证券代码：300369　　证券简称：绿盟科技　　公告编号：2026-006

绿盟科技集团股份有限公司 2025 年年度报告摘要

一、重要提示

本年度报告摘要来自年度报告全文，为全面了解本公司的经营成果、财务状况及未来发展规划，投资者应当到证监会指定媒体仔细阅读年度报告全文。

所有董事均已出席了审议本报告的董事会会议。

信永中和会计师事务所（特殊普通合伙）对本年度公司财务报告的审计意见为：标准的无保留意见。

非标准审计意见提示

□适用 ☑不适用

公司上市时未盈利且目前未实现盈利

□适用 ☑不适用

董事会审议的报告期利润分配预案或公积金转增股本预案

□适用 ☑不适用

公司计划不派发现金红利，不送红股，不以公积金转增股本。

董事会决议通过的本报告期优先股利润分配预案

□适用 ☑不适用

二、公司基本情况

1、公司简介

股票简称	绿盟科技	股票代码	300369
股票上市交易所	深圳证券交易所		
联系人和联系方式	董事会秘书	证券事务代表	
姓名	葛婧瑜	杜彦英	
办公地址	北京市海淀区北洼路 4 号绿盟科技园	北京市海淀区北洼路 4 号绿盟科技园	
传真	010-68728708	010-68728708	
电话	010-68438880	010-68438880	
电子信箱	ir@nsfocus.com	ir@nsfocus.com	

2、报告期主要业务或产品简介

报告期内，公司以“数”与“智”为核心方向，聚焦 AI 安全、数据安全与实战攻防三大领域，探索智能时代安全能力的新形态。

（1）AI 安全：双轮驱动与三位一体生态

随着人工智能的高速发展，公司紧跟新兴技术，持续强化 AI 安全的投入，形成“AI 赋能安全”与“AI 自身安全”的双轮驱动格局。在 AI 赋能安全层面，风云卫 AI 安全能力平台以多基座大模型为核心，场景化多智能体协同为主，成功构建了“模型生产、场景适配、应用赋智”的“三位一体”AI 安全生态体系，发布了自主运营、自主基线检测、未知攻击检测、钓鱼邮件检测、代码审计、自动化渗透测试以及数据分级分类等多个智能体，已在多行业现网实战中验证其价值，全面提升安全检测、运营、数据安全及蓝军对抗能力，实现全域智能赋能。在实际部署中，风云卫 AI 安全能力平台实现了平均超过 95%的告警降噪率，并能对超过 40%的安全事件完成端到端的自动化处置，将安全团队从海量重复告警中解放出来。

在 AI 自身安全层面，针对大模型应用带来的提示词注入、数据泄露、模型幻觉、内容违规等新型风险，公司在 2025 年全面升级“清风卫”AI 安全系列产品，在国内率先构建覆盖“评估-防护-响应”的 AI 安全防御体系。产品遵循 TC260-003 标准，可防护 OWASP 大模型安全风险 TOP10 主流攻击场景。产品已获公安三所“大模型安全防护围栏”认证及中国人工智能产业联盟“人工智能先锋案例”、CCIA“创新产品奖”等行业认可。在国家级测评中，“清风卫”于政务大模型安全测试中初步通过测试并取得优异成绩，全面满足 TC260-004 规范要求，并在第九届“强网杯”中获专项赛一等奖，实战效能获高度认可。同时，面向市场需求配套提供智能体红队评估与大模型安全评估备案两项专业服务，结合产品对智能体资产管理、智能体权限管理、多智能体协同行为监控等能力，形成了智能体和大模型安全评估到防护的整体 AI 安全解决方案。根据国际知名分析机构 IDC 发布的《中国大模型安全保护市场概览》报告，公司相关解决方案覆盖了模型构建安全、数据与隐私保护、应用与接口安全、内容与输出安全等全生命周期的七个关键环节，并在报告划分的全部七个细分能力领域均获得入选。

在 AI 安全研究层面，公司构建了基于可信区间与不确定性评估的安全运营智能研判机制，该机制通过告警事件置信等级分层、邻域一致性分析与历史偏离度建模实现分级处置与自动化闭环，提升了 AI 研判结论的准确性与可解释性，保证了 AI 自主决策的可控性与可审计性。在加密流量检测方面，公司重点突破了多种复杂加密隧道的隐匿识别技术，通过多维流量指纹建模与行为时序分析，实现对隧道化传输与协议滥用场景的精准识别，增强了对横向渗透与数据外泄风险的检测能力。在流量异常与未知威胁发现方面，形成小模型实时感知与大模型语义分析的协同架构，既保证了高性能筛查能力，又增强了对新型攻击与变种威胁的理解与推理能力，提升了整体安全体系的自适应与持续进化水平。基于上述研究成果，公司逐步构建起以可信 AI 为核心、覆盖检测、分析、决策与反馈全流程的智能安全技术体系，为行业提供更加成熟、可落地的人工智能安全解决方案。

（2）数据安全：完善数据要素安全体系

数据安全领域，公司持续推进数据安全业务，以“识别—保护—流通—治理”为主线完善数据要素安全体系，紧抓“数据要素 X”战略机遇，持续深化“数据要素安全流通”的战略布局，以数据保险箱为数据内生安全底座，以可信连接器为数据要素流通的核心抓手，构建了覆盖数据全生命周期的安全基础设施。报告期内，公司积极加入全国数据标准化委员会工作组，深入参与了《可信数据空间技术能力要求》等行业标准的编制工作。公司在底层安全能力与信创适配实现了关键性技术突破，完成了安全能力与可信硬件的分级方案设计与落地，实现了从通用 x86 到国产化信创硬件的全栈适配。发布可信数据空间平台、可信连接器两款新产品，并参与国家数据局可信数据空间试点项目的建设工作。此外，公司积极探索“AI+数据安全”的深度赋能，利用大模型技术提升数据分类分级效率。

在解决方案层面，公司始终秉持“有效保护、合法利用、持续安全”的核心指导理念。深度聚焦金融、运营商、能源、政府等关键行业，构建起覆盖“产品级→业务级→生态级→战略级”的四维数据安全解决方案体系，深度融合 AI 人工智能前沿技术，在智能数据分类分级、动态差异化管控、风险监测预警及数据流通安全保障等核心场景实现关键技术突破。在数据安全运营层面，公司依托 AI 驱动数据安全运营平台与自主基线分析能力，通过对多维度行为数据的深度学习，实现了“全域智能感知→自动化分析→快速处置→策略优化”的完整运营闭环，增强了客户在复杂环境中的业务韧性与数据安全自主权。伴随数据要素市场化改革深化，公司可信数据空间解决方案，融合可信执行环境、机密计算、智能识别与动态脱敏等关键技术，为公共数据授权运营与有序流通构建了“可信、可控、可计量”的安全基础设施与治理体系，有效促进了数据要素的安全合规流通与价值释放。

（3）实战攻防：智能化手段提升攻防效能

报告期内，公司持续强化实战化防御能力，依托智能化手段提升攻防效能，完善从风险发现到修复的闭环管理。面对自动化、智能化攻防技术的逐步应用，公司将 AI 与安全服务能力结合，面向客户关注的大模型安全问题，推出大模型备案以及评估服务。公司大模型内容安全能力在 2025 年度国家级攻防演练中获得 AI 内容安全赛道第一，依托相关能力，公司面向合规监管以及模型风险等场景，提供 AI 红队能力以及人工服务，配合客户消除大模型上线过程中的安全风险。

随着安全服务模型向“自动化、持续化”的演进，公司面向安全服务多个场景进行垂域风云卫+智能体的智能化改造，发布攻击面管理、漏洞情报、应急响应、云原生风险核查等多个安全服务领域智能体，实现端到端交付的同时，推动在客户侧数字人+安全专家的交付模式。在 AI 智能化渗透方面，公司正式发布绿盟 AI 智能化渗透系统，通过大模型自主规划，结合专家知识库和红队 MCP 工具集，能够显著降低漏洞挖掘门槛成本，将 0day 漏洞的挖掘时长从数天大幅压缩到小时级，显著提升了漏洞挖掘效率，在实战场景下可以快速实现目标系统的源码反编译操作，累计挖掘高价值 0day 漏洞数百个，为企业提供智能、经济、高效的渗透测试新选择。报告期内，公司凭借 Agent 赋能高效作战，成功晋级腾讯云鼎实验室发起的国内首个 AI 智能渗透挑战赛“黑客松-智能渗透挑战赛”线下赛前十，实现 AI 驱动自动化渗透测试奖项从零到一的突破。在代码审计方面，公司代码审计智能体采用多智能体（Multi-Agent）协同作

战模式，基于大量第三方产品验证漏洞检出率超过 50%，在第六届全国电信和互联网行业网络与信息安全管理员职业技能竞赛中获得团体赛一等奖。

公司安全运营中心落地 AI+SOC 的模式，支撑上百家客户在安全运营、数据安全、自动化渗透测试、应急响应等场景构建安全体系。“鹰眼安全运营中心”依托 SaaS 化服务架构，实现 L1 级人员替代，日均 Token 处理吞吐量超过 10 亿级，威胁检测与响应效率提升超过 60%。基于检测响应与暴露面管理两大核心场景双双达成 80%的 AI 独立接管目标，标志着公司安全运营业务已从“人机协同”正式跨越至“AI 主导、专家监督”的新阶段。在应急响应方面，公司应急响应智能体面向主机应急响应场景可实现自动化调查取证、攻击路径还原与调查报告生成，将单台主机人工调查取证时长从 2－6 小时压缩至 5－10 分钟，实现效率小时级到分钟级的跃升。

（4）传统安全产品与服务：构筑收入底座

在新兴业务快速发展的同时，公司传统安全产品与服务持续迭代。在安全产品方面，公司提供全线的网络安全产品，涵盖安全检查与评估、安全检测与防护、认证与访问控制、安全审计、安全运营及管理等系列基础安全产品。其中，抗拒绝服务攻击系统（ADS）、安全分析、情报、响应和编排（AIRO）、网络入侵防护系统（IDPS）、WEB 应用防火墙（WAF）等多款产品持续获得国际权威咨询机构推崇。

在安全产品及解决方案方面，结合网络空间风险与威胁变化、监管要求、行业和企业客户发展安全需求等多种因素，公司推出了一系列安全产品及解决方案。报告期内，公司持续深耕云安全领域，智安云解决方案覆盖私有云安全平台、云原生安全 CNAPP 平台等关键方向，推出融入 AI 安全智能化应用升级的“私有云安全资源池+数据安全资源池”双池联动防护体系，满足政府、运营商、能源、企业等行业客户需求。

在车联网领域，形成了以“VSOC+SDK”为核心的车联网安全监测与防护系统解决方案，并已在多家知名车企实现规模化应用。围绕行业政策与客户实际需求，公司构建了覆盖车联网全生命周期的产品与服务矩阵，主要包括：车联网安全态势感知平台、车联网安全监测与防护系统、车联网信息安全攻防靶场、车载数据脱敏与防护安全组件、车联网安全咨询与评估服务。

信息技术应用创新安全领域，公司坚持自主创新和安全可控，全面适配了申威、飞腾、兆芯、海光和鲲鹏等 CPU，麒麟、统信和新支点等操作系统。报告期内，在软件方面，公司相关产品已与数据库、中间件厂商等相关厂商完成适配合作；在硬件方面，除了 CPU，内存，硬盘之外，公司对设备中采用的所有组件进行全面梳理，按照 100%国产化的要求进行设计、生产，并提交测评机构进行国产化相关指标的检测。目前，公司主力产品已完成相应的产品改造适配，为更全面地满足客户在信息技术应用创新领域的需求打好了基础。

在工业控制系统安全方面，基于多源异构数据融合的工控系统安全评估解决方案融合系统日志和网络流量数据，利用 AI 模型提升安全评估的全面性与准确性，以应对复杂的工业攻击模式。在物联网安全领域，构建了覆盖“资产识别、风险发现、威胁检测、响应处置”全链条的物联网安全防护体系相关解决方案已在金融、能源、运营商等行业落地。在软件供应链安全领域，在中国信息通信研究院的指导下，

公司完成了软件供应链安全能力中心的全部检验流程，成为该治理范式下的首个完成全部流程的能力中心。该中心采用“本地检测+云端协同”架构，能够为软件产品提供覆盖开发、交付、运行全生命周期的安全检测。在可信计算领域，基于可信计算 3.0 的可信数据空间方案深度融合了可信连接器、机密计算、全流程审计等技术，已成功应用于医疗、政务等场景，支撑了诸如疫情防控数据共享、基因联合分析等高敏感数据的跨域安全流通与价值挖掘。

（5）安全研究前沿成果

公司在安全研究领域坚持探索新技术、新领域，重点投入 AI 安全、数据安全、暴露面管理、车联网等方向。报告期内，公司在 APT 检测/监测、APT 捕获、APT 取证等技术领域取得显著进展，率先发现多个 APT 攻击组织。同时，在供应链安全、云上风险发现、云原生安全、电信网络反欺诈、无人机安全、FPGA 硬件安全、车联网安全等多个前沿领域研究均获突破。在云智融合安全领域，公司围绕“云原生、公有云、5G 及 AI 安全”方向，依托星云实验室深耕攻防体系建设与前沿研究，构建了覆盖底层基础设施至全栈应用的安全防护矩阵。在云攻防实战与维护方面，研制的红队工具实现了对国内外主流公有云及运营商环境的安全评估能力深度覆盖，多款红队工具赋能标杆项目。针对云端部署 AI 供应链产生的安全风险，公司系统性开展 AI 组件风险梳理与指纹识别，成功识别多起真实泄露事件，有效转化了云上 AI 组件的安全研究能力。在云安全技术创新与人才培养方面，云靶场运营实现了“开源生态”与“商业赢利”，商业版云原生靶场率先实现 ATT＆CK 矩阵全覆盖，填补了国内多行业云原生靶场商业落地的空白。同时，公司构建了覆盖 5G 核心网全平面的“理论+实战”闭环培养体系，通过体系化课程有效提升了通信、能源等关基行业客户的 5G 网络安全韧性。

报告期内，公司继续保持新技术、新领域的探索和投入，依托八大实验室和四大战队持续开展场景化、体系化、实战化的安全研究，陆续发布《网络安全 2025：冲刺“十四五”》《2025 网络安全趋势报告》《低空经济启航，安全体系护航》《高级威胁研究报告（2025 版）》《APT 组织研究年鉴》《Botnet 趋势报告（2025 版）》《DDoS 攻击威胁报告（2025 版）》《车联网安全研究报告》《全球云上数据泄露风险分析简报》《绿盟数据安全 3.0 专刊》等研究报告。

3、主要会计数据和财务指标

（1） 近三年主要会计数据和财务指标

公司是否需追溯调整或重述以前年度会计数据

□是 ☑否

元

	2025 年末	2024 年末	本年末比上年末增减	2023 年末
总资产	4,778,127,141.94	4,613,581,963.76	3.57%	4,155,068,104.07
归属于上市公司股东的	2,612,538,155.47	2,547,210,725.69	2.56%	2,744,574,659.74

净资产				
	2025 年	2024 年	本年比上年增减	2023 年
营业收入	2,541,477,233.97	2,358,012,914.93	7.78%	1,680,784,351.50
归属于上市公司股东的净利润	-45,252,613.48	-364,807,400.91	87.60%	-977,101,919.56
归属于上市公司股东的扣除非经常性损益的净利润	-54,819,746.79	-396,260,179.24	86.17%	-1,005,171,662.97
经营活动产生的现金流量净额	215,576,280.72	135,912,706.16	58.61%	-202,251,738.93
基本每股收益（元/股）	-0.0564	-0.4600	87.74%	-1.23
稀释每股收益（元/股）	-0.0564	-0.4600	87.74%	-1.23
加权平均净资产收益率	-1.76%	-13.72%	11.96%	-30.59%

（2） 分季度主要会计数据

单位：元

	第一季度	第二季度	第三季度	第四季度
营业收入	363,543,374.36	436,986,705.65	479,496,350.93	1,261,450,803.03
归属于上市公司股东的净利润	-101,868,672.07	-69,628,929.50	-24,599,585.64	150,844,573.73
归属于上市公司股东的扣除非经常性损益的净利润	-107,689,706.84	-75,153,731.81	-27,960,045.26	155,983,737.12
经营活动产生的现金流量净额	51,744,309.86	30,192,295.46	-12,261,870.97	145,901,546.37

上述财务指标或其加总数是否与公司已披露季度报告、半年度报告相关财务指标存在重大差异

□是 ☑否

4、股本及股东情况

（1） 普通股股东和表决权恢复的优先股股东数量及前 10 名股东持股情况表

单位：股

报告期末普通股股东总数	39,598	年度报告披露日前一个月末普通股股东总数	47,677	报告期末表决权恢复的优先股股东总数	0	年度报告披露日前一个月末表决权恢复的优先股股东总数	0	持有特别表决权股份的股东总数（如有）	0
前 10 名股东持股情况（不含通过转融通出借股份）									
股东名称		股东性质		持股比例		持股数量		持有有限售	质押、标记或冻结情况

				条件的股份数量	股份状态	数量
沈继业	境内自然人	9.90%	80,250,145.00	0	不适用	0
中电科（成都）股权投资基金管理有限公司－中电科（成都）网络安全股权投资基金合伙企业（有限合伙）	其他	6.91%	55,984,059.00	0	不适用	0
中电产融私募基金管理有限公司－中电电子信息产业投资基金（天津）合伙企业（有限合伙）	其他	6.80%	55,097,548.00	0	不适用	0
南通金玖锐信投资管理有限公司－中汇金玖锐信定增 3 期私募股权投资基金	其他	2.65%	21,452,276.00	0	不适用	0
雷岩投资有限公司	境内非国有法人	1.71%	13,900,298.00	0	不适用	0
中电科投资控股有限公司	国有法人	1.61%	13,048,060.00	0	不适用	0
陈军	境内自然人	1.45%	11,738,700.00	0	不适用	0
北京隆慧投资有限公司－隆慧汇晨战略投资私募证券投资基金	其他	0.96%	7,755,300.00	0	不适用	0
中国农业银行股份有限公司－万家创业板 2 年定期开放混合型证券投资基金	其他	0.93%	7,500,098.00	0	不适用	0
绿盟科技集团股份有限公司－2022 年员工持股计划	其他	0.83%	6,763,500.00	0	不适用	0
上述股东关联关系或一致行动的说明	中电科（成都）股权投资基金管理有限公司－中电科（成都）网络安全股权投资基金合伙企业（有限合伙）与中电科投资控股有限公司为一致行动人。其他股东之间不属于《上市公司收购管理办法》规定的一致行动人，也不存在关联关系。					

持股 5%以上股东、前 10 名股东及前 10 名无限售流通股股东参与转融通业务出借股份情况

□适用 ☑不适用

前 10 名股东及前 10 名无限售流通股股东因转融通出借/归还原因导致较上期发生变化

□适用 ☑不适用

公司是否具有表决权差异安排

□适用 ☑不适用

（2） 公司优先股股东总数及前 10 名优先股股东持股情况表

公司报告期无优先股股东持股情况。

5、在年度报告批准报出日存续的债券情况

□适用 ☑不适用

三、重要事项

详见公司 2025 年年度报告全文“第三节 管理层讨论与分析”和“第五节 重要事项”。

绿盟科技集团股份有限公司

2026 年 4 月 21 日