆项目；在教育培训业务方面，形成产教融合立体合作形态；在产品与解决方案融合方面，重点针对云计算安全、等级保护安全、物联网安全等新技术方向，形成联合解决方案，打造优势互补、资源共享的协同发展模式，强化通信行业发展安全底板，助力数字经济产业稳步发展。

奇安信集团入选教育部 2022 年产学合作协同育人项目企业名单

5 月 16 日，教育部产学合作协同育人项目专家组发布《关于公布教育部产学合作协同育人项目指南通过企业名单（2022 年 4 月）的通知》，奇安信集团申报的“新

工科建设项目、教学内容和课程体系改革项目、师资培训项目、实践条件和实践基地建设项目”4 大类 29 个项目成功入选。

奇安信将在教育部的指导下，基于产业和技术发展的最新需求，通过以上项目推动和支持高校的网络安全人才培养和专业建设综合改革。

奇安信获选首批数字政府网络安全产业联盟副理事长单位

5 月 12 日，数字政府网络安全产业联盟理事会议暨首批理事单位授牌仪式举行，奇安信获选为联盟副理事长单位。

奇安信集团副总裁刘进表示，奇安信在广州拥有全资子公司，华南总部暨数字经济安全产业园也已落户广州。2021 年，奇安信已分别与广州广电运通金融电子股份有限公司、广州市海珠区人民政府签署战略合作协议。未来，奇安信将继续扩大在广东的业务布局与投入，通过已有的数字安全建设经验进一步支持广东的数字政府建设。

探索量子技术与网络安全融合创新之路 奇安信与国科量子达成战略合作

5 月 7 日，奇安信集团与国科量子通信网络有限公司签署战略合作，双方将围绕基于量子技术的网络安全产品和服务、“国家广域量子保密通信骨干网络”建设等方面开展深入合作，共同探索研究，推进量子保密通信技术在关键行业和领域的应用和发展。

量子技术和网络安全技术都是国家科技自立自强的重要领域。奇安信与国科量子达成战略合作后，双方将充分发挥各自领域的技术和业务优势，围绕量子技术这一关键科技领域，联合共建“基于 QKD 应用的 ICT 安全融合产品联合创新实验室”，推进基于量子技术的网络安全产品和服务；推动“国家广域量子保密通信骨干网络”建设。同时，双方还将共同推进“量子可信云”和“量子信息安全托管”业务发展，从重庆起步，打造量子信息安全业务应用标杆。

奇安信入选信通院“网络安全能力评价工作组”成员单位

由工业和信息化部网络安全管理局指导、中国信息通信研究院牵头的“网络安全能力评价工作组”正式成立，奇安信入选成员单位，并将在体系研究、标准研制、示范推进三项子工作组中与成员单位共同推进网络安全能力评价相关的研究。

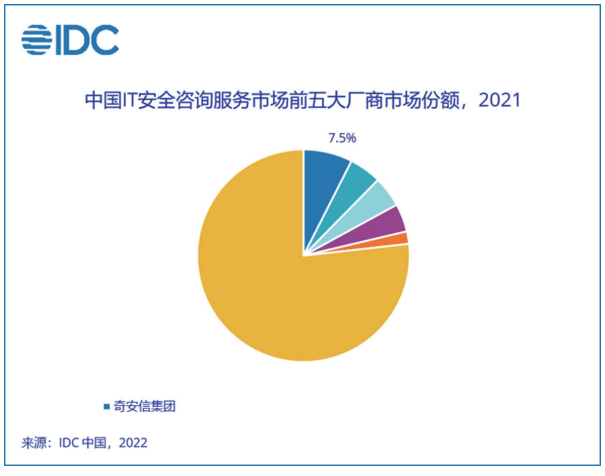
奇安信将发挥自身在体系研究、标准研制及示范推进方面的专长，分享自身在网络安全领域的经验，推动

形成人才培养、技术创新、产业发展良性生态，并为构建网络安全能力科学评价体系、引领网络安全技术产品高质量发展贡献力量。

IDC 报告：奇安信安全咨询服务连续三次位居榜首

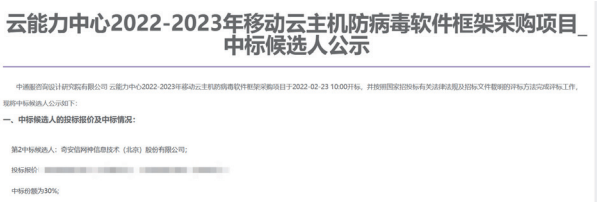
近日，国际权威咨询机构 IDC 发布《2021 下半年中国 IT 安全服务市场跟踪报告》。《报告》显示，2021 年中国 IT 安全服务市场厂商整体收入约为 28.61 亿美元（约合人民币 184.6 亿元），厂商收入规模较去年同期实现快速增长，涨幅达到 41.7%。

其中，相较于 2021 年上半年，奇安信安全咨询服务和托管安全服务市场份额持续增长，尤其是安全咨询服务，从 2020 年下半年至今已经连续三次市场份额居首，始终保持行业领先地位。



奇安信中标移动云主机防病毒软件框采项目

近日，中国移动“云能力中心 2022-2023 年移动云主机防病毒软件框架采购项目”中标候选人正式公布，经过严格的产品测试和方案评估，奇安信统一服务器安全管理系统凭借在产品性能、实施方案和售后服务方面的全面优势脱颖而出成功中标，部署规模近 5 万点。

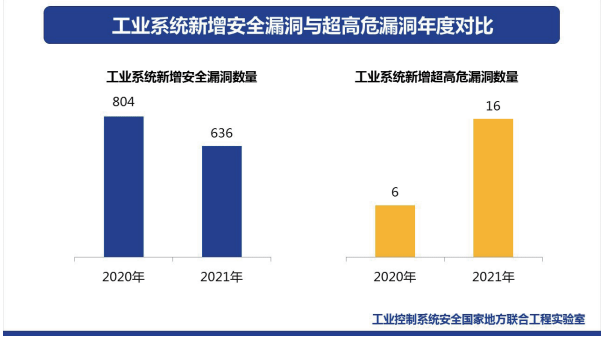


联合发布《2021 工业互联网报告》：勒索软件仍是最大威胁

近日，奇安信行业安全研究中心联合工业控制系统安全国家地方联合工程实验室，正式发布了《2021 工业互联网安全发展与实践分析报告》，从工业互联网安全态势、政策法规建设与发展、典型案例及安全发展趋势等层面，深度还原了工业互联网安全现状和发展变化趋势。

《报告》分析指出，从统计数据来看，我国工业互

联网安全形势依然严峻特别是制造业的安全防护能力薄弱，安全事件高发。需要提高整个行业的安全防范意识，加强日常安全巡检制度，定期对系统配置、网络设备及安全策略进行检查，主动发现目前系统、应用存在的安全隐患，保障工业互联网的安全稳健运行。



金隅集团走进奇安信 参观交流企业数智化转型安全建设经验

4 月 25 日，金隅集团副总经理刘文彦一行走进奇安信，参观奇安信工控安全展厅、党建室，并围绕冬奥网络安全保障和企业数智化发展中的网络安全需求，与奇安信安全专家进行了深入的交流。

奇安信集团副总裁、战略咨询规划部总经理韩永刚，涉网犯罪研究中心总经理赵晋龙，军团体系委员、关基总体部经理尹智清，分别围绕冬奥“零事故”重点工程、冬奥“动态清零”重保研判系统、数据安全治理防护工作等内容进行了分享。金隅集团运营与信息化管理部、安全与应急管理部、环境保护管理部、科技创新部、数智化办公室等部门相关人员也就日常工作中涉及的网络安全管理责任、技术需求、运营需求等方面，与奇安信安全专家进行了深入的交流。

奇安信集团发布首份社会责任（ESG）报告

2022 年 4 月 25 日，“网安一哥”奇安信发布首份社会责任（ESG）报告。报告全面展现了奇安信自上市后在守护北京冬奥、护航网络强国、赋能行业发展、抗疫救援，以及在党建、公益、员工关怀与环境可持续发展方面的成就与贡献。

报告显示，在上市一年多的时间里，奇安信利用自身科技优势，参与了北京冬奥及国家重大活动的安全保障任务，并发布多份公益研究报告。同时，在抗击新冠疫情、推进数字化党建、践行社会公益等方面，奇安信始终以守护网络强国为责任，促进社会数字安全的公平与保障，履行守护美好生活的使命。

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