SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

千亿隐私计算市场
四大技术流派大PK

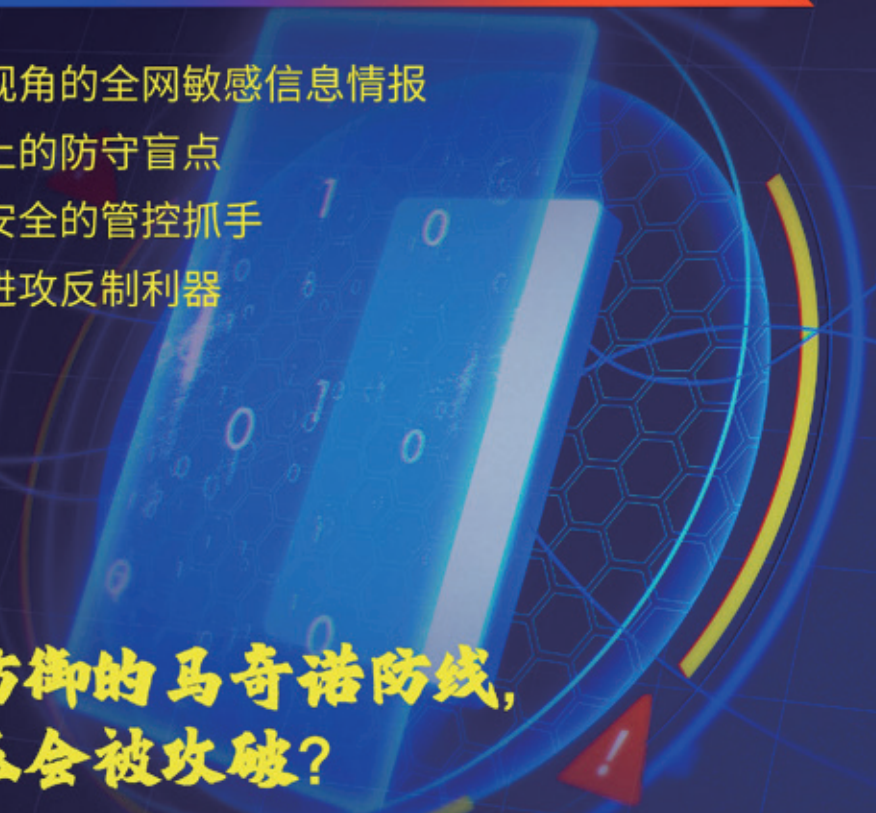
P16

第11期
2021 年 11 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

元宇宙的安全挑战准备好了吗?

近期，“元宇宙”概念不断发酵，在刷爆投资者眼球的同时，吸引各大互联网公司纷纷入场。被 Facebook 的 CEO 扎克伯格称为下一代互联网的元宇宙，究竟有何神奇之处?

元宇宙（Metaverse）概念出自科幻作家尼尔·斯蒂芬森 1992 年出版的《雪崩》一书。在书中，斯蒂芬森构思出了脱胎于现实世界并与之平行的元宇宙。前沿技术成熟度加快、数字生态的迭代和渗透，现实世界和虚拟世界的融合成为元宇宙爆发的驱动因素。

“元宇宙”引发各界人士的兴趣，但元宇宙概念仍在探索当中，对于元宇宙是什么，以及未来将发展成什么，目前仍没有固定的定义或清晰的理解。根据专家的描述，元宇宙是与现实世界平行的开放虚拟世界，可提供游戏、社交、交易等沉浸式体验，被视为下一代互联网。

今年上半年，包括 Facebook、微软、腾讯等在内的互联网巨头纷纷加入到“元宇宙”的竞赛中，从游戏、社交、硬件等不同角度切入该赛道。近期，字节跳动宣布以 90 亿人民币收购国产 VR 硬件公司 Pico，内部或在开发一款元宇宙社交产品“Pixsoul”。随着时间的推移，会有更多的企业加入这一领域。

摩根士丹利发布报告声称，元宇宙有望发展成为下一代社交媒体、流媒体和游戏平台，成为高达 8 万亿美元规模的庞大市场。

随着元宇宙逐渐成为个人数据和商业的新市场，数据泄露与攻击风险正在逼近。由于元宇宙需要数字货币来交换数字商品，这意味着数字货币的窃取将会更加盛行。目前黑客已经将网络安全漏洞做成 NFT（非同质化代币）高价拍卖。

安全专家认为，即使元宇宙成为现实仍需数年时间，业界现在所要考虑的还是元宇宙的网络安全问题，并要为可能的网络攻击做好准备，毕竟无论准备好与否，对它的网络攻击迟早会到来。思科 Talos 技术负责人舒尔茨甚至将元宇宙描述为缺少保护与管理的狂野西部。

中国现代国际关系研究院的学者在最近的《元宇宙与国家安全》报告中指出，在技术安全方面，元宇宙很可能将面临以下问题：（1）网络攻击。（2）技术安全缺陷。（3）关键基础设施风险。（4）篡改、盗取和大规模泄漏。

数字技术和生态的安全问题往往难以被提前发现。元宇宙集成了诸多信息技术，其安全隐患可能会更加突出和多元。对于新兴的元宇宙来说，此时可能有真正的机会，来践行内生安全理念，将更多的安全性融入其中。

总编辑

李建平

2021 年 11 月 1 日

CONTEN

目录

安全态势

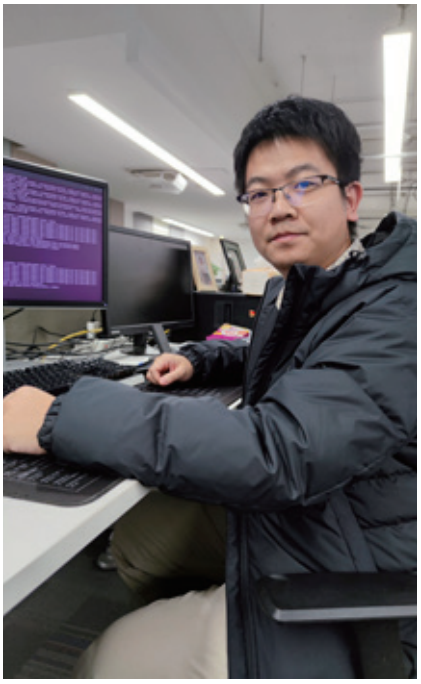
月度专题

千亿隐私计算市场 四大技术流派 大PK

P16

可用不可见的隐私计算，成了既满足合规避险又满足业务需求的优解答案，四大技术流派大 PK。

TS



奇安资讯

第 11 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

关基安全威胁形势严峻，全球多国关键行业遭受攻击，引发较大影响。我国金融、医疗等重要领域信息系统源代码数据，遭境外黑客组织窃取并非法售卖；加拿大地方卫生网络遭攻击瘫痪，并且近 14 年的患者全部隐私泄露；疑似网络攻击导致软件故障，伊朗全国加油站大面积关闭……

CNCERT 预警：近期境外黑客组织攻击我国多个企业，窃取源代码数据

2021 年 11 月 21 日，国家计算机网络应急技术处理协调中心（CNCERT）发布预警称，2021 年 10 月以来，CNCERT 监测发现有黑客组织利用 SonarQube 软件的漏洞，对我国多个企业发起攻击，窃取了我金融、医疗等重要领域信息系统源代码数据，并在境外互联网进行非法售卖。经分析，该黑客组织来自境外。该黑客组织的上述行为严重侵犯我企业知识产权，对我国国家安全和企业利益造成严重威胁。CNCERT 提醒境内使用 SonarQube 软件的相关单位及时修复漏洞，防范网络攻击行为。

FBI 服务器被黑客入侵，超 10 万人收到虚假邮件

据每日邮报 11 月 13 日消息，美国联邦调查局（FBI）披露，有黑客当天入侵其邮件服务器并发出大量虚假邮件信息。这些邮件使用的标题是“紧急：系统中存在威胁行动者”。FBI 指出，发送虚假邮件的电子邮箱域名看上去似乎是 FBI 的官方邮箱，且邮件的署名为美国国土安全部。全球最大的反垃圾邮件组织 Spamhaus 警告称，此波入侵可能导致网络攻击。目前，FBI 已就此事展开调查。

澳大利亚供水设施被植入后门长达 9 个月，直到年审才发现

据 BleepingComputer 11 月 11 日消息，澳大利亚昆士兰州审计署的最新年度财务审计报告显示，国有供水商 SunWater 遭到网络入侵长达 9 个月，自己却毫无察觉。被入侵服务器存放了客户数据，但攻击者似乎无意查看，只是植入了一个视频刷量的恶意软件。年审报告称，这是又一次发现澳大利亚的多个供水商信息系统存在控制缺陷，对供水设施而言，网络攻击仍然构成重大风险。

知名券商 Robinhood 泄露 700 万用户资料：因员工被社会工程

据 TechCrunch 11 月 9 日消息，美国知名互联网股票交易平台 Robinhood 披露，遭到黑客攻击，超过 500 万个客户邮件地址、200 万个客户姓名，以及一小批更为具体的客户身份数据被恶意人士掌握。攻击者通过电话对 Robinhood 的客服代表展开社会工程攻击，成功访问到客户支持系统，并窃取了大量用户资料。这是 Robinhood 公司迄今为止经历的最重大安全事件。针对大型互联网平台的社会工程攻击屡见不鲜，去年 7 月推特也遭遇过类似

事件，数十个超级政商名流的账号遭到劫持，发布比特币诈骗信息。

加拿大地方卫生网络遭攻击瘫痪，近 14 年的患者隐私泄露

综合多家媒体 11 月消息，加拿大纽芬兰和拉布拉多省的卫生网络在 10 月 30 日遭到网络攻击瘫痪，导致全省数千人的医疗预约被取消，急诊重回纸笔服务。官方披露称，近 14 年的东部地区卫生系统和近 9 年的拉布拉多 Grenfell Health 的员工与患者敏感信息被泄露。有安全专家表示，这是加拿大史上最严重的网络攻击，建议将此次攻击升级到国家安全层面。

网络攻击 × 虚假新闻引发银行挤兑！巴基斯坦央行紧急澄清

据 TheRecord 11 月 2 日消息，巴基斯坦国民银行在 10 月 29 日（周五）夜间遭遇一次“破坏性”网络攻击，包括 ATM 机、分行 / 支行网络、手机应用等系统均陷入瘫痪，引发民众舆论。部分民众在周一纷纷去恢复后的 ATM 机取款，而当地一些媒体发布不准确报道，声称 9 家不同银行遭到黑客攻击，数据外泄资金被盗，扩大了挤兑风波。巴基斯坦央行周一紧急澄清，称只有国民银行发生网络攻击事件，目前并未发现任何资金损失或数据泄露情况。

加拿大最大城市遭勒索攻击，公共交通 IT 系统几乎全部瘫痪

据 TheRecord 11 月 1 日消息，加拿大最大城市多伦多的公共交通系统遭到勒索软件袭击，大量内部 IT 系统瘫痪。受影响系统包括交通委员会内部的邮件服务、驾驶员通信系统、残疾人交通预定系统、出行规划应用、车站屏幕、车辆实时信息等。尽管 IT 系统大面积瘫痪，但当地公共交通出行没有中断，公交、电车及地铁仍保持正常通行。

美国乳制品巨头遭勒索攻击：工厂瘫痪数天 食品供应链被扰乱

据 ZDNet 10 月 29 日消息，美国大型乳制品供应商 Schreiber Foods 遭到勒索软件攻击，导致系统宕机，攻击者索要 250 万美元赎金。由于 Schreiber Foods 内部高度数字化，工厂与配送中心无法运行，牛奶运输商只能将牛奶运至别处，这对牛奶供应链造成了重大打击。在瘫痪 4 天后，工厂与配送中心终于再度恢复运行。近期食品供应链多次遭勒索软件攻击，美国两家农场服务商在秋收时期被攻击导致系统瘫痪。

德国汽车零配件龙头遭勒索攻击：生产系统瘫痪 员工被迫休假

据 TheRecord 10 月 27 日消息，德国跨国企业 Eberspächer Group 遭勒索软件攻击，官网、邮件、办公网络、生产系统等纷纷瘫痪。由于无法正常协调生产并管理客户订单，该公司只得通知部分工厂员工在宕机处理期间留在家中带薪休假。Eberspächer Group 为全球几乎所有的顶级汽车品牌供应空调、供暖及排气系统。

伊朗全国加油站大面积关闭：疑似网络攻击导致软件故障

据 TheRecord 10 月 26 日消息，伊朗国有天然气分销企业 NIOPDC 疑似遭到网络攻击，全国各地的加油站出现软件故障，无法正确计费收款，加油泵屏幕与油价广告牌上还莫名显示出涉政异常内容。NIOPDC 公司因此临时关闭了加油站运营，司机排长队等待加油，在社交网络引发了大面积讨论。伊朗石油部下午回应，将事件归咎于软件故障，受到影响的加油站后续也恢复了运营。

漏洞篇

近日，境外媒体相继爆料多起源代码泄露事件，涉及我国多个机构和企业的SonarQube代码审计平台，国家信息安全漏洞共享平台发布预警，建议受影响用户尽快更新修复。

SonarQube 系统存在未授权访问漏洞安全公告

2021年11月19日，国家信息安全漏洞共享平台（CNVD）日前收录了SonarQube系统未授权访问漏洞（CNVD-2021-84502）。攻击者利用该漏洞，可在未授权的情况下获取敏感代码数据。目前，漏洞利用细节已公开，SonarQube公司已发布补丁修复该漏洞。CNVD建议受影响用户尽快更新至最新版本避免漏洞攻击威胁。SonarQube是一个开源代码质量管理和分析审计平台。

英特尔多个安全漏洞预警

2021年11月18日，国家信息安全漏洞库（CNNVD）收到关于多款英特尔（Intel）产品安全漏洞情况的报送，包括Intel BIOS权限提升漏洞（CVE-2021-0157）、Intel BIOS权限提升漏洞（CVE-2021-0158）、Intel PROSet/Wireless WiFiSoftware安全漏洞（CVE-2021-0063）等。成功利用上述漏洞的攻击者可以在目标系统上提升权限等。Intel多个产品和系统受漏洞影响。目前，Intel官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

Palo Alto Networks GlobalProtect 安全漏洞预警

2021年11月11日，国家信息安全漏洞库（CNNVD）收到关于Palo Alto Networks GlobalProtect安全漏洞（CVE-2021-3064）情况的报送。成功利用漏洞的攻击者，可以绕过身份验证破坏目标系统进程，并在目标系统实现远程代码执行。PAN-OS 8.1.17以下版本均受此漏洞影响。目前，Palo Alto Networks官方已经发布了版本更新，修复了该漏洞，建议用户及时确认产品版本，尽快采取修补措施。GlobalProtect是美国Palo Alto Networks公司的一套网络防护软件。

Apache HTTP Server 代码问题漏洞预警

2021年10月25日，国家信息安全漏洞库（CNNVD）收到关于Apache HTTP Server代码问题漏洞（CVE-2021-40438）情况的报送。成功利用漏洞的攻击者，可以构造恶意数据对目标服务器进行SSRF攻击。Apache HTTP Server 2.4.48及其以下版本均受此漏洞影响。目前，Apache官方已经发布了版本更新，修复了该漏洞，建议用户及时确认产品版本，尽快采取修补措施。Apache HTTP Server是一款开源网页服务器。

对抗篇

国内攻防演习 10 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

2021 年 10 月，奇安信 Z-TEAM 团队共承接攻防演习服务 21 场，其中行业级攻防演习 1 场，省级攻防演习 2 场，地市级攻防演习 8 场，本单位自主攻防演习 10 场。

本月攻防演习成果如下表。

二、本月任务目标特点

本月攻防演习和评估任务覆盖行业比较集中，以政务和金融为主，客户存在的安全问题主要有互联网业务平台漏洞、业务系统敏感信息泄露、内部人员对钓鱼攻击防范意识不足、内部网络安全防护措施缺乏、内网弱口令及口令复用普遍等。具体情况如下。

1、漏洞利用仍是主要突破手段

本月任务中客户目标网络承载业务比较关键，网络安全体系也相对完善，外网突破主要依靠漏洞利用实现。突破利用的漏洞仍以历史漏洞为主，如 Fastjson 反序列化、Thinkphp RCE 漏洞、Shiro 反序列化及 OA 系统命令执行漏洞等，这些漏洞多因互联网侧应用组件更新不及时导致，直接给目标网络带来了严重的安全隐患。

2、钓鱼攻击是实现突破的有力辅助

本月任务中，多数目标系统的网络整体安全防护相对严密，外部系统很难直接突破，钓鱼攻击成为主要突破手段，并且具有较高的成功率。钓鱼攻击主要选择目标内部安全意识相对薄弱的人群，通过冒充其同事或客户身份，以内部业务交流或客服咨询为借口，发送木马，打开突破口。

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	32	74	150	113	27	229	306	615

3、敏感信息泄露是严重安全隐患

本月任务中目标外网敏感信息泄露情况较为突出，除了常见的目标内部人员信息，网络应用认证平台账户认证信息、业务系统注册用户信息、服务器安全日志及网络服务接口信息等也有发现。此类敏感信息泄露极容易被攻击者利用来进行有针对性的攻击，给目标网络带来严重的安全威胁。

4、供应链安全是不容忽视的一环

本月任务中多个目标网络通过供应链攻击实现突破，主要是针对目标网络平台或应用系统的供应商开展工作，通过获取产品源码并挖掘漏洞实现利用，最终打开目标网络突破口。供应链是网络构建的重要环节，确保供应链安全对保障网络安全至关重要。

5、弱口令和口令复用是重大安全威胁

本月任务表现出弱口令和口令复用仍是目标网络的重大安全威胁。弱口令或口令复用会导致网络内已有安全措施失效，尤其是内网堡垒机、网管系统、域控和网关等核心网络节点弱口令或口令复用的存在，常为渗透拓展带来极大的便利，致使业务内网全面失陷。

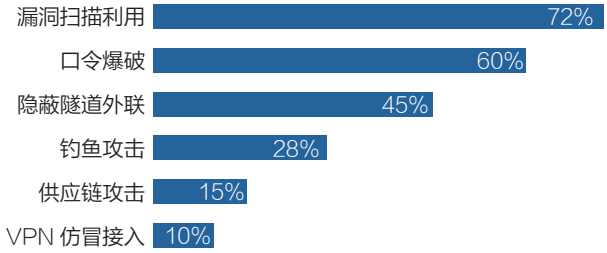
6、核心业务纵深防御措施不足

本月任务中发现目标网络对核心业务系统的纵深防御措施部署不足，核心业务网络缺乏必要的安全隔离或安全访问策略限制。主要表现为：外网突破后，通过边界服务器或普通内部人员主机就可以触及一些重要的内网业务系统；普通人员主机可以直接接入核心业务网络，对重要业务系统访问没有过滤限制。纵深防御措施的缺乏会导致核心业务系统严重的安全脆弱性。

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主要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、口令复用和内部应用漏洞为主。使用的主要技术手段分布如下。

攻击手段分布



1、漏洞扫描利用

本月任务中漏洞利用主要集中在互联网侧业务系统和门户网站，主要以敏感信息泄露、未授权访问、组件反序列化和文件上传执行等漏洞为主。这些漏洞主要是由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、对漏洞及安全威胁的应对不够高效等问题。

2、口令爆破

本月任务中口令爆破主要通过弱口令和口令复用实现，且主要存在于目标内网，是内网横向拓展的重要手段。比较常见的是应用默认口令和管理员口令设置为同一口令，反映出目标网络对弱口令和通用口令缺乏统一监管，尤其是对账号口令设置的复杂度和安全使用缺乏严格要求。

3、隐蔽隧道外联

本月任务中因客户网络安全防护较为严密，绝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网络穿透。对存在多层网络隔离的目标核心内网，也需要进行多层转发才能实现对核心业务网络的渗透控制。

4、钓鱼攻击

本月任务中因互联网侧直接突破手段受限，所以外部钓鱼攻击主要从客户中安全意识相对薄弱的人群入手，通过仿冒身份对客服人员进行业务投诉、更换头像冒充内部同事进行技术咨询等方式实现钓鱼突破。内部钓鱼则以水坑攻击为主，重点针对网络运维人员与核心

业务人员展开。

5、供应链攻击

本月任务中供应链攻击主要围绕目标网络外部业务平台或应用系统展开。通过产品特征匹配定位供应商，针对性地围绕供应商开展工作，获取产品源码、网络接口等关键信息，并进一步通过代码审计发掘安全缺陷，从而打开目标网络突破口。供应链安全缺陷的存在反映出目标客户对使用的网络产品把控不严，极易导致出现严重的安全隐患。

6、VPN 仿冒接入

本月任务中，部分金融行业分支机构多通过远程 VPN 接入业务网络，攻防演习任务中，攻击队也充分利用了现有的 VPN 资源实现对目标业务内网的隐蔽接入。在对 VPN 的攻击过程中，VPN 仿冒接入认证信息的获取是攻击的关键环节，主要利用部分 VPN 网关服务器漏洞和口令复用等方式实现。

四、典型攻击手段实现案例

1、外部漏洞利用突破

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

（2）某目标服务中心网站存在 Shiro 反序列化漏洞，通过漏洞利用获取 webshell，进一步获取网站后台服务器控制权限，为下一步拓展建立支点。

（3）某目标外部业务系统 Weblogic console 控制台存在 CVE-2020-14882、CVE-2020-14883 漏洞，通过漏洞利用获取到大量服务器控制权限。

（4）某目标任务调度中心平台存在 XXL JOB 反序列化漏洞，通过漏洞利用获取到系统服务器权限，突破网络边界。

2、口令爆破

（1）某目标安全认证数据库存在默认弱口令，通过弱口令登录数据库，可获取存储的大量人口库、信用库、法人库等密码，并可被进一步利用来获取该域内人口、信用及法人等信息。

（2）某目标电话系统存在弱口令，通过弱口令爆破登录电话系统后台修改电话模拟信息，可导致相关业务无法正常使用，也可通过 SSH 弱口令登录系统后台服务器，实现对该电话系统的完全控制。

（3）某目标数据采集平台存在弱口令，通过弱口令爆破登录平台可查看全部人员基本信息，如身份证号、家庭住址、电话号码等。

3、钓鱼攻击

（1）通过某目标官网在线客服入口，以投诉某位客服员工服务态度恶劣为由，向客服人员发送钓鱼文件，成功控制该客服人员办公机器，可进一步搜集信息积累渗透条件。

（2）通过前期搜集到的某目标内部技术人员微信号，冒充其同事添加好友并以咨询问题为由发送钓鱼文件，成功控制该人员主机，获取目标网络突破支点。

（3）某目标内网水坑钓鱼，利用前期获取到的内网服务平台控制权限，在内网服务平台的 WEB 页面插入恶意 js 代码，并引导内部人员下载，实现在内部人员点击访问时获取目标人员终端控制权限。

4、供应链攻击

（1）通过前期信息搜集确定某目标互联网业务系统开发商，利用致远 OA 漏洞控制该开发商业务服务器，从中获取目标系统源码，进一步通过代码审计挖掘漏洞，控制目标系统后台服务器，打开目标网络突破口。

（2）通过前期信息搜集，确定某目标管理中心信息平台的安全服务商，从网络内获取平台管理账号及接口信息，成功接入目标内网。

5、VPN 仿冒接入

（1）通过控制某目标网络管理员 PC 机器，从中获取该目标 VPN 后台管控权限，可添加任意 VPN 账户，并可利用仿冒 VPN 账户接入内部核心业务网络。

（2）在某目标网络机器中获取密码本，通过密码本找到该目标 VPN 日志管理系统登录口令，成功获取到服务器权限，并可通过 VPN 访问其他网络资源。

政策篇

国内，中共中央政治局召开会议，审议《国家安全战略（2021—2025 年）》；密集构筑数据安全防护网，网信办接连发布《网络数据安全管理条例（征求意见稿）》、《数据出境安全评估办法（征求意见稿）》征集意见。

国际上，美国基建法案获两院通过，将投入 19 亿美元建设网络安全；美国联邦政府网络安全事件与漏洞响应手册发布，推动安全响应最佳实践标准化。

国内

中共中央政治局召开会议，审议《国家安全战略》等重要文件

2021 年 11 月 18 日，中共中央政治局 11 月 18 日召开会议，审议《国家安全战略（2021—2025 年）》等重要文件。新版《战略》要求，确保重要基础设施安全，加快提升生物安全、网络安全、数据安全、人工智能安全等领域的治理能力。

工信部发布《“十四五”信息通信行业发展规划》

2021 年 11 月 16 日，工信部发布《“十四五”信息通信行业发展规划》，提出全面加强网络和数据安全保障体系和能力建设。规划包括增强行业关键信息基础设施安全保障能力、系统完善网络数据安全治理体系、持续提升新型数字基础设施安全管理水平、大力推动网络安全产业创新发展、全面提升网络安全应急处置水平、积极营造安全可信网络生态环境六大重点。

网信办《网络数据安全管理条例（征求意见稿）》公开征求意见

2021 年 11 月 14 日，网信办发布《网络数据安全管理条例（征求意见稿）》公开征求意见。征求意见稿指出，国家建立数据分类分级保护制度，对个人信息和重要数据进行重点保护，对核心数据实行严格保护。征求意见稿在个人信息保护、重要数据安全、数据跨境安全管理、互联网平台运营者义务、监督管理、法律责任多个方面对数据安全进一步提出了具体要求。

十二部门联合印发《关于开展 IPv6 技术创新和融合应用试点工作的通知》

2021 年 11 月 10 日，网信办等十二部门联合印发《关于开展 IPv6 技术创新和融合应用试点工作的通知》。通知提出，将开展 IPv6 网络安全保障能力建设试点，落实网络安全等级保护制度和关键信息基础设施安全保护制

度，推动网络安全保障系统改造升级，提高 IPv6 环境下漏洞监测发现与处置能力，探索在 IPv6 环境下新兴领域的网络安全技术、管理及机制创新。

网信办《数据出境安全评估办法（征求意见稿）》公开征求意见

2021 年 10 月 29 日，网信办发布《数据出境安全评估办法（征求意见稿）》公开征求意见。征求意见稿提出，数据处理者在向境外提供数据前，应事先开展数据出境风险自评估，重点评估出境数据的数量、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；数据处理者在数据转移环节的管理和技术措施、能力等能否防范数据泄露、毁损风险等。征求意见稿还要求，数据处理者累计向境外提供超过一万人以上敏感个人信息等情形的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

美国 CISA 发布联邦政府网络安全事件与漏洞响应手册

2021 年 11 月 16 日，美国网络安全与基础设施安全局（CISA）发布《网络安全事件与漏洞响应手册》，用于规划和实施联邦政府所有民事机构的网络安全漏洞与事件响应工作。这份手册为联邦民事机构提供了一套标准程序，以识别、协调、补救、恢复与跟踪影响联邦民事系统、数据及网络的事件或漏洞。手册还鼓励具有领先防御能力的联邦机构建设主动防御能力，如将对手重定向到沙箱或蜜网系统。

美国总统拜登签署《2021 年安全设备法》

2021 年 11 月 11 日，美国总统拜登签署《2021 年安全设备法》，以阻止华为、中兴等被视为所谓“安全威胁”的企业在美国监管机构获得新的设备牌照。该法案要求，美国联邦通信委员会（FCC）不再审查或批准任何所谓“对国家安全构成不可接受风险”的设备的授权申请。FCC 委员布伦丹·卡尔称，“‘安全设备法’将有助于确保华为、中兴等公司的不安全设备不再接入美国的通信网络”。

美国基建法案获两院通过，将投入 19 亿美元建设网络安全

2021 年 11 月 5 日，美国众议院批准了投资 1.2 万亿美元的基础设施法案，其中，近 20 亿美元将被用于提升整个联邦政府内的网络安全水平。美国参议院在今年 8 月通过了这项立法。该法案将分配 19 亿美元的网络安全资金，其中，约 10 亿美元将用于建立新的资助计划，帮助各州、地方、部落及领地政府提升网络安全水平。拜登大力称赞了法案的通过，“我们做出了早该做出的重要决定，这些事情在华盛顿被谈论了很久，但一直没能真正落地。”

澳大利亚拟出台《线上隐私法案》，实施最严年龄控制

2021 年 10 月 25 日，澳大利亚宣布拟出台《线上隐私法案》，要求社交媒体公司为 16 岁以下用户提供服务时，必须征得其父母的同意。在收集数据时，需优先考虑儿童的利益。用户可以提出不得使用或披露个人信息的相关要求，并有权拒绝个人信息被直销以使用。澳大利亚信息专员办公室拥有全面的调查和执法权力，如社媒平台未能遵守相关规定，将被处以其年营业额的 10% 或任何违规行为的经济利益的三倍的罚款，上限从以往的 220 万澳元提高为 1000 万澳元。

政策解读

数据出境需“安检”：《数据出境安全评估办法（征求意见稿）》深度解读

作者 国家互联网应急中心 卓子寒 张奕欣 邢 潇 北京德恒律师事务所 王一楠

一、出台背景

随着全球化与数字经济的发展，数据作为具有极大经济价值的生产要素，在国际间的流动越来越频繁，而且数量呈逐年增长趋势。然而，数据跨境的无序流动会给数据主体和数据安全带来风险，还关乎国家安全和社会公共利益。为了防范数据跨境流动中存在的各种风险，我国一直积极推动相关立法规范数据的跨境流动，如《汽车数据安全管理若干规定（试行）》和《网络安全审查办法（修订草案征求意见稿）》。

2021年10月29日，国家互联网信息办公室出台了《数据出境安全评估办法（征求意见稿）》（以下简称评估办法），全面和系统地提出了我国数据出境“安检”的具体要求。

实际上，国家互联网信息办公室分别于2017年和2019年就数据出境安全评估出台过两个办法的征求意见稿，即2017年4月11日的《个人信息和重要数据出境安全评估办法（征求意见稿）》（“17年版评估办法”）和2019年6月13日的《个人信息出境安全评估办法（征求意见稿）》（“19年版评估办法”）。本次公布的评估办法，一是落实上位法的数据出境管理规定和要求；二是保障数字经济健康有序发展；三是应对数据跨境传输和境外汇聚的安全风险。随着上位法《数据安全法》（以下简称数安法）和《个人信息保护法》（以下简称个保法）的相继实施，笔者认为这次评估办法将在征求意见之后很快正式出台。

二、适用范围

虽然《网络安全法》（以下简称网安法）、数安法、个保法均从不同角度提到过数据出境需要进行安全评估的情形，而本次发布的评估办法基于上位法的要求完整地规定了安全评估的具体适用范围。

首先，评估办法第二条将“数据出境”定义为“向境外提供”。在实践中，“提供”可以有多种呈现情形。通常理解的情形是数据处理者将数据转移至中国境外的地方。还有一种情形是数据并未转移至境外，而依旧存储在境内，不过数据处理者将境内数据库的访问登录信息或接口提供给境外主体，以便后者可以在境外远程访问查看（“远程访问情形”）。例如，有些外资企业的信息技术团队部署在中国境外，其通过互联网访问并处理境内服务器上存储的数据来提供远程技术服务。鉴于远程访问情形也会对境内存储的数据构成一定风险威胁，从数据跨境流动安全管理的角度来看，其理论上也属于

“数据出境”。

其次，评估办法第二条明确在出境数据涉及重要数据的情况下，安全评估是强制性的。需要注意的是，网信办基于数安法的授权，明确了重要数据需要进行安全评估的范围，包括关键信息基础设施的运行者和其他数据处理者。网安法第三十七条明确要求关键信息基础设施的运营者向境外提供重要数据需要进行安全评估。数安法第三十一条重申了以上立场，并在此基础上将其他数据处理者向境外提供重要数据所适用的具体出境安全管理办法交“由国家网信部门会同国务院有关部门制定”。本评估办法第二条正是呼应了数安法第三十一条，将其他数据处理者向境外提供重要数据的情形也纳入安全评估范围。

需要指出的是，超过一定量的个人信息可能会被各部门、各地区界定为重要数据，纳入重要数据目录，应当按照本办法关于重要数据的要求管理，如《汽车数据安全管理若干规定（试行）》第三条给出了重要数据的定义，其中，明确指出“涉及个人信息主体超过 10 万人的个人信息”属于重要数据，依照本评估办法的要求，出境数据中包含重要数据的，应申报安全评估。

最后，结合评估办法第四条，我们可以看到在出境数据涉及个人信息的情况下，达到一定要求才需进行安全评估。该要求可以分为三大类别：主体条件、客体条件及其他。主体条件是：关键信息基础设施的运营者，或处理个人信息达到一百万人的个人信息处理者。客体条件是：累计向境外提供超过十万人以上个人信息，或累计向境外提供超过一万人以上敏感个人信息。其他是：国家网信部门规定的其他需要安全评估的情形。

为了方便读者理解，本文通过如图 1 所示说明数据出境安全评估的适用范围。

三、评估原则

评估办法第三条明确了数据出境总体评估原则：事前评估和持续监督相结合、风险自评估与安全评估相结合，保障数据依法有序自由流动。

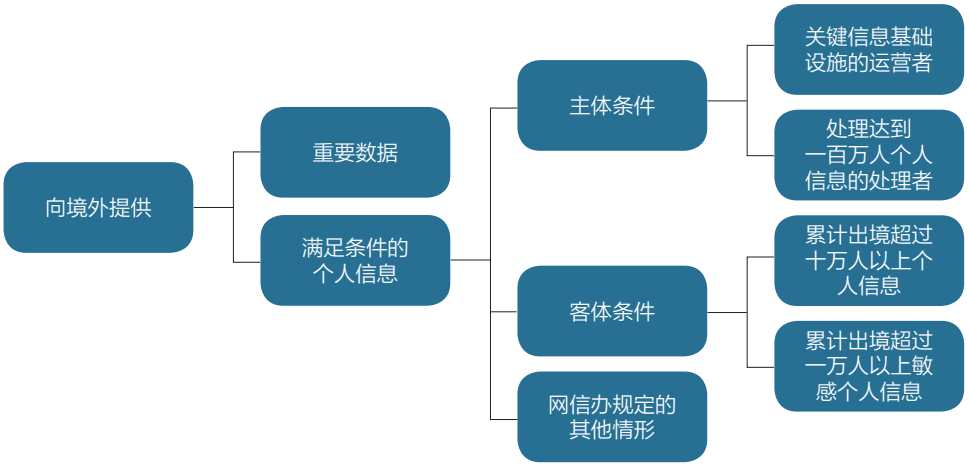


图 1 数据出境安全评估的适用范围

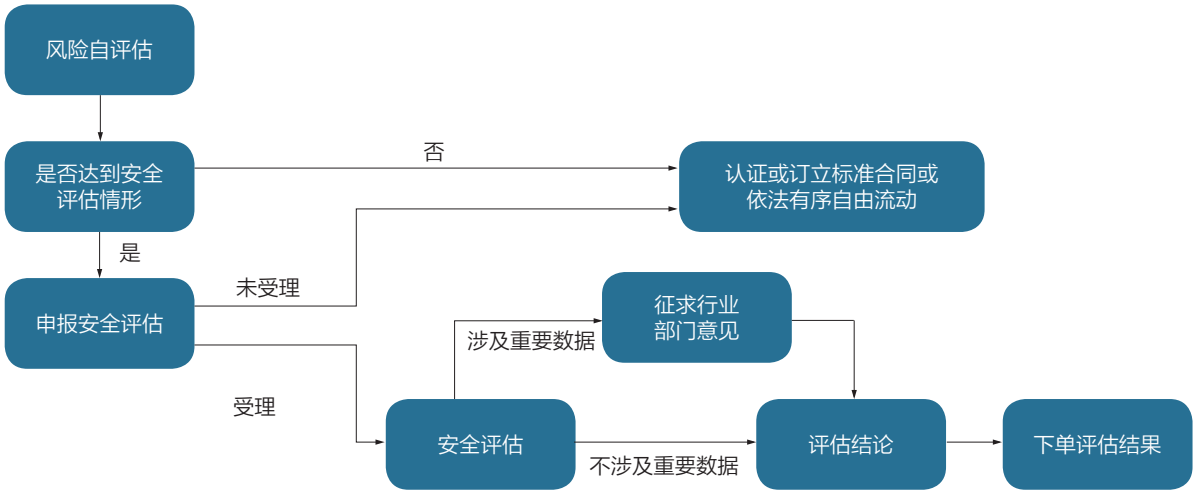


图 2 评估流程

“事前评估”即数据在安全评估通过之前不得出境。“持续监督”则体现在评估办法第十二条和第十六条，即对已经通过评估的数据处理活动在如下三种情形下需要进行再评估：1）两年期满；2）情势变化；3）违规处理。

“风险自评估”与“安全评估”的内容贯穿评估办法第五条至第十一条，具体解读详见下文。

四、风险自评估和安全评估

1、评估流程

评估办法第五条明确“数据处理者在向境外提供数据前，应事先开展数据出境风险自评估”，该表述中并未强调仅在适用安全评估的情况下才需要事先开展风险自评估。因此理论上，风险自评估适用于所有数据出境情形，无论是否涉及重要数据或上文所述满足一定条件的个人信息。

评估办法第六、七、十、十一条规定了安全评估的具体流程。为了方便读者理解，本文通过图 2 所示说明安全评估的工作流程，其中也包括个保法涉及的其他出境管理制度。

需特别说明的是本评估办法明确了国家网信部门对于数据出境安全评估的主导地位。在评估办法第十条中首次提到“专门机构”，笔者认为此机构可能为国家网信部门指定的特定评估机构。

2、评估事项及简析

评估办法第五条和第八条分别列举风险自评估和安全评估的重点事项，两者既有区别也有一致。为了方便读者理解，下文通过表 1 所示进行对比，并做简要分析。

3、关于涉及合同的几个问题

如以上表格所示，评估办法第五条和第八条均要求评估数据处理者与境外接收方订立的合同。不过，这里提到的合同与个保法第三十八条第（三）款中提到的“标准合同”不同。两者区别主要包括如下几个方面：1）前者是安全评估的申报资料之一，而后者是与安全评估并列的个人信息出境的安全管理制度之一；2）前者的主要条款由数据处理者与境外接收方在满足安全评估要求的前提下自由约定，而后者主要条款由国家网信部门制定；3）前者属于事前监管的范畴，后者属于事后监管的范畴。

合同的作用主要在争议解决程序中体现，即只有在争议解决程序中被认定有效、有约束力、最终可执行才

风险自评估事项	安全评估事项	简析
数据出境及境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性	数据出境的目的、范围、方式等的合法性、正当性、必要性	前者较后者增加“境外接收方”处理目的等合法性、正当性、必要性
出境数据的数量、范围、种类、敏感程度	出境数据的数量、范围、种类、敏感程度	前者与后者一致
数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险	数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险	虽然前者与后者一致，但后者在表述上与其他所有安全评估事项构成“总分”关系，而前者与其他自评估事项构成“并列”关系，逻辑上存在一定差别
数据处理者在数据转移环节的管理和技术措施、能力等能否防范数据泄露、毁损等风险	N/A	数据处理者防范风险的措施和能力更适合进行自行评估
境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全	境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规规定和强制性国家标准的要求	前者与后者基本一致
数据出境和再转移后泄露、毁损、篡改、滥用等的风险	出境中和出境后泄露、篡改、丢失、破坏、转移或者被非法获取、非法利用等风险	前者与后者基本一致
维护个人信息权益的渠道是否通畅等	数据安全和个人信息权益是否能够得到充分有效保障	后者涵盖的范围比前者更广
与境外接收方订立的数据出境相关合同是否充分约定了数据安全保护责任义务	数据处理者与境外接收方订立的合同中是否充分约定了数据安全保护责任义务	前者与后者基本一致
N/A	境外接收方所在国家或者地区的数据安全保护政策法规及网络安全环境对出境数据安全的影响	仅在后者列出，增加了评估部门的审核事项
N/A	遵守中国法律、行政法规、部门规章情况	仅在后者列出，增加了评估部门的审核事项

表 1 风险自评估与安全评估事项对比

能达到合同订立的目的。然而，如果在实践中安全评估未通过，数据处理者可能会面临违反已经生效且有约束力合同的风险。笔者的解决方案是将安全评估未通过情形与合同解除条款相结合，或者约定合同的生效条件为安全评估通过情形。另外，因为境外接收方在中国境内很可能没有资产，且中国法院判决会面临在境外无法得到承认和执行的风险，因此建议在合同制定过程中要特别注意争议解决条款的制定，以便满足可执行性的要求。

五、结语

相较于 17 年和 19 年两版评估办法，本评估办法所建立的管理体系更加成熟和完备，无论是在概念还是在制度建设方面，都与上位法及其他相关数据跨境流动安全管理规定形成良好的衔接。随着“重要数据”等概念的逐渐明晰，以及其他配套法规政策文件的不断出台，本评估办法的出台标志着我国在搭建数据出境安全管理制度的工作中迈出了重要且坚实的一步。

栏目主编　李建平

千亿隐私计算市场
四大技术流派大PK

可用不可见的隐私计算，成了既满足合规避险又满足业务需求的优解答案，四大技术流派大 PK。

隐私计算千亿蓝海开启

作者 奇安信数据安全研究院

11 月 1 日起，《个人信息保护法》正式施行，与《网络安全法》《数据安全法》一起，为保护数据资源安全提供了法律依据。

随着数字经济的不断发展，数据的价值越来越受到重视。充分利用数据要素的流通性，合理发掘数据价值，是满足客户差异化需求，解决供需之间信息不对称，提升市场效率的重要举措。面对趋强的监管环境时，如何在数据保护与数据价值的合理利用之间寻求合理平衡提出了更高要求。

在政策驱动下，可用不可见的隐私计算，成了既满足合规避险又满足业务需求的优解答案。

知名研究机构 Gartner 预测，到 2024 年，隐私驱动的数据保护和合规技术支出将在全球突破 150 亿美元以上，即达到千亿人民币规模以上。

兼顾数据利用与安全成挑战

2020 年，中共中央、国务院出台了《关于构建更加完善的要素市场化配置体制机制的意见》（以下简称《意见》），把数据正式纳入了生产要素，明确提出要加快培育数据要素市场。《意见》为推进数据要素市场化改革指明了方向。深圳等城市也相继发文规划设立交易场所进行大数据交易。上海、贵阳、重庆、哈尔滨等全国各地相继成立大数据交易所，各个大数据交易平台网站也陆续上线。

在政务领域，各地政府已纷纷成立数据资源管理局，在积累了大量政务数据的基础上，希望通过数据生产要素化孵化出基于数据挖掘的创新应用，促进数字经济的发展；在金融业中，金融机构需要收集消费者的资质信息、购买能力、偏好等数据，以便为信用良好的消费人群提供定制化的金融服务; 在医疗行业，精准医学、AI 制药等细分方向的发展都和数据息息相关；在 AI 领域，海量数据是计算机视觉、自然语言处理、语音识别等技术发展的基础——它们需要经过海量数据的训练才能达到理想性能水准。

此外，“新基建”的规划中明确提到了大数据产业，根据国家发改委的官方解读，新型基础设施之一的融合基础设施，主要是指深度应用互联网、大数据、人工智能等技术，支撑传统基础设施转型升级。

随着数据交易和价值挖掘的推动，实现数据保护与发展平衡提上日程。2021 年 9 月，我国第一部有关数据安全的专门法律《数据安全法》正式实施；11 月，《个人信息保护法》正式施行，强化对于个人隐私的保护。

隐私计算催生千亿市场

既要应用数据，又要保护安全，如何兼顾发展和

安全，平衡效率和风险，在保障安全的前提下发挥数据价值，是当前面临的重要课题。

《数据安全法》第十六条称：“数据安全在技术上的进步，以及监管层面的不断完善，也在为隐私计算及数据交易市场发展带来新的商机与活力。”

在数据融合应用和客户隐私保护的双重需求驱动下，作为数据安全进行协同合作，实现数据不动价值动的关键技术，隐私计算的应用可以保证参与方的数据不出本地，在保护数据安全的同时实现多源数据的跨域合作，对破解数据保护与融合应用难题提供了可行性思路。

隐私计算，广义上是指面向隐私保护的计算系统与技术，涵盖数据的产生、存储、计算、应用、销毁等信息流程全过程，想要达成的效果是使数据在各个环节中“可用不可见”。

IDC 认为，从行业应用来看，金融、医疗及公共健康行业对于隐私计算的探索尤为活跃。在数据成为新型生产要素的背景下，通过为政府大数据平台及数据交易所搭建隐私计算能力，从而推动数据的有序流动是未来几年值得关注的方向。

研究机构 Gartner 调查显示，管理技术、数据和动态风险的安全与风险管理领导者认为，隐私保护是目前面临的首要任务。在 2023 年年底之前，全球 80% 以上的公司将面临至少一项以隐私为重点的数据保护法规。

需求激增、高速增长，规模高于传统数据安全市场的行业，而新的市场必然催生新的赛道。Gartner 预计，到 2024 年，隐私驱动的数据保护和合规技术支出将在全球突破 150 亿美元以上，也就是千亿元人民币规模。

“隐私计算”江湖四大技术流派谁主沉浮?

作者 奇安信数据安全研究院

9 月 1 日，《中华人民共和国数据安全法》（以下简称《数据安全法》）正式落地实施，这是我国首部与数据安全相关的法律。

在已经到来的 DT（数据技术）时代，数据已然成为一种重要的资源，是一种重要的新型生产要素。2020 年 4 月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，明确将数据作为一种新型生产要素，与土地、劳动力、资本、技术等传统要素并列为要素之一。当各种各样的数据汇在一起时，数据便成为一种重要的战略资源。

当数据上升成为战略资源时，如何保护数据隐私安全便成为值得关注的话题。2021 年 5 月国家发改委、中央网信办、工业和信息化部、国家能源局联合发布《全国一体化大数据中心协同创新体系算力枢纽实施方案》，明确指出“试验多方安全计算、联邦学习、数据沙箱、区块链等技术模式，构建数据可信流通环境，提高数据流通效率”，以此促进数据有序流通，为培育数据要素市场奠定基础。

和传统生产要素相比，数据要想真正成为既可以自由流通，又能具备安全性的战略资源，就绕不开数据隐私计算这一环节。隐私计算可以让数据在流通过程实现“可用不可见”，在保护数据隐私的前提下，解决了数

隐私计算技术流派象限

据流通、应用等数据服务问题，成为破解数据利用和安全性这对矛盾的重要途径。

就像武侠世界里的不同门派拥有不同绝学，在隐私计算的江湖中也有不同流派，它们采用不同的技术形式实现数据隐私安全的目标。

根据数据是否流出、计算方式是否集中来划分，隐私计算可以划分为四个不同的象限，分别是数据流出、集中计算；数据流出、协同计算；数据不流出、协同计算和数据不流出、集中计算。

流派一

数据流出、集中计算。

代表技术：数据脱敏、差分隐私、同态加密

该流派的核心，是对数据进行变形、扰动、加密等操作，可保障数据流出时的隐私安全，主要有三种安全技术：数据脱敏、差分隐私、同态加密。

数据脱敏（Data Masking）是指使用脱敏规则对数据中某些敏感信息进行数据的变形，从而达到保护敏感隐私数据的目的。更具体来讲，我们可以采用删除可识别个人的信息的方式，让数据描述的人保持匿名，也可以采用对数据去标识化，让人们无法根据数据识别到具体的个人。

如果说数据脱敏是通过对敏感信息“做减法”的方式实现保护隐私，那么差分隐私（Differential Privacy）就是以“掺沙子”的方式，通过在数据或者计算结果上添加一定强度的噪声，来保证用户无法通过数据分析结果推断出是否包含某一特定的数据。

而同态加密（Homomorphic Encryption）则是用技术方式，在不影响数据运算结果的前提下，将数据变为密文，这也就不再涉及隐私的问题，而不同的加密技术允许不同的运算规则。

整体看，这些技术通过对数据操作来保障数据流出时的隐私安全，但是它们也有一些局限性：

1）数据脱敏容易遭受攻击，从技术恢复数据中的敏感信息较为容易。

2）差分隐私会降低机器学习准确率，较高强度的噪声虽然较好地保护隐私，但对数据分析的准确性也有较大的影响，令人感到得不偿失。

3）同态加密运算效率低，也会影响使用该技术的意愿。

流派二

数据流出、协同计算。

代表技术：安全多方计算平台

“两个富翁的财富是 1~10 之间的整数，如何能在不透露双方财富的前提下，比较出谁更富有？”这是姚期智院士在 1982 年提出的“百万富翁问题”。富翁不露财却又想做比较，按照这样的逻辑，如何在一个互不信任的多方系统中，各参与方能协同完成计算任务，同时保证各自数据的安全性呢？这就是网络安全版的“百万富翁问题”。而解决之道就是安全多方计算。

安全多方计算是密码学的一个子领域，其目标是为各参与方创建共同计算一个函数，这个函数的输入来自不同的参与方，同时保证这些输入内容不泄漏。目前，随着业界对安全多方计算技术的关注，其应用范围越来越广泛，国内外各大厂商也相继推出各自的安全多方计算平台或隐私计算平台。与此同时开源的安全多方计算库也越来越多，如基于 Google 公司 Tensorflow 基础上开源的 TF-Encrypted，开源社区 Openmined 基于微软 SEAL 开源的 TenSEAL，以及安全多方计算的协议实现 ABY3 与 MP-SPDZ 等。

这一流派下又有两种主流技术。一种是混淆电路（Garbled Circuit）。通过将两方参与的安全计算函数编译成布尔电路，并将电路的真值表进行加密、打乱，

就能保证电路的正常输出而又不泄露参与计算的双方私有信息。另一种是秘密共享（Secret Sharing），类似于需要将所有的秘密拼在一起才能还原全貌的思路，这种技术在参与者之间分发秘密，每个参与者都被分配了一份秘密分割，只有当足够数量的、不同类型的秘密分割组合在一起时，才能将秘密恢复出来；单个的秘密分割本身是没有任何意义的。

这一技术实现了可证明的安全性，对于安全性要求较高的场景具有较好的应用价值。但在实际落地中，仍有一定的局限性。

1）性能低下：由于使用了很多密码学方法，一些复杂的任务很难在在短时间内完成计算任务；

2）程序编写难度大：由于安全多方计算涉及密码学技术较多，且应用起来流程较其他技术相比非常复杂，通常需要借助额外的编程库进行实现，这大大增加了应用编写人员的学习成本和工作量，导致在实际落地过程中仍存在障碍。

3) 调试难度大：由于安全多方计算仅输出最终的执行结果，在面对复杂的分析问题时，使用者难以仅通过程序的最终执行结果获得反馈去优化整个数据分析过程。

流派三

数据不流出、协同计算。

代表技术：联邦学习平台

联邦学习 (Federated Learning) 的概念于 2016 年由 Google 率先提出，用于解决安卓手机终端用户在手机端使用用户数据训练模型的问题，其本质上是一种分布式机器学习。这一技术的核心思路是，尽管有同一个中央服务器或服务协同商，但参与方的原始数据都只会在本地，而不会用于交换传输，真正参与聚合的完成训练的是经过模型转换的数据信息。

由于场景的区别，联邦学习还分为了横向联邦学习、纵向联邦学习和联邦迁移学习等形式。随着欧盟《通用数据保护条例》（GDPR）的推出，数据隐私保护越来越受到各国重视，联邦学习的应用范围也愈加广泛。例如，Google 公司开源了一个学习框架，用来完成分类、回归等机器学习任务；国内以杨强教授为代表的微众银行开源联邦学习框架 FATE，提供一站式联邦模型服务解决方案。

整体看，联邦学习可以在数据不流出本地的前提下，联合多个参与方训练模型，对于打破数据孤岛具有重要意义。其局限主要在：

1）存在隐私泄露风险，联邦学习的训练模型是需要共享的，这就为攻击者根据模型信息倒推隐私数据提供可能。

2）机器学习算法兼容性较差，且目前支持的机器学习算法较少。

3）机器学习任务调试困难，要想获得最优的模型和参数往往通过不断尝试和调试获得，一个标准机器学习工作流包括数据探索、特征工程、模型选择、超参数优化等步骤，再加上在联邦学习场景下，数据分散在各地，数据可用不可见，这些步骤很难在保证安全地前提下完成。

流派四

数据不流出、集中计算。

代表技术：可信计算平台

可信计算平台就是通过隔离机制构建出一个安全可控区域，在这个足够安全的空间中，数据能够被集中训练且不流出，从而保证内部加载数据的机密性和完整性。

具体讲，可信计算平台又有两种技术。一种是可信执行环境（Trusted Execution Environment，TEE），该技术通过软硬件隔离安全机制建立一个安全隔离的执行环境，从而防止外部攻击者（包括系统管理员）

窃取 TEE 内部运行的数据。硬件上，它依赖于将其预置在 CPU 等硬件，然后再通过应用程序的参与营造出一个安全世界。TEE 具备支持多层次、高复杂度的算法逻辑实现，运算效率高以及可信度量保证运行逻辑可信等特点。然而，TEE 由于依赖于 CPU 等硬件实现，必须确保芯片厂商可信。同时，TEE 对服务器型号限制较大，其功能和性能等均受到硬件限制。

另一种技术为数据沙箱技术，该技术通过构建一个可信计算环境，使得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。对数据需求方人员，他们不能进入数据沙箱查看调阅真实的全量数据。对于数据分析师而言，由于数据沙箱将调试环境和运行环境隔离，所以他们也只能在调试环境中使用样本数据调试代码，然后将代码发送到运行环境中运行全量数据，从始至终都无法接触全量数据，这样，隐私安全的保护就得以实现。

数据沙箱技术主要特点是将隐私安全能力植入大数据计算、存储引擎等基础设施，通过将调试环境与运行环境隔离，构建一个安全可控的数据环境，提升数据融合计算过程中的隐私安全水位，实现数据挖掘计算过程中的可用不可见，且不改变业务原有技术栈和使用习惯，无需改造现有的数据分析算法和工具，同时使得业务算法模型精度折损微小。因此，可以说这是兼具安全性和可操作性的较为成熟的技术。

目前，国内学术界以中国工程院院士方滨兴为代表，基于可信计算平台技术打造 AI 靶场接收用户程序，通过防水堡过滤用户程序外传结果时夹带的原始信息。在国内产业界，奇安信、百度、京东数科、UCloud 等各大厂商均有推出数据沙箱相关产品。以奇安信率先推出的“数据交易沙箱”为例，它基于“数据不动程序动”“数据可用不可见”的安全理念，采用调试环境与运行环境隔离的技术来解决数据流通交易过程中的数据隐私安全问题。

除了上述谈及的四大流派，在网络安全的江湖中，伴随网络技术的不断发展，区块链技术与上述技术流有着融合趋势。区块链具有数据可溯源、难以篡改、公开透明、智能合约自动执行等技术特点，能够在一定程度上解决多方协作、多方信任和数据共享流通的问题。在与隐私计算相结合时，主要有三个关键技术：一是基于区块链的安全密钥管理与可信身份认证；二是链上、链下的安全计算协同；三是数据生命周期管理。

安全密钥管理与可信身份认证能够实现相对安全灵活的密钥管理体系，降低密钥中心化存储的安全风险，在防止中间人攻击和丢包攻击的同时，使得隐私管理更加安全、精细化。此外，该技术也能解决数据共享参与者身份及数据可信问题，这样，不仅可以提升恶意参与者的作恶成本，还可以保障共享计算的数据质量。

链上、链下的安全计算协同又可分为链上与链下两个部分。通过链上与链下相结合，区块链专注业务逻辑可信执行与数据权属凭证流通，而链下隐私计算网络负责大规模运算和数据价值流通，最终实现一加一大于二的效果。

数据生命周期安全管理方面需要实现全流程管理，包括数据采集、传输、存储、使用、流通、销毁等环节。数据共享计算参与者可以在链上用智能合约来实现计算过程中的协作管理功能，由参与方之间共同治理隐私计算过程，协作过程公平公正、公开透明、权责对等，避免了中心化协调方参与带来的隐私泄漏的风险，也能确保参与方按照约定方式计算 , 提升数据共享协作效率。

区块链隐私计算目前也正在投入实际场景中得到应用。然而，它仍然具有一些问题等待进一步解决。例如，区块链上数据处理能力不足，链上计算受限于虚拟机执行和网络共识性能，容易出现链上无法承载大量交易和无法即时交付等问题，难以满足支持高吞吐的交易量和即时交付的需求。其次，由于在引入区块链技术时数据半同态加密、用户身份认证等密码学保护手段。这会使得架构上引入了额外的申请审批流程，计算上引入了加密带来的额外计算开销，使得数据流通过程效率大幅降低。

综上，隐私计算四大技术流派各有千秋、各有利弊。但毫无疑问的是，隐私计算既具有技术上的先进性，又具有操作执行上的便捷性、延伸性及高效率等特点的技术，无疑能够在当前获得更大的认可。而把握未来技术的动向，占据技术发展的上风，将成为各门派都需追求之事。

距离打通隐私计算服务“最后一公里”还有多远?

——奇安信数据安全研究院执行院长、哈尔滨工业大学（深圳）刘川意教授访谈

隐私计算源起，推动数据要素价值挖掘

问雷锋网：为什么会出现隐私计算这个技术？为什么这两年发展的这么快？是什么在推动？

刘川意：2017 年开始，公安部、最高检察院进行了侵犯个人信息专项整治行动，随着执法力度的不断加大，打击了许多游走在灰色地带的非法数据交易公司。另外，国家也连续出台了一系列数据安全法律法规，如《数据安全法》《个人信息保护法》等。因此，数据市场出现了买方与卖方的断裂，数据所有方和数据需求方之间迫切需要一个安全技术手段来达成数据交换、开发利用、交易。关于为什么这一技术发展如此之快，关键还是政策推动导致的。隐私计算业务我们在 2018 年在方滨兴院士的指导下开展起来，那个时候我们在和很多政府、医疗等重要行业客户交流数据开发利用过程中的安全问题时，客户回复数据都在封闭的局域网里不会给到第三方。直到 2020 年 4 月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，明确将数据作为一种新型生产要素，与土地、劳动力、资本、技术等传统要素并列为要素之一。如何探索数据要素流通交易、数据要素市场化、多方数据如何安全融合等，

在政府单位、金融机构、运营商等成为了热门话题。直到今年 5 月，国家发改委、中央网信办、工业和信息化部、国家能源局再次联合发布《全国一体化大数据中心协同创新体系算力枢纽实施方案》，明确指出“试验多方安全计算、联邦学习、数据沙箱、区块链等技术模式，构建数据可信流通环境，提高数据流通效率”，以此促进数据有序流通，为培育数据要素市场奠定基础。随着《数据安全法》《个人信息保护法》在今年相继出台，数据如何在安全前提下实现开发利用和流通交易这一核心问题直接影响到了互联网、运营商、金融机构、政府等重点行业的核心数据业务。

问雷锋网：隐私计算技术怎么划分？这一技术的出现有何意义？

刘川意：我们从数据流动（数据流出 / 不流出）和数据计算（集中 / 协同计算）这两个维度对相关技术进行了梳理和分析，形成四大技术流派：匿名脱敏、差分隐私与同态加密；安全多方计算；可信计算平台；联邦学习。隐私计算技术的出现能够很好地平衡数据价值挖掘与数据隐私保护间的矛盾问题，解决实际中数据要素由于隐私安全问题，缺乏安全手段、安全开放与流通，为数据作为生产要素流通交易提供了技术基础，使得充分发挥数据要素的价值。

集顶尖科研实力，为隐私保护和数据安全开路

媒体：奇安信是什么时候开始做隐私计算方面的内容？过程是怎样的？有没有遇到哪些难题？有哪些重要代表性的事件或者时间节点？

刘川意：奇安信数据安全子公司云安宝在 2018 年开始做隐私计算业务，当时方滨兴院士在 2017 年就高瞻远瞩地看到了这个痛点问题，并多次和我们核心团队强调这个事情的重要性。隐私计算涉及 AI、大数据、系统、密码等多学科，属于非常前沿的新技术领域。奇安信数据安全子公司云安宝与科研机构紧密合作，2018 年与鹏城实验室、哈工大（深圳）等科研院校共同承担了广东省科技计划安全专项 – 面向大数据应用的隐私保护与对抗技术与方法；并与哈工大（深圳）成立了数据安全研究院，召集了一帮教授和博士针对隐私计算领域进行深入研究。为解决这一矛盾问题，方滨兴院士提出破局隐私保护与数据挖掘相悖的“模型加工场”方法。

这是一套系统的解决方案。

- 基于核心方法——数据不动程序动：采取网络靶场技术，构建一个可信计算平台，隐私数据可以以裸数据的形式放在该平台中，由摆渡过来的外部程序利用这些数据进行模型加工，但人员不能进入该模型加工场查看调阅数据；
- 采用关键手段——分享价值不分享数据：使用信息过滤技术构建一个“防水堡”，确保外部程序在可信计算平台中计算之后，向外输出的只能是参数之类的宏观信息，而不能是微观的原始数据；
- 基于辅助模式——数据可用不可见：使用者根据所提供的经过变换的样本数据进行潜在价值的挖掘分析，即“数据可用不可见”；
- 基于扩展模式——保留所有权释放使用权，所有权与使用权相分离，可信计算平台可提供远程控制模式，让数据的所有者来远程决定其放到平台中的数据向谁赋予使用权，且由可信计算平台来保障被赋予使用权的人只能使用数据来生成相应的模型，以此发挥出模型加工场的作用，达到交易使用权不交易所有权的目的。

在方滨兴院士的指导下，基于数据不动程序动，数据可用不可见的隐私保护新理念，创新性地提出了调试环境与运行环境分离的体系结构，研发了数据交易沙箱这一核心产品，实现了在保护数据隐私的前提下，最大限度地挖掘大数据价值。数据交易沙箱目前已应用在政务、医疗、公安等重点领域，近期，“基于数据沙箱技术的数据服务平台在医疗领域的应用”在世界互联网大会上荣获 2021 年数据安全典型实践案例。

打通隐私计算“最后一公里”

媒体：奇安信的隐私计算现在形成了怎样的体系？有哪些典型的落地案例？

刘川意：奇安信的隐私计算目前主要采用了数据沙箱和联邦学习等技术，研发了数据交易沙箱这一产品，可支持集中式数据共享开放，分布式数据融合分析等场景。合作落地案例有某健康医疗大数据平台，将临床诊断数据安全开放给药厂做真实世界研究，有利于评价该药厂抗焦虑药物的有效性以便改进；落地多个大数据局政务数据安全开放，落地客户已经完成了数据中台的建设，汇聚了社区、金融、市政、交通、环境、园区等类型的数据，希望将数据服务于整个城市不同类别业务，如政务、金融、产业等，加快智慧城市的战略发展。在公安行业，落地国内首个重点人员风险评估 AI 预警，由于公安数据极其敏感和机密难以给到第三方数据分析公司或团队，某公安基于本项目数据安全流通交易平台使得公安数据开放至第三方数据分析公司或团队，实现数据可用不可见。基于本项目平台创新性研发了国内公安行业首个基于 AI 实时计算的风险评估预警系统，以及基于自然语言处理技术的命案风险预警系统，实现了公安大数据安全融合分析，有力支撑了某省情报指挥调度工作。

媒体：相比国内隐私计算厂商，奇安信的独特性体现在哪里?

刘川意：奇安信创新性地提出了基于调试环境与运行环境隔离的数据沙箱技术，目前被国家发改委牵头的《全国一体化大数据中心协同创新体系算力枢纽实施方案》采纳，作为数据要素流通的四大技术模式之一。“试验多方安全计算、区块链、隐私计算、数据沙箱等技术模式，构建数据可信流通环境，提高数据流通效率。探索数据资源分级分类，研究制定相关规范标准”。

隐私计算商业落地任重而道远

媒体：从行业的角度来看，隐私计算解决的问题是什么？隐私计算当前遇到最大的挑战是什么?

刘川意：从数据拥有者角度（更多的是甲方，如政府、能源等），由于业务需要，得把数据共享出去，保证数据安全是他们的第一要务。从数据需求者角度（更多的是乙方，如银行等），目前无法赤裸裸地采买数据，迫切需要隐私计算作为一种获取数据的手段。隐私计算当前遇到的最大挑战是技术需要在实际场景中真正落地，现在处于市场早期，处在有了锤子（技术）到处在找钉子（实际场景）的阶段，一旦在实际场景真正趟通，进而形成可复制路径。

结语

近年来，隐私计算技术在金融、医疗、政务等多个场景开始落地，正逐渐形成跨机构、跨企业、跨行业的交叉应用。然而，隐私计算技术虽然具有广阔的商业潜力，但当前的市场还存在认知不充分、数据流通意愿不足、技术瓶颈多等问题，大规模商业化落地仍然受限。

那么如何商业化打通隐私计算服务的“最后一公里”，成为行业内大家要思考的问题。

隐私计算业务场景主要可以划分为三类参与方：作为数据源的数据方（大数据局、征信公司、拥有用户信息的互联网公司等）、使用数据的业务方（金融机构、政府机构等用在自身业务身上）和隐私计算技术服务商本身（搭建计算服务系统在业务方、数据方、可信第三方部署服务）。由此隐私计算厂商的类别可初见端倪，投入到隐私计算行业还需要根据自己的技术和商业资源进行市场定位，不同的特征决定了企业不同的市场定位和发展路线。其次继续打磨隐私计算的技术和产品，符合用户的需求。现在的产品和技术还不足以支撑用户对于完整方案的需求，隐私计算只是作为方案中的一个模块，有时需要多方合作客户进行配合。目前技术可靠性还有待提高，并且缺乏可靠的技术标准认定，用户对采纳技术有疑虑。再次，隐私计算产业需要进行推广并建立多方协同的合作模式。与一般技术的商业模式不同，隐私计算的商业天然有着多方协同的特征，是一个基于数据生态、搭建基础设施的商业。在现实情况中，有时可能会出现几家数据源，要打通数据方和业务方促进各方的合作，就需要搭建多方协同的合作模式。

隐私计算产业目前还没有成熟，不论是技术路线还是商业路径可能都会有不同的答案，究竟什么样的答案才是正确的，还需要时间来验证。

（本文采访媒体为雷锋网）

我用 12 个字母，围观了 APT 活动的所有细节

作者 公关部 魏开元

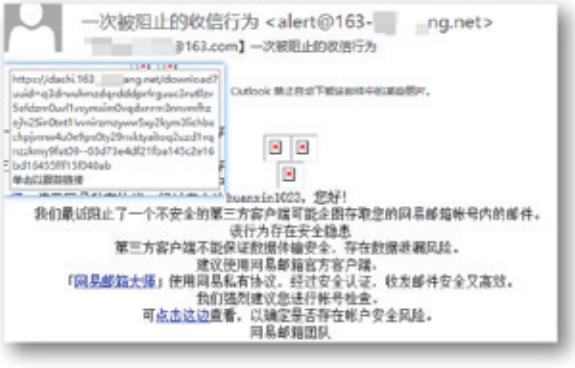
2018 年，一种伪装成邮箱登录页面的钓鱼网站，开始频繁进入奇安信威胁情报中心的视野。

说句实在话，钓鱼邮件作为最古老的攻击方式之一，大家早已司空见惯，收到之后或许一笑蔽之，转眼就抛诸九霄云外。可短时间内监测到大量相似的钓鱼邮件，还是引起了奇安信威胁情报中心分析师们的注意。

通过分析钓鱼网站的源代码发现，当受害者输入自己的账号邮箱后，该钓鱼网站并不以窃取邮箱账户为主要目的，而是将受害者访问页面的时间和当前使用的 IP 地址，一同发送到攻击者服务器。

经验丰富的分析师们敏锐地意识到，和寻常盗取账户的钓鱼邮件攻击不同的是，这或许是一次有预谋、有组织的情报搜集活动，很可能是为了后续的入侵“踩点”。

在浏览器地址栏中输入 ti.qianxin.com 共计 12 个英文字母后，奇安信威胁情报中心就此揭开了“毒云藤”APT 组织的一次精心谋划的 APT 攻击活动的神秘面纱。



“平安格勒”战役

从表面上看，ti.qianxin.com 是奇安信的一个二级域名，但它究竟是什么？为什么可以围观 APT 活动的细节？要知道，如果不是通过它寻根究底，这次 APT 攻击可能就被错过了。

在介（广）绍（告）之前，先回顾一小段电视剧。

《亮剑》这部电视剧里，有一集讲述了独立团团长李云龙冲冠一怒为红颜的故事。

在 358 团炸毁山本特工队的汽车之后，李云龙短时间内集结了近万人的武装力量，将偷袭赵家峪、劫持秀芹的山本一伙围在了平安县城里。

作为日驻晋第一军司令官筱冢义男的心头肉，山本特工队全军覆没是他决不允许的。于是在接到山本的求援电报后，筱冢义男一刻都不敢耽误，随即向平安县派遣援兵。一时间，来自太原、水泉、太古等地的日军均不顾一切向平安增援。

这样一来，本就敌、我、顽势力犬牙交错的晋西北，一下子乱成了一锅粥。

不过，由于李云龙的作战行动并没有向上级汇报，八路军总部一直被蒙在鼓里。好在总部的侦察员顺利监听到了日军的电台，并获取了一条重要的情报信息——敌人反复提到了平安县。正在认真研究作战地图的总部首长，一下子就明白了过来，所有战斗皆围绕此地打响，并判断是李云龙在搞什么大动作。

形势豁然开朗。

放眼当时的中国版图，平安县城只是一个芝麻大小的据点，如果不是山本特工队来到这里，或许八路军、晋绥军、中央军，甚至日军，都不会注意到这个地方的

存在。可当指挥员把围绕平安县城所展开的战役在作战地图上标示出来之后，却折射出了抗日战争后期，中国军民由战略相持阶段，转入战略反攻阶段的画卷。

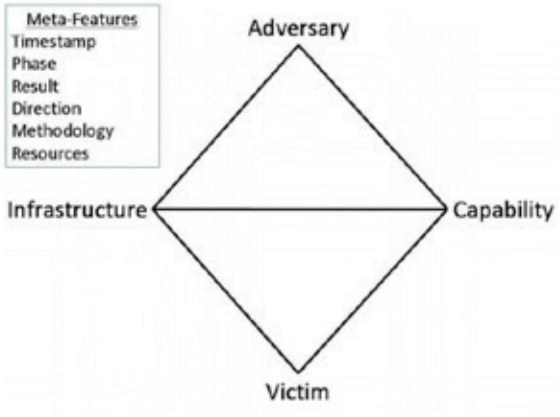
网络资源与钻石模型

在网络空间，也有无数个这样看起来并不起眼的地方，从表面上看，它可能是邮箱、域名或者 IP 地址等，从而标记出网络空间的具体位置，我们习惯把这些元素叫作网络资源。

在平时，这些网络资源之间相安无事，甚至“见面”之后还会打个招呼。比如，我在某网站注册一个会员，管理员邮箱没准会给我发一封验证邮件。可一旦发生网络攻击，它们之间也会乱成“一锅粥”。我可能在不知情的情况下就访问了一个恶意域名，管理员发给我的也可能是一封精心伪造的钓鱼邮件。

“或许这样一封钓鱼邮件的背后，就是一次策划精密的网络渗透活动。”奇安信威胁情报中心负责人汪列军说。

为了帮助安全分析师们完整的描述一次网络攻击，有人在 2013 年提出了入侵分析钻石模型，用于把对手（攻击者）、受害人、能力（攻击者使用的攻击代码或者恶意工具）及基础设施（指向服务器的 IP 地址和域名等网络资源）这四类关键元素以一定的关系关联起来。



至于为什么叫钻石模型，请看下面这张图像不像钻石？

举个例子。在李云龙率部队攻打平安县城这段故事中，从太原、太古等地开来的日军援兵就是攻击者，平安县城就是他们的增援目标，太原、太古这些增兵的地方就是网络资源，而部队番号、数量、交通工具、火力配备情况等就是能力。

八路军总部以平安县城这条情报作为基础，把所有围绕此地展开的战役，绘制成了一张作战态势图，继而下达了下一步作战命令：联系一切能联系上的部队，不惜一切代价阻敌增援。就算要枪毙李云龙，也得等打完仗再说。

搞网络安全的又何尝不是在打仗。而且这个仗是打的那么悄无声息，没有震耳欲聋的枪炮声，甚至在攻击者得手后的很长一段时间后，才会发现防线已经被对方攻破了。

由此可见，第一时间掌握对手的动向是多么重要。

想要掌握对手的攻击态势，基于网络资源进行威胁情报关联分析，是最常用也是最有效的手段，因为你能清楚地看到敌人从哪里来，要到哪里去。

而所谓威胁情报，简单来说就是一切和对手相关，能够为安全决策提供支持的知识。（有兴趣可以看看《网络空间的隐蔽战线：一场情报传递的“生死时速”》）

其中，攻击者使用的特定 IP、域名、邮箱、社交账号等网络资源，就是威胁情报来源的主力。

网络资源之所以应用最为广泛，重要的是在于其可以消除不确定的能力。尤其是域名，在特定的时间内，只会被特定的攻击者使用。相比之下，尽管某些 APT 组织（如蔓灵花等）早期使用的特种木马也有很强的特征，但大多数时候，单靠样本特征并不容易判断它到底归属哪个 APT 组织。

还是举个例子。

假设从太原方向的日军援兵为了迷惑八路军打援部队，换上了八路军的衣服向平安县城方向开进，途中被

我军侦察员发现，行动可疑。如果侦察员只是发现这伙人齐刷刷的装备日军制式步枪三八大盖，并不能完全消除不确定性，因为在对日作战过程中，八路军也大量缴获并使用这种步枪；但如果发现这伙人是从太原出发前往平安方向的，那结果就不一样了。当时，太原属于日占区，绝不可能驻扎八路军。

除了这个原因，相比其他类型的数据，网络资源的收集，可能更加容易一些。

细节决定一切

话说回来，APT 活动的关联分析并没有什么高深莫测的手法，也没有什么特别的捷径，关键在于数据收集能力。只有数据足够完整，才有可能掌握 APT 活动的所有细节。

如果你能掌握所有攻击者使用的 IP 地址、域名、邮箱、社交账号、恶意代码及这些信息之间的关系，那么攻击者的所有动向将一目了然。

说细节决定一切，一点都不为过。

假如在李云龙攻打平安县城的时候，八路军方面并没有获得太古方面日军前来增援的这个细节，没有派兵阻击，导致太古方面的日军及时赶到平安城下，独立团立马将会面对两面夹击的窘境，甚至导致整个行动功亏一篑。

那么问题来了，怎么才能获得这些信息。众所周知，APT 组织都喜欢玩捉迷藏的游戏，你想发现他们，总得费点功夫。

说起来其实很容易，收集这些信息主要有两种方法。第一种是“别人告诉你”，也就是通过收集公开的 APT 活动报告或者威胁情报共享的方式，获取 APT 组织的名字、使用的 IP 地址、域名 whois 或者恶意代码这些信息；除此之外，组织还可以购买一些商业威胁情报。

需要强调的是，千万不要忽略公开信息的重要性。基于开源威胁情报进行 APT 组织追踪，同样是一个非常重要的方法。并且，目前没有一个平台有能力收集 APT 分析所需的全部基础数据，所以多平台联合使用互相参照补充是合理的做法。

第二种是“自己告诉自己”，也就是依靠工具（如 EDR、沙箱、DNS 解析工具等），记录应用程序的网络行为，包括访问了哪些 IP 地址等。

但其实这两种方法可以归结成一种方法，无论是别人的还是自己的，都是依靠工具的记录。

“所以，APT 的关联分析，需要海量的历史数据积累和强大的信息收集和技术平台支持。”汪列军说。

没有金刚钻，还真揽不了这个瓷器活。

说起信息收集能力，奇安信还是有几样能拿得出手的“绝活”。

第一，奇安信天眼。作为一款高级威胁检测和安全态势感知的产品，天眼拥有强大的全包存储能力，能够将网络上视野范围内的 TCP 会话记录、邮件活动、DNS 交互、URL 访问、文件下载都记录并存储下来。

第二，红雨滴云沙箱。它能够基于 QOWL 反病毒引擎和文件深度扫描系统，对可疑文件进行深度动态扫描，并把文件的所有行为（如创建进程、注册表及连接外网 IP 等）都记录并存储下来。

第三，奇安信安全 DNS。它能为用户提供 DNS 解析服务，并判断所解析的域名及对应的 IP 地址是否存在威胁。仅 2021 年 6 月，奇安信安全 DNS 已对公众提供域名解析服务 570 亿次，解析域名近 2 亿，拦截威胁域名请求 1800 万次，涉及威胁域名 15 万。

至于其他的绝活，这里就不一一列举了。

“甜蜜的烦恼”——自动化分析工具不可或缺

对于 APT 活动分析来说，没有数据收集渠道自然是万万不能的，可是当你收集到的数据太多，虽然能看到非常多的 APT 活动细节，但是同样会带来甜蜜的烦恼：看不过来了（脑补一下拼图游戏，10000 个碎片起的那种）。

不过，在最开始的时候，并不是所有的信息都一股脑摆在分析师的面前。APT 活动的关联分析，往往是从

一小撮信息开始的，需要通过不断的关联拓展，最终形成一块完整的拼图。

有公开统计显示，绝大多数的恶意软件会使用 DNS 协议，比如，回连一个以 Domain/URL 呈现在互联网上的的 C2 地址、使用一个 Domain/URL 作为投递地址（如挂马、钓鱼等）。

所以，当分析师利用 EDR 或者沙箱捕获了一个恶意软件之后，很大概率能够通过 DNS 解析记录，追踪到该软件外连的域名，再继续该域名进行 whois 查询，找出域名注册信息，同时关联到其他相关的域名，而这些相关的域名又可以通过 DNS 解析信息，追踪到更多尚未被捕获的恶意软件……最终将所有攻击活动查个水落石出。

举个非常形象的例子：当你发现一张桌子的时候，你可以通过技术手段找到这张桌子的主人是谁；再通过询问主人，发现他不仅有其他桌子，还有不少椅子，并且这些桌子和椅子都有谁用过。

由于需要同时跟踪大量的数据，一个自动化的基于规则或模型的工具平台是必需的。它能够把这些数据，按照一定的规则关联起来。

在浏览器地址栏输入 ti.qianxin.com 这 12 个英文字母后，你就可以访问到这样一款工具——奇安信 Alpha 威胁分析平台。汪列军说，该平台汇集了全球数百个威胁情报源和奇安信多个安全研究团队的 APT 事件发现、跟踪成果，提供基于情报及时、精准发现关键威胁的能力。

回到文章开头那个 APT 攻击的案例。在提取到钓鱼域名之后，分析师们很快在 Alpha 威胁分析平台上查到了它的 whois 信息，管理员邮箱一目了然，并且其相关域名有 10 个。

让分析师们惊喜的是，在所有相关的域名中，除了已知的恶意域名，还发现了一个新的恶意域名。

Alpha 威胁分析平台的恶意域名标签显示，这些已知域名来自毒云藤组织。

……

经过一系列的关联分析，所有的细节一目了然。

有趣的是，当分析师将此次攻击者投递的木马，与之前追踪的毒云藤组织的恶意软件的代码对比后发现，二者出奇的一致，钓鱼页面也大致相同，能看出来是同一个团伙开发的。

“你知道吗？用这 12 个英文字母，我们已经围观了超过 46 个 APT 团伙的各种活动姿势，其中 13 个是我们首先发现并围观的，并且持续发布了超过 90 篇 APT 组织的跟踪报告。”汪列军说。安

“境外不例外，网络安全从严”

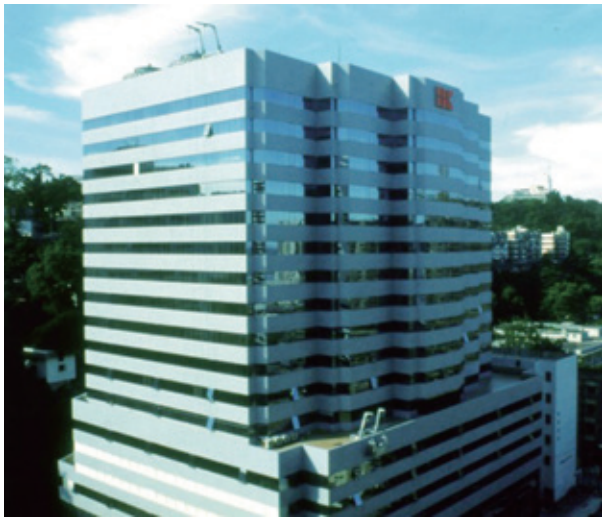
——南光集团跨境云地一体化安全实践入选世界互联网大会优秀案例

作者 公关部 张少波 安全运营 BG 张娜

在推动构建人类命运共同体思想指引下，越来越多的央企“走出去”，开拓境外市场，如何应对跨境经营带来的网络安全挑战，已经成为一道必答题。

2021 年 9 月 25 日，由 2021 年世界互联网大会乌镇峰会举办的“携手构建网络空间命运共同体最佳实践”案例集发布活动揭晓。南光（集团）有限公司（简称南光集团）作为境外央企，凭借“中央企业首个跨境云地一体化网络安全运营中心建设实践”，入选了“携手构建网络空间命运共同体优秀实践”。

“能够被国资委评为中央企业优秀案例并推荐给中央网信办，通过组委会专家组评审成为全国性的优秀案例，这是对南光集团网络安全建设的充分肯定。更重要的是，该案例模式轻、实施快，容易被复制和推广，给中国企业跨境建设网络安全和开展国际交流合作，探索了宝贵的实践路径。”南光集团企业管理部副总经理张海军表示。



图：南光集团总部大楼

集政治使命、民生使命、贸易使命于一体的境外央企

南光（集团）有限公司是唯一一家总部设在澳门的国务院国资委直属中央企业，其前身南光贸易公司成立于 1949 年 8 月，是澳门最早的中资机构。南光集团坚持“用最好的回报社会”这一宗旨，履行历史赋予的光荣职责，完成了不同时期的历史使命，为澳门回归祖国怀抱、发展内地与澳门经贸关系、推动国家对外经贸事业、凝聚广大爱国爱澳力量、促进澳门社会繁荣稳定和落实“一国两制”在澳门的伟大实践做出了贡献。

正是由于南光集团与澳门社会民生的密不可分，其网络安全也成为集团发展的重要保障和“底线”。张海军认为，相较于其他央企，南光集团网络安全面临的挑战具体表现在三个方面：

首先是南光集团作为境外央企，外部威胁环境更复杂，法规要求更加严格。澳门地区互联网高度开放，随着“数字企业、智慧南光”战略推进，企业网络安全边界外延日益扩大，网络安全环境越发复杂多变，安全形势面临着严峻的挑战。南光集团既要遵循澳门当地的《网络安全法》，也要作为央企，遵循国内相关法律法规的要求。

其次是属于多元化经营的央企集团，业务系统更加复杂多样。涉及衣食住行的方方面面，这些业务有的在内网，有的在公网对外开放。网络结构非常复杂，缺乏清晰的内外边界，给集中防御带来很大挑战。

最后是南光集团的自身安全力量不足，疫情更增加了安全建设难度。由于南光集团地处澳门，网络安全人才短缺，安全团队多数是传统 IT 人员兼职，自身力量有限。尤其疫情期间，导致外部驻场团队不能到现场实施，

增加了不少困难。

为解决这些困难，南光集团管理层高度重视网络安全的建设，集团董事长傅建国提出了“境外不例外，网络安全从严”的总体方针。从 2019 年开始，南光集团与中国电子（CEC）、奇安信集团合作，通过构建持续安全运营体系与安全运营中心，实现对集团总部及数据中心信息内外网深度安全监测预警，提升动态防御、主动防御水平，建成央企一流的安全运营中心。

主动担当 带头打造境外等保标杆

等保合规，是很多政企机构网络安全建设的重要驱动力，甚至是强制约束。南光集团主要业务系统在澳门，在澳开展等级保护面临定级备案和监督检查两个重要环节的缺失，无法形成监管闭环管理，过去也没有企业在境外开展等级保护的先例。

南光集团遵循《网络安全法》和等保相关要求，秉承“境外不例外，网络安全从严”的总体方针，坚守安全合规底线，近年来开始积极探索境外网络安全等级保护工作，参照《网络安全等级保护条例》实施定级、整改、测评和内部备案等工作。

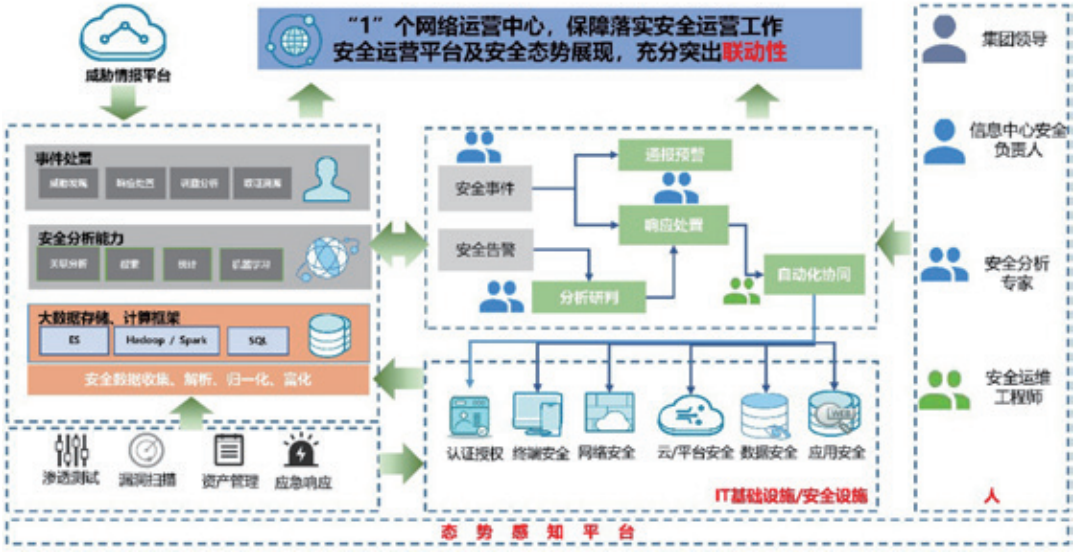
目前，南光集团已初步建立完善等保 2.0 安全防护体系，重要的核心业务系统已基本完成等保 2.0 整改工作。

“完成等保 2.0 测评不仅是为了满足合规，我们最终目的是提升集团网络安全的综合水平。”张海军为等保 2.0 测评和整改总结了三个积极意义：第一是增强了集团各层级对网络安全能力的信任，通过等保 2.0 就等于吃了“定心丸”；第二是建立了网络安全管理体系，压实了从一把手到具体岗位的各级责任；最后是提升了全集团的网络安全意识，给网络安全投入提供了保障。

更重要的是，通过等保 2.0 测评的探索实践，南光集团开创了企业在境外开展网络系统等级保护的先例，给更多“走出去”的中国企业提供了示范样板。

跨境云地一体化 解决本地安全能力短板

“聪者听于无声，明者见于未形”。习近平总书记曾指出，维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险，感知网络态势是最基础的工作。从 2018 年开始，南光集团意识到，网络安全不能局限于“事后补救”、救火式的被动防御，需要基



图：南光集团网络安全运营平台架构图

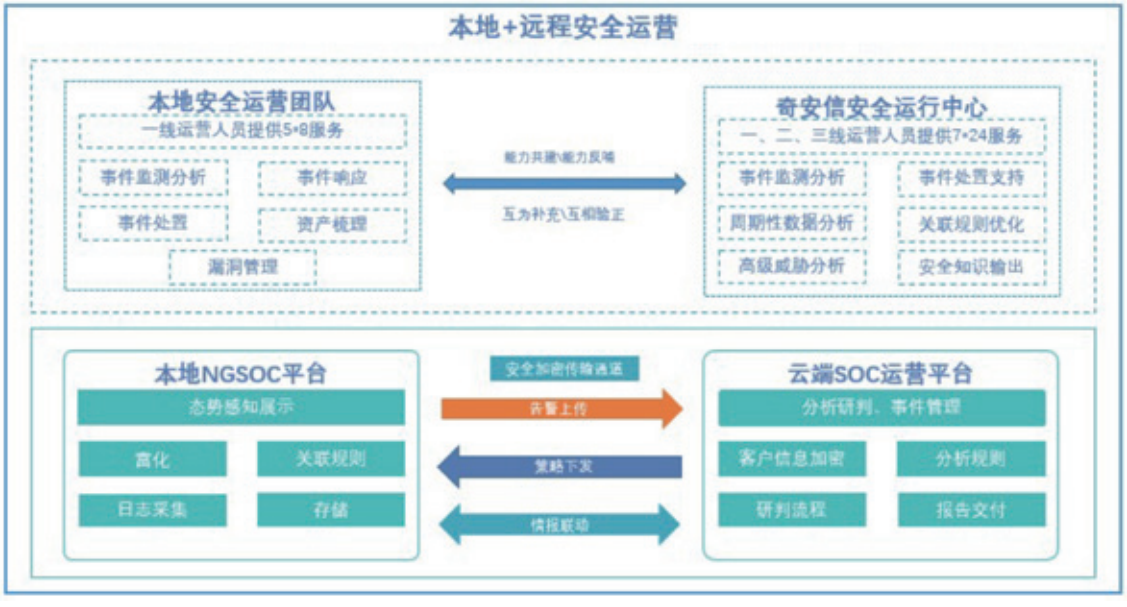
图：南光集团业务资产外连态势

于态势感知与安全运营平台，提升积极防御和情报能力。

“当时我们遇到了现实的困难，态势感知要高度依赖专业的安全运营团队，南光集团身处境外，本地人才缺乏、团队力量不足成为安全提升的最大掣肘。”张海军表示。

针对这些挑战，南光集团积极探索，通过与奇安信合作，采取能力共建、情报共享、优势互补、精准验证的跨境云地结合安全运营新模式，开创性地建成中央企业首个跨境云地一体化网络安全运营中心，实现北京主中心与澳门分中心 NGSOC 态势感知平台实时联动、常态连续运营和威胁监测可视化、场景化呈现。

目前，南光集团已经初步形成“一线驻场快速检测收缩事件影响面，二线人员快速处置处理安全事件，三线专家指导后续安全整改”的流程化处理体系，通过跨境云地一体化的无缝联动，确保安全事件“可预测、可检测、可防御、



图：南光集团“本地 + 远程安全运营”模式

强响应”，保障和促进南光集团业务的持续、稳定、安全发展。

“得益于本地+远程云地结合安全运营的理念创新，目前集团已实现‘防护—预防—监测—响应’全闭环安全运营管理，弥补了本地安全能力的欠缺，大幅度降低了安全事件对于业务的影响时间和影响程度。” 张海军谈到。

2020 年 6 月，网络安全运营中心建成投用，出色地完成了全国两会、建党一百周年期间保障任务，做到“网站不被篡改、业务不被中断、数据不丢失”，真正实现了网络安全零事故。

以攻促防 “真刀实枪”检验实战攻防能力

网络安全说一百遍，不如打一遍。如果说主动过等保是符合国家政策层面的要求，那么自发组织的攻防演习无疑是“自讨苦吃”。南光集团为了检验网络安全建设情况，连续 2 年举办全集团攻防演习。

在 2020 年 11 月，南光集团举行了实战攻防演习，主动发现了一些安全隐患，并迅速进行整改，效果显著。在今年 3 月举行的南光集团网络安全攻防实战演练中，邀请国内知名的网络安全企业攻击队，均未能攻陷标靶系统，南光集团网络安全整体防护体系在实战中经受住了考验。

“网络安全的核心在于攻防，攻防演习是‘以攻促防’的最好实践。通过两次实战攻防演习，帮我们发现了存在的技术漏洞、管理漏洞，及时弥补，从而达到完善防护体系、提高安全能力、提升应对攻击能力的目标。”

未来：三大方面发力 为“走出去”企业提供标杆示范

今年世界互联网大会的主题是“迈向数字文明新时代——携手构建网络空间命运共同体”，在“一带一路”倡议之下，将有越来越多的中国企业需要“走出去”。展望未来，南光集团将在三个方面重点发力：

首先将继续和奇安信深度合作，联手打造央企首个跨境云地一体化网络安全运营中心建设的样板工程，为“智慧南光”保驾护航。

其次，通过一系列国家级的案例申报、评优推荐，以及论坛研讨会等推广活动，为更多“出海”的央企提供可借鉴、可复制的标杆典范。

最后，南光集团将以《横琴粤澳深度合作区建设总体方案》出台为契机，加强与奇安信合作的深度和广度，优势互补形成合力，推动网络安全产业在澳门及横琴深合区的发展，为中国网安行业拓展境外市场探索新的模式与路径。

网络安全的道路上只有起点，没有终点。南光集团本次入选世界互联网大会优秀案例，不仅是智慧南光的一个新起点，更为中国企业面向海外的数字化转型和网络安全之路，揭开了新的序幕。安

图：南光 SOC 工作流程图

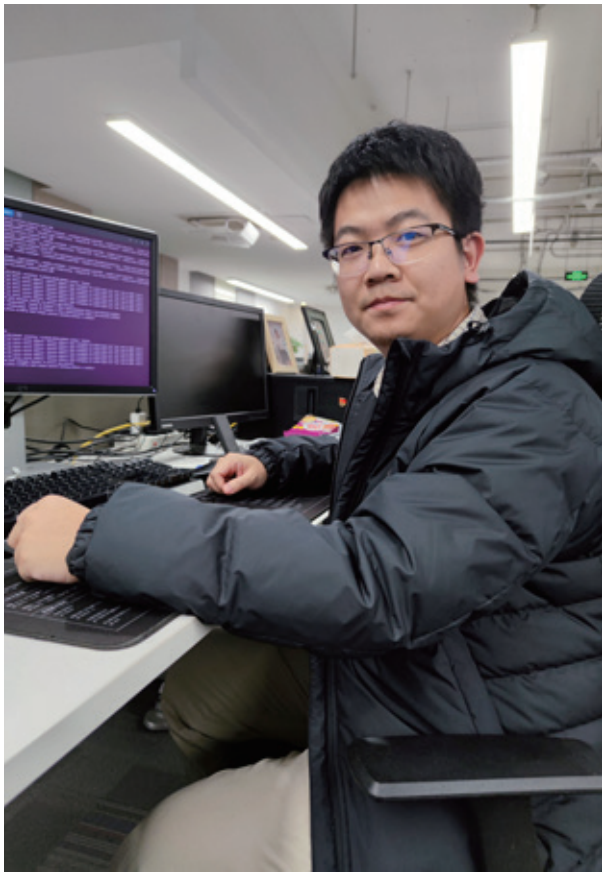
笃信而行，行必致远

——走近终端安全 BG 胡伟平

作者 公关部 庞悦宁 李恩达

“我希望奇安信做出来的终端防护软件，拿到客户那边是值得信赖的。”说话的人是胡伟平，奇安信集团终端安全 BG 的核心骨干之一。

2021年8月，国内权威咨询机构赛迪发布了《2020—2021 年中国网络信息安全市场研究年度报告》。报告显示，在终端安全细分领域，奇安信连续三年领跑，其中，信创终端安全防护市场占有率已经超过 60%。



当下，数字技术方兴未艾，信创产业迎来了一个现象级蓝海。奇安信能取得如此骄人的成绩，离不开背后强大的团队支撑。

胡伟平就是这个强大团队的核心成员之一。竖条衬衫、运动鞋是他最爱的出勤装扮，仅从外表上看，和大多数程序员没有太大差别。

2016 年，胡伟平刚从中科院软件所毕业，机缘巧合之下加入了奇安信。此后的五年时光里，他便始终与伙伴们一起，坚定地走在了维护网络空间安全这条康庄大道上。

如今，三十而立的胡伟平，已经是奇安信终端安全 BG 的一名领头雁，正带领着九人团队，继续朝着国产化终端安全防护和基础架构安全方向攻坚。

第一次对网络安全产生实感

刚进入奇安信，胡伟平一度对“网络安全”这件事没什么实感，就好像雾里看花、水中望月，让人摸不到，猜不透。

直到 2017 年 5 月 12 日，“永恒之蓝”勒索病毒大爆发。

“永恒之蓝”就好像一种终端瘟疫，安全圈里有人戏称，“给永恒之蓝一个终端，它就能攻陷全网”。“永恒之蓝”源起 NSA 黑客数字武器库，爆发后，仅用 4 天时间就横扫全球 150 多个国家，我国超 30 多万台机器中招，多所高校和关键领域的企事业单位成了“重灾区”。

“永恒之蓝”事件对整个网络安全行业，乃至我国的信息化发展历程都影响深远。当时，微软已经全面停止了对 Windows XP 操作系统的技术支持，而我国一些机构，因为还在使用 Windows XP、Windows 2003 这样老旧的操作系统，又无法及时进行更新，纷纷被波及，

损失惨重，当时就有不少人提出，操作系统等核心技术国产化已经刻不容缓。

终端安全当年还不是胡伟平的主攻方向，但是看着天擎、安服各个团队的老前辈、小伙伴为处理“永恒之蓝”这件事废寝忘食，胡伟平第一次对网络安全产生了实感。

“比起交流，我更喜欢观察。”胡伟平说道，“当时，整个天擎，包括三个跟我关系特别好的兄弟，因为‘永恒之蓝’这件事情，不眠不休，连续奋战了 30 多个小时。这件事情给我触动非常大。” 在胡伟平的回忆中，每一个对抗“永恒之蓝”的同事们，都是凭借着对网络安全极高的责任感和使命感在战斗。

在“永恒之蓝”这场战役里，奇安信先后派出安全应急响应人员超 2000 人，为 1700 多家政企机构提供了现场支持，制作了 5000 多个工具 U 盘和光盘，并且成功编写出漏洞一键修复工具，成为了第一个解决该漏洞的厂商。

在工具改进期间，还撞上了 5 月 20 号这个好日子（谐音我爱你）。这天，一位同事专门趁着午休时间，和女朋友去民政局领了结婚证。

“这件事给我的感受是，整个网络安全行业或多或少需要你贡献一份力量。为了更好的网络安全环境，个人做出一点让步和牺牲是值得的。现在回头看，同事们身体力行，让我知道了优秀的网安人是什么样子，也给我树立了成长的目标。”

至此，胡伟平切切实实地成为了一名网络安全的守护者。

风起于青萍之末，浪成于微澜之间。新兵胡伟平很幸运，刚进公司就遇到了不吝赐教的前辈。当时组里有工作经验的同事经常给他讲解业务细节，帮他 debug、review 代码。胡伟平也抓住每一个成长机会，苦心钻研技术、增强业务实力。

回看来路，胡伟平感叹，“他们把我带到这个行业里，给我指明了前进的方向。”

在“战斗小队”中破茧成蝶

在胡伟平日复一日的努力中，他成功从一名新兵变成了为别人传道、授业、解惑的那个人。他拥有了一个属于自己的小团队，开始了破茧成蝶的蜕变。

擒龙要下海，打虎要上山。想在成长的道路上夺取

甜美果实，就一定要迎难而上，经历千锤百炼。“当时，公司有个大项目出了状况，客户很着急。这个项目特别重要，整体情况比较复杂，非常棘手。”回想起当年的场景，胡伟平还依稀能感受到那种紧迫感。

胡伟平口中的这个项目，对当时的他而言的确是个不小的挑战。这个项目除了奇安信，还有国内外几家主流的安全厂商参与，客户会定期给各个厂商的产品进行排名，如果这个项目做不好，对奇安信品牌的影响很大。

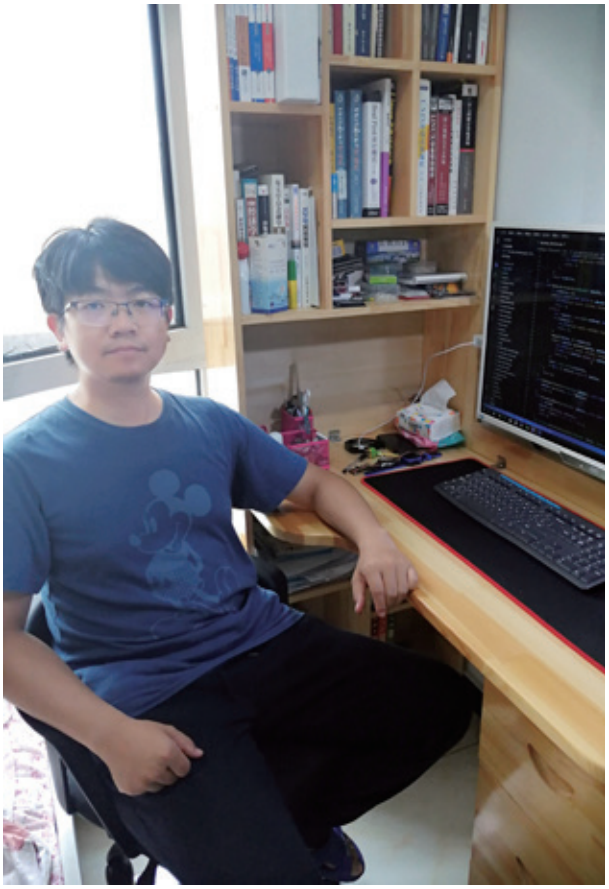
距离春节大概还有两个星期，胡伟平团队接到了有关项目问题的报告。当时，奇安信部署在客户现场的服务器，每天都要处理海量数据，有时数据流量陡增甚至会过亿。这种情况下，产品检测速度就会变慢，不时出现数据堆积、检出率低的问题，影响客户正常开展工作，产品的日常排名也很低。

“客户要求我们尽快拿出一个技术解决方案，一是修复已有的问题，二是产品参数要达到客户要求的指标。”胡伟平说，“当时那个情况，要想彻底解决客户面临的问题，维护住品牌声誉，只有一个解决办法，那就是对产品进行大改。”

面对突如其来的需求，刚成为团队负责人的胡伟平是紧张的、更是兴奋的。回想当年的心路历程，胡伟平由衷地发出了感叹，“那是我第一年带团队，也是刚开始做终端安全防护这个方向，非常渴望做出一些成绩来。”

当时团队人手紧张，胡伟平和他的领导李常坤，还有一位负责项目管理的同事，紧急组建了一个临时的产品改进小组。胡伟平主要负责编码性工作，李常坤负责流程上的沟通和处理，项目管理的同事负责进行客户对接、环境提供，三个人分工明确，各司其职，是一个高效精简的“战斗小队”。

接到客户需求的那一刻，“战斗小队”开始快马加鞭地进行问题排查和产品改进。大年三十的晚上，胡伟平还钻在电脑里解决项目问题，指尖流淌出一串串代码，眼前如黑夜般宽阔的屏幕上，弹出一行行绿色的荧光。耳边从家人的欢声笑语变换成群星合唱的难忘今宵，热



闹逐渐散去，万籁俱静里胡伟平一写就是一整夜。

整个春节，“战斗小队”都一直在处理产品改进的事情。即使陪着家里人走亲访友，胡伟平也随身带着电脑，蓝信上随时待命。春节假期一共有七天，这三个人就足足干了七天。

春节过后，通过加班加点的忙碌，硬是在短时间内把客户需求赶了出来。产品出炉后，胡伟平和李常坤就马不停蹄地跑到客户现场，部署产品、完成后续测试。对于开发人员来说，这是最紧张的时刻，成败在此一举。

“单纯算做版本，到版本发布、测试，大概有6到

7 周的时间。”胡伟平说，“当我们把打磨出来的产品部署到客户现场，所有的参数和指标都达到客户要求的时候，我感觉心里紧绷着的一根弦稍微放松些了。”在后续的排名中，奇安信部署在客户现场的产品一直名列前茅。

现在的胡伟平相比过去已经成长了很多，回想起那段时光，他的语气里满是坚定和感恩，“我挺感谢那段经历的，感觉自己一下子成长了。”

从项目角度来看，主要承担产品开发任务的胡伟平，只是当中的一环。这个项目情况复杂，流程要比普通项目更长，除了需求对接、产品部署、产品交付，后续还有很冗长的文档建设工作。

要把这种量级的项目做到完美，把奇安信“客户优先”这条价值观落地，需要每一个环节都进行长期、密切的配合。这是无数像胡伟平这样的奇安信人相互协作，共同取得的硕果。

带领团队继续“驰骋疆场”

对于任何人而言，能找到志同道合的人，一起为了感兴趣的事情而努力，都是一种很棒的体验。

学生时代，在学业科研压力颇重的中科院，胡伟平在课余时间最爱做的事情就是动手鼓捣些交互式设备。这样被技术环绕的生活，让胡伟平乐在其中。

“加入奇安信，很大一部分原因是被那种工作氛围吸引到了。”胡伟平说，“我当时的面试体验特别好，整个过程都很愉快。” 尽管当初在新人训练营结交到的伙伴们很多都已经选择了离开，但是，当年面试胡伟平的领导、老同事们都还坚守在自己的岗位上，朝着“让网络更安全，让世界更美好”的目标努力着。

这样一个气氛绝佳、能力卓越的团队，给胡伟平创造了一个宛若象牙塔的单纯氛围。他持续在技术的田野里深耕，成长为一名技术过硬、目标纯粹的一线干部。

做管理对胡伟平而言是个新挑战，但他并不畏惧，反而得心应手。他高度认同奇安信“成就事业成就人”的这条人才培养理念，也决心将这条准则贯彻到底。

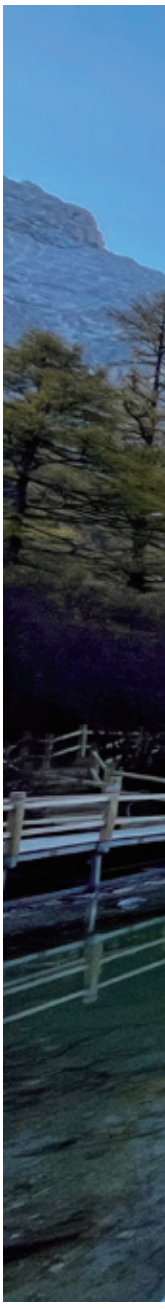
“在管理上，我有自己的原则和底线，这个基础之上，我会相对灵活一些。”胡伟平说。他鼓励团队成员们去做自己感兴趣的事情，在完成业务指标的基础之上，团队成员们会得到比较多的自由度，去做自己的个人学习成长计划、去学自己喜欢的技术。

管理的底线是什么？胡伟平给出了自己的答案，“我希望客户看到奇安信的产品就觉得安心、满意。”这是胡伟平对待产品研发的基本态度，也是他在日常管理中的一个底线。

今年，信创产业已经走到了爆发前夜。谈到未来的目标，胡伟平说，“网络安全现在正处于黄金发展期，竞争非常激烈，尤其是信创这个领域，大家都在抢市场。如果你错过了这几年的窗口，那后面会比别人落后很多。”

现在，他正带领自己一手培养起来的团队，在信创终端安全防护的道路上驰骋，主要集中力量做国产操作系统的主动防御和漏洞补丁的相关业务。接下来的几年，胡伟平都将专注于信创终端安全防护这个领域，把产品做精、做好。

每一个产品都是研发人的心血。作为奇安信信创终端安全领域的核心骨干，胡伟平希望团队研发的产品能走向更大的市场，为维护网络空间安全创造更大价值。“自己用心做出来的产品，用的人越多、采购的人越多，就是对我们工作的最大肯定。”胡伟平说。安



我穿过所有浪漫银河，所有城市烟火，只为在你心头降落。

——《你的轮廓》

奇安信集团市场部黄慧玲

10 月 27 日在甘孜州折多山、稻城亚丁拍摄

大事记

吴云坤出席 2021 中国 5G+ 工业互联网大会

11 月 20 日，2021 中国 5G+ 工业互联网大会在武汉召开，奇安信集团总裁吴云坤发表主题为“经营安全，助力工业互联网安全发展”的演讲。

他表示，工业互联网加速工业企业智能化升级的同时，面临三大新挑战，需要建立内生安全、保障经营安全，确保工业互联网安全发展。应以网络安全建设三部曲保障工业互联网发展：以内生安全为理念、内生安全框架为方法、经营安全来进行动态掌控为三部曲，建立起“一中心两体系”——零信任体系、安全防护体系与态势感知与管控中心。

奇安信与中电光谷达成战略合作 共同打造安全智慧园区

11 月 20 日，奇安信与中电光谷联合控股有限公司签署战略合作协议，共同打造安全智慧园区。双方将成立专门工作小组，在数字基建、政企信息化、技术研讨交流等方面展开深度合作，同时布局全国与地方市场，共同服务客户。

合作后，双方将为千家入驻企业搭建整体安全能力平台，建设园区安全运营中心，在全国率先打造园区安全一体化服务模式，保障数千家企业网络安全。其次，在园区建设实战平台，开展网安产业培训。此外，园区将为奇安信各地分公司、投资企业及生态企业提供优惠入驻政策。

推动工程教育改革创新 奇安信与武大网安学院达成战略合作

11 月 20 日，奇安信与武汉大学国家网络安全学院签署战略合作协议，双方将重点在实验室创建、课程研发、实验实训、重大网络安全相关项目申报等方面展开务实合作，探索新工科建设模式。

武汉大学国家网络安全学院是武汉大学在 2016 年为响应国家网络空间安全战略部署成立。2017 年 9 月，学院获批国家一流网络安全学院建设示范项目，成为中国网络安全高层次人才培养的“国家示范”。

奇安信椒图全新版本正式发布

11 月 19 日，奇安信正式发布了椒图新一代服务器安全产品。新版本椒图不仅实现了“资产 - 漏洞 - 实体 / 虚拟补丁”的闭环管理，还与 DevOps 深度融合，让安全赋能 Dev 开发阶段与 Ops 运营阶段，推动“业务的安全”向“安全的业务”转变，并且新增多维度威胁检测指标与实战化安全基线，紧密贴合服务器的安全需求，打造面向攻防实战场景的新一代服务器安全产品。

《中国网络安全企业 100 强》发布 奇安信位居第一

11 月 9 日，国内网络安全媒体安全牛发布第九版《中国网络安全企业 100 强》，从经营、用户、产业、行业贡献四大维度 27 个细分项，对网络安全企业进行综合考评。在申报的近 500 余家安全厂商中，奇安信在中国网络安全 100 强企业榜单上独占鳌头，并在技术创新、用户认可、行业贡献三个细分维度均位列第一，充分彰显了网络安全龙头企业的综合发展实力。

报告根据营收占比、用户数量、产品成熟度等，共细分为十个领域，奇安信共计上榜六个细分领域，包括基础安全防护、业务与应用安全、安全服务与运营三个收入最高的细分领域，收入增长最快的云安全领域，以及移动安全和工控安全领域。

排名	企业名称	企业经营（35%）	技术创新（30%）	用户认可（25%）	行业贡献（10%）	总分
1	奇安信	29.00	29.20	24.50	9.50	92.20
2	天融信	30.50	28.10	24.00	8.00	90.60
3	华为	31.50	28.50	22.35	8.00	90.35
4	深信服	30.00	28.20	23.00	8.00	89.20
5	新华三	31.00	27.50	22.15	8.00	88.65
6	绿盟科技	30.50	28.30	21.30	8.50	88.60
7	安恒信息	29.40	27.20	21.30	7.50	85.40
8	阿里云	29.90	28.50	18.00	8.50	84.90
9	启明星辰	30.50	26.40	20.15	7.50	84.55
10	亚信安全	24.60	27.10	22.90	7.50	82.10

5885 万元！奇安星城中标长沙市城市网络安全运营项目

作为长沙市政府与奇安信集团战略合作下成立的唯一合资公司，奇安星城近日成功中标长沙市城市网络安全运营（一期）项目，中标金额为 5885 万元，内容主要包括面向市委网信办的城市网络安全监测预警与指挥调度部分和面向市大数据中心的政务网络安全运营部分。该项目有望为筑牢城市网络安全底座、搭建智慧城市全脉络，提供高质量可复制的落地模板。

北京市通信管理局局长苏少林一行赴奇安信进行调研

11 月 4 日，北京市通信管理局局长苏少林、副局长王晖及相关部门负责人到奇安信集团进行调研，参观了奇安信集团展厅及司法鉴定中心，并进行座谈交流。

奇安信相关业务骨干在此次交流会上分享了在冬奥重保、反诈能力、隐私业务能力、工业互联网安全能力与实践等方面的经验，与会人员就相关内容进行了交流讨论。

苏少林对奇安信长期以来在国家各个重大保障活动中贡献的力量表示充分肯定，对奇安信“内生安全”三部曲理念表示高度认可。他表示，下一步双方将继续深化合作。2022 北京冬奥会即将召开，当务之急是全力以赴地共同做好冬奥的网络安全保障工作。苏少林希望，将来也要加强在反诈、工业互联网安全等领域的合作。

与乐信达成战略合作 携手保障金融科技行业数据供应链安全

11 月 2 日，奇安信与深圳乐信软件技术有限公司签署战略合作协议。双方将在金融科技行业数据供应链安全治理领域展开深度合作，共同服务客户。

作为网络安全行业龙头企业，奇安信此次与国内领先的新消费数字科技服务商乐信的深度合作，旨在通过乐信在金融科技领域的积累与奇安信的安全能力进行融合，充分发挥双方优势，打造出符合金融科技行业和客户需求的数据供应链安全治理的解决方案，共同推进金融科技行业安全发展。

奇安信与金杜律师事务所在数据合规领域达成战略合作

《个人信息保护法》正式实施同一天，金杜律师事务所与奇安信宣布达成战略合作，双方将充分发挥各自在企业安全防护技术实践与政策法律解读和法律合规方面的优势，共同探索法律专业领域与信息技术的深度融合和创新应用。

本次与金杜的深度合作，将会在隐私合规、数据处理、数据共享、数据跨境传输等数据合规场景方面得到更有力的法律专业支持，通过风险评估和筛查服务、提供整改建议和方案、协助建立网络安全和数据合规体系建设三个方面，为企业的数字化转型提供坚实底板。

赣南科技学院与奇安信集团达成战略合作 联合培养高水平网络空间安全人才

10 月 26 日，奇安信与赣南科技学院宣布达成战略合作。双方将共同组建产业学院发展规划委员会，在网

络安全人才培养和共建网络安全现代产业学院两个方面进行紧密合作，联合培养高水平的网络空间安全人才，并以现代产业学院建设为契机，探索具有创新性、领先性的校政企联合人才培养模式，引领江西省网络空间安全相关专业的建设与发展，助力地方网络安全产业和数字经济发展。

此前，奇安信集团已与赣州市人民政府签署战略合作协议。此次与赣南科技学院（赣州市唯一一所市属本科）的合作充分延伸了与政府的战略合作内容，采用政、校、企共建的方式，共同打造赣州市“国家网络安全教育基地”。

独家捕获在野完整 Chrome 浏览器漏洞利用攻击链

近日，奇安信威胁情报中心旗下红雨滴团队基于红雨滴云沙箱和蜜罐系统，在全球范围内独家监测到多例组合使用 Chrome 浏览器和 Windows 内核提权漏洞的定向攻击。据悉，本次攻击能够穿透 Chrome 浏览器沙盒，同时获取 Windows 系统内核权限，从而实现远程执行任意代码，对用户危害极大。

奇安信首次捕获到在野的完整漏洞利用攻击链，实现了基于威胁情报和流量分析的在野 Chrome 浏览器漏洞攻击检测的突破。

1835 万！奇安信中标国家级工业互联网安全项目

日前，国家工业信息安全发展研究中心工业自动化设备风险隐患分析验证能力建设项目中标公告对外公示，奇安信旗下网神公司中标工业自动化设备风险隐患分析验证能力建设项目，嵌入式操作系统缺陷检测定制化系统开发。根据公告内容，本次中标金额达到 1835 万，凸显了奇安信在工业互联网领域的强势布局和技术创新优势。

NEED 北京学习小组第一场学习活动在奇安信安全中心召开

10 月 22 日，NEED 班（新时代民营企业家培养计划）北京学习小组第一场学习活动暨启动仪式在奇安信安全中心召开。中央统战部四局有关负责人和 20 余位 NEED 学员出席活动。学习活动特邀工信部财务司有关负责人授课。NEED 班成员、奇安信集团董事长齐向东主持并致欢迎词。

齐向东表示，奇安信是 NEED 班的受益者，也是国家推动科技创新的受益者。2020 年，奇安信融资 57 亿并成功登陆科创板，并在一年内入选上交所科创 50 指数，充分体现了资本市场、证券市场对国家科创战略的支持。

荣誉墙

盘古石 5 支队伍齐获第七届中国电子数据取证大赛一等奖

在“美亚杯”第七届中国电子数据取证大赛暨网络安全执法新技术研讨会上，奇安信盘古石取证团队派出的 5 支队伍全部荣获团队一等奖，同时获得个人一等奖 11 人，二等奖 3 人，三等奖 1 人。其中，有 3 人以个人赛前十的成绩分别荣获大赛奖金 3000 元。

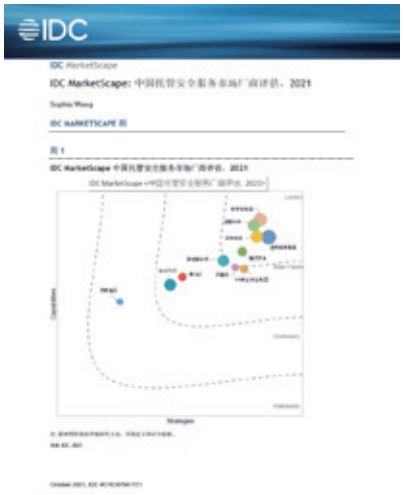
本次比赛汇集了来自国内高校、电子数据取证领域相关单位、企业组成的近 751 支队伍共同参赛、近 2020 余名选手参与本次比拼。在赛题方面，资格赛、团体赛题量、检材数均为历届之最，除了传统的介质、服务器等检材，同时还加入了无人机、物联网、矿机等结合当下新型涉网犯罪热点的创新性检材。

国家级网络安全赛事夺魁！奇安信虎符战队获工业互联网安全大赛一等奖

在重庆举办的 2021 年中国工业互联网安全大赛总决赛上，奇安信安服虎符战队从百余支战队中脱颖而出，在这一国家级网络安全赛事上摘得桂冠。

作为由中央网信办正式批复同意冠名的国家级网络安全赛事，在工业互联网安全大赛中取得的优异成绩，也证实了奇安信在安全服务、特别是工业互联网安全建设方面的能力过硬。

入围领导者象限！奇安信安全托管服务实力领跑国内市场

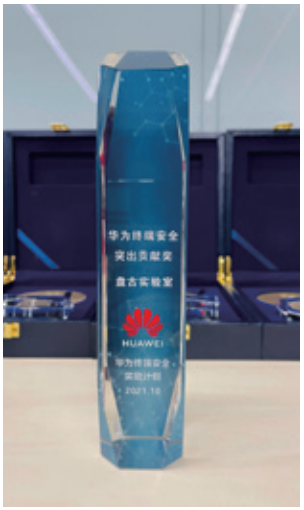


近日，IDC 正式发布《IDC MarketScape 中国托管安全服务市场厂商评估，2021》报告，深度研究国内托管安全服务市场，清晰地展现了中国托管安全服务提供商的综合实力。其中，奇安信凭借全新升级的 MSS 安全托管服务跃居 IDC MarketScape 模型领导者象限。

此前，IDC《全球网络安全支出指南，2021V1》报告显示，2020 年，全球托管安全服务以其超过 20% 的市场占有率（托管安全服务占全球网络安全市场）成为了网络安全市场中最大的子市场。作为综合型网络安全厂商，奇安信在 2021 年中国托管安全服务市场厂商评估中处于领导者位置。

连续两年获得突出贡献奖！奇安盘古获华为致谢

在华为安全应急响应中心发布的 2020 年华为终端安全奖励计划榜单中，凭借在过去一年为华为终端在漏洞挖掘和安全应急等方面做出的贡献，奇安盘古旗下盘古实验室，独家获得 2020 年“华为终端安全突出贡献奖”，同时获得 2020 年“华为终端安全杰出生态伙伴”。



这也是继获得 2019 年“华为终端安全突出贡献奖”之后，连续两年获此殊荣。

值得关注的是，除上述两大团体奖项，盘古实验室两名白帽黑客 slipper 和闻观行还获得了华为终端安全奖励计划二等奖。

首个打印机项目挑战即夺冠 奇安信天工实验室获 GeekPwn 2021 大赛冠军

2021 年，GeekPwn 以“让智能更安全、让安全更智能”为主题，并以线上真人秀《我是极客》和线下盛典“极棒之夜”的方式呈现。奇安信天工实验室战队凭借“卧底”打印机项目，成功以 6.02 的高分位居“G-TOP 年度极客榜”榜首，直通 10 月 24 日的极棒之夜，并最终获得年度冠军。

GeekPwn 发起创办人、评委大牛蛙表示，这是 GeekPwn 举办 8 年以来的第一个打印机项目，也是大赛方一直希望在赛场上看到的。

奇安信斩获“强网杯”人工智能挑战赛第一名

第五届“强网杯”全国网络安全挑战赛上，来自奇安信人工智能研究院的参赛队，在人工智能挑战赛“口令密码智能破解”科目中表现优异，一路过关斩将，最终以总分第一名的成绩斩获大赛一等奖。

本次大赛从 7 月开始，分为开放测试和现场验证两个阶段，主要通过参赛队模型生成的 1 亿规模口令字典，和测试集进行碰撞测试，以碰撞成功率作为该队测试得分，从而进行赛队排名。包括奇安信、国防科技大学、北京大学、中科院软件所，以及多家网络安全公司均派队参赛，经过数个月的角逐，奇安信代表队从众多强队中脱颖而出，摘取桂冠。

奇安信

新一代网络安全领军者

聚焦安全运营，构建智能平台

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

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

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

将平战结合进行落地

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

重大安全事件的威胁预警

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

专业的安全运营服务

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

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一——数世咨询认证

奇安信

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






网络安全科普系列




网络安全实战系列



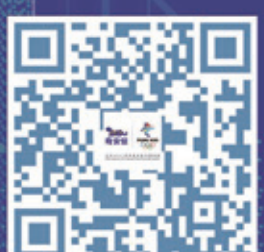
国际经验分享系列




网络安全认证系列




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。

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。


奇安信科技集团股份有限公司

CCIA 50强

2021年中国网安产业竞争力50强

编号：CCIA-2021JZL-01

中国网络安全产业联盟

2021年6月

“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