极牛网络安全通讯 • 社群期刊 2022 年 1 月 第 7 期

网安观察



P17 2022年
网络安全八个关键词

P12
企业视角下的新版《网络安全审查办法》政策解读

P17 新合规时代：主体责任进一步压实
P19 信创安全：更丰富的产品体系，更强服务能力
P20 安全左移：供应链安全严峻形势推动安全左移

第 7 期
2022年1月

极牛网

极牛网 网络安全行业媒体

致力于促进中国网络安全行业创新思维的交流与碰撞，搭建中国网络安全技术社区和交流平台



技术格局

网安工程师的成长，需要锻炼开阔的技术视野和统筹全局的战略高度，能够着眼现在思考未来，做懂业务懂策略的工程师。

管理之道

网安工程师随着职业发展，必然面临着向技术总监、CTO等管理角色转型，改变管理思维，建立属于自己的管理哲学。

人才梯队

作为技术管理者，如何建立一个稳固、高效的人才队伍是核心任务，更应该从人才梯队的角度，关注人才的培养的更迭。

企业战略

技术管理者应该建立技术以外的格局，经济形势、商业模式、投融资等等，才能助力企业发展，做与创始人同频的CTO。

产品运营

敢于拥抱和应对变化，敢于创新，在创新的基础框架下，寻找创新的实践方法论，激发技术人员创新能力，推动业务发展。

布道能力

作为技术工程师，需要重点培养自己的布道能力，能将自己的技术成果和理念传播出去，才能拓宽和升级自己的认知边界。

开启
2022年网络安全

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。

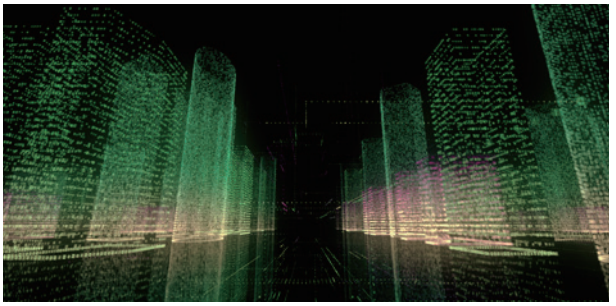
在热门的数据安全治理与隐私保护领域，期待相关的安全技术与方案逐步体系化和成熟。此外，“基础不牢，地动山摇”，安全左移与漏洞管理等安全基础工作将会受到更多重视。

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。

CONTEN

目录



安全态势

P4 | 公安部公布打击侵犯公民个人信息犯罪十大典型案例
P4 | 美医疗中心 Broward Health 披露数据泄露：影响超 130 万人
P5 | 波兰政府被指使用 Pegasus 入侵反对派成员设备
P5 | 超 22% 的阿尔巴尼亚公民个人和工资信息遭泄露
P6 | CNNVD 关于 Apache Apisix 授权问题漏洞的预警
P6 | Apache Log4j 远程代码执行漏洞安全风险通告
P6 | MinIO 权限提升漏洞安全风险通告
P7 | 国内攻防演习 12 月态势：哪些薄弱点最易被利用?
P10 | 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
P10 | 国家网信办等十三部门修订发布《网络安全审查办法》
P10 | 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》
P11 | 中央网信委印发《“十四五”国家信息化规划》
P11 | 美 CISA 发布《公共安全陆地无线移动通信安全》白皮书



政策解读

P12
企业视角下的新版《网络安全审查办法》政策解读

ONTENTS



专题报道

P17
新合规时代：主体责任进一步压实

P19
信创安全：更丰富全面的产品体系，更强服务能力

P20
安全左移：供应链安全严峻形势推动安全左移



第 7 期
《网安观察》编辑部
主办　极牛网

总　编　辑：陈鑫杰
总　顾　问：叶绍琛
副　总　编：王文彦
安全态势主编：乔跃春
网络攻击主编：王新睿
漏洞情报主编：黎治声
移动安全主编：蔡国兆
安全人才主编：林俊濠
安全产业主编：张　程

公众号　小程序　网站

电子版请访问 www.geeknb.com 阅读或下载索阅、投稿、建议和意见反馈，请联系极牛网期刊编辑部。

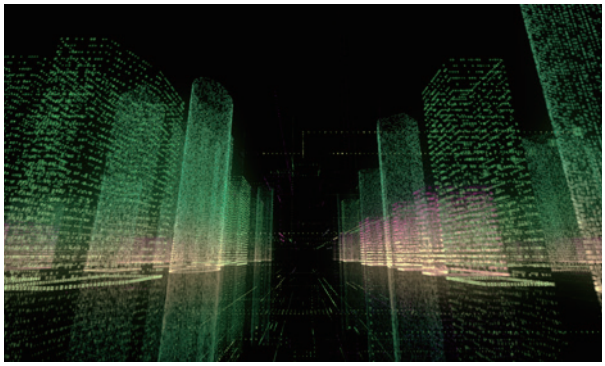
E m a i l：hi@geeknb.com
地　　址：深圳市龙岗区江灏科技园1栋西座
邮　　编：518000
电　　话：0755-33228862
印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

版权所有 ©2021 极牛网，保留一切权利。
非经极牛网书面同意，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。

无担保声明
本资料内容仅供参考，均“如是”提供，除非适用法要求，极牛网对本资料所有内容不提供任何明示或暗示的保证，包括但不限于适销性或者适用于某一特定目的的保证。在法律允许的范围内，极牛网在任何情况下都不对因使用本资料任何内容而产生的任何特殊的、附带的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉或预期节约的损失进行赔偿。

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?

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

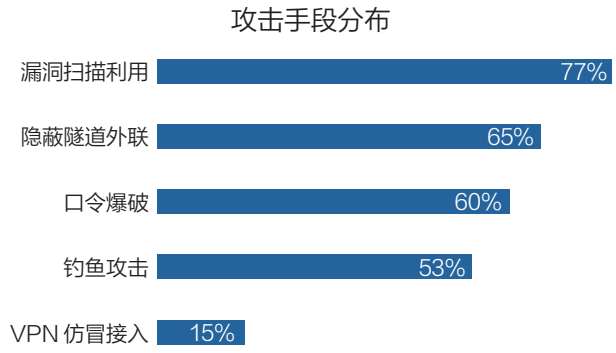
本月任务中目标网络敏感信息泄露较为严重，如内网 IP、网站目录结构、Web 后台系统、应用开发平台及后台登录地址、安全认证信息在内的敏感源码等泄露，这些敏感信息泄露原因多为安全配置疏漏、平台审核不严。此类敏感信息常常被用来实现针对性的快速突破，以及渗透。

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。



CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

CTFWAR攻防战争平台是CTFWAR网络安全攻防对抗联赛的官方平台，是由中国网络安全攻防大咖联合发起的创新型学习平台，以游戏的形式融入多种网络攻防场景进行答题、竞赛、互动。CTFWAR攻防靶场分为初级新手区、中级进阶区、高级挑战区，同学们可根据自身技术能力及技术方向进行筛选，整个学习过程将有全面的数据化呈现。

攻防答题模式

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

积分等级体系

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

极牛·产业生态

网络安全产业生态平台

极牛网络安全产业生态平台，通过产服、产孵、产投、产研四大引擎，打通技术、产品、平台能力以及B端G端场景和服务体系，构建产业核心生态圈，与合作伙伴共生共赢，助力网安产业智慧升级。



四大引擎

产服

以产业基地为载体
提供产业生态服务
助力产业发展

产孵

以产业加速器为载体
孵化优质企业
与ToB业务的合作

产投

以产业生态投资
为重要抓手
构建产业生态体系

产研

构建产学研体系
聚焦底层技术创新
全面赋能网安产业

产业生态架构

与生态伙伴一起持续加大资本 、资源 、 技术 、 能力和商机投入，助力科技创新驱动网络安全产业升级，为社会创造更大价值



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

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。

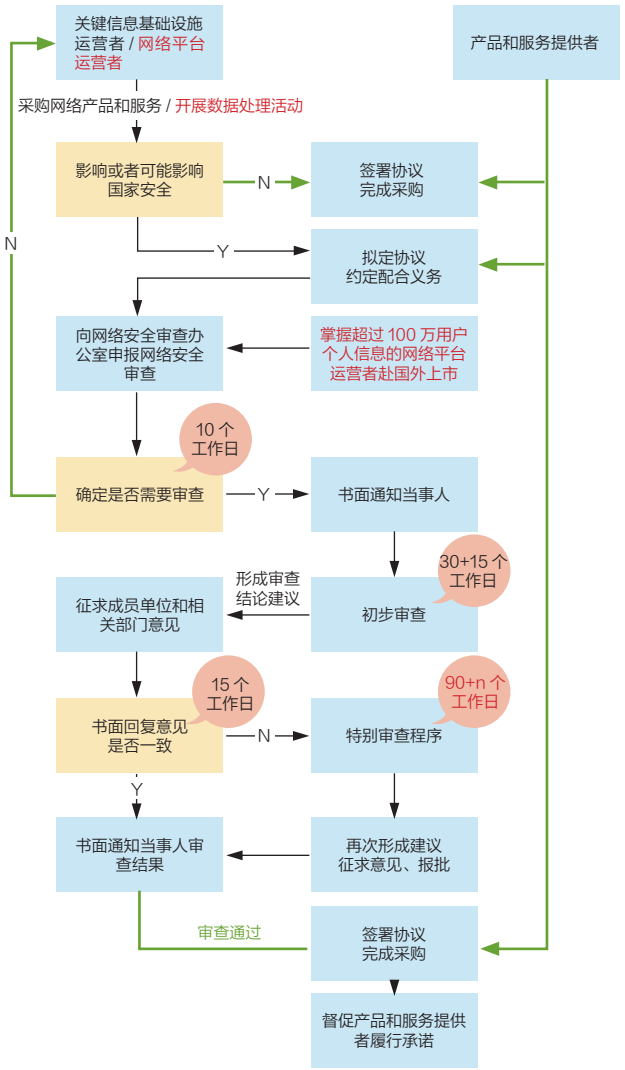
此外我们注意到，《网络安全审查办法》似乎对于上市情形格外重视，且展现了对全部上市企业风险的关注，其第七条、第八条和第十条的相关条款均展现了这种关注。我们初步认为，上市活动整体纳入国家安全风险考虑因素，不再区分国外上市、香港上市和境内上市的情形。

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。





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

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。

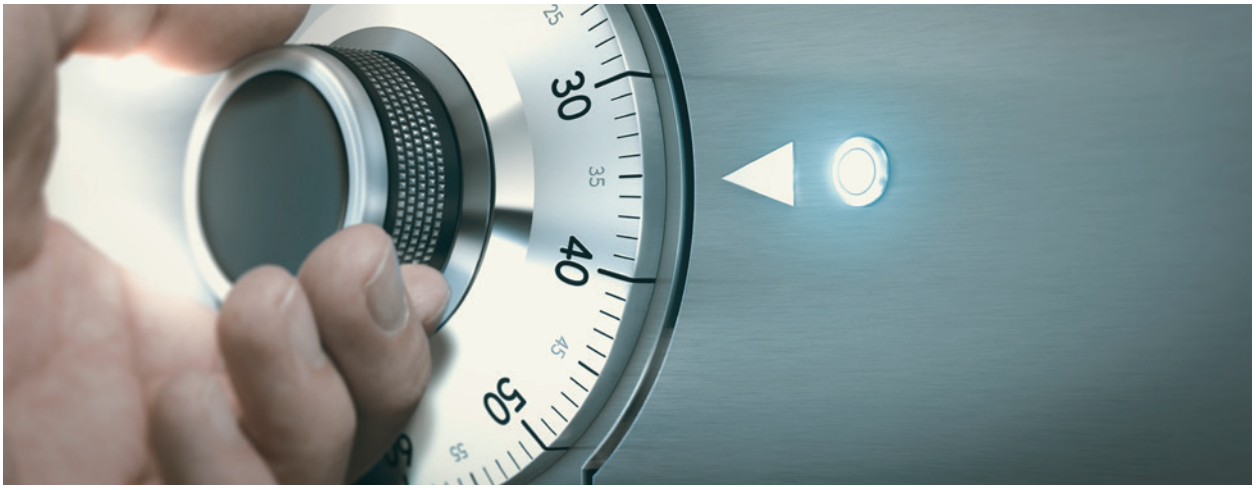
安全供给不足下的技术创新

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

华云信安·产业教育中心

网安人才培养新模式
打造产业人才成长圈

产教融合

INTEGRATION OF PRODUCTION AND EDUCATION

- 共建产业学院
- 共建合作专业
- 共建联合实验室
- 共建人才/师资培养基地
- 1+X证书合作
- 教育部协同育人项目合作

极牛技术社群

网络安全技术社群

Cyber Security Technology Community

PLATFORM

网络安全技术社群

极牛网旗下面向网络安全工程师的社群平台，汇聚行业中网安工程师的知识和社交平台，围绕『技术』『管理』和『圈子』三个核心能力，将前沿的技术内容、技术管理成长感悟、技术圈子社群平台等向优质的网安工程师开放，每月定期组织社群会员线下活动，强调内容分享的体系化和活动内容的多样性，为中国网络安全工程师打造专属的全方位综合赋能的社群平台。

技术

聚焦前沿技术、热点技术、难点技术，提升网安在企业架构中的决策能力和迭代能力。

管理

专注在帮助网安工程师在职业发展中，建立体系化的管理知识和技术管理转型路径。

圈子

建立精准的技术方向圈子，针对不同的职业发展阶段，组成技术成长小组一起结伴同行。

极牛技术站

以沙龙、峰会、圆桌论坛等深度学习的形式进行，满足知识获取与社交需求。

管理加油站

面向管理者的闭门活动，前瞻性的思维和观点，成熟的管理模式与领导模型。

极牛知识变现

通过帮助工程师打造个人品牌，从出书、录课、企培等形式帮助知识变现。

极牛训练营

面向社群成员的线下课程，技术架构、团队管理、商业模式、塑造个人品牌等。

极牛众星计划

社群中优秀的工程师将会被受邀签约极牛众星计划，平台辅助进行品牌孵化。

更多内容敬请期待

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

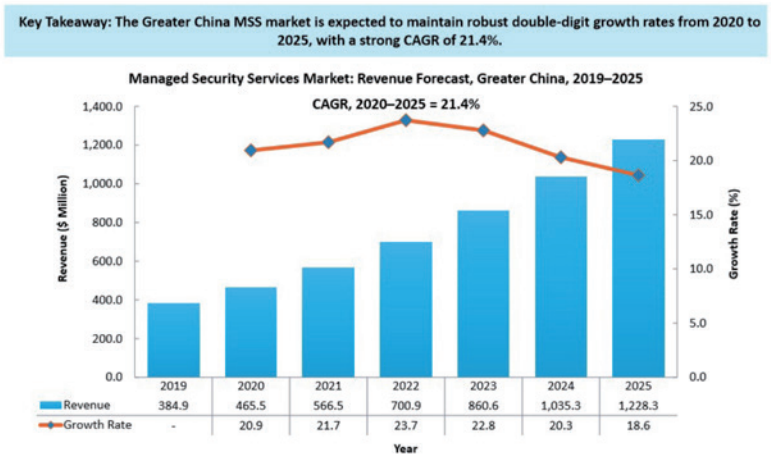
面对外部威胁的演变和政策驱动，许多政企组织缺乏拥有专业知识和技能的安全团队，来处理日常安全运营中出现的问题，这就需要将安全运营外包给服务商。

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。

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

华云信安(深圳)科技有限公司（简称 华云信安™ ）成立于2016年，是一家深耕于网络空间安全领域，拥有自主研发能力及核心知识产权，提供网络安全解决方案与技术服务的高新技术企业。华云信安™总部位于深圳，在广州、上海、武汉设有分支机构，公司核心团队来自奇安信、网易、华为、绿盟、思科等国际知名科技企业，具有深厚的网络安全技术实力和管理经验。

华云信安™目前拥有数十项计算机软件著作权和十余款自主研发产品，具备“风险评估类”和“安全工程类”两项信息安全服务资质，通过ISO9001质量管理体系认证，现为深圳市信息安全行业协会理事单位和深圳市信息网络安全管理协会会员单位。

华云信安™凭借创新的网络安全产品体系、深厚的网络安全服务能力以及丰富的服务经验，为互联网、金融、能源、制造、交通、医疗、政务等领域的广大客户，提供专业优质的网络安全产品、网络安全解决方案和网络安全技术服务。

网络犯罪研究中心

华云信安·网络犯罪研究中心，是专注于打击网络犯罪的安全服务部门，致力于打击涉网新型犯罪领域的安全技术研究与产品研发，包括涉网犯罪案件技术支撑、网络诈骗案件技术支撑、涉众型经济犯罪案件技术支撑等，以攻防实验室和极牛技术社群组成创新型的安全研究团队，为国家及各省市公安机关提供高效专业的打击涉网犯罪情报分析服务和实战解决方案。

极牛攻防实验室

华云信安·极牛攻防实验室，由内部成员及外部知名技术专家团队组成，致力于最前沿网络安全技术的研究和调研，以指导技术研发路径和产品发展方向。其职责除开展传统的网络安全技术研究外，还跟踪国内外网络安全技术趋势并进行相关技术研究。现已协助国家互联网应急中心(CNcert)发现并修复数百个安全漏洞，获得数十张高危原创漏洞证明证书。

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

我们提供卓越、丰富的信息安全产品及各行业解决方案、信息安全技术服务和基础架构咨询服务。

专业的团队服务

我们拥有资深、专业的服务团队，按需为用户提供多元化、多级别的咨询规划服务和技术实施服务。

众多的行业案例

我们拥有众多行业应用案例，包括制造、快消、航空、金融、物流、建筑、服务、互联网等行业。

深入的厂商合作

我们与多家国内外知名厂商建立战略合作关系，共同致力于优质解决方案及相关服务的推广落地。

全国范围的服务

我们公司总部在深圳，同时在上海、广州、武汉等设有分支机构，具有全国范围内的业务服务能力。

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全



7436084028