极牛网络安全通讯 • 社群期刊

2025 年 3 月 第 45 期

网安观察



P26
从2022到2024：两会“网络安全提案”的变迁

P17 两会代表聚焦AI与数据安全

P31 勒索攻击报告：威胁规模和复杂程度超过往年

P41 首席安全官权力悖论：为何责任越大权力越小？

第45期

2025年3月

CONTENTS 目录



安全态势

P4 | 强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》发布 04

P4 | 《网络安全标准实践指南——人工智能生成合成内容标识 服务提供者编码规则》发布

P5 | 《网络安全标准实践指南——个人信息保护合规审计专业机构服务能力要求》公开征求意见

P5 | 中共中央、国务院印发《国家突发事件总体应急预案》

P5 | 两部门印发《关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知》

P6 | 瑞士出台新规，关基设施遭遇网络攻击需在 24 小时内上报

P6 | 美国众议院通过法案，强制供应商设立漏洞披露计划

P7 | 美国 CISA 警告：美杜莎勒索软件已攻击超 300 家关键基础设施机构

P7 | 钓鱼攻击瞄准 DeepSeek 本地化部署场景，工信部漏洞平台发布预警

P8 | 日本电信巨头 NTT 遭网络攻击，近 2 万家企业客户采购数据泄露

P8 | 多个政府机构和企事业单位门户网站遭攻击，工信部漏洞平台发布预警

P9 | 菲律宾陆军遭网络攻击，上万名军人敏感信息或泄露

P9 | 警惕！国内企业部署大模型工具 ComfyUI 遭黑产入侵

P10 | 香港投资推广署遭勒索软件入侵，客户管理系统受影响

P10 | 知名交易所 14 亿美元数字货币被盗，损失金额创历史新高

P11 | Apache Tomcat 远程代码执行漏洞安全风险通告

P11 | 微软 3 月补丁日多个产品安全漏洞风险通告

P12 | Apache OFBiz 服务端模板注入漏洞安全风险通告

P12 | VMware ESXi 多个高危漏洞在野利用通告

P12 | 备战攻防演练：2025 年第一季度需要关注的高危漏洞合集



月度专题

聆听两会“网安声音”

2025 两会代表热议网络安全，AI 安全、数据安全成焦点。

2025 年全国两会期间，网络安全议题成为代表委员们热议的焦点。随着人工智能技术的广泛应用和数据要素的深度渗透，网络安全风险呈现出智能化、复杂化、全域化的新特征。两会代表围绕“人工智能安全”与“数据安全”两大核心领域，提出了系统性治理方案，为构建数字中国安全底座提供了重要思路。

P16

ONTENTS



专题报道

P26
从2022到2024：两会“网络安全提案”的变迁

P31
勒索攻击报告：威胁规模和复杂程度超过往年

P41
首席安全官的权力悖论： 为何责任越大权力越小?



第 4 5 期

《网安观察》编辑部

主办 极牛网

总 编 辑：陈鑫杰
总 顾 问：叶绍琛
副 总 编：王文彦
威胁情报主编：陈艇鑫
移动安全主编：蔡国兆
网安人才主编：林俊濠
涉网犯罪主编：胡铭凯
网安产业主编：张九史
网安态势主编：郑泽彬

公众号 小程序 网站

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

E m a i l：hi@geeknb.com
地 址：深圳市龙岗区天安云谷2栋2层
邮 编：518000
电 话：0755-33228862
印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

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

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



政策篇

国内，人工智能生成内容安全制度及配套规范积极推进。《人工智能生成合成内容标识办法》、强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》、《网络安全标准实践指南——人工智能生成合成内容标识 服务提供者编码规则》系列文件已发布；

国际上，关键基础设施安全备受关注。瑞士出台新规，关基设施遭遇网络攻击需在 24 小时内上报；美国会议员提出《太空基础设施法案》，将太空系统作为关基设施进行保护；美国众议院通过法案，强制政府供应商设立漏洞披露计划。

国内

强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》发布

3 月 15 日，全国网络安全标准化技术委员会网站公布了强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》（GB 45438-2025），于 2025 年 9 月 1 日同步实施。该文件规定了人工智能生成合成内容标识方法，适用于生成合成服务提供者和内容传播服务提供者开展人工智能生成合成内容标识活动。该文件支撑《人工智能生成合成内容标识办法》，对人工智能生成合成内容服务提供者与网络信息传播服务提供者，提出了内容标识方法的具体要求。

《网络安全标准实践指南——人工智能生成合成内容标识 服务提供者编码规则》发布

3 月 14 日，全国网络安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——人工智能生成合成内容标识 服务提供者编码规则》。该文件给出了人工智能生成合成内容服务提供者和网络信息内容传播服务提供者的编码结构和赋码规则，可为人工智能生成合成内容服务提供者和网络信息内容传播服务提供者，开展人工智能生成合成内容的文件元数据隐式标识活动提供参考。

四部门印发《人工智能生成合成内容标识办法》

3 月 14 日，国家互联网信息办公室、工业和信息化部、公安部、国家广播电视总局联合印发《人工智能生成合成内容标识办法》，于 2025 年 9 月 1 日实施。该文件共 14 条。《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》中提出了标识有关要求，该文件作为规范性文件，进一步细化标识的具体实施规范，明确了人工智能生成合成内容服务提供者、网络信息传播服务提供者、互联网应用程序分发平台的相关要求，重点解决“哪些是生成的”“谁生成的”“从哪里生成的”等问题，推动由生成到传播各环节的全流程安全管理。

十五部门印发《关于促进中小企业提升合规意识加强合规管理的指导意见》

3 月 13 日，工业和信息化部等 15 部门办公厅（秘书局、办公室、综合司）联合印发《关于促进中小企业提升合规意识加强合规管理的指导意见》，明确了 10 大合规管理重点领域，包括劳动用工合规、财税合规、网络和数据安全合规等。该文件要求，引导中小企业遵守网络安全、数据安全等方面法律法规，加强信息系统、网络、数据的安全防护和安全意识教育；制定实施数据安全合规管理制度，加强对数据的分

类分级和权限管理，加强人员管理和技术控制，履行重要数据识别备案、分级防护、风险评估等责任义务，防范并及时应对和处理数据泄露、篡改、丢失事件；重点梳理向第三方输出、共享、委托、提供数据，从第三方接受数据，处理个人信息及跨境传输数据等活动中的合规要求和风险，落实特定类型信息收集与使用合规义务，保护企业数据及个人信息安全。

《网络安全标准实践指南——个人信息保护合规审计 专业机构服务能力要求》公开征求意见

3 月 4 日，全国网络安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——个人信息保护合规审计专业机构服务能力要求（征求意见稿）》，现公开征求意见。该文件规定了专业机构开展个人信息保护合规审计服务的能力要求，包括基本条件、管理体系、技术能力、人员能力、场所与设备资源能力，适用于指导专业机构建设个人信息保护合规审计服务能力，也可为开展个人信息保护合规审计专业机构的认证提供依据，还可为个人信息处理者选择合规审计专业机构提供参考。

中共中央、国务院印发《国家突发事件总体应急预案》

2 月 25 日，中共中央、国务院印发了《国家突发事件总体应急预案》。该文件定义的突发事件，包括网络安全、网络数据安全、信息安全事件等事故灾难，中央网信办负责协调处理网络安全、网络数据安全与信息安全类突发事件。该文件要求，各地各有关部门应当完善监测网络，整合信息资源，加强对网络数据安全、人工智能安全等综合监测。

两部门印发《关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知》

2 月 28 日，工业和信息化部、市场监管总局联合印发《关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知》。该文件提出，推动构建智能网联汽车质量认证体系，围绕组合驾驶辅助系统的数据安全、网络安全、功能安全、预期功能安全等领域积极推行自愿性认证，服务智能网联汽车产业健康发展。该文件还要求，企业要落实智能网联汽车产品生产一致性和质量安全主体责任，持续确保汽车产品符合网络安全和密码应用安全、数据安全和个人信息保护等国家有关规定，严格履行 OTA 升级活动管理要求，规范营销宣传行为，健全产品售后服务管理体系。

《海南自由贸易港数据出境管理清单（负面清单）（2024 版）》发布

2 月 20 日，中共海南省委自贸港工作委员会办公室、海南省互联网信息办公室、海南省发展和改革委员会（海南省数据局）会同有关部门制定了《海南自由贸易港数据出境管理清单（负面清单）（2024 版）》，现正式印发。该文件主要针对五大重点领域进行分类管理，包括深海、航天、种业、旅游、免税商品零售业务。该文件覆盖 14 个具体业务场景，针对每个场景详细规定了数据子类、基本特征与描述，同时明确了适用范围、数据定义和管理要求，构建了从资源勘探、科研监测到经营管理的全方位数据治理体系。

《科学数据安全分类分级指南》等 5 项国家标准发布

2 月 13 日，国家标准化管理委员会 1 月 24 日在官方网站发布了《中华人民共和国国家标准公告（2025 年第 2 号）》，正式批准了《科学数据安全分类分级指南》《科学数据溯源元数据》《科学数据安全要求通则》《科学数据安全审计要求》《科学数据权益保护系列要求》等 5 项国家标准。该系列标准的正式发布实施，将进一步规范科学数据的管理与保护，在充分保障科学数据安全的基础上最大程度提升数据开放共享水平。遵循并实施这些标准将对《科学数据管理办法》和《数据安全法》等相关法律法规的贯彻落实产生积极影响，并将对促进科学研究的深度发展和创新活动的推进发挥至关重要的作用。

国际

瑞士出台新规，关基设施遭遇网络攻击需在 24 小时内上报

3 月 7 日，瑞士国家网络安全中心（NCSC）宣布了一项新的报告义务规定，要求国内关键基础设施组织在发现网络攻击后 24 小时内向该机构报告。根据公告，关键基础设施组织发现网络攻击后，首次报告需在 24 小时内完成，详细报告需在后续 14 天内完成，未遵守规定最高可罚约 80 万元。必须报告的网络攻击类型包括：危及关键基础设施运营的网络攻击；数据篡改、加密或窃取；勒索、威胁和胁迫行为；在系统中安装恶意软件；未授权访问系统。该规定通过《信息安全法》修订案引入，并将于 2025 年 4 月 1 日正式生效，适用于公用事业机构、地方政府和交通运输组织等关键服务提供商。

美国众议院通过法案，强制政府供应商设立漏洞披露计划

3 月 3 日，美国众议院通过《2025 年联邦承包商网络安全漏洞消减法案》，要求联邦承包商强制实施漏洞披露政策（VDP），并遵循与联邦机构一致的漏洞披露要求，以加快漏洞消减目标的实现。该法案要求，美国管理与预算办公室须与网络安全和基础设施安全局、国家网络总监办公室、国家标准与技术研究院（NIST）及其他相关机构协作，监督《联邦采购法规》的更新工作，确保联邦承包商实施符合 NIST 漏洞披露指南的漏洞披露政策。该法案还要求国防部长监督《国防联邦采购条例补充》的更新，以确保国防承包商同样执行类似的漏洞披露政策。

美国防信息系统局发布 2025—2027 财年数据战略

3 月 4 日，美国国防信息系统局（DISA）发布 2025—2027 财年数据战略，提供了全面的数据战略路线图，旨在优化网络、增强网络安全，并利用人工智能和机器学习技术来满足美国防部作战需求。根据该文件，DISA 计划强调数据治理的重要性，使国防网络数据和业务数据可操作化，并培养数据驱动的人才队伍，重点涉及加强数据架构和治理、集成高级分析、培育以数据为中心的文化三方面重点工作。该文件提出，要将数据视为战略资产予以保护，利用 DISA 零信任架构和数据目录实施安全控制，持续完善数据治理政策和标准，确保数据全生命周期的数据完整性、安全性与合规性。

欧洲委员会发布《欧盟网络安全危机管理蓝图》提案

2 月 24 日，欧洲委员会提出《欧盟网络安全危机管理蓝图》（网络蓝图）建议提案，旨在确保对大规模网络事件进行更加有效和高效地响应。该提案更新了欧盟网络安全危机管理的整体框架，明确了欧盟层面各个相关实体及网络的角色，并概述了它们在危机生命周期中的具体职能。这些职能包括：危机准备工作、共享态势感知、预测网络事件的能力、必要的检测工具以识别网络事件，以及应对和恢复这些事件所需的减缓、威慑与遏制手段。该提案还呼应即将出台的欧盟应急准备战略，并推动了安全通信与应对虚假信息的战略努力。

美国会议员提出《太空基础设施法案》，将太空系统作为关基设施进行保护

2 月 10 日，美国国会肯 · 卡尔弗特等 4 位两党议员联合提出了《太空基础设施法案》（H.R. 1154），要求将太空系统、服务和技术认定为关键基础设施，并采取必要措施加以保护，以确保太空资产的安全性与韧性。卡尔弗特表示：“随着我们的经济和重要通信系统愈加依赖太空系统和服务的支持，我们必须采取切实行动，增强防护以防范潜在威胁。”该法案目前已提交至美国众议院科学、太空与技术委员会审议。



事件篇

AI 应用火热之后网络威胁也不断增加，从训练数据到模型部署、应用使用等各个环节均发现风险隐患。OpenAI、DeepSeek 等使用的大型训练数据集暴露了约 1.2 万个有效的 API 密钥和密码，监管机构通报国内发现多个针对 DeepSeek 的仿冒手机木马和本地化部署钓鱼攻击样本，迪士尼也因员工尝鲜“AI 工具”导致 Slack 被入侵泄露了 4400 万条敏感信息。

美国 CISA 警告：美杜莎勒索软件已攻击超 300 家关键基础设施机构

3 月 12 日 Bleeping Computer 消息，美国 CISA、FBI 等最新报告警告称，截至 2025 年 2 月，美杜莎（Medusa）勒索软件攻击行动已经影响了超过 300 家美国关键基础设施机构，涉及医疗、教育、法律、保险、科技和制造业等多个领域。报告称，美杜莎组织在 2021 年 6 月首次被发现，2023 年开始活跃，据报道该组织曾攻击了美国多个校区、丰田金融等组织。CISA 公布了美杜莎攻击行动的 TT P 和 IoC 等攻击指标和缓解措施。

钓鱼攻击瞄准 DeepSeek 本地化部署场景，工信部漏洞平台发布预警

3 月 7 日网络安全威胁和漏洞信息共享平台消息，工业和信息化部网络安全威胁和漏洞信息共享平台（CSTIS）监测发现，攻击者针对大语言模型 DeepSeek 本地化部署场景实施钓鱼攻击，传播恶意程序，危害严重。攻击者通过“DeepSeek 本地部署”“深度求索”等高频关键词搜索引擎投毒，构建仿冒网站等方式，诱导用户下载伪造的 DeepSeek 本地部署工具包（如“ds 大模型安装助手”“deepseek_install”），传播 HackBrian RAT、Gh0st 和 FatalRAT 等木马程序。一旦被植入木马，攻击者可进一步控制用户服务器，导致窃取敏感信息、破坏系统数据，甚至入侵内部网络等严重危害。建议相关单位及用户优先通过官方渠道下载部署 DeepSeek，加强来源不明软件的识别与防范，谨慎下载未知来源的应用程序，并通过更新防病毒软件、实施全盘查杀等方式全面排查消除相关安全风险。

印度塔塔科技遭勒索攻击，1.4TB 敏感数据泄露

3 月 11 日 TechCrunch 消息，勒索软件组织 Hunters International 声称窃取了印度塔塔科技 1.4TB 内部数据，并在暗网门户上发布了部分数据。据称，该数据集有超 73 万份文档，包括员工个人信息、采购订单、客户合同等各类敏感数据。此前 1 月底，塔塔科技向印度证券交易所披露了勒索软件攻击事件，表示部分 IT 资产受到影响，但客户服务未受影响。目前尚不确定这两起事件是否为同一事件。塔塔科技是印度最大的集团企业塔塔集团的汽车工程业务子公司。

因 AWS S3 配置错误，美国 29 州 8.6 万名医疗工作者信息泄漏

3 月 11 日 The Register 消息，美国健康科技公司 ESHYFT 发生了一起严重的数据泄露事件，由于 AWS S3 存储桶配置错误，有超过 8.6 万名医疗工作者的敏感信息被公开暴露。安全研究员 Jeremiah Fowler 发现了这一事件，该存储桶暴露了约 108.8GB 的数据，涉及信息包括人脸照片、工作排班表、专业证书、医疗文件等个人身份信息，其中部分信息可能受到美国《健康保险流通与责任法案》（HIPAA）的保护。这些数据涉及来自 29 个州的医疗工作者，包括护士、护理助理等，给相关人员带来了巨大的隐私风险。

日本电信巨头 NTT 遭网络攻击，近 2 万家企业客户采购数据泄露

3 月 7 日 Bleeping Computer 消息，日本电信服务提供商 NTT 发布公告称，近 1.8 万家企业客户的信息在一起网络安全事件中遭到泄露。此次数据泄露事件于 2025 年 2 月初被发现，公司花费十余天时间完成应急处置，但黑客最初入侵 NTT 系统的确切时间尚未确定。NTT 透露，黑客入侵了“订单信息分发系统”，该系统存储了 17891 家企业客户的详细信息，但不涉及个人客户数据。可能被黑客窃取的数据包括：客户名称（注册合同名称）、客户代表姓名、合同编号、电话号码、电子邮件地址、物理地址、服务使用信息等。

多个政府机构和企事业单位门户网站遭攻击，工信部漏洞平台发布预警

3 月 7 日网络安全威胁和漏洞信息共享平台消息，工业和信息化部网络安全威胁和漏洞信息共享平台（CSTIS）监测发现，多个政府机构和企事业单位门户网站网页遭受攻击、篡改代码，导致违法违规信息传播、恶意链接推广、SEO 劫持和钓鱼攻击等严重危害。遭受攻击原因为网页存在安全漏洞，未严格校验上传文件格式和内容。恶意攻击者利用漏洞可上传恶意文件，植入非法链接，导致用户访问网站时被跳转到攻击者指定的恶意网站，诱导用户访问包含非法广告、钓鱼链接的网站或下载恶意代码、违法违规 App。建议各相关单位及个人加强网站网页的安全防护，强化风险防范，检查网站文件完整性，采取限制上传文件格式、严格校验文件内容、添加身份验证机制等安全措施，并做好应急响应，及时发现处置遭篡改网页代码。

VMware 虚拟机逃逸漏洞正被积极利用，国内公网暴露面最大

3 月 6 日 Bleeping Computer 消息，VMware 母公司博通 3 月 4 日向客户发布警告称，CVE-2025-22224 等 3 个 VMware ESXi 漏洞已遭在野利用。CVE-2025-22224 允许本地攻击者在拥有虚拟机客户机管理员权限的情况下逃离沙盒，并以 VMX 进程身份在宿主机上执行代码。据威胁监测平台 The Shadowserver Foundation 统计，全球近 4 万台服务器易受该漏洞影响，其中中国、法国、美国的受影响服务器数量位列前三，中国约 4400 台服务器存在风险。

业务系统被黑致客户数据泄露，美国知名连锁药房赔偿近 5000 万元

3 月 6 日 GovinfoSecurity 消息，美国知名连锁药房来爱德公司近日达成一项 680 万美元（约合人民币 4928 万元）的和解协议，以解决 2024 年 6 月发现的一起网络攻击事件引发的集体诉讼。来爱德此前公告称，一名攻击者“冒充公司员工，利用其业务凭据成功访问了部分业务系统。”攻击者窃取了 2017 年 6 月 6 日至 2018 年 7 月 30 日期间，客户购买或尝试购买商品的相关信息。被泄露的数据包括客户姓名、地址、出生日期和驾照号码，大约 220 万名客户受到影响。RansomHub 勒索软件团伙宣称对该事件负责。

泰勒演唱会门票遭黑客非法获取，牟利 600 万美元被捕

3 月 6 日 TheVerge 消息，美国纽约皇后区地方检察官办公室宣布，两名黑客因非法获取并转售超过 900 张泰勒·斯威夫特时代巡回演唱会及其他大型音乐会门票被捕。他们利用第三方售票平台 StubHub 的系统漏洞进行作案，通过伪造授权用户的身份，窃取门票的最终链接。这些链接随后被发送到该犯罪网络在纽约地区的同伙，这些同伙下载门票并在 StubHub 等平台上挂售。检方表示，如果罪名成立，嫌疑人可能面临 3~15 年的监禁。

AI 数据集泄露约 12000 个 API 密钥和密码，OpenAI、DeepSeek 等均使用

3 月 2 日 Bleeping Computer 消息，网络安全公司 Truffle Security 在对 Common Crawl 数据集 2024 年 12 月存档的 26.7 亿个网页的 400TB 数据进行扫描时，发现了 11908 个经过成功验证的密钥，涉及 AWS、MailChimp 和 WalkScore 等服务。这些密钥被开发人员硬编码，表明

LLM 有可能在不安全的代码基础上接受了训练。Common Crawl 是全球最大的开源网络数据集之一，由于该数据集体量庞大，许多人工智能项目可能至少在一定程度上依赖这些数字档案来训练大模型，其中包括 OpenAI、DeepSeek、Google 等公司的模型。



菲律宾陆军遭网络攻击，上万名军人敏感信息或泄露

2 月 27 日 The Record 消息，菲律宾陆军披露了一起网络攻击事件。此前有报道称，菲律宾本土黑客组织 Exodus Security 声称已成功入侵其系统，并窃取了 1 万名现役及退役军人的个人及军事敏感信息。菲陆军发言人 Louie Dema-ala 上校 26 日证实了该事件，并将其描述为一次“非法访问尝试”，但他强调，攻击已被迅速遏制。他未透露该黑客组织的名称，只表示已锁定其身份，目前尚未发现任何损害或数据泄露的迹象。



警惕！国内企业部署大模型工具 ComfyUI 遭黑产入侵

2 月 26 日百度安全消息，百度安全团队捕获到了一起针对大模型相关组件 ComfyUI 的攻击事件，该事件背后团伙已实际针对国内不少公网 ComfyUI 进行了入侵。据分析，攻击者利用 ComfyUI 用户错误配置问题，在无需认证的情况下进入到 ComfyUI 后台，同时利用后台模型加载功能安装攻击者提前上传在 Hugging Face 的投毒模型文件，以便利用模型加载时的 pickle 反序列化逻辑，控制受害者机器，进一步渗透目标内网。建议 ComfyUI 用户尽快排查是否受影响，并采取处置和安全加固措施。



因员工尝鲜“AI 工具”，迪士尼泄漏 4400 万条机密数据

2 月 26 日华尔街日报消息，迪士尼近期披露了去年的 Slack 数据泄露事件调查结果。据 报道，2024 年 2 月，迪士尼员工马修 · 范 · 安代尔使用家用电脑，通过 GitHub 下载了一款“免费 AI 图像生成工具”。这款表面正常的软件实则为恶意程序，黑客借此植入键盘记录木马，劫持了他存储所有密码的 1Password 管理器。更致命的是，安代尔的 1Password 账户未启用双因素认证，黑客获取主密码后提取了密码管理器中数百个账号口令。通过窃取的 Slack 会话 cookie，黑客直接登录其迪士尼内部账户，潜伏五个月后突然发难。2024 年 7 月，黑客团体 Nullbulge 在网上发布了超过 4400 万条 Slack 内部消息，包括迪士尼客户隐私信息、员工护照号码和主题公园及流媒体收入数据等。



英国关基单位南方水务因网络攻击损失超 4000 万元

2 月 26 日 Bleeping Computer 消息，英国南方水务（Southern Water）公司透露，2024 年 2 月发生的网络攻击，导致其支出达 450 万英镑（约合人民币 4127 万元）。大约一年前，南方水务曾宣布其遭遇了一次安全漏洞，当时公告称该漏洞未对公司运营、财务系统或客户服务系统造成影响。此次网络攻击是由臭名昭著的 Black Basta 勒索软件团伙实施的，该团伙以攻击关键基础设施而闻名。根据南方水务的财务报告，“为应对这一事件，我们聘请了外部网络安全专家和法律顾问，并通知了所有可能面临个人数据泄露风险的相关人员。应对此次安全事件的费用已达到 450 万英镑。”



全球大量门禁系统配置错误，导致数十万员工敏感信息暴露

2 月 25 日 Modat 消息，欧洲网络安全公司 Modat 发布文章警告，全球范围发现 4.9 万个配置错误的物理访问管理系统（AMS），导致数十万员工和组织敏感信息暴露在公网之下，涉及建筑、医疗、石油和政府等关键基础设施行业，凸显了现代企业安全防御中的致命漏洞。全球共有 4.9 万台暴露的 AMS 设备，其中大部分（16,678 台）位于意大利，其次是墨西哥（5940 台）和越南（5035 台）。这些系统通常用于管理员工的身份验证、门禁权限和生物识别数据，但因配置不当，敏感信息如个人身份详情、工作日程甚至生物特征数据被完全暴露。研究显示，攻击者可利用这些漏洞伪装成员工非法进入受限区域，或进行身份盗用。在极端情

况下，攻击者甚至能篡改员工档案，包括更换头像以假冒身份，或修改访问权限，监控员工活动轨迹。

香港投资推广署遭勒索软件入侵，客户管理系统受影响

2 月 24 日星岛环球网消息，香港投资推广署 23 日公布，于 22 日发现一起信息安全事故，涉及恶意勒索软件入侵部分电脑系统。初步显示受影响范围包括内部客户管理系统、内联网、部分投资推广署网站的运作（如经网站联络投资推广署、活动信息等）。投资推广署的公众服务则维持正常，公众可以继续透过电话热线、电邮或会面与投资推广署人员联络。至于事件是否涉及个人资料外泄及其影响范围，现仍在调查中。投资推广署发言人表示，该署在发现事件后已即时采取行动，加强系统的安全措施，防止进一步受到勒索软件入侵；并已即日按既定程序分别向警方报案、通知数字政策办公室，以及向个人资料私隐专员公署（私隐公署）和保安局通报事件，以策万全。

知名交易所 14 亿美元数字货币被盗，损失金额创历史新高

2 月 21 日 TechCrunch 消息，安全内参 2 月 22 日消息，国际加密货币交易所 Bybit 宣布，旗下一个离线钱包遭黑客攻击，401,346 个以太坊被盗，价值约 14 亿美元。这是迄今为止最大的加密货币盗窃案，超越了此前 Ronin Network 和 Poly Network 的黑客事件，分别损失 6.24 亿美元和 6.11 亿美元。Bybit 首席执行官周 Ben Zhou 称，黑客控制了公司一个未联网的“冷钱包”，将资金转移至在线钱包。尽管损失巨大，Bybit 目前仍具有偿付能力，即使无法追回被盗资产，也能承担损失。据统计，2024 年被盗加密货币的总价值约 22 亿美元，2023 年约 20 亿美元。

仿冒 DeepSeek 的手机木马病毒被捕获！国家病毒中心发布提醒

2 月 17 日央视新闻消息，国家计算机病毒应急处理中心近日在我国境内捕获发现仿冒 DeepSeek 官方 App 的安卓平台手机木马病毒。用户一旦点击运行仿冒 App，该 App 会提示用户“需要应用程序更新”，并诱导用户点击“更新”按钮。用户点击后，会提示安装所谓的“新版”DeepSeek 应用程序，实际上是包含恶意代码的子安装包，并且诱导用户授予其后台运行和使用无障碍服务的权限。该恶意 App 还包含拦截用户短信、窃取通信录、窃取手机应用程序列表等侵犯公民个人隐私信息的恶意功能和阻止用户卸载的恶意行为。经分析，该恶意 App 为金融盗窃类手机木马病毒的新变种。国家计算机病毒应急处理中心建议，仅通过 DeepSeek 官方网站或正规手机应用商店下载安装相应 App。

Palo Alto 防火墙又被黑：最新漏洞披露后第二天就遭利用

2 月 14 日 SecurityWeek 消息，美国威胁情报公司 GreyNoise 报告称，影响 Palo Alto Networks 防火墙的身份验证绕过漏洞（CVE-2025-0108）在公开披露后，短短 1 天内便遭到攻击者利用。Palo Alto Networks 于 2 月 12 日发布了针对 CVE-2025-0108 的补丁和缓解措施。该漏洞允许未经身份验证的攻击者访问防火墙管理界面，并执行特定的 PHP 脚本。GreyNoise 于 2 月 13 日透露，其已开始检测到针对 CVE-2025-0108 的攻击尝试。截至 2 月 14 日上午，该公司已观测到来自 5 个不同 IP 地址的攻击活动。可能有多方原因造成了这一状况。一方面，该漏洞利用方式与 1 月披露的已被利用漏洞 CVE-2025-0108 类似；另一方面，有安全团队在漏洞披露后马上公布了技术细节。

新一轮勒索潮来了？超级勒索软件组织宣布攻陷 47 家企业

2 月 13 日 Cybernews 消息，超级勒索软件团伙 Cl0p 在其暗网门户发帖，公布了最新一批 47 家受害组织，其中大部分受害公司位于美国，其他位于加拿大、墨西哥、英国和爱尔兰等，DXC 科技公司、芝加哥公立学校两家人员数量超 10 万的大型组织也在其中。目前相关公司尚未回应。Cl0p 团伙曾犯下多起影响面超大的数据泄露事件，如 MOVEit、GoAnywhere 事件等。由于攻击的组织数量庞大，难以逐一接触，该组织通常不直接联系受害者，而是在暗网门户发布消息，促使受害者主动联系。



漏洞篇

DeepSeek 等大模型私有化部署风险备受关注，常用部署软件 Ollama 曝出未授权访问漏洞（QVD-2025-9606），CNVD、CNNVD、NVDB、国家网络安全通报中心四大监管机构先后通报，建议相关单位和用户开展全面排查，及时修复 Ollama 已知安全漏洞。

Apache Tomcat 远程代码执行漏洞安全风险通告

3 月 11 日，奇安信 CERT 监测到官方修复 Apache Tomcat 远程代码执行漏洞 (CVE-2025-24813)，当应用程序 DefaultServlet 启用写入功能（默认情况下禁用）、使用 Tomcat 默认会话持久机制和存储位置、依赖库存在反序列化利用链时，未授权攻击者能够执行恶意代码获取服务器权限。奇安信威胁情报中心安全研究员已成功复现漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

微软 3 月补丁日多个产品安全漏洞风险通告

3 月 12 日，微软共发布了 57 个漏洞的补丁程序，修复了 Windows NTFS 文件系统、Windows 远程桌面服务、WSL2 等产品中的漏洞。经奇安信 CERT 研判，以下 21 个重要漏洞值得关注（包括 6 个紧急漏洞、15 个重要漏洞），如下表所示。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

编号	漏洞名称	风险等级	公开状态	利用可能
CVE-2025-26633	Microsoft 管理控制台安全功能绕过漏洞	重要	未公开	在野利用
CVE-2025-24991	Windows NTFS 信息泄露漏洞	重要	未公开	在野利用
CVE-2025-24984	Windows NTFS 信息泄露漏洞	重要	未公开	在野利用
CVE-2025-24993	Windows NTFS 远程代码执行漏洞	重要	未公开	在野利用
CVE-2025-24985	Windows FAST FAT 文件系统驱动程序远程代码执行漏洞	重要	未公开	在野利用
CVE-2025-24983	Windows Win32 内核子系统权限提升漏洞	重要	未公开	在野利用
CVE-2025-24045	Windows 远程桌面服务远程代码执行漏洞	紧急	未公开	较大
CVE-2025-24035	Windows 远程桌面服务远程代码执行漏洞	紧急	未公开	较大
CVE-2025-26645	远程桌面客户端远程代码执行漏洞	紧急	未公开	较小
CVE-2025-24084	WSL2 内核远程代码执行漏洞	紧急	未公开	较小
CVE-2025-24064	Windows 域名服务远程代码执行漏洞	紧急	未公开	较小
CVE-2025-24057	Microsoft Office 远程代码执行漏洞	紧急	未公开	较小
CVE-2025-24992	Windows NTFS 信息泄露漏洞	重要	未公开	较大
CVE-2025-24044	Windows Win32 内核子系统权限提升漏洞	重要	未公开	较大
CVE-2025-24067	内核流式处理服务驱动程序权限提升漏洞	重要	未公开	较大
CVE-2025-24066	内核流式处理服务驱动程序权限提升漏洞	重要	未公开	较大
CVE-2025-24061	Windows Web 查询标记安全功能绕过漏洞	重要	未公开	较大
CVE-2025-21247	MapUrlToZone 安全功能绕过漏洞	重要	未公开	较大
CVE-2025-24995	Kernel Streaming WOW Thunk 服务驱动程序权限提升漏洞	重要	未公开	较大
CVE-2025-21180	Windows exFAT 文件系统远程代码执行漏洞	重要	未公开	较大
CVE-2024-9157	Synaptics 服务二进制文件 DLL 加载漏洞	重要	未公开	较大

Apache OFBiz 服务端模板注入漏洞安全风险通告

3 月 10 日，奇安信 CERT 监测到官方修复 Apache OFBiz 服务端模板注入漏洞 (CVE-2025-26865)，Apache OFBiz 存在服务器端模板注入漏洞。攻击者可利用该漏洞，通过精心构造的输入注入恶意模板代码，从而在服务器端执行任意代码，可能导致敏感信息泄露、数据篡改或系统完全被控制。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Elastic Kibana 原型污染致任意代码执行漏洞安全风险通告

3 月 6 日，奇安信 CERT 监测到官方修复 Elastic Kibana 原型污染致任意代码执行漏洞 (CVE-2025-25012)，该漏洞源于 Kibana 中的原型污染问题，攻击者可以通过精心构造的文件上传和特定的 HTTP 请求绕过验证机制，攻击者利用该漏洞后，可以在受影响的系统上执行任意代码，可能导致数据泄露、系统被完全控制等严重后果。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 132118 个，关联 IP 总数为 29267 个。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

VMware ESXi 多个高危漏洞在野利用通告

3 月 5 日，奇安信 CERT 监测到 VMware 官方修复了三个高危漏洞，包括 VMware VMCI 堆溢出漏洞 (CVE-2025-22224)、VMware 越界写入漏洞 (CVE-2025-22225) 和 VMware HGFS 越界读取漏洞 (CVE-2025-22226)。攻击者可将这些漏洞链式利用，实现从虚拟机逃逸至宿主机。目前该漏洞已存在在野利用。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

NAKIVO Backup & Replication 任意文件读取漏洞安全风险通告

2 月 27 日，奇安信 CERT 监测到官方修复 NAKIVO Backup & Replication 任意文件读取漏洞 (CVE-2024-48248)，攻击者可利用 STPreLoadManagement 类中的 getImageByPath 方法，绕过路径验证并读取目标服务器上的任意文件（包括敏感配置文件、数据库、备份日志等）。奇安信鹰图资产测绘平台数据显示，该漏洞关联的全球风险资产总数为 3742 个，关联 IP 总数为 1352 个。目前该漏洞技术细节与 PoC 已在互联网上公开，奇安信威胁情报中心安全研究员已成功复现。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

备战攻防演练：2025 年第一季度需要关注的高危漏洞合集

2025 年第一季度，数字化进程的加速与新兴技术的普及，为企业带来效率提升的同时，也催生了更为复杂的安全威胁。从传统 OA 系统、办公软件到新兴的大模型基础设施，高危漏洞的爆发呈现多维度、高破坏性的特征：远程代码执行漏洞（RCE）可瞬间接管核心业务系统，SQL 注入与身份认证绕过漏洞成为数据泄露的“隐形通道”，而安全设备自身的漏洞更暴露出“矛与盾”的悖论。

第一季度漏洞态势凸显两大趋势：

一、“历史顽疾”未愈，SQL 注入、文件上传等传统漏洞仍在国产 OA、中间件中高频出现，折射出开发阶段安全规范的缺失。

二、“新兴威胁”崛起，大模型服务（如 Ollama）、物联网管理平台的漏洞利用门槛降低，攻击者可快速渗透 AI 基础设施与物理安防系统，威胁从虚拟空间蔓延至现实世界。

本文梳理 2025 年第一季度高危漏洞，通过分类剖析漏洞特性、总结攻击场景，并为企业提供多层级防御方案。无论是规避“0day 漏洞”的突发风险，还是加固长期暴露的薄弱环节，均可从本文中找到关键行动指引。在攻防不对称的当下，唯有前置防护、动态响应，方能在数字化浪潮中筑牢安全防线。

奇安信 CERT 贴心整理了以下高危漏洞合集，仅需复制粘贴漏洞编号，进入奇安信威胁分析平台 ALPHA 便可获取漏洞

详情。（https://ti.qianxin.com/vulnerability/list）

国产 OA

- 某微 E-Office10 远程代码执行漏洞 (QVD-2024-11354)
- 某微 E-cology9 WorkflowServiceXml SQL 注入漏洞 (QVD-2024-26136)
- 某远 OA ucpcLogin 接口身份鉴权绕过漏洞 (QVD-2024-27512)
- 某远 OA fileUpload.do 前台文件上传绕过漏洞 (QVD-2024-27266)
- 某凌 EIS 智慧协同平台 fi_message_receiver.aspx SQL 注入漏洞 (CVE-2025-22214)
- 某凌 OA sysUiComponent 任意文件上传漏洞 (QVD-2024-11115)
- 某友 NC6.5 rmwebImage 接口 SQL 注入漏洞 (QVD-2025-10301)
- 某友 U8Cloud pub.sql.query SQL 注入漏洞 (QVD-2025-1998)
- 某 WMS commonController.do 任意文件上传漏洞 (CVE-2024-57761)

国产 OA 漏洞特征：

- **代码逻辑缺陷：**多数漏洞源于未对用户输入过滤（如 SQL 注入）、接口鉴权缺失。
- **高危功能滥用：**文件上传接口未校验文件类型和路径，导致恶意文件落地。
- **历史遗留问题：**部分漏洞针对老旧版本系统，但用户未及时升级。

Web 服务与中间件

- 某通 T+ FileUploadHandler 任意文件上传漏洞 (QVD-2024-36760)
- 某应用虚拟化系统 AdminController.class.php SQL 注入漏洞 (QVD-2024-17003)
- 某维 GNRemote.dll 远程命令执行漏洞 (QVD-2024-27332)
- Fortinet FortiManager 身份认证绕过漏洞 (CVE-2024-47575)
- Palo Alto Networks PAN-OS 身份认证绕过漏洞 (CVE-2024-0012)
- GeoServer 远程代码执行漏洞 (CVE-2024-36401)
- Apache Kafka UI 远程代码执行漏洞 (CVE-2024-32030)
- EOVA JDBC 反序列化漏洞 (QVD-2025-10315)
- Nacos Derby 远程命令执行漏洞 (QVD-2024-26473)
- CyberPanel upgrademysqlstatus 远程命令执行漏洞 (QVD-2024-44346)
- 某管家 uploadFileByChunks.htm 任意文件上传漏洞 (QVD-2024-35232)
- 某点 UploadImage.do 任意文件上传漏洞 (QVD-2024-35233)
- Apache Solr 身份认证绕过漏洞 (CVE-2024-45216)
- Apache Struts 文件上传漏洞 (CVE-2024-53677)
- Apache Tomcat 远程代码执行漏洞 (CVE-2024-56337)
- Gradio 任意文件读取漏洞 (CVE-2024-1561)
- Rejetto HTTP File Server 模板注入漏洞 (CVE-2024-23692)

Web 服务与中间件漏洞特征：

- **配置管理薄弱：**默认弱口令、未启用安全模块。

- **反序列化漏洞频发：**如 EOVA JDBC 反序列化可导致 RCE。
- **横向移动风险：**攻击者利用中间件作为跳板渗透内网。

办公软件与协同平台

- 某潮海岳 HCM Cloud download 任意文件读取漏洞 (QVD-2024-45979)
- 某潮 GS 企业管理软件 biobjectwebservice.asmx 命令执行漏洞 (QVD-2024-34321)
- 某联达 GEPS 企业项目管理系统远程代码执行漏洞 (QVD-2024-27603)
- 某蝶 EAS 存在 appUtil.jsp 命令执行漏洞 (QVD-2024-46496)
- 某软 FineReport ReportServer SQL 注入漏洞 (QVD-2024-27261)
- 某软 FineReport FineVis 插件任意文件写入漏洞 (QVD-2024-35163)
- 某锁电子签章平台 ukeysign 远程命令执行漏洞 (QVD-2024-35144)
- 某电子文档安全管理系统 ClientSortLog.jsp SQL 注入漏洞 (CVE-2025-1841)
- 某电子文档安全管理系统 updateorg.jsp SQL 注入漏洞 (CVE-2025-1840)
- 某道项目管理系统身份认证绕过漏洞 (QVD-2024-15263)
- 某木报表权限绕过漏洞 (QVD-2024-35276)
- 某当 CRM getMyAmbassador SQL 注入漏洞 (QVD-2024-51803)

办公软件与协同平台漏洞特征：

- **数据暴露风险高：**如 download 接口未限制路径遍历，导致敏感文件泄露。
- **插件生态隐患：**第三方插件成为攻击入口。
- **供应链攻击可能性：**电子签章平台被控，将影响上下游业务。

安全软件与安防系统

- 某 3C 智能管理中心存在文件上传漏洞 (QVD-2025-10172)
- 某 UIS 超融合管理平台远程代码执行漏洞 (QVD-2024-38052)
- 某 3C SecCenter SMP 安全管理平台远程代码执行漏洞 (QVD-2024-48877)
- JumpServer 多个高危漏洞 (CVE-2024-40628、CVE-2024-40629)
- 某安防管理平台存在命令执行漏洞 (QVD-2024-44126)
- 某安防管理系统 uploadAllPackage 任意文件上传漏洞 (QVD-2024-35247)
- 某智能物联综合管理平台 GetClassValue.jsp 远程代码执行漏洞 (QVD-2025-1518)

安全软件与安防系统漏洞特征：

- **物理安全威胁：**安防系统漏洞可导致摄像头、门禁失控。
- **权限滥用风险：**如安全管理平台被控后，攻击者可操作全网策略。

大模型与新兴技术

- Ollama 远程代码执行漏洞 (CVE-2024-37032)
- Ollama 未授权访问漏洞 (QVD-2025-9606)

大模型与新兴技术漏洞特征：

- **资源滥用：**未授权访问 GPU 集群可能被用于挖矿或模型投毒。
- **数据泄露：**模型训练数据可能通过漏洞被窃取。

操作系统与数据库

- 微软 RDL 服务远程代码执行漏洞 (CVE-2024-38077)
- Windows TCP/IP IPv6 远程拒绝服务 / 代码执行漏洞 (CVE-2024-38063)
- 某数据库远程代码执行漏洞 (QVD-2024-38584)
- PHP CGI Windows 平台远程代码执行漏洞 (CVE-2024-4577)

操作系统与数据库漏洞特征：

- **底层协议漏洞：**利用 IPv6 栈漏洞可导致全网级瘫痪。
- **数据库提权：**可能引发核心业务数据泄露。

漏洞处置建议

1. 通用防护措施

- 补丁管理：
  建立自动化漏洞扫描与补丁更新机制，优先修复远程代码执行和认证绕过漏洞。
- 输入过滤与最小权限：
  对用户输入实施白名单校验，限制文件上传类型；数据库账户使用低权限角色运行。
- 网络隔离：
  将 OA、安防系统部署于独立 VLAN，限制中间件（如 Nacos、Kafka）的公网暴露。

2. 分场景加固

- 国产 OA 与办公软件：
  禁用不必要的接口，启用 WAF 拦截 SQL 注入和路径遍历攻击。
- 中间件：
  关闭组件的默认调试模式，配置强认证（如 Tomcat Manager 双重验证）。
- 安全设备：
  定期审计安全产品的日志与配置，禁止使用默认密码。

3. 应急响应准备

- 日志监控：
  集中收集系统日志，设置告警规则（如异常文件上传、高频 SQL 错误）。
- 定期排查：
  针对所属资产的高危漏洞定期进行排查。

2025 年第一季度高危漏洞表明，企业需构建“漏洞生命周期管理”体系，从开发、部署到运维全链路落地安全实践，重点关注边界防护、权限收敛与供应链管控，避免因单点漏洞引发全网沦陷。



CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

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

攻防答题模式

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

积分等级体系

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

聆听 | 两会“网安声音”

2025 两会代表热议网络安全，AI 安全、数据安全成焦点。

2025 年全国两会期间，网络安全议题成为代表委员们热议的焦点。随着人工智能技术的广泛应用和数据要素的深度渗透，网络安全风险呈现出智能化、复杂化、全域化的新特征。两会代表围绕“人工智能安全”与“数据安全”两大核心领域，提出了系统性治理方案，为构建数字中国安全底座提供了重要思路。



两会代表聚焦 AI 与数据安全

两会代表围绕“人工智能安全”与“数据安全”两大核心领域，提出了系统性治理方案，为构建数字中国安全底座提供了重要思路。

人工智能安全：筑牢根基与应对新型挑战

人工智能作为新一轮科技革命的核心驱动力，在推动产业升级的同时，也引发了前所未有的安全风险。全国政协委员齐向东、人大代表冯涛等从技术防御、法律规范、攻防对抗等维度，系统剖析了 AI 安全治理的关键路径。

随着“人工智能 +”的开启，大模型所面临的、带来的安全挑战亦日益严峻。如何保障人工智能时代的网络空间安全？人工智能“成长的烦恼”如何破解？齐向东表示，创新是第一动力，安全是底线要求。“人工智能 +”驱动新质生产力跃升，伴生的新型安全威胁不容忽视，尤其是智慧金融、智能制造、智慧交通等新场景的涌现，也让数据泄露、漏洞利用、深度伪造等安全风险加剧，网络攻击的频度和烈度激增。

针对这些安全问题，齐向东认为，要从技术保障、制度保障、成果应用三方面入手，系统提升安全能力，确保人工智能安全发展。其中，要推动“AI+ 安全”创新成果落地，走好提升安全能力的必经之路。

AI 换脸成侵权重灾区，强力监管势在必行

“靳东两会建议 AI 换脸立法”“雷军回应国庆 7 天被 AI 雷军骂了 8 天”……今年两会期间，AI 话题频频登上热搜，“AI 换脸”引发的风险问题更是受到代表委员的热议。尤其是深度伪造 (Deepfake) 技术正以指数级速度渗透日常生活。随着技术持续进化、门槛不断降低，“AI 换脸”的不当滥用已成为违法侵权重灾区，并有愈演愈烈之势。

面对新型侵权形态，现行法律体系正面临现实挑战。全国人大代表、小米集团创始人雷军坦言，现有法律体系仍将 AI 侵权嵌套在隐私权、肖像权、名誉权等传统框架中，而“被骂 8 天”“因 AI 谣言导致股价下跌”等损失，却因无法量化举证而难以维权。

雷军建议，加快单行法立法进程，提升立法位阶；强化行业自律共治，压实平台企业等各方的责任和义务；加大普法宣传的广度力度，增强民众的警惕性和鉴别力。

全国人大代表、TCL 创始人李东生也建议，加快人工智能深度合成内容标识管理规章制度的出台，明确惩罚制度，同时还需加强国际合作，形成人工智能生成合成内容的有效监管。

此外，人工智能技术的“双刃剑”效应在电信诈骗领域也非常突出。冯涛代表调研发现，黑客利用 AI 生成的伪造语音、视频实施钓鱼攻击，使民营企业客户信息泄露事件激增。这类攻击具有三大特征：一是低门槛化：开源 AI 工具降低了犯罪技术壁垒；二是高效精准化：AI 可批量生成个性化欺诈内容；三是隐蔽性强：深度伪造内容难以被传统风控系统识别。

对此，冯涛提出“以 AI 对抗 AI”的治理思路：通过研发 AI 驱动的反欺诈系统，通过行为模式分析实时拦截异常操作；在法律层面明确技术应用边界，将云计算、区块链等新技术服务提供者纳入监管；建立企业数据保护与公共安全协同机制，避免“一刀切”监管阻碍技术创新。

数据安全：构建数字公民防线与法治保障

数据作为数字经济的核心生产要素，其安全问题直接



关乎国家安全与公民权益。全国政协委员、新大陆科技集团总裁王晶，人大代表、荣华控股董事长崔荣华，聚焦数据确权、流通规则与法治建设，提出了系统性治理方案。

王晶指出，传统数据防护手段已难以应对海量数据泄露风险。她提出的“数字公民”理念，通过构建个人数据主权体系实现安全破局。她特别强调，需通过试点示范提升公众认知。例如，在医疗、社保等领域率先建立个人可信数据空间，让民众直观感受数据自主权带来的安全保障。

荣华控股董事长崔荣华指出，现有《网络安全法》《数据安全法》等分散立法难以适应数字经济快速发展。她力主制定《数字经济促进法》，从数据要素市场化、安全监管升级、技术融合赋能、国际规则对接等 4 个方面，完善治理框架。

崔荣华建议，数据要素市场化需要明确个人数据、企业数据、公共数据的权属边界；建立全国统一的数据交易平台与定价机制，释放数据资源价值。而安全监管方面，需要实施数据分类分级保护，健全风险评估与应急处置机制，强化平台经济反垄断监管，防止算法歧视与数据滥用。而在技术赋能方面，需要设立数字经济发展专项资金，支持 5G、工业互联网等新基建，鼓励金融机构开发数据资产质押融资产品，破解中小企业数字化转型的资金瓶颈。国际规则对接方面，需要参与全球数字贸易规则制定，建立跨境数据流动“白名单”机制；培育具有国际竞争力的数字产业集群，提升产业链抗风险能力。

安全与发展并重的数字中国之路

整体来看，2025 年两会代表关于网络安全的讨论，凸显出“统筹安全与发展”的核心逻辑。在人工智能领域，需通过技术创新与制度约束平衡效率和风险；在数据治理层面，则需以公民权利为本位重构安全范式。

齐向东的立体防御体系、王晶的数字公民构想、崔荣华的法治化路径，共同勾勒出“技术—制度—人文”三位一体的安全蓝图。未来，随着《数字经济促进法》的推进与 AI 安全标准的完善，中国有望为全球网络安全治理贡献更具前瞻性的方案。

2025 两会 “网安提案”

网络安全议题成为 2025 年全国两会备受各界瞩目的热点话题之一。人大与政协代表提出了多个具有较大影响力、引发广泛讨论的提案。不仅涵盖人工智能安全这一前沿领域，还涉及大模型安全、数据安全及网络谣言和网络暴力治理等领域。

人工智能安全



齐向东
全国政协委员

从技术保障、制度保障、成果应用三方面入手，确保人工智能安全发展

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建议，随着人工智能技术的深度应用，大模型带来新的安全挑战，要从技术保障、制度保障、成果应用三方面入手，系统提升安全能力，确保人工智能安全发展。

齐向东委员建议，建立适配大模型的纵深防御体系，打造适用于人工智能的立体纵深防御体系，为人工智能大模型安全稳定运行保驾护航；制定大模型安全强制合规要求，明确大模型安全的组织架构，界定安全主体责任，对基础安全、数据安全、应用系统开发安全、运行安全等方面提出清晰的技术保障要求；推广“人工智能 + 安全”创新成果落地，鼓励更多产业用上、用好“人工智能 + 安全”创新成果，提高千行百业的网络安全防护效能。（光明网）

推动大模型安全赋能与基础安全能力协同发展

全国政协委员、安天集团创始人肖新光认为，先进制造业中使用的工业装备、数智系统和工业机器人等无人设备，已成为新的网络攻击目标，网络安全技术要跟得上数字化、智能化发展速度。肖新光建议，在大力推动数字技术赋能制造业发展的同时，要实现大模型的安全赋能与基础安全能力的协同发展，带动相关产业链升级，更好地、更安全地培育新质生产力。（中国经济网）



肖新光
全国政协委员



雷军

全国人大代表

加强“AI 换脸拟声”治理 压实平台各方责任

全国人大代表，小米集团创始人、董事长兼 CEO 雷军指出，“AI 换脸拟声”的不当滥用已成为违法侵权行为的重灾区，人工智能深度合成技术所需素材获取便利、技术使用门槛低、侵权主体及其手段隐蔽性强等特点给治理带来较大挑战。

雷军建议，一是针对“AI 换脸拟声”等问题，探索推出人工智能单行法，提高立法位阶及其效力，在分级分类的基础上进行务实治理，明确“AI 换脸拟声”应用边界红线，完善侵权证据规则，加大对利用人工智能技术实施犯罪行为的刑事处罚力度。

二是强化行业自律共治，压实平台等各方的责任。支持平台企业开发可精准识别人工智能深度合成内容的技术能力，确保及时阻断问题内容传播。

三是建议加强人工智能方面的法治宣传教育，增强民众的警惕性和鉴别力，特别是要聚焦重点人群，在全社会夯实“以人为本、智能向善”的人工智能发展生态。（人民法院报）

治理 AI 虚假信息，完善监管体系

国政协委员、四川大学华西医院教授甘华田计划提出关于加强 AI 生成虚假信息治理的建议，呼吁从法律、技术、监管、公众教育四个方面加强治理，确保 AI 技术在合法、合规、安全的框架内发展。

首先是完善 AI 生成内容监管法律法规体系，其次，加强技术监管与防范。研发更加先进的人工智能算法，提高其对信息的识别和判断能力。最后是建立健全监管机制。设立专门的监管机构，负责对 AI 产品和服务进行审查和监督，确保其符合法律法规和道德规范。



甘华田

全国政协委员

数据安全



邓中翰
全国政协委员

筑牢数据主权安全防线，构建全国统一数据市场

全国政协委员、中国工程院院士邓中翰建议，建立数据分类分级制度，结合原生数据安全技术和可信执行环境技术，从芯片层实现数据防篡改、防伪造，确保数据内容真实性与完整性，防范恶意内容渗透，从源头确保数据在采集、传输、分析全流程安全可控。

从技术角度，建议强化技术与标准支撑，加大数据加密、数字水印等关键技术攻关，推进视音频编解码、智能感知等领域自主标准制定，以标准优势带动产业优势，筑牢数据主权安全防线。

从数字经济发展角度，建议构建全国统一数据市场，统筹国家数据基础设施，推动跨层级、跨领域数据可信流通；建立健全国家公共数据资源体系，支持公共数据与行业数据融合开发，在国家安全、经济民生等关键领域实现数据“有标识、受监管、被保护、可交易、能使用”。（新华网）

定期清理 AI 幻觉生成数据 构建可信环境

全国人大代表、科大讯飞董事长刘庆峰建议，应预防大模型生成“幻觉数据”充斥互联网带来的危害，从技术研发和管理机制上构建可信的信息环境。

刘庆峰建议，构建安全可信数据标签体系，提升内容可靠性，建立安全可信、动态更新的信源和数据知识库，对不同类型数据的可信度和危害程度建立标签体系，降低人工智能幻觉出现概率，提升生成内容可靠性；研发 AIGC 幻觉治理技术和平台，定期清理幻觉数据，研究幻觉自动分析的技术和软件平台，开展幻觉自动分析、AIGC 深度鉴伪、虚假信息检测、有害内容识别及互联网传播溯源，由中央网信办、国家数据局等部门定期清理幻觉数据，为公众提供 AIGC 幻觉信息检测工具与服务。



刘庆峰
人大代表



柳江

全国人大代表

促进可信数据空间应用落地 推动数字经济和实体经济深度融合

全国人大代表、长虹控股集团董事长柳江聚焦“可信数据空间应用落地”建设，提出多项建议。柳江表示，可信数据空间是规模化数据流通利用的“中国方案”，是平衡数据安全与发展的关键基础设施，对 AI 技术应用发展具有深远影响。因此，加快可信数据空间建设与应用落地，对促进数字经济发展意义重大，是推动数字经济赋能实体经济的关键抓手。

AI 技术的广泛应用仍面临可信数据空间技术标准不统一、数据要素市场机制不健全等问题，柳江提出三大核心建议：加快技术标准化，加强互联互通；规范数据流通利用，强化监管合规；加快数据产业发展，着力人才培养。

以数字公民建设筑牢数据安全新防线

全国政协委员、新大陆科技集团 CEO 王晶表示，数字公民建设是新时代背景下保障数据安全、促进人工智能等新产业健康发展的重要举措。通过完善数字身份认证体系、构建广泛的应用接入与数据服务能力、构建可市场化运营的第三方服务模式等措施，可以构建起数据安全的新防线，为推动数字中国建设贡献力量。

王晶建议，应由国家层面统筹规划，构建以法定身份证件为根的多级可信个人身份服务体系，推动跨部门数据互认共享，并通过试点示范提升公众数字素养，最终形成政府主导、社会协同、市场运作的数字公民发展格局，为网络强国和数字经济健康发展提供底层支撑。



王晶

全国政协委员



董进
全国人大代表

前瞻布局下一代高可信区块链网络

全国人大代表、国家区块链技术创新中心主任董进在今年全国两会上建议，我国应前瞻布局下一代高可信区块链网络，打造超大规模、超强算力、超高安全的数字基础设施，为数据可信安全高效地流通提供坚实基座，加速海量高价值数据在流通中释放活力。

董进建议，面对新需求、新形势，我国应前瞻布局，加快建设覆盖全国的下一代高可信区块链网络，打造新型数据流通基础设施。这套数字基础设施应支撑千万级节点分布式部署、每秒千万笔数据交易，加密技术确保数据在传输和存储过程中安全可靠，融合高性能隐私计算实现敏感数据“可用不可见”。

推动网安立法

加快出台相关制度，加强 AI 深度伪造欺诈管理

全国人大代表，TCL 创始人、董事长李东生提出《关于加强 AI 深度伪造欺诈管理的建议》。李东生建议，从加快出台管理规章制度、明确惩罚制度、标识技术标准和发布管理、国际合作等方面，加强 AI 深度伪造欺诈管理。一是加快人工智能深度合成内容标识管理规章制度的出台；二是明确对人工智能深度合成服务商未履行标识义务的惩罚制度，完善对深度合成内容服务提供商未按要求进行标识的行为界定、分类细则，以及相应的处罚标准；三是加强深度合成内容标识技术标准和发布的管理，出台深度合成内容标识的技术标准，保证标识的有效性。对相关内容平台出台要求，用户在发布深度合成的视频、音频等内容时，有义务对其进行标识；四是加强国际合作，形成人工智能生成合成内容的有效监管。（蓝鲸财经）



李东生
全国人大代表



李景虹
全国政协委员

加快制定人工智能促进法，营造更好创新发展环境

全国政协委员、中国科学院院士李景虹表示，中国作为人工智能综合实力较强的国家，应该制定人工智能促进法，凝聚共识，形成合力，推动人工智能向造福于民的方向发展。同时，将该项立法提升至战略高度，立足于发展，结合最小化的包容性审慎监管规则，为社会各界提供最大程度的确定性和明确的预期。他认为立法应聚焦促进有效应用、普惠服务、技术创新、人才培养（包括尖端人才和复合型人才）、就业保障（包括扩大职业教育和全民通识教育）、国际合作等六个方面。（红星新闻）

建议加快制定生成式人工智能的行政法规

全国政协委员、中华全国律师协会监事长吕红兵在今年全国两会上关注生成式人工智能的立法问题，建议加快制定一部有关生成式人工智能的行政法规。

吕红兵建议，应明确规定将社会主义核心价值观贯穿生成式人工智能全生态，并由其统领。行政法规应对生成式人工智能的技术开发者、服务提供者、使用者、监管者及社会公众，分门别类明确各自权利和义务、职能与责任。他建议，应明确统一的监管者，对网信、发展改革、教育、科技、工信、公安、广电等部门的相关职责合并同类项，组建统一的监管部门，提高监管的专业性与权威性。（央广网）



吕红兵
全国政协委员



冯涛
全国人大代表

依法防范人工智能变“数字利刃”

随着人工智能（AI）技术广泛应用，网络安全面临新形势。全国人大代表、国网山东省聊城供电公司数字化与通信工作部（数据中心）信息运检班班长冯涛提出了“AI 对抗 AI”的解决方案，并优化完善成“关于完善相关法律应对新型网络安全攻击手段的建议”。

冯涛建议，要规范 AI 技术和区块链技术的使用，明确技术应用的边界和责任；将网络所有者、管理者、服务提供者，以及通过云计算、人工智能平台、区块链等新技术提供服务的组织和个人纳入监管范围；在依法监管框架下平衡企业数据保护与公共安全需求。（本文来自《检察日报 · 法治中国》两会特刊）



张毅

全国政协委员

推动人工智能立法，开创发展新局面

全国政协委员、金杜律师事务所高级合伙人张毅表示，加快《人工智能法》立法，既是应对技术风险的紧迫需求，也是推动高质量发展、提升国际竞争力的重要举措。

张毅建议，立法应当涵盖算法和算力的监管，因为算法的偏差和算力的滥用可能引发社会的歧视与不平等。通过针对不同应用场景进行风险等级的划分，实施分级分类监管，明确全生命周期的监管义务，都是保障公众利益和社会公正的有效手段。

此外，立法应明确数据要素的权属定义，推动隐私计算、区块链等技术在数据安全与流通中的应用，构建“政府监管 + 市场自律”协同的监管生态圈。同时，企业应在产品研发阶段嵌入合规要求，确保数据合规贯穿产品全生命周期，并推动第三方合规服务机构的发展，提供专业的数据安全评估和流通治理支持。

强化网络谣言与网络暴力综合治理体系

全国人大代表、格力电器董事长董明珠提交了一份“关于强化网络谣言与网络暴力综合治理体系建设的建议”。董明珠建议，净化网络环境需要从法律层面加大打击力度。一是尽快全面修订《中华人民共和国网络安全法》；二是国家网信办尽快出台《网络谣言、网络暴力信息互联网平台治理规定》；三是在拟出台的新《治安管理处罚法》中新增对网络谣言、网络暴力信息的分类界定与处罚条款；四是两高尽快出台统一的专门针对网络谣言、网络暴力信息犯罪行为的司法解释；建议最高人民法院出台专门针对网络谣言、网络暴力信息民事侵权的司法解释。（中国经营网）



董明珠

全国人大代表

红帽人才工程

Cyber Crime Governance Talent Training Project

工程简介

在“全国网络警察培训基地”的指导下，中国下一代网络安全联盟牵头发起「红帽人才工程」，联合华云信安、美亚柏科、高联通信等知名网络安全企业，围绕“网络犯罪治理、涉网犯罪打击”等相关网络安全课题，持续挖掘、培养、资助、赋能网络安全人才，构建红色基因的网络空间安全人才防线。

申报流程

课题征集 → 课题公示 → 立项评审

研究课题计划征集

研究课题信息公示

研究课题立项评审

申报说明

项目资讯

培养对象

政企单位在职人员、高校全日制在校生（含研究生）、互联网企业技术人员、网络安全企业技术人员以及社会网络安全人才...

核心课题

内网攻防、社工钓鱼、远控木马、免杀加壳、情报甄别、资金分析、调证溯源、取证固证、远程勘验、APP反编译、二进制逆向...

从 2022 到 2024：两会“网络安全提案”的变迁

在历届两会议程中，网络安全议题逐渐占据重要位置，成为代表委员们热议的焦点。专家、学者、企业大咖，以及来自各行各业的代表们纷纷就网络安全问题建言献策，提出了一系列具有前瞻性和针对性的提案。

本文对 2022—2024 年两会期间提出的关于网络安全领域的提案进行了全面又细致的梳理。这些提案涵盖了网络安全政策法规的完善、网络基础设施的安全防护、个人信息保护的加强、人工智能安全技术的研发 , 以及网络安全应急响应机制的构建等多个方面。这些提案不仅反映了当前网络安全领域的热点问题和紧迫需求，也为未来网络安全的政策导向与发展走势提供了重要参考。

2024

一、主题

加强智能安全

二、关键词

人工智能、智能汽车、智能制造、云安全、网络空间生态治理

三、主要内容

（一）AI 人工智能安全领域

1、加强培养人工智能人才，满足科技变革需求

（1）从义务教育阶段普及人工智能素养教育；

（2）大力推进高校人工智能相关专业的建设；

（3）支持大型科技企业和教培机构培育人工智能应用型人才。

2、创新发展“AI+ 安全”， 护航中国式现代化

（1）从供给侧看，开展联合创新，围绕攻防实战和应用场景实现“AI+ 安全”尖端技术研发突破；

（2）从需求侧看，强化政策牵引，推动“AI+ 安全”技术创新产品在各行业落地应用；

（3）从人才侧看，壮大“AI+ 安全”领域的实战型、复合型人才队伍。

3、深化人工智能多场景应用支持大模型向垂直化、产业化方向发展

（1）建议政府、央国企率先提供更多应用场景，聚焦“小切口，大纵深”，推动大模型垂直化、产业化落地；

（2）建议鼓励企业在定制 AI 前，做好知识管理，将企业大数据平台升级为企业知识平台；

（3）建议鼓励和引导企业将大模型与数字化业务系统深度结合，同业务流程相结合充分发挥大模型价值。

4、鼓励兼具“安全和 AI”能力的企业，解决通用大模型安全问题

（1）建议国家更加重视通用大模型安全问题，给予兼具“安全 AI”能力的企业专项扶持政策，更好地发挥其解决通用大模型安全问题的重要作用；

（2）建议国家研究制定保障通用大模型安全的标准体系，推动通用大模型开展安全评测、接入安全服务，降低通用大模型安全风险；

（3）建议政府、央国企与兼具“安全和 AI”能力的企业，在大模型安全领域展开深入合作，发挥此类企业在人工智能安全领域的优势作用。

5、呼吁制定通用人工智能发展规划

（1）建议加快推广大模型赋能全学段，以全新机制加快探索我国人工智能拔尖创新人才培养；

（2）建议研究通用人工智能时代人才能力素质模型和培养方案，加快应用型人才培养；

（3）建议加速通用人工智能技术相关的法律法规制定与审议；

（4）建议设立软课题进行通用人工智能相关的伦理人文研究。

6、推进《人工智能法》立法 筑牢关键信息基础设施安全屏障

（1）增强人工智能技术安全应用的法治保障能力；

（2）增强关键信息基础设施智能化安全合规的监管能力；

（3）增强关键信息基础设施智能化全域方案的解决能力；

（4）增强关键信息基础设施智能化保护人才的培养能力。

7、构建人工智能技术标准和评估体系

（1）应积极推动人工智能领域立法进程；

（2）明确生成式人工智能“事前—事中—事后”全链条监管机制；

（3）建立人工智能责任认定和追责机制、各利益相关方共同参与的系统化治理体系。

8、建议探索用 AI 技术监管 AI

（1）尽快推进《人工智能法》的出台，构建人工智能算法治理体系，弥补监管体系空白；

（2）强化和创新算法监管。强化由网信牵头，发展改革、数据、工信、公安等；

（3）多部门共同参与的算法治理联席会议制度，完善“横向协同，纵向联动”算法治理格局；

（4）进一步保障用户权利；

（5）拓展算法侵害行为维权路径与责任模式，增强用户维权力量。

（二）网络安全建设领域

1、全面建设安全云推广数字安全云化服务

（1）统筹建设数字安全公共服务基础设施，集中数字安全能力；

（2）改变重建设轻效果的思路，鼓励各单位购买数字安全云化服务，作为传统网络安全建设的升级路径；

（3）鼓励网络安全企业积极转型，以“安全即服务”方式为国家整体数字安全水平提升做出贡献，尤其是鼓励具备核心技术的、被美制裁的龙头企业发挥更大作用。

2、强化网络安全效能导向建设机制

（1）构建基于运行价值和风险后果的“新度量衡”；

（2）建立效能导向建设机制，牵引关基安全建设向高限落实；

（3）建立以责任主体投入为主、机动弹性赋能辅助的多元投入保障机制。

2023

一、主题

构筑数字安全屏障

二、关键词

数字安全建设、人工智能安全等

三、主要内容

（一）数字安全

1、要筑牢服务数字经济发展与安全的司法屏障，严格把握《网络安全法》《数据安全法》等划定的涉及国家安全

的数据安全红线，用好域外追责、刑事打击等规范跨境数据流动的司法武器，坚决保护我国享有自主知识产权的先进数字技术。

2、建立统一的国家数字信任平台

（1）要将数字信任的构建纳入数字政府治理的范畴，制定我国数字信任体系的远景、目标、领域、指导原则、责任模型和关键能力等，制定数字信任新型基础设施建设相关政策。同时，要统筹规划数字信任制度体系和技术体系，建立数据安全、权利保护、跨境传输管理、交易流通、开放、共享、安全认证等基础制度和标准规范，建立统一、规范的数字身份和数据安全合规监管体系；

（2）自主突破区块链、AI、隐私计算、量子密码等技术关键点，加强对区块链、AI 等技术的安全合规体系建设，建立自主可控、安全可靠的数字信任创新技术体系；

（3）建设以人为中心、构建有序治理的数字身份体系，包括建立一致性的监管和治理规则，针对个人身份信息在数据共享流通中的使用，建立授权、救济、问责机制，保护身份主权，维护国家安全；

（4）鼓励各地紧扣“一个码”，有序整合分散的身份信息，推动建立以各地城市码为入口的个人数字身份集约化管理和应用机制；

（5）强化数据安全合规监管能力，加速数据共享流通信任体系建设，尽快明确数据要素在流通中的权属认定、安全性、合规性、完整性及可追溯性等方面的要求，建立数据要素确权、存证等规则体系，运用密码学和区块链等技术实现穿透式、全方位的监管。

3、要筑牢服务数字经济发展与安全的司法屏障

（1）应当严格把握《网络安全法》《数据安全法》等划定的涉及国家安全的数据安全红线，用好域外追责、刑事打击等规范跨境数据流动的司法武器，坚决保护我国享有自主知识产权的先进数字技术；

（2）我国应当在创新数字经济治理规则的基础上，积极参与全球治理，推动在我国司法过程中行之有效的治理规则成为国际治理规则。

4、“下海”是下产业数字化蓝海把城市数字安全服务中心建设作为扩内需、稳增长的重点内容，列入省、市、县及产业园区的发展规划中，组织城市数字安全服务中心优秀案例评选，推动城市数字安全建设模式的持续优化和完善。

5、“助小微”的含义是通过 SaaS 服务，助力数字化“共同富裕”，鼓励帮扶中小微企业构建数字安全能力，补齐国家数字安全的缺口。

6、确立网络“零事故”目标

（1）网信办将“零事故”目标转化为政企机构网络安全建设的标准规范；

（2）财政部明确要求政企机构在新增 IT 预算中 10% 用于网络安全建设；

（3）政企机构建设纵深防御的内生安全系统。

7、强化企业数据安全管理与评估

（1）应完善数据安全评估体系；

（2）推动数据安全合法评估；

（3）突出数据安全风险防范。

8、推进数据要素市场化，数字经济新生态

（1）探索建立数据交易的备案管理机制，健全第三方评估体系建设。统筹推进各地数据交易所建设，强化数据全生命周期运营能力，试行公共数据内部结算模式与商业数据资产定价模式；

（2）以区块链技术为核心，构建安全高效的数据要素交付通道，并建立评估准入机制，核心技术要自主可控，确保数据安全。

（二）人工智能安全

1、大力发展自主创新的人工智能通用基石模型

（1）修订《网络安全法》《数据安全审计法》等已有互联网法律法规，明确人工智能通用基石模型及生成式 AI 技术和应用中涉及政治、民族、宗教和互联网等相关的法律底线和红线问题；

（2）应加快人工智能通用基石模型带来的知识产权保

护研究，推进 AI 内容监控平台建设。

2、关注人工智能大模型技术发展

（1）建立大型科技企业 + 重点科研机构的产研协同创新模式，打造中国的“微软 +Open AI”组合引领大模型技术攻关；

（2）支持设立多个国家级人工智能大模型的长期开源项目，打造开源众包的开放创新生态。

3、“上山”是上科技高山

（1）建立大型科技企业 + 重点科研机构的产研协同创新模式，打造中国的“微软 +Open AI”组合引领大模型技术攻关；

（2）支持设立多个国家级人工智能大模型的长期开源项目，打造开源众包的开放创新生态。

4、在自主可控平台上让行业尽快享受 AI 红利

（1）重视认知智能大模型研发，形成以领军企业为主体、产学研合作的创新体系，加速跟进和追赶国际前沿水平；

（2）支持认知智能大模型技术的行业示范应用，推动认知智能大模型在教育、医疗、办公、人机交互和 AIGC 领域的价值落地；

（3）进一步加大支持人工智能国产软硬件技术底座，让大模型建设和运行在国产化的存储、算力、操作系统等基础平台上，中国认知智能大模型只有在国产技术底座上发展，才能有自主可控的大未来；

（4）建设认知智能大模型公共算力平台，设立使用平台的揭榜挂帅机制，让更多科研院所和科技创业企业有机会站到国家公共算力平台上进行模型训练和算法创新；

（5）构建国家数据资源平台，汇聚认知智能大模型所需要的基础性数据，在依法合规基础上搭建数据共建共享机制，支持战略科技力量站在国家数据资源的平台上加速认知大模型的研发和产业化；

（6）鼓励产业基金参照 OpenAI 和微软等股东的投资协议模式，积极探索更有利于创业团队和核心技术骨干为梦想长期奋斗的股权投资协议模式，构建更好的科技创投生态和创新创业环境。

2022

一、主题

加强网络安全、数据安全和个人信息保护

二、关键词

勒索攻击、关基保护、数据保护等

三、主要内容

（一）数字安全

1、网络安全升级为数字安全，亟待将数字安全纳入新基建。

网络安全升级为数字安全，打造覆盖所有数字化场景的数字安全防范应急体系，包括应对工业互联网、车联网、智慧城市，以及云安全、数据安全、供应链安全等挑战。同时，建议国家把数字安全纳入新基建，各地数字化建设之初便将安全考虑在内，并互联互通，调集社会各方力量共同参与数字安全体系建设，真正提升国家的数字安全能力。

2、帮扶中小企业数字化转型，数字安全“一个都不能少”。鼓励和支持大企业以创新轻量化产品、SaaS 服务为抓手，消除中小微企业在认知、资金、技术、人才等方面的差距，推动中小企业实现数字化转型。

3、关于构建可信数字身份认证服务体系。

一是围绕可信数字身份健全法律法规或管理办法，明确以居民身份证信息为根，为公民建立可信数字身份。建议聚焦可信数字身份认证加强技术创新和规范统一，支撑可信数字身份认证服务体系与数据治理体系的融合，实现数据资源的可用不可见、可算不可识；

二是基础设施以统一规范的“可信数字身份 +”的形式规划公民身份信息集合，做到标识可信；使用手机 SIM 卡、

银行卡等安全芯片承载可信数字身份，做到载体可信；依托中央企业构建国家级数字身份认证服务平台，做到平台可信；统筹各行业身份认证服务，关联用户行为认证，做到服务可信，从而为数据治理提供安全环境，为社会提供数据安全感及信任感。

（二）网络安全与数据保护

1、设立网络安全和数据保护指导窗口，解答企业及个人疑难。设立网络安全和数据保护指导窗口，负责接受投诉举报，解答企业、个人及专业服务机构在网络安全与数据保护方面的实际问题。对于涉及不同主管部门的咨询内容，窗口应该具备能力进行内部的资源共享、协调统合，通过统一窗口给出权威答复。

同时，加强职责部门之间的统筹协调。在形成监管合力的同时，明晰各部门在网络安全及数据保护领域的监管重点和边界，促进部门间的资源共享与协作，逐步健全跨部门的综合监管制度。

2、明确数据权属，规范交易活动要明确数据所有权、使用权、处理权、控制权、收益权等各种权利属性，确定各种数据权拥有者的相关权责。对涉及个人隐私、商业秘密和国家安全等数据在大数据营销、企业数据共享、数据跨境流动、政府社会治理、公共服务、公共安全应用等特定使用场景下进行使用约束，避免隐私权与财产性数据权属混同。

3、加快制度建设促进网络安全保险健康发展。

一是完善相关标准与法律体系。我国急需构建更为完整的网络安全等级管理体系，加快建立统一的数据安全分类管理制度，为保险公司、网络安全服务商提供网络安全保障服务，及时处理网络经济纠纷有法可依，有效保障网络安全行业的高质量发展。

二是制定网络安全保险发展的相关战略规划。提供政策支持和组织保障，建议工信部指导网络安全保险市场发展，可借鉴国外经验，出台优惠政策，鼓励责任主体购买网络安全保险。

三是建立统一的网络安全风险数据库。网络安全保险市场发展缓慢的一个重要原因是缺少经验理赔数据，从而使数据安全风险量化成为难题。

四是加大网络安全保险的宣传推广力度。充分利用国家安全教育日、全国保险公众宣传日等全国性宣传机会，介绍网络安全保险的承保范围、真实案例、作用意义等。

（三）关键信息基础设施与网络安全

1、新型电力系统与网络安全应同步规划建设新型电力系统发展与安全同步规划建设。统筹安排电力部门、网络信息安全部门、创新企业等多方力量，联合开展顶层设计和规划论证。

注重构建能源网络全要素安全技术体系，在大力提升能源网络数据智能自动化安全调度运营管控能力的同时，同步安排新型电力系统网络安全防护体系的规划建设。多领域专家交叉融合开展创新工作，建立与系统相匹配的、可持续更新的新型电力系统、网络安全、数据安全等工程标准体系。

在预防预测、防护保障、监测预警、应急处置等方面，打通产品、服务、人员和流程等关节，通过一体化安全运营模式，不断提升新型电力系统的网络和数据安全保障水平。

2、设“首席安全官”，加强重大交通基础设施保障，借助港珠澳大桥的智能化运维技术和物联网、大数据、云计算、人工智能等新一代信息技术，建立一套系统科学的重大交通基础设施全生命周期运营规程，从整体上为重大交通基础设施安全管理的各个方面打造一个标准完善、责任清晰的基础环境。

（四）国家网络空间安全

1、加强防范勒索软件攻击，提升国家网络空间安全防御能力强化网络漏洞发现能力；提升基础设施安全应对能力，及时对系统漏洞进行补丁升级；共建网络空间国际新秩序。

2、网络安全规划应放在严峻国际形势下做出敌情想定相关部门设立专项，研究推动软硬件研发场景安全防护工作；制定对应标准规范体系，覆盖开发环境、生产环境安全防护、软件强制签名要求与签发环境安全要求、软件分发升级环境安全规范等。通过建立试点示范项目等机制，引导基础软硬件、共性软件、政企场景工具软件等相关研发企业机构，重视网络安全工作，加大安全防护力度。

勒索攻击报告：威胁规模和复杂程度超过往年

奇安信威胁情报中心收集了全球安全机构发布的勒索攻击有关的安全报告，根据这些公开报告梳理了 2024 年全球范围内的勒索攻击活动，介绍其中出现的值得关注的攻击手法，最后总结 2024 年全球勒索攻击活动特点和趋势。

一、勒索攻击概览

根据国外安全机构的统计，勒索软件攻击在 2024 年 5414 名已公布的受害者与 2023 年相比，增长了 11%，是 2021 年以来最多的一年。2024 年第四季度尤为显著，共公布了 1827 起勒索软件事件，成为一年中最活跃的季度，与 2023 年同期相比，增长了 29%。

从更广泛的角度来看，2024 年下半年的事件比上半年多 46%，比 2023 年下半年多 17%，突显出在此期间勒索软件活动的显着增加。这可以归因于新专业攻击团伙的大幅增加，这些团伙可能由传统经验丰富团伙的附属机构组成。

2024 年勒索软件攻击升级到新高度，威胁规模和复杂程度超过了 2023 年。攻击者比前一年更加激进，使用双重和三重勒索等高级策略。

二、攻击手法

勒索攻击的过程总体上可以分为三个阶段：（1）初始入侵，进入目标网络，并创建立足点；（2）实施网络侦察和凭证收集，并进行权限提升和横向移动，在此过程中还伴随着建立持久化和禁用安全防护措施的操作；（3）渗出数据，并通过部署勒索软件加密、删除原始数据等方式实施勒索。根据以上划分，勒索攻击除了最后一

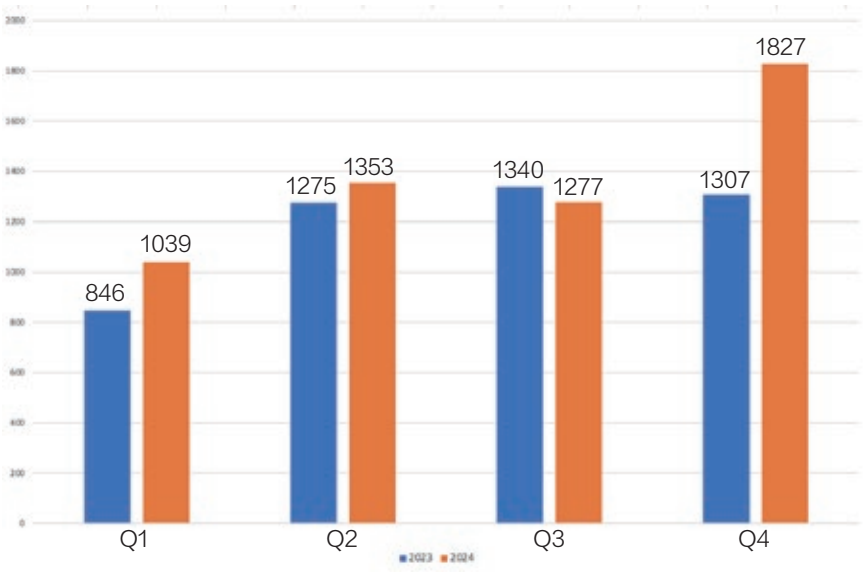


表 1 2024 年全球勒索攻击活动

个阶段，前两个阶段和针对目标机构的渗透攻击过程基本一致。

在 2024 年勒索攻击活动中值得关注的攻击手法包括：不同攻击环节出现的漏洞利用、各类初始入侵方式、合法工具被滥用于数据渗出。

（一）不同环节的漏洞利用

如果目标网络存在未及时修补漏洞的软件产品，很可能会被攻击者利用。在今年的勒索攻击活动中，多个漏洞被攻击者用于进入目标网络、植入恶意软件和提升权限等目的，其中不少是已披露的漏洞，而非 0day 漏洞。

漏洞编号	相关产品	勒索软件 / 攻击组织	漏洞用途说明
CVE-2024-1708 CVE-2024-1709	远程桌面管理软件 ScreenConnect	Black Basta、Bl00dy 勒索组织 [164]	植入木马和勒索软件
CVE-2024-27198 CVE-2024-27199	TeamCity CI/CD 服务器	Jasmin 勒索软件 [165]	植入勒索软件
CVE-2024-1853	Zemana AntiLogger	Qilin 勒索组织 [120]	恶意软件 Killer Ultra 使用 BYOVD 技术借助该漏洞禁用 EDR
CVE-2024-37085	VMware ESXi	Black Basta 勒索软件 [124]、BlackByte 勒索组织 [133] 等	提升权限
CVE-2024-3400	PanOS 防火墙	Fox Kitten 组织 [134]	获取目标网络初始访问权限
CVE-2024-21887	Pulse Secure/ Ivanti VPN	Fox Kitten 组织 [134]	获取目标网络初始访问权限
CVE-2024-24919	Check Point 安全网关	Fox Kitten 组织 [134]	获取目标网络初始访问权限
CVE-2024-40766	SonicWall SSL VPN	Akira、Fog 勒索软件 [138, 154]	获取目标网络初始访问权限
CVE-2024-40711	Veeam 软件	Akira、Fog 勒索软件 [150]	提升权限

表 2 2024 年勒索攻击活动涉及的漏洞

（二）多样化的初始入侵方式

除了借助网络边界设备的漏洞进入目标网络，勒索攻击团伙还会采用以下不同的方式实现初始入侵。

(1) 暴力破解登录密码

EstateRansomware 勒索组织的一次攻击活动，始于对 FortiGate 防火墙 SSL VPN 账户的暴力破解 [118] 攻击者以防火墙设备为跳板，通过 RDP 接入受害者网络的另一台服务器，创建立足点后执行后续攻击操作。

(2) 网络钓鱼邮件传播恶意软件

UNC4393 攻击团伙部署 Black Basta 勒索软件，曾借助多种由网络钓鱼邮件传播的木马和后门恶意软件，包括 QAKBOT、DARKGATE。Head Mare 组织在针对俄罗斯企业机构的勒索攻击中，通过网络钓鱼邮件的附件投递自定义恶意软件 PhantomDL 和 PhantomCore，实现对攻击目标的初始访问。

(3) 利用合法身份凭证

利用合法身份凭证是最为隐蔽的初始入侵方式，攻击者收集这些合法身份凭证有多种渠道，如通过早期攻击活动主动窃取、从地下市场购买、寻找受害者因错误配置而泄露的敏感信息。

Crypt Ghouls 组织疑似通过攻击目标单位的承包商，得到承包商的登录信息，然后从承包商网络的 VPN 接入目标单位的内部系统。SCATTERED SPIDER 团伙可能会从地下论坛购买 AWS、Azure 和 GCP 等云平台的身份验证令牌和用户凭证 [140]。如果受害者对服务和源代码配置不当，可能会导致身份凭证等敏感信息泄露，进而被攻击者利用，泄露源包括托管在 GitHub 平台上含有硬编码凭证的源代码、Web 应用暴露的 .env 环境文件。

(4) 使用社会工程学手段

Black Basta 勒索软件攻击团伙伪装成攻击目标组织的 IT 服务或支持团队人员，攻击前向目标组织内的受害者发送大量电子邮件，通过 Microsoft Teams 联系受害者，假装提供帮助，说服受害者为完成故障排查，在计算机上安装合法的远程管理控制工具，

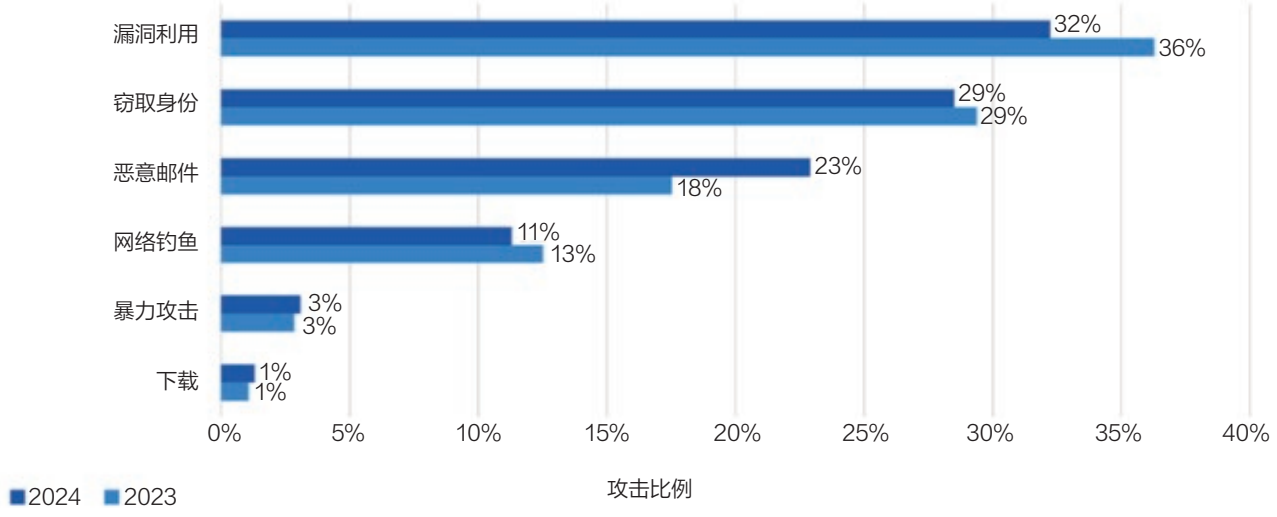


表 3 2024 年全球勒索攻击手法

如 QuickAssist、AnyDesk 等，攻击者趁机获得对受害者设备访问权限，接下来部署其他恶意软件。

（三）滥用于数据渗出的合法工具

勒索攻击者常用 Rclone 和 WinSCP 完成攻击中的数据渗出操作。在 2024 年的勒索攻击活动中，还有其他合法工具被发现用于数据渗出。

INC Ransom 团伙在一起攻击活动中的数据泄露可能使用了开源备份工具 Restic。SCATTERED SPIDER 团伙使用 AirByte、Amazon S3 浏览器、Stitch 等 ETL（Extract Transform Load，提取转换加载）工具将受害者环境中的数据同步和泄露到指定的远程存储服务。

BianLian、Rhysida 等勒索组织借助 Azure 存储资源管理器和 AzCopy 泄露敏感数据，Azure 存储资源管理器适用于 Windows、Linux、macOS 设备，提供图形化界面管理各种 Azure 存储类型和组件，并支持文件夹 / 文件上传和下载功能。伪装成 LockBit 的 Go 勒索软件利用 Amazon S3 Transfer Acceleration（传输加速）功能，将受害者的文件泄露到攻击者控制的 S3 存储服务。

2024 年勒索攻击中值得关注的手法包括：
不同攻击环节出现的漏洞利用、
各类初始入侵方式、合法工具被滥用于数据渗出。

三、攻击活动特点和趋势

（一）勒索仅仅是出于经济目的

2024 年披露的勒索攻击活动不完全是出于经济利益，一些勒索攻击以对目标组织的破坏性攻击为目的，甚至涉及国家背景的 APT 组织。

在俄乌冲突背景下，多个针对俄罗斯和白俄罗斯的的黑客组织出现，其中包括 Head Mare 和 Twelve 等攻击团伙，这些团伙针对受害者组织部署 LockBit 3.0 和 Babuk 勒索软件，Twelve 团伙还会运行数据擦除器恶意软件销毁加密数据，防止数据被恢复，表明攻击者希望对受害组织造成最大伤害。

部分勒索攻击事件还出现 APT 组织的身影。一起 Play 勒索软件攻击事件的受害组织曾被东亚地区的 Andariel 组织入侵。中东地区的 Fox Kitten 在针对美国等国的攻击活动中，向多个勒索组织提供目标网络的访问权限，并同这些勒索组织合作，制定勒索受害者的方法策略。

（二）攻击团伙间存在复杂的关系

从初始入侵到部署勒索软件的整个攻击流程，不一定由单个团伙实施。勒索软件部署者可以借助其他团伙攻击时所获取的访问权限进入网络。

UNC4393 团伙通过与投递 QAKBOT、DARKGATE、SILENTNIGHT 等木马后门恶意软件的多个团伙合作，获得对勒索目标的初始访问，然后部署 Black Basta 勒索软件。

勒索团伙使用的攻击武器也可能由其他团伙提供。FIN7 团伙制造的用于禁用安全软件的恶意工具 AvNeutralizer 早期与 Black Basta 勒索软件攻击活动有关，由于该工具在地下论坛进行售卖，导致现在它出现在 AvosLocker、MedusaLocker、BlackCat、Trigona 和 LockBit 等多种勒索软件的攻击事件中。

勒索攻击世界中不乏团伙更名或分支机构派生的情况。以泄露、售卖等多种途径被传播的勒索软件源码也让不同勒索团伙之间的关系变得交错。BlackSuit 勒索软件疑似为 Royal 勒索软件的新名称或者变种，Cicada3301 勒索团伙可能源自 BlackCat/ALPHV 勒索软件组织，Lynx 勒索软件与出售的 INC 勒索软件源码有关。

（三）勒索攻击涉及多种平台和环境

勒索攻击对象覆盖了 Windows、Linux、macOS、FreeBSD 等多个平台。

BlackSuit 勒索软件以 Windows 和 Linux 用户为目标，伪装成 LockBit 的 Go 勒索软件，目标运行环境是 Windows 和 macOS，Interlock 勒索软件针对 FreeBSD 服务器发起攻击。

VMware ESXi 虚拟化环境已成为多种勒索软件的攻击目标，且不少 Linux 平台的勒索软件均指向 ESXi 服务器和虚拟机。Eldorado 勒索软件的加密程序有 4 种格式，分别为 esxi、esxi_64、win 和 win_64。

Play 勒索软件针对 ESXi 环境的 Linux 变种，在执行前会验证是否在 ESXi 环境中运行，从而避免在其他环境中被检出 [122]。ESXi 漏洞 CVE-2024-37085 被多个勒索攻击团伙利用，用于获取已加入域的 ESXi 虚拟机监控程序的完全管理权限，进而影响到整个 ESXi 服务器和所有虚拟机。

勒索攻击也会发生在云环境中。攻击者将受害者存放在云环境中的数据渗出之后，直接借助此前获取的权限删除受害者数据，留下勒索信或邮件告知受害者。

2024 年披露的勒索攻击活动
不完全是出于经济利益，
一些勒索攻击以对目标组织的破坏性攻击为目的，
甚至涉及国家背景的 APT 组织。

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

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

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

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

网络犯罪研究中心

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

极牛攻防实验室

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

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

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

专业的团队服务

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

众多的行业案例

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

深入的厂商合作

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

全国范围的服务

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

从安全工具到数字化平台：企业浏览器的崛起与未来

当前，浏览器已从单纯的访问工具演变为数据安全的第一道防线，企业浏览器更是从“可选工具”进化为“数字基建的核心组件”。在政策驱动、技术革新及市场需求的三重因素推动下，企业浏览器市场即将迎来爆发式增长。

本文基于赛迪报告与行业热点对企业浏览器的应用价值与未来发展，进行深度解读。

一、企业浏览器的市场现状

根据赛迪顾问《中国企业级安全浏览器市场研究报告（2024）》提供的数据，2023 年中国企业浏览器市场规模已达 2.5 亿元人民币，预计 2026 年将达到 5.5 亿元人民币，年复合增长率高达 30%。这一增长数字背后，是政企机构对“浏览器作为数字化办公核心入口”的战略性认知转变。随着 Web 化办公的全面普及（90% 的办公系统为 Web 应用，平均每个团队使用 40~60 个 Web 应用，员工 85% 以上的工作日时间是在浏览器上度过的），浏览器已从单纯的访问工具演变为数据安全的第一道防线。

在国际市场上，企业浏览器的资本赛道日益火热，热度持续攀升。2025 年 2 月初，企业浏览器厂商 Island 正处在由投资公司 Coatue Management 领投的一轮融资中，估值达 45 亿美元；2023 年，Talon Security 被 Palo Alto Networks 以 6.25 亿美元收购。此外，行业巨头们也纷纷入局，Google 推出了 Chrome Enterprise Premium，微软推出了 Edge for Business，这些事件也无疑为全球企业浏览器市场注入了强进动力。

根据 Gartner 的预测，到 2026 年 60% 的企业将使用专用浏览器作为核心安全控制点，预计将替代至少 3 种传统安全工具。

值得注意的是，国内安全厂商展现出更强的创新势能。例如，奇安信、360 等网络安全厂商在海外尚未提出企业浏览器的概念时，便已推出了相应产品。展现出国内厂商在网络安全行业的创新突破。

表 1　企业级浏览器与个人版浏览器对比

	企业级浏览器	个人版浏览器
使用场景	办公	日常上网
解决痛点	浏览器运维难题、浏览器技术断供难题、数据安全防护挑战；信创迁移、密评合规挑战	上网冲浪、游戏娱乐、影音视频； 网速（缓存加载）、内容丰富性等问题
解决方案集成	企业浏览器可联动其他产品组合成不同的解决方案，例如：零信任安全防护体系、数据安全防护体系等	无
其他能力	可满足企业需求进行深度定制	无

数据来源：赛迪顾问　2024，07

二、企业浏览器重构了安全技术范式

由于 Web 应用成为主流，通过 Web 应用产生的数据泄露事件日益增加。数据显示，80%的数据泄露来自 Web 应用程序和电子邮件（主要通过

浏览器访问），53% 的企业对自己解决未管理 / 管理不善的设备中的安全问题的能力没有信心（只有 6% 的企业非常有信心），这表明现有的安全技术并未很好地解决 Web 应用的数据安全问题。

与此同时，传统的安全防护依赖多层独立工具（如防火墙、DLP、VPN 等），形成复杂且低效的“堆叠式”架构。而企业浏览器通过将安全能力原生集成到浏览器本身，在可见性、控制力、防护力、用户体验和部署成本等方面具备独特优势，真正实现从“堆叠式安全”到“原生集成”的范式升级，具体表现如下。

1. 工具替代：企业浏览器可以替代 VDI（如 Citrix、VMware）、安全网关（如 Zscaler）、Web 隔离（如 Menlo Security）等至少 5 类传统工具，从而减少 30% 以上的综合成本；

2. 攻击面收敛：浏览器作为统一入口，集中管控 90% 以上的 Web 应用访问行为，减少因多工具接口不一致导致的安全盲区；

3. 策略一致性：传统方案需跨终端、网络、云端配置策略，易产生规则冲突。企业浏览器支持基于身份的动态访问控制（集成零信任），确保策略在混合办公场景下无缝生效。这不仅提升了策略的实施效率，还降低了企业合规管理的复杂度；

4. 落地便利性：企业浏览器与市面上的主流浏览器（如 Chrome、Edge）保持一致的使用体验，集成的安全功能通常在员工正常使用流程中自然触发，不会产生工作流摩擦造成员工抵触。此外，企业浏览器也能透明地获取业务访问中的相关数据，并进行标准化处理，大幅降低后续的数据运营成本。

图 1 企业级安全浏览器功能特点



数据来源：赛迪顾问 2024，07

三、国产企业浏览器的独特价值

国产企业浏览器不仅在数据安全方面发挥着作用，还在多个其他场景展现了独特价值：

1. 统一浏览器管理。自 2008 年 Google 发布 Chrome 浏览器以来，其全球市场占有率快速提升，并早已成为全球 Web 领域的事实标准。国际上的多数业务系统默认基于 Chrome 浏览器进行开发，随着 Chrome 版本的迭代，业务系统的接口更新也迅速跟进。然而，国内浏览器在这一过程中通过集成双内核引擎，实现了对基于 Chrome 和 IE 内核的业务系统的兼容，同时还延续了支持 Chrome 迭代过程中所废弃的重要接口（如 Flash、NPAPI 等），客观上推迟了国内 Web 开发标准的迁移速度。

因此，在近二十年的数字化建设过程中，国内并存大量的基于不同内核、不同版本的浏览器建设的业务系统，企业需要多款浏览器进行管理，运维工作因此变得愈加复杂。通过部署统一的企业浏览器，可以实现一款浏览器对企业内部的业务系统全面兼容，避免员工在工作中频繁切换浏览器，还能避免消费者浏览器接口变动导致的业务中断，同时通过集中管理平台也能降低运维成本，提高效率。

2. 信创平台兼容。信创平台作为我国自主研发的全新计算平台，国产浏览器进行了深度适配优化。而国际

主流浏览器（如 Chrome、Edge）并未针对信创平台开发专用版本，且其 Linux 版本在信创平台上存在兼容性问题，不能满足信创平台的使用要求。此外，信创平台不支持 IE 内核，导致访问基于 IE 标准建设的业务系统时出现兼容性难题。国产企业浏览器则提供了相应解决方案，可以保障企业业务系统的平稳过渡。

3. 密评合规。随着《中华人民共和国密码法》《网络安全等级保护条例》和《商用密码管理条例》等法规的推进，浏览器需支持国产密码算法以满足合规要求。国产企业浏览器能够集成这些算法，确保企业在业务访问中的合规性。

企业浏览器的另一个优势在于其定制化能力，通过定制化的企业浏览器，可以帮助企业打通应用开发、终端运维的权限管理、数据流转等环节。为企业提供便捷高效的解决方案，推动了企业浏览器逐渐成为统一的业务访问平台。

四、企业浏览器未来发展趋势

根据 Gartner、赛迪等机构的预测，未来几年，企业浏览器市场将继续呈现高速增长趋势。Gartner 预测，2027 年企业浏览器将成为企业超级应用战略的核心，并推动企业安全的重大转型。

企业浏览器厂商应意识到，组织需要的不仅仅是一个具有安全特性的消费者浏览器，它们需要一个完整的平台，能够将安全性、合规性和生产力工具深度整合到员工日常工作的核心区。从分散的工具到以浏览器为中心的企业平台的转变，有望通过使浏览器本身成为企业工作环境的基础。

未来企业浏览器将在以下几个方面持续演进。

1. 更强大的安全能力：企业浏览器将通过集成更多的安全能力（如 UEBA），取代更多的传统安全工具。此外，企业浏览器将与终端安全工具（如 EDR）、数据安全工具（如 DLP、RBI）、网络安全工具（如 CASB、云防火墙）深度协作，构建更为精细化的多层次防护网，深入实现零信任细粒度的动态访问控制，并成为 SASE 解决方案的重要组成部分。

2. 智能办公赋能：企业浏览器将进一步渗透到员工的工作流中，集成 AI 工作流引擎，分析员工的浏览行为和需求，为不同的业务场景提供个性化的智能建议和优化。通过集成的低代码自动化构建器，帮助员工在熟悉的工作流程中便捷实现任务自动化，显著提高工作效率和准确性。

3. 生态开放平台化。企业浏览器将逐步发展为一个开放平台，连接更多企业安全、运维及生产力工具。它将通过标准化 API 和插件接口，与其他企业工具（如身份认证、数据加密、自动化运维系统等）无缝对接，推动工作生态的灵活构建。此外企业浏览器将在合规框架下，通过标准化的数据传输与分析接口，将浏览数据、行为数据和安全事件数据发送到外部分析系统（如 SIEM、SOC）。帮助企业进行安全事件监控、数据分析和趋势预测，进一步提高企业的响应能力和数据价值。

五、企业浏览器供应商选择建议

由于企业浏览器具备平台化基础设施的特性，企业用户在选择企业浏览器供应商时，需要进行综合考虑，应特别关注以下因素。

- 厂商规模与经验
- 产品方案能力
- 产品创新能力
- 生态协同能力
- 产品可扩展性

总之，企业用户应选择具有长期稳定支持能力、强大创新动力的供应商，确保在未来的数字化转型中获得持续的技术保障。

结语

企业浏览器已从“可选工具”进化为“数字基建的核心组件”。在政策驱动（如数据安全法）、技术革新（如 AI、GPT）与市场需求（BYOD、混合办公）的三重因素推动下，企业浏览器市场即将迎来爆发式增长。厂商需以技术为矛、生态为盾，在竞争激烈的市场中抢占先机，推动企业浏览器的快速普及和发展。市场和客户也应加快认知转型，将企业浏览器视为企业数字化战略的重要组成部分，积极推动其在安全、生产力和协同办公中的应用，推动行业规范的制定与标准化，促进整个生态的健康成长。

特朗普网络团队任命 预示美国政府将转向进攻性网络政策

编者按：美国总统特朗普已任命多名进攻性网络行动的倡导者担任国家安全委员会关键网络职务，预示美国政府未来将采取更加强硬和主动的网络政策。

美国国家安全顾问迈克·沃尔兹预测，在特朗普第二任期内，美国可能会展现出更多的攻击能力，以威慑国家行为者。迈克·沃尔兹曾表示，美国需要改变多年来专注于提高网络防御的做法，转而采取更强硬的立场并开始采取攻势，让恶意国家和个人行为体付出更高的代价并接受惩罚；历史情况表明，仅通过加强网络防御已无法阻止日益增多的网络攻击，美国需要转变理论和政策，通过向对手展示自身所具有的“毁灭性”攻击性能力来重建威慑力。

美国国家安全委员会网络事务高级主管阿列克谢·布拉泽尔是迈克·沃尔兹的论调的支持者，并一直强调使用攻击性网络行动的必要性。阿列克谢·布拉泽尔曾表示，美国当前的网络空间防御行动是“僵化和规避风险的官僚主义”的产物，只发表声明却不采取实际行动；美国必须停止害怕运用所拥有的“令人难以置信的攻击性网络力量”。阿列克谢·布拉泽尔的下属将包括艾米丽·戈德曼、JD·沃克和罗伯特·布罗斯。

艾米丽·戈德曼曾担任美国网络司令部的网络战略家，在特朗普第一任政府期间曾参与制定了美国网络司令部激进的“持续交战”战略，该战略直接催生了美网络司令部的“前出狩猎”行动。JD·沃克曾担任美国国防大学网络情报与战略专业教授，其坚决反对通过要求私营部门承担更多责任来保护美国网络。JD·沃克表示，通过减少漏洞进行威慑的做法将防御性网络行动及数字取证和事件响应作为主要响应行动方案，这减轻了政府机构的责任，并将直接对抗敌对外国军事和情报部门的任务和风险转嫁给私营部门；美国需要采取更加积极的政策，实施综合性反网络行动，通过





进攻性网络行动削弱对手的能力，并结合其他非网络国家权力工具让对手付出代价。罗伯特·布罗斯将担任网络情报主管，曾任职于美国国家情报总监办公室，其情报界背景可能助益于网络攻击行动；曾担任过中国和东南亚专家，这可能表明美国国家安全委员会网络团队的“地理重点”。

（奇安网情局编译有关情况，供读者参考。）

美国国家安全委员会的四名关键网络工作人员现已到位——其中多人一直是进攻性网络行动的坚定倡导者，这可能预示着美国总统特朗普的网络政策走向。

美国国家安全委员会是美国总统用来审议国家安全、军事和外交政策事务的国家安全委员会。该委员会设在白宫，是美国总统行政办公室的一部分，由高级国家安全顾问和内阁官员组成。特朗普对美国国家安全委员会成员的任命表明，在近年来遭受的数次美国网络遭入侵事件后，美国政府希望在网络空间采取更积极的措施。

大多数拥有网络能力的国家都会开展“进攻性网络行动”，即主要旨在通过网络空间产生影响的行动，而不是主要旨在收集情报或提供网络“球门线”保护的行动。无论是在和平时期还是在战争时期，进攻性网络行动通常都涉及影响、误导或以其他方式影响竞争对手或对手的认知，如植入虚假信息。但进攻性网络行动也可用于破坏，这可能包括从低级的暂时中断政府网站或切断犯罪集团的互联网连接，到高级的破坏国家关键基础设施的一部分。这可能包括破坏一个国家的电网，就像俄罗斯在俄乌战争前和战争期间所尝试的那样。在战时，进攻性网络行动还可用于破坏对手的指挥控制、武器系统和态势感知。

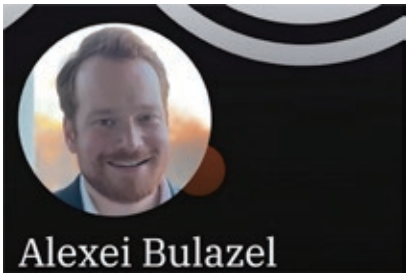
美国国家安全顾问迈克·沃尔兹在政府成立初期就定下了基调。迈克·沃尔兹预测，在特朗普第二任期内，美国可能会展现出更多的攻击能力，以威慑国家行为者。

迈克·沃尔兹 2024 年 12 月接受媒体采访时曾表示，“多年来，我们一直在努力提高网络防御能力。我认为，我们需要开始采取攻势，对那些继续窃取我们的数据、继续监视我们的私人行为者和国家行为者施加更高的代价和惩罚……我认为我们需要采取更强硬的立场。”

迈克·沃尔兹 2025 年 1 月接受媒体采访时表示，“在网络攻击方面，我们一直在努力防御，并且我们一直在努力把防御做得越来越好。我们将为他准备的其中一种理论或政策转变是，我们能否在进攻方面做得更好？我们如何改变行为？如果你无法阻止每天发生的数百万次攻击，我们如何重建威慑力，以便让其中一些行为者，尤其是国家行为体停止其行径？我个人认为，如果你在我们的港口和电网中放置网络定时炸弹，我们也可以对你这样做，所以让我们都不要——相互确保毁灭——并缓和一下气氛。这就是我认为我们可能会看到转变的一个例子。”

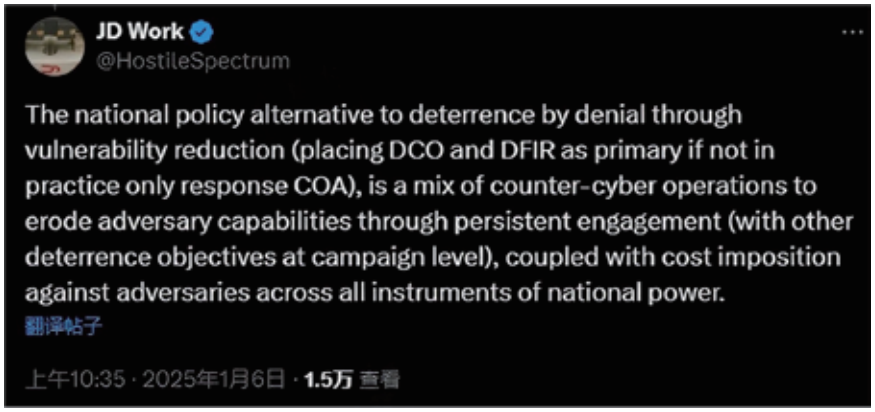
与此同时，迈克·沃尔兹的国家安全委员会顾问们表示，他的想法将会拥有热切的支持者。

位于网络指挥链顶端是阿列克谢·布拉泽尔，他担任美国国家安全委员会网络事务高级主管。阿列克谢·布拉泽尔拥有私营部门网络安全背景，并曾在特朗普第一届政府的国家安全委员会担任网络政策主管。



阿列克谢·布拉泽尔一直强调使用攻击性网络行动的必要性。他曾于 2024 年 12 月 25 日在社交媒体发帖呼应迈克·沃尔兹的说法，称：“美国拥有令人难以置信的攻击性网络力量。我们必须停止害怕使用它。”

阿列克谢·布拉泽尔还对美国当前的网络空间防御行动提出了批评，



称其是“僵化和规避风险的官僚主义”的产物，只发布“新闻稿”而不是采取行动。

阿列克谢·布拉泽尔手下是艾米丽·戈德曼，她曾担任美国网络司令部的网络战略家。

艾米丽·戈德曼曾在特朗普第一任政府期间参与制定了激进的“持续交战”战略，后来还合著了一本有关该战略的书。“持续交战”术语涵盖了美国的活动，例如，“前出狩猎”行动，即美国派遣网络安全团队到国外，以根除盟友网络中的对手恶意软件。

与艾米丽·戈德曼一同参与研究的还有前美国情报官员、后来担任美国国防大学网络情报与战略专业教授的 JD·沃克。

JD·沃克反对简单地保护美国网络，他认为这是将责任转嫁给私营部门。他曾表示：“对于政府中的许多人来说，甚至在业界，误解或曲解有关应对网络威胁的政策选择的基本论点是很常见的。通过减少漏洞进行威慑的论点受到青睐，因为它允许放弃政府责任，并将直接对抗敌对外国军事和情报部门的任务（和风险）转嫁给私营部门，这是其他战争领域所没有的。当顽固的对手取得立足点、维持访问权限或产生影响时，这使得责任可以从官僚机构转移开。它避免了必须提倡在特定情况下可能失败的干预措施，甚至只是结果与预期不同，因为没有任何计划能够在与敌人接触后幸存下来——而软性建议首先没有可衡量的结果。另一种选择是采取积极的政策，需要做一些对于那些没有足够技术和操作经验的人来说难以理解的困难事情。这些都是罕见的经验，不仅仅是系统管理员或补丁管理甚至数字取证和事件响应活动，而且只能通过参与网络活动才能获得。因此，从克制和其他冷战遗留概念的角度来反对这些新想法是很流行的，但没有完全理解这些新想法与在线活动的联系。但旧的东西显然不起作用，而且我认为不能按照所追求的方式起作用。

JD·沃克认为，防御政策的替代方案将包括“削弱对手能力”的进攻行动，并结合其他非网络工具。他称，“通过减少漏洞（将防御性网络行动及数字取证和事件响应作为主要响应行动方案）来替代拒止威慑的国家政策是反网络行动的结合，通过持续交战（以及战役层面的其他威慑目标）削弱对手的能力，再加上运用所有国家权力工具向对手施加成本。”

两位知情人士透露，最新加入该团队的是罗伯特·布罗斯，他已被任命为网络情报主管。一位不愿透露姓名的美国白宫发言人证实了这一任命。

罗伯特·布罗斯曾任职于美国国家情报总监办公室。他还担任过中国和东南亚专家，这可能表明美国国家安全委员会网络团队的地理重点。

罗伯特·布罗斯很少公开发表有关网络攻击的文章。他曾于 2015 年发表题为《赛博战、网络战和赛博防御的未来》的文章称，“正如赛博防御组织被要求对抗赛博战（cyberwar）一样，网络战（netwar）组织或精通网络战的网络防御组织也越来越需要对抗网络战。”他的履历表明，他将为这份工作带来对情报界的深入了解，这一背景很可能对网络攻击行动大有裨益。

关于作者



赵慧杰

虎符智库专家、网络空间安全军民融合创新中心高级研究员。长期从事网络安全、互联网发展等领域研究工作，对外军网络战、国际网络安全态势、全球网络空间竞合及新技术新应用发展等具有深厚研究造诣，先后获得军内成果奖七项。

首席安全官的权力悖论：为何责任越大权力越小？

首席信息安全官并不能完全掌控其领域，但是当出现问题时却需承担责任。这种高风险的权力不平衡，可能会付出高昂的代价。

首席安全官（CSO）或首席信息安全官（CISO）的头衔表明，该职位具有与其他“首席”官员（如首席执行官或首席财务官）相同的权力——可以掌控组织的安全运营、战略和资源分配。

但对于大多数 CISO 来说，真正的指挥权往往是一种令人沮丧的幻觉。他们肩负着保护组织敏感信息的责任，但却没有实际权力自主做出重要决策。

对于许多人来说，指挥的权力（即对决策、资源和人员的控制）是有效领导的基础。在军事等领域，指挥与责任是同义词；领导者可以承担责任，因为其有权采取行动。

对于 CISO 来说，缺乏指挥权力不仅是一个挑战，更是一个根本缺陷。

> CISO 尽管拥有“首席”地位，
> 但许多人缺乏做出影响组织安全态势的决策权。
> 如果 CISO 必须不断听从其他高管的意见，
> 可能会削弱团队对 CISO 和组织安全承诺的信心。

CISO 角色的现实情况是，尽管拥有“首席”地位，但许多人缺乏做出影响组织安全态势的决策权。批准预算、部署关键缓解措施和实施政策变更的权力通常分散在其他高管领导手中。

网络安全的投资、政策甚至人员配置的决策通常属于首席财务官、首席信息官甚至首席执行官的职权范围。对首席信息安全官来说，这种情况就像被要求保护城堡，但又无法完全控制城堡的防御。他们识别风险、提出解决方案并制定战略计划，但执行取决于其他人的批准、时间表和优先事项。

CISO 被迫向上级“推销”安全重要性

缺乏指挥权使得网络安全决策对 CISO 来说变得乏味且常常令人沮丧。尽管人们期望首席信息官期望快速行动，在安全事件发生现前能够预测并消除风险。但如果没有指挥，他们就会陷入“推销”安全投资重要性、等待批准及依赖他人确定投资优先顺序的循环中。

这种持续的投入需求会减慢响应时间，并为安全事件发生创造机会。在网络安全领域，时间就是一切，这些延迟可能会造成高昂的代价。

除了时间安排，指挥权对战略协调和授权也至关重要。在 CISO 缺乏

真正指挥权的组织中，他们被迫被动而不是主动地采取行动。

例如，CISO 可能认识到需要高级威胁检测软件或扩大员工培训，但如果无法掌控预算和资源分配，他们就无法直接实施这些计划。相反，他们必须证明这笔开支的合理性，让利益相关者相信这些计划的重要性，并希望与其他业务重点保持一致。这种依赖性削弱了其战略能力，迫使其不断验证其角色的必要性。

让其他高管理解和了解网络风险的挑战，也增加了首席信息安全官的负担。网络风险不像财务或运营风险那样简单，可以使用成熟的指标和绩效指标来量化和评估。网络风险往往模糊而抽象——新漏洞会在一夜之间出现，威胁不断演变，网络攻击的后果也可能千差万别。

即使没有完全的权力，仍需承担责任

对于许多不熟悉网络安全的高管来说，网络风险的紧迫性可能难以理解，这使得 CISO 不得不持续证明其策略的合理性。这种“说服”并不是对其他高管职位的典型要求，它会让 CISO 的工作感觉像是一场持续的艰苦战斗。

这种情况尤其具有挑战性的原因，归根结底是首席信息安全官仍要为失败负责。当发生黑客入侵或暴露漏洞时，首席信息安全官首当其冲。尽管首席信息安全官应该管理和预防这些安全事件，但如果没有权力实施必要的措施，他们注定会失败。

这种情况其他高管中少有经历：例如，首席执行官通常可以控制与公司战略方向和资源相关的决策，首席信息安全官则需要防止网络入侵，而没有同等程度的控制权。有问责制，但没有指挥权，这种模式不会让任何人取得成功。

这种缺乏控制力的情况不仅会影响组织的安全，还会影响 CISO 的内部和外部关系。CISO 经常需要与董事会成员、同事和利益相关者沟通，以解释安全计划、应对潜在威胁并讨论风险缓解策略。

缺乏权威削弱对 CISO 的信心

没有命令，他们只能提供建议，而不能执行。在同事看来，这会让 CISO 看起来像一个中层管理者，而不是领导者；在董事会看来，CISO 似乎无法完全履行职责。随着时间的推移，这既会削弱人们对该职位的信任，也会削弱 CISO 从组织获得所需支持的能力。

在组织内部，缺乏指挥权也会影响 CISO 与其团队的关系。安全团队需要采取紧急行动，实时响应威胁并根据需要实施新规定。如果 CISO 无权对资源使用和实施必要变革做出最终决定，团队士气可能会受到影响。

在能够做出自信、明确决策的领导下，安全团队会蓬勃发展，但如果 CISO 必须不断听从其他高管的意见时，这可能会削弱团队对 CISO 和组织安全承诺的信心。

CISO 缺乏指挥权对组织整体安全态势产生了切实的影响。如果 CISO 认识到迫切需要更新安全工具或增加人员，但在保护相关资源方面却不断遇到障碍，显然组织就可能容易受到威胁。在网络安全领域，等待批准或说服利益相关者可能是防止攻击和处理漏洞之间的区别。

CISO 需要有真正指挥权才能成功

如果组织想要真正保护自己，就应该认识到 CISO 需要真正的指挥权。最能发挥作用的 CISO 是那些能够完全控制负责领域、不受内部障碍困扰的安全负责人。

当企业考虑如何最好保护数据时，就应该扪心自问，是否真正为 CISO 的成功做好了准备。是否赋予 CISO 采取行动所需的资源、权力和自主权？还是只是指派 CISO 去承担一项高风险的责任，而没有权力去应对？

除非各类组织开始将 CISO 视为真正的领导者（拥有完全掌控权），否则网络安全将仍是充满挑战且不稳定的领域，其障碍和责任同样重要。



关于作者

Tyler Farrar

资深首席信息安全官 (CISO)，在网络安全领导、风险管理和保护多个行业的关键资产方面拥有丰富的经验。Tyler 目前领导 Exabeam 和 Maxar Technologies 的安全项目，负责监督安全运营、基础设施管理和美国政府项目保护。

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全



7436084028