SECURITY INSIDER

# 网安26号院

奇安信网络安全通讯 · 安全快一步

## 2021 网络安全的上半场

P14



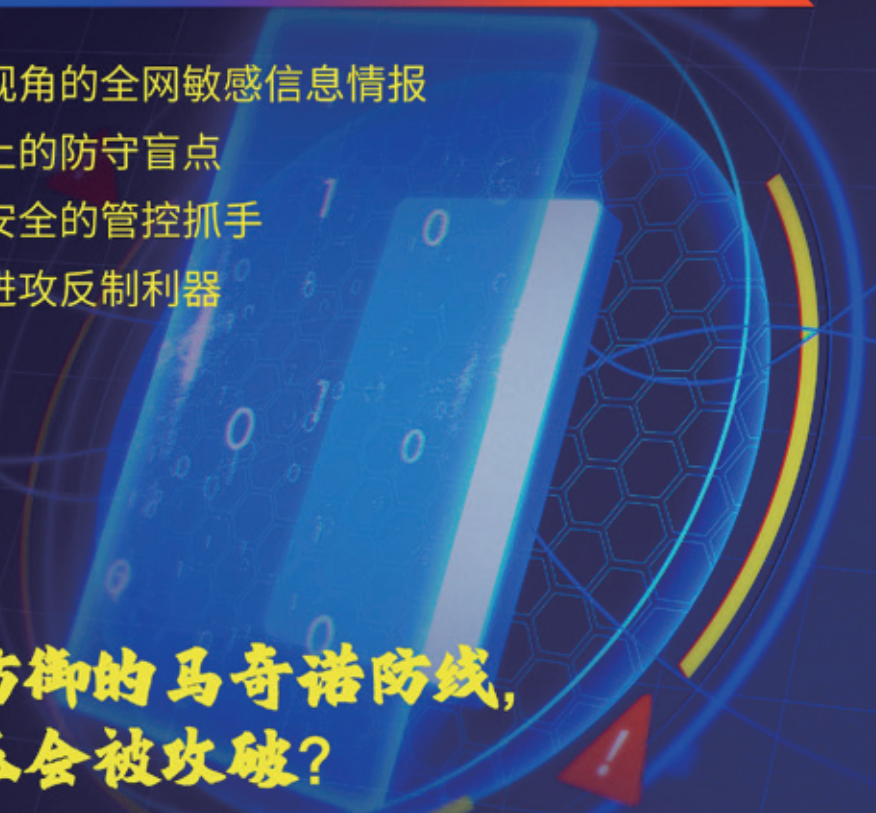
第 8 期

2021 年 8 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

# 形势与合规双重压力 网络安全进入最好时期

2021年过去的数月，网络安全形势日趋严峻：勒索攻击频发，影响日益严重，危及关键基础设施。危害严重的软件供应链攻击则令众多政企机构更加防不胜防。

与此同时，我国连续密集出台多项网络安全法规，法律框架与制度日趋完善，给政企机构带来前所未有的合规压力。《数据安全法》《个人信息保护法》先后通过，与《网络安全法》构成数字经济时代三大法律支柱体系，搭建起数字经济“生态保护系统”。

9月1日施行的《数据安全法》，明确了相关管理者、运营者和经营者的数据安全保护责任。7月印发的《网络产品安全漏洞管理规定》明确了网络产品提供者、网络运营者，以及从事漏洞发现、收集、发布等活动的组织或个人等各类主体的责任和义务。

《网络安全审查办法（修订草案征求意见稿）》，则扩大了原本针对关键基础设施运营者的审查范围，新增了“数据处理者”。9月1日施行的《关键信息基础设施安全保护条例》，对《网络安全法》规定的关键信息基础设施运营者的安全保护义务进行了细化及补充。《个人信息保护法》则强化了重要互联网平台服务提供者的个人信息保护义务。

在安全形势和政策合规压力下，加强网络安全建设已从共识转化为行动，部委与地方政府对网络安全网投入做出了规定。工信部发布的《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》提出， 电信等重点行业的网络安全投入在信息化投入中的比例，2023年要达到10%。上海市经信委透露，网络安全“十四五”规划以及即将发布的网络安全产业行动计划中，将进一步明确政府和公共企事业单位在网络安全上的投入比例不低于10%。

对政企网络安全负责人来说，法规密集出台在带来更多合规压力的同时，也意味着正迎来最好时期。面对日益受到重视，以及更多的资源，你准备好了吗？

总编辑

李建平

2021年8月1日

CONTEN

目录




**月度专题**

TS

## 安全之道

# P40

270+ 城市、400+ 门店，
居然之家快速扩张背后的组网秘诀

## 奇安信人

# P44

我是程序媛，
我想让我的名号被所有人知道

## 奇安资讯





第 8 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

Email: 26hao@qianxin.com
地 址：北京市西城区西直门外南路 26 院 1 号
邮 编：100044
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

## 事件篇

关基网络威胁形势严峻，美国电信巨头近 5 千万用户数据外泄，南非重要港口系统瘫痪数天官方称属于“不可抗力”；勒索软件持续猖獗，美国数十家医院诊所系统瘫痪致使患者紧急转移，咨询巨头埃森哲数据外泄被索要 3.2 亿元赎金，知名计算机制造商技嘉上百 GB 数据外泄……


### 美国数十家医院诊所遭勒索攻击系统瘫痪，患者紧急转移

据 Arstechnica 8 月 17 日消息，8 月 15 日凌晨，美国医疗连锁机构 Memorial Health System 遭遇勒索软件攻击，致使 IT 系统瘫痪，旗下 3 家医院无法正常运营。Memorial Health System 旗下拥有 3 家医院和 64 家诊所，遭到攻击后，3 家医院着手将急诊病患转移至卡姆登克拉克医疗中心，大部分诊所取消了安排在次日的所有非紧急手术和放射性检查，建议患者提前来电沟通商议应对办法。今年以来，已出现数十起针对医疗机构的网络攻击活动。

### 国际电信巨头 T-Mobile 遭遇重大安全事件，近 5 千万美国用户数据泄露

据 Vice 8 月 15 日消息，国际电信巨头 T-Mobile 旗下美国公司遭遇了一起重大安全事件。有网络犯罪论坛上兜售其超过 1 亿用户的敏感数据，包括姓名、社保号码、电话号码、居住地址、IMEI、驾照等信息。卖家声称，在两周前入侵了 T-Mobile 的生产、部署和开发服务器，窃取了多个数据库共计 106GB 数据，包括可以追溯到 2004 年的 IMEI 历史数据库。卖家还声称，此举是为了对美国情报机构进行报复，打击美国的基础设施。T-Mobile 后续回应称，确认近 5000 万用户的个人信息遭泄露。

### 咨询巨头埃森哲遭勒索软件攻击数据外泄：对方索要 3.2 亿元赎金

据 The Record 8 月 11 日消息，勒索软件团伙 LockBit 发布公告，声称已攻破国际咨询巨头埃森哲的内网，窃取了 6TB 内部数据，要求支付 5000 万美元（约 3.2 亿人民币）的赎金。根据泄露数据样本显示，主要有埃森哲的产品手册、员工培训课程及各类营销材料等，似乎不包含任何敏感信息。埃森哲随后承认，确实遭到勒索软件攻击，但公司运营未受到影响，相关系统已通过备份副本恢复。

### 越南知名安全厂商 Bkav 源代码泄露，售价 25 万美元

据 VNExpress 8 月 11 日消息，越南知名网络安全公司 Bkav 旗下产品的源代码遭到窃取，在一个数据泄露论坛上被出售，总价 25 万美元。卖家声称，已成功入侵了 Bkav 的服务器并窃取了产品源代码，被出售的源代码包括反病毒等产品，以每个 1 万至 3 万美元的价格出售，其中一个人工智能程序的源代码标价 10 万美元。Bkav 公司确认泄露的源代码是真的，但都是旧代码，泄漏不会

影响到客户。该公司还表示，该事件是一名前雇员造成的，泄露时间在一年前。

## 国内摄像头黑产治理：发现 4 万多个联网摄像头漏洞

据网信中国 8 月 9 日消息，今年 5 月以来，中央网信办会同多部门深入推进摄像头偷窥等黑产集中治理工作。其中，网信办对存在隐私视频信息泄露隐患的 14 家视频监控 APP 厂商进行了约谈，并督促其完成整改。工信部组织对 18 家具有行业代表性的视频监控云平台开展检查，发现处置 SQL 注入、越权操作等一批高危漏洞；全面排查联网摄像头存在的安全隐患，发现 4 万多个弱口令、未授权访问、远程命令执行等摄像头漏洞，取证并处置 500 余个。公安部查获非法控制的网络摄像头使用权限 2.5 万余个。

## 知名计算机制造商技嘉遭勒索软件攻击，上百 GB 数据失窃

据 The Record 8 月 6 日消息，中国台湾知名计算机制造商技嘉遭 RansomExx 勒索软件攻击，位于总部台湾的系统被迫关闭，多个网站无法访问，超 112GB 签署过保密协议的商业数据遭泄露，涉及英特尔、AMD 等合作伙伴。攻击者威胁称，除非支付赎金，否则将公开被窃取的数据。过去几年来，台湾电子制造业一直笼罩在勒索软件攻击的阴影之下，富士康、宏碁、研华、仁宝、广达以及佳明等知名厂商均遭受过重大打击。

## 内部人员反水！勒索软件团伙 Conti 攻击手册泄露

据 BleepingComputer 8 月 5 日消息，一名反水的 Conti 加盟机构成员在地下论坛发帖，公开泄露了有关 Conti 勒索软件操作的信息，包括 Cobalt Strike C2 服务器的 IP 地址和一个 113MB 的档案，其中包含大量用于进行勒索软件攻击的工具和培训材料。该成员表示，他发布这些材料的原因是在一次攻击后的分赃中只获得了 1500 美元，而团队的其他成员却将赚取数百万美元。有威胁情报专家指出，此次泄露的攻击手册与 Conti 的活跃案例相符，基本可以确认是真实泄露。

## 意大利地方疫苗接种预约系统因网络攻击被迫关闭

据路透社 8 月 1 日消息，意大利拉齐奥地区政府表示，黑客攻击了管理罗马周边的拉齐奥地区 COVID-19 疫苗预约的公司的 IT 系统，导致疫苗预约系统被迫关闭。该地区官员在 Facebook 上说：“一场针对该地区数据库的强大黑客攻击正在进行中。”所有的系统都被停用，包括该地区的卫生门户网站和疫苗接种网络的系统，接种计划可能会因此受到延误。意大利警方正在调查此事，找出攻击的幕后黑手。近日，意大利跟随法国宣布，接种疫苗或提供 COVID-19 免疫证明，将成为参加各种聚集活动的强制要求。

## 南非重要港口因网络攻击系统瘫痪近一周，官方称属于“不可抗力”

据 Moneyweb 7 月 27 日消息，南非国家运输公司（Transnet）港口部门在 7 月 26 日宣布，近期遭遇的网络攻击事件属于不可抗力性质，这在全球尚属首次。该事件导致其港口运输系统瘫痪近一周，该公司随即将港口系统转为手动操作，但随着卡车运输的进一步延误，导致多个港口出现故障，特别是负责南非全国超六成运输量的德班港遇到严重阻塞问题，港口部门只能发布“不可抗力”通报。港口部门是南非国家运输最大和最重要的部门，它的发声可以证明这家公司甚至南非全国港口物流确实遭受了重大打击。

## 漏洞篇

8月，微软爆出多个漏洞预警，包括Exchange服务多个远程代码执行漏洞、Windows打印服务最新0day漏洞、Windows NTLM中继攻击漏洞等；奇安信CERT研判发现，近期需重点关注27个高风险漏洞……

### Linux kernel 拒绝服务漏洞（CVE-2021-38207）预警

2021年8月16日，网络安全威胁和漏洞信息共享平台发布预警，Linux发布了Linux kernel存在拒绝服务漏洞（CVE-2021-38207）的风险通告。攻击者可利用该漏洞导致拒绝服务，Linux kernel低于5.12.13的版本均受影响。目前官方已修复该漏洞，建议受影响用户及时更新至安全版本，并做好资产自查及预防工作，以免遭受黑客攻击。

### Realtek SDK 多个高危漏洞预警

2021年8月18日，网络安全威胁和漏洞信息共享平台发布预警，国外研究人员公开披露了多个Realtek SDK高危漏洞（CVE-2021-35392、CVE-2021-35393、CVE-2021-35394、CVE-2021-35395）的细节和POC。攻击者可利用这些漏洞使设备崩溃、注入任意命令并以最高权限执行任意代码。该漏洞影响范围较广，且危害较大，目前厂商已修复漏洞，建议受影响用户及时更新至安全版本，并做好资产自查及预防工作，以免遭受黑客攻击。Realtek SDK是瑞昱（Realtek）公司的一套SDK开发包。

### Windows Print Spooler 远程代码执行0day 漏洞安全风险通告

2021年8月12日，奇安信CERT监测到微软紧急发布Windows Print Spooler远程代码执行漏洞（CVE-2021-36958）通告。该漏洞细节已公开披露，当Windows Print Spooler服务不正确地执行特权文件操作时，存在远程执行代码漏洞。成功利用此漏洞的攻击者可以使用SYSTEM权限运行任意代码。截至本文发布时，微软尚未发布针对此漏洞的补丁程序。鉴于此漏洞影响较大，建议客户尽快自查，并采取处置建议中的措施以缓解此漏洞。

### 微软8月安全更新多个漏洞预警

2021年8月11日，国家漏洞库CNNVD发布预警，微软官方发布了多个安全漏洞的公告，包

括 Microsoft Windows TCP/IP component 缓冲区错误漏洞（CNNVD-202108-856、CVE-2021-26424）、Microsoft Windows 代码注入漏洞（CNNVD-202108-863、CVE-2021-26432）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据、提升权限等。微软多个产品和系统受漏洞影响。目前，微软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。

## Microsoft Exchange 多个远程代码执行漏洞预警

2021 年 8 月 9 日，网络安全威胁和漏洞信息共享平台发布预警，有关 Microsoft Exchange 多个远程代码执行漏洞（CVE-2021-34473、CVE-2021-34523、CVE-2021-31207）的技术细节以及 POC 已在互联网上公开，攻击者可根据这些漏洞细节开发出漏洞利用代码，从而在无需身份验证的情况下组合这些漏洞在目标服务器上执行远程代码，从而接管目标服务器。微软已在 7 月补丁日发布这些漏洞的修复补丁，建议受影响用户及时更新漏洞补丁，做好资产自查及预防工作，以免遭受黑客攻击。

## Linux eBPF 本地提权漏洞安全风险通告

2021 年 8 月 6 日，奇安信 CERT 监测到有安全研究员发布了 Linux kernel eBPF 本地提权漏洞 (CVE-2021-3490) 的漏洞细节和 POC，并在 Ubuntu 21.04 上进行了演示。该漏洞是由于按位操作（AND、OR 和 XOR）的 eBPF ALU32 边界跟踪没有正确更新 32 位边界而导致，利用该漏洞可触发越界读写，从而从普通权限提升到 root 权限。鉴于漏洞危害较大，建议用户及时升级版本。

## Windows NTLM 中继攻击漏洞安全风险通告

2021 年 8 月 5 日，奇安信 CERT 监测到微软发布了针对 Active Directory 证书服务 (AD CS) 的 NTLM 中继攻击漏洞缓解通告（ADV210003）。此漏洞允许攻击者强制域控制器向指定机器进行 NTLM 身份认证，未经身份认证的攻击者可利用此漏洞发起 NTLM 中继攻击并接管 Windows 域。目前该漏洞的细节及 POC 已公开，漏洞危害上升，奇安信 CERT 强烈建议客户实施微软推送的缓解措施，以缓解该漏洞危害。

## Node.js 远程代码执行漏洞 (CVE-2021-22930) 预警

2021 年 8 月 4 日，网络安全威胁和漏洞信息共享平台发布预警，Node.js 发布安全更新，修复了 Node.js 中的一个释放后使用 (Use-After-Free) 漏洞（CVE-2021-22930）。攻击者可利用该漏洞执行远程代码攻击，最终获取服务器控制权。建议受影响用户尽快更新至安全版本，并做好资产自查及预防工作，以免遭受黑客攻击。

## 奇安信 CERT：近期需重点关注的 27 个高风险漏洞

2021 年 7 月，奇安信 CERT 监测到新增漏洞 2072 个。经人工研判，本月值得重点关注的漏洞共 103 个，其中高风险漏洞共 27 个，包括多个 WebLogic 远程触发漏洞、多个遭在野利用的 Windows 内核漏洞等，约一半漏洞细节和 POC 已公开或遭到在野利用。

（关注公众号“奇安信 CERT”，发送“202107”可查看 7 月需重点关注的漏洞完整清单）

对抗篇

# 国内攻防演习7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7月，奇安信Z-TEAM团队共承接攻防演习服务11场，其中包括地市级攻防演习服务3场，本单位自主攻防演习服务8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多个行业，客户存在的安全问题主要涉及互联网侧应用更新不及时、内网安全设备策略配置不当，以及人员网络安全意识不足。具体情况如下。

### 1、钓鱼攻击方式多样

本月任务中针对不同目标，根据业务特点不同，在钓鱼目标选择、钓鱼木马素材及话术组织方面均做了针对性的准备工作。比如，针对客服人员和人事部门目标，采取业务咨询、第三方合作或网络应聘等方式；针对管理人员和职能部门目标，则采取业务申请或报告提交等方式进行钓鱼突破。

### 2、供应链攻击途径丰富

本月任务中供应链攻击手段运用比较丰富，除了常见的第三方软件代码审计、漏洞挖掘，还根据目标业务自身特点，针对目标网络内自研产品的开发包进行恶意代码植入来完成供应链攻击。

### 3、业务网络缺乏纵深防护机制

目标网络及关键业务安全防护缺乏纵深防护机制。主要表现为：从外部突破进入目标内网后，内网安全部署缺乏功能域划分、Vlan隔离等措施，尤其是核心业务系统强防护或隔离措施缺乏。

### 4、人员网络安全意识不足

本月任务中发现各目标客户在网络安全意识方面存

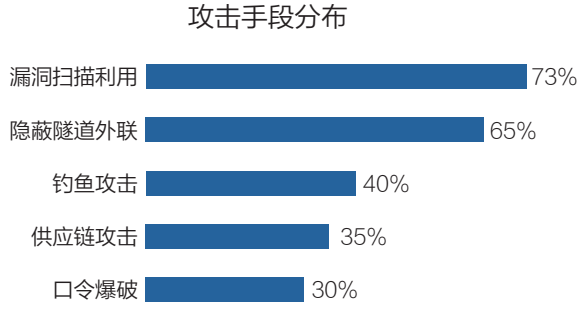
本月攻防演习成果：

| 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 | 15 | 6 | 15 | 48 | 5 | 36 | 72 | 2110 |

在严重不足，在弱口令、防范钓鱼攻击方面意识淡薄，为攻击队突破网络提供了可乘之机。

## 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，对目标业务突破，采用互联网侧系统漏洞利用和钓鱼攻击进行突破，内网横向拓展则以隐蔽隧道外联、内网漏洞利用、水坑攻击、仿冒认证、弱口令（口令复用）等手段为主。使用的主要攻击手段分布如下：




### 1、漏洞扫描利用

本月任务中发现的漏洞主要集中在行业应用系统上，主要以 Weblogic 反序列化、Shiro 反序列化、Fastjson 反序列化、WebSphere 反序列化漏洞为主。这些漏洞大量存在主要是由于相关行业应用开发平台比较集中，应用组件多存在缺陷导致。而目标系统运维人员安全意识不足、没有形成常态化的安全运营机制则导致应用系统版本更新不及时、安全策略设置不严格。

### 2、隐蔽隧道外联

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

### 3、钓鱼攻击

本月任务中外网突破钓鱼手段丰富，有针对性地对客服人员、第三方服务支持或人事招聘人员开展钓鱼诱骗，通过业务咨询、业务合作及岗位应聘等途径进行诱骗。

### 4、供应链攻击

本月任务中采用多种途径对目标网络进行了供应链攻击，主要包括：针对某目标官网的第三方开发应用，通过特征定位搜索开源代码，对源码审计、挖掘漏洞并成功利用；针对某目标内网自研安全浏览器，分析发现该浏览器基于 Chrome 内核调用实现功能，利用 Chrome 安全机制提取相关缓存认证信息；针对某目标应用系统的开发环境，对其可调用的 PIP 工具包进行污染，植入恶意代码来完成供应链攻击。

### 5、口令爆破

本月任务中的弱口令爆破全部存在于目标内网，主要针对目标内网的相关网络应用、安全设备和服务器。通过搜集目标网络中各种设备的默认口令、弱口令来分析其密码组合规律，从而实现快速爆破。

## 四、典型攻击手段的实现案例

### 1、外部漏洞利用突破

（1）某目标互联网回溯管理平台系统存在 Shiro 反序列化漏洞，可通过漏洞利用获取服务器控制权限。

（2）某目标外网 e-learning 学习系统存在 Fastjson 反序列化漏洞，可通过漏洞利用获取服务器控制权限。

（3）某目标电子文档管理系统存在 Apache Solr 远程命令执行漏洞，可通过漏洞利用其突破外网。

（4）某目标外网 OA 系统存在 0day 漏洞，可通过漏洞利用远程命令执行控制 OA 服务器。

### 2、钓鱼突破

（1）针对某电子商务平台客户服务、第三方合作客

服业务较多的特点，以假冒客户投诉、第三方业务合作咨询等身份对相关客服人员进行钓鱼攻击，成功获取内网个人终端控制权。

（2）利用某目标单位正在招聘的时机，以应聘的名义对目标 HR 人员进行钓鱼诱骗，获取人事部门计算机控制权。

（3）针对某政务系统对外服务的特点，以相关业务报告形式对目标职能人员进行钓鱼诱骗，获取该政务系统运维人员主机控制权限。

## 3、供应链攻击

（1）本月任务中通过对某目标官网进行分析，利用系统特征定位服务商为 bocadmin，进一步通过 GitHub 寻找到相关代码，对代码进行审计，挖掘出未授权任意密码重置漏洞，利用此漏洞获取该目标官网后台控制权限。

（2）本月任务中发现某目标业务内网使用内部自研浏览器，经分析发现该浏览器基于 Chrome 内核调用实现功能，遂利用 Chrome 安全认证机制成功提取到目标业务人员的浏览器缓存认证信息，获取了对内网进一步拓展的关键条件。

（3）经前期信息搜集发现，某目标业务部署较多是自研应用或平台，分析发现其主要开发语言为 Python，随即对开发所需的 PIP 工具包进行污染，植入恶意代码，来完成供应链攻击。

## 4、内网弱口令横向拓展

（1）某目标内网 mysql 数据库服务器普遍存在弱口令，通过弱口令可控制内网 594 台数据库服务器。

（2）某目标内网域控存在弱口令，通过弱口令控制域控后，同时可控制内网 13 个域控、16 万 + 域内主机和 8 万 + 域内用户。

（3）某目标内网 vCenter 服务器存在弱口令，通过弱口令拓展控制该 vCenter 服务器，可控制内网百余台测试服务器，其中包括 OA 系统、数据库测试集群、Zabbix、动态感知、POC 链路监控系统等核心系统服务器。

## 政策篇

国内，《个人信息保护法》通过，我国个人信息保护有了法律“安全锁”；《关键信息基础设施安全保护条例》历经四年打磨终于发布，标志着我国网络安全保护进入了以关键信息基础设施安全保护为重点的新阶段。

国际上，美参议院通过基础设施法案，为网络安全拨款 20 亿美元；拜登总统签发改善关键基础设施控制系统网络安全备忘录，为关基设施制定网络安全绩效目标；NIST 发布《零信任架构规划指南》草案，概述了如何用风险管理框架帮助开发和实施零信任架构。


### 《个人信息保护法》表决通过，2021 年 11 月 1 日起施行

2021 年 8 月 20 日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，自 2021 年 11 月 1 日起施行。其中明确：通过自动化决策方式向个人进行信息推送、商业营销，应提供不针对其个人特征的选项或提供便捷的拒绝方式；处理生物识别、医疗健康、金融账户、行踪轨迹等敏感个人信息，应取得个人的单独同意；对违法处理个人信息的应用程序，责令暂停或者终止提供服务。

### 网信办等五部门发布《汽车数据安全管理若干规定（试行）》

2021 年 8 月 20 日，网信办、发改委、工信部、公安部、交通运输部联合发布《汽车数据安全管理若干规定（试行）》），自 2021 年 10 月 1 日起施行。《规定》倡导，汽车数据处理者在开展汽车数据处理活动中坚持“车内处理”“默认不收集”“精度范围适用”“脱敏处理”等数据处理原则，减少对汽车数据的无序收集和违规滥用。

### 李克强签署国务院令，公布《关键信息基础设施安全保护条例》

2021 年 8 月 17 日，国务院总理李克强签署国务院令，公布《关键信息基础设施安全保护条例》，自 2021 年 9 月 1 日起施行。《条例》明确了关键信息基础设施范围和保护工作原则目标；明确了监督管理体制；完善了关键信息基础设施认定机制；明确运营者责任义务；明确了保障和促进措施；明确了法律责任。《条例》的公布，标志着我国网络安全保护进入了以关键信息基础设施安全保护为重点的新阶段。

### 工信部印发《关于加强智能网联汽车生产企业及产品准入管理的意见》

2021 年 8 月 12 日，工信部印发《关于加强智能网联汽车生产企业及产品准入管理的意见》，要求加强汽车数据安全、网络安全、软件升级、功能安全和预期功能安全管理，保证产品质量和生产一致性，推动智能网联汽车产业高质量发展。《意见》从加强数据和网络安全管理、规范软件在线升级、加强产品管理、保障措施等方面提出了 11 项具体意见。

## 《党委（党组）网络安全工作责任制实施办法》公开

2021年8月4日，《人民日报》头版发布《中国共产党党内法规体系》一文。同时，《中国共产党党内法规体系》公开出版发行，收录了《党委（党组）网络安全工作责任制实施办法》，这是该文件首度解密公开。《实施办法》提出，各级党委（党组）领导班子主要负责人是本地区本部门网络安全工作的第一责任人。《实施办法》作为《中国共产党党内法规体系》唯一收录的网络安全领域的党内法规，它的公开发布对厘清网络安全责任、落实保障措施、推动网信事业发展将产生巨大影响。此前在2017年8月15日，中共中央印发《党委（党组）网络安全工作责任制实施办法》。

国际

## 美参议院通过基础设施法案，为网络安全拨款20亿美元

据ITPro 8月12日消息，美国参议院8月10日通过拨款总额过万亿美元的《基础设施投资和就业法案》。参议院多数党领袖查克·舒默表示，该法案是“数十年来最强劲的基础设施注入资金”，将振兴美国的基础设施。该法案为网络安全拨款约20亿美元，其中约10亿美元将用于设立州和地方政府网络安全拨款；3.5亿美元用于加强电网安全；2.5亿美元用于加强能源网络安全；1.57亿美元用于国土安全部科技署开展网络安全研究；1亿美元用于网络响应和恢复基金等。

## NIST发布《零信任架构规划指南》草案

2021年8月4日，美国国家标准与技术研究院（NIST）发布了《零信任架构规划：管理员入门指南（草案）》白皮书，本白皮书提供了NIST风险管理框架的顶层概述及其如何帮助开发和实施零信任架构。NIST认为，零信任是在规划和实施企业体系架构时使用的一系列网络安全原则。零信任架构要成功地改善企业安全态势，需要来自企业各利益相关方的输入和合作，但由于其中一些利益相关方可能不熟悉风险分析和管理，风险管理框架为安全规划人员和系统操作人员提供了一套通用的概念和任务。

## 美国海岸警卫队发布2021版《网络战略展望》

据Defense Daily 8月3日消息，美国海岸警卫队发布《网络战略展望》，这是其2015年发布初版以来的首次更新。该文件重申将网络空间确立为海岸警卫队的新作战领域，将采取行动保护海上运输系统免受在网络空间和通过网络空间传递的威胁，以及追究那些通过攻击美国的网络、操作或海上运输系统对美国造成伤害人员的责任。该文件共八个部分，简介、海岸警卫队和网络空间行动、网络空间中的海上运输系统、行动1- 保卫和运行企业任务平台、行动2- 保护海上运输系统、行动3- 通过网络空间开展行动、关键赋能者和结论。

## 拜登总统签发改善关键基础设施控制系统网络安全备忘录

据美国白宫7月28日消息，美国总统拜登签署了改善关键基础设施控制系统网络安全国家安全备忘录。该备忘录通过指导国土安全部和商务部与其他机构一起合作，制定网络安全绩效目标，设定一个清晰、易于理解的安全基线，向改善关键基础设施网络安全迈出了关键的一步。近半年来，美国白宫和相关部委发布了多项网络安全政策文件。

奇安信

# 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

# 2021 网络安全的上半场

攻击事件激增，
政策密集出台，
行业投资暴涨，
一起盘点 2021 网络安全的上半年。

# 2021 上半年全球网安政策趋势报告

作者 公关部 张文辉

转眼间，2021 年已过大半。回顾 2021 年上半年，新冠疫情的影响还未消退，网络攻击态势却愈演愈烈。

勒索软件为代表的安全事件频发。据统计，2021 年平均每 11 秒就发生一次勒索攻击事件，预计今年全球勒索软件损失将达到 200 亿美元。5 月，美国最大燃油运输管道公司科洛尼尔和全球最大肉类供应商 JBS 集团遭勒索攻击，造成短期内石油、肉类供应紧张。

数据泄露数量规模不断扩大，对国家安全、企业安全、民众安全均带来了严重的危害。2021 年以来，社交巨头 LinkedIn 已经历了三轮大规模用户个人资料被恶意抓取，共计 18 亿用户数据遭泄露；4 月，Facebook 超 5 亿用户信息泄露，涉及全球 106 个国家。

此外，重大安全漏洞不断涌现，涉及众多知名厂商。3 月，苹果公司紧急修复远程命令执行漏洞，影响涉及数十亿设备；4 月，国内厂商小米披露了其 MIUI 系统的越权漏洞预警，攻击者可利用该漏洞获取前台运行进程信息；5 月，高通移动调制解调器 MSM 芯片被曝存在安全漏洞，影响全球 40% 手机。

2021 年网络安全进入新阶段：安全事件频发、影响日益严重，促使多国竞相出台加强网络安全建设的政策、法律和规划。

本文梳理全球主要国家在 2021 年上半年发布的政策法规，从国家战略、新兴技术、数字治理、供应链安全和关键信息基础设施保护等角度，展示全球网络安全发展态势。

## 一、多国出台国家网络安全战略，占据网络空间竞争优势

2021 年上半年，美国、欧盟、英国、俄罗斯、日本等国纷纷出台国家安全总体战略，重点加强网络安全顶层规划建设，力图在全球网络空间激烈竞争局势中占得先机。

### （一）美国将网络安全列为国家优先级别

随着年初美国总统拜登正式上任，加之近期出现的一系列重大安全事件，美国政府加紧出台新版国家安全总体战略，并提出将网络安全列为国家安全首位。

2021 年 3 月，美国白宫发布《国家安全战略临时指南》，作为拜登政府发布的第一份全面应对国际国内局势的政策指导文件，该指南提出加强美国在网络空间中的能力和弹性。通过鼓励公私合作、加大资金投资、加强国际合作、制定网络空间全球规范、追求网络攻击责任、增加网络攻击成本等方式保护美国网络安全，同时特别强调国家网络人才库多样化的重要性。

2021 年 5 月，美国总统拜登签署发布了《改善国家网络安全行政令》，旨在从保护联邦网络、改善美国政府与私营部门间信息共享以及增强美国对安全事件响应能力等方面，提高国家网络安全防御能力。美国政府将通过推动联邦政府采用零信任架构、改善软件供应链安全、建立网络安全审查委员会以及提升漏洞和事件处置能力等措施，实现网络安全现代化的目标。

2021 年 6 月，美国国会参议院高票通过了《2021 美国创新和竞争法案》，该法案主要由 1 个拨款方案和 4 个相互独立的法案构成，涉及芯片、5G、航空航天、网络安全及人工智能、医学研究、美国制造等多个领域，相关投资额约 2500 亿美元，包括：向半导体制造业补贴逾 500 亿美元；向美国国家科学基金会（NSF）拨款 810 亿美元，用于人工智能、计算机技术等 10 个重点领域研究；向 5G 行业提供 15 亿美元以鼓励技术创新等。

### （二）欧盟制定数字十年的网络安全战略

欧盟在“战略自主”的框架下全面提出数字主权建设，并计划围绕这一整体战略出台一系列政策法规。未

来十年，欧盟将通过大力发展数字技术和数字基础设施，推进全球网络空间开放合作。

2021 年 3 月，欧盟委员会发布《关于欧盟数字十年网络安全战略的结论》文件。该战略于 2020 年 12 月底发布，旨在增强欧洲抵御网络威胁的能力，并指出未来欧盟主要行动包括建立欧盟安全运营中心网络计划；明确欧盟网络安全危机管理框架；加强与国际组织和伙伴国家的合作，以增强网络威胁形势的共识等。

2021 年 3 月，欧盟委员会发布《2030 数字指南针：欧洲数字十年之路》报告，明确了到 2030 年，欧洲数字化转型的目标和实现途径。报告制定了包括提升公民数字素养、建立安全和可持续的数字基础设施、推动企业数字化转型、促进公共服务数字化在内的四大类目标。为落实欧盟总体数字计划中的部分规定，欧盟委员会于 2021 年 6 月提出欧盟数字身份框架计划，敦促成员国为欧盟所有公民设立数字身份档案系统，提供数字身份钱包。

### （三）英国制定战略重塑国家网络安全愿景

在面对新冠疫情、地缘政治与脱欧等多重挑战的背景下，英国政府制定“全球英国”的战略规划愿景，并提出总体目标，将网络安全列为英国目前面临的核心问题。

2021 年 3 月，英国政府正式发布《竞争时代的全球英国：安全、国防、发展与外交政策综合评估》报告，该报告提出四项总体目标：一是通过科学和技术来维持战略优势；二是塑造未来的开放国际秩序；三是加强国内外的安全与防御；四是在国内外建立弹性。

根据报告显示，英国即将发布 2021 年新版网络战略。该战略明确了五大优先事项：一是加强英国的网络生态系统，采取一种整体的网络方法，并加深政府、学术界和业界之间的合作伙伴关系；二是建立一个弹性和繁荣的“数字英国”，使民众在网络中感到安全，并对个人数据受到保护充满信心；三是引领对网络力量至关重要的技术，包括微处理器、安全系统设计、量子技术和新形式数据传输等；四是与其他政府和业界合作，并利用英国在网络安全方面的思想领导力，促进自由、开放、和平与安全的网络空间；五是发现、破坏和威慑英国的对手。

### （四）俄罗斯新版国家战略中新增信息安全保障

2021 年 7 月，俄罗斯总统普京签署新版《国家安全战略》。此战略由俄罗斯联邦安全会议制定，是国家安全保障领域的最高层次指导文件。俄罗斯《国家安全战略》每六年更新修订一次，与 2015 年底颁布的上一版战略相比，新版战略首次加入信息安全章节，体现了俄罗斯对于网络信息安全的重视程度日益增加。

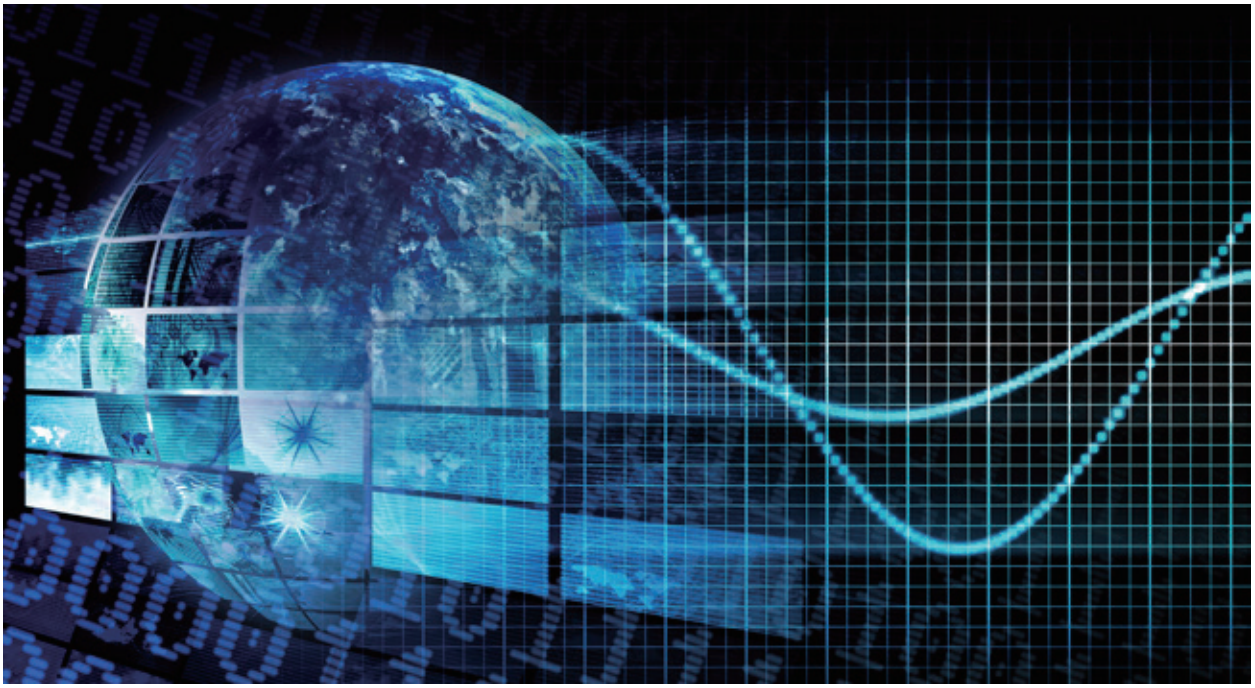
新版《战略》主要分析了当前全球和俄罗斯的发展态势及安全环境，提出了国家和社会安全、信息安全、科学技术发展等九个国家战略性优先事项，并明确了各优先事项框架下的形势、目标与任务。

在信息安全领域，该战略明确反对他国运用信息通信技术对俄罗斯实施网络攻击、情报侦察，防止运用互联网散布不利于俄罗斯政治局势稳定的不实信息等，提出包括加强电子数据管理系统防护、建立信息安全威胁预警系统、应用人工智能技术和量子计算等先进技术改进信息安全保障方法等 16 项任务。

### （五）日本发布网络安全战略应对复杂安全形势

为应对日益严峻的数字化威胁以及东京奥运会网络安全挑战，日本发布一系列网络安全战略文件。2021 年 5 月，日本内阁秘书处内阁网络安全中心（NISC）发布《下一代网络安全战略纲要》《网络安全研发战略（修订版）》《网络安全委员会倡议》等多份有关网络安全的政策文件，进一步推进数字社会建设，构建网络防御体系，以建立自由安全的公共网络空间。

2021 年 7 月，日本发布新版《网络安全战略》草案并征求公众意见，战略草案确定了实施有关网络安全措施的五项基本原则，确保信息的自由传播、法治、开放性、自主性和多方合作。战略草案指出，为确保“自由、公平和安全的网络空间”，应从以下三个方向推进相关工作：一是在数字化变革的基础上，同步推进数字化转型和网



络安全；二是促进网络空间安全，“实现公民在社会能够安全的生活”；三是从安全角度加强努力，增强参与、协调和合作。

## 二、新兴技术构建万物互联，制度建设推动安全建设

近年来，以5G、人工智能、物联网等为代表的新兴技术迅猛发展，一个万物互联的智能时代即将诞生。物联网正在推动人类社会从“信息化”向“智能化”转变，促进信息科技与产业发生巨大变化。

在新兴技术为人类社会带来新一轮科技革命与产业变革的同时，其中也蕴藏着许多网络安全风险。

纵观全球，各国都在加快新兴技术战略布局，出台相应政策法规，确保智能时代的经济发展安全有序。

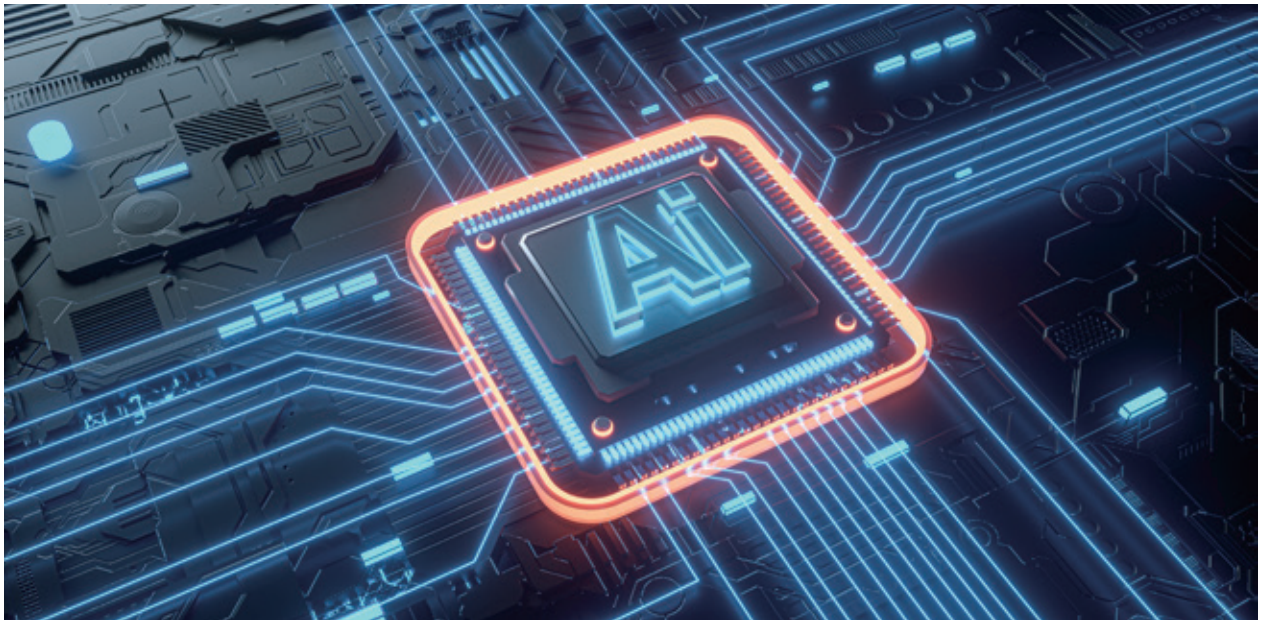
### （一）5G建设步入高速发展期，安全风险引发关注

如果说2020年是5G建设之年，那么2021年就是5G高速发展之年。随着5G技术的蓬勃发展，由此引发的网络安全问题成为各界关注的重点。2021年2月，移动安全公司AdaptiveMobile向GSM协会报告了最新研究成果，发现5G架构的网络切片与虚拟化网络功能存在安全漏洞，恶意攻击者可能借此跨越移动运营商5G网络上的各个不同网络切片，发动数据访问与拒绝服务攻击。

因此，各国纷纷发布与5G安全相关的战略、政策和标准，同时加大资金投入，致力于建立一个完善的5G发展体系。

**美国方面**，在2021年2月，美国国家标准与技术研究院（NIST）发布了《5G网络安全实践指南》草案，该指南旨在帮助使用5G网络的组织以及网络运营商和设备供应商提高安全能力。

2021年3月，美国国际战略研究中心（CSIS）发布《加速美国5G发展》报告，报告提出完善电信法规以消除监管障碍、与盟国建立网络安全合作机制等11项具体建议，确保美国5G发展能够最大程度的降低国家




安全风险，同时最大化经济回报。

2021 年 5 月，美国国家情报总监办公室、美国国家安全局和国土安全部网络安全与基础设施安全局联合发布《5G 基础设施潜在威胁载体报告》，分析了 5G 在政策标准、供应链、5G 系统架构三个领域的威胁载体，以加强对 5G 应用面临威胁的了解，制定全面的解决方案。

**欧盟方面**，在 2020 年 12 月，欧盟网络安全局（ENISA）发布《5G 网络威胁态势报告》，探讨了未来应如何利用安全技术帮助减轻 5G 网络安全风险的措施，对 5G 安全生态系统中的利益相关方提出了创新性建议。

2021 年 3 月，欧盟委员会在《关于欧盟数字十年网络安全战略的结论》文件中要求实施并加速完成欧盟 5G 工具箱，努力确保 5G 网络安全性和未来网络发展。

**对我国来说**，2021 年 6 月，国家发展改革委等四部门联合发布《能源领域 5G 应用实施方案》。实施方案提出进一步拓展能源领域 5G 应用场景、加快能源领域 5G 专用技术研发、加大相关基础设施和安全保障能力建设三项重点任务。在安全保障能力建设方面，实施方案要求构建 5G 应用安全保障体系，确保 5G 融合应用相关网络基础设施和核心系统安全。同时健全能源领域 5G 应用安全技术标准，将 5G 网络安全保障纳入能源领域 5G 应用的全流程、全环节。

2021 年 7 月，工信部、中央网络安全和信息化委员会办公室等十部门联合发布《5G 应用“扬帆”行动计划（2021-2023 年）》，旨在显著提升我国 5G 应用发展水平，保护 5G 应用安全等。根据行动计划，提升 5G 应用安全的具体举措包括以下四个方面，一是加强 5G 应用安全风险评估；二是开展 5G 应用安全示范推广；三是提升 5G 应用安全评测认证能力；四是强化 5G 应用安全供给支撑服务。

### （二）人工智能引发双重考验，政策监管仍需加强

近年来，人工智能技术日趋成熟，应用十分广泛。伴随而来的网络安全问题对现实生活也造成一定影响，Facebook 创始人兼 CEO 扎克伯格、美国前总统奥巴马均遭遇过“AI 换脸”，引发社会广泛关注。目前，以美欧为代表的西方国家正加快出台监管政策，规范人工

智能领域发展。

**美国方面**，在2021年3月，美国国家人工智能安全委员会向国会提交发展人工智能的最终建议报告。报告规划了美国在人工智能时代取胜的战略，并制定了行动路线图。报告中首次提及，中国拥有在未来10年超越美国成为人工智能领域领导者的“潜力”，建议美国政府在领导力、人才、硬件和创新投资等四个方面立即采取应对行动。

2021年7月，美国国土安全部科学技术局发布《人工智能与机器学习战略计划》，提出了未来三大战略目标：一是推动用于跨领域国土安全能力的下一代人工智能和机器学习技术发展；二是促进在国土安全任务中使用经过验证的人工智能与机器学习能力；三是建立经人工智能与机器学习技术培训的跨学科员工队伍。

**欧盟方面**，在2021年4月，欧盟委员会通过了《人工智能法》提案，旨在建立关于人工智能技术的统一规则。提案不仅对人工智能技术在诸如汽车自动驾驶、银行贷款、社会信用评分等一系列日常活动中的应用设定了限制，而且还对欧盟内部的执法系统和司法系统使用人工智能的情形提出了相应的问题解决方案。

2021年5月，欧洲政策研究中心（CEPS）成立的人工智能和网络安全工作组，发布了《人工智能与网络安全：技术、治理和政策挑战》报告。该报告概述了人工智能在网络安全领域的有效应用，以及人工智能系统可能被操纵所带来的风险，并介绍了与人工智能实施相关的主要伦理影响和政策问题。报告根据欧盟数字战略的目标，提出了建设性和具体的政策建议，以确保人工智能的安全应用。

### （三）物联网成网络攻击重灾区，相关政策加紧出台

随着万物互联时代的到来，机构物联网设备数量不断增加，但缺乏对应保护措施，相关网络攻击事件频发。2021年3月，特斯拉工厂摄像头供应商被黑，导致多家机构共计15万个监控访问权限被获取。近期，各国政府加快出台有关政策法规，加强物联网安全防范。

**美国方面**，在2021年3月，美国参议院与众议院再次引入《网络护盾法案》，其中建议为物联网设备创建一个自愿的网络安全认证计划。该法案建议由各界网络安全专家组成的咨询委员会负责为物联网设备定义一个安全标准。所生产产品符合这些标准的物联网制造商可以将此认证展示给公众并打上“网络护盾”标签，这将有助于消费者在购买物联网设备时做出决策。

**英国方面**，在2021年4月，英国数字、文化、传媒和体育部（DCMS）发布了对《物联网设备网络安全提案》征求意见稿的回复。该提案概述了英国政府对调控物联网设备网络安全的意图和政策主张，并倡导通过完善立法来促进消费者使用物联网设备的安全性。根据该提案，英国政府将制定新的监管计划，以保护消费者免受不安全的物联网设备的伤害。同时能够在不影响有效性的情况下，采取合适的方法赋予制造商一定的义务和责任，以实现对公民、网络和物联网基础设施的持续性保护。

**对我国来说**，2021年6月，工信部发布《车联网（智能网联汽车）网络安全标准体系建设指南》（征求意见稿）。该指南针对车载联网设备、基础设施、网络通信、数据信息、平台应用、车联网服务等关键环节，提出覆盖终端与设施安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等方面的技术架构。

2021年6月，工信部发布《关于加强车联网（智能网联汽车）网络安全工作的通知》（征求意见稿），其中要求加强车联网网络安全、平台安全、数据安全防护，强化安全漏洞管理。具体包括落实企业网络安全主体责任，建立健全数据安全管理制度，加强个人信息与重要数据保护等。

## 三、数据安全成为全球关注重点，各国加快数据治理进程

随着全球数字化转型，数据资源已经成为数字时代的“软黄金”，推动国民经济快速发展。与此同时，数据泄露事件屡见不鲜，对国家安全、企业安全和民众

安全均带来了严重的危害。根据安全公司 Risk Based Security 最近发布的《2021 年上半年数据泄露速览报告》显示，2021 年上半年共有 1767 起公开报告的泄露事件，美国报告的泄露事件数量增长了 1.5%，泄露数据总量达 188 亿条记录。

当前，各国都在加紧制定数字战略，力求在数字化发展的浪潮中为数据安全保驾护航。以欧盟、美国为代表的西方国家和组织，相继推出较成熟且侧重点不同的配套数据安全政策法规。我国在数据安全方面也陆续推出了一系列法律法规及标准规范。

### （一）加强数据安全顶层规划

**对欧盟来说**，其数据安全立法处于全球领先地位，颁布的众多政策法规都颇具影响力。2018 年 5 月正式实施的欧盟《通用数据保护条例》（GDPR）是全球第一部全面的隐私保护法，对各国的立法均具有启示意义。2021 年 2 月，欧盟发布的《电子隐私条例》草案，是作为 GDPR 在电子通信领域的细化和补充的特别法，通过对数据类型的分类保护（例如区分电子通信内容和元数据）和对法人、自然人共同保护的方式加强和扩大了对隐私保护的力度和范围。

**对美国来说**，其跨国信息巨头遍布全球，数据资源为美国创造了巨大的利益，因此美国数据治理模式更偏向于利益导向。美国目前尚未出台国家层面统一的数据安全立法，大多是各州颁布的数据法案。例如，美国加利福尼亚州的《加州隐私权法案》、弗吉尼亚州的《消费者数据保护法》和科罗拉多州的《科罗拉多州隐私法案》等。此外，美国政府还通过了《统一个人数据保护法》，该法案将成为各州数据隐私法案范本。

**对我国来说**，随着数据安全保护浪潮的兴起和各国数据安全保护实践的深入，我国逐步建立了以《中华人民共和国网络安全法》《中华人民共和国数据安全法》为统领，专项法律、行政法规、部门规章为支撑，标准规范文件为配套的制度体系。同时，《个人信息保护法》正式通过，进一步完善了我国个人隐私保护法律体系。

### （二）规范数据跨境流动制度

近年来，各国都在出台有关数据保护的法律法规，其中大多涉及数据跨境流动的法律或政策，但不同国家的立法标准不一致。

欧盟以“构筑单一数字市场”为战略目标，按照“外严内松”原则引领建立全球数据规则体系。2021 年 6 月，欧洲数据保护委员会正式通过关于英国的充分性决定，该决定表明未来 4 年内，英国和欧盟的个人数据可以自由合法地流动。同月，作为对 Schrem II 案（该案废止了美欧数据跨境转移机制“隐私盾协议”）的回应，欧盟数据保护委员会正式通过两份关于数据跨境传输合法性的指导性意见。此外，欧盟委员会还颁布了新的关于数据跨境传输的标准合同条款的最终版本。

美国以维护数字竞争优势和强化“长臂管辖”为主旨，构建数据跨境流动与限制政策。2021 年 6 月，美国白宫颁布《关于保护美国公民敏感数据免受外国对手侵害的行政令》，该行政令撤销了特朗普政府针对 TikTok 等与中国相关软件应用程序的限制性政策，同时提出了一套全新的审查流程，由美国商务部持续评估国外联网软件应用的安全风险。该行政令表明美国政府正逐步出台相关法规限制本国数据跨境流动。

我国以维护国家数据主权、确保安全与发展并重为目的，逐步建立数据跨境流动保护体系。首先，《数据安全法》中规定了对跨境数据实施数据安全审查制度和数据出口管制，初步确立了我国针对数据跨境流动的基本法律框架。其次，《个人信息保护法》中规定跨境传输个人信息时需要对数据进行脱敏处理，同时在操作前要进行风险评估。最后，新修订的《网络安全审查办法》也增加了对数据安全方面的审查，同时要求掌握超过 100 万用户个人信息的企业赴国外上市，必须申报网络安全审查。

可以看出，各国数据跨境流动法律法规的主旨是在本国利益最大化的前提下合法推进数据跨境流动。在复杂形势下，我国应当建立完善数据跨境流动保障机制，确保国家安全、经济发展、维护公民权益的有效协同，真正推动我国数字经济的发展，维护数据主权。

### （三）个人隐私保护成为热点

随着新技术、新应用的快速发展，以人脸识别为代表的人工智能技术带来的隐私问题持续引发全球关注。今年3·15晚会，央视曝光了不少非法采集用户人脸信息的不良商家，引发民众对隐私数据的担忧。

生物识别数据披露的个人特征精确，且采集门槛较低、极易获取，一旦遭到泄露、篡改或非法共享，极易带来“身份盗窃”风险，且正在成为攻击者的主要目标。对此，各国政府纷纷出台相关政策，开始规范和限制生物识别数据的使用。

**在人脸识别信息保护方面**，2021年3月，我国国家互联网信息办公室、公安部发布通告称将加强对语音社交软件和涉“深度伪造”技术的互联网新技术新应用安全评估工作。腾讯、阿里巴巴、字节跳动、快手、小米等11家企业因未履行安全评估程序被国家有关部门约谈。2021年7月，我国最高人民法院审委会通过的《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》也进一步明确，处理人脸信息必须征得自然人同意，不得强迫、变相强迫同意处理其人脸信息。

**在车联网数据保护方面**，2021年3月，欧盟数据保护机构发布了《车联网个人数据保护指南》。该指南聚焦于欧洲车联网个人数据保护，并提出指纹等生物识别数据应当存储在车内，应当从车联网设计阶段即将数据保护纳入考虑等建议。我国也发布了一系列有关联网汽车的数据保护制度，2021年8月，国家互联网办公室等五部门出台《汽车数据安全管理若干规定（试行）》；2021年6月，工信部出台《关于加强车联网（智能网联汽车）网络安全工作的通知》（征求意见稿）。

**在APP个人信息保护方面**，近期我国有关机构颁布一系列技术规范与标准文本，旨在规范APP个人信息收集行为，保障公民个人信息安全。2021年3月，国家互联网信息办公室秘书局、工信部办公厅、公安部办公厅、国家市场监督管理总局办公厅四部门联合发布《常见类型移动互联网应用程序必要个人信息范围规定》；2021年4月，工信部发布《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》。

此外，我国不同行业主管部门也针对各领域特点制定相应政策法规，重点保护各行业有关数据。例如，交通运输部制定《交通运输政务数据共享管理办法》、国家医疗保障局制定《加强网络安全和数据保护工作指导意

见》等。

## 四、加强勒索软件防范，完善供应链风险管理与关基保护制度

近年来，勒索软件事件频发，造成的危害也愈加严重。近期，一起影响广泛的软件供应链勒索攻击事件引发全球关注。美国 IT 管理软件厂商卡西亚（Kaseya）遭遇勒索软件攻击，黑客组织利用一个 0day 漏洞将恶意软件部署至卡西亚的管理系统，全球上千家企业客户超 100 万个系统通过软件更新感染了勒索病毒，而勒索团伙开出了价值 7000 万美元的比特币赎金。

随着安全防护技术的升级，黑客开始对软件供应链及能源、医疗等关键信息基础设施行业等薄弱环节实施攻击。因此，各国纷纷出台相关举措以应对此类安全威胁。

### （一）积极防范勒索软件攻击

2021 年上半年以来，勒索软件攻击十分猖獗，根据安全厂商 SonicWall 报告显示，该公司检测到的攻击尝试达到 3.047 亿次，超过了 2020 年全年的攻击总数。美国是受勒索软件攻击最严重的国家之一，其中美国受影响较大的地区是佛罗里达州，有 1.111 亿次攻击尝试。美国政府近期接连出台多项打击勒索软件攻击的新举措。

**一是出台有关政策法规**，2021 年 6 月，美国司法部提交《关于勒索软件和数字勒索调查和案件的指导意见》备忘录，旨在通过一系列安全指令实践来阻止勒索软件感染、数据盗窃和向网络犯罪集团支付巨额款项等违法行为。

**二是成立打击勒索软件工作组**，成员包括网络安全和互联网企业、政府部门、执法机构、非营利组织以及国际组织等 50 余家机构。工作组通过公私部门合作的方式，共同研究提出应对勒索软件攻击的解决方案。

**三是建立专门网站**，用于汇集各机构最新勒索软件预警信息和应对指南。民众也可通过该网站向政府报送遭受勒索软件攻击的情况。

**四是美国司法部实施奖励计划**，提供 1000 万美元

的奖金，用于鼓励相关机构和个人提供具有国家背景的黑客身份或位置信息。

对我国来说，尚未出台专门针对勒索软件攻击的法律法规，更多是偏执行层面的规章制度。2021 年 7 月，国家互联网应急中心发布了《勒索软件防范指南》，其中规定了防范勒索软件要做到九要、四不要。包括要备份重要数据和系统、要设置复杂密码并保密、要做好身份验证和权限管理、要制定应急响应预案等九项建议。不要点击来源不明邮件、不要打开来源不可靠网站、不要安装来源不明软件，以及不要插拔来历不明的存储介质等四项建议。

### （二）着力加强软件供应链风险管理

根据奇安信《2021 中国软件供应链分析报告》数据显示，国内企业软件项目 100% 使用开源软件；近 9 成软件项目存在已知开源软件漏洞；平均每个软件项目存在 66 个已知开源软件漏洞，软件供应链安全面临巨大风险。

美国在遭遇 SolarWinds 大型供应链安全事件后，紧急出台了一系列有关供应链安全的政策法规。2021 年 2 月，美国总统拜登签署《确保信息和通信技术及服务供

应链安全》行政令，要求对半导体芯片等四类供应链产品开展审查，并在一年内完成对美国国防、通信科技、能源等六大部门的生产供应链进行风险评估，提出改善措施。

2021年4月，美国网络安全和基础设施安全局（CISA）和美国国家标准技术研究院（NIST）联合发布《防御软件供应链攻击》报告，描述了与软件供应链攻击相关的信息、关联风险及缓解措施。

2021年5月，美国总统签署的《关于改善国家网络安全的行政命令》，要求联邦政府采取行动确保软件供应链的安全性和完整性，其中包括要求向政府出售的软件必须符合基准安全标准，并引入软件物料清单。

2021年6月，美国参议院在通过的《2021年美国创新和竞争法案》中也提到要推进“弹性供应链战略”、帮助美国公司“获得稳定可控的全球供应链”等，从而确保美国在供应链安全方面的领导地位，减少网络攻击的产生。

目前，我国在软件供应链方面的政策法规较为缺失，从国家和行业监管层面来讲，应当制定有关政策要求、标准规范和实施指南，确保我国软件供应链安全有序的发展。

### （三）加大关键信息基础设施保护力度

美国是世界上最早意识到关键信息基础设施重要性并出台一系列完备政策法规的国家，但依然面临严峻的网络安全态势。最为严重的是美国最大燃油运输管道公司科洛尼尔遭到网络攻击后被迫停运，直接造成美国东海岸燃油短缺，美国运输安全管理局（TSA）由此宣布美国多个州进入紧急状态。针对该事件，美国政府部门随即出台了一系列措施。

2021年5月，美国国土安全部运输安全管理局（TSA）发布一项关于加强管道网络安全的安全指令，要求各管道供应商应及时向运输安全管理局与网络安全及基础设施安全管理局上报网络安全事件，并指派一位网络安全协调员，全天候待命。

2021年7月，TSA再次发布针对关键管道运营者的网络安全新要求的安全指令，该安全指令要求TSA指定的关键管道的所有者和运营商实施具体的缓解措施，以防止勒索软件攻击和对信息技术和运营技术系统的其他已知威胁，制定并实施网络安全应急和恢复计划，并进行网络安全架构设计审查。

此外，美国政府还采取建立网络安全审查委员会、启动针对关键基础设施保护的试点项目等措施，保障关键基础设施的安全，如电力行业网络安全“百日计划”等。

我国正加速推进以《网络安全法》为核心的关键信息基础设施保护法律体系建设。近日，国务院颁布出台《关键信息基础设施安全保护条例》（以下简称《条例》），这是我国首部专门针对关基安全保护工作的行政法规，开启了我国网络安全工作的新篇章。

《条例》对《网络安全法》所确立的关基安全保护制度作了进一步细化完善，明确了国家网信部门、国务院公安部门以及重要行业和领域的主管部门、监督管理部门等相关职能部门的责任边界和职责要求，明确了关基认定原则和认定机制，细化了运营者的主体责任和义务，形成了关基安全保护工作相关各方的法律责任体系。

此外，漏洞管理也属于关键信息基础设施保护的重要组成部分。2021年7月，工信部、国家互联网信息办公室、公安部联合发布《网络产品安全漏洞管理规定》，其中明确了网络产品提供者、网络运营者，以及从事漏洞发现、收集、发布等活动的各类主体的责任和义务。此项规定的出台，推动了网络产品安全漏洞管理工作的制度化、规范化、法制化。

回顾2021年上半年，全球面临严峻的网络安全态势，各类攻击事件层出不穷。各国都在加强网络安全顶层规划及细分领域制度建设。

2021年下半年，数据安全及个人隐私、供应链安全和关键信息基础设施保护等方面仍将是网络安全行业讨论的热点。我国对网络空间安全的重视程度正日益增强，未来网络安全行业必将迎来高速发展期。安

感谢李建平老师、包世玉同学对本报告的大力支持

# 2021年上半年5大安全热词

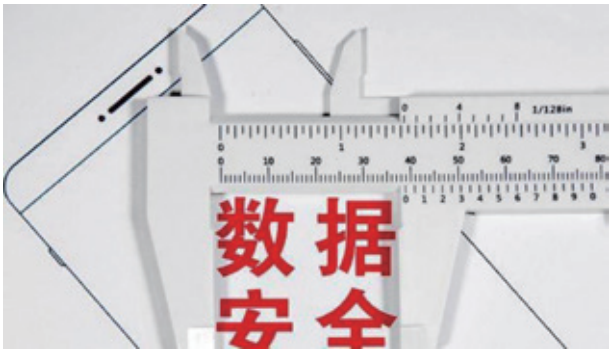
作者 公关部 张少波 魏开元 李建平 王梦琪 张雪丹

1 数据安全

## 2021年成数据安全产业“元年” 千亿级风口呼之欲出

2006年，英国数学家克莱夫·汉比（Clive Humby）第一次将“数据”比喻成“新的石油”。从那时起，数据即石油的新颖观点，就被经济学家、学者和CEO们屡次引用。

时至今日，克莱夫·汉比的论断，已经变成了现实。2018，我国即全面实施国家大数据战略，将数据定义为一种“战略资源”，把数据作为国家主权安全的保护对象。




2020年，中共中央、国务院发布了《关于构建更加完善的要素市场化配置体制机制的意见》，正式将数据作为与土地、劳动力、资本、技术并列的生产要素。在政策驱动下，互联网所产生的数据量呈现指数级增长，数字经济时代已然来临。

伴随着数字化转型进程的推进，数字技术的快速发展与广泛应用，数据价值的重要性随之递增。而围绕数据的安全保护，成为2021年最热的概念。

### 频频“霸屏” 数据安全概念“出圈”

“实体经济离不开数据要素的时候，数据的安全问题，就会成为牵一发而动全身的关键问题。”在第四届数字中国建设峰会上，奇安信集团董事长齐向东表示，数字经济时代，数据已经成为核心生产要素，数据经济这艘大船要想行稳致远，必须维护好数据安全这块“压舱石”。

从年初至今，数据安全的热度，就被持续关注。查看“数据安全”的微信指数，可以发现，第一次出现的峰值是6月11日，微信指数高达18,168,769，和《数据安全法》获得表决通过的时间点也完全吻合。

第二次的峰值，一度达到26,613,239，时间是7月5日，和某出行APP被通知下架完全吻合。

从《数据安全法》通过审议，到某出行公司因数据安全问题被国家七大部门调查，再到今年的数字中国峰会、数博会、中国网络安全年会，“数据安全”已经从专业领域，进入了社会大众的热议话题，频频在各主流媒体、各大社交平台上霸屏。

“如果数据不安全，就会带来两个方面的严重问题。一是严重威胁了国家和社会稳定，二是严重影响了老百姓

的日常生活。”齐向东多次提到数据安全的重要性。例如，在2020年，青岛某医院多名就诊人员的姓名、住址、联系方式等个人信息遭到泄露，还被造谣感染了新冠肺炎，严重影响了个人生活，对受害者造成了巨大的心理压力。

数据也验证了这一论点。根据信通院发布的白皮书显示，到2035年全球总数据量将超过2万亿TB，为目前数据总量的42倍。如此巨量的数据背后，隐藏的是严峻的数据安全挑战。

同样，市场调研公司Canalys的最新报告《网络安全的下一步》显示，2020年数据泄露呈现爆炸式增长，短短12个月内泄露的记录比过去15年的总和还要多。显而易见，保护数据安全已成为当务之急。

## 多重利好刺激<br>数据安全需求即将井喷

6月10日，十三届全国人大常委会第二十九次会议表决通过包括《数据安全法》在内的多项法案及两项决定。本次《数据安全法》相比此前草案，强调了建立工作协调机制，加强对数据安全工作的统筹；明确对关系国家安全、国民经济命脉、重要民生、重大公共利益等数据实行更严格的管理制度；同时，新法案进一步完善了保障政务数据安全方面的规定；并加大了对违法行为的处罚力度。

“《数据安全法》的出台，把数据安全上升到了国家安全层面，基于总体国家安全观，将数据要素的发展与安全统筹起来，为我国的数字化转型，构建数字经济、数字政府、数字社会提供法治保障。”奇安信集团总裁吴云坤对本次通过的《数据安全法》，第一时间进行了解读。

吴云坤认为，《数据安全法》的出台，将成为继《网络安全法》实施后，网络安全行业的又一个里程碑，势必驱动政府、机构和企业增加在数据安全领域的投资，用以完善安全防护体系，从而推动网络安全行业在数据安全领域的技术、产品加快创新和产业创新发展。

同样，7月初的滴滴事件，相当于给全民上了一堂“数据安全”普及课。7月2日开始，网信办旗下网络安全审查办公室宣布对“滴滴出行”实施网络安全审查，原因是“为防范国家数据安全风险，维护国家安全，保障公共利益。”

分析人士称，大数据时代，数据安全事关网络安全和国家安全，从无小事。滴滴被调查事件，给所有互联网平台敲了一记警钟，数据安全就是国家安全，更是企业的生死红线。

中国信息安全研究院副院长左晓栋表示，“我认为这次审查主要关注的是，重要数据和公民个人信息的出境安全风险。停止新用户注册，我认为是对这个数据进行保护的一个措施。”

而随着滴滴事件的发酵，资本市场开始关注相关板块。有研究人员表示，网络安全板块可能会因滴滴事件而爆发。当天，受此类消息影响，网络安全板块大涨，龙头股奇安信（688561）涨幅超过10%，蓝盾股份、绿盟科技、北信源涨幅均超过5%。随后四个交易日内，奇安信涨幅超过30%。

受多重政策利好消息影响，有观点认为，2021年或是数据安全的元年。

## 千亿风口浮出水面<br>体系化建设势在必行

“数据安全”引起社会各界紧密关注的同时，其蕴藏的庞大市场机遇，也随之浮出水面。根据工信部发布的统计数据显示，" 十三五 " 期间，我国大数据产业年均复合增长率超过了30%，2020年产业规模超过了1万亿元人民币。

中国社科院博士方燕预计，在万亿级别数据产业大盘子中，数据安全产业至少也是千亿级别，新的产业风口呼之欲出。

国泰君安证券认为，《数据安全法》的出台，将推动数据安全需求的释放。“由于数据流动贯穿信息化和业务系统的各层面、各环节，这对行业上下游的厂商提出了更高的要求，未来安全领域厂商将聚焦数据安全新

赛道、新业态。因此，那些有资源提前布局数据安全领域技术、产品、解决方案的头部厂商最为受益。

另一方面，数据泄露事件屡见不鲜，数据安全问题带来的损失与日俱增。有研究机构统计，2020年数据泄露总条数约为360亿条，数据泄露事件给企业造成的平均损失达386万美元。由于数据泄漏事件而造成经济损失极其重大，且负面影响也极为深远。


齐向东认为，全社会对数据安全的重视，包括《数据安全法》的审议通过，给安全行业带来了空前机遇，也给企业带来了更高要求。安全企业需为客户尽快开展数据安全治理和建立数据安全保护体系，尤其在身份安全、零信任、行为审计、数据敏感地图等领域加速技术创新。

在7月20日举行的2021年中国网络安全年会上，奇安信为了保护数据安全流动，对外发布了数据安全的“九板斧”，分别为：态势感知、零信任、云锁、特权账号安全管理、资配漏补的系统安全、邮件威胁检测系统、审查供应链、内生安全框架、隐私计算沙箱。

齐向东表示，“九板斧”从制度、人员管理、系统防护、供应链上下游、数据交易等方面，对数据流动形成完整的安全防护体系，在保障安全的前提下，对数据价值进行充分挖掘利用，推进数字经济安全稳步发展。

同时，奇安信还对外发布了“数据安全治理与保护体系建设路径图”，为数据安全治理和保护勾勒了面向未来的体系化建设路线。其中该路径图包括了精准防护、基于数据流转的安全保护、数据安全态势感知、数据要素数据交易安全等几大关键举措，涵盖了体系化建设的各个方面。

## 新赛道催生新机会 奇安信相关收入增速超100%

2021年9月1日，我国首部与数据安全相关的法律《数据安全法》将正式实施，该法律将成为继《网络安全法》实施后，网络安全行业的又一个里程碑，势必驱动政府、机构和企业增加在数据安全领域的投资，用以完善安全防护体系，从而促进网络安全行业在数据安全领域的技术、产品加快创新步伐，推动数据安全产业创新发展。

分析人士认为，在《数据安全法》的风口效应带动下，更多的新赛道、新技术和创新企业将不断涌现，和数据安全相关的市场规模也将快速提升。以奇安信为例，受益于国内数据安全与隐私保护政策及立法的快速推进，数据安全产品成为奇安信上半年增速最快的产品，整体收入同比增长率超过100%。（文/张少波）

2

## 软件供应链安全

# 定向爆破，广泛传播，供应链成安全最薄弱环节

2020 年 12 月，一场严重的安全危机在网络管理软件供应商 SolarWinds 内部爆发，全球超过 18000 家机构都受到了此次事件的影响。这次严重的安全事件，让供应链攻击再次回到了人们的视野中。

2021 年，这一上升趋势并未放缓。欧洲网络和信息安全局（ENISA）的报告分析认为，与去年相比，2021 年供应链攻击预计将增加 4 倍。

## 愈演愈烈的供应链安全威胁

顾名思义，供应链攻击是一种针对软硬件供应链的网络攻击形式。由于攻击目标往往处于供应链的上游，因此通常具备“攻其一点，伤及一片”的特点，尤其是攻击那些使用较为广泛的软硬件产品。

说起来，供应链攻击并非一种新出现的攻击手法，只不过在网络安全越来越受重视的今天，它作为一种效率极高的方式，而受到攻击者的青睐。《2020 软件供应链状态》报告显示，攻击者主动渗透开源项目向其植入被黑组件的“下一代”供应链攻击，在 2020 年同比暴增 430%。

2021 年，这一上升趋势并未放缓。ENISA（欧洲网络和信息安全局）报告——《供应链攻击的威胁分析》分析认为，与去年相比，2021 年供应链攻击预计将增加 4 倍。

并且仅在 2021 年上半年，就爆出影响广泛的数起软件供应链攻击事件。2021 年 2 月，研究员通过新颖的软件供应链攻击方式，成功侵入了微软、苹果、PayPal、特斯拉、Uber 等 35 家国际大型科技公司的内网。

2021 年 3 月 28 日，攻击者使用 PHP 的开发者账号，在 PHP 代码中植入了后门，其目标是可以通过该后门获得运行 PHP 的网站系统的远程代码执行权限。

2021 年 4 月 15 日，Codecov 宣布 bash uploader 脚本被攻击者修改，导致用户使用 Codecov 上传测试数据时，向攻击者的服务器发送敏感信息。通过该恶意脚本，攻击者可以获取客户软件源代码等机密信息。

甚至，供应链攻击开始与勒索攻击相结合。6 月底 7 月初，又一家美国 IT 管理软件 Kaseya 被黑，攻击者篡改了软件更新包用于向其客户传播勒索软件。上千家企业或受影响，包括至少 8 家使用其软件的托管服务商客户也被勒索，受影响最大的瑞士最大零售连锁店 Coop，旗下至少 800 家门店被迫停业。这也是全球首个重大供应链勒索软件攻击事件。

## 定向“爆破”，广泛传播

通过分析最近发生的较为严重供应链安全事件，我们不难发现在攻击路径上有一个明显的共性：攻击者利用 0day 漏洞攻陷软件供应商，并在软件中植入后门或者其他恶意软件，以此在该软件用户中进行广泛传播。

ENISA 的报告也印证了这样一个判断。根据其调查的供应链攻击事件显示，约 66% 的攻击者为了攻击目标客户，将注意力集中在供应商的代码上。

造成这种现象的原因主要有两个。

第一，在软件开发环节，上游软件供应商针对漏洞的防护以及响应能力不足，导致攻击者能够突破其安全防线，造成软件源代码或者更新包被攻击者篡改。

尽管在部分事件中，攻击者利用了多个 0day 漏洞进行组合攻击，客观上大幅度提升了防护难度，但通常而言，大量软件开发商对已知漏洞也依然“置若罔闻”。

根据奇安信发布的《2021 中国软件供应链安全分析报告》显示，在奇安信代码安全实验室分析的 2557 个国内企业软件项目中，平均每个软件项目存在 66 个已知开源软件漏洞，最多的软件项目存在 1200 个已知开源软件漏洞。其中，存在已知开源软件漏洞的项目占比高达 89.2%；存在已知高危开源软件漏洞的项目占比为 80.6%；存在已知超危开源软件漏洞的项目占比为 70.5%。

第二，在软件交付环节，下游用户在引入软硬件产品时，对其安全检查能力和意识不足，难以检测出软硬件产品中，被攻击者植入的后门或者其他的恶意模块，导致大范围传播。无论是去年的 Solarwinds 事件，还是最近发生的 Kaseya 供应链勒索攻击事件，下游用户都未能检测出软件产品已被篡改。

类似的事情其实早已发生。2014 年爆出的 OpenSSL 心脏滴血漏洞，据当时统计，国内超过 3 万台主机受到波及。事实上，早在 2012 年的版本中该漏洞就已经存在了，但直到被曝光才引起重视。没人知道有多少数据已经被泄露，更没有人知道这期间，有多少黑客利用这个漏洞发起过网络攻击。

有趣的是，在今年 RSA 创新沙盒大赛上，专注于代码风险可视化管理平台的初创公司 Apiiro 获得了冠军，这家公司号称可以发现和阻止类似 SolarWinds 的供应链攻击。

## 多措并举，从源头遏制供应链攻击

正是由于看到了供应链攻击的隐蔽性、影响的广泛性，以及防护的紧迫性，中美等国开始下大力气整治软件供应链。

2021 年 2 月，美国总统拜登签署《确保供应链安全》的行政命令，强化关键供应链的安全管理；2021 年 5 月 12 日美国总统拜登发布行政命令，要求联邦政府必须采取行动，以快速改善软件供应链的安全性和完整性，其中包括要求向政府出售的软件必须符合基准安全标准，并引入所谓的软件物料清单。这意味着供应商必须列出产品中使用的所有第三方代码和开源代码。

就国内而言，2020 年 4 月，国家网信办等 12 个部门联合发布了《网络安全审查办法》，要求关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当进行网络安全审查。

今年 7 月，工信部、国家互联网信息办公室、公安

部联合印发《网络产品安全漏洞管理规定》，首次以产品视角来管理漏洞，通过对网络产品漏洞的收集、研判、追踪、溯源，立足于供应链全链条，对网络产品进行全周期的漏洞风险跟踪，实现对我国各行各业网络安全的有效防护。

尽管如此，相比美国等国家，我国在软件供应链安全方面的基础依旧比较薄弱。亟需从国家、行业、企业等各个层面建立软件供应链安全风险综合防护体系，整体提升软件供应链安全管理的水平。

对此奇安信代码安全实验室建议，在国家与行业监管层面：制定软件供应链安全相关的政策要求、标准规范和实施指南，建立长效工作机制；建立国家级 / 行业级软件供应链安全风险分析平台，及时发现和处置安全风险；同时，在产品测评、系统测评等工作中，纳入软件供应链安全的内容。

在软件最终用户层面：建议明确本单位内部软件供应链安全管理的目标、工作流程、检查内容、责任部门；在采购商业货架软件时，应充分评估供应商的安全能力；在自行开发软件系统或委托第三方定制开发时，应遵循软件安全开发生命周期管理流程，针对软件源代码进行安全缺陷检测和修复，同时要重点管控开源软件的使用。

在软件厂商层面：建议提高安全责任意识，严控产品的安全质量；建立清晰的软件供应链安全策略；严格管控上游，尤其重点管控开源软件的使用，建立开源软件资产台账；严控自主开发的代码质量；建立完善的产品漏洞响应机制。

与此同时，奇安信还针对用户和开发者两大供应链安全场景，发布了软件供应链安全解决方案，为客户提供代码安全能力、软件空间测绘能力、感知与自主测试能力、自动化流程管理能力。（文 / 魏开元）

3

## 勒索攻击

# 攻击模式不断创新，2021 可能成为勒索史上最糟年份

今年上半年，勒索软件攻击数量同比增长了 151%；平均赎金要求上涨了 518%。随着勒索运营者关注供应链攻击，盯上基础设施与金融服务业，2021 年有可能成为勒索攻击史上最糟糕的一年。

国土安全部部长亚历杭德罗 · 马约卡斯近期表示，网络安全的新闻头条已经从数据泄露和间谍活动转变为破坏医院、学校、食品供应商和输油管道的勒索软件攻击。

勒索软件攻击者的商业模式变得更有组织性和效率，而安全防护却难以跟上，令机构陷入困境。安全公司 SonicWall 首席执行官比尔康纳说：“勒索软件攻击的狂轰滥炸迫使机构持续处于被动的防御状态。”

## 2021 有望成勒索攻击史上最糟糕一年

7 月，SonicWall 报告称，相比 2020 年上半年，今年上半年勒索软件攻击数量增长了 151%。5 月份发生了 6230 万次攻击，是自 SonicWall 于 2013 年开始跟踪以来最多的勒索软件攻击，而 4 月份则创下了 4830 万次的历史新高。SonicWall 在今年第二季度记录了近 1.89

亿起勒索软件攻击，为其史上最糟情况。

总体上看，安全厂商在 2021 年上半年记录的勒索软件攻击尝试达3.047亿之多，而2020年全年也就3.046亿。

SonicWall 称，该攻击量使 2021 年有望成为勒索软件史上最糟糕的一年。

今年迄今为止，最值得关注的攻击包括 5 月份科洛尼尔输油管道遭攻击，导致美国东海岸出现暂时性的天然气短缺；此后不久，肉类加工巨头 JBS Foods 遭遇攻击，6 月发生针对 Kaseya 的勒索攻击。

## 勒索攻击的成本越来越高

肉类加工巨头 JBS 表示，它向与俄罗斯有关联的集团 REvil 支付了 1100 万美元的赎金，而 1100 万美元的支付额超过了 2020 年支付的创纪录的 100 万美元赎金。

Palo Alto Networks 旗下 Unit 42 安全团队新发布的报告显示，2021 年上半年勒索软件平均支出上涨了 82%，高达破纪录的 57 万美元。这一数字远超去年 31.2 万美元的平均支出，而去年平均支出比前年增长了 171%。2021 年以来，最大支付金额是肉类加工企业 JBS 遭攻击后披露的 1100 万美元。

2021 年上半年 Unit 42 安全团队服务过的事件中，单个受害者遭遇的最高勒索赎金是 5000 万美元，比去年的 3000 万美元高出 66.7%。在 Unit 42 安全团队 2021 年上半年参与的数十起安全事件中，平均赎金要求为 530 万美元。这比 2020 年的平均 847,000 美元上涨了 518%。

## 攻击模式与往年大不相同

在近期的黑帽大会上，埃森哲公司战略网络威胁情报主管巴顿 · 亚当斯表示：“攻击模式已经改变。2021 年看起来与往年大不相同。” 埃森哲在研究报告中，强调了勒索软件的新趋势——网络犯罪分子使用更激进的策略迫使受害者付款。

首先，勒索软件攻击者日益将关键基础设施作为攻击的目标，科洛尼尔输油管道勒索攻击就是个“典型的案例”。

安全公司梭子鱼（Barracuda）也发现：尽管政府机构、医疗和教育产业仍是勒索软件攻击的重灾区，金融服务业、旅游业和基础设施等之前遭受勒索软件攻击相对较少的行业，渐渐吸引了更多攻击火力。梭子鱼在过去 12 个月分析的所有勒索软件攻击中，针对这些行业的攻击占据 57%，而 2020 年这一数字仅为 18%。

此外，网络攻击者越来越多攻击虚拟专用网络（VPN）等网关服务。 在科洛尼尔输油管道攻击事件中，勒索软件团伙使用泄漏的 VPN 凭据，侵入公司的 IT 系统，而不是通过可关闭物理燃料管道的运营技术 (OT) 控制系统。

“如果他们使用泄露的 VPN 凭据入侵企业网络，将来没有什么可以阻止同样的事情直接发生在 OT 网络，而且更难检测到。”

研究人员发现，勒索软件运营者越来越关注供应链攻击，比如针对可信软件供应商和 IT 服务提供商的攻击，其目的是通过一次攻击就拿下多家企业。近几个月来，最引人注目的案例就是 7 月份 Kaseya 遭受的攻击。这场攻击中，勒索软件成功渗透进该公司多家下游托管服务提供商客户的系统。

目前，攻击者围绕勒索软件建立起了完整的生态系统：他们在暗网论坛上分享和改进策略，买卖恶意软件、被盗凭据和其他工具来帮助其入侵网络。 除了在暗网上买卖恶意软件之外，网络犯罪分子还滥用和盗用商业技术。当威胁行为者使用 Cobalt Strike 等合法的渗透测试工具时，就很难区分敌友，使得检测变得困难。

## 从双重勒索到四重勒索

研究结果表明，网络攻击者采用“四重勒索”的情况日益普遍。研究人员称，勒索软件攻击者使用多达四种技术来迫使受害者支付赎金——加密、数据窃据、拒绝服务（DoS）和骚扰。

其中，加密导致受害者不得不支付赎金，以恢复混乱的数据和受损的系统；数据盗窃则意味着只要没拿到赎金，攻击者就公布受害者的敏感信息。拒绝服务（DoS）代表勒索软件攻击团伙发起 DoS 攻击将受害者的公开网站挤下线。骚扰则是攻击者联系受害者的客户、商业合作伙伴、雇员和媒体，告诉他们这家企业被黑了。

研究人员表示：“尽管一家企业沦为全部四种技术受害者的情况很少见，但 2021 年发现，在受害者遭遇加密和数据盗窃后拒不支付赎金时，勒索软件攻击团伙施加其他攻击方法的现象越来越多了。”

## 防护从基本的网络使用习惯开始

与所有安全策略一样，防止勒索软件从安全健康的网络使用习惯开始。

Arctic Wolf 联盟副总裁 Odin Olson 认为，“这些攻击事件的根源与安全行业几十年一直存在的问题相同：是否具备基本的网络安全习惯，并保持更新。”

“无论是科洛尼尔输油管道，还是其他几十个安全事件，这些机构都没有安全健康的网络使用习惯。它们并不是因为没有先进的安全工具。 据发现 SolarWinds 漏洞的威胁研究团队 Mandiant 称，黑客通过使用已泄露的 VPN 密码侵入了科洛尼尔输油管道的网络。该账户不需要多重身份进行验证。

应对勒索软件攻击的关键在于是否能够快速检测和响应。遭受入侵不等于发生损害——这就是攻击者驻留时间、入侵与损害之间带来的差异。

与其他形式的恶意软件相比，勒索软件攻击者的驻留时间（攻击者在检测到之前在组织环境中驻留的天数）通常较短。检测入侵所用的时间越长，攻击者窃取数据的时间就越长——甚至跳入客户和合作伙伴的网络。（文 / 李建平）

4

## 隐私安全

# 隐私安全问题日益尖锐 保护治理需多方合力

今年的央视 3.15 晚会首次聚焦隐私安全，接连曝光人脸识别数据泄露、简历任意下载和清理软件暗藏诈骗信息等问题，将大数据时代下的隐私安全问题推向台前。在 2021 年上半年中，诸多数据泄露事件及相关新闻的曝光让社会各界对此高度关注，成为网络安全领域的热词之一。

## APP 用户隐私泄露事件频发 过度索取权限现象泛滥

2021 年初，报道称国外安全研究团队 Cyble 发现有多个帖子正在出售中国公民相关的个人数据。经分析，这些数据很可能来自微博、QQ 等多个社交媒体，涉及身份证、性别、姓名、手机号、地址等个人隐私信息，而被发现的帖子中涉及到的数据总数超过 2 亿。

其后不久，有网友在知名开发者社区 V2EX 发帖称，自己测试发现，QQ 会试图读取电脑里所有谷歌系浏览器的历史记录并提取链接。这一消息引发国内舆论热议，APP 过度获取用户权限问题开始走向大众视野。

在 3.15 晚会上，APP 权限越界的危险再次被提及：许多针对老年人开发的手机清理 APP 背地里不断获取手机信息，并推送带有欺骗套路的内容。

在 2021 年上半年，国内外最为轰动的隐私泄露事件还有美国知名社交媒体 Facebook 超 5 亿用户的个人数据遭到泄露。据俄媒报道，被曝光的 5.33 亿用户个人数据涉及 106 个国家和地区，信息包括 ID、用户全名、位置、生日、个人简介及电子邮件地址，甚至其中不乏名人信息。

## 黑产售卖个人信息猖獗 数字化时代风险加倍

从 3 · 15 晚会曝光的其他两起隐私安全事件来看，均与个人信息售卖有关：商家安装摄像头捕捉记录顾客人脸信息，多门店共享并进行综合报价；智联招聘、猎聘等平台简历给钱就可随意下载，大量简历流入黑市……这些也只是个人信息售卖黑产的冰山一角。

在我们拥抱万物互联时代的同时，新技术、新应用和新场景也在不断蚕食用户隐私。4 月 6 日，一位黑客曝光了特斯拉车内摄像头的高清画面，清晰可见车内情况，这一问题再次引发舆论关注并登上热搜。原本作用是监控驾驶员疲劳状态、及时提醒的车内摄像头，一旦被攻击，窃取影像数据，其危害可想而知。

8月初，新闻曝光以色列某软件监控公司对外售卖“飞马”（Pegasus）手机间谍软件，该软件可安装并窃取受害目标设备中的所有数据；其后不久，苹果也陷入了隐私信任危机。根据苹果官网消息，苹果计划在 iOS 15、iPadOS 15、watchOS 8 和 macOS Monterey 的更新中通过两项举措加强对儿童的保护。

该计划中的第一项是推出名为 neuralMatch 的工具，用来扫描用户上传到 iCloud 之前的图片。第二项是苹果将在 Messages 应用程序中添加新工具，能够自动识别色情图片，以在接收或发送色情照片时警告儿童及其父母。这一举措加剧了人们对隐私安全的担忧，国外安全工程师认为苹果这一技术路线终将导致对用户的大规模监控。

## 隐私安全问题日益尖锐 保护治理需多方合力

在简单盘点过上半年较为重要的隐私安全事件后，我们需要做的还有总结与思考：谁在获取我们的隐私信息？隐私泄露的后果有多严重？隐私安全保护该从何下手？

从数据来看，《2021 年数据泄露调查报告》称，网络钓鱼、勒索软件和 Web 应用攻击成为 2021 年数据泄露的主要原因。网络钓鱼的人为违规行为较去年增加了 11%，占比达 36%；Web 应用程序的攻击占比则为 39%。除了钓鱼、勒索软件、病毒木马等网络攻击手段，APP过度申请权限、恶意诱导链接与广告弹窗、大数据“杀熟”等常见的移动端安全隐患，在 PC 端同样存在。

关于隐私泄露的后果，奇安信安全工程师曾对此作出了形象的解释：如果有人在没有经过用户同意的情况下，私自查看、篡改、传播甚至摧毁你电脑中的数据和文件，比如，有人在你不知道的情况下查看了你的搜索记录，查看了你的网站浏览记录，他就能获取你可能关注的东西，如果这些事情是敏感内容，就可能对你造成困扰；如果是你的竞争对手知道了这些内容，就可能让你暴露目标和底线，失去非常重要的先机；广告商也能针对你泄露出去的隐私，进行精准的营销和推送。

这就是大数据时代下，隐私安全的重要性和宝贵价值。实际上，隐私安全这个议题热度近年来始终经久不衰，尽管在保护隐私层面上我国起步较晚，但随着数据价值的重要性凸显，保护隐私安全，我们已经在路上。

从国家立法情况来看，相关部门一直在加强法律法规层面对数据安全和隐私保护的力度，《网络安全法》《数据安全法》的相继出台，都为数据安全和隐私保护提供了相应的保障。8 月 17 日，个人信息保护法草案也已经提请十三届全国人大常委会第三十次会议三审。据悉，三次审议稿进一步完善个人信息处理规则，特别是对应用程序过度收集个人信息、大数据“杀熟”以及非法买卖、泄露个人信息等作出有针对性规范。

从企业厂商角度，对于拥有用户数据的企业来说，保护用户信息、防止用户信息发生泄露是基础，还需要为收集个人信息划下红线，避免过度获取用户权限，为隐私泄露增加风险。对此，华为、小米、魅族、OPPO 等国内手机大厂都重点升级了隐私保护功能。除此之外，隐私保护还需要借助专业的技术力量，安全厂商同样责无旁贷。

针对现阶段的隐私安全情况，日前，国内安全厂商奇安信上市了第三代安全软件——奇安信安全防护软件冬奥版全新版本，在病毒木马查杀的基础上，重点强化了隐私保护能力，当用户对办公、学习等重要文件，以及上网历史记录、聊天软件记录、电子邮件等个人重要信息设置成为特别保护模式时，奇安信安全防护将禁止其他应用软件访问，进而提高保护强度，防止隐私泄露。

最重要的是，从用户角度而言，在国家有措施、防护有工具的情况下，面对严峻的隐私安全形势，自身的防护意识同样必不可少。个人信息保护和隐私安全是“长跑”，需要国家监管、技术手段、安全意识等多维度共同作用，才能保护我们的隐私不变透明。（文 / 王梦琪）

5

## 未成年人网络安全

# 守护网络世界“少年的你”需要共同努力

随着信息技术的不断发展与普及，互联网对未成年人的日常生活和社会化的影响持续加强，网络成为形成塑造青少年思维观念、行为方式和价值取向的重要场域，同时未成年人也是参与网络的重要群体。

《2020年全国未成年人互联网使用情况研究报告》显示，2020年，我国未成年网民达到1.83亿人，互联网普及率为94.9%，高于全国互联网普及率（70.4%）；中国互联网络信息中心(CNNIC)发布的第47次《中国互联网络发展状况统计报告》显示，截至2020年12月，中国网民规模达9.89亿，19岁及以下网民群体占比16.6%。两个数据都表明，青少年已经成为我国网民的重要组成部分。

近年来，党和政府对未成年人网络保护高度重视，针对网络时代加强互联网和虚拟社会的监管和治理，出台了一系列政策法规。自2021年6月1日起，新修订的《中华人民共和国未成年人保护法》（简称《未成年人保护法》）已正式实施，其中新增的“网络保护”专章，首次在法律中规定未成年人网络保护，具有里程碑意义。

## 法律条文明确未成年网络安全保护多主体责任

近年来，以游戏为代表的行业不断探索实名注册、身份认证等手段，识别未成年人身份以采取限制措施，但只单纯从技术角度进行限制，并不能有效解决问题。为此，基于《未成年人保护法》“多方主体的共同责任”的思路，“网络保护”专章对国家、社会、学校、家庭四个相关责任主体分别提出了相关要求。

首先，监护人应当“以身作则”地引导和监督未成年人。第71条规定，未成年人的父母或者其他监护人应当提高网络素养，规范自身使用网络的行为，加强对未成年人使用网络行为的引导和监督。未成年人的父母或者其他监护人应当通过在智能终端产品上安装未成年人网络保护软件、选择适合未成年人的服务模式和管理功能等方式，避免未成年人接触危害或者可能影响其身心健康的网络信息，合理安排未成年人使用网络的时间，有效预防未成年人沉迷网络。

在“家庭保护”章第17条中，也对监护人的网络保护义务提出了明确规定：“监护人不得放任未成年人沉迷网络、不得放任接触危害或可能影响其身心健康的网络信息等。”这也体现了网络保护与传统保护的紧密结合。

其次，学校作为网络保护的重要场所，应合理使用网络开展教学，并重点关注沉迷网络现象。第70条规定，学校应当合理使用网络开展教学活动。未经学校允许，未成年学生不得将手机等智能终端产品带入课堂，带入学校的应当统一管理。学校发现未成年学生沉迷网络的，应当及时告知其父母或者其他监护人，共同对未成年学生进行教育和引导，帮助其恢复正常的学习生活。

同时，社会各界也应积极参与未成年人网络保护。第69条规定，学校、社区、图书馆、文化馆、青少年宫等场所为未成年人提供上网设施的，应安装未成年人网络保护软件或采取其他安全保护措施；智能终端产品的制造者、销售者，应在产品上安装保护软件，或以显著方式告知安装渠道和方法。

当然，政府的网络保护义务是不可替代的。新修订的《未成年人保护法》中，对网信及相关部门、新闻出版等部门均提出了明确要求，鼓励有利于未成年人健康成长的网络内容的创作与传播，惩处危害活动，开展预防宣传教育、监督企业履行预防义务等。

## 疏堵结合 防治网络沉迷

沉迷网络一直是社会各界关注的热点，在《未成年人保护法》中，以“疏堵结合”的方式，就防治沉迷网络问题，对政府、学校、家庭、社会四个责任主体分别提出了规定。

首先，第68条指出，政府有关部门应当定期开展预防宣传教育，监督企业履行预防义务，指导家庭、学校、社会组织互相配合，以科学、合理的方式预防和干预沉迷网络；其次，第70条指出，学校发现未成年学生沉迷网络的，应当告知其父母或者其他监护人，共同进行教育和引导，帮助其恢复正常的学习生活；再次，第71条规定监护人应当合理安排未成年人使用网络的时间，有效预防沉迷网络；最后，第74条规定，“网络游戏、网络直播、网络音视频、网络社交”等网络服务提供者应当针对未成年人使用其服务设置“时间管理、权限管理、消费管理”等功能。

中央网信办在今年7月还启动了“清朗·暑期未成年人网络环境整治”专项行动，聚焦解决包括直播、短视频平台涉未成年人问题，防沉迷系统和“青少年模式”效能发挥不足问题等在内的7类网上危害未成年人身心健康的突出问题，要求对于侵害未成年人合法权益的问题保持“零容忍”态度。

## 未成年个人信息保护要求列入多项法案

未成年的个人隐私、个人信息保护一直是相对薄弱的环节。但庞大的未成年网民直接关联的海量个人信息，其安全问题绝不容忽视。

在新修订的《未成年人保护法》中，首次明确将14周岁作为未成年人个人信息处理的同意年龄，并赋予未成年人及其监护人更正、删除权，信息处理者遵循合法、正当和必要的原则，针对未成年人私密信息，网络服务提供者应当及时提示并采取必要的保护措施。这些规定充分体现了本次修法对于未成年人使用网络权利及保障其个人信息安全的同等重视。

8月20日，十三届全国人大常委会第三十次会议表决通过了《中华人民共和国个人信息保护法》，将不满十四周岁未成年人的个人信息作为敏感个人信息，并要求个人信息处理者对此制定专门的个人信息处理规则。该法案将于2021年11月1日起施行。

## 综合治理应对网络欺凌

据中国预防青少年犯罪研究会调查显示，有50%的中学生在网上聊天、游戏过程中遭受过不同程度的“网络欺凌”，有23%左右的中学生在个人主页或博客、音视频网站的运用过程中有过此类遭遇。相对于传统的线下侵害，网络侵害的影响范围较广、持续性更强，对未成年人造成的伤害更大。对网络欺凌坚决说不，需要群策群力、综合治理。近年来，自国家到教育部门，从修订文件到出台法律，对网络欺凌进行了全面治理。

新修订的未成年人保护法针对未成年人遭受网络欺凌的现实情况，在第77条中进行了明确规定：遭受网络欺凌的未成年人及其监护人有权通知网络服务提供者采取删除、屏蔽、断开链接等措施；网络服务提供者接到通知后，应当及时采取必要的措施制止网络欺凌行为，防止信息扩散；网络产品和服务提供者应当为未成年人提供便捷、合理、有效的投诉和举报渠道。

将于9月1日起实施的教育部发布的《未成年人学校保护规定》中明确了应当制止学生“通过网络或者其他信息传播方式捏造事实诽谤他人、散布谣言或者错误信息诋毁他人、恶意传播他人隐私”，强调对欺凌行为“零容忍”，规定学生欺凌教育制度和调查评估制度。

维护未成年人的网络权益，是未成年人网络保护的初级层次，让未成年人全面掌握安全、合理、科学的互联网技能，提升未成年人的网络素养，是未成年人网络保护的更高层次。让青少年拥有健康的网络环境，需要政府、平台、社会、家长等多方协力、各司其职，也需要有常态化的机制和制度予以保障。（文/张雪丹）安

# 网安行业投融资大爆发：2021 年上半年已超去年全年

作者 虎符智库

一系列震惊世界的网络攻击事件正在加速对网络安全初创公司的投资。

2021 年刚刚过去七个月，投资者已经向网络安全公司投入了 122 亿美元，这比 2020 年全年还要多 20 亿美元以上。

业内人士认为，今年全球网络安全领域的投资总额，将达到前所未有的 150 亿至 200 亿美元之间。

由于勒索软件攻击和国家支持的黑客都十分活跃，导致油气管道停运，医院和零售中断，供应链安全危及国家情报机构。这些威胁都利好网络安全初创公司。投资者认为，安全公司将比以往拥有更广阔的市场前景和国家使命。

行业资深专家 Dave DeWalt 表示：“网络安全发展的超级周期已经到来，网络威胁空前严峻，疫情和监管倒逼企业安全支出大幅增长，行业投融资规模也远超往年，这是头一次威胁周期、客户周期、投资周期几乎同时出现。”

Dave DeWalt 曾先后担任 McAfee 和 FireEye 首席执行官十余年，目前在多家明星安全公司担任董事，并正在运营一家刚刚募得 7.5 亿美元的网络安全专业基金。

## 20 年未见安全公司估值如此快速上升

自 2019 年开始，网络安全领域的投资增速就超过风投行业的整体增速。近期出现的激增则是由于一系列备受瞩目的网络攻击的发生，包括针对美国油气运输管道 Colonial Pipeline、软件制造商 Kaseya、肉制品加工商 JBS 等公司的攻击。

美国总统拜登和俄罗斯总统普京也在会谈中深入探讨了有关网络攻击的问题。

日益增长的网络攻击引发了公司和政府的担忧，这会促进网络安全产品的销售。Gartner 预测，今年全球信息安全和相关服务支出将达到 1500 亿美元，相比去年增长 12%。

Dave DeWalt 说，据他担任董事的多家安全公司了解，目前接触的财富 500 强企业，全部都在为正在发生的事件而大幅增加网络安全支出。

线上借贷平台 LendingTree 公司的信息安全经理 John Turner 表示，原来安全团队在艰苦的条件下艰难地保护每一分钱。现在，形势逆转了。公司高管开始主动询问：“我们是否受到了合适的防护，安全团队还需要什么？”

所有这些都推动了网络安全公司的业务发展。根据 PitchBook 的数据，今年融资的网络安全公司的平均估值，从 2020 年的 2.218 亿美元增长到 2021 年的 5.241 亿美元。

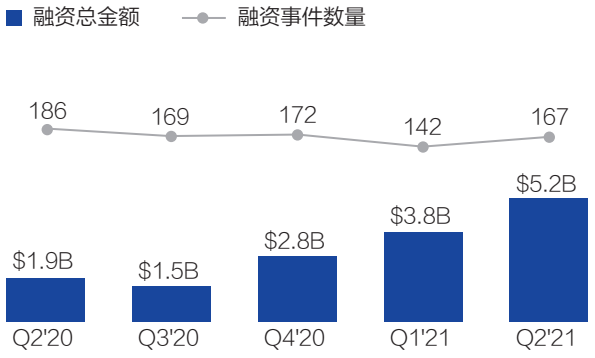
Greylock Partners 的投资人 Asheem Chandna 曾成功投资过 Palo Alto Networks 等安全公司。他表示，“作为风险投资人，二十年来都没有见过公司估值上升的如此之快”。

## 2021 年网络安全投资将达去年 2 倍

2020 年是网络安全投资创纪录的一年，全球网络安全行业投资超过了 78 亿美元。但 2021 年的网络安全投资总额有可能将达到 2020 年的 2 倍以上。

业内人士表示，几乎可以肯定的是，2021 年全球网络安全领域投资总额将至少达到 150 亿美元；如果热度毫不衰退，200 亿美元也将不在话下。

全球网络安全融资数量及金额统计




数据：CrunchBase

据投融资数据平台 CrunchBase 统计，今年上半年，网络安全行业共完成 309 笔交易，总融资高达 90 亿美元，是去年同期 44 亿美元融资金额的 2 倍以上。

单是今年第二季度，网安行业的融资数字就达到 52 亿美元，去年同期则不到 20 亿美元。

截至 2021 年 7 月底，投资者已经向网络安全公司投入了 122 亿美元，这比 2020 年全年还要多 20 亿美元以上。实际上根据统计，自 2011 年以来，对网络安全公司的投资已增长了 9 倍以上。

## 大手笔并购和 IPO 层出不穷

除了融资，安全初创公司也被大手笔收购或者筹备 IPO。

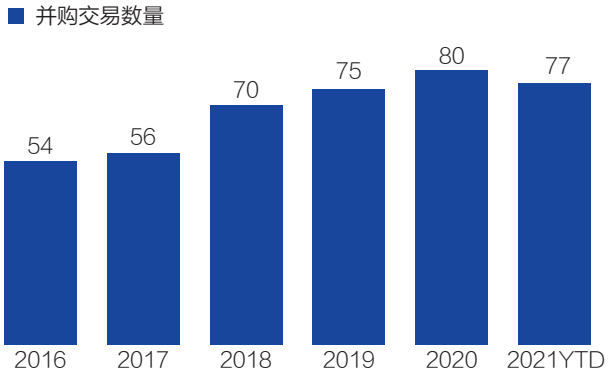
2021 年 6 月，端点安全公司 SentinelOne 成功上市，以 90 亿美元估值募资 12 亿美元，这被认为是网络安全史上规模最大的 IPO。

身份识别公司 Clear Secure、反欺诈公司 Riskified、AI 安全公司 Darktrace、安全意识培训公司 KnowBe4 等也纷纷上市，均募集了数亿美元规模的资金。

此外，还有数家募资数亿美元、专门针对网络安全行业的 SPAC 壳公司成功上市，充分展示了本行业的资本吸引力。

2021 年 4 月，私募股权巨头 Thoma Bravo 宣布以 123 亿美元的价格收购综合安全公司 Proofpoint。5 月，身份认证公司 Auth0 被 Okta 以 65 亿美元的价格收购。

全球风险投资支持的网络安全并购交易数量统计




数据：CrunchBase

根据 CrunchBase 的数据，2021 年前七个月，风险投资支持的网络安全企业并购交易数量几乎达到去年全年总数。今年已经有 77 笔交易——而去年则是创纪录的 80 笔。

## 云安全与身份安全是投资热点

2021 年 7 月，云安全初创公司 Netskope 以 75 亿美元估值融资 3 亿美元，这是今年网络安全领域内较大规模的融资。

过去几年，机构向云端转移。新冠疫情大大加速了数字化转型和云化。连接互联网的资产数量日益增长，攻击面也随之扩大。传统依赖边界防护的思路正在失效，这为更多的安全公司提供了机会：云安全和身份认证是新的行业热点。

云计算普及加速 Lacework、Aqua Security、OwnBackup、Axonius 等云安全公司的发展势头。

自疫情爆发以来，云安全公司已筹集了超过数十亿美元的资金。今年仅前七个月，投资者已向云安全、身份认证和隐私保护等细分领域的公司投资超过 122 亿美元。

根据 PitchBook 的数据，这一数字已经超过 2020 年的总投资额 104 亿美元，更是远远超过 2016 年的 48 亿美元的投资额。

网络安全投资咨询公司 Momentum Cyber 创始董事 Dino Boukouris 表示，除了云安全，身份与访问管理、风险与合规等细分领域在 2021 年上半年同样表现良好，在可预见的未来应该会保持强劲势头。

Thomvest Ventures 的合伙人 Umesh Padval 表示，今年下半年将重点关注云安全（典型代表如 Lacework、Wiz）、API 安全与持续上下文身份验证等技术方向。

API 安全在 2021 年二季度迎来了一波融资热潮：总部位于伦敦的 42Crunch、来自帕洛阿尔托的 Salt Security、位于科罗拉多的 ThreatX 以及来自加利福尼亚州桑尼维尔的 API 安全厂商 Cequence Security 等均宣布了新的融资。

随着许多机构宣布无限期延续远程工作优先政策，预计安全公司高速发展的势头将会一直保持下去。

## 中国投融资交易数量超以色列，但金额远逊

以色列国家网络局（INCD）表示，2021 年上半年，以色列网络安全公司总共融资 50 笔，筹得 34 亿美元，融资金额已占据全球总额的近四成。

从数据来看，今年有 7 家以色列企业成功跻身网安独角兽行列，全球超过三分之一的网安独角兽企业来自以色列。独角兽是指估值超过 10 亿美元的私营公司。

据《安全内参》基于公开信息梳理，2021年1-7月，国内共计发生61起网络安全投融资事件，公开披露涉及金额超59亿元，约占全球总额的10%。

2021年1-7月我国网络安全初创企业投融资事件数据

| | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 | 7月 |
|---|---|---|---|---|---|---|---|
| 融资事件数量/起 | 6 | 6 | 12 | 9 | 7 | 10 | 11 |
| 披露融资金额/亿元 | 7.8+ | 2+ | 13.6+ | 7.45+ | 3.3+ | 12+ | 13.3+ |

其中，风控厂商数美科技、主机安全厂商青藤云安全、威胁检测厂商微步在线，分别以1.35亿美元（约8.78亿元）、6亿元、5亿元位列融资金额前三，数美科技融资后的估值接近独角兽。

国家工业信息安全发展研究中心统计数据显示，2021年1-7月，国内近四成网安企业融资事件的融资额超过1亿元，近两成事件融资额超过2亿元，超亿元融资事件数量较去年同期增长约1.2倍。

统计数据还显示，投资机构对网络安全领域早期、中后期项目的关注度较为均衡，中后期项目占总融资事件近一半，所占比例略高于早期项目（部分项目未披露具体融资轮次）。

从上述数据可以看出，中国网安初创企业投融资的繁荣度已和全球接轨，规模上也有大幅增长，但总金额和网络强国相比还有较大差距，特别是在领军企业上，今年没有一家新晋独角兽。

以色列国家网络局经济与增长主任Roi Yarom表示，网络安全行业已成为以色列国家经济的增长引擎，同时也将提高以色列对于未知网络攻击的抵御能力。

## 豪赌下一个CrowdStrike

随着网络安全企业的不断发展，投资者的心态发生变化：从平均投资多家创业公司，转向为少数公司提供巨额资金——他们的目标非常明确，豪赌其中某家能成为下一个CrowdStrike。

但SineWave Ventures创始人、SentinelOne早期投资者Yanev Suissa表示，目前很多融到大量资金的解决方案，仍然属于“治标不治本”的低价值产品，只能解决某些非常具体的安全问题或特定场景。

“现在市场上仍然缺乏充足的革命性技术平台，我们只看到了一大堆「还可以」的解决方案。”

但或许正如微软公司首席信息安全官Bret Arsenault在RSAC 2021演讲时指出的那样，完美不是安全的目标，改进才是。当前影响安全提升的一大原因，是对完美主义的过分追求。

其实，安全专家早就放弃寻求银弹的希望。最近热门的零信任、SASE等创新技术不会是安全挑战的终结者，也不能取代现有边界防护手段。

在没有银弹的世界，任何的技术进步都应是我们积极把握的机会。这或许才是推动我们实现安全能力逐步提升的最现实道路。

附：2021年网络安全重大融资事件

2021年1月，云安全厂商Lacework获5.25亿美元融资，投后估值超10亿美元。

2021年3月，云安全初创公司Orca Security宣布融资2.1亿美元，投后估值12亿美元。

2021年3月，开发安全厂商Snyk宣布融资3亿美元，投后估值47亿美元。

2021年6月，威胁检测厂商Exabeam获2亿美元融资，投后估值24亿美元。

2021年6月，身份验证公司Trulioo获得了3.94亿美元投资。

2021年6月，数字资产安全厂商Ledger宣布融资3.8亿美元。

2021年6月，无密码验证厂商Transmit Security宣布A轮融资5.43亿美元，投前估值23亿美元。

2021年7月，云安全初创公司Netskope融资3亿美元。

2021年8月，云数据备份公司OwnBackup宣布融资2.4亿美元，投后估值33.5亿美元。安

# 270+ 城市、400+ 门店，居然之家快速扩张背后的组网秘诀

作者 公关部 张少波 魏开元

“截至 2020 年底，居然之家门店网络遍布全国 30 个省市自治区、272 个城市，签约门店数量达到 706 家，累计直营开店数量达到 416 家。”自 1999 年成立到现在，居然之家作为有着 22 年历史的家居行业龙头，依然奔驰在高速扩张的快车道上，历久弥新。

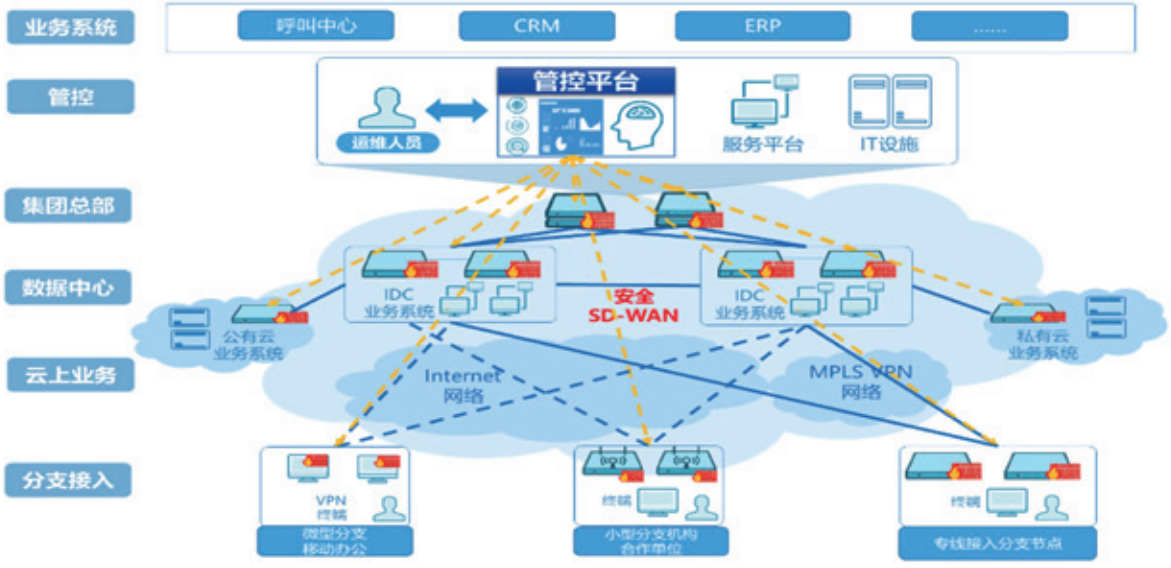
为适应家居消费能力向区域市场下沉的趋势，居然之家近年来加速布局下沉的战略，作为居然之家的掌门人、董事长兼 CEO 汪林朋，早在 2018 年就曾对外表示，“居然之家的全国连锁一直在加速，将来会成为第一个从北上广一线城市到县级城市全覆盖的企业。”

与此同时，居然之家进行了业务系统上云的规划，逐步将企业的业务系统迁移到云上。线下门店与总部的互联互通、线上与线下业务的融合，给网络基础设施建设提出了新的要求。为了满足新业务平台的组网、安全和运维需求，居然之家选择了奇安信合作，通过部署奇安信安全 SD-WAN，实现了组网、安全和运营的三同步。

## 高速扩张带来的三大挑战

“不仅我们的门店数量在快速增长，同时也在加速向三四五线城市的区域下沉，这样的连锁化扩张速度，给我们信息化网络设施建设带来空前挑战，此项工作加快推进，花多少钱都值得，一方面规范员工上网行为，另一方面防止外部恶意攻击。” 汪林朋多次强调。

更具体来说，这些挑战包括 IT 系统上云，以及安全边界从局域网络延伸到广域网络等趋势下，信息化网络所遇到的投入成本和运营成本居高不下，可用性、可靠




性和安全性难以保障等问题。

**首先网络初期建设时，传统专线模式的投资成本居高不下。**过去在门店扩张或改造时，分部与全国的各分支机构采用了多家运营商的 MPLS 专线，持续性成本高昂，开通周期长，变更复杂，且以服务形式提供，不存在投资保护。

“我们在新疆某地区新建门店时，因为当地偏远，没有任何基础网络通信设施，采用传统的组网方式，还需要找市政申请和审批，甚至还需要专门架电线杆子，少说也需要十天半个月。其成本之高、周期之长，可想而知。” 新零售集团 IT 管理部王欢分享了一个故事。

**第二是运维成本较高，难度很大。**由于分公司、门店网络环境变动较频繁，设备上线时间长，而且割接过程复杂，维护人力成本居高不下。同时由于网络、业务服务质量和安全风险不可见，不同分支机构与中心节点之间需要采用不同产品进行组网，运维难度较高，排错效率较低。

王欢表示，我们的门店和分支机构分布在全国各地，他们不一定有专业的 IT 维护人员，采用传统专线网络方式，无论是新建部署还是后期维护，配置都是很大的工程。同时后期运维管理的难度也非常之大。

**第三在可靠性和安全性方面难以保障。**传统的专线组网方式，无法满足业务高可用性、高可靠的需求，单链路故障所造成的业务瘫痪不可避免，遭遇链路故障后无法迅速进行链路切换。同时对用户访问互联网缺乏安全管控，对用户访问业务系统缺乏审计手段，对网络内外的僵尸、木马、蠕虫、病毒等威胁缺乏相对应的防护措施。

## 通过 SD-WAN 化繁为简 实现组网、安全、运营一步到位

“为了解决这些挑战，SD-WAN 技术进入了我们的视野。所谓 SD-WAN，就是“软件定义广域网”，它的 ZTP 技术、云连接技术、LLB 技术，配合集中管控平台，可以有效解决快速组网、弹性扩展、运维可视的问题。”王欢回忆道。

尽管有诸多优点，但传统 SD-WAN 也存在一些不足：其一，无法解决安全问题，攻击者能够以分支机构为跳板，绕过 SD-WAN 设备向总部进行渗透攻击，想要解决安全问题就还需接入防火墙、IPS 等多个安全设备，

必然带来成本的大幅度提升；其二，无法实现全网安全风险的统一管理和可视化分析。

“信息化建设如同盖房子，如果业务规划初期忽视了安全，短期看似乎走了捷径、上线更快，但长线来看，后期补救所付出的成本和代价，远远大于忽视安全的短期便利。”对于具有多年信息化实践经验的新零售集团IT管理部薄青松而言，对信息化和安全“三同步”的重要意义，具有深刻的体会。

显然，将组网、安全和运营一步到位无疑是适合的选择。作为边缘组网的重要设备，SD-WAN天生就是网络安全的“兵家必争之地”。凭借一站式组网和实战化的网络安全能力，奇安信安全SD-WAN方案自然而然成为了居然之家的首选。

新零售集团IT管理部朱思霖表示，奇安信安全SD-WAN方案采用了更适合多分支型连锁企业的“all in one”，避免了在网络边界处同时串接大量网络设备。尤其是网络与安全部署同时进行，杜绝有网必有毒、流量无名氏等安全风险出现。同时，奇安信SD-WAN方案的多链路均衡使用，互相存在替代可能，提升了全网健壮度，增强投资保护。

由于奇安信安全SD-WAN解决方案正好契合居然之家的需求，通过规划、建设和运营的“三同步”方案，为该连锁商企客户量身打造了安全组网一体化解决方案，支持“总部－数据中心”“总部－分支”“分支－云”“数据中心－云”等多种复杂的网络安全互联，并在非常短的时间内进行了全网升级部署，实现了对300多家门店的安全网关统一上线、监测和运维。

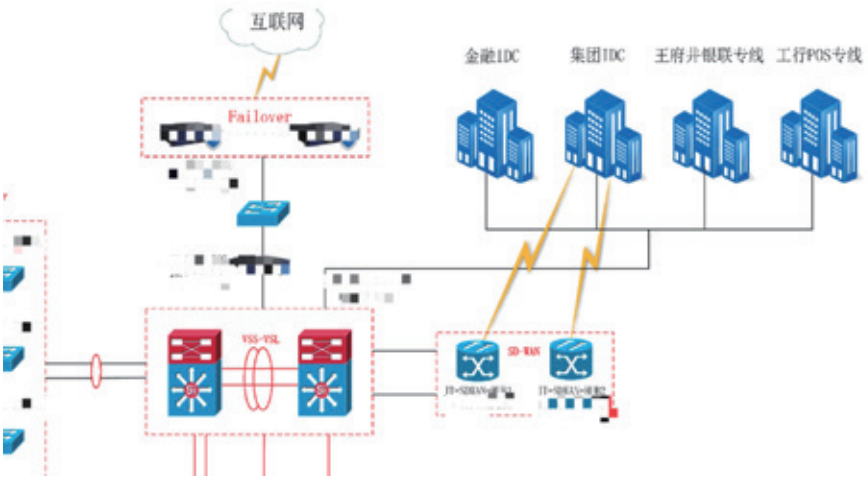
## 降本提效、安全可靠 奇安信SD-WAN优势显著

据介绍，居然之家安全SD-WAN混合云解决方案兼具了SD-WAN的组网优势，以及奇安信赋予的安全防护，最终带来的价值体现在以下几方面。

**首先是投资成本上的大幅度降低。**

“对于任何企业而言，成本降低都是极具诱惑的。传统点对点的专网方式，单个门店而言，同是2Mb带宽，同城每月大约1500元，跨城每月4000元。全国数百家门店累积起来，每月都是近百万的花销。通过奇安信安全SD-WAN，这笔费用可以省下来。”薄青松说道。

据介绍，一方面，奇安信安全SD-WAN为居然之家在Internet网络打造了一个媲美专线网络的安全可靠私密空间，替换客户原本开通的大部分专线，为门店提供访问业务系统的安全稳定通道。客户仅保留少量专线作为部分重要业务系统备份。另一方面，安全SD-WAN支持防火墙、入侵防御、反病毒、上网行为管理等安全功能，无需在边界重复部署安全设备。通过以上两方面，显著降低客户的投资成本。




**其次是运维管理成本上的极大降低，以及维护效率的指数级提升。**

“在过去，网络开通之后，初始配置是一个庞大的工程。受制于不同门店的技术水平，如果不能如期配置完毕，各门店的收银、进销存、财务、库存、内网OA等业务终端无法与总部互联，可直接导致分店不能如期营业。对于零售行业而言，

晚一天营业都是不能容忍的事故。”王欢说道。

安全 SD-WAN 的零配置上线、自动 VPN 组网、自动化部署等，可以极大缩短节点上线时间并节省运维人力资源，做到分支门店免 IT，无需为门店配备专业的运维人员，显著降低客户的 OPEX，并让分店人员专注于业务之上。

在分店运行过程中，经常会根据业务需求，进行更改配置。以前这些工作量非常之大，需要挨个门店进行逐一解决。通过安全 SD-WAN 的管控平台，可实现可视化集中管理、批量化变更、下发配置，批量化维护系统、备份系统，可视化故障排查工具。运维人员可轻松通过管控平台，实现对全网安全网关的运维，大大提高运维人员的工作效率，解决了客户原本组网设备零散、品牌杂且无法统一运维、排障难的问题。

“以前要耗费一整天的烦琐配置工作，现在可以在家里用 iPad 就能轻松解决，用‘享受’来形容也不为过。”朱思霖感叹道。

**最后是可靠性和安全性方面的强大保障。**

家居零售属于资金密集行业，任何业务中断、网络故障都会造成极大影响。在业务系统安全可靠上云方面，安全 SD-WAN 通过可适配主流云服务提供商的虚拟化安全网关，为客户的云上业务系统提供了与客户门店、集团大厦、私有云之间安全互通的网络。并通过全自动组网、智能路径优选、云端双设备冗余提高上云的网络可靠性。

而在边界安全方面，安全 SD-WAN 通过安全网关自带的安全能力，为客户的边界提供基于应用层的业务策略控制、入侵防护、病毒防护、URL 过滤、有线 / 无线接入认证、基于用户的策略控制、威胁情报联动等安全功能，使得居然之家在分支机构的网络边界可以只部署一台设备，避免一系列安全设备串接的现象，减少边界的故障点，同时极大提高业务的转发效率，又保障业务的安全。

“在和奇安信合作的过程中，团队的配合度和支持度，给我们留下了深刻的印象。”朱思霖表示，“我们是奇安信安全 SD-WAN 的第一批客户，奇安信团队始终非常专业和敬业，每次版本更新，都会第一时间主动给我们完整的配置手册。在项目实施中，奇安信还会和我们一起结合实际场景，挖掘需求，推动功能更新迭代，更加完美地支撑居然之家的业务高速发展。

## 未来：部署态势感知平台 加速安全与信息化融合

居然之家安全 SD-WAN 项目的成功实施，充分体现了信息化和安全同步规划、同步建设、同步运营所带来的巨大价值。在“2019（暨第二届）中国 SD-WAN 峰会”上，该项目在“2019 SD-WAN Awards 年度评选”中，斩获“优秀应用奖”和“年度新锐企业奖”双料大奖。

展望未来，薄青松表示，居然之家将进一步贯彻“三同步”的原则，将安全和底层基础能力，以及业务场景需求紧密结合到一起，形成不可分割的整体。更具体来说，下一步居然之家计划部署态势感知与安全运营平台（NGSOC），成为整个业务系统的安全监控平台，通过安全大屏构建出指挥中心，紧密连接九大场景，打通底层数据，并融合奇安信的威胁情报能力，实现从点到线，从线到面的策略统一化，最终为居然之家构建出面向运营的实战化态势感知平台。


“安全的最大价值，恰恰是不容易看到价值。假如安全价值被显而易见看到了，说明安全的投入还不够。”薄青松谈到，“安全不可能到达终点，无法从 0 到 100，只有不断提升攻击者的攻击门槛和攻击成本，才能获得相对的安全，为业务提供可靠的保障。” 安

# 我是程序媛，我想让我的名号被所有人知道

## ——走近锡安平台研发部王倩楠

作者 公关部 孙丽芳

一头利落的短发，T 恤仔裤球鞋，这是王倩楠最喜欢的装束。打开电脑，敲击代码，这是王倩楠最喜欢的日常。

长期以来，程序员领域一直都是男性的天下，女程序员则是“珍稀物种”。网络上，她们被亲切地称作“程序媛”。

是的，任职奇安信锡安平台研发部的王倩楠，就是一名“程序媛”。

“程序媛虽然少，但生活上跟普通女生没什么不一样，工作上跟普通程序猿也没啥大差别。”对于这个话题，王倩楠云淡风轻。因为很早就对编程充满兴趣，当一名程序媛，对王倩楠来说，是再自然不过的事。

2019 年 7 月，刚从西南石油大学软件工程专业毕业的王倩楠，就入职奇安信。虽然在校时学习成绩优异，但王倩楠很清楚，书本知识和实际研发之间还有很大差距，非常盼望自己能在这里真正历练成一名优秀的程序媛。

### 临时入列的校招生

在以“强研发”著称的奇安信，王倩楠绝佳的历练机会很快到来，它就是新一代天擎项目。

“天擎”之名，取意于擎天之柱，比喻能担负重任的人。天擎对于奇安信，对于整个终端安全市场，正是这样的“顶梁柱”产品。它是奇安信自主研发的、以安全防御为核心、以运维管控为重点、以可视化管理为支撑、以可靠服务为保障的全方位终端安全解决方案。作为数据和业务的最终载体，也是网络安全的最后一道防线，终端安全历来是网络安全的焦点之一。

而尽管在市场上，天擎连续多年位居行业第一，但奇安信从未停止技术创新的脚步。2019 年下半年，奇安信组建了由天擎产品线、应用技术开发平台、锡安核心云平台、安全能力中心等部门 150 多人组成的新天擎 V10 研发项目组，依托川陀技术平台，对天擎的底层架构方面进行重新设计、实现和优化，以提供更好的安全性、可靠性和可扩展性。

“公司在来广营组织进行新天擎的封闭开发，我刚入职，当时是在做和新天擎完全没有关联的另外一个项目的事。但因为我们锡安平台数据部有多一半的人都进入新天擎项目组了，为了方便工作开展，我也就一起过去了。”

换句话，刚开始，对于新天擎来说，新人王倩楠的角色只是“路人甲”，连“打酱油的”都算不上。

不过，没过多久，事情有了转机。

在新天擎项目中，锡安平台负责的有一项工作是重建日志线。客户端会产生很多类型的日志，比如，进程信息、防病毒信息、防火墙信息、IP 信息，等等。这些信息汇总到一起，组建起来，可以分析出一个终端的行为。一个终端是不是受到了威胁，或在一个预期的时间段内将受到威胁。这样，也就能相应地下发处置策略，大幅降低安全风险。

重建的第一步是调研组件。

“这条日志线由很多组件构成，在日志线形成之初我们先要调研各个组件的可行性。内容包括看某个组件是否适合我们的场景，可以怎么用它，怎么把它发挥到最大价值。比如说 Apache 的开源项目，能不能在改变里面的部分源码后，用到我们的场景中，并且带来很好的价值，如让速度变得更快。这里很关键的部分就是要能快速读懂源码，并能在此基础上，进行改造，为我们所用。当时调研的工作量很大，而我也拥有当前调研工作的技术栈，所以我就主动向我的Leader鹏哥提出申请，希望能参与进来。”

源码是所有框架的根基，比较复杂深邃，对资深的程序员来说，也不是好啃的“骨头”。王倩楠的主动请缨，让正在发愁人手的日志线项目负责人舒鹏感到欣喜。

“我看源码的速度很快，比如说定位问题。当我们把开源项目拿过来用之后，肯定会出现各种各样的问题，我定位问题会很快。我比较能理解它整体架构的思路，有了问题该往哪方面去找，往哪方面去改，这个我比较擅长。这可能得益于我大四实习的时候，每个周末我都泡在 GitHub（世界上最大的源码托管平台）上看源码。我对开源社区有一股热血的劲儿。”

“确实很快，这跟她的代码功底好有关系。” 既是领导也是导师，舒鹏对王倩楠的技术特点很了解。

“我交给她的第一件事情就是让她调研一个EasyScheduler（现在更名为 DolphinScheduler），并且在公司环境部署一套。这是一套开源的大数据任务调度系统，有不少分布式组件，有相当的复杂度。她用了大概2周左右的时间，就了解了所有的组件并部署完成，并且还对这个产品做了少量改进，贡献给了开源社区。”

## 每秒处理日志 5 万条

就这样，新人王倩楠正式成为新天擎项目组的一员，全面参与到新天擎日志线开发工作中。

“每台终端的每次点击，都会产生原始日志，我们要把日志分配好，哪些有用，哪些没用，建好索引，给相关的安全人员去搜索，让他们能从中得出一些有用的信息。日志非常难的一点是，量特别巨大，有用的信息混杂其中，我们要做的就是披沙拣金。”

事实上，日志服务功能在哪家公司都特别重要。但有的公司虽然日志很重要，但可能没那么紧急，止步于监控或者对外展示。

“而我们是最终要得出结论，下发策略，而且还要非常及时，从客户端到云端要控制在秒级，要做到实时。”王倩楠非常清楚手头这项工作的意义和关键点。

以战领训，舒鹏也把这次项目工作，作为带新人的好契机。

“天擎的日志线确实非常重要，倩楠加入到这个项目中，是有几方面的原因：一是在让倩楠做新天擎项目之前，我对她的能力有了比较清楚的认识，她有快速学习和接受新事物的能力；二是项目时间紧任务重，人力不够，只能让新人也多承担一些，多点复杂项目的历练。事实证明，参与了新天擎项目的新同学都成长得非常好；第三，倩楠不是从头开始构建新天擎日志线，而是在已有的模块基础上做一些功能改进，然后我会做设计和代码评审。这种循序渐进的方法有助于她快速了解全部逻辑，又不至于难得无法动手。另外，在评审的过程中，通过方案间的比较，她很快学会了取舍和思辨能力。”

“总共用时近 2 个月吧，主要就是鹏哥带着我做。当时快发测试版的时候，我们天天加班到晚上 11、12 点。累是肯定的，但非常充实。”

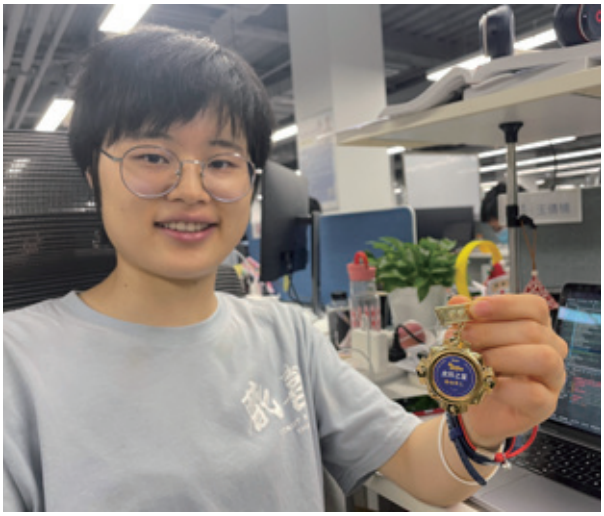
经过近 2 个月废寝忘食的集中开发，舒鹏带领王倩楠顺利完成了新天擎日志线开发工作，实现了 10 万终端量从上报原始日志到最终建好全文索引，每秒处理日志可以达到 5 万条左右，延迟在秒级，各业务的多项性能指标均超出了预期。

而经过这次历练，原本就具备代码规范、单元测试意识好等扎实基础素质的王倩楠，个人技术有了很大提升。 除此之外，王倩楠更是对于协同优先、客户优先等公司价值观有了自己的实践和体会，真正完成了从在校生到职场人的转变。

“协同优先是贯穿新天擎开发始终的。这是一项非常复杂的工作，涉及到公司很多部门，仅我负责的这一块，就需要对接很多人。比如，日志系统跟川陀 DA 基础平台有比较深的交互，需要掌握网络相关的知识，才能正

确使用 grpc 流的各种姿势，期间曾经出现一个底层基础的 Bug ，我和 DA 相关开发人员一起排查，最终把它找了出来。客户优先方面，日常工作中，我除了日常编码任务，大部分都是倾听使用我们系统客户的使用体验，做到开发迭代闭环。”

2020 年，在天擎产品线和应用技术开发平台、锡安核心云平台、安全能力中心等部门的高效协同下，基于“川陀终端安全管理技术平台”的一体化终端安全管理系统——新天擎 V10 全新构建完成，实现了很好的扩展性，单中心可支撑百万级终端的管理。



因为在新天擎日志线项目中的突出表现，入职仅一年多的校招生王倩楠被评为当年的虎符之星“最佳员工”。

## 逛 GitHub 比逛街有意思

“旗开得胜”的王倩楠没有满足于现状。

“刚工作前几年就是拼加速度，大家的起点可能差不多，之后能跑多远就看加速度。对比很多同届生来说，我可能已经算成长得比较快了，我也很满意现在的工作内容，但互联网是日新月异的行业，只有不断学习才能持续进步。”

学习是王倩楠一直身体力行的坚持。如果说程序媛和普通女生真有什么区别，那应该就是在这里了。

例如，普通女生都很喜欢逛街，而程序猿喜欢逛 GitTHub。

“逛 GITHUP 比逛街有意思多了，里面也是琳琅满目，有各个大神写出的各种组件、优秀的项目。公司内部的学习氛围也很浓。每周五下午 5 点到 7 点，我们部门会组织集体学习，比如，学习《机器学习实战：基于 Scikit-Learn、Keras 和 TensorFlow》。而每周末，只要没有特别的事，我都是 9 点多就来公司，上午学习，下午去公司健身房锻炼。生活开销之外的钱，我基本也是花在去“极客时间”上买课程。它们帮助我在代码技术上不断进阶。”

王倩楠现阶段的工作目标，是把目前正在做的锡安云平台 XDR 项目做得更优秀。

“XDR 不光是天擎的数据，还有锡安本地化自身的数据。这部分数据很有价值，如云查杀日志。XDR 是把我们锡安的数据和新天擎的数据结合，产生更多、更有用的信息。”

而对于自己，对于程序媛这个群体，王倩楠最后想说些心里话。

“许多人都觉得女生应该做轻松的工作，程序员加班多的工作性质，使得外界不大认同女生去做，并且有的时候许多人还有些刻板印象，认为女程序员技术还是不如男程序员。但我觉得，这个行业真正需要的是兴趣和天赋，和性别无关。我身边的程序媛很多都是自愿加班，她们都是喜欢这一行，愿意不断去钻研。而且女生天生心思细腻，比较有耐心，这是我们做软件编码的天然优势。

作为程序媛，我自己下一步的目标，是能成为开源社区的一个 Committer（apache 社区的正式成员），更希望有一天能成为 PMC Member（项目管理委员会的一员），让我的名号被所有人知道。”

程序媛王倩楠的成长故事，只是奇安信庞大研发人员群体故事中的一个。这样的故事每天都在发生。2021 年上半年，奇安信研发投入 7.7 亿元，同比增加 40.4%。重研发的奇安信拥有一流的研发队伍。正是这支队伍，为公司的持续高速发展提供了源源不断地强大动力。安

奇安信

新一代网络安全领军者

# 聚焦安全运营，构建智能平台

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


## 国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

## 首款分布式关联分析引擎 - Sabre

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

## 将平战结合进行落地

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

## 重大安全事件的威胁预警

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

## 专业的安全运营服务

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

## 市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一——数世咨询认证

# 寻找网络安全行业中的“奥运精神”

作者 公关部 魏开元 王梦琪 包世玉

“2分3秒86！中国选手张雨霏夺得200米女子蝶泳金牌，并创造了新的奥运会纪录！”

“6分20秒！我们第一时间发现并拦截了黑客攻击，资产、数据未受任何影响！”

“本届奥运会的跳高记录又升高了2公分。”

“经过大量机器学习和算法优化，恶意攻击检测的准确率和检出率分别提升0.5%。”

……

7月23日，延期一年的东京奥运会终于正式开幕。和往届相比，本届奥运会在国际奥委会的全会表决下，同意在奥林匹克格言“更快、更高、更强”。（Faster，Higher，Stronger）之后再加入“更团结”（Together）。内涵更丰富的奥运精神，将激励着运动健儿，在东京赛场上再创佳绩。


奥运精神，不仅仅存在竞技赛场之内。每一个平凡人，背后都有着不平凡的故事；每一个平凡人，都在自己的人生赛道上，不断突破自我，做自己的冠军。在网络安全行业上，就有这样一群人，他们在平凡的岗位上，践行着奥运精神。

## 更快：6分钟锁定攻击队 攻防战场上的速度与激情

一个普通人百米冲刺的速度大约是13~15秒，而奥运冠军的百米速度已经从100年多前的12秒提升至10秒以内，不断追求极致速度与自我超越，这大概就是对奥运精神“更快”最生动的诠释。用奥运速度与时间赛跑，奇安信的交付、安服和安运工程师们同样在属于自己的赛道中争分夺秒。

### （1）6min

“可能被攻破了！”驻守在攻防演习一线的安全监测工程师的一句话，让现场的气氛陡然凝重起来。

奇安信监测工程师通过防守方的“眼睛”——奇安信天眼发现了多条异常告警信息，在第一时间查看了精确告警和详细日志记录内容后，锁定了攻击方IP地址同步给分析研判组和应急处置组。应急处置组本着“先处置再分析”的方针，随即精准封禁攻击源IP地址，切断攻击链，阻止攻击者进一步下探攻击的可能性。

从发现告警到阻断攻击，各小组协同联动，他们只用了短短6分钟。

然而，在没有弄清楚“攻击从何而来”之前，工程师们的任务还远没有结束。接下来最重要的一步就是快速溯源，经过现场工程师的进一步分析发现，防守方被攻击的业务系统可能存在“未经身份认证可任意上传和读取下载文件”的0day漏洞，影响范围涉及该业务系统的所有用户。

下一步，就是还原攻击者是如何利用漏洞发起攻击的。研判专家通过对 VPN 日志审计，发现并还原了攻击者的完整链路：通过非正常手段获取了合规的 VPN 账户密码信息，并且成功将接收 VPN 验证的手机号由注册人员手机号改为自己所使用的手机号。

研判专家将收集到的所有线索、情报与证据素材统一反馈至产线，大家连夜赶工于次日凌晨分析事件原因并推出了安全加固解决方案。

至此，从成功发现攻击告警，到高效响应处置攻击事件、推出解决方案消除安全隐患，他们仅用时 7 小时。

### （2）5h

“李工！客户在召开政务视频会议时突然中断了 40 秒，我们必须赶快找到原因！”在听完现场工作人员焦急的报告后，奇安信驻场工程师李工即刻展开检查，并初步判断为客户边界安全设备链路切换导致断网。

与此同时，原本休假中的两位交付工程师义无反顾地放弃休假，立即赶往客户现场协助排查，二线专家也秉承着“客户优先”原则奔赴现场指挥。现场工程师们开始梳理各边界安全产品日志锁定事故发生时间，然后逐一对边界所部署的安全产品进行链路切换测试。

连续排查 5 小时后，直至深夜 24:00，经过交付工程师、现场专家等多方工作人员的测试，最终确认某边界安全产品出现软件故障，下联主路设备死机，导致此次视频会议期间断网。而奇安信防火墙在链路探测失败后触发链路切换，才使得客户网络得以恢复。

第一时间发现威胁、第一时间响应处置、第一时间多方联动……正是所有一线人员的“第一时间”，加上奇安信安全产品的强强联合，才能更快地消除安全隐患，让“网络安全快一步”。在奇安信眼中，这群同样追求“更快”速度、践行奥运精神的工程师们，也是平凡岗位中不平凡的特别“冠军”。

## 更高：用工匠精神打磨出奥运高标准

“作为奥运会史上首个网络安全的赞助商，我相信我们的产品能力和技术水平绝对能让客户感受到高标准和高品质。”

在去客户现场的路上，项目经理大鹤与研发经理小志这对“黄金搭档”，不停地回想老板在会上说的这句话。

究竟怎么才能够上奥运标准?

思忖间，客户的电话打过来了：“快到了吧？就等你们来了。我简单跟你们说下我们领导的要求……其实最重要的一点就是数据高可用要达到 99.99%，你们也知道，我们单位比较特殊，一旦系统数据中断时间过长，风险是非常大的。”

大鹤与小志相视一笑，他们心里很清楚，此次客户选择奇安信态势感知与安全运营平台（NGSOC）作为网络安全核心监测平台，就像火箭升空时的远程监控室，需要全盘掌握整体安全信息，对云上、云下的数据接入和应用提出了很高的要求，涉及物理机、虚拟机甚至包括友商的安全设备等，给项目建设带来了比较大的挑战。

到客户现场后，大家傻了眼：机房还未建立完善，里面没有办公桌和座椅，小志只好把旁边的服务器箱子搬过来，当办公桌和座椅。

不过，办公条件的简陋或许还能克服，但机房的低温却让他们直跺脚。“我去找客户再过一遍需求，顺便看能不能借几条毯子或者厚衣服过来。”大鹤站起来对哥儿几个说到。

研发计划、产品功能模块、项目分工表、技术难关攻克方案……会议室里，大鹤把项目计划讲的井井有条，另一边，他向客户借的毛毯也同时送到了研发同学的手里。此时，机房里噼里啪啦的键盘声如同夺冠的背景乐那样铿锵有力。

转眼十五天过去了，代码一行行如瀑布般随着鼠标滚轮倾泻而来，客户需要的配置核查、日志关联分析、告警管理、威胁可视化等功能模块也一个接着一个开发完成。这十五天的时间克服了多少技术难题，只有大鹤与小志他们自己知道。

临近计划交付的最后两天，各项指标经过测试已完全满足客户要求，数据高可用已完全达标，可以交付上线了。“前面大家拼的太猛了，看这进度，我们是不是可以提前回去休整一下了？”一位研发同事说到。

“别着急，咱们再多 POC 几次，看看是否还有优化空间，将数据可用性再迈上一个新台阶。”连轴转了不知道多少个日夜的小志，依然还是不依不饶。

若干次测试，若干次代码排查，还真发现了一些小瑕疵。

“这段调用接口的代码还可以再精简一下！”

一天半下来，经过反复测试之后，数据可用性达到了 99.999%，远远超出了客户预期和同行标准，获得了客户的赞誉。

这次项目结束之后，客户专门写了感谢信到公司，感谢项目团队的工匠精神，用更高的品质保证了各项业务系统稳定运行。

在小志与大鹤他们心里，或许也再次明白了奥运精神“更高”的真谛。

突然，大鹤接到了领导的来电：“客户那边来信，为了验证防护的有效性，他们马上就要组织内部的实战攻防演习，NGSOC 预计将成为网络安全防护的核心系统，你们有信心吗？”

大鹤心里一惊，原来更高的背后，还意味着更大的挑战。

## 更强：三年团队筑梦，一朝夺魁

网上总有人调侃：销售的强项嘛，无非就是请客喝酒，酒喝到位了，单子就谈下来了。

小葛是奇安信电力行业营销负责人之一，他对此直接说道：“网安行业的销售绝不是大家想象中的这样。我们对接的电力行业是很专业的，大多公司是半军事化管理，客户的网络安全建设非常成熟，对于我们的要求标准很高。想要拿下客户，技术、服务都要够强才可以。所以我们的销售和售前人员都要优中选优，综合素质和技术能力缺一不可。”

在最近的一次竞标中，小葛团队面临一个很大的挑战。原本在前期与客户沟通顺利的他们，突然发现半路杀出的 “程咬金”似乎想要 “截胡”。

狭路相逢，勇者胜。在网安行业，真正的强者才能胜出。

小葛回忆说：“细节不赘述，这次能够拿下此局，虽说不在我的意料之外，但也并非轻而易举。要说我们‘强’在了哪里，我认为这之前三年的 ‘团体训练’，打磨出了我们的‘最强阵容’。”

2018 年才开始涉足电力行业，他打趣道：“打造、训练团队就像是奥运会的团体赛准备，2018、2019、2020 年三年打磨，今年正式亮相。”打造团队，小葛有着自己的见解：“团队间给力的配合，是拿下一个个比赛赛点的关键！”

每一次比赛都凝聚了多方面努力。协同配合，各司

其职，劲儿往一处使，拧成一股绳的力量才更强大。

这个团队做到了，并最终得到了客户的认可。

同样提到了团队合作的，还有拿下银行 2000 多万大单的金融行业营销群大柯。聊起这次工作，他感慨颇多：“这次团队之所以能够有足够的底气给客户提供优秀且恰当的解决方案，背后少不了公司的法务、交付、安服的伙伴的支持。我们奇安信有技术、有产品，但把我们的技术和产品能够真正落实到一个个产品方案给到客户，团队中的每一个人都功不可没。”

有强大的公司品牌和平台背书，在遇到关键时刻有公司强大的资源储备力量支持。团队内技术有担当，策略有担当，投标有担当。能够赢得客户，靠的是强大的专业技术能力，以及将技术转化成方案的智慧，而这些都少不了一同协作的“最强阵容”。

有技术有头脑、有能力有担当，将公司产品、技术、服务通过一单单转化落地，销售团队的每一个队员都在一起努着一股劲儿，争取拿下“更强”的一单。

## 更团结：携手构建网络空间命运共同体

疫情深刻改变了世界的前行轨迹，也使通向东京奥运会的道路颇为曲折。它带来前所未有的挑战，也带来前所未有的启示：人类命运与共，我们需要更团结。在网络安全行业的每个岗位、每个故事中，也都离不开一个词：团结。

如果没有天眼产品及研发，以及安服、安运、交付等多团队之间的默契配合，6 分钟完成发现告警到阻断攻击，基本是天方夜谭。

没有项目经理和研发经理的配合无间，没有研发团队的戮力同心，就不可能实现产品高标准飞跃。

没有前方的销售和售前团队，以及后方的安服、法务、大客户服务、交付团队劲儿往一处使，拧成一股绳，就不可能在激烈的竞争中攻城略地、所向披靡。

从宏观层面看，当今世界正处于百年未有之大变局，做好新时代的网络安全，是中国与世界各国共同构建人类命运共同体，尤其是网络空间命运共同体的基础，更是打造网络空间新格局的现实需求。“更团结”的奥运精神，在这样的环境下显得愈发应景。

“更快”“更高”“更强”“更团结”，向外，体现了不断进取、永不满足、挑战极限的张力；向内，体现了戮力同心、配合无间的凝聚力。不仅在奥运赛场，也不仅仅在网络安全行业，每一个普通行业，每一个平凡岗位，每一个工作细节，都需要一种奥运精神。安

## 大事记

### 奇安信与广东联通产互达成战略合作 打造多元化安全合作“广东模式”样板

8月18日，奇安信与联通（广东）产业互联网有限公司（以下简称广东联通产互）签订战略合作协议。双方将在云安全、智慧城市、工业互联网、人才培养方面展开深入合作，重点打造华南安全创新运营中心，助力广东联通产互实现政企数字化转型，并以推动“广东模式”合作试点案例成功落地并复制到全国业务为战略目标。

本次战略合作的成功签署，双方将发挥各自专业优势、资源能力优势，聚焦云安全、互联网+安全、大数据安全、智慧城市数据安全和工业互联网安全等方面技术，积极推进产品方案和服务的深入探讨，共同打造战略协同、优势互补、资源共享、共同发展的生态合作伙伴关系，推动双方业务深度融合，促进行业可持续发展，从而打造“共享·共生·共赢”的多元化安全合作创新生态。


### 以安全信创助力碳中和 奇安信与恒华科技达成战略合作

8月17日，奇安信集团与恒华科技在奇安信安全中心举办战略合作签约仪式。根据协议，双方将在电力能源、轨道交通、教育培训等方面深度合作，形成数字化应用解决方案，并通过数字化业务场景实践和技术创新，以安全信创助力碳中和发展。

在最新发布的《北京市关于加快建设全球数字经济标杆城市的实施方案》中明确提出了支持碳中和的数字能源产业，“加快能源企业数字化转型，建设智能电网、智慧热网，率先建成全领域、全过程数字化智能化的城市能源系统”。双方作为北京市科技创新企业，战略合作的达成将有利于进一步发挥双方科技创新主体作用，壮大国家战略科技力量，推动新基建健康发展、助力碳中和目标实现。


### 奇安信与 UCloud 优刻得达成战略合作 共建云安全创新生态

8月13日，奇安信集团与UCloud优刻得战略合作签约仪式在UCloud优刻得上海总部举办。根据协议，奇安信与优刻得将发挥各自专业优势，在大数据、云计算等产品与服务方面展开深度合作，推动网络安全与云计算业务深度融合，促进行业可持续发展。


### 2021 虎符安全训练营圆满结营 16 门干货课程云端开讲

8月12日下午，历时三天的2021BCS特色活动－虎符安全训练营顺利结束，由27位行业顶尖高手组成的讲师团队，从工控安全、IoT安全、区块链安全、账号安全、电子取证、源代码安全、漏洞挖掘、红队战法、CTF实训、

逆向工程、大数据安全分析等多个热门领域，结合实战训练讲授网络安全攻防技巧，共有 300 余名学员顺利结业。

作为由奇安信集团主办的高端网络安全培训活动，本届虎符安全训练营以真实攻防场景还原为基础，聚焦实战化技术的要点和难点，设置了“虎符安全大师班”和“虎符安全精英班”两大部分，在云端授课过程中，各位讲师带着学员从行业痛点着手，理论结合实践，由浅入深，循序渐进，结合经典案例展开教学，分享实战经验、调试及挖掘技巧，将安全研究的过程拆解，并辅以相应的实操练习，还设置了答疑环节，讲师与学员克服远程不便，在云端积极互动。


## 2021 北京网络安全大会网络安全技能邀请赛（上海站）圆满落幕

8 月 11 日，2021 北京网络安全大会网络安全技能邀请赛（上海站）（以下简称“ 大赛”）颁奖仪式即赛事专项培训会在上海奇安信总部成功举办，来自上海市政府单位、金融机构、综合型央企国企、广电传媒等多个行业数十家单位参赛。国家计算机网络应急技术处理协调中心上海分中心运行部主任戴沁芸出席并为参赛队伍颁奖。


赛后，为确保参赛队伍实现“练习 – 竞技 – 复盘”的闭环学习，提升参赛者网络安全攻防实战能力，将网络安全实战化思路能有效地运用于信息安全系统建设与管理，面向全部参赛队伍及从事信息化建设、信息系统开发、网络建设、网络维护的信息技术人员等，举办了“基础攻防技能和 CTF 技能培训”，推动政企单位实现“内生安全”闭环建设。

## 北京市领导实地调研奇安信

8 月 9 日下午，北京市委常委、副市长殷勇携市“两区”办、市国资委等相关部门，实地调研奇安信公司并召开西城区“两区”建设和产业发展调研工作会。市政府副秘书长张劲松，区委副书记、区长孙硕，副区长聂杰英参加调研。

在奇安信公司，市领导一行参观公司文化墙及展厅。奇安信公司成立于 2014 年，为政府、企业用户提供新一代企业级网络安全产品和服务，凭借持续的研发创新和以实战攻防为核心的安全能力，已发展成为国内领先的基于大数据、人工智能和安全运营技术的网络安全供应商。

## 奇安信安全防护软件冬奥版正式上市

8 月 5 日，奇安信安全防护软件冬奥版（简称：奇安信安全防护）正式上市，奇安信集团副总裁张庭表示，针对 PC 端隐私保护等场景，安全防护冬奥版在病毒木马查

杀的基础上，重点强化了电脑隐私保护能力，并且能够将各类应用的运行和信息收集情况以图表可视化的形式呈现给用户，让用户对自己的电脑的运行状态、安全威胁、隐私保护等了如指掌。

张庭表示，针对PC端的安全防护软件，截至目前已经历三代。第一代安全软件以病毒查杀为核心，主要依赖本地病毒库的静态规则匹配技术，但随着病毒的变种、传播速度加快，以“月”为时间单位的病毒查杀效率已经失效；第二代安全软件更聚焦于查杀盗取账号、控制电脑的木马恶意程序，同时，加入了云防护技术，依靠云端的安全大数据进行实时分析，将病毒和木马的查杀效率大大提高至“分钟级”。

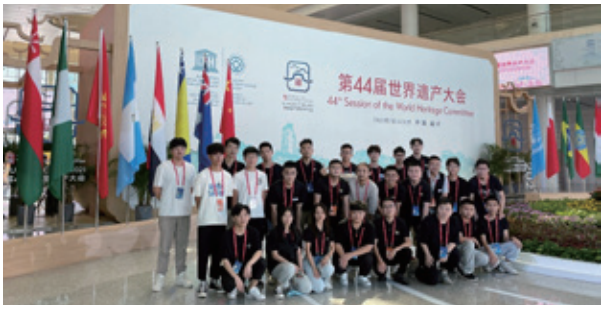
在奇安信安全防护软件冬奥版为代表的第三代安全软件中，病毒和木马的查杀是基础功能，重点是监测和约束正常软件的行为，保护用户的隐私信息。在安全能力方面，奇安信安全防护采用了冬奥标准的网络安全防护能力，内置猫头鹰（QOWL）反病毒引擎、深度学习（QDE）引擎、云规则（QCE）引擎，可覆盖百亿病毒木马样本。


## 奇安信圆满完成第44届世界遗产大会网络安全保障工作

7月31日，第44届世界遗产大会在福建省福州市闭幕。本次“加长版”会议审议了2020年和2021年两个年度的世界遗产项目。作为此次大会网络安全保障的核心力量，奇安信集团以创新的技术、丰富的经验积累、强大的安全能力和专业的团队服务，圆满完成了网络安全保障工作。

据统计，奇安信共计投入保障力量近1000人天，重保决战期间昼夜奋战768小时，配合组委会完成了大会网络安全实施方案制定、安全测试、攻防演练、7*24小时值守驻点、应急处置等保障工作。

除了一线重保服务团队，奇安信还投入了二线安全分析与应急处置专家团队、三线安全实验室安全研究团队及安全产品保障团队，以“实战化、体系化、常态化”理念为引领，在指挥调度、态势感知、安全编排与响应等产品和技术层面形成完整的技术支撑体系，圆满完成了此次网络安全保障工作。




## MOSEC 2021 移动安全技术峰会隆重召开

7月30日，由知名移动安全团队盘古实验室和韩国POC主办的2021MOSEC移动安全技术峰会在上海隆重举行。作为国内极负盛名的移动安全盛会，本次大会吸引到了数百名来自移动安全领域的顶级白帽黑客及行业专家，围绕iOS、Android等主流移动操作系统的漏洞挖掘、

漏洞利用以及安全防护等话题，为业界奉献了一场饕餮盛宴。

MOSEC 2021 涉及的细分领域更加广泛，包含了操作系统内核安全、浏览器内核安全、iOS 安全、Android 安全、5G 通信安全、芯片安全等多个维度，全方位展示相关漏洞的原理、危害及防护方法。

## 盘古实验室签约赛博昆仑 国内两大白帽天团强强联合

在 2021 第七届 MOSEC 移动安全技术峰会上，国内知名移动安全团队盘古实验室与赛博昆仑达成战略合作，双方将在漏洞挖掘、高级威胁防护等领域展开全方位的合作。

盘古实验室创始人韩争光（TB）表示，本次合作，双方将充分发挥各自团队在漏洞挖掘、漏洞防护、高级威胁检测与响应等领域的优势，着力打造新一代移动安全产品和解决方案，帮助政企机构构建完善的安全防护体系。


## 奇安信与新疆信息产业有限责任公司达成战略合作

7 月 27 日，新疆信息产业有限责任公司与奇安信集团战略合作协议签约仪式在新疆乌鲁木齐举行，双方将在创新研发，安全服务能力，产品销售业务等领域展开深度合作，共同促进推进电力行业网络安全生态发展与融合。

根据协议，信息产业公司与奇安信集团将充分发挥自身优势，为对方提供各自优势领域的资源，以实现共赢：在产品研发方面，双方携手研究安全与创新产品，深度挖掘用户需求，实现客户价值；在安全服务方面，双方合作打造“以人为核心的安全运营服务”队伍，联合探索电力行业网络安全服务新模式；在人才培养方面，双方共同建设一流的安全人才发展与交流平台，培养实战型、多层次的网络安全专业人才。


## 2021 北京数字经济体验周系列活动走进奇安信 让网络安全“可触摸、能体验”

“2021 北京数字经济体验周”是“2021 全球数字经济大会”的三大特色活动之一，与大会形成“高峰论坛 + 落地普及”双互动。体验周系列活动下设四大板块，共计覆盖 22 处数字经济场景地、11 处数字经济网红打卡地及 12 处信息消费体验中心，为北京市民呈现一场全方位、零距离的数字经济触达式体验。奇安信安全中心云展厅成为北京 22 处数字经济场景开放地之一。

体验周期间，北京市国资委及市属重点企业、市教委、市税务局、市住房公积金管理中心、市城市建设档案馆、

经开区管委会、东城区应急局、海淀区统计局等部门及领导来到奇安信云展厅参观体验。

## 奇安信亮相 2021 政法智能化建设技术装备及成果展并获多项荣誉

7 月 27 日，由法制日报、北京安全防范行业协会主办，中国警察网、北京法安网络文化传媒有限公司（法安网）承办的“2021 政法智能化建设技术装备及成果展”在北京国家会议中心开展，200 余家科技企业参展，一大批政法领域高新技术装备亮相展会。

奇安信集团携“网络安全快一步 助推政法智能化”主题展区亮相展会，司法部戒毒管理局二级巡视员李晓，法制日报社党委书记、社长邵炳芳等领导莅临奇安信展台并指导工作。

展会期间，奇安信还喜提多项荣誉：奇安信“智慧监狱”人员行为数据分析系统经过前期申报、网上投票、专家评审等多项角逐、脱颖而出，荣获“智慧司法”创新产品一等奖；《从企业角度看智慧监狱建设中 AIOT 技术在监狱业务的实践与探索》荣获 2021 政法智能化建设智慧司法论文三等奖。


## 奇安信与工信部电子一所达成战略合作

7 月 26 日，奇安信集团与国家工业信息安全发展研究中心（工业和信息化部电子第一研究所，以下简称“国家工信安全中心”）签署战略合作协议，双方将在工业安全、车联网安全、数据安全、开源代码、信创、漏洞发现与检测、安全测评等领域，共同促进推进安全产业生态发展与融合。

本次战略合作的达成，将形成资源、技术的优势互补。双方可充分发挥各自特长，从政策研究、标准制定、技术研发、咨询规划等方面推动行业趋向于良性有序的发展；开展试点应用、测试验证等工作，共同促进推进安全产业生态发展与融合，携手为我国网络安全强国的建设提供支持。

会议由国家工信安全中心党委书记、副主任蒋艳主持，国家工信安全中心主任、党委副书记赵岩，中国电子总经理助理、数字办常务副主任、中电互联董事长朱立锋出席并见证签约。

## 2021 央企网络安全运营体系建设研讨会在京召开

近日，由奇安信集团主办的“央企网络安全运营体系建设研讨会”在北京召开。会议以“实战化安全运营体系建设”为主题，围绕“安全运营体系建设及实践经验”展开。

来自中国电子集团、中国交通建设集团、中国中化、中储粮集团等四十余家大型中央企业信息化负责人、网络安全专家出席，围绕会议主题，以不同行业视角结合实战经验进行深度剖析和解读，为安全运营体系的建设提供了新的思路，助推行业更好的落地网络安全运营体系。

## 2021 中国网络安全年会数据安全分论坛顺利召开

7 月 21 日下午，由国家计算机网络应急技术处理协调中心指导、奇安信主办的“数据安全分论坛”顺利举办。

作为第 18 届中国网络安全年会的重要分论坛，数据安全分论坛以“数据安全新要求 风险治理新理念”为主题，围绕数据安全法律法规、数据安全治理、跨国企业用户数据隐私保护、数据要素流通交易等行业热点进行深入交流沟通。

作为本届中国网络安全年会的重点论坛之一，本次“数据安全分论坛”，为政、产、学、研各部门搭建起交流平台，加强各方在数据安全与风险治理方面的交流互鉴，协同行业共同助力国家数字经济的安全健康发展。


## 奇安信当选零信任联盟常务理事单位

7 月 21 日，零信任联盟（以下简称“联盟”）第一届理事会第一次会议在京正式召开。会议表决通过了《零信任联盟章程（草案）》等联盟文件，奇安信当选为常务理事单位，奇安信副总裁、首席战略官刘勇当选联盟执行理事长，奇安信副总裁陈华平当选联盟副理事长，奇安信身份安全事业部总经理张泽洲被任命为联盟秘书长。


据介绍，零信任联盟是国内首个以零信任为主题的联盟组织，在中国电子信息产业集团指导下，由中国信息安全研究院和奇安信集团牵头发起正式发起成立，目前已有 53 家成员单位，旨在扩大自主安全信创生态零信任架构落地应用，推进零信任教育、技术、产业融合发展，加快形成人才培养，技术创新，产业发展的良性生态。

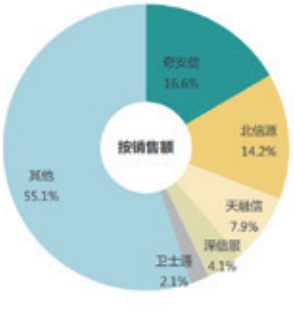
## 荣誉墙

### 赛迪报告：2020 年奇安信在网络安全整体市场位列第一

国内权威咨询机构赛迪顾问发布《2020-2021 年中国网络信息安全市场研究年度报告》（以下简称《报告》），数据显示，2020 年中国网络信息安全市场达到 718.8 亿元，增长率为 18.2%。其中，奇安信集团安全业务以 41.6 亿元的营业收入再次位居市场第一位，并在终端安全、安全服务市场等重要细分领域持续领跑。

《报告》显示，2020 年奇安信集团坚持“强研发”战略，从“快速上规模”迈向“高质量发展”阶段，于 7 月科创板开市一周年之际，正式登陆科创板，并成为国内首家在网络安全行业营业收入迈入 40 亿大关的网络安全公司。

图 12 2020 年中国终端安全市场品牌结构



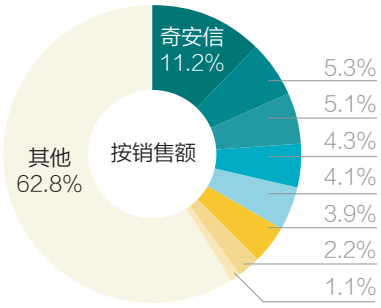

数据来源：赛迪顾问 2021，02

## 赛迪发布云安全市场研究报告 奇安信连续三年稳居市场份额首位

赛迪顾问发布的《2020-2021 年中国云安全市场研究年度报告》显示，奇安信以 7.25% 的占比稳居市场份额榜首，并在云计算安全这一重要细分领域，以 11.2% 的市场份额位列第一。从 2018-2019 年度报告开始，奇安信已经连续三年蝉联云安全市场份额第一。

赛迪顾问直属于中国电子信息产业发展研究院，此次报告主要聚焦于我国云安全总体及细分领域发展情况。报告中指出，2020 年，中国云安全市场规模增长迅猛，共计 82.5 亿元，同比增长 49.7%。受到合规需求等影响，政府、电信与互联网、金融依旧是 2020 年占比最大的行业市场。奇安信凭借全面、立体的云安全能力，云安全解决方案已成功应用于政府、央企、金融、运营商、交通、医疗卫生等多个行业，成为国内云安全市场首屈一指的领军者。

**2020 年中国云计算安全市场品牌结构**




数据来源：赛迪顾问 2021,02

## Gartner 发布 CWPP 和 ICT 技术成熟度曲线两项报告 奇安信入选代表能力供应商

近日，Gartner 发布《Hype Cycle for ICT in China, 2021》(《2021 中国 ICT 技术成熟度曲线》)和《Market Guide for Cloud Workload Protection Platforms》（《云工作负载保护平台市场指南》）两份报告，奇安信凭借全面、立体的云安全能力入选 Gartner 上述报告的代表能力供应商。

奇安信服务器安全管理系统（云锁）与奇安信统一服务器安全管理系统（虚拟化安全）均受到 Gartner 推荐，符合云工作负载保护平台（CWPP）品类能力要求的代表性产品。奇安信基于新一代网络安全框架体系，通过云安全管理平台、云安全运营中心、服务器安全管理系统（云锁）、统一服务器安全管理系统（虚拟化安全）等产品，合力打造面向多云环境的全面、立体的云安全能力。

## 奇安信荣膺 Frost&Sullivan“中国安全编排自动化与响应（SOAR）市场领导奖”

近日，国际咨询公司 Frost&Sullivan（弗若斯特沙利文）公布 2021 年度“最佳实践奖”获奖情况，奇安信集团凭借安全编排自动化与响应 (SOAR) 产品的突出表现，荣膺“中国安全编排自动化与响应（SOAR）市场领导奖”，在产品创新实力与行业贡献、领导地位等层面获得了充分肯定。

据了解，Frost&Sullivan 最佳实践奖是对全球和各个地区的企业在领导力、技术创新、客户服务和战略产品开发等方面取得的卓越表现以及杰出成绩的表彰，其评定标准基于企业收入、市场份额、企业能力和行业总体贡献四大指标，经过 10 余年的发展，已经取得了业界的广泛认可。

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



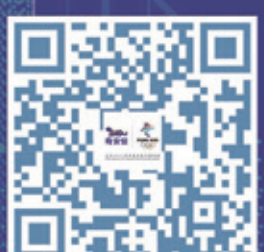
国际经验分享系列




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 |