SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

网络安全八大关键词

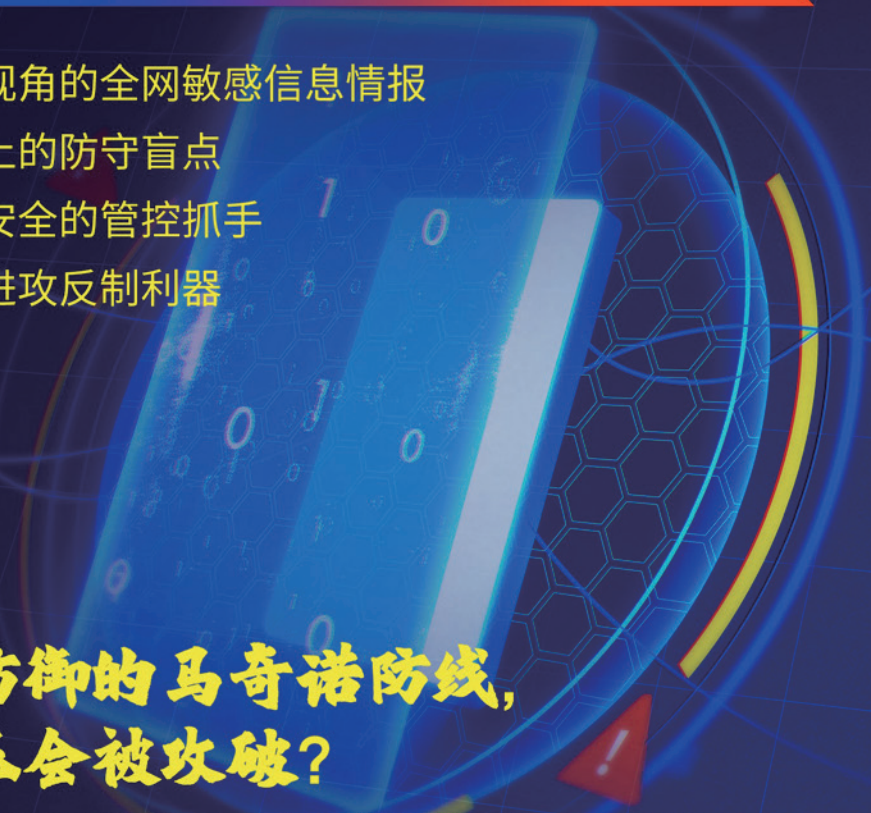
P16

第13期
2022 年 1 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

开启 2022 年的钥匙，还是猴子扔出的飞镖

岁末年初，又到回顾展望的时节。

网络安全行业的一大特色是特别重视总结与展望。每家安全公司都要根据自身的业务特点，以及传播需要，总结出未来一年的安全趋势：2022 年十大数据安全趋势、2022 年十大物联网安全趋势……

诺贝尔经济学奖获得者、美国普林斯顿大学教授，丹尼尔·卡尼曼在其《思考，快与慢》一书中认为，未来是不可预测的。“各类专家预测的准确度还比不上扔飞镖的猴子。”

但我们实在难得抗拒预测的乐趣，依然不能免俗地呈现给大家 2022 网络安全关键词。

基于对 2021 年的分析与观察，我们认为未来一年，八个安全热点将主导安全建设趋势与方向：新合规、信创安全、安全左移、数据安全治理、隐私保护、漏洞管理、安全网格、托管安全服务。

这其中包括政策与产业纬度的新合规与信创安全。在过去的 2021 年，我们经历了前所未有的网络安全法律法规密集出台；发生了《网络安全审查办法》发布以来的首次审查行动。在配套规范逐步细化的 2022 年，企业用户将无疑会面临更加明确的合规需求。

在热门的数据安全治理与隐私保护领域，期待相关的安全技术与方案逐步体系化和成熟。此外，“基础不牢，地动山摇”，安全左移与漏洞管理等安全基础工作将会受到更多重视。

在安全能力不足、人员匮乏，安全合格压力倍增的背景下，托管安全服务可能是更多政企用户的最现实选择。

这些预测是开启 2022 年的钥匙，亦或是猴子扔出的飞镖？且留待明年这个时候再来评估吧。

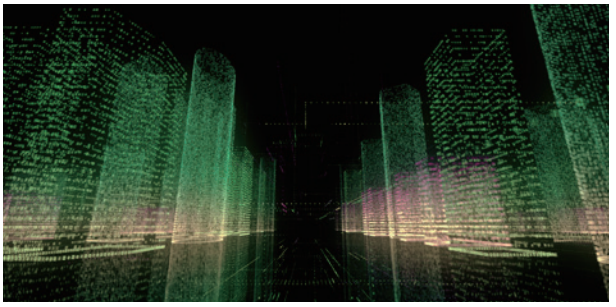
总编辑

李建平

2022 年 1 月 1 日

CONTEN

目录



安全态势

月度专题

网络安全八个关键词 P16

未来一年，八个安全热点将主导安全建设趋势与方向：新合规、信创安全、安全左移 、数据安全治理、隐私保护、漏洞管理、 安全网格、托管安全服务。

TS

攻防一线

P28

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

安全之道

P34

十年“四级跳”中国电建如何打造网络安全的“眼手脑”

奇安信人

P38

万物之中，理想至美

奇安资讯

第 13 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

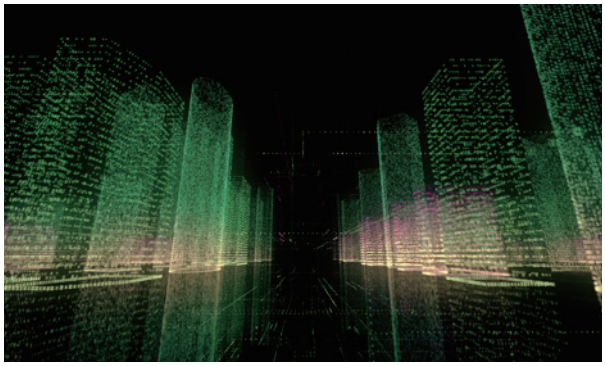
奇安信集团　虎符智库　安全内参

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

近日，公安部公布了打击侵犯公民个人信息犯罪十大典型案例，其中何某非法获取公民个人信息 54 亿条并通过暗网出售；国外多名政要高官被曝出遭遇非法入侵个人信息，包括 NASA 局长、波兰公民平台党领导人等。



公安部公布打击侵犯公民个人信息犯罪十大典型案例

2022 年 1 月 9 日，公安部公布了 2021 年侵犯公民个人信息犯罪打击破获情况。全国公安机关全年共破获侵犯公民个人信息案件 9800 余起，抓获犯罪嫌疑人 1.7 万名。侵犯公民个人信息犯罪十大典型案例，包括何某非法获取医疗、出行、快递等公民个人信息 54 亿条并通过暗网出售，徐某等人利用外挂程序非法获取公民个人信息 3000 余万条用于债务催收，以及吴某等人非法获取老年人个人信息 200 余万条推销虚假保健品骗取资金 1500 余万元等案件。

美医疗中心 Broward Health 披露数据泄露：影响超 130 万人

据 cnBeta 2022 年 1 月 4 日消息，美国 Broward Health 公共卫生系统披露了一起大规模数据泄露事件。Broward Health 是一个位于佛罗里达州的医疗系统，其在 2021 年 10 月 19 日发现了这次入侵事件，并立即通知了美国联邦调查局和美国司法部。调查显示，入侵网站的黑客获得了病人的个人医疗信息，其中可能包括全名、出生日期、实际地址、电子邮件地址等关键信息，影响到 1357879 人。

英国国防学院遭遇网络攻击并引发了“重大”影响

据天空新闻 2022 年 1 月 3 日消息，现已退休的英国空军元帅爱德华表示，发生于 2021 年 3 月对英国国防学院的“复杂”黑客攻击产生了深刻影响。英国国防部的数字部门对网络攻击展开了调查，但结果尚未公开。当时的负责官员透露，一场网络攻击——可能是俄罗斯——攻击了英国国防部的学术部门，并产生了“重大”影响。

美国宇航局局长社交账户被希腊一黑客组织入侵

据 E 安全 2022 年 1 月 2 日消息，美国宇航局局长的 Twitter 帐户于 1 月 2 日被希腊一黑客组织——“希腊陆军集团”入侵。该组织发言人告知这次袭击不是出于政治动机，是为了好玩，以证明“没有人在网上是安全的”，并且声称有一个漏洞可以让他们接管 Twitter 帐

户，但至今无法验证。该组织的受害者名单包括尼日利亚外交部和财政部、尼日利亚银行、北马其顿国家银行和阿塞拜疆国防部等。

波兰政府被指使用 Pegasus 入侵反对派团体成员设备

据 Politico 2021 年 12 月 24 日消息，波兰数个政治反对派团体成员拿出了被间谍软件 Pegasus 入侵的证据，其中公民平台党领导人的手机在 2019 年大选前的六个月里总共被入侵 33 次。波兰政府否认使用了间谍软件，波兰国防部副部长表示：“Pegasus 系统不是由波兰部门使用的。它没有被用来跟踪或调查我们国家的任何人。”据了解，这一丑闻可能对波兰在欧盟的地位产生重大影响，并为进一步限制 Pegasus 建立了理由。

超 22% 的阿尔巴尼亚公民个人和工资信息遭泄露

据 Therecord 2021 年 12 月 23 日消息，阿尔巴尼亚政府证实并致歉称，637138 名公民（在总人口中占比超过 22%）的个人信息和工资信息遭泄露。被泄露的详情包括姓名、身份证卡号、工资、工作职责和工作单位，以及企业向阿尔巴尼亚政府上报的 2021 年 1 月的税务和工资信息。“初步分析显示，事件是由内部渗透而非外部网络攻击造成的。”政府发言人指出。目前地拉那检察院正在调查此事。

阿里云被暂停工信部网络安全威胁信息共享平台合作单位

据观察者网 2021 年 12 月 22 日消息，工信部网络安全管理局通报称，阿里云计算有限公司发现阿帕奇（Apache）Log4j2 组件严重安全漏洞隐患后，未及时向电信主管部门报告，未有效支撑工信部开展网络安全威胁和漏洞管理。通报指出，阿里云是工信部网络安全威胁信息共享平台合作单位。经研究，工信部网络安全管理局决定暂停阿里云作为上述合作单位 6 个月。暂停期满后，根据阿里云整改情况，研究恢复其上述合作单位。

四家运动装备网站遭受攻击，180 万客户信用卡数据被盗

据 Security Affairs 2021 年 12 月 18 日消息，四家在线运动装备网站遭受网络袭击，有超过 180 多万客户信用卡数据被盗。安全漏洞最早出现在 2021 年 10 月 1 日，但是在 10 月 15 日才被发现，11 月 29 日网站确认了其客户个人和财务数据被盗，主要包括：姓名、金融账户号码、信用卡号码（含 CVV）、借记卡号码（含 CVV）、网站账户密码。12 月 16 日，四家网站通知了受影响客户。截至目前，这些网站还没有披露出现安全漏洞的具体原因。

物流巨头遭遇勒索攻击后，攻击组织发布 70G 被盗数据并支持个人下载

据 BleepingComputer 2021 年 12 月 17 日消息，国际物流公司 Hellmann Worldwide 于 2021 年 12 月 9 日遭遇勒索软件攻击，并被迫关闭了系统。公司已公开承认数据遭窃的事实，但哪些数据被盗仍在调查中。研究人员发现一个名叫 RansomEXX 的攻击组织在其门户网站上发布了被盗数据信息，共计 70.64GB，包括文件、凭据、通信号码、协议和订单等。这些数据支持个人下载，导致了大量 BEC 相关攻击的增加。

漏洞篇

2021年12月29日，Apache Apisix曝出授权问题漏洞，远程攻击者可通过访问特定API绕过权限控制，造成未授权访问。目前，Apache官方已发布可更新版本，建议尽快自查并修复。

CNNVD关于Apache Apisix授权问题漏洞的预警

2021年12月29日，国家信息安全漏洞库（CNNVD）收到关于Apache Apisix授权问题漏洞（CNNVD-202112-2629、CVE-2021-45232）情况的报送。成功利用漏洞的攻击者，可以在未经授权的情况下获取或更改设备的配置信息，进而构造恶意数据对目标设备进行攻击。Apache APISIX Dashboard 2.10及其之前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 Log4j远程代码执行漏洞安全风险通告

2021年12月29日，奇安信CERT监测到Apache官方发布了Apache Log4j远程代码执行漏洞（CVE-2021-44832），在某些特殊场景下（如系统采用动态加载远程配置文件的场景等），有权修改日志配置文件的攻击者可以构建恶意配置，成功利用此漏洞可以实现远程代码执行。目前官方已有安全版本，鉴于Log4j在全球范围内部署量较大，建议用户使用处置建议中的缓解措施或升级到最新版本。

MinIO权限提升漏洞安全风险通告

2021年12月28日，奇安信CERT监测到MinIO官方发布CVE-2021-43858MinIO权限提升漏洞安全通告。拥有MinIO普通用户账户权限的攻击者可通过构造恶意数据包调用AddUser()API，从而更新用户的Policy获得更高的权限。目前，MinIO官方已发布可更新版本，建议客户尽快自查并修复。

Apache Log4j拒绝服务漏洞安全风险通告

2021年12月19日，奇安信CERT监测到Apache官方发布了Apache Log4j拒绝服务攻击漏洞（CVE-2021-45105），此漏洞需要在非默认配置下才能触发。攻击成功利用此漏洞将触发无限循环，导致系统崩溃。目前官方已有安全版本，鉴于Log4j在全球范围内部署量较大，建议用户使用处置建议中的缓解措施或升级到最新版本。

对抗篇

国内攻防演习 12 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 12 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，地市级攻防演习 3 场，本单位自主攻防演习 17 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分散，包括金融、政务、医疗、交通、教育等目标。客户存在的安全风险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疏于防范、内网功能区域缺乏安全隔离、弱口令及口令复用等。具体情况如下：

1、历史漏洞依然是主要突破口

本月任务中发现大部分目标被攻陷的原因在于互联网侧应用存在漏洞，且可被利用进行突破渗透。突破利用的漏洞以应用历史漏洞为主，其出现原因多为外部应用或系统组件未及时更新。外部应用中 Shiro 组件漏

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	23	51	97	101	38	218	302	511

洞、Weblogic 反序列化漏洞、log4j2 远程命令执行漏洞等历史漏洞的存在是客户目标网络的重大安全威胁。

2、弱口令和口令复用是内网安全的严重风险

本月任务中发现目标网络内网弱口令和口令复用情况比较突出，其作为内网横向拓展的主要实现手段之一，为攻击者实现内网的拓展控制带来极大便利。其中，内网安全设备、堡垒机、网管系统和域控等存在弱口令和口令复用的情况，致使业务内网随时面临被攻陷的安全风险。

3、钓鱼攻击是具有较高成功率的突破辅助手段

本月任务中，针对特殊行业目标网络，钓鱼攻击在外网突破中的使用占比有所提升，主要原因是政务、金融这类目标客户的网络相比其他行业具有更高的安全要求，整体网络安全外部防护相对严密，对客户内部网络安全意识比较薄弱的人员开展钓鱼攻击，是实现外部突破比较高效的手段。

4、敏感信息泄露安全威胁严重

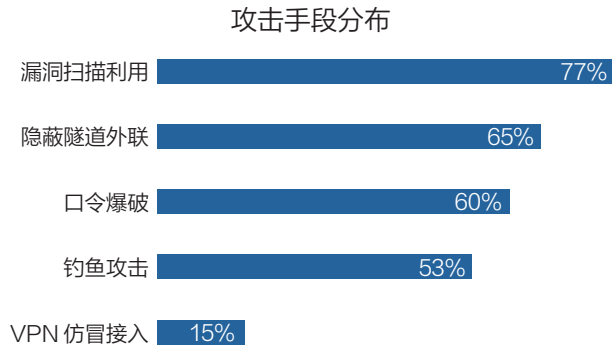
本月任务中目标网络敏感信息泄露较为严重，如内网 IP、网站目录结构、Web 后台系统、应用开发平台及后台登录地址、安全认证信息在内的敏感源码等泄露，这些敏感信息泄露原因多为安全配置疏漏、平台审核不严。此类敏感信息常常被用来实现针对性的快速突破，以及渗透。

5、目标网络缺乏纵深防护机制

本月任务中发现目标网络缺乏纵深安全防护机制，即内网安全部署缺乏功能域划分、Vlan 隔离等措施。内网纵深防御措施的缺乏，造成核心业务系统存在严重的安全隐患。

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，多采用互联网侧系统漏洞利用和钓鱼攻击的手段，内网横向拓展则以隐蔽隧道外连、内网漏洞利用、水坑攻击、弱口令和口令复用等手段为主。使用的主要技术手段分布如下：



1、漏洞扫描利用

本月任务中漏洞利用主要集中在互联网侧应用或网络平台组件，被利用漏洞以网络组件反序列化漏洞、SQL 注入、任意文件上传和未授权访问为主。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安全意识不足、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实时高效等问题。

2、隐蔽隧道外联

本月任务中涉及的目标客户以金融、政务等业务为主，这些客户内网安全体系建设比较完善、防护相对严密，互联网侧系统可利用漏洞和其他突破途径较少，目标系统网络无法通过外网直接访问，需借助端口转发、隧道技术等手段实现转发通信，如果网络功能区域划分严格、核心业务隔离措施完善，往往需要借助多层隧道转发才能实现对目标核心业务的渗透拓展。

3、口令爆破

本月任务中发现弱口令和口令复用问题主要存在于客户内网，随着人员网络安全意识提升，互联网侧系统应用的弱口令问题逐渐改善，但弱口令、口令复用问题在内网业务系统中依然严重，主要原因是目标网络缺乏对弱口令和通用口令的统一监管，没有依据安全规范要求进行账号口令设置和使用，如禁止使用弱口令，密码应当由 12 位以上数字、字母大小写、特殊字符组成，重要系统、数据库的密码更应依据规范，避免常用口令、通用口令。

4、钓鱼攻击

本月任务中，安全体系建设比较完善、防护相对严密的金融、电力业务网络，很难从外部直接突破，针对这些目标，通过冒充身份对客服人员或人事人员进行钓鱼攻击，以此打开突破口，对目标网络进行渗透。一旦进入目标网络，则通过水坑攻击对网管、核心业务人员进行钓鱼突破。

5、VPN 仿冒接入

本月任务中因目标行业限制，VPN 使用范围有限，只有少量目标业务网络使用 VPN 组网，通过 VPN 网关漏洞、内网口令复用、弱口令获取认证信息等手段，实现 VPN 网络仿冒接入渗透。

四、典型攻击手段实现案例

1、外部漏洞利用突破

（1）某目标虚拟化系统存在 CVE-2021-21985 漏洞，并且可实现本地 sudo 提权为 root 权限，进而添加此虚拟化系统管理员账号，可控制 111 台虚拟机。

（2）通过对某公司微信公众号抓包，获取到域名，并且发现该域名存在 Log4j2 命令执行漏洞，利用此漏洞成功写入 WebShell 并进入目标内网。

（3）某目标分析管控系统存在未授权访问和 SQL 注入漏洞，通过漏洞利用获取该系统后台服务器控制权限。

（4）某目标调查系统存在 Shiro 反序列化漏洞，通过该漏洞获取系统权限，并成功控制 4 台虚拟机、获得一个 REDIS 数据库权限。

2、口令爆破

（1）通过内网信息收集、口令抓取复用，获得某目标综合管理平台数据监视系统的系统管理员权限、后台管理员权限及数据库管理员权限。数据中包含 1470 个站点，数据库数据量达数千万行。

（2）某目标堡垒机存在默认口令漏洞，通过默认口令获取堡垒机管理权限，可管控 78 台内网主机设备，12 台安全设备，8 台网络设备，7 台存储设备等。

（3）某目标数据库存在弱口令漏洞，通过漏洞利用获取到 2 台数据库权限，可查看 12 万余条个人信息，包括姓名、身份证、电话、地址等敏感信息。

3、钓鱼攻击

（1）通过某目标公众号找到服务投诉电话，并添加微信，利用某系统存在问题，以问题反馈进行钓鱼攻击，最终获取网站后台权限。

（2）抓住某目标单位正在招聘的时机，以应聘名义对目标内部人员进行钓鱼诱骗，发送钓鱼邮件到招聘人员邮箱，成功钓鱼进入内网，获得敏感信息，并登录邮箱系统及内网门户，开展进一步横向扩展工作。

（3）通过某目标内网 OA 办公系统进行水坑钓鱼，成功上线 26 台 PC，对上线 PC 进行浏览器密码抓取，得到某采集系统后台管理员权限，可获取和管控大量敏感业务数据。

4、VPN 仿冒接入

（1）某目标外网系统存在信息泄露漏洞。通过漏洞利用可直接获取管理员的 VPN 账户、密码，成功进入目标内网。

（2）针对某金融目标，通过组合用户名与弱口令字典成功爆破并控制目标网络边界设备，并获得 VPN 服务器访问权限，成功接入目标内网。

政策篇

国内，《网络安全审查办法》发布，将数据处理可能影响国家安全等情形纳入审查范围；《“十四五”国家信息化规划》发布，要求切实守住网络安全底线，统筹提升信息化发展水平和网络安全保障能力。

国际上，美国总统拜登签署《国防授权法案》，网络空间授权资金高达 104 亿美元；英国政府发布《2022 年国家网络战略》，意图在重要网络技术方面处于领先地位，通过开发框架确保未来技术安全，并检测、干扰和威慑对手。

国内

证监会发布《证券期货业移动互联网应用程序安全检测规范》金融行业标准

2022 年 1 月 7 日，证监会发布《证券期货业移动互联网应用程序安全检测规范》金融行业标准，自公布之日起施行。《安全检测规范》规定了证券期货业移动互联网应用程序安全检测的总体要求及检测方法等，适用于信息安全检测服务、移动互联网应用程序的安全测试评估、自动化安全检测工具的设计与开发等。标准的制定实施，将统一行业对移动互联网应用程序的安全要求。

国家网信办等十三部门修订发布《网络安全审查办法》

2022 年 1 月 4 日，国家网信办等十三部门联合修订发布《网络安全审查办法》，自 2022 年 2 月 15 日起施行。《办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，并明确掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。此外，增加证监会作为网络安全审查工作机制成员单位。

中国银保监会印发《银行保险机构信息科技外包风险监管办法》

2021 年 12 月 31 日，银保监会发布《银行保险机构信息科技外包风险监管办法》，明确银行保险机构应当将信息科技外包风险纳入全面风险管理体系。《办法》要求，银行保险机构应当坚持以下原则：不得将信息科技管理责任、网络安全主体责任外包；以不妨碍核心能力建设、积极掌握关键技术为导向；保持外包风险、成本和效益的平衡；保障网络和信息安全，加强重要数据和个人信息保护；强调事前控制和事中监督；持续改进外包策略和风险管理措施。

《网络安全标准实践指南——网络数据分类分级指引》发布

2021 年 12 月 31 日，全国信息安全标准化技术委员会秘书处发布了《网络安全标准实践指南——网络数据分类分级指引》，给出了网络数据分类分级的原则、框架和方法。《实践指南》提出，常见的数据分类维度包括公民个人维度、公共管理维度、信息传播维度、组织

经营维度、行业领域维度。从国家数据安全角度可将数据分为一般数据、重要数据、核心数据共三个级别。

中央网信委印发《“十四五”国家信息化规划》

2021 年 12 月 27 日，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》。《规划》指出要坚持安全和发展并重。树立科学的网络安全观，切实守住网络安全底线，以安全保发展、以发展促安全，推动网络安全与信息化发展协调一致、齐头并进，统筹提升信息化发展水平和网络安全保障能力。

美 CISA 发布《公共安全陆地无线移动通信安全》白皮书

2022 年 1 月 10 日，美国网络安全与基础设施安全局（CISA）发布了《公共安全陆地无线移动通信安全》白皮书。白皮书简明扼要地解释了通信安全的重要性、通信安全计划的基本要素，以及如何制定有效的策略来防止和减少未经授权的信息访问。同时，白皮书是在不影响互操作性的情况下实施加密的最佳实践。

美联邦贸易委员会要求企业保护消费者数据免受 Log4shell 攻击

2022 年 1 月 4 日，美国联邦贸易委员会 (FTC) 发出警告称，它将跟踪并问责那些未能保护其客户数据免受持续 Log4j 攻击的美国企业。根据《联邦贸易委员会法》和《格拉姆 · 里奇 · 布莱利法》，依赖 Log4j 的公司及其供应商有责任立即采取行动，以减少对消费者造成伤害的可能性。此前，CISA 曾命令美国联邦民事行政部门机构在 2021 年 12 月 23 日之前修补被积极利用的 Log4Shell 漏洞以及联邦机构在 12 月 28 日之前报告其环境中受 Log4Shell 影响的产品。

美国网络空间日光浴委员会正式解散

2021 年 12 月 30 日，经过两年多的时间，数十项建议和一系列立法改革，美国网络空间日光浴委员会正式解散。该委员会一直在处理从虚假信息到供应链风险的网络政策问题，已经取得了几项重大成果：

①设立了国家网络总监；

②推动发布了以网络安全为重点的行政命令；

③扩大了网络安全和基础设施安全局的权限。

美国总统拜登签署《国防授权法案》，网络空间投入超百亿美元

2021 年 12 月 27 日，美国总统拜登签署 2022 财年《国防授权法案》，正式通过了价值近 7700 亿美元的国防总开支。网络空间作为美国国防的重要组成部分，授权资金高达 104 亿美元，在 2022 财年国防授权法案中占比超过 1.3%。其主要思路和特点为强化国防部的网络安全态势、增加网络司令部的权利和能力、加强联邦政府的网络安全态势、应对网络威胁环境等能力。

英国政府发布《2022 年国家网络战略》

2021 年 12 月 15 日，英国政府发布《2022 年国家网络战略》，以强化英国的网络空间安全、保护和促进网络空间利益。该战略提出了英国未来五年的五项“优先行动”（支柱），包括建设有弹性和繁荣的数字英国，降低网络风险，在重要网络技术方面处于领先地位，以开发框架确保未来技术安全；以及检测、干扰和威慑对手，加强英国网络空间安全等。

政策解读

企业视角下的新版《网络安全审查办法》解读

作者 北京德和衡律师事务所 周杨 史蕾

新年第一个工作日，《网络安全审查办法》经过将近半年的征求意见公布了正式稿。与征求意见稿相比，正式稿的最大变化之处在于：

(1) 限缩了《网络安全审查办法》的适用对象和情形，更加清晰地将网络安全审查流程确定在关键信息基础设施运营者和网络平台运营者主体身份上。

(2) 上市活动整体纳入国家安全风险考虑因素，不再区分国外上市、香港上市和境内上市情形。

(3) 首提审查期间当事人的“预防和消减风险”的义务。

(4) 明确了网络安全审查制度与数据安全审查制度、外商投资审查制度的并行关系。

总体而言，《网络安全审查办法》是一部简明扼要地以维护国家安全为宗义的法规，因而其每一条款均掷地有声。无论是原则性条款，还是要件式列举，均会对企业在下一步工作中的合规理解和具体执行发生重大影响。我们拟从《网络安全审查办法》的出台背景及本次正式稿的主要调整内容入手与大家共同讨论这部法规带来的挑战和困惑。

一、出台背景

若需理解《网络安全审查办法》正式公布带来的瞩目的原因，就必须了解《网络安全审查办法》的出台背景。网络安全审查制度的根本目标在于维护国家安全。早在《国家安全法》和《网络安全法》中即对国家安全审查制度进行了确立，并最终作为《网络安全审查办法》的立法背景予以确认。《数据安全法》的出台进一步重申了数据安全审查制度，《网络安全审查办法》正式稿也将其吸纳为制定依据之一。

> 《国家安全法》第五十九条规定，国家建立国家安全审查与监管的制度和机制，对影响或者可能影响国家安全的网络信息技术产品和服务，以及其他重大事项和活动，进行国家安全审查。
> 《网络安全法》第三十五条规定，关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。
> 《数据安全法》第二十四条规定，国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。依法作出的安全审查决定为最终决定。

在此基础上，监管机构通过多层次的立法尝试，逐步探索出网络安全审查的基本监管框架（见下图立法沿革）。例如，在2017年网信办公开征求意见的《网络产品和服务安全审查办法（征求意见稿）》中，首次提出网信办将会同11个部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，统一组织网络安全审查工作，协调网络安全审查相关重要问题。网络安全审查委员会的组织架构最终在正式版本的《网络产品和服务安全审查办法（试行）》中确立，该试行办法作为《网络安全法》的重要配套规章，与《网络安全法》一同正式实施，直至2020年，该试行办法才被《网络安全审

查办法》（2020 版本）所取代，而前述网络安全审查委员会也被网络安全审查办公室取代其职能。

可见，《网络安全审查办法》始终密切围绕维护国家安全这一目的，在有限的可能涉及国家安全的领域内展开监管并默默无闻，直至其在 2021 年 7 月 2 日被网络安全审查办公室发布的通告所引用，该通告为——《网络安全审查办公室关于对“滴滴出行”启动网络安全审查的公告》。由于滴滴与民众出行的密切相关性，网络安全审查制度乃至其背后的国家安全利益才首次进入公众视野，并引发强烈关注。

法律法规 / 立法政策	颁布时间
《建立信息安全审查制度》的立法提案	2013
《信息化发展规划》	2013.10.24
《关于建立网络安全审查制度的公告》	2014.05.22
《关于加强党政部门云计算服务网络安全管理的意见》	2015.12.30
《中华人民共和国国家安全法》	2015.07.01
《国家信息化发展战略纲要》	2016.07
《中华人民共和国网络安全法》	2016.11.07
《网络产品和服务安全审查办法（试行）》	2017.05.02
《关键信息基础设施安全保护条例（征求意见稿）》	2017.07.10
《贯彻落实总体国家安全观健全完善关键信息基础设施安全保护法律体系》	2018.04.19
《网络安全审查办法（征求意见稿）》	2019.05.21
《网络安全审查办法》	2020.04.13

二、适用主体进行明确梳理

在 2020 年旧版本的《网络安全审查办法》中，适用主体仅有“关键信息基础设施企业”（CIIO），适用情形则为关键信息基础设施企业“采购网络产品和服务”“影响或可能影响国家安全的”情形。因此，当滴滴受到网络安全审查的通报公布后，大量质疑滴滴是否构成关键信息基础设施企业从而具备适用《网络安全审查办法》资格的声音不绝于耳，而随后公布的《网络安全审查办法》修订稿中，迅速将适用主体由 CIIO 扩展到包括数据处理者这一边界广泛的概念。需要看到，数据处理者则是《数据安全法》提出的正式概念，但凡实施了数据处理的主体，均可以被认为是数据处理者，而数据处理活动的定义贯穿数据全生命周期，包括“数据的收集、存储、使用、加工、传输、提供、公开等”。因而以“数据处理者”作为《网络安全审查办法》的适用主体仍有可能分散“网络安全审查”的执法精力。

在本次《网络安全审查办法》的正式稿中，适用主体被调整为明确的两类，即“关键信息基础设施企业”（CIIO），和“网络平台运营者”。关键信息基础设施企业已经由《关键信息基础设施安全保护条例》提供了明确的识别和认定，而“网络平台运营者”尚且缺乏明确定义。根据公开检索，相近定义为《网络数据安全管理条例（征求意见稿）》和《互联网平台落实主体责任指南（征求意见稿）》确认的“互联网平台运营者 / 经营者”概念，《网络安全法》中确立的“网络运营者”概念，以及《电子商务法》中的“电子商务平台经营者”概念，相关概念内涵分别如下所列：

《网络安全法》

– 网络运营者，是指网络的所有者、管理者和网络服务提供者。

《互联网平台落实主体责任指南（征求意见稿）》

– 互联网平台，是指通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。

– 平台经营者，是指向自然人、法人及其他市场主体提供经营场所、交易撮合、信息发布等互联网平台服务的法人及非法人组织。通过互联网等信息网络从事销售商品或者提供服务的自建网站经营者，可参照平台经营者适用本指南。

《网络数据安全管理条例（征求意见稿）》
– 互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。
– 大型互联网平台运营者是指用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者。
《电子商务法》
– 电子商务平台经营者，是指在电子商务中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展交易活动的法人或者非法人组织。

除了CIIO作为适用主体的确定性，目前来看“网络平台运营者”并非一个具有普遍通识的法律概念。从对“平台”的朴素理解来看，其功能必须具备撮合和连接性。例如，《互联网平台分类分级指南（征求意见稿）》中即根据其平台中所撮合和连接的双方不同，而将平台进行了如下类别划分。因此，我们谨慎认为“网络平台运营者”应该是针对此类具备多方交易功能、提供综合服务的平台运营者，并非单纯的通过网络仅提供自身服务的运营者，或仅提供平台搭建等技术服务的运营者。就这个层面而言，《网络安全审查办法》的适用主体实际上相比征求意见稿进行了范围限缩。

平台类别	连接属性	主要功能
网络销售类平台	连接人与商品	交易功能
生活服务类平台	连接人与服务	服务功能
社交娱乐类平台	连接人与人	社交娱乐功能
信息资讯类平台	连接人与信息	信息资讯功能
金融服务类平台	连接人与资金	融资功能
计算应用类平台	连接人与计算能力	网络计算功能

三、适用情形的梳理和澄清

正式稿第五六七八一共四个条款中简明扼要的说明了申报网络安全审查的适用情形，我们试简单区分如下:

类别	适用主体	适用情形
强制申报	关键信息基础设施企业	采购网络产品和服务，并预判影响或者可能影响国家安全（第五条、第六条）
强制申报	网络运营者	掌握超过100万用户个人信息的网络运营者赴国外上市（第七条）
自发申报	网络运营者	经分析认为自身活动可能影响或者可能影响国家安全的（包括全部上市活动）（第八条）

值得注意的是，尽管“预判义务”被确立为关键信息基础设施企业的专门义务，但并不完全排斥其他当事人（网络运营者）对自身数据处理活动进行预先分析的要求，因为《网络安全审查办法》第三条开宗明义地指出其审查范围囊括了“产品和服务以及数据处理活动”。因此，从《网络安全审查办法》第八条的规定可以合理推测，一旦当事人在数据处理活动中“经分析认为自身活动可能影响或者可能影响国家安全的”，均应申报网络安全审查。换句话说，赴港上市企业仍应时刻自省是否存在可能影响或者可能影响国家安全的数据处理活动，一旦存在应主动申报网络安全审查。这一规定实质也与《网络数据安全管理条例（征求意见稿）》确立的网络安全审查制度接壤，后者第十三条规定：“处理一百万人以上个人信息的数据处理者赴国外上市的”，或“数据处理者赴香港上市，影响或者可能影响国家安全的”，应当申报网络安全审查。可见，《网络数据安全管理条例（征求意见稿）》确立的网络安全审查原则同样区别了赴国外上市和赴境外上市情形，即赴国外上市企业只要包含处理个人信息过百万，则必须申报；但赴港上市企业若自行分析认为影响或者可能影响国家安全的，同样应申报网络安全审查。

《网络数据安全管理条例（征求意见稿）》
第十三条 数据处理者开展以下活动，应当按照国家有关规定，申报网络安全审查：
（一）汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、

重组、分立，影响或者可能影响国家安全的；
（二）处理一百万人以上个人信息的数据处理者赴国外上市的；
（三）数据处理者赴香港上市，影响或者可能影响国家安全的；
（四）其他影响或者可能影响国家安全的数据处理活动。
大型互联网平台运营者在境外设立总部或者运营中心、研发中心，应当向国家网信部门和主管部门报告。

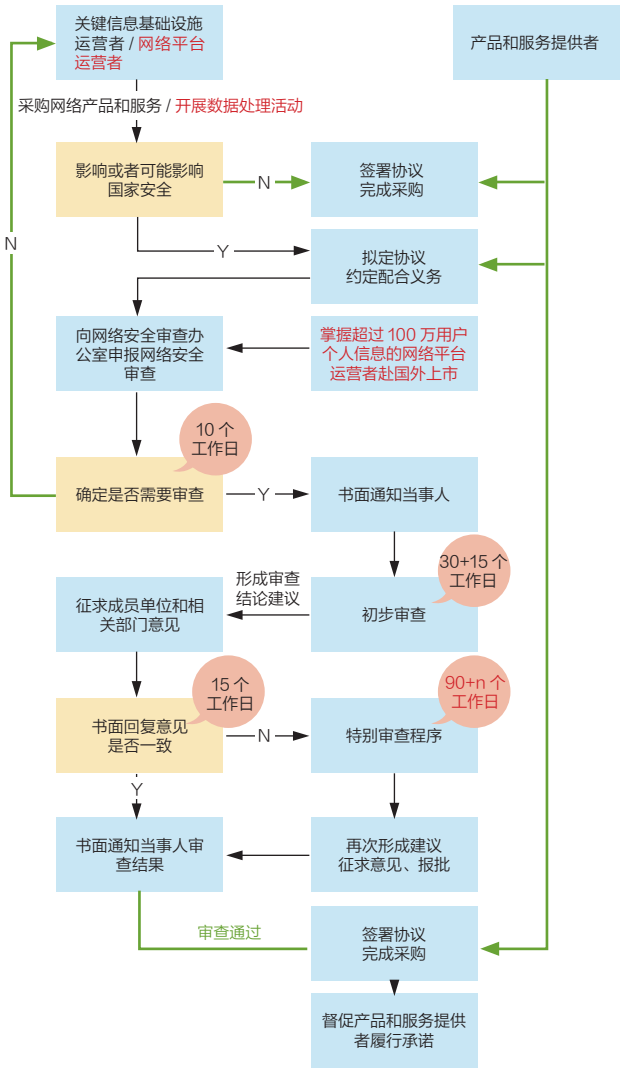
此外我们注意到，《网络安全审查办法》似乎对于上市情形格外重视，且展现了对全部上市企业风险的关注，其第七条、第八条和第十条的相关条款均展现了这种关注。我们初步认为，上市活动整体纳入国家安全风险考虑因素，不再区分国外上市、香港上市和境内上市的情形。

同时，为具体落实赴国外上市企业的网络安全审查工作，《网络安全审查办法》答记者问中专门公布了接收审查资料的窗口单位，即网络安全审查办公室设在国家互联网信息办公室，具体工作委托中国网络安全审查技术与认证中心承担。中国网络安全审查技术与认证中心在网络安全审查办公室的指导下，承担接收申报材料、对申报材料进行形式审查等任务。中国网络安全审查技术与认证中心设立网络安全审查咨询窗口。

第七条 掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。
第八条 当事人申报网络安全审查，应当提交以下材料：…（三）采购文件、协议、拟签订的合同或者拟提交的首次公开募股（IPO）等上市申请文件。
第十条 网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：（六）上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险。

四、申报流程调整

在申报流程方面，为方便各位理解，我们将最新流程进行了整理，具体请见下图。根据最新公布流程，全部网络安全审查程序履行完毕最长需要约 160 个工作日。



栏目主编　李建平

网络安全八个关键词

未来一年，八个安全热点将主导安全建设趋势与方向：新合规、信创安全、安全左移 、数据安全治理、隐私保护、漏洞管理、 安全网格、托管安全服务。

2022 年网络安全八个关键词

作者 奇安信公关部

关键词 1

新合规时代：主体责任进一步压实

在 2022 年网络安全的八大趋势预测中，Gartner 指出，网络安全和政策合规已成为企业董事会最关心的两大问题。在刚刚过去的 2021 年，全球各地陆续推出网络安全法律法规，尤其是我国出台了多项网络安全与数据报告相关的法律法规及政策文件，预计 2022 年，随着相关配套法规的密集出台，我们将迎来新合规时代。

2021 年 6 月 10 日，《中华人民共和国数据安全法》简称《数据安全法》）正式发布（于 2021 年 9 月 1 日实施）。2021 年 8 月 20 日，《中华人民共和国个人信息保护法》简称《个人信息保护法》）正式发布（于 2021 年 11 月 1 日实施）。这两部法律同《中华人民共和国网络安全法》一起，共同构建了我国的数据治理立法框架。2021 年 8 月 17 日，《关键信息基础设施安全保护条例》发布（于 2021 年 9 月 1 日实施）。至此，我国全面建成以网安法、数安法、个保法和关基条例为基础的“三法一条例”安全法规体系。

随着 2021 年多项法律法规相继实施，各行业正落实法律法规的保护要求，建立健全网络安全保障体系。例如，国家医保局 2021 年 4 月发出《关于印发加强网络安全和数据保护工作指导意见的通知》，要求到 2022 年，基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作体制机制。

目前中央网信办正在抓紧制定数据安全法、个人信息保护法配套法规规章，包括《网络数据安全管理条例》《数据出境安全评估办法》《个人信息出境标准合同规定》《人脸识别技术应用安全管理暂行规定》，以及数据安全、个人信息保护的合规审计制度和相关标准规范。信安标委和行业标准制定机构也密集推出一批国家和行业标准，尤其是聚焦于金融数据、平台数据、车联网数据等领域。

2022 年 1 月，《网络安全审查办法》修订后正式发布。新版《审查办法》完善了国家网络安全审查有关要求，压实了网络平台运营者的国家安全和数据安全主体责任。

预计 2022 年，随着各项配套法规规章的完备，我国企业将会面临更具体的合规要求。企业收集数据后的保管和使用面对增大的安全风险与合规需求，需要认真研判法律法规、监管规定、行业准则、国际标准有关合规管理的新变化，建立健全企业数据合规管理体系。

如何规范数据处理活动，保障数据安全，成为企业面临的重要的课题，数据合规将会发展成独立专业领域，推动对数据合规人才的旺盛需求。

关键词 2

数据安全治理：从“设计”走向落地

刚刚过去的一年，绝对是数据安全的“法律大年”。《数据安全法》《关键信息基础设施安全保护条例》2021 年 9 月 1 日正式实施，《个人信息保护法》2021 年 11 月 1

日正式实施。这些法律法规不仅给企业数据安全提供了重要的法律依据和支撑，更对数据合规治理提出了更高、更明确的要求。

2022 年开年伊始，国务院办公厅印发了《要素市场化配置综合改革试点总体方案》，其中对数据安全进行了多处论述。在数字经济时代，企业数据安全治理体系的建设和能力提升已势在必行。

数据安全治理的广义和狭义

中国信通院发布的《数据安全治理实践指南（1.0）》认为，数据安全治理的定义分为广义和狭义两方面。从广义的国家层面来看，数据安全治理是国家有关部门、行业组织、科研机构、企业、个人共同参与和实施的一系列活动集合。包括完善相关政策法规，推动政策法规落地，建设与实施标准体系，研发并应用关键技术，培养专业人才等。

从狭义的组织内部来看，数据安全治理是指在组织数据安全战略的指导下，为确保数据处于有效保护和合法利用的状态，多个部门协作实施的一系列活动的集合。主要包括组织机构建设、制度流程规划、技术工具构建、人员能力培养等方面的工作。

在具体落实上，信通院认为，数据安全治理是一项系统化工程，包括治理目标，治理参考框架和实践路线三部分。其中，数据安全治理的目标是在合规保障和风险管理的前提下，充分利用数据的价值，保障业务的持续健康发展，从而实现安全与发展的双向促进。参考框架主要是依据团体标准《数据安全治理能力评估方法》的内容进行制定。围绕数据安全治理参考框架，可以实践路线分为治理规划、建设、运营、成效评估四个环节。

中国信通院指出，作为维护国家安全的战略需要，也是组织重构竞争力的必要手段，未来数据安全治理将从国家、行业、企业三个层面，围绕“行业化”“场景化”两方面展开，同时也将促进“离散化”治理方式到“体系化”治理模式的转变。

数据安全治理的趋势

数据安全不仅是技术问题，而是合规、管理与技术体系的融合。对于企业而言，数据在多方参与计算、内外部流转中产生价值，但同时数据流转也带来更多的安全风险。从数据安全体系建设方面来看，新的法律法规的合规要求，加上数字化转型的驱动，可能会促使企业管理组织架构调整、管理规章制度及数据安全策略的演进，进而到技术体系构建与运营的逐步构建，这些策略的改变如何转化成为能力框架，并落地到技术和运行方

面，其复杂度非常高。

金杜律师事务所法律专家做了一个形象的比喻：“法律是蓝图设计师或者概念设计师，而科技恰恰是工程师，将概念落到工程图。如果只有法律概念图，无法直接施工；如果不对法律进行解读，工程图怎么画、‘水电’怎么走，也无法确定。这正是数据安全保护和数据安全治理中，法律和科技结合最紧密的地方。”

奇安信推出的数据安全运行构想图，基于系统工程的方法，从数据安全运行视角，以新型数据中心的业务场景为依托，基于业务到技术实现的层次化视角，囊括了数据安全应具备的三个状态：治理态、规划态和运行态，细致展现了数据安全治理结果转化到规划设计、技术落地的过程。

预计 2022 年，将法律和科技结合的数字安全治理将是企业机构巨大的需求增长点。企业应该基于数据应用场景、业务逻辑与数据的流转，从“管理、技术、运行”来开展数据安全的治理与防护工作，以数据安全治理为前提，通过数据安全态势感知进行数据安全运营，从数据资产管理、数据流动态势、数据风险分析、用户行为分析等维度，促进数据安全治理的闭环形成，实现数据安全能力的持续演进。

信创安全：更丰富全面的产品体系，更强服务能力

2021 年，信创产业进入高速发展、全面开花阶段，成为现象级的新风口。信创是为了解决本质安全的问题，通过发展信创产业构建自主的 IT 产业和生态，使得 IT 产品和技术安全可控。

信创产业发展始终围绕安全问题展开，信创安全的本质是护航国产化厂商 / 产品的数字化转型，为各行各业提供安全基石与技术服务保障。信创产业发展和网络安全产业结合愈加紧密。2021 年，奇安信信创安全龙头企业加大对基础设施能力、工业智能能力和国产化能力的投入，加大基础化、国产化、智能化的投资力度，助力国家信创生态建设。我国的信创安全防护已从“单领域防御”转到“全域安全防御”，在产业上、下游协同推动下，信创产业安全发展全域开启。

但目前信创安全能力仍需不断提升：目前信创安全普遍以政策驱动为主，真正市场驱动较少，尚未形成规模化发展态势。整体来看，信创安全目前渗透率较低。当前信创产品生态不够成熟，产品销售、服务、维护等能力尚在建设中，相关的国家标准、产品测试规范不够充分，操作系统漏洞、应用程序漏洞隐患未知，仍需加强信创安全技术应用创新的深度，构建信创安全产业生态，保障产品和技术安全可控。

预计 2022 年，信创安全领域将依靠构建更加丰富、全面的产品体系，更强的服务支撑能力，来保障信创网络安全，全面助力安全生态体系建设与信创产业的快速发展。

总得来看，未来信创安全将从以下几个方面推进。

首先，重视高级威胁。依靠体系化、系统化设计，应对信创安全的高级攻击，从最底层的 IT 基础设施到最高层的业务应用，针对产品安全、运行安全和业务安全，同步全面进行安全设计与实施。

其次，内生安全保障信创环境。为基于信创的信息化环境构建内生安全能力，摆脱局部与外挂，实现网络安全能力与信息化环境的融合内容。按照系统工程的思想，将安全能力组件化，由规划方法、工具集、模型、架构和项目纲要构成，能够让安全产品和服务相互联系、相互作用，在整体上具备单个产品和服务所没有的功能，从而保障复杂系统的安全。目前奇安信的安全与中国电子 PK 体系深度融合，构建强大的 PK-S 体系，可以实现本质安全 + 过程安全的有效结合，提供有力的安全防护方案。

信创提供了更好的开放性和权限控制，可以从底层来解决安全问题，例如，采用于内存指令层的漏洞攻击检测技术等。人工智能、数据引擎等技术也在信创安全广泛应用，解决产品安全和供应链安全问题。此外，信

创应用的产业领域大多场景复杂、应用繁多，更强调通过持续运营的方式与政企 IT 系统的不断发展相匹配。

安全左移：供应链安全严峻形势推动安全左移

据 Verizon、Forrester 以及 Gartner 等全球知名机构、咨询公司发布的统计研究数据显示，软件系统自身漏洞已成为黑客攻击和数据泄露等安全事件发生的主要原因之一，且基础软件类漏洞易引发超大规模安全事件，更是屡次占据近几年的新闻头条。2020 年底，针对 SolarWinds 的复杂供应链攻击成为全球头条新闻。2021 年 SonarQube 系统未授权访问漏洞、被全球广泛应用的组件 Apache Log4j 曝出高危漏洞，几乎所有行业都受到重大影响。

供应链安全面临的严峻形势，激发了安全左移需求。“安全左移”是指在软件开发生命周期（SDLC）早期阶段就将安全机制（代码审查、分析、测试等）嵌入，从而防止缺陷产生和尽早找出漏洞。安全左移已经成为实现 DevSecOps 的重要部分。

安全左移是一项复杂工程

要通过安全左移实现真正高级别的安全，是一项十分复杂工程，面临严峻挑战。其中包括：开发人员如何了解行业面临的一线安全风险和防范这些风险的手段；如何创建系统性协作方法来同时实现技术创新和安全防护；开发人员需要代码安全检测工具和流程的支持，使他们能够在研发时不必放慢速度以实现安全合规，因此推动了安全左移相关技术和框架的进一步发展。

谷歌在 2021 年发布了用来检测端到端供应链完整性的框架（Supply Chain Level for Security Artifact，SLSA）。该框架设计了由低到高的四个级别，分别是一系列由易到难逐渐采用、业界一致认可的安全准则。最高级别下，SLSA 支持自动创建可审核元数据。这些元数据可以输入到策略引擎中，以便为特定包或构建平台提供“SLSA 认证”。一旦某个软件达到了最高级别，消费者就可以确信它没有被篡改，可以安全地追溯到源代码。但这对大多数软件都很困难，连谷歌自己也难以把内部软件全部实现最高级别的安全。

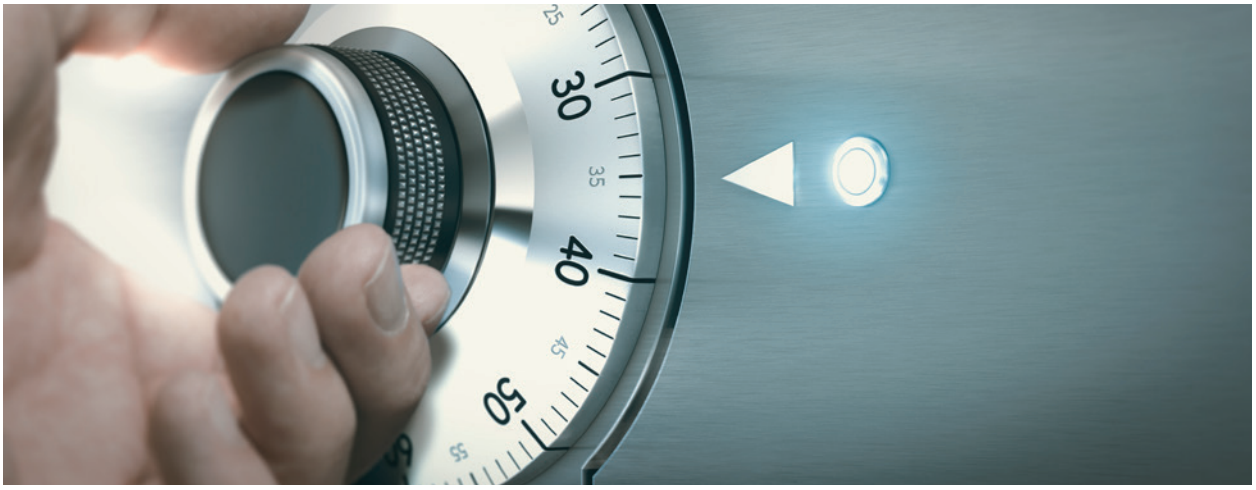
安全供给不足下的技术创新

为快速发现软件的漏洞和缺陷，目前业界形成了 SAST、DAST、IAST、SCA 四类主要技术，分别覆盖了软件开发生命周期的代码、制品、使用、组件溯源环节的安全。但这些技术的商业化产品都是偏工具性质的，距离代码安全平台解决方案差距还比较大。并且它们在国外的应用范围更加广泛，国内仍处于早期阶段。

安全左移正向着面向开发人员的代码安全管控、默认安全框架组件、嵌入基础设施的代码安全检查等方向发展，当前仍需要体系化的框架和解决单点难题的技术创新，这些新技术在不断涌现并逐步得到市场认可。

软件物料清单 (Software Bill of Materials，SBOM) 通过列出和记录软件组件来有效地显示整个供应链，可以有效解决企业内部软件的组件可见性和安全溯源难题。2021 年 9 月，Software Package Data Exchange（SPDX）规范发布，被认定为安全性、许可合规和软件供应链构件领域的国际开放标准。包括英特尔、微软、西门子、VMware 和 WindRiver 在内的众多公司已经使用 SPDX 在政策或工具中传达软件材料清单信息，以确保在全球软件供应链中实现合规和安全开发。

代码风险管控平台是另一种可行思路。RSAC 2021 创新沙盒冠军 Apiiro 通过 UEBA、SAST 技术联动构建了首个代码风险平台，智能检测并阻止代码的恶意提交，实现从设计到代码再到上云整个流程对任意更改风险的全面可见。同时，该平台可全方位查看应用程序、基础架构、开发人员的知识和业务影响方面的安全和合规风险。



关键词 5

隐私保护：隐私计算进入产业化时代

搜索记录、购物清单、出行轨迹、人脸和指纹……如今，我们在网络空间的每一次停留或操作，都会被存储为数据形态的“痕迹”。“远程办公”“数字社区”“外卖快递”“健康宝”和“行程大数据”这些数字化产品成为我们生活、办公的必需品，我们的隐私信息被应用在了越来越多的场景中。不仅是窥探和数据滥用，近几年频频爆出的各类隐私泄露丑闻更让人触目惊心。

数据采集、存储、流通、使用等环节缺乏规范，数据隐私管理制度不健全，大数据、人工智能等产业的发展存在隐患。2021 年，《 数据安全法 》《 个人信息保护法 》相继落地，《 个人信息保护法 》明确规定，不得进行大数据杀熟；不得向用户强制推送个性化广告；限制过度收集用户个人信息等。数据安全和隐私保护有了更强有力的法律保障，大大小小的企业开始重视隐私保护，并着手建立企业的隐私保护体系，一些常见的隐私保护工作也被逐步推广。在数据融合应用和隐私保护的双重驱动下，隐私计算等新技术进入产业化时代，隐私保护迎来全新的阶段。

隐私保护的主要问题

企业面临的是云计算、物联网、大数据、移动互联、边缘计算这些数字化技术背后的隐私风险，传统的安全技术、冗长的合规流程、人工的处理方式无法解决如下隐私保护的困难和痛点：如何应对变幻莫测并日益严格的隐私监管环境；无法充分全面地识别企业各个业务线收集、存储、处理和分享的隐私数据；隐私管理部门难以及时掌握业务部门的数据需求变更信息；隐私风险评估的实现方式较为传统，无法跟上产品开发的迭代速度；数据的共享受阻导致无法更好挖掘数据价值；用户隐私权利的响应大量依赖于人工处理等。应对数字化时代下的隐私保护痛点，也需采取数字化的方式，隐私保护技术和平台工具成为热门并得到迅速发展。

隐私保护的技术发展

随着隐私的关注度越来越高，加之企业日趋复杂的业务场景、海量的数据计算与流通需求，市场上涌现了不少隐私保护技术，有的已经在其他领域应用实践多年，开始更多地用于隐私数据的保护；而有的则是应用了新兴的技术，为企业的隐私管理带来了新的思路和方案，比如， 炙手可热的隐私保护计算，被 Gartner 认为是

2021 年需要深挖的 9 项重要战略科技趋势之一。

隐私计算全称是隐私保护或者隐私增强计算模式，结合了密码学、软件工程、分布式计算、人工智能及其他的硬件技术形成的技术体系，能够在提供隐私保护的前提下，实现数据价值的挖掘。隐私计算是指在保护数据本身不对外泄露的前提下，实现数据分析计算的一类技术集合，它具备“可用不可见，可控可计量”的特点。

其中，联邦机器学习是一个机器学习框架，能有效地帮助多个机构在满足用户隐私保护、数据安全和政府法规的要求下，进行数据使用和机器学习建模，能够解决多机构之间数据孤岛的问题。同态加密是基于数学难题的计算复杂性理论的密码学技术。对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。差分隐私提供一种当从统计数据库查询时，最大化数据查询的准确性，同时最大限度减少识别其记录的机会。安全多方计算主要针对无可信第三方的情况下，如何安全地计算约定函数的问题。安全多方计算是电子选举、门限签名及电子拍卖等诸多应用得以实施的密码学基础。这些技术和解决方案已经开始从概念阶段转向实施阶段，在金融信贷风险评级、精准营销、广告投放、政务数据共享、人工智能疾病联合诊断等领域都已经有了应用场景。

市场上也涌现出不同类型的管理工具和平台，基于平台工具的管控对象，可以分为隐私体系管理平台和企业隐私数据管理工具。前者更偏向于借助平台来支撑隐私保护管控的流程，为数据保护管理或隐私保护相关人员提供更高效的方式；后者更偏向于借助平台对隐私数据进行管理，为企业管理者或数据主体提供更透明的视角。

关键词 6

漏洞管理：未来将向攻击面管理发展

网络安全工具和方法日新月异，但漏洞管理始终是企业网络安全的致命环节。美国国家标准与技术局 (NIST)、国家漏洞数据库 (NVD) 有数据显示，90% 以上的网络安全问题是由软件自身的安全漏洞被利用导致。近年来，60% 的企业数据泄露与安全漏洞未得到修补有关。企业漏洞预防、检测和修补的成本正在不断上升。且尽管大多数安全企业都了解及时修补漏洞的重要性，但由于各种原因，这个过程可能会延迟。越来越多的企业通过漏洞管理平台和技术对网络进行及时、全面、自

动化的安全评估和保护，降低网络安全风险。

国际咨询机构 Gartner 认为：漏洞管理是在安全脆弱性被利用前，发现并做出修补的关键流程。这个流程包括定义安全策略、评估、防护、消减和监控等环节。且漏洞管理流程同时还需要完善的管理制度，自动化 IT 安全漏洞管理平台，执行制度的人，等共同支撑流程的运转，来形成漏洞管理的闭环。

评估方式改进成未来趋势

资产类型的不断扩充成为目前漏洞管理面临的主要问题。尤其是在云计算、容器技术和 IoT 相关的场景下，需要思考资产的特殊性来进行漏洞管理的适配。在上云的趋势下，传统的部署模式面临很大的挑战。尤其是容器技术的大规模使用，之前网络类的还是基于 agent 的方式，都很难对容器进行有效的漏洞扫描，都需要对容器的文件系统进行理解，对每个 layer 分析来进行漏洞的分析和扫描。因为容器的网络组织形式以及在运行时状态，会让传统的漏洞扫描失效，基本原理发生了根本的变化。此外，随着 OT 和 IT 的进一步融合，相关应用场景更加复杂，OT 领域的漏洞管理首当其冲，但却仍处在比较初级的阶段，需要更多培育和关注。

漏洞评估方式的改进成为未来发展的新趋势。漏洞评估方式包括基于漏洞本身的评价、基于资产的评价和基于风险和威胁的评价。漏洞评估方式的改进是目前漏洞管理的痛点所在，如果没有基于风险和威胁的角度，修复漏洞的优先级就无法做出判断，漏洞管理就会走入程式化，效果可能很难得到最好的体现。以威胁为中心的评价方式是近几年提出的，不是取代前面两者，而是这个基础上综合考虑加入威胁的因素，合起来的模型叫作逐渐降低风险和立即处理威胁，已成为漏洞的主流评价方式。

2021 年，Gartner 将攻击面管理相关技术定义为新兴技术，从漏洞管理到攻击面管理，网络安全攻防博弈将真正意义上迎来升维跨越。攻击面管理强调的，不仅仅是已存在的静态漏洞及其闭环跟踪，而是任何可能发生安全问题进而演化为安全事件的网络风险和脆弱性。攻击面管理将成为未来漏洞管理发展的趋势。

漏洞管理平台的新类型

漏洞的管理数据维度多、来源杂，要将该类数据纳入到统一管理平台涉及的工作十分烦杂，维护起来也非常复杂，要做好自动化调度更是涉及烦复的工作内容。好的漏洞管理平台应该具备全面且开放、自动化和流程化、及时响应和数据支撑决策等特征。传统漏洞管理平台发展至今，出现了新的类型，如威胁漏洞管理（TVM）和泄露攻击模拟（BAS）。

TVM 产品将漏洞和威胁信息结合归并，可以理解为漏洞领域的 SoC。TVM 可以使用漏洞扫描数据并利用威胁情报（TI）、攻击的漏洞及内部资产的重要性，实现让组织更好地理解漏洞风险，防止泄漏产生。同时也可以跟 IPDS 和 WAF 类产品对接作为漏洞处理的方式进行迅速响应。代表厂商有 Kenna Security 和 NopSec，这两家厂商对于漏洞的评估比传统的漏洞扫描厂商更有针对性，更基于威胁和风险本身。

BAS 以攻击者视角来看待漏洞，自动化模拟攻击行为来利用漏洞，更真实，也更具实际意义。BAS 会将漏洞识别和漏洞利用合二为一，让客户感觉更真实有效。代表厂商有 AttackIQ 和 Core Security。AttackIQ 基于 MITRE 的 ATT&CK 的矩阵模型进行的攻击模型来设计的产品更切实落地，基本实现方式是安装 agent、运行测试脚本和场景模拟，最后查看结果，更贴近于实际的攻击场景。包括 TVM 和 BAS 类型的威胁管理平台产品，在向着更有安全价值的方向演进。

关键词 7

网络安全网格：未来的网络安全基础设施

近两年来，Gartner 在其网络安全趋势预测中，反

复提到了一个全新的网络安全架构——网络安全网格。Gartner 对此解释到：如今数据和资产可能出现在任何地方，这意味着传统的网络安全边界已经消失，需要一种方法为任何位置的资产提供安全保障。

Gartner 在试图提出一种统一的安全方法，来解决网络边界日益模糊时代的网络安全问题。尽管人们已经意识到日益扩大的风险暴露面积，让以内外网边界为基础的被动防御模型不再可靠，并且不断尝试零信任网络访问、威胁情报、扩展检测与响应、安全访问服务边缘等新一代安全技术，但这些技术依然是零散的，需要具有灵活性、敏捷性、可扩展性和可组合性的安全选项。

Gartner 研究副总裁 Jay Heiser 谈到了关于网络安全网格的三个特点：

第一，网络安全网格是一种分布式架构方法，实现了在分布式策略执行架构中实行集中的自动化策略编排，用于实现可扩展、灵活和可靠的网络安全控制；

第二，网络安全网格允许身份成为安全边界，使任何人或事物能够安全地访问和使用任何数字资产；

第三，网络安全网格这种分布式、模块化架构方法，正迅速成为分布式身份结构（The Distributed Identity Fabric）、基于上下文的安全分析、情报和响应（EDR、XDR）、集中式策略管理和编排、ZTNA、云访问安全代理 (CASB) 和 SASE 的安全网络基础设施。

如果用一句话来概括，网络安全网格正在成为一种安全基础设施，能够为离散的安全产品提供统一的自动化编排策略，使其形成一个有机的整体，确保无处不在的资产享有一致的安全防护水平。

对此，部分国内外头部网络安全厂商已经在逐步探索过程中。例如，Fortinet Security Fabric 安全架构能够实现飞塔 50 多种安全和组网技术的组合，共享威胁情报、关联数据，并作为协调的系统自动响应威胁。

同时作为 Fortinet Security Fabric 安全架构开放生态系统的一部分，Fortinet 已经与 450 多家第三方技术合作伙伴实现了集成和交互操作。

奇安信的大禹平台提供面向大数据安全的通用开发平台及配套的内置安全能力，其核心能力包括数据接入、数据治理、云地协同、联合分析系统、事件分析与管理、安全设备接入与控制及资产管理和运营。

值得注意的是，网络安全网格架构为网络安全产品提供了一致的底层安全能力，从而避免了重复造轮子的

问题，将带来网络安全研发效率的大幅提升。

关键词 8

安全托管：走向本土特色、符合业务需求

网络安全威胁形势的演变和日益复杂的业务环境驱动着安全托管服务（Managed Security Service，MSS）高速增长。IDC 在《全球网络安全支出指南》指出，2020 年，全球托管安全服务以其超过 20% 的市场占有率成为了网络安全市场中最大的子市场，未来五年 MSS 年复合增长预计超过 20%。

与国外发展成熟度较高的 MSS 市场相比，中国安全托管服务市场仍处在增长期，具有较大的上升空间。国际权威机构 Frost & Sullivan 报告显示，2020 年大中华区 MSS 市场年增长率高达 20.9%，预计将在 2020 年至 2025 年保持强劲的两位数增长率，复合年增长率高达 21.4%。

越来越多企业选择 MSS

在数字化转型，人才缺乏和威胁激增的背景下，MSS 成为一种潮流。

1）数字化转型

我国正处于数字化转型的关键时期，5G、人工智能、物联网、大数据等新技术与业务环境相融合，导致政企组织内部环境愈加复杂，给运营和管理带来更多挑战。新业务、新场景带来更多新的安全威胁，外部威胁的演变迫使政企组织采取更加积极有效的方式来保护网络安全。

2）政策背景

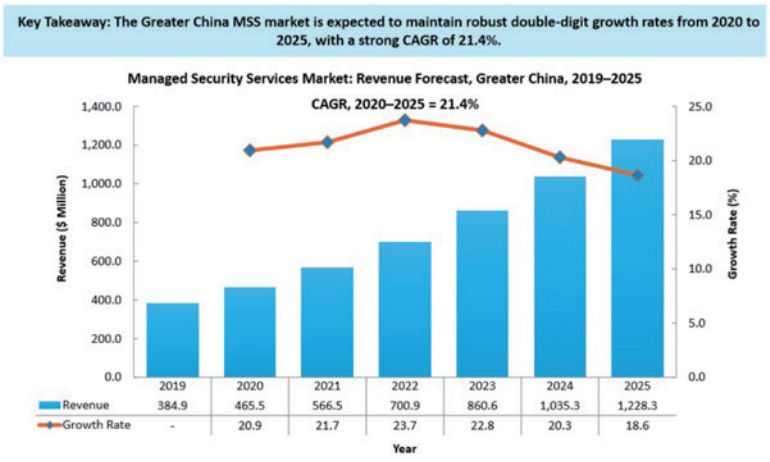
2021 年，《数据安全法》《网络产品安全漏洞管理规定》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规相继出台，政企组织网络安全建设从合规驱动向合法驱动转变，各单位需要更加专业安全团队满足需求。

3）人才缺失

面对外部威胁的演变和政策驱动，许多政企组织缺乏拥有专业知识和技能的安全团队，来处理日常安全运营中出现的问题，这就需要将安全运营外包给服务商。

4）高级威胁

数字化转型、疫情等背景影响下，针对政企组织的高级威胁数量显著增加，尤其是勒索软件攻击和 APT 攻击。缺乏专业领域知识和威胁环境的了解，再加上现有的安全产品不足以检测和应对更高级的安全威胁，都促使越来越多的组织寻求服务商帮助，以加强面对高级威胁的检测和响应能力。



5）市场变化

在过去几年，国内一直是倾向于以产品为导向的市场，以奇安信为代表的国内领先的服务商通过扩展服务组合，迅速进入 MSS 市场。随着外部环境的发展变化，政企组织已经意识到依靠安全产品难以满足需求，MSS 凭借“服务组合灵活”“专业人才能力”“服务标准化”“服务管理能力”等优势，使得政企组织从产品导向向服务导向的持续转变，国内 MSS 市场将迎来强劲增长。

本土特色 MSS 势在必行

安全托管服务的形式与内容是多元的。IDC 将安全托管服务（MSS）定义为安全服务提供商（MSSP）通过安全运营中心（SOCs）进行全天候监控和管理的 IT 安全服务。服务范围包括部署在本地、外部数据中心和云上的安全托管服务。Frost & Sullivan 则将 MSS 划分为安全资产监控 / 管理、托管威胁检测与响应（MTDR）和其他新兴 MSS 服务三类。Gartner 认为除了威胁检测和响应服务，安全托管服务通常还应包括事件响应服务、漏洞评估以及漏洞管理服务和网络威胁相关情报服务等。

在国内，由于中国自身实际情况的特点，相对“远程服务”，国内更为青睐“驻场运维”模式。近几年，在政策、市场需求等因素的推动下，中国网络安全服务市场的快速发展。其中，智慧城市场景下的安全运营需求和上云后的安全托管需求，直接推动了中国托管安全服务市场规模的快速增长。目前大部分中国的托管安全服务还处于‘设备托管 + 合规 + 初级分析与检测 + 应急响应’的发展阶段，重人工轻流程、重定制化轻标准化等发展问题逐渐显现，我们需要更具本土特色、更符合业务需求的安全托管服务。

奇安信 MSS 安全托管服务的不断围绕政企客户的需求进行改进，已形成“两种模式、三种形态、两化融合”的具有中国特色的安全托管服务模式。其中，两种模式即直接服务模式与合作伙伴模式，直接服务通过奇安信“MSS+”的模式，联合奇安信 NGSOC、天眼、天擎等产品，形成“组合拳”，构筑整体的安全托管服务；合作伙伴模式是奇安信通过整体的技术体系、产品体系、服务体系的整合托管模式输出，形成企业安全运营中心、行业安全运营中心及城市运营中心，输出能力、集约化服务。在各类运营中心中，面向主管部门和总部机构的监管需求形成“集中服务化”，统一监测、预警与通报。各所属机构在其中存在的服务需求，可运用共享服务的理念，利用运营中心将各单位的需求进行“服务集中化”予以提供，具有服务标准统一、服务质量可控、资源高效利用等优势。

国内政企用户在选择 MSS 服务商时，应从自身实际情况出发，重点关注整体服务能力、咨询服务能力、人才、创新和生态合作等方面。同时，服务提供商应更加注重服务工具的智能化、自动化、服务内容的标准化、服务人才的专业化、专业知识的流程化、服务生态的规模化等内容，真正帮助用户降本增效，从而做大中国托管安全服务市场的蛋糕，最终实现用户与厂商的双赢。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

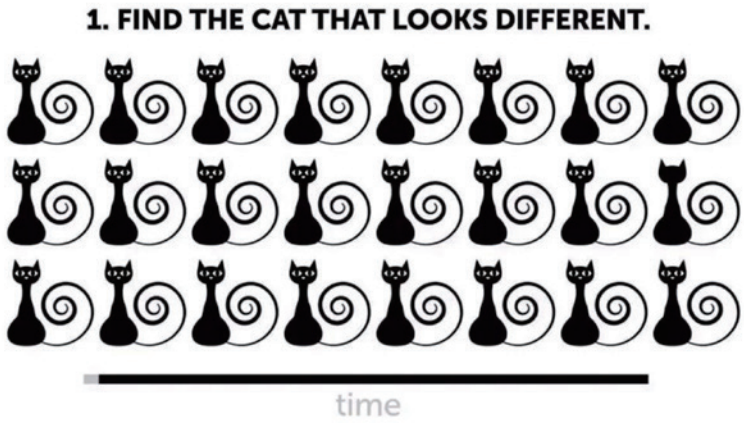
扫码购书

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。

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

作者 公关部 魏开元

猫大家都认识吧！那我们不妨来回答一下这个陌生而又熟悉的问题，请从下图中找出不一样的猫。（不熟悉的读者可以回看《灵魂拷问：如何把网络攻击从数百万合法行为里抓出来？》）



细心的朋友可能很快就发现，第二排最后一只猫没有眼睛，用时都不到一秒。

但问题来了，毕竟这只是 3x8 的矩阵，如果这里有几万只甚至几百万只猫呢？怎么才能找到不一样的那只？

想要解决这个问题，首先得有一个标准，换个高大上的词来说就是基线。

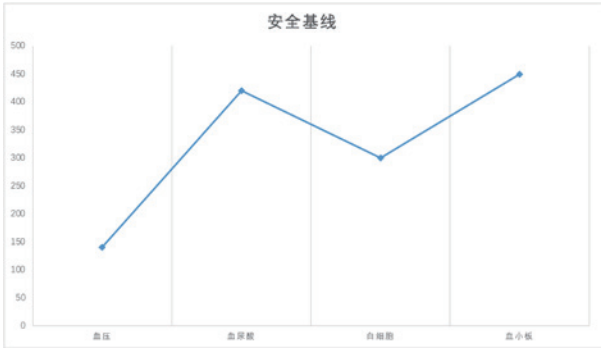
如果觉得猫不够熟悉，那换个话题，什么人才不是正常人？

有人肯定会说，长了三只眼睛的肯定不是正常人，应该是二郎神。此话有理，但恐怕这个世界上 99.99% 的人，一辈子都没见过谁长三只眼。如果用这个或者一组类似的标准来判断，全世界怕是没几个不正常的。

但有一类人肯定对这个问题很有感觉，他们一项很重要的工作就是告诉别人你是不是有病，这类人叫作医生。

关于如何判断就诊人员是否患有某些疾病，很多国家和地区的卫生组织都发布了自己的标准：比如，在中国，舒张压大于等于 90 或者收缩压大于等于 140（单位：毫米汞柱）就被认为是高血压，对脏器会产生明显危害；非同日两次空腹血尿酸水平，男性大于 416.5umol/L，女性大于 357umol/L 即可诊断高尿酸血症，痛风概率就非常大了。

我们可以把所有的这些标准给串起来，这条线就叫作生命健康的安全基线。凡是在超出了安全基线的，或



多或少都有点“毛病”。

那么问题来了，安全基线到底是怎么来的呢?

有一点可以肯定，这是长期的诊疗实践再加上科学研究得出来的结果。

所幸的是，人与人之间的差距并不算大。无论是东方人还是西方人，血压长期 180 都是有可能猝死的；无论男人女人，BMI 超过 30，怎么着也不会是个瘦子；无论大人小孩，体温 39 度都不会舒服。

但很多时候并不是这样，尤其是信息系统。某国内知名电商网站单日访客量破亿稀松平常，但大多数企业官网一年都很难达到，要是达到了，作为网管就得考虑是不是被攻击而出现了大量的恶意访问。这就好比你在闹市区里开 120 公里 / 时和在跨省高速上开 120 公里 / 时，交警对你的态度肯定不一样。

给每个信息系统画一条安全基线，是奇安信态势感知与安全运营平台（NGSOC）基线引擎最重要的任务，对于检查信息系统是否“有病”至关重要。这就像规定了一条跑道，信息系统一旦跑过线就犯规了。

公交车老司机

与田径赛场上的跑道不同，安全基线并不是笔直或者椭圆形的那么有规则，设计起来还颇有点难度。

设计基线的方法大概有以下几种。

假设你是一名公交车老司机，疫情期间你发现经常有学生党、上班族因赶时间而忘记戴口罩。出于好心，你决定发起“口罩工程”，自掏腰包在车上准备一些口罩，免费给那些忘记的人使用，免得他们还得跑回去取，耽误行程。

但口罩数量毕竟有限，为了让真正的乘客使用，你制定了一个规则：乘车才能使用，不乘车不可以。

刚开始一切正常。但很快口罩就从最开始的平均消耗一两个，变成了后来的一天能送出去十多个。这让老司机颇为不解，怎么记性不好的人越来越多。经过一段时间的仔细观察，老司机发现原来是有人故意不戴口罩就等着上车拿。由于很难确定到底谁是故意的，于是老司机决定每天限量供应五个。

这就是统计类安全基线，它主要来自长期的数据统计和机器学习。一旦一段时间内的平均数值明显高于或者低于统计结果，就可能出现问题了。

限量规则的实施，使得那些投机不戴口罩的数量随之大幅减少，大家都很担心自己成为第六个或者之后的人。但很快老司机又发现了一个问题，下午要口罩的人明显增多。通常而言，忘带口罩的人多出现在早晨 8:00–9:00 上班或者上学高峰，下午则几乎没有。几经调查老司机发现，由于免费口罩需求量减少，到下午仍有剩余，因此开始出现了下午来“免费蹭口罩”的人群。于是老司机又决定，非早高峰时间限量两个。

这就产生了序列类安全基线，它有明显的时间先后顺序或者周期性。一旦事件发生明显偏离了预定的先后顺序或者违背了周期规律，则会判定为异常。

一段时间后，老司机逐渐和那些忘带口罩的人混了个脸熟。他发现，经常忘戴口罩的总是那么几个。尽管一个口罩值不了多少钱，但为了帮助这些经常忘记戴口罩的人养成好习惯，老司机决定凡是在他脑袋里挂了号的人，以后再领口罩时，就象征性的收五毛钱口罩费，让他们在出门前想想今天是不是戴口罩了。

老司机人工学习（机器学习）出了忘记带口罩人的

特点并完成聚类，就产生了机器学习类安全基线。

经过老司机几个月的实践，口罩工程基本走上了正轨。在这个过程中，他使用的统计类安全基线、序列类安全基线和机器学习类安全基线，就是网络安全检测与分析中使用最为广泛的三类安全基线。

实时计算

相比之下，网络安全分析要复杂的多。

首先需要快速的响应。说简单点，安全检测其实就是把发生的事件与安全基线进行比对，找出异常。由于安全事件经常是突发的，而且发现和处理的速度越快损失就会越低，这就意味着需要用一种简单快速的方式，快速生成安全基线，并与突发的安全事件进行比对。反观老司机可以无所谓，无非就是多发几个口罩。

其次是场景定制。作为学生党或者上班族，每天上班的时间、线路都相对比较固定，对于老司机而言大家都差不多。但安全分析不同，它的对象有数据、时间、流量、文件甚至还有很多安全领域独有的一些需求，所以定制开发很常见。

第三是资源受限。没有谁的资源是无穷无尽的，在预算有限的情况下，计算、存储、带宽这些资源要优先保证组织自身业务的正常开展，别像某一码通隔三差五就被搞宕机了，被上级有关部门要求扩容。因此，网络安全分析要在确保性能的基础上，尽可能更少的占用资源。例如老司机，虽说一天也能拉上千个乘客，但每天最多就发五个口罩。

基于上述特点，NGSOC 安全基线引擎就必须具备强大的实时计算能力，说白了就是左边输入数据，右边就能输出结果，同时还不能占用太多资源，支持定制化开发。

这里解释一个概念。

如果按照时效来分类，计算类型主要包括实时计算和延迟计算。所谓的延迟计算就是指在某一时间点，对过去的某一段时间内发生的事件、产生的数据进行计算。老司机的做法就是一种典型的延迟计算，过一段时间会对之前的口罩发放情况进行总结。

实时计算则是指能够在事件发生的同时，快速统计并输出检测结果。对于 IT 系统而言，事件会持续发生，比如，防火墙会不停的过滤数据包，公司的办公系统会不停地被访问，因此事件是无穷无尽的。这就像地铁安检系统，只要乘客经过安检系统，实时的影像就已经在电脑上显示出来了。如果地铁安检也搞延迟计算那一套，整个地铁站还不堵成一锅粥了。

那么有没有什么技术可以实现这些要求呢?

“还记得在 2018 年的时候，我们比较了很多技术栈，最终选择了 Apache Flink 作为实时计算框架。基于这个开源框架，我们设计出了国内首款分布式关联分析引擎 Sabre 和安全基线引擎。”

说这句话的人是奇安信 NGSOC 基线引擎负责人覃永靖，一名深耕大数据安全检测领域多年的高级技术专家。

毫不夸张地说，Flink 是时下最流行的数据计算框架之一。

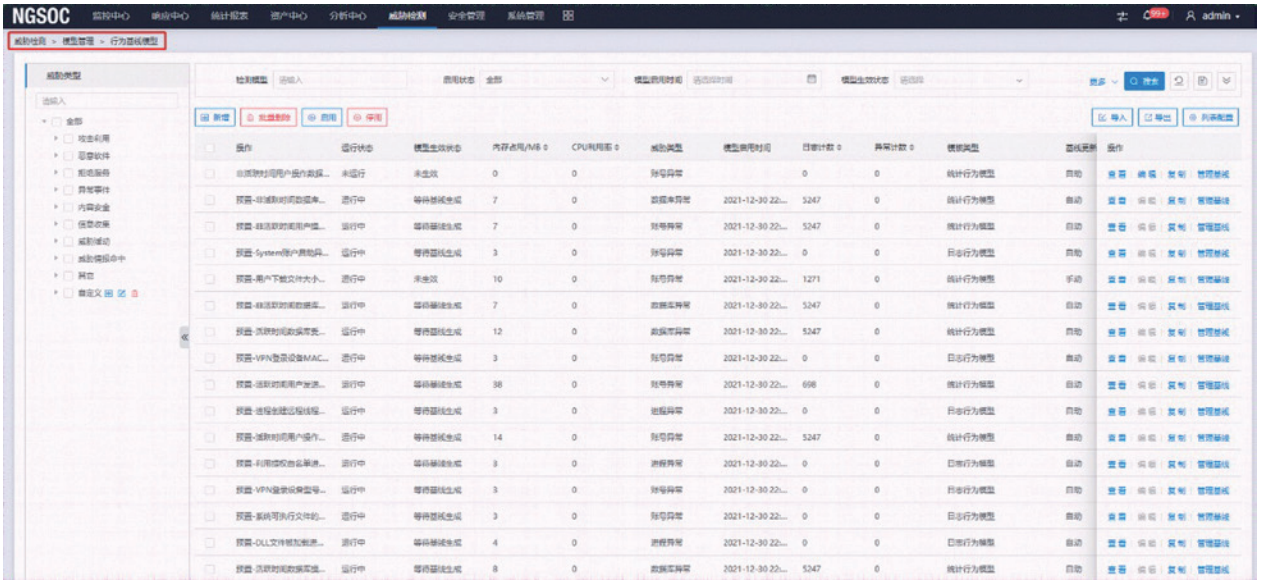
事实上，Flink 最开始并不叫 Flink，它的前身是 Stratosphere，中文翻译是平流层，位于离地表 10 千米至 50 千米的高度。当然最开始也不属于 Apache，而是由一群技术宅在开发完成后，于 2014 年捐献给 Apache 基金会的。

说到这儿，或许 Flink 的诞生与平流层通信有着密切的关系。与卫星通信相比，平流层通信的极低延迟正是开发者追求的目标。

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。正是这个特点，Flink 让实时计算从“奢侈品”变成了“日用品”。想象一下大量工业制品在多条流水线上“奔跑”的样子，而 Flink 就是在数据流水线上的自动化生产机器。

安全基线引擎

不过直接把 Flink 拿过来，离覃永靖脑海中的实时



感受一下基线数量（基线引擎后台部分基线截图）

基线引擎还差的很远。

至于差在哪，先看基线引擎最常见的三个实战案例。

第一种是数据库管理员（DBA）账户登录异常，基线引擎可以学习 DBA 账户的登录习惯，比如，当账户登录位置偏离了常见的登录位置时，就反馈为异常登录，账户有可能被盗用。

第二种是邮件异常，基线引擎可以学习某一个用户或者是整个组织的收发邮件行为，例如，当用户邮件数量或者附件数量远远超出历史学习水平，则邮件系统可能正被控，制对外发送大量垃圾邮件。这个时候组织可以用设置邮件发送数量上限来达到限制的目的。

第三种是 VPN 账户异常，基线引擎可以学习用户登录 VPN 服务的次数和登录 VPN 后的行为（如访问哪些系统、做了什么操作等），一旦检测到用户登录行为和学习结果有出入，例如，在敏感时间访问了某些敏感数据，则可能 VPN 账户已被入侵或者出现了内鬼。

这三个实战案例首先讲述了一个事实：在安全检测的场景中，Flink 框架上可能同时运行着大量的安全基线。然而，它并没有针对大规模语义和规则进行优化，直接拿过来用可能根本无法同时跑起来这么多基线，大多数情况下上超过 100 条 SQL 语句系统就得“罢工了”。

这显然无法满足安全分析的需求。更无奈的是，Flink 的使用和调优门槛非常高。

这里再普及一个知识。基线的生成分为三个阶段。第一阶段是学习阶段，在这一段时间内基线引擎的任务就是不断学习数据；在学习阶段结束后，系统往往会设置一段等待时间，在等待的时间里，基线不再学习新的数据，可以投入安全检测，也可以不投入；等待时间结束后，基线就会全面投入到安全检测中，直到这条基线被删除或者失效。

需要注意的是，从基线引擎学习完毕到基线正式投入使用，这两个阶段之间还需要经过一个编译的过程。打个比方，部队集结完毕之后直接拉上战场肯定是不行的，上级首长需要一点点把任务布置下来，再由分队主官把任务分解给每一名士兵，否则还不全都乱套了。

Flink 难就难在这里。

这个过程难到什么程度呢？大概类比一下，差不多和电脑小白用户抛弃 Windows 桌面操作系统去使用

DOS 命令差不多。你想执行个什么操作，光靠鼠标还不行，得编写好长一段代码。但很多时候，用户根本就没有太多开发经验，只会启用规则、停用规则、看报警之类的。

“这肯定不行，我们的初衷应该是用户想象中该怎么用，系统就该怎么用。”覃永靖说到。

所以基线引擎引入了一个特殊的组件 DSL，全称 Domain Specific Language，中文翻译成领域专用语言。这里的 DSL 主要是相对于通用机器语言，如 Python、C++ 等，特地用于安全分析领域。

很明显，DSL 就是专门给安全分析人员用的。

DSL 提供了一个非常友好的使用界面，能够以极短的代码来表达复杂的语义，并且支持的语义数量十分丰富。语义下发后，编译器能够快速编译成一条规则，从而首先解决了简单易用的问题。

除此之外，DSL 还很大程度上解决了性能的问题。

DSL 编译器在给基线布置任务的同时，会对公共表达式也就是任务进行优化，从而降低资源占用。比如，有 500 个分析场景，这 500 个分析场景很可能会使用相同的计算公式，还要同时处理大量的威胁情报数据，此时就需要支持对公共表达式的优化，同样的任务不用为每一条基线都布置一次。这样一来，在有限的资源下，引擎就可以同时运行更多数量的安全基线。

“矫情的”基线

基线运行起来也不是就万事大吉了。作为指挥官，除了要时刻关注检测结果，还要关注士兵的作战状态。

因此基线引擎需要重点关注两个方面：第一是基线的资源消耗情况，第二是基线自身还能不能满足安全检测的需要。

首先，基线引擎的运行要保证稳定性，保证稳定性的根本就在于资源。俗话说兵马未动粮草先行，如果说基线是作战的士兵，那么 CPU、内存、带宽这些资源就是粮食弹药了。粮食弹药不足，军心必乱。当年袁绍七十万大军，就因屯粮的乌巢被袭占，而在官渡之战中输给了兵力只有其十分之一的曹操。

假如基线引擎同时运行了几十上百个基线，如果发现某一条基线的资源占用大大超出预估，那么就需要对它采取保护性措施，把它隔离出来或者干脆删除这条基线，防止它影响其他基线的运行。

覃永靖解释说，我们的基线引擎提供了资源保护机制，会根据安全检测的重要性顺序，为用户提供优先级管理，如果基线的优先级本身比较低，但是却占用了大量的资源，就应该适当削减资源分配甚至停用。

其次，基线本身并不是一成不变的，业务系统的变化必然导致基线也随之需要更改。举个例子，有安全研究表明，近些年来，人们的平均体温在逐年降低，若干年后如果再用大于等于 37.3℃这个标准来判断是否发热，可能就不合适了，基线标准也要适时调整。

但基线在运行过程中要实现在线编辑，并不是一件非常容易的事情，搞不好就容易出错，出错的点就在于如何把修改成功的基线再发送到对应的节点上去。很多人都看过类似的剧情：一名士兵在受伤后被送到战地医院救治，出院后就找不到自己的队伍了。

因此，基线引擎设计了一套“路由机制”，它支持全局基线更新流图，能够在基线更改之后实现精确基线数据分发。

作为奇安信 NGSOC 的核心能力，关联分析引擎、安全基线引擎提供的实时安全分析能力，不知道打败了多少丧心病狂的黑客。

还有值得一提的是，这个引擎并不是 NGSOC 独享的，它目前正服务于公司大部分大数据产品，比如，大数据与安全运营平台、态势感知、EDR、云安全、工业互联网安全、智能安全等，并随着这些产品服务了不计其数的客户。

从一到几百台集群规模，从几百到上百万 EPS 的安全事件，在成千上万的实战中，它见证了光。安

PS：2022 年 1 月 8-9 日，Flink Forward Asia 2021 线上举办，以上内容根据覃永靖在会上分享的《如何设计信息安全领域的实时安全基线引擎》议题整理。

规划一步 快一步

奇安信 | BEIJING 2022

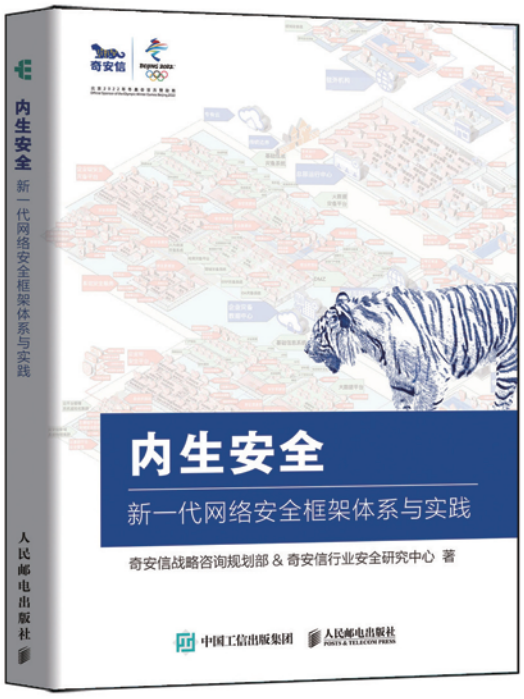
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

新书发布

内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍



- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

十年“四级跳”
中国电建如何打造网络安全的“眼手脑”

作者 公关部 张少波

午夜两点，某攻击组织利用一个 0day 漏洞攻入企业内网，正欲进行横向渗透，此时，触发报警，迅速被防火墙、终端 EDR 等联合阻断拦截，并被溯源锁定，整个防护一气呵成、密不透风，攻击完败！ 这个不需要人工干预响应的智能化网络安全防护，是中国电力建设集团有限公司（以下简称“中国电建”）正在构建的整体防御体系。

在中国电建看来，网络安全需要“眼、脑、手”并用，应具备一定的 AI 水平，可以在不依赖人的条件下，迅速完成检测发现、阻断拦截、溯源分析等防护措施。

中国电建成立于 2011 年，是全球清洁低碳能源、水资源与环境建设领域的引领者，服务“一带一路”建设的龙头企业。2021 年《财富》世界 500 强企业第 107 位。

中国电建是国有资产监督管理委员会直接管理的中央企业，拥有 63 家二级单位，业务涉及水利电力工程及基础设施投融资、规划设计、工程施工、装备制造、运营管理等，引用中国电建董事长丁焰章的一句话说，就是“懂水熟电、擅规划设计、长施工建造、能投资运营”。

在“云大物移智”等新技术风起云涌的数字时代，中国电建的数字化转型走在了前列，借助数字技术不断提升企业的精益化生产、数字化建造、现代化管理和智

能化决策能力。在这个过程中，网络安全的重要性日益凸显，中国电建始终将网络安全作为数字化转型的底板工程，其中包括通过部署以奇安信态势感知与运营平台（NGSOC）为基础的“电建眼”，实现了从传统防护到主动对抗检测的跨越，为打造国资、国企一体化网络安全保障体系奠定基石。

一次域名事件推动中国电建从基础安全到纵深防御

中国电建集团成立之初，网络安全就已经同步推进。据中国电建信息化管理部副主任王海涛介绍，电建的网络安全建设可以分为四个阶段，其中，第一阶段是 2011 年到 2013 年，旨在为集团构筑网络安全基础能力。该阶段，电建按照“急用先行”原则，围绕网络终端开展了主机安全、防病毒、主机加固、防篡改等安全能力的建设。

这些防护应对一些日常的黑客、病毒攻击游刃有余，但面对有组织、有预谋的复杂攻击，还显得有些力不从心。

“网络攻击曾给我们造成过切身之痛。” 王海涛回忆道。“大约在 2014 年北京 APEC 会议期间，我正在西安出差，突然接到电话，说网站被篡改了，替换成了不良图片，影响非常恶劣。当天晚上，我就改变行程飞回北京紧急处理。”

“经排查，有一个域名被黑客篡改，导致该域名下的网站出现故障。我们自身团队通过各种措施都未能解决，最终找到了奇安信安服团队，借助后者提供的 DNS 解析故障修复方案，确保域名不被污染，官网很快恢复了正常，问题得以彻底解决。”王海涛表示：“可以看出，网络安全是一项非常专业的工作，仅依靠被动防守措施和自身安全力量还不够。”

2014 年到 2016 年，中国电建跨入了第二阶段，即大规模建设阶段：一方面是从管理的角度，完善组织机构，包括搭建领导机构，进行人员意识培训管理提升等；另一方面，就是从技术角度，建设纵深防御的技防体系，包括：系统安全、应用安全、身份安全、数据安全、边界安全和分权分域等。

自此，中国电建已经建成了从管理到技术的大纵深防御体系，极大提升了集团信息化平台的网络安全能力。

纵深防御难以应对高级威胁“电建眼”应运而生

自国内安全机构捕获海莲花 APT 组织攻击后，2016 年开始，各类 APT（高级可持续威胁）屡次被发现，给政府、央企机构造成极大威胁，也给被动防护为主的纵深防御体系带来了新挑战。

王海涛表示，当时中国电建已完成了纵深防御的部署，安全能力得到显著提升，但实际运行中还存在五大方面问题：资产烦多难管理、运维数据巨大、威胁发现能力不足、安全威胁不可见、缺乏联动防御等。加上《‘十三五’国家信息化规划》中重点强调了网络安全攻防的全面性，以及对动态网络安全的全天候全方位的态势感知能力，因此，构建积极主动的防御体系，被中国电建提上了日程。

从 2017 年起，中国电建迈入第三阶段，即精细化管理与运维阶段。该阶段充分采用云计算、大数据、态势感知和威胁情报等新技术，强化新 IT 环境下的安全防护和态势感知能力建设，提高网络安全的精细化管理水平。

为了在网络攻防对抗中变被动为主动，中国电建在符合国家要求、集团规划的前提下，建立威胁可知、威胁可查、应急可控、服务可靠、管控可视的大数据预警监测分析及防御系统，即“电建眼”平台。

具体实现上，“电建眼”以态势感知与安全运营平台（NGSOC）为核心，汇集各类数据，包括原始流量日志、安全设备日志、系统日志、终端日志等，利用流量检测引擎、关联分析引擎、威胁情报等技术手段对政企内部网络进行持续安全监测。发现安全事件后，可进行研判及溯源，同时可通过 NGSOC 与 EDR/NDR 联动机制及专家服务对事件进行及时响应处置，实现安全运营能力的落地。

可以说，“电建眼”完成了从威胁发现、研判、分析溯源到响应处置的安全业务闭环，从而助力中国电建从纵深防御迈向主动防御阶段。

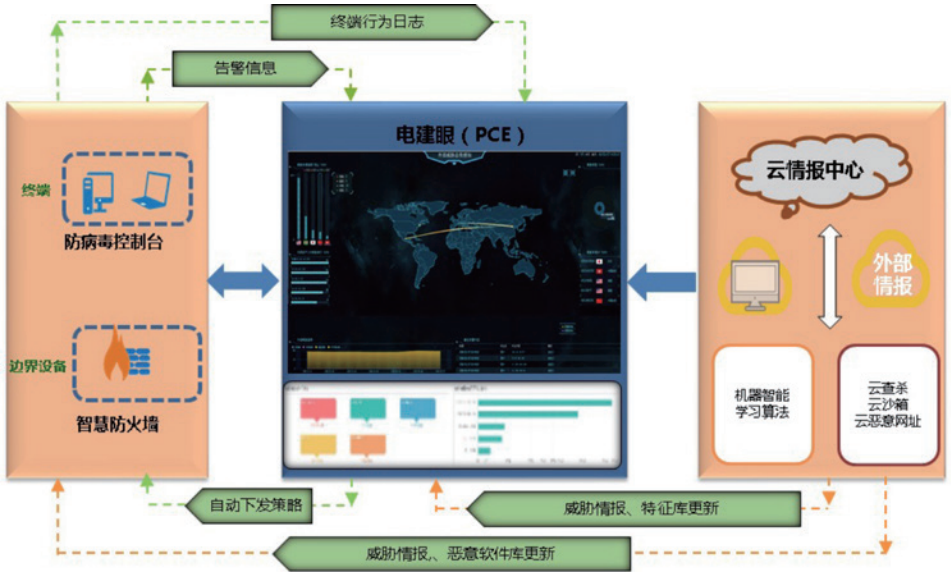
“眼脑手”联动实现五大能力 并向集团分支机构普及

目前，以 NGSOC 为基础的电建眼，已经在中国电建总部顺利实施，逐步构建了 IT 资产管理能力、安全大数据整合能力、智能分析与回溯能力、安全威胁可视化能力、协同防御联动能力等五大能力。并在 2018 年的数博会上，获得了“大数据安全优秀案例”及中国信息协会颁发的“电力企业信息安全管理创新成果三等奖”。

王海涛用“眼脑手”来形象的比喻中国电建的技术防护体系。“眼”主要指全方位的监控和检测能力。即需要“眼观六路”，知道攻击者“在哪儿干”“谁在干”“干了啥”“啥结果”。例如，生产系统、客户系统、供应链系统、财务系统哪里受到攻击，攻击者的身份和行为是谁，造成什么结果等。这项工作主要由“电建眼”来完成。

“脑”主要指多维度的分析。由“智慧中枢”来完成，它主要完成用户风险分析，行为风险分析、事后调查取证，实现分析溯源等，为响应处置提供指挥决策基础。这项工作既需要机器来自动化分析处理、直观可视展现，更依赖于安全运维、分析师的日常处置和分析研判，以及安全负责人和领导的指挥决策。

“手”体现以最快速的响应和执行。一旦发现攻击，准确分析和定位之后，能够以最短时间阻断攻击，并实现应急响应，将损失降至最低。该项工作需要由终端安全天擎、边界安全防火墙组成的电建盾来完成，通过协同联动实现纵深防护。



概括来说，电建眼负责看见威胁，大脑通过分析研判来揪出威胁，最终由电建盾阻断威胁，实现全天候、全方位的感知网络安全态势，形成“人 + 机 + 服务” 的主动防御体系，提升整体安全综合能力。

“眼脑手”联动能力的实现，标志着中国电建已经完成网络安全建设的

第四阶段：针对新 IT 环境安全防护风险态势感知。

中国电建集团邀请了公安部网络安全保卫局、国资委综合局、国家能源局安监司、工信部国家工业信息安全发展研究中心、公安部一所网络攻防实验室五个部委单位网络安全专家对“电建眼”项目进行了评审，专家组对项目取得的成果高度肯定，并一致认为电建眼的建设模式和应用实效在行业内，乃至央企范围内具有典型性和示范性，同意通过验收。

此后，为全面落实中央、国务院关于增强国企抗风险能力和保障国家安全的决策部署，中国电建按照“成员单位自身感知、数据本地采集、集团统一汇总、集中监控上报”的原则，逐步覆盖完成成员单位侧电建眼网络安全态势感知系统建设，并将成员单位本地采集数据上报至集团“电建眼”平台，实现数据统一汇总。集团总部“电建眼”平台按照《国资国企网络信息安全在线监管平台企业侧技术规范》要求的接口标准进行改造后，与集团总部本地部署的在线监管平台对接融合，向国资委监管平台上报所需数据，实现信息情报共享。由此，“电建眼”平台发挥了统一采集、统一上报、统一监测的关键作用。

电建眼在实战中屡立奇功 未来重点是增强 AI 能力

实战是效果的最好检验。在最近几年的实战攻防演习中，电建眼立下了赫赫战功，有 70%~80% 的攻击行为，都是由电建眼第一时间检测发现并告警，继而协同联动其他产品进行拦截，这也使得中国电建在连续 3 年实战攻防演习中，都取得了优异成绩。

“安全工作，永远在路上。”王海涛表示，“针对攻击手段日新月异的外部严峻环境，中国电建希望电建眼融入更多的 AI 能力，逐渐减少在实战攻防中对于人的过度依赖。尤其在流量和日志的数据分析方面，运用更多的机器学习、人工智能等技术，实现基于机器的分析研判，从而实现无人操控的‘眼脑手’联动。”

对于中国电建网络安全建设的当下和未来任务，王海涛表示，“目前电建眼已经完成了二级单位的全覆盖，未来 2~3 年将逐步下钻到更多成员单位和项目部，从而形成集团立体式的网络安全态势感知体系，补齐分支单位的安全短板，提升全集团的整体主动防御能力，保障数字化转型行稳致远。安

万物之中，理想至美

——走近奇安信华南基地负责人徐贵斌

作者 公关部 孙丽芳

候鸟南飞又北归。

而徐贵斌自从 2017 年带领奇安信的一支研发团队驻扎珠海，一去未归，如今已进入第五个年头。

君问归期未有期。

要知归期，还要先从这次迁徙的起因，从徐贵斌斯人说起。

徐贵斌，75 年生人，著名反黑工具“狙剑”的作者，资深网络安全从业者，奇安信副总裁、华南基地负责人。

“喧宾夺主”的副业

中国网络安全行业的发展历史并不很长，徐贵斌几乎全程参与，但入行纯属偶然。

“我所处的年代，电脑正从单机时代向互联网时代转换，各种问题特别多。我当时在做校园网络，也销售一些硬件。客户的机器都装过一套甚至是多套杀毒软件，但还是屡屡中招，于是频频找我们。虽然不是我们的问题，但客户有需求我们肯定还是要尽力去解决。做售后的时候，我就发现，面对各种攻击，当时的杀毒软件根本解决不了问题，只能借助各种工具，去帮客户手动处理。那个时代各种工具层出不穷，公司的、个人的。”

徐贵斌所说的是 2000 年左右，传统的杀毒软件沿用杀毒引擎 + 特征码的技术，20 年没有创新，已经不能有效解决互联网的安全问题。市场的安全需求和实际安全产品的供应差距很大。

本来的主业是搭网、卖货，副业是修电脑，但后来，找徐贵斌解决网络安全方面问题的客户越来越多。徐贵斌的副业逐渐“喧宾夺主”。再后来，徐贵斌写出了功能强大的安全反黑工具——“狙剑”。它可以提供系统监视、进程管理、磁盘文件管理、注册表检查、内核检查等多个功能，从而方便地手工查杀木马。

“狙剑”一经推出，很快就在圈内打响了名气。徐贵斌对此却表现得谦逊而坦诚。“狙剑的创造性并不是很强，更多的是对过往大家群体经验的汇总。当时民间的技术氛围很浓，很多技术都是大家讨论出来的，也有借鉴国外的，但都是散点。而安全不是解决某个点的问题，

我把各个技术点汇总到了一起，就形成了一个综合性的工具。”

更大更专业的舞台

通过编写“狙剑”，徐贵斌展现出卓越的技术才能，他就此进入了专业的安全公司，也在那里遇到了自己的伯乐，彻底投身网络安全事业。

“2008 年，我就成为了齐总的部下”。

以前单打独斗，仅凭个人兴趣和个人能力兼职做网络安全的徐贵斌，拥有了更大更专业的舞台。

对此，奇安信集团董事长齐向东在自己的专著《漏洞》中有专门的记述。“徐贵斌刚加入公司时，被安排在查杀组，他的能力在团队中很快得到了凸显。比如，在 2008 年，我们推出的系统急救箱就是徐贵斌带领团队开发出来的。这只是徐贵斌能力的冰山一角。更重要的是，他领导查杀部门，把公司的查杀能力提升了一个大台阶。简单来说，当时业内主要是基于病毒库来扫描查杀木马病毒，也就是俗称的‘黑名单’机制。但我们创新推出了以‘查白’为核心的网络安全技术，应用了搜索引擎、云技术、人工智能等互联网技术，攻克了黑名单瞬息万变不可捕捉的难题，积累了比较全面的白名单样本数据库。”

有了领导的支持和团队的助力，徐贵斌大展拳脚。“在 2000-2006 年期间，电脑带毒运行是常态。而在那之后的两三年时间内，我们就把绝大多数安全问题都解决了，个人电脑中毒成了小概率事件。”

在之后很长的一段时间，网络安全江湖有些波澜不惊，守方的力量似乎稳稳占据了上风。

真实的情况是这样吗?

一计重重的耳光

2017 年 5 月 12 日，“WannaCry”勒索病毒在全球爆发，波及 150 多个国家和地区、10 多万个组织和机构，以及 30 多万台电脑，损失总计高达 500 多亿人民币。众多医院、教育机构及政府部门遭受攻击。

这次病毒感染事件突发性强、波及面广，在全球范围内引起巨大恐慌，也给网络信息安全尤其是关键信息基础设施行业的网络信息安全敲响了警钟，把所有人都拉回了现实。

网络安全江湖外表波澜不惊，实则暗流涌动，因为 0day 漏洞始终存在。

此次勒索病毒之所以造成严重损失，一个重要原因是美国国家安全局的“永恒之蓝”网络武器流入民间，被黑客利用，使勒索病毒可以“蠕虫式”传播。

面对这样的现实，徐贵斌毫不讳言。“这是给整个网络安全行业一计重重的耳光。作为在网络行业从业多年的资深技术人员，我觉得挺丢人的。面对这种级别的网络武器的攻击，网络安全行业没有发挥任何作用，很多只能断网。”

即便如此，危急时刻，网安人还是竭尽全力。“永恒之蓝”勒索病毒爆发之后，我国有关部门迅速组建了应急指挥部，奇安信担任总指挥，利用自己在安全大数据和态势感知领域的优势，很快推出了“永恒之蓝”勒索蠕虫传播专项态势感知，并以此为基础建立了应急响应体系，先后派出了超过 2000 位安全应急响应人员，为超过 1700 家政企机构提供了现场支持。

虽然奇安信在“永恒之蓝”一役中表现优异，但董事长齐向东认为，问题并没有真正被彻底解决。“永恒之蓝”只是美国国家安全局众多网络武器之一，面对这种级别的网络武器，传统安全防护技术已经失灵。网络被彻底打开，传统边界属性改变，传统的 IT 安全架构已经跟不上时代的发展，需要探索全新的安全解决方案。

现实印证了齐向东的观点，在这一年中，继“永恒之蓝”席卷全球之后， NSA/CIA 等核武器级网络军火库持续“失火”引起恐慌。从操作系统到应用软件，从 Web 容器到服务插件，各种 0day 漏洞应接不暇。总之，

2017 年的网络安全，用“多灾多难”来形容，绝不为过。

当然，事物总有双面性。在历史性经历过这些安全大事件之后，上到国家，下至民众，开始对网络安全这个行业投入更多关注。2017 年 6 月，我国的《网络安全法》终于颁发。也是在 2017 年，奇安信做出了一个重要的战略决定。

珠穆朗玛峰级的问题

2017 年 7 月，奇安信在珠海设立华南基地，“天狗漏洞攻击防护系统”正式立项。目标：基于内存指令调用序列检测技术解决 0day 漏洞攻击问题。

南下带队开展这项工作的，正是徐贵斌。

“天狗要解决最新的网络攻击问题，对标的就是‘永恒之蓝’这个级别的 0day。”

“已知漏洞”的问题容易解决，是因为我们明确的知道漏洞存在于哪一个文件、哪一个函数的哪一条指令中。而“未知的 0day 漏洞”难以解决，是因为它有可能存在于任一文件或服务的、任一函数与指令中，已知未知，天差地远。

很显然，天狗想解决的是网络安全领域珠穆朗玛峰级的问题。

“我们核心是利用机器学习与智能采集技术，学习并采集系统中所有可能存在被利用风险的程序的指令序列，并构造成‘指令序列白名单’，当实际在内存中执行的任意一条指令序列不在白名单中时，即认为是非原生的额外出现的异常攻击指令。0day 漏洞的确是未知的，但系统及程序却是已知的，利用已知发现未知，是可行的。”

理论上虽然可行，但要实践验证可行，并最终产品化，还有漫长的路。徐贵斌就这样扎在了珠海，越来越多致力于这一研究方向的小伙伴聚到了他的周围。

“我一直觉得我就是搞技术的，我绝大多数精力都放在技术上。‘天狗’是我一手设计的，我也亲自做验证。虽然我也做管理，但更多是聚一帮人，大家一起想解决高精尖的问题。”

这帮人夜以继日，埋头一干就是两年。2019 年，“天狗”完成了工程化，开始在华为做试点。

同为技术公司，华为对合作方的选择一向以严苛著称，为什么愿意当“天狗”的试验田?

“华为是一家很专业的公司，它对技术的要求很直接，就是要解决来自国家级的网络攻击。而 2017 年‘永恒之蓝’把所有安全公司全部打穿，想找一款能应对 0day 攻击的产品，除了‘天狗’，别无选择。所以，即使是我们第一个客户，华为也愿意。华为的安全系统搭建的非常完善。作为一家国际化的公司，华为在全球都有分支机构，‘天狗’也随之部署到了全球。”

试点结束，徐贵斌团队对试点工作情况进行了总结。依据华为提供的数据，试点期间，其分布在世界各地的

办公网络、内部网络、生产系统遭受到来自全球的攻击，有 60% 的攻击是“天狗”独立发现的。

“华为的试点情况非常好，‘天狗’的有效性得到了检验。之后，我们继续扩大试点范围，在多家客户超过 50 万 + 的终端和服务器上进行了超过 2 年的部署。稳定性和兼容性，以及包括对性能的影响问题都已解决。”

一战成名的“天狗”

奇安信投入 300 多人，历经 3 年自主研发的全新一代安全技术——“天狗漏洞攻击防护系统”，最终取得了 200 多项技术专利，将安全技术带入内存指令检测的时代。

“天狗”在面对 0day 漏洞、可信程序被恶意利用，以及后门的检测方面，都有显著的防护效果。在 2021 年年底的 Log4j 漏洞事件中，“天狗”一战成名。

“我们进行了漏洞影响验证，包括所有客户，发现 2021 年 10 月发布的天狗 -JAVA，完全不受该漏洞的影响。”

无需更新就能直接防御 Log4j 漏洞，要归功于“天狗”引擎的技术特点。

基于内存指令层的漏洞攻击检测技术，脱离了传统上对具体漏洞特征、文件特征、行为特征的依赖。因不依赖于特征，才不需要更新特征，这是专为应对 0day 漏洞攻击而生的技术。

尽管“天狗”技术已经在全球处于领先地位，但徐贵斌不敢有任何松懈。

“此前只是完成了工程化，但还需要继续完成新技术的产品化。面对华为这种对技术很了解的公司，大家就很契合。但是还有很多别的公司，技术和需求无法建立联系，怎么让技术在具体的用户场景下发挥作用，这就需要对技术进行产品化。这也是我们 2022 年的核心工作内容。Log4j 漏洞事件后，主动了解‘天狗’的客户突然激增。为此我们将原本计划 2022 年 Q2 上线的天狗 JAVA 漏洞攻击防护系统提前到了 Q1 发布。”

理想主义的光芒

从 2017 年的毅然南下，到 2022 年的上市发布，一路走来，徐贵斌感慨良多。

“搞技术最怕的就是领导的不信任。做创新研究存在成功率的问题，可能投入很多但没有结果。很多人有想法，做不出来，不是能力问题，是没有人愿意持续给他投入。我们 2017 年立项，2019 年试点，到 2022 年是第五年，每年都有大量投入。齐总给予了我们极大的信任。一方面这是因为我们有十几年合作的基础。更重要的是齐总对集团目标定的足够高。我们没有把自己仅仅定位于和国内厂商竞争，我们是要成为世界上最强、最大的网络安全公司。所以，我们愿意投入时间、精力、成本去研究世界前沿的技术，去进行面向未来的研发，这必然会承担更多的风险。”

齐向东的信任徐贵斌非常珍视，而对自己的这名爱将，齐向东也由衷地肯定：“奇安信新一代网络安全技术体系的突破和实践中，徐贵斌做出了不可磨灭的贡献。”

从“狙剑”到“天狗”，又是什么推动着徐贵斌始终冲在网络安全技术一线呢?

“和圈里很多从那个年代过来的人一样，我经历了网络安全从一穷二白到如日中天。我们这个群体，价值观还是很好的。刚开始是想炫技，自己能做很多别人做不到的，但道德观会约束你，也就是看一看逛一逛，慢慢就很无聊，没有办法再去证明自己。后来，随着互联网的发展，我们也逐步成长，更加成熟。之前的网络安全主要出于经济利益的考虑，影响到办公、生产，导致经济损失，个人财产被盗。过去很多年都停留在这个层次，但后来慢慢在向国家安全层面靠拢。海湾战争最先打起来就是信息化战争。美军发动电子作战，伊拉克的防空雷达基本失效，很快失去了制空权，处于被动挨打的情况。在国际形势日益严峻的今天，我们不免会问，如果有别的国家针对我国信息化发起攻击，我们能防住吗? 结果显然并不乐观，而覆巢之下安有完卵，历史早已经告诉我们家、国、天下的关系，无人能独善其身。当意识到

这个问题的严重性的时候，我就会想，自己能用专业能力为国家和民族做些什么。这种价值感，远远比干掉一个系统的价值感更强。”

很显然，在网络安全圈早就功成名就的徐贵斌，内心始终闪耀着理想主义的光芒。

“奇安信就是一家有理想的公司，从老板到每个人。公司在营收压力很大的情况下，仍然在前沿技术上进行持续投入，哪怕短时间看不到回报。没有理想的公司做不到，它们只会挣钱。”

春节临近，当被问到是不是可以好好享受闲暇时间，徐贵斌坦言：“我没有什么闲暇时间，基本上 24 小时都在考虑网络安全技术问题。哪怕是人在看电视，心里还是想着这个事。因为攻击者随时随地都有可能发起攻击。我觉得一天不退休就很难真正有闲暇时间。”

当被问到，如果将来退休了，有闲暇时间了，想干点啥。徐贵斌的回答让人有些忍俊不禁。

“我以前很爱玩网络游戏，进入网络安全行业后很少碰。没时间，没精力，也怕沉迷。但是我攒了一堆游戏。一出新游戏，我就保存下来一份，就怕以后网上都找不到了，到现在攒了几千个 G 了。”

作为一名枕戈以待的网络安全工作者，徐贵斌离痛快玩游戏，离真正有闲暇时间，恐怕还有很久。但想必，他仍然是快乐的。

因为，万物之中，理想至美。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

大事记

政协委员齐向东：建设数字经济标杆城市，北京要实现“全面引领”

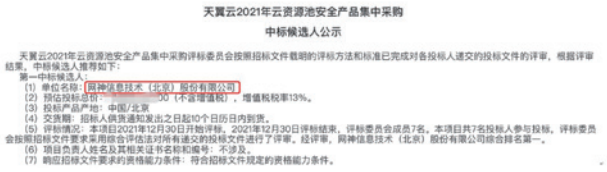
在 1 月 5 日开幕的北京市政协十三届五次会议上，来自科学技术界别的北京市政协委员、奇安信集团董事长齐向东提出，北京应重点围绕智能社会乱象和数字经济发展两个维度，实现“全面引领”，建设“全球标杆”。

为此，齐向东提交了《关于加强隐私保护和加大对网络诈骗打击力度的提案》《关于加大对弹窗广告、大数据杀熟治理力度的提案》《关于北京市完善数字经济安全制度的提案》《关于北京市加快建设国际科技创新中心的提案》四个提案，并受到媒体广泛关注。

开门红！奇安信云安全中标中国电信天翼云集采大单

日前，中国电信天翼云公布 2021 年云资源池安全产品集中采购候选人名单，奇安信集团旗下网神公司以综合排名第一的成绩，成为该项目第一中标候选人。这是奇安信近一年以来连续中标中国联通、中国移动硬件防火墙，中国移动总部态势感知采购、中国电信服务器安全软件集采等之后，在运营商行业的又一重大突破。

中国电信天翼云作为云计算领域的“国家队”、政务云的“领头羊”，在安全建设方面一直坚持高标准、


天翼云2021年云资源池安全产品集中采购
中标候选人公示
天翼云2021年云资源池安全产品集中采购评标委员会按照招标文件载明的评标方法和标准已完成对各投标人递交的投标文件的评审，根据评审结果，中标候选人推荐如下：
第一中标候选人
(1) 单位名称：网神信息技术（北京）股份有限公司
(2) 预估投标总价：00（不含增值税），增值税税率13%。
(3) 投标产品产地：中国/北京
(4) 交货期：招标人供货通知发出之日起10个日历日内到货。
(5) 评标情况：本项目2021年12月30日开始评标，2021年12月30日评标结束，评标委员会成员7名。本项目共7名投标人参与投标，评标委员会按照招标文件要求采用综合评估法对所有递交的投标文件进行了评审。经评审，网神信息技术（北京）股份有限公司综合排名第一。
(6) 项目负责人姓名及其相关证书名称和编号：不涉及。
(7) 响应招标文件要求的资格能力条件：符合招标文件规定的资格能力条件。

高规格要求，因此在本次安全产品选型中指标要求非常严苛，是对安全厂家产品、技术和服务等综合能力的全面考验。此次奇安信能够成功以综合排名第一的“第一中标候选人”入围天翼云年度云资源池安全集采，无疑是对奇安信云安全实力的充分认可。

奇安信召开万人誓师大会 “网络安全中国代表队”集结出征

2022 年 1 月 5 日，北京冬奥会倒计时 30 天。奇安信网络安全中国代表队百地万人誓师大会，在奇安信北京总部冬奥网络安全保障指挥中心线上、线下同步举行。即日起，奇安信 11 支冬奥保障团队，将与奇安信全国 64 个分支机构、上万员工，以及由数百名白帽子组成的“冬奥网安卫士”一起出发，全力以赴守护冬奥网络安全防线。

“希望大家拿出最高昂的斗志、保持最高效的协同、执行最严格的标准，共同筑起牢固的网络安全防线，誓保北京冬奥圆满成功！”奇安信冬奥网络安全保障总指挥、

奇安信集团董事长齐向东表示，“保卫北京冬奥会的网络安全，是我们对国际奥委会和北京奥组委的庄严承诺，是对奇安信实力的一次大检阅，也是实现个人价值的绝佳机会。我们必须全力以赴，打赢这场网络安全保卫战。”

加速出海 奇安信国际业务拿下 7000 万元大单

近日，奇安信国际业务取得重大突破，获得 7000 万元大单，合作重点聚焦于 APT 监测方向。本次国际业务大单或将引领国内网络安全厂商发展新范式，为网安市场开辟新的增量空间打下坚实基础。

根据 Grand View Research 的研究表明，从 2020 年到 2027 年，全球网络安全市场将保持 10.0% 的复合年增长率（CAGR），到 2027 年全球网络安全市场规模将扩张至 3264 亿美元。工信部发布的《网络安全产业高质量发展三年行动计划》提出，到 2023 年我国网络安全产业规模要超过 2500 亿元。网安企业在深耕国内市场的同时，国际市场也成为兵家必争之地，网安企业出海或将拉升网安股整体业绩。

奇安信牵头的零信任团体标准正式发布

在“PKS”安全先进绿色计算 2021 生态大会上，中国信息产业商会现场发布了“PKS 体系团体标准”，奇安信牵头编制的 T/CIITA 117-2021《信息安全技术 零信任参考架构》团体标准位列其中，并将于 2022 年 2 月 1 日起正式实施。这是奇安信首个以第一完成单位的身份正式对外发布的零信任架构标准，是对公司目前正在牵头制定的国家标准《信息安全技术 零信任参考体系架构》的细化。

标准名称	标准编号	发布日期	实施日期
PKS体系 术语	T/CIITA 100-2021	2021-12-20	2022-02-01
PKS体系 参考架构	T/CIITA 101-2021	2021-12-20	2022-02-01
PKS体系 中央处理器参考板	T/CIITA 102-2021	2021-12-20	2022-02-01
PKS体系 以太网交换芯片参考板	T/CIITA 104-2021	2021-12-20	2022-02-01
PKS体系 操作系统安全可信技术要求	T/CIITA 113-2021	2021-12-20	2022-02-01
PKS体系 UEFI固件内置可信启动技术要求	T/CIITA 114-2021	2021-12-20	2022-02-01
PKS体系 可信网络架构要求	T/CIITA 115-2021	2021-12-20	2022-02-01
PKS体系 数据备份与恢复产品技术要求	T/CIITA 116-2021	2021-12-20	2022-02-01
信息安全技术 零信任参考架构	T/CIITA 117-2021	2021-12-20	2022-02-01
PKS体系 生态软件可信安全认证分发流程	T/CIITA 118-2021	2021-12-20	2022-02-01

中国信息产业商会

编制过程中，奇安信充分借鉴了国内外零信任标准构建的相关理念和实践经验，深度融合了国内产业市场现状及未来发展需求，充分结合了零信任在 PKS 技术体系中的实践应用，最终形成了标准内容，以期对零信任理念及相关技术在国内的发展和应用，具有重要的指导作用。

广东省科学院与奇安信达成战略合作 共同打造科研安全

12 月 28 日，广东省科学院与奇安信签署战略合作协议，省科院党委副书记、院长陈为民，奇安信集团副总裁刘进等参加签约仪式。

根据协议，双方将秉承“优势互补、深度合作、持续发展”的原则，建立工作联系机制，在院企成果孵化、联合课题申报、人才培养、技术研讨交流等方面展开深度合作，发挥双方技术和资源优势，深入推动“科技 + 安全”的全新模式探索，以更好应对和化解网络风险挑战，落实“网络强国”战略使命与责任。

冬奥网络安全卫士招募完成并正式颁发聘书

12 月 28 日，冬奥网络安全卫士聘任仪式在奇安信安全中心线上、线下同步举行。即日起，正式受聘的数百名白帽子将作为“冬奥网络安全卫士”，和奇安信冬奥保障团队一起，共同承担守护北京冬奥会网络安全的责任。

为集结更多可靠力量，保卫北京冬奥网络安全，12 月 16 日，北京冬奥组委技术部牵头组织，由奇安信及旗下补天漏洞响应平台提供技术平台和运营支持，招募白帽子作为“冬奥网络安全卫士”，参与冬奥网络安全工作，为守护冬奥网络安全贡献专业力量。招募一经发出，便收到数万名白帽子踊跃报名。

DataCon2021 大数据安全分析竞赛圆满落幕

12 月 27 日，DataCon2021 大数据安全分析竞赛颁奖典礼在京举行。本届大赛的获奖战队代表，以及往届大赛优秀战队与全国数十家高校、科研机构、企业的安全专家、研究员等齐聚线上、线下，共同探讨如何推动 DataCon 这一“数据安全分析竞赛第一品牌”进一步融入安全教学与科研发展，以及网络安全的高水平人才发掘和培养。

自 2019 年举办首次比赛，DataCon 一直致力于通过更加接近真实的网络攻防场景，设计竞赛的内容和形式，在赛题中融入最新研究成果，并将数据集用于支撑前沿学术研究。在本次比赛中，更是紧扣数据安全主线，

采取周密的数据安全评估，采取多样化的数据安全保护措施的前提下，为选手提供真实的数据集。

吴云坤出席“网信企业发展和社会责任论坛”

“企业是一个社会单元，受益于国家社会发展红利，也必须积极承担国家社会赋予的责任和义务。”12 月 27 日，奇安信集团总裁吴云坤受邀参加“网信企业发展和社会责任论坛”，并发表“实力担当国家和产业责任，创新驱动产业发展”的主题演讲。

发展和责任不是对立的两面，而是相互缠绕形成的企业 DNA，一个企业只有勇于承担社会责任，才能获得更好的发展。吴云坤表示，奇安信作为国内网络安全领域的龙头企业之一，自成立以来，在承担保卫经济社会数字化发展的安全责任的同时，围绕承担保护国家网络安全责任，持续发展公司能力；立足发展壮大网络安全产业，坚持创新驱动发展；坚持用技术回报社会。

齐向东出席 APEC 工商领导人中国论坛

12 月 25 日，APEC 中国工商理事会数字经济委员会执委会成员、奇安信集团董事长齐向东受邀出席“中国加入 APEC 三十周年工商界主题活动暨 2021 年 APEC 工商领导人中国论坛”，并发表“走网络安全科技自立之路”的主题演讲。他指出，网络安全科技自立是应对网络安全挑战和有效解决国际贸易纠纷的必然选择，更是国家发展的战略支撑。

与此同时，作为“中国数字经济产业示范样本行动”的重要成果，大会正式发布“中国数字经济产业示范样本 50”名单中，奇安信入选。该行动由亚太经合组织（APEC）中国工商理事会及 APEC 中国数字经济委员会联合发起。专家调研组围绕数字科技、产业数字化、乡村振兴、碳达峰与碳中和、医疗与健康、数字生活与服务、中小企业产业集群七大核心方向深入开展调研，旨在推选出引领科技创新、践行数字普惠、彰显产业担当的最佳实践。50 家入选企业代表的是中国数字经济独特优势的年度产业示范样本。奇安信此次入选，是委员会对其在创造中国网络安全产业长期价值中做出贡献的充分肯定。

奇安信北京冬奥网络安全保障中心启动

奇安信北京冬奥会网络安全保障指挥中心 24 日在北京奇安信安全中心正式启动。北京冬奥会期间，该指挥中心将为冬奥会及全国奇安信用户提供全天候、全覆盖、高质量网络安全保障。

奇安信冬奥保障团队总指挥、奇安信集团董事长齐向东表示：“今天启动的奇安信网络安全保障指挥中心，是保卫冬奥网络安全的重要‘神经中枢’，是网络安全保卫各专业兵种联合作战的‘参谋部’。在接下来的近 100 天里，奇安信上万人将在这里 24 小时全天候、全方位保护冬奥期间每个客户、每个环节的网络安全，为冬奥筑起牢固的网络安全防线。”

当日，北京赛区分队、延庆赛区分队、张家口赛区分队、威胁情报分队、专家分队、应急响应分队、后勤保障分队等十余组保障中心分队一同启动。

“安全先进绿色计算 + 安全实践” 论坛成功举办

12 月 24 日，PKS 安全先进绿色计算 2021 生态大会“安全先进绿色计算 + 安全实践”专场论坛，在北京

分会场线上、线下同步举行。天津市委网信办副主任徐滨彦，中国电子信息产业集团有限公司副总经理、党组成员陈锡明，奇安信集团董事长齐向东等领导和数十家生态合作伙伴出席会议，并围绕如何在不同业务场景下利用安全先进绿色的计算体系，保障数字化发展与安全的平衡等问题进行了分享交流。

奇安信董事长齐向东表示，PKS 计算体系是打造信创“中国赛道”、推动数字经济发展的关键所在。中国电子和奇安信联合打造的 PKS 体系，将安全能力植入到 CPU 和操作系统中，同时采用基于内存指令执行序列检测技术，可通过创新底层架构来保障信息系统安全。未来，奇安信也将继续推动 PKS 体系的体制增效，全力支持信创产业发展，不断做强、做优、做大中国的数字经济。

为充分发挥奇安信行业地位和资源技术优势，进一步链接更多生态合作伙伴，奇安信与 20 家不同行业、不同领域企业进行战略合作签约，结成战略合作伙伴，共同打造具有影响力的网络安全行业新生态。

齐向东连任雄安科企联会长：为雄安新区高质量发展注入“源头活水”

雄安新区科技创新企业联合会（以下简称雄安科企联）召开会员大会暨理事会一届三次会议，表决通过了会员企业增补名单、联合会章程修改、监事单位提名、会长连任等决议。科企联会长、奇安信集团董事长齐向东再次连任。

齐向东表示，2021 年是雄安新区从规划建设为主、进入承接非首都功能和大规模建设同步推进的重要时期，2022 年，是雄安推进启动区和起步区建设的关键年。要抓住发展机遇，集中力量做好三件事：做好组织建设工作，为雄安的高质量发展提供支持；做好政企间的沟通桥梁，继续优化雄安营商环境；做好产学研合作服务平台，打通科技创新“最后一公里”。

全国工商联授予奇安信董事长齐向东“信息工作先进个人”称号

12 月 23 日，全国工商联通报 2021 年信息工作情况，北京市工商联副主席、奇安信集团董事长齐向东被授予“全国工商联 2021 年信息工作先进个人”称号，以表彰他在 2021 年全国工商联在网络安全领域信息报送工作的突出贡献。

信息报送是工商联系统一项重要的工作。通过信息报送，不但是加强政治机关建设、发挥桥梁纽带和助手作用的重要方式，更在全面、准确、及时反映民营经济领域重要情况和问题建议，以及广大民营经济人士所思所想所忧所盼和在服务科学决策、服务促进“两个健康”方面上发挥了重要作用。

四实训基地授牌、五校签约 打造产学研用闭环人才培养生态

12 月 23 日，2021 网络空间安全人才峰会在长沙举行，奇安信集团作为网络安全行业领军企业受邀亮相，并充分发挥自身技术和资源优势，与五大高校签署战略合作签约、落地四学院网络空间安全人才培养实训基地，积极推进“产学研用”闭环人才培养生态建设，培养高素质创新型网络安全人才。

在“产学研用”人才供需战略合作签约仪式上，奇安信集团作为产业代表，联合中国网络空间安全人才教育论坛、和国家网络安全产业园区（长沙）城市网络安全运营中心，与南开大学网络空间安全学院、中南大学、湖南大学信息科学与工程学院、广州大学网络空间先进技术研究院、广东技术师范大学电子与信息学院五大高校学院签署战略合作协议。在校企合作基础上，广州大学网络空间先进技术研究院、南开大学网络空间安全学院、湖南大学信息科学与工程学院、广东技术师范大学，为奇安信集团授牌“人才培养实训基地”。

荣誉墙

第二十三届高交会闭幕 奇安信三项产品获评“优秀产品奖”

第二十三届中国国际高新技术成果交易会在深圳举办。本届高交会以“推动高质量发展，构建新发展格局”为主题，聚焦各行业专业化、国际化、便利化、高水平的科技成果，经专家评审，共计 599 个项目获评优秀产品奖。其中，奇安信旗下新一代安全感知系统（简称天眼）、全

球鹰网络空间测绘系统和开源卫士系统三款产品，凭借领先的产品优势及技术水平，获评“优秀产品奖”。

奇安信荣获 2021 中国电子“i+”创新创业大赛两项大奖

12 月 29 日，2021 第五届中国电子“i+”创新创业大赛奖项揭晓。奇安信“PKS 体系之漏洞攻击防护关键技术（天狗）的研发与应用”和“基于 PKS 的大数据环境零信任动态授信体系”两个项目，分获一等奖和三等奖。

由奇安信集团自主研发的新一代安全技术“天狗”，承担了打造 PKS 安全底座的重任。具备完全自主的知识产权，已申请相关发明专利 152 项，已授权专利超 30 个，并已在各领域头部客户中进行了推广和应用，帮助相关政企机构及时发现高危安全事件；基于 PKS 的零信任动态授信体系化产品，并经过近两年的技术研究和产品迭代研制，可适用于多种大型应用场景，确保

PKS 内生安全体系管控能力在网络安全和业务安全的全面覆盖。

奇安信副总裁张聪当选 2021“北京青年榜样”年度人物

在“请党放心，强国有我”——党的十九届六中全会精神宣讲暨 2021 北京青年榜样发布活动上，奇安信集团副总裁张聪被评为 2021“北京青年榜样”年度人物。

作为北京市西城区青年联合会委员、奇安信集团副总裁的张聪，长期以来深耕网络安全行业，以创始团队成员参与创建 “隐形冠军”企业奇安信。工作中主持了大批重要的政企单位网络安全项目，共获得发明专利 20 余项，覆盖了网络支付安全防护、恶意软件防护、恶意进程防护、可疑进程检测、网络数据安全检测、视频安全防护、漏洞检测防护等诸多安全领域。

在 2021 年 Apache Log4j 高危漏洞披露后，张聪带领团队第一时间发布天擎终端安全管理系统解决方案，最终无一客户受到影响，避免了该网络安全事件给政企机构和关键信息基础设施单位造成的损失，有效保障了网络空间的安全。

奇安信 Q-SASE 亮相信通院首届混合云大会 包揽所有 SASE 相关成果

12 月 23—24 日，由中国信息通信研究院、中国通信标准化协会主办的首届“混合云大会”在京召开。作为混合云产业的首个行业盛会，2021 混合云大会发布了多项重磅成果。其中，奇安信安全访问服务（Q-SASE）作为 2021 年 8 月才正式对外发布的解决方案级服务化新品，一举拿下了“SASE 成熟度能力评估”“年度 SASE 优秀案例”“混合云产业全景图（混合云网络与混合云安全领域）”三项含金量极高的荣誉。在本届混合云大会发布的所有 SASE 相关成果中，奇安信均占据一席之地。

奇安信集团上榜 Gartner 威胁情报市场报告

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

Gartner 预测数据显示：“威胁情报支出预计将以 15.8% 的复合年增长率增长，到 2025 年将达到 26 亿美元。”

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
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