

谨防境外 AI“后门”风险

近日,工业和信息化部网络安全威胁和漏洞信息共享平台(NVDB)发布风险提示,明确指出美国 Anthropic 公司旗下 AI 编程工具 Claude Code 存在安全“后门”隐患,危害严重。

Claude Code 是一款可根据文字需求自主完成代码编写、修复等工作的 AI 编程工具,在 2.1.91 版本至 2.1.196 版本中内置了隐蔽监控机制,可绕过用户授权,静默向境外服务器回传用户地域、设备标识乃至研发代码等核心敏感数据。

此前,阿里巴巴已率先将 Claude Code 列入高风险软件名单。从企业主动“拉黑”到国家级平台公开警示,这一事件为我们敲响警钟:AI 虽好用,但安全防线绝不能失守。

Claude Code“后门”事件绝非孤例,它暴露了 AI 时代安全的深层困境。

其一,AI 工具的权利边界正在失控。相较传统软件,AI 编程工具拥有读取代码库、编辑文件、运行命令等“超级权限”。这种

“超级权限”使其成为窃取商业机密、进行供应链污染的绝佳突破口。

其二,地缘政治因素加剧了安全风险。Claude Code 内置的隐蔽监控机制会读取用户系统时区,精准识别并标记中国用户。在技术博弈日益复杂的背景下,海外 AI 工具的可信度正面临严峻质疑。

应对 AI“后门”风险,不能仅靠事后卸载补救,企业、开发者、行业监管需构建全链条防护体系,守住 AI 使用安全底线。

立即开展全面排查与清理。针对 NVDB 通报的受影响版本,各单位和个人应立即停止使用并彻底卸载相关软件。对于政企核心业务网段,应加强网络边界管控,通过流量监测等手段拦截 AI 工具的异常外联行为,严防敏感数据违规出境。

树立“最小权限”与“数据隔离”原则。在使用任何 AI 编程或办公工具时,坚决拒绝授予超出实际需求的系统权限,避免让 AI 工具直接处理企业核心代码、客户隐私、财务

凭证等敏感信息。对于必须使用的 AI 功能,应尽量在物理隔离或严格沙箱环境中运行,确保数据不出内网。

加速推进国产 AI 工具的替代与适配。此次事件暴露出过度依赖境外 AI 基础设施的巨大风险。当前,国内科技型企业已推出多款 AI 编程工具,在中文场景理解、代码补全等方面已具备较强竞争力,且数据合规路径清晰。政企单位应抓住政策窗口期,加快国产工具的测试与部署,从根本上筑牢数字安全防线。

强化日常安全审计与法律意识。开发者应养成定期审查 AI 工具出站流量的习惯,排查未经授权的数据携带行为。同时,要严格遵守相关法律法规,明确 AI 工具使用的合规红线。

Anthropic 长期以来将“透明、可信、责任”作为核心理念,但此次曝光的隐蔽监控机制却与这些公开承诺相悖。Claude Code“后门”事件是一面镜子,照见了 AI 时代供应

链安全的脆弱性,也照见了部分境外科技型企业对用户傲慢与偏见。

AI 越智能,越需要安全的缰绳。工信部的及时预警,是对整个行业的一次深刻警示。技术可以跨越国界,但数据安全必须守住底线。唯有将安全意识嵌入每一次代码提交、每一次工具调用,方能在享受 AI 红利的同时,不让“后门”成为数据资产的漏洞。



□ 本报记者 谢瑶

开发区在转型③

“整合重组”激发市场活力

园区整合重组,是国家级开发区提质增效、破解碎片化发展的关键改革。2022 年,湖南湘江新区完成里程碑式体制优化,将原湘江新区、长沙高新区、长沙岳麓区平台资源全面整合,托管长沙望城区部分街道,通过大部制、扁平化改革,推动原有 56 个党政机构精简为 20 个,在人员、职能、体系层面实现了整体性重构。

不同于各地园区简单的合并挂牌,湘江新区“三区合一”并非物理上的整合,而是先后完成产业布局、运营机制、队伍活力的全方位重塑,实现从“物理合并”到“化学融合”的实质性跨越。“十四五”期间,湘江新区 GDP 突破 5000 亿元,跃居全国国家级新区第六位,上市企业数量等 5 项关键指标位列国家级新区第二,交出了一份成色十足的改革答卷。

产业链条做精做优

改革之前,湘江新区的产业布局一度缺乏系统的链式发展思维。2023 年,新区全面铺开 15 条产业链;2024 年至 2025 年,进一步优化整合为 10 条。然而,随着产业发展深化,原有的 10 条产业链逐渐暴露出重点不够突出、资源配置交叉分散等深层次问题,“全域发力”陷入“全域不强”的发展瓶颈。

2026 年 3 月,湘江新区出台产业链建设新方案,将 10 条产业链进一步精简为航空航天及北斗、新材料、新一代信息技术及人工智能、先进装备制造(含智能网联汽车)、生物医药、检验检测 6 条,完成了从全面布局向重点突破的战略转型。

此次精简并非随意取舍,而是基于产业基础、科创优势、省市战略的精准筛选。湘江新区集中政策、资金、土地、招商资源,聚焦六大高成长性、高附加值、强带动性的核心产业。6 条赛道精准匹配湘江新区“2+4+N”现代化产业体系,深度对接长沙市重点产业链布局,实现与省市产业错位发展、精准互补。

“产业链不是越多越好,而是越准越好。”岳麓区科学技术局局长余亚锋介绍,精简的核心逻辑是聚焦突破、聚力攻坚,实现发展质量与规模同步提升。为适配新赛道布局,湘江新区重构资源配置体系,构建起“链长挂帅、链办牵头、专员负责”的工作架构,推动政策、资金、土地等要素向核心产业、龙头企业和关键技术集中倾斜。

赛道聚焦带来产业能级显著跃升。航空航天及北斗产业链依托北斗产业园实现全链条集聚,园区整体出租率为 100%,形成从芯片研发、终端制造到位置服务的完整生态;先进装备制造(含智能网联汽车)赛道集聚近 700 家关联企业,集齐五块国家级测试牌照,成为国内智能网联产业配套最完善的片区之一;新材料、检验检测等特色赛道持续突破技术瓶颈,填补省内多项产业空白。

为进一步在新赛道上加速领跑,湘江新区明确了“往深走、往实走、往准走”的实施路径:深调研,绘制产业图谱与清单;实培育,助力企业扩能倍增、成果转化;明确年度目标;准招商,建立信息共享机制,靶向引进核心企业,推动产业向高端化、专业化、精细化发展。

运营模式破旧立新

产业赛道重塑,离不开体制机制的护航。长期以来,部分园区存在政企边界模糊、管理模式单一等短板,发展高度依赖政策红利,市场化造血能力不足。依托“三区合一”改革契机,湘江新区直属的产业园



区——岳麓高新区率先试水市场化管理改革,推动核心竞争力从政策引导向专业运营迭代升级。

改革的核心是厘清政企边界,探索“小管委会+大公司”市场化模式。其中,岳麓高新区管委会聚焦园区顶层规划、政策制定、监督考核等核心职能,有序退出具体建设性、服务性事务,切实当好“掌舵人”。区属国企智谷集团作为市场化运营主体,全面承接片区综合开发、招商引资、企业服务、园区运营等市场化业务,获得完整的人事、财务、运营自主权。改革后,集团构建起党委、董事会、经理层“5+7+5”法人治理结构,6 家子公司协同效应显著,园区项目落地效率提升 40%。

为持续激活市场活力,园区以人事制度、考核机制改革为突破口,破除体制机制壁垒。智谷集团全面推行经理层契约化管理和不胜任退出机制,关键岗位实行“市场化选聘”,近两年从行业头部企业引进一批紧缺人才。同时配套建立市场绩效考核体系,提高营收、利润、项目落地率等市场化指标权重,实行奖优罚劣、末等调整,全面激发队伍活力。

在产业培育方面,园区聚焦智能网联、检验检测、新型储能材料、生物医药 4 个赛道,以“基金+招商”模式引育企业。产投公司构建“母子基金+专项基金”体系,总规模 24 亿元,撬动社会资金超 200 亿元,推动希迪智驾、伊鸿健康、锐异资环等重点企业入驻。基金投资企业中已有中微半导体、卡莱特等 8 家公司成功上市。

一系列靶向改革,推动岳麓高新区实现从政策依赖向市场驱动的蝶变。“过去是‘等政策、靠补贴’,现在按市场规则办事,决策快了、服务好了、活力也上来了。”岳麓高新区党工委委员、管委会副主任陈建湘说。2025 年,智谷集团全年实现营收 14.62 亿元,净利润 2.07 亿元。同时母子公司双 AA+ 的信用矩阵推动融资成本从 3.79% 降至 2.95% 以下,全年节省财务费用超 7500 万元。

人才生态筑巢兴业

制度改革、产业升级,归根结底是人的改革。“三区合一”前,原湘江新区、长沙高新区、长沙岳麓区人才政策标准不一、认定体系分立、服务资源分散,难以适配一体化发展布局。

整合后,湘江新区立足核心产业赛道,在落实省市人才政策基础上,制定出台新区人才政策,实施“湘江英才”集聚行动,围绕航空航天、人工智能、新材料等主导产业,量身定制分层扶持细则,同时放宽新兴业态、中小科创企业人才认定门槛,扩大政策覆盖范围。

“‘三区合一’带来的最大人才红利,就是告别各自为政,把分散的政策、资金、平台攥成一个拳头,精准对接产业刚需。”湘江新区人才服务中心主任银红玉表示,改革后不再简单以头衔、资历判定人才价值,而是以产业贡献、技术突破、项目实效为评价标尺,

让实干型、技术型人才真正享受政策红利。

政策革新同步带动激励机制优化。湘江新区加快人才资金拨付,2025 年累计兑现人才奖励资金 3.25 亿元,有效激发人才创新创业热情。依托整合后的科创载体,1009 家省级以上创新平台向全域人才开放共享,20 亿元人才支持基金配套支持,“柳枝行动”“红枫计划”及“揭榜挂帅”项目持续发力,引导人才扎根一线攻克技术难题。

在培育管理方面,湘江新区借助扁平化管理优势,深化校企协同育才,紧扣产业缺口,联合高校定制培养方案,选聘科技总监、产业教授深入企业车间与实验室,批量培育适配本地产业的技能人才与管理人才。同时统一搭建人才交流、研修深造平台,配齐青年人才驿站、国际人才社区、专家公寓等生活配套,提供医疗、安居、出行等标准化便利服务。

统一的政策体系、完善的配套保障,广阔的干事平台,推动湘江新区人才集聚效应持续增强。截至今年 4 月,湘江新区共集聚两院院士 38 人、国家级人才 134 人、省级人才 552 人,市两大人才工程 419 人、湘江英才 2776 人,人才总量超过 100 万人,高层次人才数量占长沙全市近一半,为新区产业升级和高质量发展夯实了根基。

湘江新区用实践证明,改革的最大红利在于打破边界、重塑逻辑、激活人效。从“物理合并”到“化学融合”,这片改革试验田的故事正日新月异。

求真

防晒是遮得越严越好吗

本报记者 李彦臻

炎炎夏日来临,如何做好防晒,成为人们热议的话题。有网友认为,涂得越厚、遮得越严,防晒效果就越好,应将防晒霜、帽子、口罩、墨镜等防晒装备全部用上,全方位遮盖皮肤。这种观念是否正确?

“长时间严密包裹会形成密闭闷热环境,阻碍汗液与油脂排出,破坏皮肤微生态。”中国医学科学院整形外科医院主治医师吴荣薇表示,皮肤需要正常散热代谢,无法长期适应闷热环境。高温天气长时间“全副武装”防晒,面部易形成密闭闷热环境,导致汗液、油脂无法正常排出,淤积堵塞毛孔。这些物质长期堆积附着在皮肤表面,持续刺激面部皮肤,容易破坏皮肤屏障功能,甚至引发红斑、丘疹、瘙痒等皮肤炎症。

河北医科大学第四医院急诊科主治医师程子安提醒,不科学地使用防晒产品会加重皮肤负担。比如,过量厚涂防晒霜,不仅容易造成黏腻不适,其成膜剂、乳化剂等基质成分在湿热、皮脂分泌旺盛的环境下还可能加重毛囊口的堵塞风险,成为诱发或加重痤疮的“帮凶”。“防晒霜涂抹的厚度与防护力并不直接成正比。防晒霜的防护效果取决于是否达到标准用量,面部约需一元硬币大小的量。对于敏感肌肤而

国家林业和草原局日前公布的一组数据显示:“十四五”期间,我国累计完成沙化土地治理 1.52 亿亩,石漠化土地治理 2932 万亩。沙化土地由 20 世纪末的年均扩展 515 万亩转变为目前的年均缩减 1000 万亩。曾经肆虐的流沙,正被牢牢锁住。

我国荒漠化土地面积 2.57 亿公顷,占国土面积的 27%,主要分布在西北、东北和华北,这里分布着全国 84% 的沙化土地和八大沙漠、四大沙地。1978 年,党中央作出建设“三北”防护林体系的重大决策。经过 40 多年接续奋斗,工程区森林覆盖率从 1978 年的 5.05% 提高到 13.84%。

2023 年,“三北”工程攻坚战打响。国家林业和草原局 2025 年 8 月发布的数据显示,两年来,“三北”工程攻坚战累计实施项目 415 个,完成建设任务 1.64 亿亩。据悉,东部歼灭战区,辽蒙在科尔沁沙地南缘联合打造“千里锁边”林草带,平均宽度由 11 公里拓宽到 31 公里,科尔沁沙地正重现往日稀树草原风光;中部攻坚战区,黄河“几字弯”4 省 5 市在毛乌素沙地同步构筑 4 条防风阻沙带,内蒙古在乌兰布和沙漠与黄河交汇处的刘拐沙头建设 3 道防线,每年输入黄河的泥沙量已减少至 150 万吨左右;西部阻击战区,塔克拉玛干沙漠边缘在补齐最后 285 公里缺口后,形成一条全长 3046 公里的绿色防护带。

在沙区生态改善的同时,沙产业也在蓬勃发展。国家林业和草原局荒漠司司长黄采艺介绍,通过因地制宜发展优质牧草、经济林果、中药材、沙漠旅游等沙产业,沙区年产干鲜果品 4800 万吨,约占全国总产量的四分之一,年总产值达 1200 亿元,重点地区林果收入占农民纯收入的 50% 以上。

2025 年,中国“三北”工程荣获联合国粮农组织“全球技术成就林业奖”。我国防沙治沙取得了重大阶段性成果,但还远未到松劲歇脚的时候。

中国林业科学研究院荒漠化研究所所长吴波表示,当前,我国防沙治沙依然面临多重挑战。沙化土地存量依然庞大。我国现有可治理沙化土地面积 7.09 亿亩,其中尚未治理的 3.33 亿亩,主要分布在“三北”地区,都是难啃的“硬骨头”。

水资源约束日益趋紧。“三北”地区年均降水量 100 毫米以下的沙区占全国沙区面积的 56%,早期不少地方选择杨树作为造林树种,但因未充分考虑水资源承载力,造成部分防护林死亡或衰退,重建轻管的问题仍然存在,治理成果巩固压力较大。区域联防联控仍需深化。省际联防联控项目距实现预期目标还有差距。气候变化也带来新的不确定性,全球变暖导致蒸发加大、极端天气加剧,新疆等地年平均气温上升速率远高于全国平均水平。

“十五五”时期是纵深推进全国防沙治沙以及打好“三北”工程攻坚战的攻坚期和决胜期。国家林业和草原局三北局局长刘冰表示,按照“十五五”规划纲要,到 2030 年,“三北”工程区林草覆盖率达到 40.9%,沙化土地综合植被盖度达到 22%,全国完成沙化土地治理任务近 1 亿亩。下一步,将从以下几方面发力:

以水定绿,科学治沙。坚持宜林则林、宜草则草、宜荒则荒。大力发展节水林草,推广喷灌、渗灌等节水抗旱技术。2024 年,水利部向石羊河补水 1.03 亿立方米,向乌梁素海补水 3.77 亿立方米。

联防联控,协同攻坚。以自然地理为单元,统筹沙尘源和路径区、上风口和下风口,推动跨区域协同作战。划定联防联控重点区域,突出抓好黄河岸线主要“沙头”系统治理。

科技赋能,创新驱动。草方格铺设机械、治沙机器人等新装备投入使用,治沙效率提升 3 倍以上。“光伏+治沙”“以路治沙”等治理模式日渐成熟,正全面推广。

产业富民,绿富同兴。将防沙治沙与改善民生紧密结合,推动红枣、核桃、肉苁蓉、沙棘等特色沙产业蓬勃发展。2025 年,“三北”工程区林草产业总产值达 8000 亿元。

本版编辑 李苑 康琼艳 美编 夏祎 来稿邮箱 jirgbgz@163.com

言,由于部分化学防晒剂具有潜在刺激性,超过标准用量可能引发接触性皮炎。”程子安说。

过于追求全身性防晒,除了增加皮肤负担,还将产生其他不良影响。吴荣薇认为,防晒过度或将减少皮肤合成维生素 D 所需的中波紫外线(UVB)接触。若常年进行严格防晒,建议多关注自身维生素 D 水平,可通过增加摄入海鱼、蛋黄、强化奶制品或遵医嘱补充维生素 D 制剂来弥补,这对骨骼健康至关重要。

程子安建议,防晒应遵循按需防护、适度平衡原则。一是物理遮挡按需搭配,如在雪山、海滩、高原、夏季正午等强光场景下,可短时使用衣帽、遮阳伞、墨镜组合;在日常通勤、室内等场景下,则无需全套包裹。二是根据场景选择对应指数的防晒霜,并按标准剂量使用,在使用方式上建议出门前 15 分钟涂抹,每 2 小时至 3 小时补涂,不必盲目追求超高倍防晒值与厚涂。



更多

扫码