

SECURITY INSIDER

# 网安 26号院

奇安信网络安全通讯

## 十大技术趋势

P14

2024



### 第36期

2023年12月

# 打造新一代中国特色的 安全托管服务

时刻守护您的网络安全



奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7\*24小时全天候全方位守护客户网络安全。

## 两种模式

模式随心选择

- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

## 多种形态

全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

## 两化融合

帮您真正实现

- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享



### 首创“云地结合” 模式

打破传统的托管仅限“云端监测”的认知，开辟“云地结合”模式，云端+地端实现真正的闭环服务。



### 7\*24h实时 持续监测

“地球不爆炸，我们不放假”——7\*24h持续监测，充分保障常态化运营。



### 安全事件响应 快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。



### 安全事件处置 规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加强。



### 专家“一对一” 指导

专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

# 不确定性中的确定性

预测未来的趋势可能是件愚蠢的事。比如一年前有人悲观地预测，对基础设施的网络攻击可能会引发世界大战；也如很多人在年初乐观地预测，2023年将会出现强劲的经济复苏。

在网络安全领域，最大的确定性就是不确定性。很多人认为，网络安全领域正处于变革的边缘。IT架构复杂性不断增加，网络攻击频率不断上升、愈加复杂。面对快速发展的攻击媒介，预测和对特定威胁做好应对的传统方法越来越不可行。这也是业内人士认为网络安全需要进行范式转变的原因。

网络安全行业似乎陷入了没有尽头的循环之中，只要有新技术，就会出现新的零日漏洞和利用漏洞的攻击者：开发人员构建新的安全软件，而犯罪分子则不断寻找新的方法进行破坏，随后零日漏洞被发现、利用，然后被修复，最后重新开始新的循环。

因此很多人关心，范式转变何时会发生？有迹象表明，技术进步、地缘政治、社会影响和其他外部因素为托马斯·库恩所提出的“范式转变”创造了条件。推动网络安全范式转变的条件是网络攻击的广度、类型和严重程度，这些在2024年可能会显著增加。据预计，2023年全球网络攻击的损失将达8万亿美元，比中美之外其他任何国家的经济规模都要大。

谷歌曼迪安特、派拓网络及奇安信等全球网络安全企业预测，2024年生成式AI将会重塑网络安全。2024年生成式AI将趋于成熟，可以显著提高安全运营的效率。与此同时，攻击者利用大型语言模型和生成式AI改进钓鱼邮件、大幅提高点击率。生成式AI还会降低攻击的门槛，利用AI发起的攻击数量激增，网络威胁形势正发生重大转变。

生成式AI的重要性如此之高，派拓网络CSO甚至认为，首席信息安全官将成为首席人工智能安全官(CAISO)。未来显然需要重视利用AI大模型，通过实时和自主系统帮助主动预测威胁。

此外，攻击者使用暴力破解工具，以及生成式AI增强的社工攻击，可轻松攻破身份验证机制，在2023年已制造数起重大的安全事件。专家预计，2024年业界将会在更大范围向零信任框架过渡，从而为更强大的安全态势奠定基础。

利用AI大模型主动预测威胁，向零信任框架转变，这是否代表网络安全的范式转变？或许吧。面对日趋复杂的安全态势和IT环境，安全从业者唯有从被动式响应转向主动威胁管理转变，才能适应不断变化的形势。

总编辑

李建平

2023年12月1日



### 安全态势

- P4 | 《工业和信息化领域数据安全事件应急预案（试行）》公开征求意见
- P4 | 国家网信办《网络安全事件报告管理办法》公开征求意见
- P4 | 25 项密码行业标准发布，明年 6 月 1 日起实施
- P4 | 中国民航局发布《民用航空生产运行工业控制系统网络安全防护技术要求》
- P5 | 信安标委发布《网络安全标准实践指南——网络安全产品互联互通 告警信息格式》
- P5 | 欧盟就《人工智能法案》达成三方协议
- P5 | 欧盟就《网络弹性法案》达成非正式协议
- P5 | 英美等 18 国联合发布《安全 AI 系统开发指南》

- P6 | 俄乌网络战再升级：乌克兰全国断网、俄罗斯税务系统瘫痪
- P6 | 重庆一企业泄露大量数据，被当地网信办罚款 10 万元
- P6 | 美国知名基因测试公司 23andMe 被黑，或泄露 30 万华人血缘数据
- P6 | 美国金融行业云被勒索，超 60 家信用社服务中断
- P7 | 埃及电子支付巨头遭勒索攻击，花费近半个月恢复正常
- P7 | 美国大型医院集团遭勒索攻击，多州急诊室紧急转移救护车
- P7 | 美国地方城镇供水系统遭伊朗黑客破坏，美监管机构发布预警
- P8 | Apache Struts 代码执行漏洞安全风险通告
- P8 | Apache OFBiz 远程代码执行漏洞安全风险通告
- P8 | Apple 多产品多个在野高危漏洞安全风险通告 08
- P8 | Apache ActiveMQ Jolokia 代码执行漏洞安全风险通告
- P9 | 2023 年漏洞态势简报
- P10 | 国内攻防演习 11 月态势：哪些薄弱点最易被利用？

### 月度专题

网络威胁、安全态势，以及攻防对抗力量的变化，驱动网络安全技术持续创新。奇安信认为，2024 年需要关注 10 大技术趋势，积极拥抱技术创新，才能更好地适应应对网络威胁和保障数字经济稳定发展的需要。



## 年度回顾

### P28

2023 年数据安全 10 大事件

### P34

2023 年 AI 安全 10 大事件

### P40

2023 年 15 起重大云服务中断事件

### P46

2023 年勒索软件攻击盘点

### P50

2023 年全球 10 大网络攻击事件

## 安全叨客

### P54

完了！我被公司高管们包围了

## 报告速递

### P58

2024 年网络安全趋势，  
国外大厂怎么看？



## 奇安资讯

- P62 | 香港科技园与奇安信集团签署合作备忘录 将在港设国际研发中心
- P62 | 国际化业务新突破 奇安信与四家港企签署合作协议
- P63 | 齐向东连任中国网络空间安全协会副理事长
- P63 | 浪潮集团董事长邹庆忠一行到访奇安信安全中心
- P64 | 清华大学创新领军工程博士班师生到访奇安信
- P64 | 齐向东：用“四道防线”筑牢数字政府安全根基
- P65 | 紫金山实验室与奇安信集团达成战略合作
- P65 | 奇安信集团入选教育部 2023 年供需对接就业育人项目企业名单
- P66 | 齐子昕出席第五届“一带一路”女性论坛：青年领导力推动科技创新再提速
- P66 | 吴云坤：创新思维和技术 构建保密安全体系
- P67 | 南水北调集团联合奇安信牵头的水网安全融合工程创新中心正式揭牌
- P67 | 奇安信中标某有色金属集团态势感知平台项目
- P68 | 北京网神洞鉴入选北京法院对外委托专业机构备选名册
- P69 | 奇安信获得国家级数据安全服务资质
- P70 | 奇安信入选 SSE 权威报告代表厂商
- P71 | 奇安信集团入选首批可信数据空间应用解决方案供应商
- P72 | 2023 北京企业百强榜单出炉 奇安信集团连续两年登榜
- P73 | 奇安信基金会积极组织开展扫雪铲冰志愿服务

《网安 26 号院》编辑部

主办 奇安信集团

总 编 辑：李建平

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

安全叨客主编：魏开元

奇安资讯主编：陈 冲

报告速递主编：赵天宇

专 栏主编：李建平



奇安信集团



虎符智库



安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com

地 址：北京市西城区西直门外南路 26 院 1 号

邮 编：100044

联系电话：(010) 13701388557

出版物准印证号：京内资准字 2123- L0058 号

编印单位：奇安信科技集团股份有限公司

发送对象：奇安信集团内部人员

印刷数量：4500 本

印刷单位：北京博海升彩色印刷有限公司

印刷日期：2023 年 12 月 26 日

**版权所有 ©2023 奇安信集团，保留一切权利。**

非经奇安信集团书面同意，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，奇安信集团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适用于某一特定目的的保证。在法律允许的范围内，奇安信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。

内部资料 免费交流



## 政策篇



国内，临近年关时节，部委机构密集发布多项政策公开征求意见，包括国家网信办《网络安全事件报告管理办法》、工信部《工业和信息化领域数据安全事件应急预案（试行）》、国家数据局《“数据要素×”三年行动计划（2024—2026年）》等；

国际上，英美等18国网络安全机构联合发布《安全AI系统开发指南》，以指导使用了AI的系统提供商，构建按预期运行、在需要时可用且不与未经授权方泄露敏感数据的AI系统。



## 《工业和信息化领域数据安全事件应急预案（试行）》公开征求意见

12月15日工信部消息，工业和信息化部网络安全管理局起草了《工业和信息化领域数据安全事件应急预案（征求意见稿）》，现公开征求意见。该文件正文共8章三十九条，4份附件《工业和信息化领域数据安全事件分级》《数据安全事件上报（模版）》《数据安全事件应急处置工作总结报告（模版）》《数据安全事件应急处置流程图》。该文件提出，数据安全风险预警等级分为红色、橙色、黄色和蓝色四级，数据安全事件应急响应分为I级、II级、III级、IV级四级，分别对应可能发生特别重大、重大、较大和一般数据安全事件。



## 国家网信办《网络安全事件报告管理办法》公开征求意见

12月8日国家网信办消息，国家互联网信息办公室起草了《网络安全事件报告管理办法（征求意见稿）》，现公开征求意见。该文件共14条正文，2份附件《网络安全事件分级指南》《网络安全事件信息报告表》。该文件所指网络安全事件是指由于人为原因、软/硬件缺陷或故障、自然灾害等，对网络和信息系统中或其中的数据造成危害，对社会造成负面影响的事件。该文件要求，运营者在发生网络安全事

件时，应当及时启动应急预案进行处置。按照《网络安全事件分级指南》，属于较大、重大或特别重大网络安全事件的，应当于1小时内进行报告。



## 25项密码行业标准发布，明年6月1日起实施

12月6日国家密码管理局消息，国家密码管理局发布了25项密码行业标准，自2024年6月1日起实施。同时，2012年发布的18项标准旧版本同日起予以废止。包括《密码应用标识规范》《数字证书认证系统密码协议规范》《密码设备应用接口规范》《IPSec VPN技术规范》《SSL VPN技术规范》《安全认证网关产品规范》等。



## 中国民航局发布《民用航空生产运行工业控制系统网络安全防护技术要求》

12月6日中国民航局消息，中国民用航空局发布《民用航空生产运行工业控制系统网络安全防护技术要求》，自2024年1月1日起实施。该文件界定了民用航空生产运行工业控制系统的安全防护对象，规定了现场设备、控制设备、工业主机、网络设备、网络安全设备等设备级安全技术要求，以及分区分域与隔离防护、数据与通信安全、安全监控与应急处置、系统运维安全、软件供应链安全等系统级安全技术要求。



## 信安标委发布《网络安全标准实践指南——网络安全产品互联互通告警信息格式》

11月28日全国信安标委网站消息，全国信安标委编制发布了《网络安全标准实践指南——网络安全产品互联互通告警信息格式》。该文件给出了网络安全产品互联互通时告警信息的描述格式，可用于指导网络安全产品互联互通功能的设计、开发、应用和测试。告警信息，是指网络安全产品依据设定的规则或模型，对采集到的网络安全信息自动进行规则匹配、归并、分析等活动后产生的警示信息。该文件将告警分为恶意程序告警、网络攻击告警、数据安全告警、异常行为告警和其他告警5类，每个类别分别包括若干子类。



## 欧盟就《人工智能法案》达成三方协议

12月9日新华社消息，欧洲议会、欧盟成员国和欧盟委员会三方8日晚就《人工智能法案》达成协议，该法案将成为全球首部人工智能领域的全面监管法规。欧盟委员会于2021年4月提出《人工智能法案》提案的谈判授权草案，将严格禁止“对人类安全造成不可接受风险的人工智能系统”，包括有目的地操纵技术、利用人性弱点或根据行为、社会地位和个人特征等进行评价的系统等。该草案还要求人工智能公司对其算法保持人为控制，提供技术文件，并为“高风险”应用建立风险管理系统。每个欧盟成员国都将设立一个监督机构，确保这些规则得到遵守。



## 欧盟就《网络弹性法案》达成非正式协议

12月1日欧洲议会消息，欧洲议会议员与欧盟理事会主席于11月30日就《网络弹性法案》达成非正式协议，以保护欧盟所有的数字产品免受网络威胁。《网络弹性法案》是全球首个数字产品安全立法，它对所有硬件和软件设置了不同级别的强制性网络安全要求，制造商需要在产品生命周期内实施对应措施，并附带CE标志表明符合法律要求，才可以在欧盟销售。该法案下一步需欧洲议会和欧盟理事会通过才能成为法律。



## 英美等18国联合发布《安全AI系统开发指南》

11月27日NCSC消息，英国国家网络安全中心（NCSC）、美国网络安全与基础设施安全局（CISA）等18国23家政府安全机构联合发布《安全AI系统开发指南》，以指导使用了AI的系统提供商，构建按预期运行、在需要时可用且不向未经授权方泄露敏感数据的AI系统。该文件将AI安全开发生命周期分为4个部分，包括安全设计、安全开发、安全部署、安全运营，并针对每部分给出考虑因素和缓解措施。该文件将有助于降低AI系统开发过程的总体风险。



## 美国海军部发布2023版《网络战略》

11月21日美国海军官网消息，美国海军部发布2023版《网络战略》，旨在指导海军和海军陆战队加强网络态势，利用网络领域的非动能效应实现海军部任务目标。该战略建立在美海军多年全球网络领域行动的经验教训之上，概述了海军部计划如何强化现有成功举措并改进弱项，将重点解决体系网络安全、网络防御和进攻性网络作战问题。战略指出海军部在网络空间领域的7个重点工作方向：一是建设网络人才队伍；二是从合规性转向网络战备；三是保护体系信息技术、数据和网络；四是确保国防关键基础设施和武器系统的安全；五是开展并推进网络行动；六是与合作伙伴确保国防工业基地安全；七是促进协同合作。



## 美国国防部公开发布2023版《信息环境作战战略》

11月17日美国国防部官网消息，美国国防部公开发布2023版《信息环境作战战略》。该战略旨在提高国防部规划、配置资源和运用信息力量的能力，以实现综合威慑并建立持久优势。战略提供了国防部体系方法，以确保改进信息部队和信息能力、作战、活动、项目和技术的整合和监督。这将使国防部能够在全球范围内跨所有域提高其在信息环境中并通过信息环境开展行动的能力，利用电磁频谱实现持久的战略成果。为了支持国防部全面整合信息环境中的作战并使之现代化，该战略确定了四方面工作内容：人员与组织、项目、政策与治理、伙伴关系。该战略于今年7月由国防部长劳埃德·奥斯汀签署，标志着自2016年以来的首次更新。

## 事件篇



针对产业链关键环节的勒索攻击频频发生，以小切口实现大影响。美国金融行业云被勒索，导致超 60 家信用社服务中断；以色列产控制器遭利用，美国近 10 个水务系统遭攻击；英国爆发网络攻击级联效应，托管服务商被黑影响数百律所影响全国房产交易……



### 俄乌网络战再升级：乌克兰全国断网、俄罗斯税务系统瘫痪

12月12日综合消息，俄罗斯与乌克兰关键基础设施日前分别遭受重大网络攻击，昭示着双方网络战已出现再次升级。乌克兰最大的移动运营商 Kyivstar 遭遇严重网络攻击，导致该公司官方网站下线，发生全国性的通信和数据服务中断，甚至空袭警报通知和银行业务都受到严重影响。Kyivstar 在推特上告知用户，遭到黑客攻击导致技术故障。Kyivstar 首席执行官在公开讲话中暗示，Kyivstar 遭受的重大攻击来自俄罗斯黑客。同日，乌克兰国防情报局宣布，成功用恶意软件感染并瘫痪了俄罗斯国家税务系统的数千台服务器，并破坏了数据库和备份。根据乌克兰国防情报局的说法，俄罗斯联邦税务局的基础设施已经“被完全摧毁”，“多年来确保俄罗斯税务系统正常运转的配置文件也被销毁”，这将导致俄罗斯联邦税务系统至少要瘫痪一个月，而且“永远不会从攻击中完全恢复”。这也是乌克兰国防情报局第二次公开承认对俄罗斯国家机构发动重大网络攻击。



### 重庆一企业泄露大量数据，被当地网信办罚款 10 万元

12月11日网信重庆公众号消息，根据上级部门移交的线索，渝中区网信办在重庆市网信办指导下，依法对属地一科技公司涉数据泄露等违法违规行为进行立案查处，作出责令限期五日改正，给予行政警告并处 10 万元罚款的行政处罚。经查，该公司开发运营的某 OA 信息系统因未履行好网络数据安全保护义务，导致大量数据泄露，情节严重。且该公司作为网络数据处理者，未依法建立健全全流程网络数据安全

管理制度，未依法组织开展网络数据安全教育培训，未采取相应的技术措施和其他必要措施等保障网络数据安全。渝中区网信办依据《中华人民共和国数据安全法》规定，对该公司作出了限期五日改正、给予行政警告，并处罚款 10 万元的行政处罚。目前，该公司已完成整改，建立健全相关管理制度，并全额缴纳罚款。



### 美国知名基因测试公司 23andMe 被黑，或泄露 30 万华人血缘数据

12月4日纽约时报消息，美国基因测试公司 23andMe 透露，黑客利用客户的旧密码，成功窃取了约 690 万份用户档案的个人信息。23andMe 在 SEC 披露文件中称，攻击者通过撞库攻击，窃取了该公司约 1.4 万用户的账号访问权，可以访问这些账号下的用户基因和健康数据，还可以通过 23andMe 共享功能，访问近 700 万用户的个人信息（DNA 相似度、双方血缘关系预测等）。据悉，此前攻击者在地下论坛中公布了约 100 万犹太裔和 30 万华裔的样例用户数据，并对外报价 1~10 美元单个账号数据进行售卖。



### 美国金融行业云被勒索，超 60 家信用社服务中断

12月1日 The Record 消息，美国国家信用合作社管理局（NCUA）发言人称，由于云服务提供商 Ongoing Operations 遭勒索软件攻击，大约有 60 家信用合作社面临各种程度的服务中断。Ongoing Operations 于 11 月 26 日向多家信用合作社发送消息，称公司遭到勒索软件攻击。该事



件对平台上的解决方案厂商及信用社造成了较大影响，如山谷联邦信用合作社发布通知，警告客户他们正在应对严重的服务中断。NCUA 发言人表示，“该部门正在与受影响的信用合作社进行协调。受影响的联邦保险信用合作社的会员存款由国家信用合作社股份保险基金承保，金额最高可达 25 万美元。”



## 埃及电子支付巨头遭勒索攻击，花费近半个月恢复正常

11 月 29 日 DarkReading 消息，LockBit 3.0 勒索软件团伙宣布攻击了埃及最大的电子支付提供商 Fawry，不仅成功加密了文件，还声称窃取了数据。11 月 8 日，LockBit 在其专用泄漏网站发布了 Fawry 相关数据样本，将这次入侵行动公之于众。次日，网络安全监控平台 Hackmanac 声称，此次 LockBit 3.0 勒索软件攻击窃取了 Fawry 客户的个人详细信息，导致多家银行建议客户删除 Fawry 平台上的账户信息。Fawry 起初否认数据泄露，后续再次声明表示发现测试环境泄露的数据可能包含一些客户个人信息。Fawry 聘请了安全厂商 Group-IB 来调查此次事件，经过近半月时间彻底清除了勒索软件的痕迹，使得业务环境恢复正常。



## 美国大型医院集团遭勒索攻击，多州急诊室紧急转移救护车

11 月 27 日 CNN 消息，由于遭受网络攻击，美国得克萨斯州东部地区多家医院在感恩节当天被迫转移救护车。医院代表表示，这次攻击还迫使新泽西州、新墨西哥州和俄克拉荷马州的医院转移救护车。所有受影响医院都由 Ardent 健康服务公司全资或部分拥有。该公司总部位于田纳西州，在至少五个州拥有二十多家医院。目前，部分医院无法接收救护车，成千上万的患者受影响。这是又一例勒索攻击严重扰乱医疗服务的案例，其特殊之处在于美国 CISA 曾联系 Ardent 公司警告存在恶意活动，但此时已为时已晚，该公司已经中招。



## 美国地方城镇供水系统遭伊朗黑客破坏，美监管机构发布预警

11 月 25 日 BeaverCountian 消息，美国宾州阿里奎

帕市市政供水系统遭到黑客组织 Cyber Av3ngers 部分控制，该组织自称隶属于和伊朗政府有关的网络游击队，正在攻击以色列公司制造的关键基础设施硬件。他们关闭了该市一条输送饮用水供应管道的水泵，该系统的控制器由以色列公司犹尼康生产。阿里奎帕市水务局主席 Matthew Mottes 表示，“他们侵入了一台帮助系统向高处供水的增压水泵。除此之外，他们没有侵入我们实际水处理厂中的任何东西。”阿里奎帕市政工作人员已经停用了受影响设备，依靠备用方法维持社区的供水水压。美国网络安全与基础设施安全局后续发布安全警告，称美国有近 10 个系统遭到攻击，并面向水务系统管理员给出缓解措施。



## 英国爆发网络攻击级联效应，托管服务商被黑影响数百律所影响全国房产交易

11 月 24 日 The Record 消息，英国律师事务所托管服务提供商 CTS 遭网络攻击引发服务中断，这可能导致了数百家英国律所无法访问客户案件管理系统，并使得下游的房地产交易公司无法进行房产交易。Today's Conveyancer 出具一份报告显示，估计约有 80 到 200 家客户“无法访问电话、电子邮件或案件管理系统。”O' Neill Patient、Talbots Law 和 Taylor Rose MW 等多家英国律师事务所均发表声明，通知客户“由于法律行业内的多个组织受到技术故障影响，目前正在经历服务困难”。该事件可能会严重耽误许多本应在当天完成的房产交易工作。英国政府发言人表示，政府正在“密切监控该公司的情况”。



## 美国最大产权保险商被黑后关机断网，全美大量购房交易被迫暂停

11 月 21 日房地产新闻消息，美国最大的产权保险公司富达国民金融（Fidelity National Financial）遭黑客攻击，导致原定房产交易无法进行，经纪人和购房者被迫匆忙寻找解决方案。富达国民金融向美国证券交易委员会（SEC）提交报告表示，产权相关服务的系统已经隔离。有知情者称，该公司内网已经全面封锁，决定关机断网以清理服务器，防止出现任何问题。有房产经纪人表示，由于结算系统停机，购房者已收到银行贷款但无法购房，将承担额外的负担。据悉，如果短期无法恢复系统，购房者将采用线下购买的传统办法。



2023年已经进入倒计时，奇安信 CERT 基于监测数据整理了全年漏洞态势简报，其中有整体数据、重点漏洞、最热漏洞等多维度数据，可供各位读者参考。如需更多细节数据，可通过文末的联系方式联络。



### Apache Struts 代码执行漏洞安全风险通告

12月8日，奇安信 CERT 监测到 Apache Struts 代码执行漏洞 (CVE-2023-50164)，攻击者可以控制文件上传参数执行路径遍历，在某些情况下可以上传恶意文件，从而执行任意代码。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。



### Apache OFBiz 远程代码执行漏洞安全风险通告

12月7日，奇安信 CERT 监测到 Apache OFBiz 远程代码执行漏洞 (CVE-2023-49070)，由于 XML-RPC 仍然存在于 Apache Ofbiz 18.12.10 之前的版本，远程未授权攻击者可绕过防护措施访问 /webtools/control/xmlrpc 利用此漏洞导致任意代码执行，接管目标服务器。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。



### Apple 多产品多个在野高危漏洞安全风险通告

12月1日，奇安信 CERT 监测到 Apple 多产品发布新版本修复了存在在野利用的 Apple WebKit 越界读取漏洞 (CVE-2023-42916) 与 Apple WebKit 代码执行漏洞 (CVE-2023-42917)，未经身份验证的远程攻击者可以诱导受害者访问特制的网站，成功利用这些漏洞读取敏感信息或执行代码。目前 Apple 获悉一份报告，称这些漏洞可能已在 iOS < 16.7.1 版本中被积极利用。鉴于这些漏洞已发现在野利用，建议客户尽快做好自查及防护。



### Apache ActiveMQ Jolokia 代码执行漏洞安全风险通告

11月29日，奇安信 CERT 监测到 Apache ActiveMQ Jolokia 代码执行漏洞 (CVE-2022-41678)，在 ActiveMQ 中，经过身份验证的远程攻击者可通过 /api/jolokia/ 接口操作 MBean，成功利用此漏洞可导致远程代码执行。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。



### Google Chrome 整数溢出漏洞安全风险通告

11月29日，奇安信 CERT 监测到 Google Chrome 浏览器整数溢出漏洞 (CVE-2023-6345)，在 Chrome 的 Skia 中存在整数溢出，攻击者可以构造恶意站点诱使受害者访问，成功利用将导致安全特性绕过。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。



### I Doc View 在线文档预览系统代码执行漏洞安全风险通告

11月22日，奇安信 CERT 监测到 I Doc View 在线文档预览系统代码执行漏洞 (QVD-2023-45061)。远程未经身份验证的攻击者可通过构造特殊请求，目标应用将下载恶意文件，成功利用此漏洞可能在目标服务器上执行任意代码。I Doc View 在线文档预览是一款在线文档预览系统。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。



## 2023 年漏洞态势简报

2023 年 1 月 1 日至 12 月 15 日期间，奇安信 CERT 共监测到新增漏洞 26750 个，其中有 8068 条敏感信息触发了人工研判。经研判，本年度值得重点关注的漏洞共 638 个，达到奇安信 CERT 发布安全风险通告标准的漏洞共 373 个，并对其中 103 个漏洞进行深度分析。

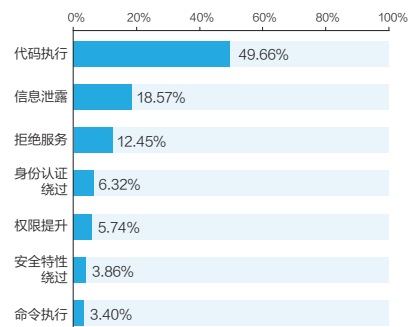
### 1. 漏洞威胁类型占比

代码执行漏洞共 13,224 个，占比为 49.66%；

信息泄露漏洞共 4,944 个，占比为 18.57%；

拒绝服务漏洞共 3,315 个，占比为 12.45%；

身份认证绕过漏洞共 1,683 个，占比为 6.32%；



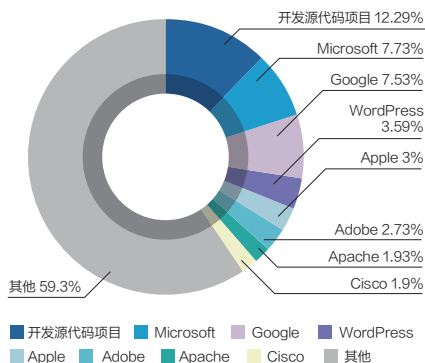
### 2. 漏洞影响厂商占比

开放源代码项目漏洞共 1,458 个，占比为 12.29%；

Microsoft 漏洞共 917 个，占比为 7.73%；

Google 漏洞共 893 个，占比为 7.53%；

WordPress 漏洞共 426 个，占比约 3.59%；



### 3. 漏洞热度排名

根据奇安信 CERT 的监测数据，2023 年监测到的所有漏洞中，总舆论热度榜 TOP10 漏洞如下：

热度排名	漏洞名称	危险等级	修复建议
1	Nacos 身份认证绕过漏洞 (QVD-2023-6271)	高危	升级至 2.2.0.1 或以上版本
2	curl SOCKS5 堆溢出漏洞 (CVE-2023-38545)	高危	升级至 8.4.0 及以上版本
3	Microsoft Word 远程代码执行漏洞 (CVE-2023-21716)	高危	安装补丁
4	PowerShell 远程代码执行漏洞 (CVE-2022-41076)	高危	安装补丁
5	泛微 E-Cology SQL 注入漏洞 (QVD-2023-15672)	高危	升级至 10.58 及以上版本
6	Fortinet FortiOS SSL-VPN 远程代码执行漏洞 (CVE-2023-27997)	高危	升级至安全版本
7	Apache Kafka Connect JNDI 注入漏洞 (CVE-2023-25194)	高危	升级至 3.4.0 及以上版本
8	JumpServer 未授权访问漏洞 (CVE-2023-42442)	高危	升级至安全版本
9	MinIO 信息泄露漏洞 (CVE-2023-28432)	高危	升级至 RELEASE.2023-03-20T20-16-18Z 及以上版本
10	泛微 e-cology9 SQL 注入漏洞 (QVD-2023-5012)	高危	升级至 10.56 及以上版本

在本年度总热度舆论榜前十的漏洞中，热度最高的漏洞为 Nacos 身份认证绕过漏洞 (QVD-2023-6271)。该漏洞是由于开源服务管理平台 Naco 在默认配置下未对 token.secret.key 进行修改，导致远程攻击者可以绕过密钥认证进入后台，造成系统受控等后果。该系统通常部署在内网，用作服务发现及配置管理，历史上存在多个功能特性导致认证绕过、未授权等漏洞，建议升级至最新版本或修改默认密钥，并禁止公网访问，避免给业务带来安全风险。2023 年 3 月 14 日，奇安信 CERT 通过技术手段分析出该漏洞并编写出此漏洞验证 PoC 并对外发布漏洞安全风险通告。

注：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。



## 国内攻防演习 11 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

2023年11月,奇安信Z-TEAM团队共承接攻防演习服务 20 场,其中,行业级攻防演习 1 场,省级攻防演习 2 场,地市级行业攻防演习 3 场,客户自主攻防演习 14 场。

本月承接攻防演习数量与上月对比呈上升趋势(见图 1)。

本月承接的攻防演习涉及政府部委、金融、企业行业较多,此情况较上月承接攻防演习涉及行业范围数据变化显著,政府部委和金融行业攻防演习数量明显增加(见图 2)。

本月攻防演习成果如表 1 所示:

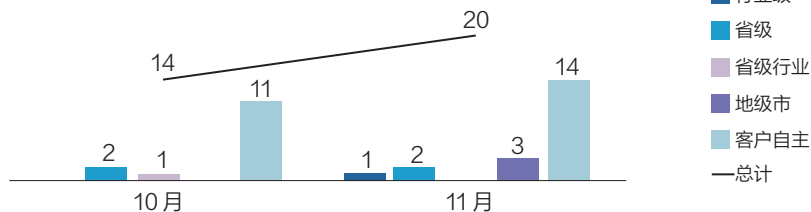


图 1 10-11 月 Z-TEAM 承接攻防演习数量统计

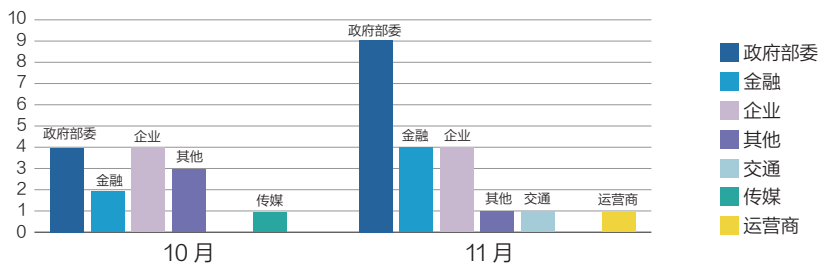


图 2 2023 年攻防演习涉及行业统计

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	58	67	81	117	105	131	718	13210

表 1

## 二、本月任务目标特点

本月攻防演习和评估任务行业比较分散，演习目标覆盖面比较广，涵盖了政府部委、金融、企业、交通、运营商等其他行业。金融市场的稳定性对整个经济体系至关重要。网络攻击可能导致金融系统的瘫痪、交易中断或市场混乱，对整个金融市场产生严重影响。通过构筑坚实的网络安全防护体系，金融机构能够有效降低信息系统遭遇故障或恶意攻击的风险，从而确保金融市场的正常运行和稳定。在本月攻防演习中，金融行业占比为20%（见图3）。

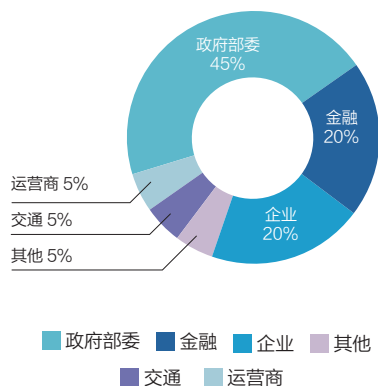


图3 11月攻防演习分布

## 三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果，对本月任务中多个行业的网络目标进行了攻击分析，对不同的行业目标使用不同攻击手段，交通、运营商行业的外网安全防护相对较弱，容易被漏洞扫描利用和弱口令攻击等手段成功突破；政府部委、企业、其他行业的外网安全防护相对较强，但仍需防范漏洞扫描利用和 VPN 仿冒接

入、弱口令等手段的威胁；金融行业的外网安全防护最强，但也不能忽视漏洞利用、钓鱼攻击和隐秘隧道外联等手段带来的风险。本月攻击队突破目标安全防护使用的主要技术手段分布如下（见图4）。

本月攻防演习服务中，攻击队使用攻击手段主要有：漏洞扫描利用、钓鱼攻击、口令爆破、VPN 仿冒接入、隐秘隧道外联等。

整体攻击手段与上月对比，钓鱼攻击和隐秘隧道外联手段利用率基本趋同，漏洞扫描利用手段和 VPN 仿冒接入有明显下降趋势，口令爆破有明显上升趋势（见图5）。

在本月的金融行业攻防演习中，通过深度分析演习数据，我们发现攻击者擅长利用外网资源，寻找薄弱点

进行漏洞扫描和利用，并结合钓鱼攻击纵向突破。一旦纵向突破成功，攻击者便在内网隐蔽实施隐秘隧道外联、VPN 仿冒接入等攻击手段，实现横向拓展和渗透。在攻防演习中，攻击者通常需要巧妙运用多种攻击手段相互配合，才能实现成功渗透和拓展。这种精湛的攻击技巧令人叹为观止，也提醒我们在网络安全防护上必须时刻保持警惕，不断加强防范措施，才能确保金融行业的安全稳定。

## 四、典型攻击手段实现案例

金融行业的稳健发展离不开健壮的信息系统和网络基础设施。网络攻击可能导致系统故障、服务中断，对

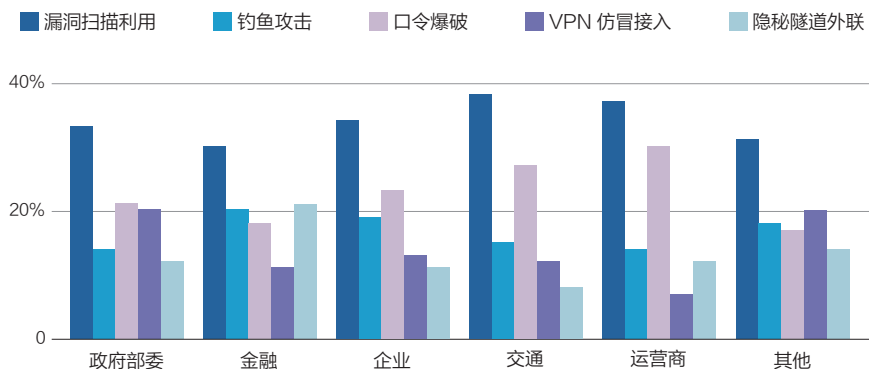


图4 行业攻击手段分布

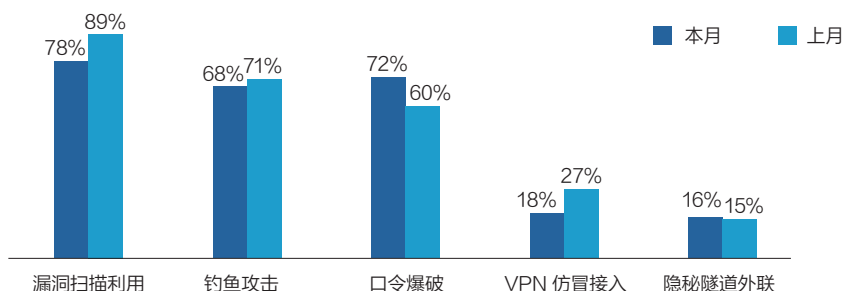


图5 攻击手段对比

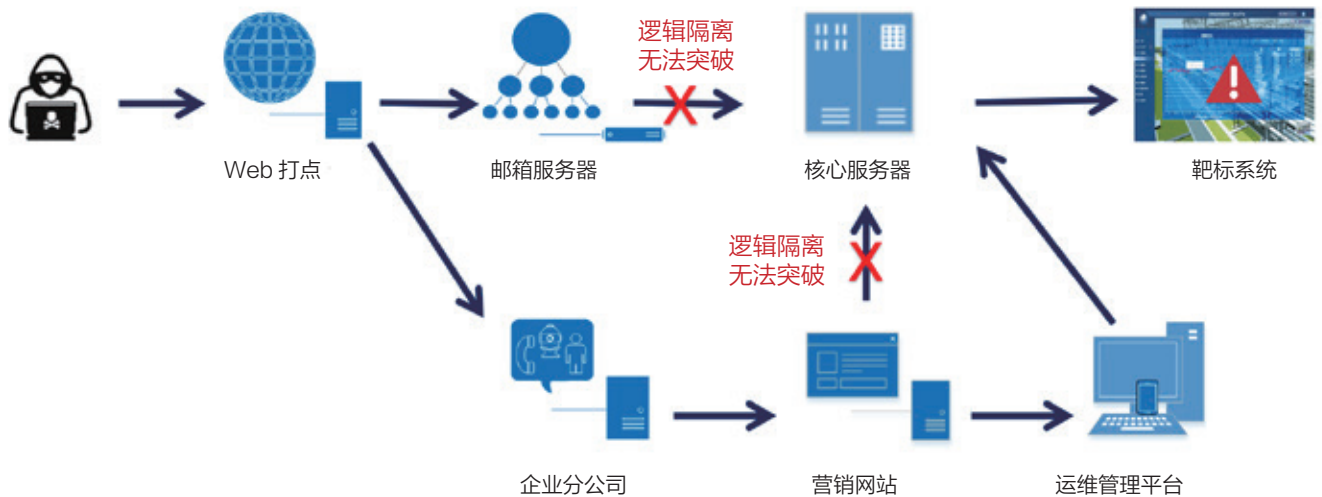


图 6 案例攻击路线图

金融市场和行业发展造成的冲击影响严重。通过加强网络安全，金融机构可以减少，甚至预防这些风险，确保金融系统的稳定运行。

#### 案例：迂回渗透取得突破

在针对某金融企业攻防演练中，前期信息收集后，奇安信攻击队决定铤而走险，利用反序列化漏洞尝试正面突破，这还是第一次在攻击行动中通过反序列化漏洞进行正面突破，喜出望外的是居然成功了。攻击队顺利渗透进该企业的邮箱服务器，随后通过永恒之蓝漏洞利用将邮件服务器作为跳板，尝试进入核心服务器区域，直接拿下靶标系统，但恰恰在这一关键操作时，被客户流量监测设备识别到了，随即 IP 封堵与绕过、WAF 拦截与绕过、Webshell 查杀与免杀，攻击队、防守方之间开展了一场没有硝烟的战争。最终防守方发现并封禁了跳板机和攻击队的域名及 IP，导致该条突破路径被彻底封堵。

针对存在靶标系统的核心资产进

行正面突破，犹如啃一块硬骨头，正面攻击路径中系统漏洞相对较少，防护设备与安全措施相对更加严密，客户高度警觉、严防死守，时时刻刻盯着从外网进来的全部流量，且攻击队极易触发蜜罐等设备，从而被防守方察觉，故攻击难度非常大。

攻击队始终在目标的外围打转，此路困难重重，但时间紧迫，攻击队展开头脑风暴，最终决定兵分两路，一面继续正面寻找其他突破机会，一面寻找该企业的分公司进行迂回攻击。考虑到大多数情况下，分公司都配备了与总公司通信的专用线路，因此，这无疑是一条值得探索的途径。

通过信息搜集，攻击队发现了该企业某分公司的一个营销网站，通过黑盒测试，发现网站存在文件上传漏洞，并利用此漏洞获取到该网站服务器的管理员权限，凭此成功进入业务内网，并希望通过该分公司跳板进入目标公司的内网，但在此尝试中被 ACL 限制，导致无法连通。



但是攻击队没有放弃，希望能够在在这条路上再找到一些可利用的信息，功夫不负有心人，通过该分公司的运维管理平台，攻击队成功进入该分公司的核心服务器区，发现此处与总公司的核心区域可直接通信，并由此攻击路径成功拿下系统靶标。

## 五、安全加固建议

### 1. 案例剖析

随着数字化转型和金融科技创新的不断深化，金融行业客户的信息化资产数量和复杂性前所未有的增加，而暴露在互联网侧的资产更是直接面向外部攻击者的威胁，这就导致互联网资产暴露面成为攻防对抗中的主战场，防御的重点在于比攻击者更快更全更准地发现薄弱环节，更早地响应。案例中攻击者利用对互联网暴露面的梳理、脆弱性识别以及利用，形成互联网资产攻击面，从而突破互联网边界，成功获取靶标系统权限。

案例暴露问题：对于互联网资产

攻击面没有进行体系化管理，导致互联网侧资产存在风险隐患。

### 2. 防护策略

结合案例暴露出的安全隐患，需从安全管理和技术防护两方面提升互联网资产攻击面的管理能力：

- 安全管理上，建立或完善互联网资产攻击面管理体系，包括资产管理规范、资产变更流程及资产脆弱性管理要求等；

- 技术防护上，借助平台 + 服务，开展互联网资产攻击面管理，包括但不限于：

- 1) 建立网络资产攻击面管理 (CAASM) 平台，通过聚合 IT 资产、配置、漏洞、补丁、漏洞情报等数据，持续监控信息系统的资产状态，进行多维度数据碰撞分析、关联分析，发现资产安全问题，驱动资产发现、配置采集、风险持续监测和资产安全整改等安全运行工作。

- 2) 常态化互联网资产发现，基于 IP 或域名，采用 WEB 扫描技术、操作系统探测技术、端口的探测技术、

服务探测技术、WEB 爬虫技术等各类探测技术，对客户信息系统内的主机 / 服务器、安全设备、网络设备、工控设备、WEB 应用、中间件、数据库、邮件系统和 DNS 系统等进行主动发现，全面、精准解决互联网资产边界盲区问题。

- 3) 常态化应用系统安全检测，通过渗透测试及众测的方式，对全量应用系统的安全做深入的探测，发现系统最脆弱的环节，充分挖掘业务系统可能被攻击者利用的安全漏洞。

网络安全的本质在对抗，攻击面管理是攻防实战和对抗的下的的一种主动防御的思想与理念，奇安信《网络资产攻击面管理解决方案》，是站在攻击者的视角来不断审视与管理资产和薄弱环节的持续过程。致力于打通“资配漏补”安全运行流程与 IT 服务流程，形成跨团队、跨组织的协同运营机制，将传统事件驱动的、临时抱佛脚资产安全运营模式转变为以数据驱动的常态化运行模式，实现系统资产安全控制措施落地。安

# 十大技术趋势

2024



网络威胁、安全态势，以及攻防对抗力量的变化，驱动网络安全技术持续创新。奇安信认为，2024 年需要关注 10 大技术趋势，积极拥抱技术创新，才能更好地适应应对网络威胁和保障数字经济稳定发展的需要。



# 奇安信发布 2024 十大网络安全技术趋势

2023 年我国经济恢复回升向好。2024 年进入实施“十四五”规划的关键一年。多家国际金融机构普遍预计，新兴市场将在 2024 年重新迎来较快增长，并认为其加速复苏的重要动力就是中国经济的发展。

12 月 11 日至 12 日召开的中央经济工作会议再次提出发展“数字经济”，至此已连续五年在中央经济工作会议中被提及。今年会议还大篇幅提及发展数字经济的各方面，包括加快推动人工智能发展、广泛运用数智技术、大力发展数字消费、支持新型基础设施、拓展数字贸易、认真解决数据跨境流动等，凸显出数字化持续深化的趋势与潮流，也给网络安全行业提出了更高要求与责任。

2023 年地缘政治冲突令网络空间紧张态势加剧，具有国家背景的网络攻击持续升级；同时，以“经济利益”为目的的勒索攻击持续高发。全球多家云服务商发生服务中断事件，凸显出数字基础设施的可靠性挑战。现象级技术生成式人工智能正在改变网络攻防的格局。

网络威胁、安全态势，以及攻防对抗力量的变化，驱动网络安全技术持续创新。奇安信认为，才能更好地适应应对网络威胁和保障数字经济稳定发展的需要。

## 趋势一

### 生成式 AI 重塑安全行业， 利用与防护成热点

在 Gartner 发布的 2024 年十大战略技术趋势中，生成式 AI 与大模型当仁不让占据了第一名的位置。Gartner 预测，生成式 AI 或将迎来全民化时代，到 2026 年，将有超过 80% 的企业使用生成式 AI 的 API 或模型，或在生产环境中部署支持生成式 AI 的应用，而在 2023 年年初这一比例还不到 5%。

Gartner 同时将“AI 信任、风险和安全管理”摆在了第二的位置，可见，人工智能给网络安全带来的将是颠覆和机遇并存。生成式人工智能技术如何应用到安全攻防领域，以及大模型带来的安全防护问题，成为行业热点。

展望 2024 年，生成式 AI 将在几个方面持续发展，重塑安全行业。

**首先是人工智能驱动安全运营与威胁分析成为趋势。**

当前，企业网络安全普遍面临着

网络威胁、安全态势，以及攻防对抗力量的变化，  
驱动网络安全技术持续创新。

告警疲劳、效率瓶颈、专家稀缺等三大问题，尤其是生成式 AI 如果被黑客滥用用在网络攻击领域，会给防护带来更加严峻的挑战。因此，将人工智能和机器学习集成到网络安全实践中变得越来越重要。

到 2024 年，预计人工智能驱动的安全运营与威胁分析将进一步发展，尤其是生成式人工智能技术将大量应用于智能威胁分析和响应领域。通过对网络流量、安全告警等大量数据进行深入 & 实时的安全分析，可以协助安全专家甄选出真实有效的威胁告警，并生成相应的响应策略，从而大大降低网络安全运营难度，提升安全运营效率，提高安全运营能力水平，让网络威胁处置更快一步。

**其次是针对人工智能带来安全风险的防范技术，将进一步发展。**

生成式 AI 风靡全球的同时，其带来的数据安全与隐私风险也受到业内的强烈关切。据统计，使用 ChatGPT 的员工中大多数会泄露数据，其中 11% 的数据为企业商业机密。Gartner 也认为，AI 的全民化使得对 AI 信任、风险和安全管理（AI TRISM）的需求变得更加迫切和明确。在没有护栏的情况下，AI 模型可能会迅速产生脱离控制的多重负面效应，抵消 AI 所带来的一切正面绩效和社会收益。

2024 年，随着 AI 的普及，越来越多企业需要更先进的 AI 风险与安全工具，全面掌控大模型的使用情况；依托领先的大模型风险发现能力及风险检测库，可以检测大模型应用自身安全风险、服务商风险及大模型使用过程中产生的数据泄露风险、数据跨境风险、服务风险、用户及设备风险、业务安全风险等多维度安全风险，帮助企业及时感知大模型风险情况。因此，AI 大模型风险管理将成为行业



创新热点。

**第三，打击人工智能网络诈骗的鉴伪、取证等技术，将进一步发展。**

近年来，人工智能越来越成为网络诈骗、违法犯罪的工具，严重威胁公众利益。AI 诈骗是利用 AI 技术模仿、伪造他人的声音、面孔、视频等信息，进行欺骗、敲诈、勒索等犯罪活动，令人防不胜防，并给鉴别取证带来了许多困难。

只有魔法才能打败魔法，2024 年针对 AI 网络诈骗和违法犯罪的防御技术进一步发展，包括深度鉴伪、智能鉴别取证等，可以对海量涉网违法犯罪行为进行不断学习和训练，为识别网络诈骗提供工具，为电子取证提供技术支持。

IDC 预测，2026 年中国 AI 大模型市场规模将达到 211 亿美元，人工智能将进入大规模落地应用关键期。生成式 AI 对网络安全来是一把双刃剑：一方面，它将带来新的安全威胁，另一方面，它可以帮助企业安全体系提高威胁检测和响应能力，提高预测能力和安全运营效率。可以预见，2024 年，围绕生成式 AI 的“攻防博弈”，将贯穿始终，并推动行业加速升级。

## 趋势二

### 数据要素撬动万亿市场，数据安全流通成技术趋势

回顾整个 2023 年，数据要素成为科技行业的高频热词。从年初的十六部门促进数据安全产业发展《指导意见》，到各地开通公共数据授权运营，“数据二十条”加速探索落地，以及国家数据局正式挂牌等，数据要素、数据流通交易、数据安全等无疑是贯穿全年的社会关注焦点。

从长远看，数据要素将为下一个 30 年黄金发展期打开一扇战略性的大门，国家发展改革委价格监测中心副主任王建冬曾表示，数据资产化催生的相关市场潜在规模有可能达到 10 万亿元级。

展望即将来到的 2024 年，至少有四大趋势，对数据要素高质量发展产生实质性的影响。

**首先是数据要素基础制度完善，从顶层设计到细化落地，推动数据要素高质量发展。**

“数据二十条”、数字中国建设整体布局规划是数据要素基础制度，数据要素全流程合规与监管体系的顶层设计，企业数据资源相关会计处理暂行规定推动了数据资产入表的关键政策，也是数据要素资本化的重要的一步；各地方也在陆续推出数据要素市场化改革规范，数据基础制度综合改革先行先试，如：北京“数据二十条”，北京数据基础制度先行区启动等。

**其次，构建多层次数据要素流通体系是未来的大趋势。**

数据要素流通的路径多样化趋势明显，从数据的共享开放、开发利用到公共数据授权运营、数据交易、数据信托等，构建多层次数据要素流通体系是未来的大趋势，也是持续释放数据要素价值动力源。

**第三，多层次、全生态的安全合规，是数据要素高质量发展的基础和保障。**

只有构建数据要素生态，促进数据合规、高效的流通使用，才能充分赋能实体经济。数据要素生态需要多层次的安全和合规保障体系，其中底层主要是数据要素流通基础设施，如可信计算环境、传输网络、云平台、数据平台等，需要从端（服务器、终端主机等）、网、云、数等层面构筑对应的纵深安全防御体系；中间层主要是数据要素流通平台，如数据共享平台、开放平台、授权运营平台、交易平台、数据专区，需要进行隔离交换、API安全网关、WAAP、数据脱敏、数据集保护、API保护等安全保障；而最上层是数据要素流通活动，需要围绕数据供给、流通、使用等环节，需要匹配去标识化、分级分类、数据空间、可信计算、数据沙箱等安全技术，确保流通中的全过程安全与合规。

**第四，数据安全合规新技术需要与新场景、新模式等做深度融合。**

2023全球数商大会上提出的“数据要素×”行动，给技术型的数商企业带来了广阔机会。随着数据要素与其他要素的结合，新产业、新业态、新模式、新应用、新治理等不断被催生出来，而数商企业在开发数据产品以及数据产品上架时，就面临着各种合规和安全挑战。这意味着数据安全合规技术需要不断创新，如隐私计算、数据空间、区块链等，能够与新业态、新场景、新模式等实现深度融合，适应数字基础设施建设和“数据要素×”行动的发展潮流，保障数字经济的合规有序发展。

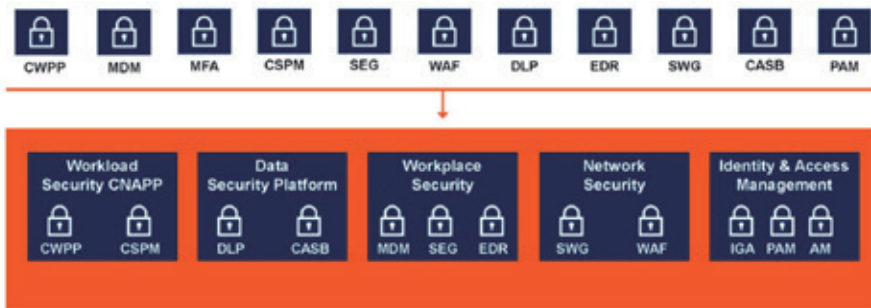
随着国家数据局的正式挂牌，预计未来相关顶层设计指导文件也将陆续出台。同时，数据资产入表即将在2024年1月1日正式施行，为数据要素发展提供了更加完善的政策配套。预计2024年数据要素将进入政策密集推动期，相关数据流通交易、数据安全保障等市场将掀起新一轮增长浪潮。

## 趋势三

### 复杂性推动网络安全供应商与平台走向整合

复杂性成为网络安全的大敌。政企攻击面持续扩大，网络威胁日趋严峻，导致网络安全工具数量激增，对

数据安全合规技术需要不断创新，  
如隐私计算、数据空间、区块链等，  
能够与新业态、新场景、新模式等实现深度融合。



## 同时推动供应商与工具整合，才能让安全运营更加高效

推动供应商整合，并不意味着从单一供应商采购依然孤立的单点安全产品。只有当组织同时考虑供应商整合和工具整合时，这种整合协同才会有效。如果让安全运营人员依然去管理分散、集成度差的工具，单一整合供应商就没有什么价值。

简言之，没有集成平台的供应商整合或不同工具的紧密集成，并不会让网络安全运营变得更轻松。它可能会提高采购的效率，但同时会增加开支，降低安全操作的效率，反而会使企业面临更大的网络攻击风险。

目前，组织安全团队面临着管理孤立漏洞监控工具，应付过载警告，以及被动式安全响应策略的挑战。为了提高安全性的有效性和效率，许多企业正在尝试合并单点产品，大型集成自动化平台是实现这一目标的手段。通过整合供应商和单点产品并构建集成的网络安全平台，对其网络安全战略采取更全面的方法，可以提供组织急需的整体可见性、加强威胁识别和响应的自动化能力，在日常安全运营中提升效率，对企业提供更好的保护，并提高组织的合规水平。

值得注意的是，网络安全整合不是一次性的项目，而是一个持续的过程。因此，将供应商和产品整合到网络安全平台中并不是一朝一夕的事。第一步是致力推动构建集成平台，并与在产品开发设计时考虑到集成和自动化的供应商合作。理想情况下，组织应该寻找方法来整合两个或三个集成平台，而不是数十个孤立的产品。

整合过程可以从端点、云或网络安全整合平台开始。也还可以从网络安全运营中心的整合开始，目标是减少到只有两个或三个平台。

安全运营人员来说，理解、协调和统一众多的安全工具就充满挑战。推动安全供应商整合和安全工具平台化整合成为提升安全运营效率的现实需求。

Gartner 发布的《2024 年及未来中国网络安全七大趋势》认为，中国企业机构希望降低复杂性、简化运营并提高员工效率。精简供应商数量之后，企业机构可利用数量更少的产品降低运营复杂性、提升员工效率、实现更广泛的集成，并获得更多类型的功能。

对于组织的安全主管来说，不应部署新的单点产品，而应考虑从供应商采购技术，作为平台的一部分协同工作。

### 更多供应商意味着更多复杂性

随着新型攻击的出现，安全团队急于保护其组织免受新威胁的侵害，第一本能是采用任何“最好”的安全技术来防范最新的威胁，部署旨在解决特定攻击向量或增强特定平台安全性的单点安全产品，无论这一产品是来自现有供应商还是新供应商。

当安全基础设施由不同供应商的孤立产品混合而成时，就会带来新的挑战。例如，不同供应商的产品难以

协同工作，就会出现安全漏洞，使组织成为攻击的目标。面对过多的单点安全产品，安全团队面临信息过载的问题。每个安全工具独立运行，生成自己的警报，很难共享信息和有效协调团队对潜在安全事件进行响应，从而导致容易错过网络攻击的基本指标。

Gartner 调查显示，75% 的组织正寻求整合所使用的网络安全供应商的数量。

在当前的宏观经济环境下，组织寻求整合并与数量较少的供应商合作，这是可以理解的。不仅可以减少潜在成本并使供应商关系更易于管理，还可获得更有利的议价地位。

正如 Gartner 所指出的，供应商整合可能导致风险集中，但这一顾虑并不能削弱组织对供应商整合和集成的需求。整合和减少供应商有助于简化组织的业务流程，由于接触的供应商更少，可以获得一站式采购流程，不仅可以提高效率，还可能会降低总体成本。

需要指出的是，成本或采购因素并不是整合的主要驱动力。65% 的受访组织希望通过整合改善其整体风险状况。只有 29% 的受访者预计支出会减少。

## 趋势四

### 2024 零信任：持续演进，持续向前

2023 年零信任市场持续火热，少了一些泡沫，多了一些务实，正在逐步褪去浮华，聚焦场景和价值。

从全球市场情况来看，零信任已经成为现代企业的安全架构蓝图。Forrester 2022 年安全调查显示，88% 的安全负责人表示，他们的高层领导已承诺推动企业组织采用零信任安全战略。在零信任架构体系中，相对产品标准化的 ZTNA 市场份额也在不断攀升，据 Gartner 数据显示，在 2021 年至 2022 年间，中国 ZTNA 市场的终端用户支出增长了 86%，并预测在 2022 年至 2023 年间将增长 54%。

在中国，许多行业代表性企业也已经将“零信任”作为重要的网络安全体系建设方向，列入企业长远规划。具体表现在，零信任能力供应不断丰富，产品联动能力正在同步提升。例

如，目前，国内有近 50 家企业提供零信任集成产品，超半数企业的零信任产品支持与客户已有的安全运营中心、态势感知、威胁情报等安全分析系统联动，占比 53.6%。零信任和终端安全的联动也在持续深入。

不难发现，企业安全负责人已经不会再问“什么是零信任”的问题，转而专注于“怎么实现零信任”的问题。当然，大多数企业选择了远程访问作为实现零信任的第一步，零信任的产品也主要集中在 ZTNA 领域，应用场景略微不足，价值体现以“可信接入”为主。

2024 年，基于客户已经构建的零信任能力基础，未来零信任的应用场景和价值呈现会进一步深化，场景方面将从单一的远程接入场景进化到全面的数字化工作场景，在价值方面，将进一步凸显零信任在数据安全方面的价值。

**首先，未来零信任将兼顾提升数字化工作生产力和保护企业数据资产安全。**

业务发展和安全需要相辅相成、协同并进。当基础的远程接入问题已



经得到有效的解决后，如何持续提升企业面向数字化作业态的生产力同时保护企业数据资产安全，将是未来持续关注的问题。甲方将需要一套基于零信任理念的一体化工作系统，真正构建身份可信、行为合规，实现数据安全保护、工作敏捷开展，完善数字化工作基础设施。

**其次，零信任在数据安全方面的价值呈现也将变得更迫切。**

零信任在诞生之初，就摒弃了一些相对滞后、固化的安全思维，强调以数据保护为中心去思考安全风险及安全机制的建立，这使得其在数据安全方面具有先天优势。因此，零信任架构本来就是以数据资产为中心的安全体系，数据保护一直是零信任的核心目标。展望 2024 年，随着数据安全受到越来越多客户组织的关注与重视，如何实现面向数据的动态策略管控是基于零信任构建数据安全能力的关键。

**最后，零信任将提供更高效的集中管理功能并提高用户体验。**

许多供应商都声称提供集中管理的功能，但供应商们很少提供覆盖多个零信任组件的统一用户界面。Forrester 认为，多个零信任组建的合并，不仅可以创建统一的控制平面，还可以提供原生工具和服务来帮助、训练并提高对网络安全意识，并提升用户体验。从趋势来看，集成化、统一化、协同化的用户

界面，可创造更轻便、一站式工作体验，实现业务访问简便易用，业务协同高效便捷，跨终端、跨系统实现无缝兼容，最终让企业的数字化工作拥抱轻简、效率倍增。

总之，零信任的核心价值是可信访问和数据安全，其落地关键是和业务场景的聚合，当然，这也是零信任落地实践的深水区，2024 年，供给双方都会往这个方向稳步迈进。

## 趋势五

### 云原生安全向全生命周期扩展

云原生产业联盟(CNIA)在《2020 年云原生发展白皮书》指出，2019 年中国云原生市场规模已达 350.2 亿元。云原生市场的快速发展有赖于其相对传统云技术的重要优势。从技术特征来看，云原生拥有极致的弹性能力、服务自治、故障自愈能力和大规模可复制能力；从应用价值方面来看，云原生异构资源标准化，加速了数字基础设施解放生产力，提升业务应用的迭代速度，在赋能业务创新方面有重要价值；从产业效用来看，云原生极大地释放了云的红利，成为驱动业务的重要引擎。

随着云计算大步迈向“云原生”，云上快速迭代、弹性伸缩、海量数据处理等特征要求安全防护体系相应升级，为动态变化、复杂多元的运行环境提供有效的安全防护。为此，面向云的安全也在悄然发生变革。越来越多的云基础设施从虚拟机、云主机转变为容器，越来越多的安全需求从云旁挂安全转向云原生安全，传统开发、运维、安全分离的状态转向 DevSecOps 体系流程。

为什么会有这样的转变？这主要是因为，在以前的云计算时代，安全和云平台的结合不算紧密，大部分以安全资源池这种外挂形式来实现云安全，而云原生安全需要安全能力和云原生平台紧密结合，真正成为内生安全，这将是云安全的巨大挑战和机遇。

从大量实践中可以看出，云原生安全主要体现出三方面的价值：

全链路风险可视可控。将安全和合规要求贯穿软件生产和服务全链路，及时扫描检查关键环节，避免后期处置造成被动，最大程度降低整体风险管控成本。

基础设施安全运营闭环高效。安全防护功能融合化，可以实现异常事件响应处置流程的闭环管理；策略执行自动化，可减少对安全运营人员的依赖，降低误操作概率；同时，自动阻断机制可以为应对攻击和修复争取更充分的时间。

云上客户资产全面保障。帮助客户全面、实时监测各类数据资产；在身份验证、配置管理、应用运行时监控、数据安全保护等方面提供多元化、灵活调用的安全服务。

不过，云原生安全正面临来自监管和实战的双重挑战，这就对云原生使用场景下的安全防护能力提出了新的需求。目前云原生环境的安全风险

2024 年，

基于客户已经构建的零信任能力基础，

未来零信任的应用场景和价值呈现会进一步深化。

主要存在于容器环境的风险暴露面增加、业务开发运行模式的变化带来的安全挑战、云原生应用全流程的供应链风险、全流量安全检测存在困难等。

基于云原生环境目前存在的风险、痛点和需求，需要设计一整套云原生安全防护体系和运营体系，确保云原生应用全生命周期的安全可靠，这就是全生命周期云原生安全的由来。

未来一段时间内，全生命周期的云原生安全服务，将更好地适应多云架构，帮助客户构建覆盖混合架构、全链路、动态精准的安全防护体系。其核心包括：建立向开发左移的云原生安全体系；提供面向云原生基础设施的云原生安全防护能力；提供与云原生运行环境深入融合的运行安全防护能力；构建覆盖开发、测试与运行阶段的一体化安全运营平台等若干方向。

## 趋势六 安全运营走向知识驱动， 降本增效加速实质落地

企业平均每年面临 44 起重大网络安全事件，但检测和响应较慢，有 3/4 的企业需要六个月或更长时间才能检测和响应事件。在过去五年中，已知的网络攻击数量增加了约 75%。

……

安永发布的《2023 全球网络安全领导力洞察研究》显示，尽管网络攻击威胁不断增加，对网络安全方面的投资也在持续增长，但只有 1/5 的首席信息安全官（CISO）和高管团队认为他们的网络安全措施在目前是有效的，并为未来做好了充分的准备。更多的企业组织对无处不在的网络攻击依然是准备不足，企业的安全运营之路依

未来，安全运营中心将更广泛的集成 AI 功能，  
依托 AI 大模型、知识库等，  
为运营人员提供专业的安全知识问答，  
辅助研判、辅助处置，大幅提升运营效率。

然任重而道远。

Gartner 指出，构建安全运营中心（SoC）是一个永无止境的旅程，因为需求不断变化。它需要持续的增长和分析来确保 SoC 的性能不会下降并且其成本不会超出预算。展望 2024 年，降本增效的紧迫性将更加强烈，作为一个知识高度密集领域，安全运营未来呈现以下三大趋势。

首先是从数据驱动走向知识驱动。

长时间以来，数据一直是驱动安全运营的核心，它强调数据、系统和人联动的安全运营，通过将数据的安全价值赋能设备和人，驱动设备协同联动的同时，让人更智能，进而全方位提升防御内外部安全威胁和业务风险的能力。

时至今日，由于攻防对抗的不断升级和变化，仅仅依靠数据和技术平台已经不够，没有专业的安全知识积累，就无从谈起检测、研判、调查、响应等。因此，安全运营逐渐从数据驱动迈向了数据 + 知识双驱动。

知识驱动安全运营的核心，是依托强大的行业专家系统，以及大量经过实战检验的领域知识、专业经验，实现由专家经验模型和人工智能模型共同驱动。通过专业知识的赋能，SoC 在对于海量告警的自动化分析和处理，



解除分析师告警疲劳，快速聚焦高价值威胁，以及专业的安全知识问答，辅助研判等具有显著优势。

### 其次是从关注告警到关注事件。

处理海量告警是安全运营的基础，但要保证企业的“零事故”“零通报”，还需要依赖于事件调查与响应。这就如同公安部门不仅要接受报警、调查和发现线索，还需要完整的案件侦办和破获。

从关注告警到关注事件，是安全运营自动化跨越的一大步。未来的安全运营中心（SoC）需要将相关联告警自动汇聚形成完整事件卷宗，自动补充上下文证据，自动映射攻击者战术和技术，自动解读攻击者意图、自动识别关键攻击痕迹、自动评估影响面并计算处置对象，即使是复杂事件，也能轻松看懂事件的来龙去脉和完整信息，最终完成安全事件的快速闭环。

### 最后是从人员堆砌到 AI 提效。

国外安全机构的一项调查报告显示，有超过八成的安全运营团队正在遭受告警疲劳的折磨。尤其是随着生

成式 AI 的普及，如果被黑客用滥用在网络攻击领域，会给防护带来更加严峻的挑战，告警疲劳现象会更加严重，企业的运营人员短缺愈发矛盾。

未来，安全运营中心将更广泛的集成 AI 功能，依托 AI 大模型、知识库等，为运营人员提供专业的安全知识问答，辅助研判、辅助处置，大幅提升运营效率，缓解分析师压力，让响应流程有章可循，实现安全事件的快速闭环。

可以预见，通过 AI 的赋能，安全运营中心很大程度上解决了工作难度大、重复性高、人力不足、专业人才匮乏，专业知识要求高等业界难题，实现真正的降本增效。

## 趋势七

### 攻击面持续扩大，持续威胁暴露管理成安全建设重点

研究机构 Gartner 公司发布的

《2024 年十大顶级战略技术趋势》报告，持续威胁暴露管理（CTEM）位列第二。与传统的网络安全战略不同，持续威胁暴露管理（CTEM）的目的是从攻击者的视角来管理企业暴露风险面。

### 攻击面持续扩大，推动威胁暴露管理需求

随着数字化转型的深化，新的系统与应用快速增加，组织增加更多面向互联网的资产，导致暴露面和攻击面以指数级的速度持续扩大：据哈佛商业评论的报告，组织通常使用 130 个 SaaS 应用，高于五年前的 16 个应用；此外，网络组织的攻击手段与能力持续提升，网络攻击者已在使用自动化工具来发现资产、识别漏洞并发起攻击，组织面临应对数字资产风险的严峻挑战。

面对不断扩大的攻击面和持续恶化的安全形势，目前很多机构的安全建设重心却仍聚焦安全事件的快速响应和处置上，但这种期望通过提升安全响应能力，减少网络威胁和降低安全事件影响的被动策略，既不能降低企业面对的安全风险，也不能减少网络攻击事件的发生。

因此，各类组织除了增加被监管部门通报的压力，甚至还面临遭受入侵和数据泄露的高危风险。

在此背景下，Gartner 于 2022 年提出持续威胁暴露管理（CTEM）。可以说，威胁暴露管理源于对漏洞管理日益增长的挫败感，是对传统补丁管理缺点的回应，以及满足主动进行风险管理、提升网络弹性的需求。

作为集成的安全策略，持续威胁暴露管理（CTEM）整合了网络安全多个要素，包括攻击面管理（ASM）、基于风险的漏洞管理（RBVM）、第三



方风险管理 (TPRM)、网络威胁情报和安全评级。其中，暴露面与攻击面管理是其主要要素，成为网络安全的重要支柱和首道防线。

威胁暴露管理推动组织网络安全工作的重心从事件响应转向主动威胁管理。因此，CTEM 关注广泛的未知威胁，通过持续监控和管理其面临的潜在攻击，从而增强整体安全防御能力。

奇安信认为，作为威胁暴露管理主要环节，目前攻击面管理主要存在四个明显问题：一是资产梳理不清晰、缺乏统一的管理视图；二是暴露面无法实时全面监测；三是攻击面难以全面发现；四是资产安全管理的意识有待建立。

### CTEM 成未来五年安全管理趋势

Gartner 将持续暴露管理 (CTEM) 称为“务实和系统持续调整网络安全优先级的方法”。通过采用这种积极主动、具有成本效益的方法，资源有限的团队可以专注于对其业务至关重要的风险。

这种以动态主动防御思路去解决安全问题，向网络弹性的范式转变可以降低数据泄露、身份盗窃和数据泄露的风险，同时确保业务连续性和信息安全。Gartner 认为，到 2026 年，根据 CTEM 计划进行安全投资的组织，其遭受的入侵和数据泄露事件将减少三分之二。

业内人士预计，2024 年持续暴露管理 (CTEM) 将广泛集成到业务实践中。为此需要将 CTEM 与目前安全管理保持一致，将其视为整个组织安全策略的组成部分，需要结合管理者 and 攻击者不同视角，利用多源资产数据，实现高效的资产信息安全运营。

因此，奇安信认为，作为 CTEM

主要环节的攻击面管理，政企用户在推进建设时可参考如下步骤：一是重视攻击面管理的价值；二是确定攻击面管理目标，建立相关运营流程；三是确定攻击面管理能力建设顺序；四是建设攻击面管理核心能力；五是开展攻击面运营服务。

最终实现有效提升资产可见性，最小化资产暴露面，持续发现攻击面，并提供高效的收敛方案，能指导用户收敛攻击面，快速应急响应等诸多能力。

Gartner 将持续暴露管理 (CTEM) 分为 Scoping (资产范围界定)、Discovery (资产和风险发现)、Prioritization (风险优先级排序)、Validation (风险验证)、Mobilization (修复动员) 等 5 个阶段。

持续暴露管理 (CTEM) 以动态主动防御的思路去解决安全问题，将会成为是未来五年的企业安全管理的



趋势，尽早进行规划，将会有助于政企消除风险和提升网络弹性。

## 趋势八

### 专用 SASE，助力政府企业网络安全架构演进

在信息数字化转型和业务上云的大趋势下，越来越多的政府企业面临多云互通难、边缘接入能力弱、多分支安全管理难、数据防泄露难等问题，网络和安全融合产品 SASE 以简洁统一的服务形式能够为政府企业解决这些问题，满足办公环境随时随地安全访问互联网和应用的要求。据 Gartner 统计显示，2022 年 SASE 全球市场规模已达到 66 亿美元，未来五年市场规模将以 36% 的复合年增长率高速增长，预计到 2025 年，全球 SASE 市场规模将达到 150 亿美元，亚太区市场规模将达到 23 亿美元，将有 80% 的企业将会制定明确的战略采用 SASE 架构。

SASE 架构将“网络 + 安全”相融合，通过统一安全管理和运营服务

平台，集成 SD-WAN、FWaaS、SWG、ZTNA 等多种安全防护能力，构筑“云网边缘”安全防护体系。当前业内大多数 SASE 服务供应商采用的方案是将企业的业务访问流量牵引到供应商提供的安全公有云上，在供应商提供的安全云里进行网络优化和各种安全检测、防御。这种将内部业务访问的流量牵引到公有云上的方式，有助于企业客户方便快捷的接入 SASE 安全访问服务，但是对于一些重点单位，如政府、央企及业务数据敏感的企业而言，还是会考虑到企业的业务隐私、数据安全等因素，对采用 SASE 架构持观望态度。换个角度，如果不考虑把安全能力集中在公有云上执行，而是将企业业务流量及安全数据相关的功能都保留在客户的自治可控环境中，即在企业级私有数据中心建设专用 SASE，就可以避免以上公有 SASE 存在的问题。

专用 SASE 不是一系列独立的技术或功能，而是集成式安全和网络融合服务平台，SASE 服务平台支持对专用 POP 安全资源池的安全能力的编排、安全策略统一管理，状态监测和运行管理；支持对专用 POP 安全资源

池的流量进行统一监测和安全日志收集，在满足监管部门日志留存合规要求的同时，还能有效对出入流量的安全告警数据进行挖掘并分析，从而实现深度运营，及时分析和处置安全风险，并针对安全事件进行通告。专有 SASE 成为主流应用技术，可以帮助信息化管理团队减轻安全和网络运行压力，已成为客户基础设施的一部分。

Q-SASE 为奇安信推出的 SASE 架构的解决方案，针对大中型企业或者政府机构多分支、移动办公场景下的互联网访问、私有云和公有云应用访问的统一安全防护水平、统一安全访问策略、统一安全管理运营的需求，以 SDN（软件定义网络）和 SDS（软件定义安全）为技术体系基础，为客户提供分布式部署的安全资源池防护能力，支持以上安全能力按需订阅、弹性扩容、多租户分权分域、可视化监控等功能，并在多个大中型央企、民营企业、政府机构得以实践落地。

随着人工智能、大数据分析等技术发展，SASE 作为数字基础设施一部分，出现了新的发展趋势，包括：

- 1) 建立云端大数据分析平台，支持 SASE 访问数据的智能分析，做到资产、安全威胁深度可视可预警；
- 2) 将 AI 用于安全事件异常检测及分类，加快检测速度，减少误报，实现自动化运营；
- 3) 通过访问控制、数据加密、网络防御等功能，保护应用系统和数据免受恶意攻击和泄露，提升应用访问的安全性；
- 4) 新建或扩容资产运营平台，做好网络资产、终端资产、云上资产等全量资产发现和风险发现，利用多个自动化技术组合实现威胁持续性监测，让安全分析更全面。

威胁暴露管理源于对漏洞管理日益增长的挫败感，是对传统补丁管理缺点的回应，以及满足主动进行风险管理、提升网络弹性的需求。

## 趋势九

### 身份凭证泄露成重要攻击途径，无密码验证技术迎来拐点

密码目前依然是安全链的薄弱环节，往往是数据泄露和网络攻击的根本原因。根据美国运营商威瑞森《2022年数据泄露调查报告》，81%与黑客有关的数据泄露事件都归因于身份窃取和登录凭证不够强大。

生成式人工智能的引入将网络钓鱼攻击推向新的高度，可以大幅度提高钓鱼邮件的点击率；与此同时，借助AI的加持，攻击者可以实施社工攻击，轻松绕过身份验证措施。

据访问管理公司 SecureAuth 的调查，当前最具代表性的访问管理和身份验证形式仍然是传统的多重身份验证(80%)，其次是单点登录(79%)和双因素身份验证(60%)。

无密码身份验证技术进入拐点，包括大型银行和零售商在内的大企业正在推进部署。在过去三年，埃森哲公司已将超过60万名员工转为无密码身份验证方式。过去埃森哲要求员工每75天重置一次密码，给员工制造了不少的混乱和麻烦。在该公司将关键资产转移到云端后，就开始转向了无密码验证。

无密码身份验证是一种能够保护企业免受身份验证攻击影响的解决方案，它消除了用户摩擦的根本原因和安全体系中最薄弱的环节，是网络安全领域最重要的范式转变之一。

无密码身份验证抹掉了记住、存储和传输密码及在设置或重置密码时遵守复杂规则的挑战，消除了从凭证信息获取到网络钓鱼攻击等一长串攻击媒介，提供了一个没有密码的世界，



与传统的PIN码、密码短语和密码相比，具有更高的安全性和更好的用户体验。

这项技术在行业内的势头正在不断增强。2022年以来，谷歌、苹果和微软陆续宣布支持FIDO联盟和W3C联盟的无密码身份验证标准，逐步在所有主流平台上实现无密码登录体验。Transmit Security、Beyond Identity、SecureW2、Descope等初创公司获得了千万乃至数亿美元的巨额融资。据市场研究机构MarketsandMarkets预测，到2027年，无密码身份验证市场规模将达212亿美元，年复合增长率为26.2%。

不过，Gartner表示，虽然无密码身份验证前景广阔，但它并不是一项独立的技术或市场。无密码身份验证目前只是一种愿景，而非一个目标。身份领域的领导厂商们并不确定，无密码身份验证实际上应该是什么样的。

对于企业而言，部署会产生新的成本、部分用户不愿放弃密码登录，是横亘在无密码身份验证面前的难题。企业需要采购新的软件或硬件，并对内部员工开展配置，还要考虑软件迁

移、维护等意外费用。有部分用户由于习惯了使用密码登录，特别是容易记住的密码，切换到无密码身份验证可能看起来不太方便，企业会认为改用无密码会对用户体验产生负面影响甚至破坏生产力。

因此，Gartner 提出了一套“三步走”的指南，通过制定灵活的路线图、最大限度缩短价值实现时间、为普遍采用做好准备等步骤，以指导企业更好地实现无密码身份验证。Gartner 认为，到 2025 年，超过 50% 的员工和超过 20% 的客户身份验证交易将实现无密码。

## 趋势十

### 一体化 UES 将成为终端安全的标配

Gartner 曾预测，预计在 2024 年，超过 50% 的终端安全产品将支持统一终端安全 (UES) 框架。

提到终端安全，脑子里第一反应是什么？是反病毒？是威胁检测与响应？还是桌面终端管控或者其他什么？显然，这些都是终端安全的“必选项”。随着网络威胁的不断演进，

任何单一的产品或者技术都无法独立承担起终端安全的重任，这其中包含两个方面的原因。

其一，威胁的多样化倒逼防御技术的多样化。网络安全没有“银弹”，不可能做到一招鲜吃遍天，任何一项新的攻击技术或者战术的出现，都倒逼着防守方采用新的技术去应对。譬如，过去做终端安全只需要做好病毒查杀一件事就可以了；但现在高超水平的攻击者能够利用多个漏洞组合攻击、可以利用凭证窃取绕过身份认证、可以通过社工渗透甚至近源攻击穿透内网，这并非单一能力可以解决，而是需要多种不同安全能力的深度融合。

其二，IT 系统的复杂化、BYOD 的兴起倒推动了终端多样化。随着云计算、移动互联、物联网的发展，传统 PC 终端、虚拟终端、移动终端及新型的物联网终端逐渐走进了工作中的各个角落。与此同时，BYOD 的兴起让使用自有设备办公成为主流，各种搭载不同平台的终端，都可能成为攻击者入侵的目标。此前各类终端安全产品都有自己的“一亩三分地”，自扫门前雪，不能兼容其他平台，这给防守方带来了很大的压力。

因此，市场对于终端安全方面的需求也越来越清晰，那就是为了应对

层出不穷的终端安全风险、安全态势及适应性的安全风险，将采用统一的终端安全方案，也就是 UES，Unified endpoint security，直译为统一终端安全或者终端安全一体化。显然，这非常符合组织对于网络安全的需求，对于大部分普通用户来说，都希望只用一套客户端，就覆盖绝大部分终端安全需求，否则只会陷入到多个不同的客户段之中而无法自拔，同时也是对计算和网络资源的浪费。

根据 Gartner 的定义，UES 是将终端保护平台 (EPP)、威胁检测与响应 (EDR)、移动威胁防御 (MTD) 功能单一的控制台整合到一个统一的平台下，从而提供更好的安全概况和更简单的管理，这符合客户对于简化安全的强烈需求。

但值得注意的是，UES 并非简单的“all in one”策略，而是一整套完善的终端安全体系，否则只是单纯的产品或者能力堆砌，相互之间不能形成合力，无法起到“组合”的作用。就像砌墙，如果攻防们只是把砖头堆成一堵墙，那么这堵墙一推就倒；因此砖头之间需要用水泥，消除不同砖块之间的缝隙，让砖块能够更加紧密地结合在一起。

通常情况下，UES 主要包含两个部分，即能力一体化和终端一体化。能力一体化基于“一套客户端与一套管理平台”，深度整合系统合规与加固、威胁防御与检测、运维管控与审计、终端数据防泄漏、统一管理运营等各项安全能力，为客户提供体系化的终端安全能力；终端一体化则强调对 Windows、Linux、macOS 及各类移动终端的全面覆盖，提供一致的终端安全体验。安

(本文执笔：张少波 魏开元 李建平 王彪)



# 「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结  
从红队、蓝队、紫队视角全面解读攻防演练



扫码购买

# 2023 年数据安全 10 大事件

数据安全的 2023，顶层设计不断完善，数据要素开启无限想象空间。

还有不到 30 天，2023 年就要说再见了。回顾这一年的科技行业，从年初的十六部门促进数据安全产业发展《指导意见》，到近期国家数据局提出的“数据要素 ×”，和数据相关的概念，如数据要素、数据流通交易、数据安全等，无疑是贯穿全年的政策热点。作为第五大生产要素，数据资源的运用，对推进数字中国、数字经济、数字社会规划和建设起着不可忽视的重要作用。

让我们以时间为轴，以大事件为线，回顾一下这一年对于数据安全紧密相关的重大政策和文件，以及背后的演进轨迹。



## 十六部门联合促进数据安全产业发展，1500 亿市场呼之欲出

2023 年 1 月，工信部、国家网信办、国家发展改革委等十六部门联合发布《关于促进数据安全产业发展的指导意见》（以下简称《指导意见》），目标到 2025 年，数据安全产业基础能力和综合实力明显增强，数据安全产业规模超过 1500 亿元，年复合增长率超过 30%，建成 5 个省部级及以上数据安全重点实验室，攻关一批数据安全重点技术和产品。

《指导意见》的总体思路中，明确了 7 个战略任务、3 个保障措施。包括贯彻总体国家安全观，统筹发展和安全，以全面提升数据安全产业供给能力为主线，加强核心技术攻关，加快补齐短板，推动数据安全产业高质量发展，促进以数据为关键要素的数字经济健康快速发展等。

**点评：**

《指导意见》是第一个对数据安全产业发展规模提出了数字预估（1500 亿元）的政策文件，它标志着





英文名称: 工业和信息化部 国家互联网应急中心 国家发展和改革委员会 教育部 科学技术部 公安部 国家安全部 财政部 人力资源和社会保障部 中国人民银行 国务院国有资产监督管理委员会 国家税务总局 国家市场监督管理总局 中国银行保险监督管理委员会 中国证券监督管理委员会 国家知识产权局
标 题: 工业和信息化部等十六部门关于促进数据安全产业发展的指导意见
英文文号: 工信部联网安〔2022〕182号
英文日期: 2023-01-03 发布日期: 2023-01-13
发布机构: 网络安全管理局 分 类: 产业政策

### 工业和信息化部等十六部门关于促进数据安全产业发展的指导意见

工信部联网安〔2022〕182号

数据安全产业将不仅仅是网络安全产业的一个子集，而是具有独立的发展逻辑和市场空间，1500 亿的产业规模，将大大加速数据安全的产品和技术创新，使其成为数字经济健康快速发展的重要基石。



## 数字中国建设顶层规划：数字安全被列为“两大能力”之一

中共中央、国务院印发了《数字中国建设整体布局规划》（以下简称《规划》），并发出通知，要求各地区、各部门结合实际认真贯彻落实。《规划》指出，要强化数字中国关键能力，其中包括筑牢可信可控的数字安全屏障，切实维护网络安全，完善网络安全法律法规和政策体系。增强数据安全保障能力，建立数据分类分级保护基础制度，健全网络数据监测预警和应急处置工作体系。

党的二十大报告提出了加快建设网络强国、数字中国，这为推进中国式现代化提供了顶层指引。《规划》

贯彻了党的二十大精神，指出建设数字中国是数字时代推进中国式现代化的重要引擎，是构筑国家竞争新优势的有力支撑。加快数字中国建设，对全面建设社会主义现代化国家、全面推进中华民族伟大复兴具有重要意义和深远影响。

#### 点评：

《规划》进一步明确了建设数字中国对于推进中国式现代化的核心地位，同时将数字技术创新体系与数字安全屏障并列作为“两大能力”，凸显了安全在数字中国中的底板作用。尤

其是《规划》从宏观指引到微观落实，对建设数字中国给予了全方位的保障，充分体现了“统筹发展和安全”的理念。



## 央行发布数据安全管理办法，填补该领域制度空白

7 月，中国人民银行发布关于《中国人民银行业务领域数据安全管理办法（征求意见稿）》（以下简称《办法》）公开征求意见的通知。《办法》分成总则、数据分类分级、数据安全保护总体要求、数据安全保护管理措施、数据安全保护技术措施、风险监测评估审计与事件处置措施、法律责任、附则八章，共五十七条。

可以看出，《办法》依据相关的网络安全和数据安全法律法规制定，其目的在于规范中国人民银行业务领域的数据安全管理办法。《办法》明确了其适用范围是我国境内开展的中国人民银行业务领域数据相关的处理活动，提出了“谁管业务，谁管业务数据，谁管数



据安全”的基本原则，要求数据处理者采取有效措施保护数据安全，同时压实了数据处理活动全流程安全合规责任和底线。

**点评：**

《办法》全面衔接了《中华人民共和国数据安全法》，细化明确中国人民银行业务领域数据安全合规底线要求，填补了该领域数据安全管理制度保障空白，具有很强的指导意义。



## 财政部发布重磅文件， 数据资产入表倒计时

2023年8月，财政部发布《企业数据资源相关会计处理暂行规定》（以下简称《暂行规定》），规定符合企业会计准则中无形资产或存货定义的数据资源可以作为数据资产进行入表，同时明确企业确认的数据资源在初始计量时需以历史成本入账。就此，数据资产“入表”正式提上日程。《暂行规定》对于推动数据要素市场化配置、提高相关会计信息支撑、激活数据价值方面有重大意义。

**点评：**

数据资产“入表”，意味着数据完成了从自然资源到经济资产的跨越，作为数字经济时代的第一生产要素，数据有望成为政企报表及财政等收入

的重要支撑。后续数据要素确权、定价、交易流通、收益分配、试点等进展有望陆续推出。未来随着国家数据局正式揭牌，数据要素相关政策有望加快落地。



## 各地开通公共数据授权运营，“数据二十条”加速探索落地

今年以来，数据要素市场获得地方性政策的密集支持。自7月下旬至8月初，北京市、上海市、广东省、江西省等地陆续出台政策文件，进一步深化数据要素市场改革和创新。

7月18日，北京市经济和信息化局印发《北京市公共数据专区授权运营管理办法（征求意见稿）》，其中提出优先支持与民生紧密相关、行业增值潜力显著和产业战略意义重大的信用、交通、医疗、企业登记监管等领域开展公共数据授权运营。

7月20日，江西省人民政府印发的《江西省数字政府建设总体方案》提出，推进政务数据开放利用，加强数据授权运营，探索数据资源确权、开放、流通、交易相关制度，充分释放数据要素价值。

8月7日，深圳市政府办公厅印发《深圳市优化市场化营商环境工作方案（2023—2025年）》指出，“加快培育数据要素市场，健全深圳市公共数据开放平台，2024年在企业登记监管、卫生健康、交通运输、气象、金融、电力等重点领域开展公共数据授权运营试点。”

**点评：**

自2022年12月“国家数据二十

同时将数字技术创新体系与数字安全屏障  
并列为“两大能力”，  
凸显了安全在数字中国中的底板作用。



条”发布之后，各地方积极落实针对性举措，开展各类创新实践探索，基本形成了公共数据的授权运营模式。公共数据授权运营是推进公共数据开发利用和价值生成的重要方式，也是激活全社会数据要素市场的关键抓手。随着后续数据要素市场的进一步开放，公共数据有望运行开放，企业通过数据交易获取相关数据，进一步探索出成熟的商业模式。而全国性的数据要素市场建设也将全面提速。



## 促进开放和发展，网信办出台数据跨境流动规定

2023年9月底，国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》（以下简称《规定》），旨在保障国家数据安全，保护个人信息权益的基础上，进一步规范和促进数据依法有序自由流动。

该规定本着发展、开放优先的原则，在个保法及相关数据跨境传输规定的基础上，大幅调整了数据出境评估备案工作的适用标准。在仅涉及少量个人信息出境、具有强出境必要性的情形等特定情形下，减轻或豁免原有的数据出境合规义务。

### 点评：

《规定》回应了数据出境合规实践中大量企业的合规困惑，明确了数据跨境流动的豁免情形，且其效力优先于《数据出境安全评估办法》《个人信息出境标准合同办法》，它使得很多数据出境行为免于评估或者通过认证、签订标准合同，在确保数据有序跨境流动的同时，降低了部分企



业开展数据跨境业务过程中不必要的合规成本，从而极大便利了企业日常业务的开展，实质性响应了我国政府坚持经济全球化的倡议，有助于促进经济交流和发展。



## 国家数据局正式揭牌，数据要素万亿市场加速开启

国家数据局从2023年3月7日提请组建，到2023年10月25日上午正式揭牌，充分彰显了国家对数据的生产要素和资源属性的高度重视。国家数据局负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等，由国家发展和改革委员会管理。

“国家数据局挂牌为数字经济和数据要素发展上提供有了强有力的组织保障，是中国顺应数字经济潮流的重大举措。”随着数据局的正式挂牌，未来会有很多措施加速落地，例如“数据二十条”细则的落地、公共数据授权运营、数据产权确权等，有利于万亿级数据要素流通市场的加速释放，进而对数据安全市场带来重磅利好。

### 点评：

对于广大数字化进程中的政企机构而言，数据局挂牌在以下几个层面带来重要影响：第一是为统筹数字经济发展提供强大的组织保障，有利于集中各方资源全面推进数字中国。第二是进一步强调了在数字经济发展和数据要素释放价值过程中，安全和合规是生命线；第三是安全和合规需要贯穿数据要素化的全过程，数据要素化的全过程中需要用技术赋能合规，将安全技术与业务发展相融合。



## 北京数据基础制度先行区启动运行

2023年11月10日，作为全国首个数据基础制度先行区，北京数据基础制度先行区（以下简称“先行区”）正式启动运行。先行区将按照适应数字经济特征的监管方式，建立先行先试机制，建设数据基础制度综合改革试验田和数据要素集聚区，促进数字经济高质量发展。

国家发展改革委党组成员，国家数据局党组书记、局长刘烈宏表示，希望北京市在数据“三权”分置制度落地、数据流通交易、数据基础设施建设等领域持续探索、先行先试。其中指出，推动数据基础设施建设，让

数据安全“动”起来。数据基础设施是让数据“供得出、流得动、用得好”的关键载体，让数据安全可信流通才能实现数据的高效利用。我们正积极关注数据流通相关技术演进，希望北京市充分发挥人才、技术等优势，积极推进隐私计算、数据空间等数据流通技术研发和集成应用，布局建设数据基础设施，为数据可信、高效流通的基础支撑。

### 点评：

奇安信集团董事长齐向东在2023年BCS大会上曾讲过，数据从“死”到“活”，在复杂流动中产生更大风险。数智时代以前，数据是相对静止、缺少流动的，只是单纯地存储在数据中心、服务器中，价值没有得到充分的利用。数智时代，数据时刻在流动，并在全生命周期的流转中持续创造价值。数据流动越复杂，安全风险更需要警惕。



## 工信部起草数据安全行政处罚裁量指引，合规落地有据、有度

11月23日，工信部官网发布信息，为贯彻落实《数据安全法》《工业和信息化领域数据安全管理办法（试行）》，推动工业和信息化领域数据安全行政处罚工作制度化、规范化开展，工业和信息化部网络安全管理局研究起草了《工业和信息化领域数据安全行政处罚裁量指引（试行）》（以下简称《裁量指引》），现向社会公开征求意见。

《裁量指引》在内容上，指出了三大类数据安全行政处罚情形，数十



小类细分情形。三大类情形包括不履行数据安全保护义务、向境外非法提供数据、不配合监管等。其中，不履行数据安全保护义务包含了 20 余种细分情形，向境外非法提供数据包括 4 种细分情形，不配合监管也包括 4 种细分情况，基本涵盖了数据安全违法违规的各种细分场景。

#### 点评：

《裁量指引》征求意见稿的出台，一是为数据处理者明确了数据安全保护义务，并提供了安全合规建设的落地指引；二是细化处罚裁量基准和裁量尺度，使得监管部门执法有法可依、有章可循、有据有度。



## 国家数据局首提“数据要素 ×”，2000 亿市场激活安全需求

11 月 25 日，国家数据局局长刘烈宏在上海举行的 2023 全球数商大会开幕式上表示，国家数据局将围绕发挥数据要素乘数作用，与相关部门一道研究实施“数据要素 ×”行动，从供需两端发力，在智能制造、商贸流通、交通物流、金融服务、医疗健康等若干重点领域，加强场景需求牵引、打通流通障碍、提升供给质量，推动数据要素与其他要素相结合，催生新产业、新业态、新模式、新应用、新治理。

根据 2023 全球数商大会——上海数据交易所年度发布会上发布的《2023 年中国数据交易市场研究报告》显示，2021 年至 2022 年，中国数据交易行业市场规模由 617.6 亿元增长至 876.8 亿元，年增长率



约为 42%。预计未来 3 年至 5 年，中国数据交易市场仍能保持较高速增长，到 2025 年，规模有望增至 2046 亿元。

#### 点评：

随着数据要素与其他要素的结合，新产业、新业态、新模式、新应用、新治理等不断被催生出来，而数商企业在开发数据产品及数据产品上架时，就面临着各种合规和安全挑战。这意味着数据安全合规技术需要不断创新，如隐私计算、数据空间、区块链等，能够与新业态、新场景、新模式等实现深度融合，适应数字基础设施建设和“数据要素 ×”行动的发展

潮流，保障数字经济的合规有序发展。

## 结束语

对于数据安全而言，2023 年最具标志意义的事件，莫过于国家数据局的成立和挂牌，专业人士预计，相关顶层设计指导文件也将在 2024 年陆续出台。同时，数据资产入表即将在 2024 年 1 月 1 日正式施行，为数据要素发展提供了更加完善的政策配套。政策的密集推动，数据流通交易的活跃，相信即将到来的 2024 年，将奏响数据安全市场新一轮腾飞的序章，向 1500 亿市场规模稳步前行。

# 2023 年 AI 安全 10 大事件

不久前，《咬文嚼字》编辑部发布了 2023 年十大流行语，“人工智能大模型”位列其中。英国《柯林斯英语词典》出版方也对外公布，2023 年年度词汇为“AI”，定义为“人工智能的缩写”。2023 年英文维基百科上，阅读次数最多的词条是“ChatGPT”，浏览量为 4949 万。

无论是“人工智能大模型”，还是年度词汇 AI，都折射出以 ChatGPT 为代表的人工智能正走进一个全新时代，这将改变人类的生产、生活甚至思维方式，为经济社会发展和人类文明带来巨大机遇。

然而，当潘多拉的盒子刚被打开时，我们很难知道它会给世界带来什么，就连马斯克都感叹，“人工智能是未来人类文明最大的风险之一。”可以预见，以 ChatGPT 为代表的人工智能迅速发展，也伴随着潜在的技术安全隐患及国家安全风险，甚至在不久的将来，会深刻改变现有的国际安全格局。

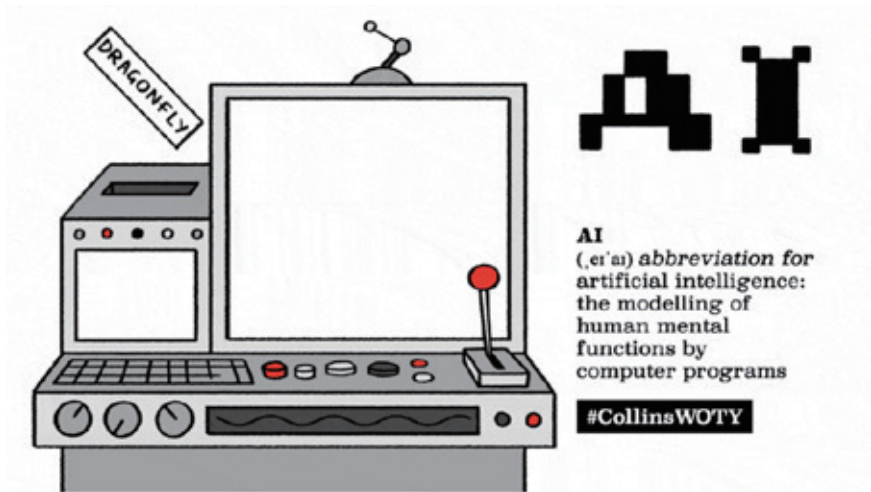
就让我们一起回顾 2023 年，和 AI 安全相关的大事件。

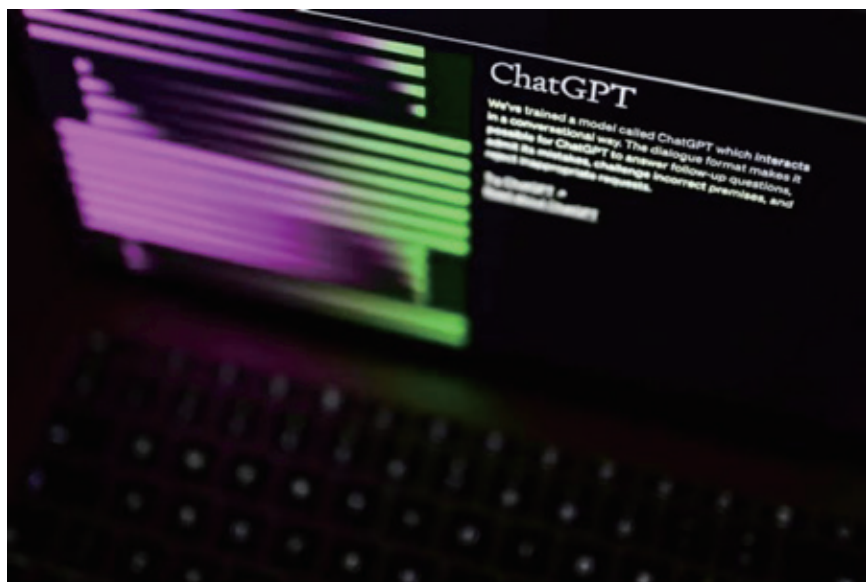


## 敏感数据占比 11%， 研究机构首度披露 ChatGPT 数据泄露

今年 2~3 月，数据安全公司 Cyberhaven 的研究人员分析了不同行业客户的 160 万员工的 ChatGPT 使用情况。其发布的报告称，自 ChatGPT 公开发布以来，5.6% 的知识工作者在工作中至少尝试使用过一次。4.9% 的员工就向 ChatGPT 提供了企业数据，其中 2.3% 的员工将公司机密数据贴入 ChatGPT。

Cyberhaven 研究人员指出，企业员工平均每周向 ChatGPT 泄露敏感数据达数百次，目前敏感数据（包括企业商业机密）占员工粘贴到 ChatGPT 内容的 11%。例如，在 2 月 26 日至 3 月 4 日一周内，拥有 10





万名员工的机构，向基于 AI 的聊天机器人提供机密文件 199 次、客户数据 173 次，以及源代码 159 次。

这是业内首次对于 ChatGPT 使用中数据安全隐患的调查分析。奇安信安全专家认为，随着越来越多的办公产品如 Microsoft 365 Copilot、WPS AI、通义听悟等都集成了大模型，意味着将有更多的员工使用大模型，这会加剧企业敏感数据的泄露风险。解决大模型数据泄露难题，迫在眉睫。



## 涉嫌侵犯用户隐私，ChatGPT 遭意大利禁用

意大利个人数据保护局宣布，从即日起禁止使用聊天机器人 ChatGPT，并限制开发这一平台的 OpenAI 公司处理意大利用户信息。同时个人数据保护局开始立案调查。

这是第一起政府禁止使用聊天机器人的案例。

意大利个人数据保护局认为，ChatGPT 泄露了用户对话数据和付款服务支付信息，没有告知用户将收集处理其信息，缺乏大量收集和存储个人信息的法律依据，同时缺乏年龄验证系统，因此未成年人可能接触到



## 10 分钟被骗 430 万！AI 诈骗正在全国爆发

随着 ChatGPT 和各类 AI 技术的广泛应用，AI 诈骗手段日渐丰富，各



类案件层出不穷。AI 诈骗是利用 AI 技术模仿、伪造他人的声音、面孔、视频等信息，进行欺骗、敲诈、勒索等犯罪活动。其共性包括，诈骗分子利用受害者好友发布过的视频，截取画面再利用“AI 换脸”技术合成，制造和好友视频聊天的假象骗取受害者信任，从而实施诈骗。这种利用人工智能的高科技诈骗方式，的确让公众难以辨别、防不胜防。

今年 4 月，内蒙古包头警方通报一起利用 AI 实施诈骗的案件。在该案件中，福州市某公司法人代表郭先生 10 分钟内被骗 430 万元。据通报，骗子通过 AI 换脸和拟声技术，佯装熟人实施诈骗。同样在 4 月份，在安徽安庆经开区发生一起 AI 换脸诈骗案中，诈骗分子使用一段 9 秒钟的智能 AI 换脸视频佯装“熟人”，让受害人放松警惕被骗走 245 万元。



## 网信办发布《生成式人工智能服务管理暂行办法》

7 月 13 日，国家网信办联合国家

发展改革委、教育部、科技部、工业和信息化部、公安部、广电总局公布《生成式人工智能服务管理暂行办法》（以下简称《办法》），自 2023 年 8 月 15 日起施行。

这是国内首个专门面向生成式 AI 安全领域的规范意见稿。从《办法》可以看出，数据安全和隐私保护贯穿于生成式人工智能数据的标注、模型预训练、模型训练、提供服务等各个环节，避免了监管盲区导致的安全风险。

《办法》明确要求，提供具有舆论属性或者社会动员能力的生成式人工智能服务的，应当按照国家有关规定开展安全评估，并按照《互联网信息服务算法推荐管理规定》履行算法备案和变更、注销备案手续。这意味着每一个通用大模型企业的生成式 AI 若想要“持证上岗”，都需要根据《办法》中各项要求逐条进行安全性评估，是否符合文件要求。这无疑从监管层面最大程度降低了生成式 AI 的安全风险。



## 50 分钟内被攻破，大模型将引入人类难以控制的风险

在 8 月份 DEF CON 2023 上，由 AI Village、SeedAI 和 Humane Intelligence 组织的大模型红队挑战赛，比以往任何时候都更清晰地展示了生成人工智能如何可能被滥用。

大约 2,244 名黑客参加了这场有史以来最大规模的大模型红队演习，研究人员有 50 分钟的时间来尝试破解随机选择的大型语言模型。接受测试的大

数据安全和隐私保护贯穿于生成式人工智能数据的标注、模型预训练、模型训练、提供服务等各个环节。

## 首批大模型产品获批名单



安信依托安全和人工智能两大领域的深厚积累，发布业内首款大模型卫士产品 GPT-Guard。它可以帮助客户有效监控和防护大模型在使用过程中可能引发的数据泄露、法律合规、知识产权等一系列安全风险，实时管控大模型访问和数据投喂过程，提升企业的大模型应用能力、溯源违法违规行为。从而消除其对于大模型“想用不敢用”的顾虑，让企业更安全的使用大模型应用，向科技要生产力，走好数智时代的发展之路。

## 7

### 中方提出《全球人工智能治理倡议》，坚持智能向善

2023年10月举行的第三届“一带一路”国际合作高峰论坛上，习近平主席宣布了中方提出的《全球人工智能治理倡议》。

《全球人工智能治理倡议》围绕人工智能发展、安全、治理三方面系统阐述了中国方案：一是坚持“以人为本、智能向善”，确保人工智能始终朝着有利于人类文明进步的方向发展。二是坚持“相互尊重、平等互利”，应共同努力弥合“智能鸿沟”，共享“智能红利”。三是坚持“凝聚共识、协同共治”，在充分尊重各国政策和实践差异性基础上，推动多利益攸关方积极参与，在国际人工智能治理领域形成广泛共识。

《全球人工智能治理倡议》将为中外深化人工智能合作提供广阔前景。中外可以在《全球人工智能治理倡议》基础上，加强沟通对话，求同存异，共同推动全球形成具有广泛共识的治

## 6

### 首批国产大模型“持证上岗”，业内首款大模型卫士发布

型语言模型由 Anthropic、Cohere、谷歌、Hugging Face、Meta、英伟达、OpenAI 和 Stability 构建。

结果显示，这些大模型技术具有可被利用的较高漏洞。在 50 分钟内，研究人员发现了包括 Google 和 Open AI 等八种大模型的漏洞或错误，利用这些漏洞不仅可以传播不准确信息、错误信息，甚至为实施犯罪提供指南。

DEF CON 2023 期间的研究显示，这些大语言模型可能泄露数据、传播错误信息、支持仇恨言论，甚至为犯罪提供指导。DEF CON 2023 人工智能红队演习表明，大模型在阻止产生错误信息、偏见和不正确信息方面，以及信息泄露，还有很长的路要走。

8 月底，百度旗下大模型应用文心一言正式面向社会全面开放。在 8 月 15 日《生成式人工智能服务管理暂行办法》正式实施的半个月里，字节、商汤、中科院旗下紫东太初、百川智能、智谱华章等 8 家企业 / 机构的大模型位列首批通过《生成式人工智能服务管理暂行办法》备案的名单，可正式上线面向公众提供服务。

可以说，首批 8 家大模型产品已然拉开了“八仙过海”的序幕。根据百度官方数据，在文心一言开放首日，App 已经被下载超过 100 万次，回答了超过 3342 万个问题。

针对汹涌而来的大模型浪潮，奇

理框架和标准规范。人工智能合作符合中外各方利益，这种合作有助于防止技术滥用和失去对这一快速发展领域的控制。



## 首届全球人工智能 (AI) 安全峰会在英召开

11月1日至2日，首届全球人工智能 (AI) 安全峰会在英国召开。包括中国在内的28个国家的政府高官签署《布莱奇利宣言》，这是一份承认人工智能技术风险的联合声明。警告了最先进的“前沿”人工智能系统所带来的危险。

本次按安全峰会强调各国需共同协作，共同建立AI监管方法，同时宣言各方承诺共同在发布前对先进的人工智能模型进行一系列安全测试。

奇安信安全专家认为，尽管各国在如何监管人工智能及由谁来领导这些问题上存在分歧，但对于监管人工智能的必要性达成共识，相信中外各方通过平等对话和协商，可以找到有效监管人工智能的方式，让这一技术可以真正造福人类。



## Gartner 发布 2024 年十大战略技术趋势，AI 安全受关注

10月17日，Gartner 正式发布了2024年十大战略技术趋势，生成式AI的全民化，以及AI信任、风险和安全管理分列第一和第二位。据Gartner预测，生成式AI或将迎来全民化时代，到2026年，将有超过80%的企业使用生成式AI的API或模型，或在生产环境中部署支持生成式AI的应用，而在2023年年初这一比例还不到5%。

Gartner 将“AI信任、风险和安全管理”摆在了第二的位置。Gartner 写到，AI的全民化使得对AI信任、风险和安全管理 (AI TRiSM) 的需求变得更加迫切和明确。在没有护栏的情况下，AI模型可能会迅速产生脱离控制的多重负面效应，抵消AI所带来的一切正面绩效和社会收益。

根据Gartner的解释，AI TRiSM提供用于模型运维 (ModelOps)、主动数据保护、AI特定安全、模型监控 (包括对数据漂移、模型漂移和/或意外结果的监控) 及第三方模型和应用输入与输出风险控制的工具。除此之外，AI TRiSM 还有助于满足全球范围内激增的人工智能法规。





## 10 &gt;&gt;

## 全面监管人工智能 欧盟达成“历史性 AI 立法”

12月8日，欧洲议会、欧盟成员国和欧盟委员会三方就《人工智能法案》达成协议。欧盟表示，此举是为了让这项技术的使用更加安全，并更好地促进行业发展。这一法案将成为全球首部人工智能领域的全面监管法规，意在保护人类基本权利和不阻碍人工智能行业发展之间寻求平衡。

该法案按照不同的风险类别为人工智能技术应用进行了分类，从“不可接受”，也就是必须禁止的技术，到高、中、低风险的人工智能等，通过识别不同风险来进行监管。

根据法律，对人类安全具有不可接受的风险的人工智能系统将被禁止使用。对高风险的人工智能技术应用，欧盟将在使用相关技术的产品投放市场前进行严格评估，建立风险管理体系。

不仅是欧盟，美国政府也一贯重视人工智能的应用与监管。就在2023年10月30日，美国总统拜登签署了一项《关于安全、可靠、值得信赖地开发和人工智能的行政命令》。该行政命令为人工智能安全和保障建立了新的标准，被外界称为“有史以来政府为推进人工智能安全领域所采取的最重大行动”。

### 结束语：

一年多前，当人工智能公司 OpenAI 发布 ChatGPT 时，谁都无法准确预言它对未来意味着什么。如



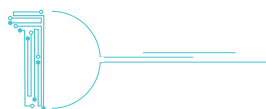
今，全球“百模大战”如火如荼，通用类、垂直类井喷之势发展。IDC 预测，2026 年中国 AI 大模型市场规模将达到 211 亿美元，人工智能将进入大规模落地应用关键期。而麦肯锡《生成式人工智能的经济潜力：下一波生产力浪潮》报告更是显示，如果将分析的 63 种生成式 AI 应用于各行各业，将为全球经济每年带来 2.6 万亿~4.4 万亿美元的增长。

然而，如同《布莱奇利宣言》指出的那样，人工智能的许多风险本质上是国际性的，因此“最好通过国际合作来解决”。人工智能作为当今科技领域的热门话题，其发展速度之快、应用范围之广、影响力度之大，技术之复杂性，单靠一个国家或一个组织的力量很难全面应对其安全风险。因此，各国机构需要加强合作，共同研究和分析人工智能的安全风险，并采取有效的措施来降低这些风险，包括加强对人工智能技术的监管，共同制定人工智能安全治理的国际标准和规范等。

# 2023 年 15 起重大云服务中断事件

2023 年亚马逊网络服务(AWS)、微软、谷歌和其他云服务供应商屡屡发生重大的服务中断事件,造成的损失越来越大,未雨绸缪的防范工作愈显重要。

专业 IT 媒体 CRN 梳理了 2023 年规模最大的 15 起云服务中断事件。



2023 年 1 月

## 微软服务中断

1 月 17 日,北美地区的 Microsoft Teams 和 Microsoft 365 用户遭遇服务中断,中断从美国东部标准时间 9:17 持续到 14:18。

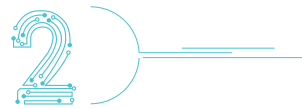
服务中断跟踪网站 Downtime-detector 显示了大量与 Teams 相关的问题报告。上午 10 点左右,累积报告了 504 个问题;在上午 11 点前,又报告了 503

个问题。这些问题中大约 66% 由服务器连接引起,20% 由应用程序引起,14% 属于登录问题。

1 月 25 日,路透社报道称,网络问题导致美洲、欧洲、亚太、中东和非洲等地 Azure、Teams、Outlook 和其他服务中断。上午晚些时候,经过全面系统恢复各项服务恢复正常。

微软将服务中断归咎于微软广域网(WAN)设备之间的网络连接问题。根据 Quest Software 的 Practical 365 报告,服务中断事件持续了大约 5 个小时。问题根源是一条授权 WAN 路由器发送消息的命令,导致邻接核算和表格转发,阻碍了数据包转发。

根据 CRN 2023 年统计数据,微软全球约有 40 万个渠道合作伙伴。



2023 年 1 月

## IT Glue 服务中断

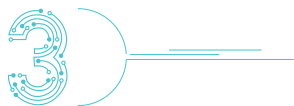
太平洋标准时间 1 月 18 日上午 8 点左右,Kaseya 旗下云文档软件厂商 IT Glue 报告称,他们必须进行“紧急数据库维护……以解决一些客户遇到的问题”。

根据事件报告,这家供应商启用了只读模式,直到太平洋标准时间上午 9:33 才恢复正常。IT Glue 在 1 月 20 日之前恢复了所有密码和文件。

Reddit 用户在 1 月 9 日和 1 月 11 日发帖报告了 IT Glue 平台的问题,尽管后者并没有这两天的事件报告。

IT Glue 用户群包括全球超过 1.3 万家组织、逾 35 万个个体。





2023年2月

## 甲骨文、NetSuite 服务中断

甲骨文联合创始人兼首席技术官 Larry Ellison 曾公开表示，旗下甲骨文云基础设施（OCI）“不会崩溃”。但据 Network World 报道，2月 OCI 发生了一次持续数日的服务中断。

问题始于美国太平洋标准时间 2 月 13 日周一上午大约 10:30，并持续到 2 月 15 日周三下午大约 3:30，主要影响美洲、澳大利亚、亚太、中东、欧洲和亚洲的用户。

事件原因是，支持 OCI 公共域名系统 API 接口的后端基础设施出现性能问题，导致无法处理一些传入服务请求。甲骨文使用了实时后端优化和 DNS 负载管理微调来减轻问题。

根据 Network World 的报道，中断期间，OCI Vault、API Gateway、Oracle Digital Assistant 和使用 OpenSearch 的 OCI Search 都出现了问题。

Data Centre Dynamics 报道称，甲骨文子公司 NetSuite 在美国东部标准时间 2 月 14 日中午左右发生服务中断，原因是马萨诸塞州沃尔瑟姆的 Cyxtera 数据中心起火。

据 The Register 报道，Cyxtera 数据中心切断了服务器电源，账户恢复工作大约在美国东部标准时间晚上 10:26 左右开始。

根据 CRN 2023 年统计数据，NetSuite 在全球约有 880 个渠道合作伙伴，其中有 300 个位于北美。



2023年3月

## Datadog 服务中断

从 3 月 8 日开始，美国云监控和安全工具供应商 Datadog 持续遭遇服务中断，解决问题花了近两天时间。

据 MarketWatch 报道，这家供应商在美国东部夏令时上午 1:31 通知用户其 Web 应用出现问题。富国银行分析师甚至发布报告，表示担忧这次中断会影响 Datadog 收入。

根据该供应商 5 月季度收益电话会议的一份文字记录，这次事件使 Datadog 损失约 500 万美元，需要 500 到 600 名工程师三班倒工作才能解决。

文字记录显示，Datadog 联合创始人兼首席执行官 Pomel 表示他并不“太担心再次发生这样的事情”，Datadog 学会了如何“更快地恢复”，以及“更好地帮助我们的客户在发生问题时减轻影响”。

科技专栏作家 Gergely Orosz 写道，Datadog “很可能在系统中断期

间没有向客户收取数据传输费用”，而“这次损失大约相当于公司一天的收入”。

Orosz 说，操作系统更新是中断的一个因素，并称该供应商理应更好地与用户沟通。



2023 年 4 月

## 微软服务中断

4 月 20 日，Microsoft 365 在线应用和供应商的 Teams 协作应用出现问题，持续近 6 个小时。

微软在太平洋夏令时上午 6:56 发布推文，表示正在“调查 Microsoft 365 在线应用和 Teams 管理中心的访问问题”。

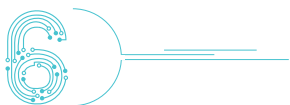
公司在太平洋夏令时下午 1:10 发布推文称，“经过我们内部遥测和受影响用户的积极确认，服务已恢复。”

Ookla 旗下的 Downtetector 网站当天记录了数千个 M365 的中断报告，报告数量在太平洋夏令时上午 7 点左右超过了 3000 个，在太平洋夏

令时上午 9 点左右达到峰值。

根据 The Register 的报道，Teams、SharePoint Online 和 Outlook 在 4 月 24 日再次出现中断。微软在太平洋夏令时上午 4:17 和上午 7:17 分别发布推文，表示“大部分影响”已得到纠正。

Bleeping Computer 报道称，4 月 25 日 Exchange Online 发生另一起中断。微软在太平洋夏令时下午 1:21 发布了有关问题的推文，大约一个小时后表示问题得到解决。



2023 年 4 月

## 谷歌服务中断

据 The New Stack 报道，4 月 25 日太平洋夏令时下午 5:20 左右，法国巴黎一家数据中心发生火灾，导致欧洲地区的谷歌云服务和超过 90 个云服务受影响。

据 IT Pro 报道，受影响服务包括谷歌云储存、云密钥管理服务、云身份和访问管理和谷歌 Kubernetes 引

擎。

5 月 10 日，谷歌报告称“位于受影响数据中心部分的一些实例仍然不可用”。



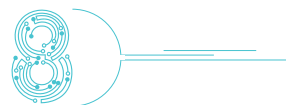
2023 年 4 月

## 甲骨文中心问题

据 Federal News Network 报道，4 月 17 日，美国退伍军人事务部遭遇甲骨文中心电子健康记录（EHR）系统中断，中断持续 5 个小时，起因是数据库能力升级和故障转移。

随后，在 4 月 25 日，甲骨文中心系统再次遭遇了近 4 个小时的中断，影响到了美国退伍军人事务部、美国国防部和美国海岸警卫队。

据报道，美国退伍军人事务部决定暂停进一步使用该系统，直到使用该系统的五个部门站点对系统功能性恢复信心为止。



2023 年 5 月

## 思科 SD-WAN 问题

此次问题属于云服务中断的硬件方面。思科多种 vEdge 平台的公共根证书过期，导致该供应商在推特公开道歉，并在 Reddit 论坛的思科板块发布帖子，引发 80 多条评论。

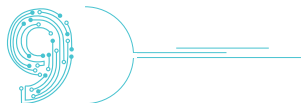
5 月 10 日，思科在推特发帖表示，“对于造成的问题，我们深感抱歉。”

思科在网站上发帖表示：“我们发布了软件的升级版本以永久解决这个问题。”

根据思科的说法，vEdge 路由器

考虑到服务中断已经司空见惯，以及损失越来越大，做好准备工作变得尤为重要。

提供了“思科 SD-WAN 解决方案的广域网、安全和多云能力。思科 SD-WAN vEdge 路由器以硬件、软件、云或虚拟化组件的形式提供，位于站点的边缘，如远程办公室、分公司、校园或数据中心”。



2023 年 6 月

## 微软服务中断

微软 365 服务，如 Teams 和 Outlook，在 6 月初连续几天经历了广泛的中断，随后几天又发生了重大的 OneDrive 中断。

次日，数千用户发现微软 Azure 云平台门户下线。

当月晚些时候，微软确认事件是分布式拒绝服务(DDoS)攻击造成的。

事件细节如下。6 月 5 日上午，上万名微软 365 用户受中断影响。这家软件巨头表示暂停了某项“更新”计划。

美国东部夏令时上午 11:45 左右，微软发表推文表示，“我们确定了 Microsoft Teams、SharePoint Online 和 OneDrive for Business 的下游影响。”

微软表示，发现有一项“更新存在潜在问题”，该公司已经阻止其在更多服务部分传播，并正在审查已应用该更新的微软基础设施中是否有迅速撤销该更新的选项。

第二天，微软发现服务问题的“再次发生”。美国东部夏令时下午 12:03，微软表示“确定了事件影响再次开始”，并正在落实进一步的缓解措施。

微软表示，“遥测数据显示，相

对于先前事件，影响已经减少，这要归功于先前采取的缓解措施。”

美国东部夏令时上午 11:22，有 3118 个 Downtetector 用户报告了 Microsoft 365 出现问题。

6 月 8 日，一家名为“匿名苏丹”的黑客组织声称对微软 OneDrive 中断负责。美国东部夏令时下午 3 点，微软表示正在“继续分析监控遥测数据并实施负载平衡措施，以缓解事件影响”。

当天稍后的状态页面更新显示，中断仅影响了通过 Web 浏览器访问 OneDrive。微软在更新报告中说，“使用桌面客户端、同步客户端或 Office 客户端访问 OneDrive 服务没有受到影响。”

第二天，6 月 9 日，微软用户发现 Azure 云平台门户经历了一次重大中断。

微软似乎在当天下午解决了问题。美国东部夏令时上午 11 点后不久，Downtetector 上开始出现关于 Azure 可用性问题的用户报告。在接下来的两个小时内，数千名用户在该网站报告 Azure 中断。

“匿名苏丹”组织声称对 Azure 门户进行了 DDoS 攻击。

6 月 12 日星期一，微软表示“已确定网络流量激增”是造成中断的可能原因。



2023 年 6 月

## AWS 问题

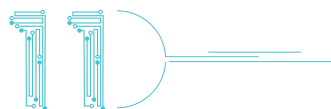
根据云巨头 AWS 在网站发布的一份事件报告，亚马逊网络服务在 6 月经历了数小时的中断事件。

报告称，“从2023年6月13日太平洋夏令时上午11:49开始，客户在美国东部北弗吉尼亚（US-EAST-1）地区对Lambda函数调用的错误率和延迟增加。由于降级的Lambda函数调用，一些其他AWS服务——包括Amazon STS、AWS管理控制台、Amazon EKS、Amazon Connect和Amazon EventBridge——也出现错误率和延迟增加。Lambda函数调用在太平洋夏令时下午1:45开始恢复正常，所有受影响的服务在太平洋夏令时下午3:37完全恢复。”

报告称，为了防止再次发生此事件，AWS“立即禁用了触发事件的Lambda前端集群活动的扩展活动，同时我们努力解决导致问题的潜在漏洞；此漏洞已经被解决，解决方案已部署到所有地区”。

报告称，“此事件还揭示了我们Lambda细胞架构中扩展Lambda前端的一个空白。由于该空白，受影响细胞扩展时，潜在漏洞会产生影响。我们已经对Lambda采取几项行动，解决细胞扩展的直接问题，并计划在今年早些时候完成更多工作，确保所有细胞大小都得到合理限制，避免未来的意外扩展问题。”

根据Downdetector，在太平洋夏令时中午左右，成千上万用户报告称西雅图AWS中断。



2023年7月

## Slack 中断

7月27日，由Salesforce拥有的协作平台Slack经历了持续约1小



时的系统范围问题，问题在太平洋夏令时上午3点解决。

Slack公司在一篇在线帖子中表示，中断期间，“用户无法在多个平台上发送或接收消息”。

根据帖子所述，“我们的工程团队在更改管理内部系统通信的服务后发现了一个问题。问题导致了Slack功能下降。变更最终被撤销，为所有用户解决了问题。”



2023年7月

## IT Glue 问题

7月发生的IT Glue问题持续了约一小时，导致“502错误网关”。

IT Glue在太平洋夏令时7月18日上午11:54发布帖子称，性能问题“可能会阻止我们的一些合作伙伴访问IT Glue”。该事件在太平洋夏令时

12:46解决。



2023年9月

## 微软 Teams 问题

Microsoft Teams在九月中旬经历了长达两个多小时的问题。

微软在太平洋夏令时9月13日上午7:10发推文说，这家科技巨头正在“调查影响Microsoft Teams的事件。用户可能会遇到消息发送和接收延迟或失败等问题”。

供应商“确定问题仅影响通过受影响基础设施为用户提供服务的某些用户”，并将“受影响的服务流量路由到健康基础设施以减轻影响”。

微软在太平洋夏令时上午9:43发推文说：“我们确认与此问题相关的影响已解决。”

思科的ThousandEyes网络情

报公司发帖表示，“应用程序前端是可访问的，但尝试登录系统和/或与其交互导致 500 错误和超时。”

根据这篇帖子，这表明“某种后端系统或分发层问题”。



2023 年 9 月

## Salesforce 中断问题

Salesforce 发布一份报告称，该供应商于 9 月 20 日遭遇服务中断，持续大约两个小时，影响了其产品和服务。但 MuleSoft 和 Tableau 受到的影响时间长达约四个小时。

根据公司的审查报告，这次中断是由于一项政策变更而意外引发的，该变更是“我们持续审查和更新安全控制的标准操作流程的一部分”。

报告称，“虽然这项变更旨在增强防御深度，但无意中阻止了对其意图范围之外的其他合法和必要资源的访问。最终结果是，访问权限不足导致服务之间通信中断，进而在我们系统内部产生了故障。这导致部分客户无法登录和使用服务。”

作为供应商，Salesforce 已经修改了其变更审查和批准流程，并修复了 Tableau 中的启动竞争条件错误，以防止类似问题再次发生。Salesforce 还承诺：

“启用专门的自动化部署流程，以强制执行分阶段政策部署”，“启用额外的监控和警报功能，以更快地诊断与策略相关的问题”，并“对 MuleSoft CloudHub 的后端组件进行重新架构……以增强弹性”。



2023 年 11 月

## Cloudflare、Workday 服务中断

Workday 和 Cloudflare 将从 11 月 2 日开始的服务中断归因于俄勒冈州的一处设施出现的问题。思科的 ThousandEyes 推测这两者受到了同一数据中心的影响。

Cloudflare 首席执行官 Matthew Prince 在该供应商网站上的一篇文章中表示，对于 11 月初连续多日的事故感到“抱歉和尴尬”，并将部分责任归咎于俄勒冈州 Flexential 运营的数据中心。

11 月 2 日，Cloudflare 面向客户的控制面板界面和分析服务出现中断。该事件持续到 11 月 4 日。

Prince 表示：“截至协调世界时 11 月 2 日 17:57，我们已经在灾难恢复设施恢复了大部分控制平面。灾难恢复设施上线后，许多客户不太可能在我们大部分产品中遇到问题。然而，其他服务的恢复时间较长，使用这些服务的客户可能在完全解决事件之前遇到问题。在整个事件期间，我们的原始日志服务对大多数客户不可用”。

Prince 致歉，表示 Cloudflare “相信我们已经建立了高可用性系统，即使我们的核心数据中心提供商发生了灾难性故障，也应该能够阻止这样的中断”。

他表示：“尽管许多系统确实按设计保持在线，但一些关键系统存在非明显的依赖关系，导致它们不可用。”

Workday 在其关于该事件的

报告中表示，这次中断持续了 3 个小时。报告没有提及 Cloudflare 或 Flexential，但将事件归咎于“我们在俄勒冈州波特兰的数据中心发生了电力中断，导致部分客户服务中断”。

这家供应商表示：“由于备用电源故障及电力环境不稳定，导致了额外的问题，服务恢复所需的时间比通常情况下要长。”

据 KRON4 报道，Downdetector 曾记录了与 Workday 中断相关的超过 1200 起报告。

根据 Parametrix Insurance 2023 年发布的报告，AWS 位于美国东部 1 区 (us-east-1) 的关键业务服务如果停机 24 小时，可能会导致 34 亿美元的直接收入损失，停机 48 小时可能会导致 78 亿美元的损失。该区域是服务《财富》世界 500 强公司数量最多的 AWS 区域。

根据报告，东部 1 区 (east-1) 和西部 2 区 (west-2) AWS 服务停机 24 小时可能会导致 82 亿美元的损失，停机 48 小时可能会导致 175 亿美元的损失。

Aviatrix 预计 2024 年 1 月发布的一份报告发现，“在过去一年中，由防火墙导致的云网络中断次数是组织内部遭遇的网络攻击次数的两倍多。”

考虑到服务中断已经司空见惯，以及损失越来越大，做好准备工作变得尤为重要。云服务巨头 AWS 在 11 月的 re:Invent 大会上宣布提供更多故障注入服务场景，方便客户测试应用程序在极端情况下的表现，比如某个云可用区完全断电或与另一可用区失去连接。

# 2023 年勒索软件攻击盘点

作者 | 魏开元

2023 年以来，尤其是近几个月，勒索软件的活动更为猖獗，在数量上再次创下了历史新高。据 Zscaler 发布的《2023 年全球勒索软件报告》显示，截至 2023 年 10 月，全球勒索软件攻击数量同比增长 37.75%，勒索软件的有效攻击载荷激增了 57.50%。

高速增长的勒索软件活动背后，一方面是网络安全体系亟待完善。奇安信安服团队在事件响应中发现，遭到勒索病毒攻击的政企单位，绝大多数网络安全建设基础极其薄弱，存在显而易见的安全建设漏洞的单位。终端没有采取任何安全防护措施、内网服务器近乎裸奔、关键漏洞长期得不到修复等情况非常普遍。

另一方面则是勒索软件即服务的兴起。网络勒索产业链已然形成，相关利益方分工明确。技术提供方编写勒索程序、漏洞利用代码等攻击工具，并以 SaaS 服务的形式，提供给攻击者使用；攻击者只需要利用现成的工具，寻找特定的目标即可实施勒索攻击，这大幅度降低了攻击者的门槛。

下面就来盘点一下，2023 年业内都发生了哪些骇人听闻的勒索攻击事件，这些事件的背后，都有哪些团伙在作祟，攻击手法上出现了哪些变化，政企机构又当采取怎样的应对措施。

## 第一部分：勒索攻击事件

### 1、英国皇家邮政遭遇勒索攻击事件

2023 年伊始，英国皇家邮政成为了勒索团伙 LockBit 今年的第一个大型受害者，后者在勒索发生的两周后，被前者要求支付高达 8000 万美元的赎金，否则便公开窃取到的数据。媒体公开报道显示，勒索软件加密了用于国际运输的设备，并在用于海关备案的打印机上打印勒索赎金票据。

1 月 12 日，皇家邮政声称，网络攻击事件迫使他们停止了国际邮政服务。有趣的是，皇家邮政并没有向攻击者“屈服”，而是按照有关监管机构的要求拒绝支付赎金，并聘请专业机构帮助恢复业务。遗憾的是，勒索





攻击的影响一直在持续。国际分销服务业务（包括皇家邮政和 GLS）的半年财务报告显示，截至 2023 年 9 月，收入同比下降 6.5%。给出的原因是工业行动和勒索软件入侵。

## 2、达拉斯市遭遇大面积勒索攻击

5 月初，美国得克萨斯州达拉斯市本遭受了来自 Royal 皇家勒索团伙的勒索攻击，导致其多项市政服务中断。据官方确认，达拉斯市许多服务器已被勒索软件破坏，影响了几个功能区域，包括达拉斯警察局网站，该市数千台设备中只有不到 200 台受到影响。

有消息称，由于此次攻击，26,212 名得州居民和共计 30253 个人的私人信息或被曝光。根据得州总检察长网站信息显示，泄露的信息包括姓名、地址、社会保障信息、健康信息、健康保险信息等内容。

## 3、因 MOVEit 漏洞，美国多个机构遭遇大范围勒索攻击

6 月 15 日，美国官员称，勒索软件组织 Clop 利用 MOVEit 文件传输软件的 0day 漏洞发动攻击，窃取并高价售卖美国能源部在内的多个联邦机构用户数据。分析报告显示，至少有几家公司和组织受到了影响，多个州级组织也宣布遭遇 MOVEit 漏洞相关的数据泄露事件。安全厂商 Emsisoft 的威胁分析师 Brett Callow 称，已统计到 63 名已知 / 确认受害者和数量不详的政府机构。

业内人士认为，此次入侵具有“高度随机性”，既没有专注于“特定的高价值信息”，也没有像之前针对美国政府机构的网络攻击那样具有破坏性。

## 4、波音公司遭遇勒索软件攻击



11 月 1 日，美国航空航天巨头波音公司发表声明称，正在调查一起上周曝光的安全事件，此前臭名昭著的 LockBit 勒索软件团伙将波音列为攻击受害者。一位波音发言人表示，这起网络事件影响了部分零部件和分销业务。不过，飞行安全不会受到影响。

值得关注的是，此前 Lockbit 曾表示，其勒索软件附属团伙利用 0day 漏洞获得了波音公司系统的访问权限，但并未透露漏洞的具体细节，也未透露赎金情况。不过就在工行披露遭遇勒索软件攻击的当天，Lockbit 公布了据称从波音公司窃取的超过 40GB 的敏感数据。

## 5、某银行在美全资子公司遭遇勒索攻击事件

某银行股份有限公司在美全资子公司

公司在官网发布声明称，美东时间 11 月 8 日，遭勒索软件攻击，导致部分系统中断。随后，LockBit 组织代表在 Tox 上公开确认对攻击负责。

据彭博社报道，对某银行美国子公司的攻击已经扰乱了美国国债市场。证券行业和金融市场协会的一份声明显示，由于工商银行遭到勒索软件的攻击，无法代表其他市场参与者结算国债交易，这可能对美国国债的流动性产生巨大影响，并可能引发监管审查。

## 第二部分：勒索攻击组织

### 1、LockBit

今年以来，LockBit 绝对是所有勒索团伙中当之无愧的“老大”，包括波音、泰国气象局、法国司法部、

工商银行在美全资子公司、曼谷航空公司及多家政府机构，都成为了 LockBit 的受害者。今年早些时间，Bleeping Computer 网站披露，该团伙对美国实体组织发动了约 1700 次攻击，成功勒索了约 9100 万美元。但随着 LockBit 的愈发猖獗，无论是攻击次数，还是赎金数量，都在不断增长。

相较于其他勒索团伙，LockBit 具备和 APT 组织无二的高水平攻击渗透能力，无论是社工钓鱼还是 Web 渗透甚至是 Oday 漏洞的挖掘与使用，都能够得心应手。更糟糕的是，LockBit 还对外提供勒索软件即服务，这在一定程度上使整体勒索形式更为严峻。安全人员最新的研究显示，LockBit 勒索软件加密效率惊人，4 分钟内就可加密完成 10 万个 Windows 文件。

## 2、Clop

如果说在 2023 年，有能够和 LockBit 掰手腕的勒索团伙，那一定非 Clop 莫属。尽管 Clop 并没有像 LockBit 有如此强的存在感，但仅在 MOVEit0day 漏洞攻击的一系列事件中，便有西门子能源、壳牌及美国多家联邦政府机构，被 Clop 洞穿了防线，

足以评为今年最大规模的勒索攻击事件。据某私营机构的初步报告显示，至少有几家公司和组织受到了影响。

Clop 组织发起的网络攻击最早在 2019 年被业界发现，他们主要针对大型成熟企业，尤其是金融、医疗保健和零售领域的组织，其核心目的是窃取数据并索要赎金，他们善于利用网络漏洞和网络钓鱼来获取网络访问权限，然后横向移动以感染尽可能多的系统。

## 3、Royal

美国联邦调查局（FBI）和网络安全和基础设施安全局（CISA）在 9 月份联合发布的一份咨询报告显示，Royal 勒索软件组织在过去一年中已经侵入至少 350 个组织的网络系统，与其关联的勒索软件攻击索要的赎金规模已超过 2.75 亿美元。

值得一提的是，在 2022 年 1 月浮出水面时，Royal 还相当低调，甚至在使用其他勒索软件组织的加密器（如 ALPHV/BlackCat），以免引人注目。然而，他们后来在 2022 年其余时间开始将自己的加密器 Zeon 用于攻击。临近 2022 年底，该组织更名为 Royal，迅速成为最猖獗的勒索软件组织之一。

除上述三大老牌知名勒索团伙外，今年还诞生了许多新兴的勒索软件团伙，如 8Base 和 Akira 等。仅在第二季度，8Base 就制造了 107 起（观察到的）勒索软件事件，Akira 则制造了 60 起。有数据显示，与一季度相比，二季度“首次亮相”的勒索软件组织数量同比暴增了 260%。有分析人士认为，Babuk、LockBit 和 Conti 的加密器均已在网上泄露，使得技术专业度知识较少或不熟悉加密的攻击者可

高速增长勒索软件活动背后，  
一方面是网络安全体系亟待完善；  
另一方面则是勒索软件即服务的兴起。

以稍微更改并部署功能齐全的“高端”勒索软件。

### 第三部分：勒索攻击技术

为了提高勒索成功率，勒索团伙策略和技战术方面不断推陈出新。

在策略方面，勒索团伙并不在拘泥于单纯的加密重要数据来要挟受害者支付赎金，而是多管齐下，一方面继续对重要数据进行加密处理，另一方面一旦受害者拒绝了支付赎金的要求，勒索团伙将在公开渠道公开窃取到的敏感数据，甚至以对目标发动 DDoS 攻击为要挟手段。

更有趣的是，某些团伙开始尝试无加密勒索。11月7日，一名来自 ALPHV 勒索团伙的内部人士爆料，称已成功入侵了数字借贷服务提供商 MeridianLink，在未加密其文件的情况下窃取了数据。11月8日，ALPHV 在其泄露网站上发布了这些数据。此外，该团伙向 SEC 提交了一份关于自己所犯罪行的报告，声称受害公司没有遵守 SEC 关于公司必须在什么时限内公开披露所遭攻击的新规定。

在技战术方面，除了常规钓鱼邮件攻击，更多犀利的攻击手段开始频频出现在勒索攻击中，如凭证窃取、漏洞利用、供应链攻击等。奇安信威胁情报中心判断，Oday 漏洞利用逐渐成为勒索团伙武器库的备选项。

在达拉斯遭遇大范围勒索攻击事件中，Royal 组织利用一个窃取到的特权账户，获取了初始访问权限，最终完成了勒索病毒的投递；而在 Clop 发起的大规模勒索攻击事件中，Clop 甚至利用了一个 Oday 漏洞，从而发起了大规模的供应链攻击。

种种迹象表明，勒索团伙已经不

在勒索软件攻击的防范策略方面，  
首当其冲的还是提升安全意识。

再是人们印象中的“草台班子”，而是已经成长为具有高超技术手段、分工明确、产业链上下游齐全的“江洋大盗”。尤其是在攻击水平上，已经和全球顶尖 APT 组织别无二致。

### 第四部分：勒索防范策略

尽管勒索攻击愈演愈烈，但也并非无迹可寻。

在防范策略方面，首当其冲的还是提升安全意识。和其他类型的攻击一样，勒索攻击的开端，往往是由于攻击者抓住了一些容易被疏忽的“低级错误”，如接收了安全性未知的邮件，账户口令过于简单，老旧漏洞没有修补等，据奇安信发布的《2023年中国企业勒索病毒攻击态势分析报告》显示，全国发生的勒索攻击重大事件中，49.5%的勒索攻击事件明确与弱口令有关。

实际上只要安全意识足够，这些问题都可以避免。

其次，在安全建设方面，要注重安全基础能力建设，摒弃银弹思维。

奇安信应急响应实践表明，遭到勒索病毒攻击的政企单位，绝大多数都是网络安全建设基础极其薄弱，存在显而易见的安全建设漏洞的单位。譬如终端没有采取任何安全防护措施、

内网服务器近乎裸奔、关键漏洞长期得不到修复等情况非常普遍。没有整体安全规划、没有全局安全策略、没有有效运营手段，都是勒索病毒受害机构的典型通病。

因此对于绝大多数网络安全能力相对薄弱的机构而言，有针对性地部署安全产品弥补安全团队尤为重要。如部署邮件安全网关拦截钓鱼邮件；在终端和服务器上部署安全软件提升防病毒能力，如奇安信天擎终端安全管理系统、椒图服务器安全管理系统。

第三，要做好同勒索攻击长久战斗的准备，建设实战化、常态化安全运营能力。事实证明，勒索团伙的攻击能力正在不断攀升，随着生成式人工智能的应用，AI 驱动或许会成为驱动勒索攻击增长新的动力，这就要求组织必须建立起常态化的安全运营能力，不断调整、升级策略，以应对不断升级的攻击手法。

与此同时，机构应制定应对计划，以便在发生勒索软件攻击时能够快速有效地采取行动。这应包括数据恢复、事件响应及与客户和员工的沟通。制定一致的安全策略，确保组织内外的所有用户都遵循相同的安全流程。定期进行安全意识培训，帮助员工识别和避免勒索软件攻击。

# 2023 年全球 10 大网络攻击事件

2023 年，数据泄露和网络攻击事件频发，涉及面广，影响力大，全球知名企业组织也因此面临着监管合规与社会舆情的双重压力。

IT 专业媒体 CRN.COM 梳理了 2023 年受到行业广泛关注的十大网络攻击和数据泄露事件，并对事件进行了点评分析。



2023 年 2 月

## ESXi 勒索软件攻击

2023 年 2 月，“ESXiArgs”

勒索软件组织攻击了运行 VMware ESXi 虚拟机管理程序的客户。据美国联邦调查局和美国计算机安全管理局调查数据显示，全球受到攻击影响的服务器数量超过了 3800 台。

据网络安全供应商 Censys 的安全研究人员介绍，这起活动的目标主要是针对美国、加拿大、法国和德国等国家的企业组织，攻击者利用了一个已经存在两年之久的漏洞（编号为 CVE-2021-21974），主要影响旧版本 VMware ESXi 中的 OpenSLP 服务，可以被用来远程执行代码。此次 ESXiArgs 勒索软件攻击事件，再次凸显了保护虚拟化应用基础设施的重要性。



2023 年 2 月

## GoAnywhere 攻击

2023 年 2 月，Fortra 公司紧急发布公告并通知其客户，在其 GoAnywhere 文件传输平台上发现了一个被大肆利用的 Oday 漏洞，该漏洞可用于在被控制的计算机系统上远程执行恶意代码。调查显示，在此次 GoAnywhere 漏洞利用攻击活动中，最具代表性的事件是黑客攻击了医疗福利服务机构 NationsBenefits，并获取了其 300 万会员的部分个人隐私信息。

据了解，黑客还利用 GoAnywhere 平台漏洞窃取了包括宝洁和数据安全



公司 Rubrik 在内的众多大型组织业务数据。根据 Fortra 在调查攻击的过程中发现，GoAnywhere 漏洞被用来攻击少数运行特定配置的 GoAnywhere MFT 解决方案的内部部署环境，这种情形早在今年 1 月就已经出现。



2023 年 3 月

## 3CX 软件供应链攻击

2023 年 3 月，全球知名的通信软件服务商 3CX 遭到网络攻击，在许多关键特征方面与 2020 年爆发的 SolarWinds 供应链攻击非常相似。

在此次事件中，攻击者们主要利用了 3CX 的一款 VoIP 电话系统应用软件，该软件的客户群涵盖了全球 60 余万家组织，以及 2.5 万个渠道合作伙伴，其中主要的客户包括美国运通、麦当劳、可口可乐、NHS、丰田、宝马和本田。

网络安全 Mandiant 声称，3CX 攻击有别于以往软件供应链攻击的地方在于：3CX 活动是由早期的供应链攻击造成的。Mandiant 的研究人员透露：我们监测到攻击者篡改了金融软件公司 Trading Technologies 发布的一款软件包。这是 Mandiant 首次看到由一起软件供应链攻击导致了另一起软件供应链攻击。

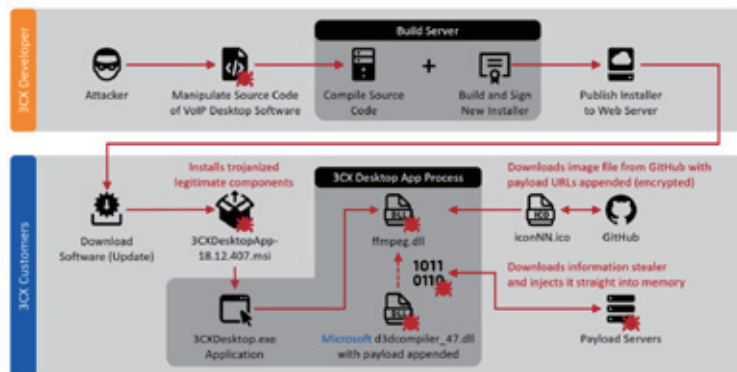


2023 年 5 月

## MOVEit 攻击

2023 年 5 月，勒索软件 Clop 组织利用了 Progress 的 MOVEit 文件传输工具中的一个严重漏洞，开始了大规模的勒索软件攻击活动。与传统

### 3CX Supply Chain Attack



SOPHOS

的勒索软件攻击不同，本次的攻击行动并没有采用任何加密机制，而是以非法泄露数据作为勒索条件。Clop 声称，如果受害者公司支付赎金，它不会在其暗网网站上泄露受害者的被盗数据。针对数百家选择不支付赎金的公司，Clop 确实是这么做的。

目前尚不清楚哪些公司实际上支付了赎金。但据网络安全事件响应公司 Coveware 估计，Clop 将从攻击活动中获利 7500 万美元至 1 亿美元。截至目前，受 MOVEit 活动影响的组织总数或许已经接近 3000 家。就已知受影响的个人而言，如今总数接近 8400 万人。这使其成为 2023 年影响最广泛的攻击之一，也使其成为近年来最严重的数据泄露事件之一。在 IT 行业，MOVEit 数据勒索活动的受害者包括 IBM、高知特、德勤、普华永道和安永。

5

2023年5月

## PBI Research Services 泄密

2023年5月，同样是受到MOVEit漏洞影响，导致了一家大型软件系统开发供应商的众多下游客户企业泄密。数据显示，就受影响的人员数量而言，PBI Research Services (PBI) 泄密事件或许是与MOVEit相关的最大单一事件，最终导致超过1400万人的个人隐私数据遭到泄露。

使用PBI服务的组织包括政府养老金系统、保险公司及知名的投资公司。美国最大的公共养老基金CalPERS在事件说明的新闻发布会上就表示，有76.9万名退休人员的个人数据遭到泄露。

6

2023年6月

## 梭子鱼电子邮件安全网关攻击

2023年6月，知名网络安全公司梭子鱼发布公告披露，超过5%的该公司生产的ESG设备已被攻击者入侵。攻击活动利用了该公司电子邮件安全网关(ESG)内部设备中的一个严重漏洞。通过进一步调查发现，该漏洞早在2022年10月就被利用了。这些攻击促使梭子鱼建议其受影响的客户免费更换ESG设备。

Mandiant公司将这次大范围的活动归咎于编号为UNC4841的黑客组织。该公司的研究人员报告，政府

部门是该攻击团伙特别偏爱的目标，尤其是针对美国的政府机构。

7

2023年6月

## 微软云电子邮件泄露

2023年6月，属于多家美国政府机构的微软云电子邮件账户遭到非法入侵，其中包括了多位高级政府官员的电子邮件。据报道，美国国务院的10个邮件账户中共有6万封电子邮件被盗。这起事件促使美国参议员Ron Wyden要求联邦政府展开调查，以确定微软公司松懈的安全防护措施是否是导致本次泄密事件的主要原因。

微软公司表示，安全专家已经发现了使威胁团伙“Storm-0558”得以闯入美国官员云电子邮件账户的原因和问题。在2021年Windows系

统崩溃后，一个漏洞导致攻击中使用的Azure Active Directory密钥被不适当地捕获，并存储在一个文件中。微软表示，有一个漏洞导致这些不规范存放的密钥没有被检测出来。

此外，这次攻击的幕后黑手是通过侵入属于微软工程师的公司账户来访问含有密钥的文件。而微软此前表示，被盗的Azure Active Directory密钥可以被用来伪造身份验证令牌，并访问来自约25家组织的电子邮件。

8

2023年9月

## 赌场运营商被攻击

2023年9月，攻击者针对赌场运营商米高梅和凯撒娱乐发起了极具破坏性的攻击，攻击手法包括利用社会工程伎俩欺骗IT求助台，非法进入米高梅的网络系统。在此次攻击的



调查中还发现，一个名为 Scattered Spider 的年轻黑客组织与俄罗斯背景的勒索软件团伙 Alphv 相互勾结、狼狈为奸。

据安全研究人员声称，Scattered Spider 的黑客使用了 Alphv 提供的 BlackCat 勒索软件（Alphv 团伙的成员之前隶属于发动 Colonial Pipeline 攻击的 DarkSide 团伙）。虽然多年来勒索软件即服务在东欧一直日益猖獗，但欧美黑客与俄罗斯背景黑客团伙结为联盟似乎再让威胁领域向更加令人不安的新方向发展。



2023 年 10 月

## 思科 IOS XE 攻击

2023 年 10 月中旬，针对思科 IOS XE 客户的攻击迅速成为有史以来影响最广泛的边缘攻击之一。据 Censys 研究人员表示，10 月 16 日发现的一个严重 IOS XE 漏洞导致近 42000 台思科设备中招。

思科在当天的安全报告中表示，IOS XE 中的 0day 漏洞被攻击者大肆利用。思科对这个特权升级漏洞赋予了最严重的 10.0 分。思科的 Talos 威胁情报团队表示，利用这个严重漏洞，恶意分子就可以全面控制中招的设备。在大量的思科设备中使用了 IOS XE 网络软件平台，其中许多设备被部署在企业网络边缘环境中。这些产品包括分支路由器、工业路由器和聚合路由器，以及 Catalyst 9100 接入点和支持物联网的 Catalyst 9800 无线控制器。

10 月 23 日，思科发布了针对该漏洞的首个补丁，以限制严重的 IOS XE 漏洞。



2023 年 10 月

## Okta 支持系统泄密

2023 年 10 月 20 日，身份安全厂商 Okta 公司披露一起影响其支持案例管理系统的数据泄露事件。该公司最初以为只影响其 18000 家客户中的很小一部分。然而在 11 月下旬却改口表示，称所有支持客户的姓名和电子邮件都可能被攻击者非法窃取。在 Okta 最初披露支持系统泄密后，BeyondTrust、Cloudflare 和 1Password 都表示自己是这次事件中受影响的客户。

这家身份管理公司在 11 月底的最新披露中表示，它一直在重新检查攻击者执行的操作。攻击者运行并下载了一份报告，其中包含所有 Okta 客户支持系统用户的姓名和电子邮件地址。然而，攻击者下载的报告不包含用户凭据及其他敏感数据。

在最新披露之后，该公司将产品更新推迟 90 天发布，以优先考虑安全。安

# 完了！我被公司高管们包围了

## 序

我姓王，被同事们亲切地称作老王，家住公司隔壁。

作为一名安全工程师，我时常为自己的工作成果感到焦虑：

前脚刚说不得随意外发公司敏感信息，结果后脚就有人把客户聊天记录上传到了 ChatGPT 上，原因是想帮客户写一篇文案；

苦口婆心地劝说不要随便下载未知来源的软件，结果有人不知道从什么地方搞来一堆“破解版”资源，杀毒软件还报了毒；

……

这事能写到年终总结里面的吗？

眼瞅着到了年底，感觉升职加薪又要“明年复明年”了。

但抱怨归抱怨，工作还得继续。

就在我差点被海量告警淹没的时候，收到了一封全员邮件：大致内容是说为避免侵权，请不要使用盗版软件。

邮件是法务发的，他们一连收了三份和软件版权问题相关的律师函。

我突然脑子一抽，直接在全员邮件回复了一句“好，我来想办法处理”。

万万没想到，命运的齿轮从此开始转动起来。

## 第一章：有人“投毒”

我并没注意到邮件这档子事，因为注意力全在一份黑产活动分析报告上。

报告的名字是“关于近期某黑产团伙利用搜索引擎进行供应链投毒的详细分析”，事件描述如下：

某黑产团伙将木马程序与多达数十款热门软件进行捆绑传播，包括办公软件、浏览器、图像处理软件、视频剪辑软件、聊天软件等；

该团伙利用关键词优化、竞价排名的方式，让用户在搜索关键词时，可在前排位置看到植入木马的钓鱼链接；

该团伙会把钓鱼网站伪装成官方网站，使其更具迷惑性。

目前，奇安信天擎已支持对相关





木马样本的精准查杀，建议广大天擎用户及时自查。隔离网用户请及时升级病毒库，如有问题请及时与奇安信技术人员联系。

“好家伙，直接在搜索引擎上‘投毒’啊。”我不禁吐槽，也来不及仔细阅读技术细节，赶紧查看天擎告警。

## 第二章：这就“中招”了？

果不其然！天擎检测到内部某台计算机已经感染。

“还真就这么巧。”我叹了口气，迅速联系了那位中招的同事，顺便知会了我领导。

“您好，我是公司网络与信息安全中心的老王，我们后台显示您计算机上\*\*\*\*\*.exe 应该是一个木马程序，想跟您了解一下情况。”

“啊？中毒了？不是吧！我就在他们官网下的啊，这也有问题？”

“嗯？您确定是官网吗？”

“是啊，你看。”

看着对方发过来的网址，我百分之百肯定，这官网是仿冒的。

“好的，我知道了。建议您先断开计算机的网络连接，稍后我们会跟进处理。”

“有必要开展一次安全意识培训，甚至是全员参与的攻防演习。”我心里默默盘算着。

虽说不能完全杜绝类似事情再次发生，但大幅降低事件发生次数，我还是很有信心的。

如果做成的话，年终总结可算是有点干货。

想到这里，我嘴角忍不住上扬。

正当我满脑子都是活动怎么搞的时候，办公室响起了我们领导极具穿透力的嗓音。



“老王，你来一下。”喊话的是公司首席信息安全官 CISO，我的直属上级。

嗯？这是要谈涨薪的节奏？趁这个机会，我把想法跟他聊一下。

在和同事交代完后续处置动作后，我推开了领导办公室的大门。

## 第三章：尴尬，全都是大佬

一进办公室我就傻眼了。

除了我领导，公司首席信息官 CIO、首席法务官 CLO、首席财务官 CFO，都在这里。

我颤颤巍巍坐下，一脸无辜地问：“啥事儿？”

“你怎么想办法解决？”领导笑眯眯地反问。

“什么想办法？”我一脸懵。

“不是你在全员邮件回复说要想办法解决么？这么快忘记了？”领导

接着说。

我一下子反应了过来，赶紧打开邮箱查看，尴尬得想找个地缝钻进去。

“Emmmm……”我吭哧半天，“这个事情还是得有一套可执行的规范。”

“其实我们一直都有。”CLO 打断了我的发言，“但标准规范并不能完全解决问题，你看你都不知道。”

软件或者字体版权纠纷，法务每年都要处理很多起。

我无言以对，刚才准备好的安全意识培训说辞，一句也没想起来。

“我们每年都跟财务那边做预算，拉着采购一起买一堆正版软件，到头来还得给人赔钱。”CIO 补充说到。

一旁的 CFO 也深表赞同，经他手花出去的预算，他再清楚不过了。

“嗯，没错，是这样的……”我不断点头迎合，试图让自己尽快进入角色。

为了想出解决办法，我感觉我这



辈子脑袋都没转这么快过。

## 第四章：防不胜防

“怎么样，有什么想法吗？”一番讨论之后，CISO将话题又引向了我。

我深呼一口气，缓缓说道：“关于软件正版化，您 CLO 是专家；但应对供应链投毒，这是我们搞安全的特长。”

话音未落，在座领导的眼神，都齐刷刷地看向我。

“嗯，你接着说。” CISO 不置可否。

“通常情况下，我们下载软件都是这么干的。

第一步，打开浏览器，在搜索框内输入关键词，回车；

第二步，在首页靠前位置，找到一个相对靠谱的链接，点击进入；

第三步，下载安装。

正是因为公司没有统一的软件下载渠道，所以大家会去网上搜，感染木马是早晚的事儿。

就在刚才，我们一位同事已经中

招了。”我连珠炮似地说着，一边向在座各位领导展示刚才天擎产生的告警和奇安信发过来的事件分析报告。

“如果我们能建设一个统一的软件渠道，那大家还会在网上自己搜么？”

## 第五章：花钱？省钱！

我的想法很明确，公司需要一套完整的技术方案，具体包括：

首先，要有统一的软件下载渠道，能够快速下载所有主流办公软件；

其次，要能生成软件资产清单，准确识别哪些是正版、哪些是盗版；

最后，要具备统一管控能力，阻断不安全的下载源，对于已安装的不可信软件要能够统一卸载。

如此一来，不仅可以大幅度缓解供应链投毒，盗版问题也顺手解决了。

“我明白你的意思了。” CFO 接过了话茬，“但预算的事情，并不太容易解决。”

这句话把我噎住了。我很清楚，今年以来各部门都在缩减预算，作为以花钱为主的部门，安全部门预算就更加紧张了。

“话虽是这么说，但如果能全面解决问题，光是侵权赔偿这一项，我们就能省下不少钱。”沉默许久的 CISO 开口了，他甚至开始和 CLO 掰着指头算这笔账。

我笑而不语，算账是我们领导的长项，我们的每一分钱预算，都是他一点一点抠出来的。

他总爱和我们说一句话：你们不要总觉得网络安全是成本中心，干得好是可以省钱的。

没多一会儿，我感觉在座几位都被说动了，有点跃跃欲试的样子。

尤其是 CIO，公司内部的资产统

计，向来是一个麻烦事，部门之间经常扯皮。这事儿如果干成了，除了法务之外，他们也能省下不少事。

“那我和领导商量一下，出一个项目需求，然后再开会讨论。”我趁热打铁说到。

## 第六章：还得是它

一连几天，除了一堆看不完的告警，我主要精力都花在了完善项目需求上。那几位参与会议的 CXO 也都很支持，安排专人和我对接，我这儿算是有求必应。

不像以前，我们前脚刚发通知说不能干什么，业务那边后脚准备了好几句在等着我，说这也不能干、那也不能干，干脆业务你来做吧。

我领导私下里对我说，那天他们来我这儿开会，我也一时半会儿没想到好的对策。突然 CLO 在那哈哈笑说，你们部门有人不小心回了全员邮件。

“所以您就想到我了么？”我笑着对 CISO 说。

“没错！哈哈。”

……

在大家的共同努力下，项目推动得很顺利。

“我记得天擎好像是有软件管家模块吧。”带着讨论通过的需求，我拨通了奇安信联系人的电话。

“那可太有了，怎么了，有需求？”对方回答到，语气中略带兴奋。

“嗯，事情是这样的……你看天擎软件管家能搞定么？”

在得到对方问题不大的答复后，我约了对方的时间：“OK，你明天有时间的话我们公司一趟详细聊一下，我们领导也在。”

“行，明早十点，我和我们天擎的产品同事一块过去。”

## 第七章：奇安信来人

第二天，奇安信详细介绍了天擎软件管家的能力。

### 第一，建立可信下载源平台。

借助天擎运营团队的持续运营，天擎软件管家云中心软件商店拥有 1000+ 款面向政企机构日常办公使用的热门软件，如 PS、Chrome、WinRAR、WPS 等，每款软件在云端商店上架都经过运营人员的严格把关，会对软件本身是否有捆绑、流氓、插件等行为检验，并进行病毒的检测，以及软件信息的录入，以确保上架的软件安全可靠、信息完整。

### 第二，禁用非可信来源软件。

针对非可信软件安装渠道带来的内部网络安全问题，奇安信天擎软件管家提供了事前 + 事后的双重管控能力。事前管理，针对非可信来源软件的安装，发现即时弹窗、管控、处置；事后管理，针对事前绕过，配置兜底策略进行弹窗、管控、处置。处置方式为审计、锁屏、断网、关机。

### 第三，一键卸载可疑软件

在针对内部安装违规、可疑软件的处理上，天擎软件管家通过控制台下发卸载任务后自动调取软件自动卸

载能力，在终端零参与的情况下，完成威胁软件的一键卸载。

看到领导频频点头、详细询问具体细节的样子，我就知道差不多了。

## 第八章：难道是真的？

若干天后，项目已经成功完成交付并上线运行，各部门的需求也基本全部满足。

“我们总算是能把软件资产盘清楚了，不用再跟各部门扯皮了。”CIO 说。

“上次上面搞软件正版化工作检查，我们结果非常好，项目上线后没收到版权问题的律师函。”CLO 说。

“别的不知道，反正信息化预算这块，我是好跟老板交代了。”CFO 说。

……

我摸着后脑勺忙着迎合各位老板的夸奖，被各种 CXO 包围着表扬的感觉，真好！


“老王！在不在？”一阵熟悉又富有穿透力的声音从办公室方向传来。

我突然从桌子上爬起来，看了看手机，已经两点多了。最近一直忙着项目测试，是有点缺觉。

不过我依然惊奇，这次午睡竟然睡了这么久，还做梦了。

“老王，来一下！”领导的声音再次响起。

“来了来了！”我擦了擦嘴角的口水，快步向办公室走去。

这次不会是真的了吧？



# 2024 年网络安全趋势， 国外大厂怎么看？

数字化转型有两面：一面是价值，另一面则是事故。大数据、云、人工智能等新兴技术的广泛应用，在提高效率改变生产生活的同时，也导致网络安全事故激增。这种趋势在 2024 年将如何变化？国外安全大厂又是如何看待的？《网安 26 号院》进行了梳理和汇总。

## Fortinet：事件驱动可能引发新一轮攻击浪潮

Fortinet 发布的《2024 年网络威胁趋势预测报告》分享了 2024 年值得关注的最新威胁趋势，并给出了组织开展网络安全防御的建议。Fortinet 预测，2024 年及未来将呈现全新的攻击趋势，全球各地的安全团队需对此保持高度警惕。



**趋势 1: Attack Playbook 再升级。** Fortinet 预测 2024 年网络犯罪分子将更加猖狂，抱着“要么出众，要么出局”的心态，争相扩大目标列表和 Attack Playbook（攻击预定步骤和策略）。将攻击目标转向医疗保健、公用事业、制造业和金融业等关键基础设施行业，试图挖掘成功入侵后可对社会产生重大不利影响的目標。



**趋势 2: Oday 威胁更易获利。**  
Fortinet 预测许多 Oday 漏洞不会被公开披露。这意味着安全团队需时刻保持高度警惕，沉着布防汹涌而来的 Oday 漏洞攻击。与此同时 CaaS 社区将出现“Oday 经纪人”，即一类在暗网上向多个买家兜售 Oday 漏洞的网络犯罪集团。“Oday 经纪人”的兴起将成为网络犯罪分子扩展攻势的有效路径，并通过更协同配合的攻击活动挖掘更广泛的攻击面。

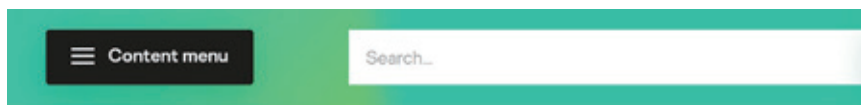
**趋势 3: 内部威胁持续上升。**网络犯罪分子可轻易使用生成式 AI，克隆高管或授信人员的声音，继而利用这些伪造录音，迫使毫无戒心的目标执行命令、泄露密码或数据甚至进行资金转账。Fortinet 预测，招募即服务模式将发展为下一个新趋势，帮助攻击者获得更多信息以分析其潜在攻击目标。

**趋势 4: 事件驱动成为新一波攻击浪潮。**2024 年攻击者将聚焦更具针对性和事件驱动性的攻击机遇。例如，2024 年巴黎奥运会，与会者和观众可能遭遇来自“铁粉”的骗局轰炸。随着各大赛事越来越依赖各项技术进行比赛计时、赛事管理和转播，相关赛事系统可能沦为攻击者的靶标。

**趋势 5: 缩小 TTP 攻击范围。**攻击者将不可避免地继续扩大其用以入侵目标的策略、技术和战术 (TTP) 集。然而，通过缩小攻击范围并找到破坏这些活动的方法，防御者可以抢占先机。

## 卡斯基：人工智能将给网络犯罪带来新变革

卡斯基公司的安全研究与分析团队对 2024 年高级威胁 (APT) 攻击的发展趋势进行了展望和预测。研



## Advanced threat predictions for 2024

KASPERSKY SECURITY BULLETIN

14 NOV 2023

15 minute read



### // AUTHORS

究认为，现有的 APT 攻击技术不会淘汰，在人工智能、系统入侵和智能家居等领域还可能出现新的技术应用。与此同时，新的僵尸网络和 rootkits 会出现，黑客雇佣服务和供应链攻击会增加，这些都属于网络罪犯攻击方式的变革。

据卡斯基的观察，APT 攻击者可能会扩大他们的监视范围，以囊括更多智能家居设备，像智能摄像头和联网汽车系统。攻击者对此感兴趣是因为这些设备通常不受控制，没有更新或补丁，且容易受到错误配置的影响。

随着地缘政治紧张局势加剧，国家支持的网络攻击数量也有可能在未来一年激增。这些攻击可能会导致数据被盗或被加密、IT 基础设施损毁、长期的间谍活动和网络破坏活动。

另一个值得注意的趋势是黑客行动主义，卡斯基认为，黑客行动主义活动可能会增加，既具有破坏性，又旨在传播虚假信息，从而导致不必要的调查及 SoC 分析师和网络安全研究人员随后产生的警报疲劳。

生成式人工智能工具有助于鱼叉式网络钓鱼电子邮件内容的大规模生产。因此卡斯基预计，攻击者未来会开发新的方法来实现网络间谍活动的自动化。一种方法是自动收集与受害者有关各种线上信息，包括社交媒体、网站等。

目前，雇佣黑客组织的服务已超越网络间谍，延伸到商业间谍活动，可能收集竞争对手的并购、扩张、财务和客户信息。卡斯基预测，这种趋势在全球范围内蓬勃发展，预计将在明年继续扩大。一些 APT 集团可能扩大业务以产生收入并支持成员活动。

## Google：安全领域将进入惨烈“大模型作战”阶段

谷歌发布的 2024 年云安全预测报告指出，新一年恶意生成式 AI 的流



行将引发大规模网络攻击活动。网络安全领域将进入惨烈的“大模型作战”阶段，并深刻地改变安全运营、云安全、黑客与网络犯罪模式、政治选举、巴黎奥运会和关键基础设施防护。

**生成式 AI 将被大规模用于网络钓鱼和虚假信息传播：**2024 年，AI 和大型语言模型将被广泛用于提高钓鱼邮件和社会工程攻击的专业化水平。攻击内容更加难以辨别，且攻击者能够利用 AI 工具实施大规模攻击。与此同时，生成式 AI 将被攻击者用于大规模创建虚假新闻和深度伪造内容，可能影响主流新闻，并降低公众对新闻和在线信息的信任。

**美国总统大选将遭受网络攻击：**2024 年是多国大选年，国家级和其他黑客组织将发动各种网络攻击活动，包括针对选举系统的间谍行为、舆情操弄、在社交媒体上冒充总统候选人发布虚假内容，以及针对选民本身的信息操作。

**将发生针对太空基础设施的攻击：**乌克兰的局势表明了地缘军事冲突对太空技术的高度依赖。预计 2024 年将有国家支持的黑客组织全方位地利用计算机网络开发能力，侵入太空基

预计 2024 年将有国家支持的黑客组织全方位地利用计算机网络开发能力，侵入太空基础设施及相关地面支持基础设施和通信渠道。

基础设施及相关地面支持基础设施和通信渠道。

**移动网络犯罪日益普及：**预计2024年大量网络犯罪分子或电诈人员将采用全新的社交工程策略，例如，伪造家政服务信息、假社交媒体账户、银行或政府官员的信息，以及伪造的弹出警报，诱骗受害者在其移动设备上安装恶意应用。

**2024年奥运会扩大巴黎的攻击面：**预计在2024年巴黎夏季奥运会期间，网络犯罪分子将瞄准售票系统和商品，通过大量的网络钓鱼活动窃取财务信息或凭证，公共机构和银行需要保持警惕。

**网络安全保费趋于稳定：**网络安全保险市场以其波动性而闻名。过去几年，由于安全风险不断累积，网络安全保险费不断上涨且保险覆盖范围缩小。2024年，随着网络安全保险市场的竞争加剧，网络安全保险费用将趋于稳定，承保范围扩大。

## Gartner：安全将成为驱动企业业务增长手段

Gartner发布的《2024年及未来中国网络安全重要趋势》主要包括以业务为中心的安全投资、网络安全判断力、零信任采用、网络安全平台整合、威胁暴露面管理、网络韧性、身份优先安全等内容。

Gartner强调，企业机构不应将安全视为维持业务运营所必需但又会造成不便的因素，而应将其视为业务的赋能因素，并据此开展工作。这一转变使企业机构能够迅速占据有利地位。

零信任曾是近年来炒作热度最高的技术之一，其中疫情和数字化进程对零信任落地有着很大帮助。Gartner

预计在2024年巴黎夏季奥运会期间，网络犯罪分子将瞄准售票系统和商品，通过大量的网络钓鱼活动窃取财务信息或凭证。

将零信任定义为安全范式，可明确识别用户和设备，并授予其适当的访问权限，以便企业能够以最小的摩擦进行运营，同时降低风险。

**持续威胁暴露面管理（CTEM）**既是Gartner认为的未来网络安全重要趋势，也是其认定的2024企业机构需要探索的十大战略技术之一。CTEM结合了攻击者和防御者的视角，最大限度地减少企业当前和未来面临的

的威胁。采用CTEM项目的企业机构会使用工具来记录资产和漏洞、模拟或测试攻击，同时利用其他形式的态势评估流程和技术。

**网络安全平台整合**已连续多年出现在Gartner对未来的趋势预测当中。Gartner认为，精简供应商数量后，企业机构可利用数量更少的产品降低运营复杂性，获得更多功能，但也可能导致风险集中、价格更高。虽然存在这种顾虑，但是企业机构依然有对供应商进行整合和集成的需求。

**身份安全**是Gartner最近几年来频繁提及的重要未来趋势之一：Gartner认为，数字身份的应用越来越广泛，用户的个人信息不仅只属于他们自己了，而是被广泛应用于多个组织、系统、算法和智能设备中。如何管理这些设备和工作的可信身份？这给企业机构带来了一项新的挑战。安



大事记

## 香港科技园与奇安信集团签署合作备忘录 将在港建设国际研发中心

12月15日，香港科技园公司（科技园公司）与奇安信科技集团股份有限公司（奇安信）在香港签署合作备忘录。奇安信将落户香港科学园，并设立国际研发中心，成为园区规模最大的网络安全企业，双方将携手建设香港成为国际创新科技中心。

奇安信国际研发中心将以终端安全、电子资料取证和网络安全管理服务营运平台为重点领域，并开展包括网络安全技术研究、网络安全检测及实验室建设、网络安全人才培养、网络安全竞赛等业务，务求为政府、公营机构、金融业、教育、医疗及交通运输等行业提供更加优质的网络安全服务。



## 国际化业务新突破 奇安信与四家港企签署合作协议

12月15日，奇安信在香港与华润创业、中国联通国际、



德勤中国、香港电讯四家在港企业签署合作协议。根据协议，奇安信与四家在港企业将在创新研发、数据安全、服务保障、生态合作等领域展开全面深入的合作，共同为香港科技创新、智慧城市、数字经济发展助力。



## 齐向东：从五个方向推动“内生安全”理念落地

12月14日，网络安全技术论坛 2023 在香港会展中心举办。香港特别行政区创新科技及工业局局长孙东，香港互



联网注册管理有限公司主席陈细明，全国政协委员、全国工商联副主席、奇安信集团董事长齐向东及多家网络安全、数字科技企业代表参会，共同探讨如何加强网络安全建设，提升香港整体应对网络攻击的防御及复原能力。

齐向东在演讲中表示，推动数字经济发展，建设智慧香港，必须构建符合时代要求的网络安全能力，安全建设视角也应该从外部向内部转化。要做好“盘家底、建系统、抓运营”三个重点工作，从五个方向推动内生安全理念落地，构建无处不在的网络安全“免疫力”。



### 齐向东连任中国网络空间安全协会副理事长

12月13日，中国网络空间安全协会召开第二届理事会第一次会议，中央宣传部副部长、中央网信办主任、国家网信办主任庄荣文出席会议并讲话。中央网信办副主任、国家



网信办副主任王京涛，第十四届全国政协委员、经济委员会委员赵泽良，中国科学院院士冯登国出席会议。会议选举赵泽良担任第二届理事会理事长，王小云、王芸、卢卫、冯登国、齐向东等担任副理事长，郝晓伟担任秘书长。

2016年，中国网络空间安全协会成立，齐向东担任中国网络空间安全协会第一届副理事长。在过去的七年里，他一直积极响应协会号召，参与各项工作，为推动我国网络空间安全建设贡献力量。此次连任，齐向东表示，将继续发挥副理事长单位的责任与义务，着眼于数字经济发展过程中产生的新技术、新风险、新挑战，持续参与中国网络空间安全协会的各项工 作，积极发挥企业在网络安全领域的优势力量，引领网络安全行业高质量发展，为中国式现代化建设保驾护航。

### 浪潮集团董事长邹庆忠一行到访奇安信安全中心

12月11日，浪潮集团党委书记、董事长邹庆忠一行到访奇安信安全中心。在奇安信集团党委书记、董事长齐向东的陪同下，邹庆忠一行先后参观了奇安信安全中心展厅、工控实验室、司法鉴定所、车联网实验室、网络安全保障指挥中心等地，并就工业互联网、云计算服务等领域进行了交流。



## 清华大学创新领军工程博士班师生到访奇安信

12月10日，清华大学国家卓越工程师学院创新领军工程博士23级1班师生到访奇安信集团安全中心开展访学调研活动，并与奇安信集团副总裁陈华平围绕奇安信发展历程、网络安全产业前沿趋势及新环境下面临的新挑战等话题进行了分享交流。



## 齐向东：用“四道防线”筑牢数字政府安全根基

12月8日，第二届数字政府建设峰会暨“数字湾区”



发展论坛网络与信息安全论坛在广州举行。广东省省委常委、常务副省长张虎，广东省通信管理局党组书记、局长蔡立志，中山市市长、市委副书记肖展欣，中国工程院院士方滨兴，中国工程院院士沈昌祥，全国政协委员、全国工商联副主席、奇安信集团董事长齐向东等主管领导和业内专家出席，共同探讨数字政府网络安全治理之道，护航数字政府高质量发展。

齐向东在主题演讲中表示，“三重三轻”是数字政府安全建设的突出短板。要坚持以内生为本，确保业务安全和网络安全合一，确保业务持续稳定，用“四道防线”为数字政府安全建设保驾护航。

## 吴云坤：从业务出发构建安全防护体系

面对网络空间新的压力和挑战，如何将网络安全与数字业务相结合，以切实保护数字化业务价值链？在12月8日举行的第三届网络空间内生安全发展大会主论坛上，奇安信集团总裁吴云坤提出了新的解决思路：转变思维和方法，以内生为本，从业务出发构建安全防护体系。

吴云坤表示，奇安信希望与更多的行业客户一起，从业务视角出发，共同开展行业安全研究，运用系统工程的方法将安全架构与业务架构相融合，以及通过具有行业特色科创装置来开展业务内生安全方案的验证，从而提供真正适合行业数字化业务的安全体系构建。



## 紫金山实验室与奇安信集团达成战略合作

12月8日，在南京市委网信办、紫金山实验室和中国通信学会主办的第三届网络空间内生安全发展大会上，紫金山实验室与奇安信集团签署了战略合作协议，双方将共同建设“紫金山-奇安信网络安全研究中心”，并在网络安全领域开展深入合作，积极推进成果转化落地，为网络强国和数字中国战略安全助力。



为进一步增强内生安全人才培养与知识体系共建，会上还发起了“五色石”伙伴计划。该计划由内生安全联盟发起，紫金山实验室牵头，联合东南大学等高校及奇安信等企业，共同构建“自主知识、教育培养、实践实训、评价认证、意识推广”五大体系，把内生安全理论、设计安全方法嵌入开发者培养过程。



## 奇安信集团入选教育部 2023 年供需对接就业育人项目企业名单

12月7日，教育部高校学生司专家组发布《教育部高校学生司关于公布第三期供需对接就业育人项目申报指南的函》，奇安信集团申报的“定向人才培养培训项目、就业实习基地项目、人力资源提升项目”3大类项目成功入围。

奇安信集团将在教育部的指导下，开展供需对接就业育人项目，旨在深化产教融合，全面提升高校大学生就业创业能力和质量，推动高校人才培养与就业有机联动、人才供需有效对接。拟设立定向人才培养培训项目 30 项，就业实习基地项目 30 项，人力资源提升项目 25 项。

## 吴云坤出席 2023 电力行业信息化年会

12月7日，2023 电力行业信息化年会在南京召开，来自电网公司、发电集团、产业集团、设计科研单位、高等院校、ICT 公司、网络安全等业界专家应邀参会并做演讲。奇安信集团总裁吴云坤受邀出席并发表主题演讲，他指出，数字化时代关键基础设施的安全防护需要新思维和新方法。

他还表示，数字化的安全保障，需要用系统工程方法体系化构建安全能力，专注于系统整体设计和应用。从网络安全问题的整体性出发和审视，将问题的所有方面和变量都考虑在内，梳理其相互依赖关系，并达到“涌现”的效果。



## 齐子昕出席第五届“一带一路”女性论坛：青年领导力推动科技创新再提速

第五届“一带一路”女性论坛7日在三亚开幕。论坛以“她力量：共建·共享美好生活”为主题，多国驻华使馆使节、企业代表等约400人受邀参会。奇安信集团副总裁、奇安信公益基金会荣誉理事长齐子昕出席此次论坛。

她表示，青年领导力是塑造未来社会的重要力量，不仅体现在科技创新领域，更体现在对社会问题的关注、公益意识的培养上。她还提出，青年朋友是最富行动力、好奇心和热情的一群人，在科技创新上有天然优势。同时，还要汇聚更多青年领导力，推动公益事业发展。

## 吴云坤：创新思维和技术 构建保密安全体系

近日，以“深化保密科技应用 推动保密创新发展”为主题的2023保密科技产业发展与应用交流会暨产品博览会在苏州举行，奇安信集团受邀出席。

在“树立动态综合防护理念，应对网络安全风险挑战”专题交流会上，奇安信集团总裁吴云坤提出，针对当前保密管理工作的新要求、新趋势，安全保密思路和保密技术能力都需要进行改变和创新，构建保密行业的新生态圈，全面有效支持国家保密工作。



## 齐向东担任京津冀企业家联盟主席

12月6日，京津冀企业家联盟成立大会暨第一次全体理事会议在京举行。中央统战部副部长、全国工商联党组书记徐乐江出席会议并讲话；北京市委常委、统战部部长杨晋柏，天津市委常委、统战部部长冀国强，河北省常委、统战部部长夏延军出席会议并致辞；北京市政协副主席、市工商联主席燕瑛出席会议并发布京津冀企业家联盟“同心工程”行动；北京市委统战部副部长、市工商联党组书记赵玉金主持会议。

大会公布了联盟第一次全体理事会议选举结果，全国政协委员、全国工商联副主席、奇安信集团董事长齐向东当选联盟首届轮值主席。



## 2023年金砖国家新工业革命技术与治理卓越人才培训班在奇安信举办

12月5日，2023年金砖国家新工业革命技术与治理卓



越人才培训班到奇安信开展培训、座谈活动。本期培训班由金砖国家新工业革命伙伴关系创新基地主办，厦门大学、中国信息通信研究院承办，共有来自 21 个国家和地区的 20 余名官员参加。

## 南水北调集团联合奇安信牵头的水网安全融合工程创新中心正式揭牌

在 12 月 5 日的世界 5G 大会上，由中国南水北调集团水网智慧科技有限公司、奇安信科技集团股份有限公司联合牵头建设的“水网安全融合工程创新中心”正式揭牌。

今年 9 月，南水北调集团联合奇安信等 12 单位共同成立水网数字化产业链创新联盟，此次水网安全融合工程创新中心的揭牌，标志着我国水网数字化建设在网络安全高质量发展方面迈出了新的一步。



## 奇安信中标某有色金属集团态势感知平台项目

近日，奇安信中标某有色金属集团态势感知平台项目，涵盖态势感知与安全运营平台（简称“NGSOC”）、远程运营服务、天擎（终端安全管理系统）、安全准入、智慧防火墙等安全产品。该项目的实施，为奇安信在有色金属及非金属产业树立了新的标杆案例，更为行业用户安全运营建设提供非常重要的参考价值。

## 上海公安学院侦查系与奇安盘古战略合作签约

近日，上海公安学院侦查系与奇安盘古战略合作签约——暨“产学研合作基地”揭牌仪式在奇安信上海总部举行。未来，奇安盘古与上海公安学院将共同围绕新型犯罪侦查、互联网取证等前沿技术，按照侦查学、刑事科学技术专业人才培养目标，优化完善专业课程内容，从而实现产学研用的结合。



## 奇安信助力全国刑事技术技能大赛圆满落幕

11 月 21 日至 25 日，第三届全国刑事技能大赛决赛在中国人民公安大学圆满落幕。大赛由公安部、中华全国总工会主办，中国人民公安大学协办，来自全国公安机关刑侦部门从事案件现场勘查和检验鉴定工作的 160 名优秀刑事技术人才组成 32 支队伍参加决赛。

作为国内领先的网络安全企业，奇安信集团受到公安部刑事侦查局的信任与委托，为本次技能大赛提供网络安全防护装备，同时为电子物证方向赛道提供专项支持，保障本次技能大赛圆满成功。

## 奇安信集团与联通集团签署共链行动产业链生态合作协议

11 月 21 日，由中国联通联合中国工业经济联合会举办的网络安全现代产业链共链行动计划暨战新共创启航大会在

京举行。奇安信集团总裁吴云坤做《融入产业链，共融共创网络安全保障能力》主题演讲，分享了奇安信与中国联通在网络安全领域的合作经验与成果，并与中国联通签署共链行动产业链生态合作协议。

根据协议，联通集团与奇安信集团将在通信网络及新型基础设施建设领域、数字中国及数字化转型建设、数字安全能力建设，以及产业生态合作等方面展开深入合作。围绕双方在各自领域的核心能力优势，共同为解决“安全响应”的卡脖子问题探索创新之路，共同建立世界领先的数字安全能力体系和方法论，共同打造产业链融通发展新模式。



## 北京网神洞鉴入选北京法院对外委托专业机构备选名册

近期，北京法院对外委托专业机构备选名册的入围机构名单正式公布，奇安信旗下的北京网神洞鉴司法鉴定所荣幸入选。这一成绩不仅标志着北京网神洞鉴在电子数据司法鉴定领域的卓越实力和专业服务获得了法院体系的高度认可，也预示着其在推动法律公正和保护人民权益方面将发挥更加重要的作用。

## 圆满完成首届学青会网络安全保障任务

11月15日，第一届全国学生（青年）运动会（简称“学

青会”）在广西南宁落下帷幕。作为本届学青会“大家庭”的一分子，奇安信组织了一支数十人的网络安全专家队伍，圆满完成了本届学青会的网络安全保障任务，为学青会的成功举办做出了重要贡献。

截至目前，奇安信已完成2022北京冬奥会和冬残奥会、建党100周年、国庆70周年、全国两会、春晚、中非合作论坛、上合组织成员国峰会等国家级网络安全保障任务，用自己的能力和行动捍卫着国家和企业的网络安全。

## 奇安信中标华晨宝马网络安全情报平台项目

近日，奇安信中标华晨宝马网络安全情报平台项目，中标产品包括安全网络安全情报平台（TIP）、网络安全漏洞情报订阅、高级咨询服务等。

未来，奇安信将为华晨宝马提供高质量的网络安全情报分析服务，赋能现有安全大数据平台，并为安全运营团队的事件研判分析、响应处置等提供能力支撑。

## 荣誉墙

## 奇安信 NGSOC 荣获“首届红数麟杯数字化创新大赛百强成果”奖

近日，由大湾区中央企业数字化协同创新联盟主办，粤港澳大湾区中央企业承办的央国企数字化转型分论坛暨第二届中央企业数字化转型峰会在深圳市召开。会议期间，大湾区中央企业数字化协同创新联盟发布了首届红数麟杯数字化创新成果大赛成果，奇安信态势感知与安全运营平台（NGSOC）从409个项目中脱颖而出，荣获“首届红数麟杯数字化创新大赛百强成果”奖。

## 奇安信获得国家级数据安全服务资质

12月15日，中国信息安全测评中心对外公布了国内首批数据安全服务一级资质名单。奇安信凭借在数据安全服务领域的技术研发、流程管理及人才积累等方面的综合实力，成为国内首批获得此项资质的企业。



至此，奇安信已获得“安全工程类三级”“安全开发类二级”“风险评估类二级”“云计算安全类一级”“安全运营类一级”“数据安全类一级”六个方向的国家信息安全测评信息安全服务资质证书，均为最高级别。

## 奇安信国企云安全案例获“2023数字化应用场景十佳解决方案”

12月15日，2023中关村数字经济产业联盟会员代表大会暨数字经济高质量发展论坛在京举行，会上发布了《2023全国数字经济典型场景与解决方案》研究报告并举行了颁奖仪式。凭借国企云安全方案中的技术体系和服务能力的出色表现，奇安信集团“国企云安全案例”获评2023数字化应用场景十佳解决方案。



## 奇安信云原生安全取得重大突破 成国内首家通过CASB权威检测厂商



近日，奇安信网络云访问安全代理系统(CASB, Cloud Access Security Broker)在功能、性能、兼容性、易用性、可靠性、安全性等方面通过中国泰尔实验室检测，获得由泰尔实验室、中国信通院、网络安全卓越验证示范中心联合颁发的“云(原生)安全产品检验证书”，是国内首个通过权威机构检测的CASB产品，充分彰显奇安信在云原生安全领域的深厚技术实力。

## 奇安信获评2023工业信息安全监测应急优秀支撑单位

12月5日，由国家工业信息安全发展研究中心主办的第五届国际工业领域网络安全应急大会在京召开。大会为过去一年来优秀的工业信息安全监测应急支撑单位举行颁奖仪式。奇安信集团被国家工业信息安全发展研究中心授予“2023年工业信息安全监测应急优秀支撑单位”。



## 奇安信入选 SSE 权威报告代表厂商

近日，全球知名的独立研究咨询公司 Forrester 发布 SSE (Security Service Edge 安全服务边缘) 全球报告《The Security Service Edge Solutions Landscape》，报告中，将奇安信纳入了 SSE 领域的代表性供应商之列。充分彰显奇安信在云安全领域深厚的技术积累和市场认可。

## 奇安天盾荣获中国网络安全与信息产业“金智奖”优秀产品

近日，2022—2023 年年度中国网络安全与信息产业“金智奖”获奖名单正式公布。凭借风险能看清、内鬼能管好、攻击能防住的体系化数据安全能力，奇安信集团数据安全产品“奇安天盾数据安全保护系统”从多款产品中脱颖而出，荣获年度优秀产品。



## 奇安信连续 3 年蝉联中国网络安全 100 强榜首

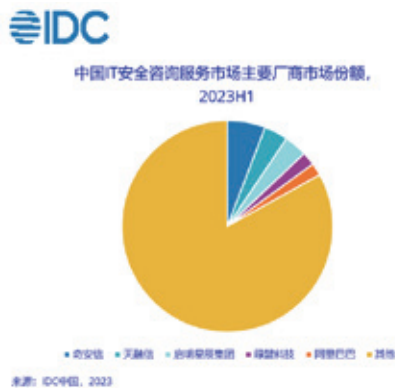
12月1日，国内网络安全媒体安全牛发布第十一版《中国网络安全企业 100 强》。在申报的 300 余家安全厂商中，

奇安信以 90.60 的总分，连续三年获得中国网络安全 100 强榜首，并在企业经营、行业应用等维度均位列第一，充分体现了网络安全龙头企业的整体竞争实力。



## 双细分领域第一！奇安信稳居国内安全服务市场头名

近日，全球领先的 IT 市场研究和咨询公司 IDC 发布了





《2023 上半年中国 IT 安全服务市场份额》（以下简称《报告》）。《报告》显示，奇安信分别以 5.8% 和 10.5% 的市场份额，位列安全咨询服务和托管安全服务两大细分领域第一。另据 IDC 数据显示，奇安信以 4.98% 的市场份额，同样拿下了 2023 上半年国内安全服务市场头名。



### 奇安信集团入选首批可信数据空间应用解决方案供应商

11月26日，由工业互联网产业联盟主办，中国信通院、华为云等承办的 2023 全球数商大会数据基础设施暨可信数据空间创新发展论坛上，发布了首批 15 家可信数据空间应



用解决方案供应商和国内首个可信数据空间标准《可信数据空间系统测试规范》。经过专家组的资格审查、专家评审等环节，奇安信集团入选首批可信数据空间应用解决方案供应商。

### 奇安信摘得中国智能交通创新挑战赛一等奖

11月19日，由中国智能交通协会主办，以“创新 协同 可持续发展”为主题的 2023 中国智能交通大会在厦门闭幕。2023 中国智能交通创新挑战赛为大会活动的重要组成部分，是搭建智能交通行业内创新成果展示平台。

奇安信集团携手深圳市城市交通规划设计研究中心股份有限公司打造的“基于机器学习及指纹建模技术的车路协同路侧安全可信防护方案”，成功摘得赛题四——智能网联汽车网络与数据安全赛题一等奖。



### 车云一体！奇安信获评车联网安全代表厂商

近日，安全牛发布了《车联网安全技术应用研究报告》（以下简称《报告》）。凭借车-云一体化持续风险监测方案，奇安信成功入选该报告，并被评选为车联网安全代表厂商。

目前，奇安信车联网安全产品、解决方案及配套安全服务已经得到多家国内领先车企的认可。随着奇安信车联网安

全总部在重庆市两江新区的投入使用，将不断去积累更多的安全模型、威胁模型、情报库、漏洞库，让安全漏洞和风险发现更加及时，响应更加快速。

## 2023 北京企业百强榜单出炉 奇安信集团连续两年登榜

近日，由北京市人民政府、天津市人民政府、河北省人民政府、中国国际贸易促进委员会共同主办的 2023 年京津冀产业链供应链大会在北京举行。北京企业联合会、北京市企业家协会在会上发布了 2023 北京企业百强榜及其发展报告。凭借扎实的科技创新能力和领先的企业综合实力，奇安信集团连续两年入选“北京企业百强”“北京高精尖企业百强”“北京数字经济企业百强”三大榜单。

### 社会责任

## 和美乡村计划新篇章 三县五地近万村民将受益

近期，奇安信公益基金会“和美乡村计划”与河北盐山县、内蒙古敖汉旗和贵州织金县签署捐赠协议，向三县（旗）5 地提供支持，开展包括乡村电商发展支持、乡村环境治理、乡村基础设施建设在内的支持，预计将帮扶近万名村民受益。

至此，奇安信基金会 2023 年年度“和美乡村计划”支持项目全部顺利落地，共计支持北京、广东、安徽、河北、内蒙、贵州等多地乡村建设，累计受益乡村居民、学生 3 万余人。

## 学先进、访榜样 心安助农·巴林左旗项目赴四川考察学习

为推动“心安助农·巴林左旗乡村振兴项目”深入开展，

切实帮助当地牧户深入发展，12 月 8 日—13 日，北京奇安信公益基金会牵头，委托北京农禾之家农村发展基金会组织，邀请中国社会科学院杨团、刘建进研究员指导，组织巴林左旗乌兰达坝苏木党委政府相关人员、嘎查书记、为农服务公司代表等 12 名骨干，赴四川战旗村、仪陇县开展考察学习交流。

“心安助农·巴林左旗乡村振兴项目”是响应全国工商联对口帮扶乡村振兴重点帮扶县的号召，旨在探索适合当地的乡村振兴路径和落地解决方案，由北京奇安信公益基金会发起，委托北京农禾之家执行，为期三年。项目组在实地调研的基础上，确定了乌兰达坝苏木作为试点乡镇。目前已深入苏木开展专家调研两次，并带领苏木团队外出考察经棚镇、战旗村、仪陇县等地进行学习，通过共创的方式，深入谋划未来发展规划。



## “心安助学”走进齐鲁 与山东科技大学等三所院校签署捐赠协议

近日，北京奇安信公益基金会与山东科技大学、青岛理工大学、青岛幼儿师范高等专科学校三所院校签署了捐赠协议，在三所院校设立奇安信奖助学金，帮助这三所院校有志于网络空间安全的学生创建安全、有保障的学习生活环境，改

善他们的学习和就业状况。

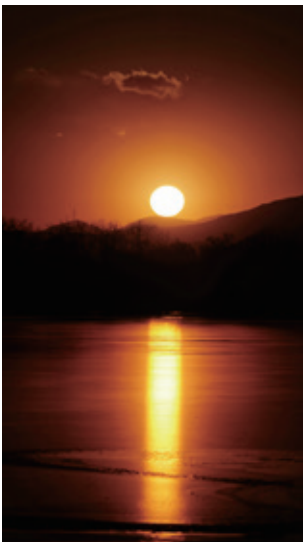


## 奇安信基金会积极开展扫雪铲冰志愿服务

12月13日起，北京出现明显降雪过程，给大地披上银装的同时也造成了道路积雪、结冰等现象，给道路交通和群众出行带来诸多不便及安全隐患。

为积极应对积雪对出行造成的困难，响应北京市志愿服务联合会倡议，保证降雪后车辆、行人出行安全，确保道路干净整洁，北京奇安信公益基金会联合奇安信集团党委迅速号召组织志愿者十余人，到西城区展览路街道分配的街区开展扫雪铲冰志愿服务工作。





一夜银装裹，雪落满京城——这是多少人期待的冬日画面。本次冬日首场降雪终于如约而至，颐和园的雪后景色更是美得如诗如画，雄伟壮丽。

军团技术支持部 杨许明



# 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。

规划一步快



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

# 新书发布

## 内生安全权威解读

19支团队、37位专家倾力打造  
政企“十四五”网络安全规划必读书籍



什么是内生安全

内生安全从何而来

为什么要内生安全

内生安全如何落地

新一代网络安全框架

“十工五任”建设要点

扫描二维码  
专享内购价



奇安信连续三年位居  
“中国网安产业竞争力50强”  
第一名



6月20日，中国网络安全产业联盟（CCIA）  
公布“2023年中国网安产业竞争力50强”榜单，  
凭借扎实的技术实力和领先的市场表现，  
奇安信连续三年高居榜单第一名。



“2022年中国网安产业竞争力50强”榜单

TOP15 公司名称

- 1 奇安信科技集团股份有限公司
- 2 深信服科技股份有限公司
- 3 启明星辰信息技术集团股份有限公司
- 4 华为技术有限公司
- 5 天融信科技集团股份有限公司
- 6 绿盟科技集团股份有限公司
- 7 腾讯云计算（北京）有限责任公司
- 8 新华三技术有限公司
- 9 阿里云计算有限公司
- 10 杭州安恒信息技术股份有限公司
- 11 三六零数字安全科技集团有限公司
- 12 亚信安全科技股份有限公司
- 13 中电科网络安全科技股份有限公司
- 14 杭州迪普科技股份有限公司
- 15 山石网科通信技术股份有限公司