启明星辰 20260824

AI 驱动安全防御范式变革，数字人与合规产品开启增长新周期

摘要

- AI 驱动安全防御模式从被动转向智能闭环，由 AI 驱动的感知、研判与处置闭环成为应对高频 AI 攻击的必然选择。
- “安心数字人”已在党政、金融等行业落地，通过 7x24 小时运营替代 4 倍人力，预计 2027-2028 年将迎来大规模集中采购爆发期。
- 大模型应用防火墙（MAFW）因合规刚需实现收入快速增长，定价参考算力规模、QPS 或 Token 处理量，典型配置为双机热备模式。
- 2026H1 安全运营与服务收入 6.14 亿元（+28%），营收占比升至近 50%，与中国移动协同及 AI 降本增效是核心驱动力。
- 毛利率受存储类硬件涨价（部分超 3 倍）影响下降 7.6pct，但研发费用因人员优化及 AI 辅助编程应用实现同比下降。
- 与中国移动“九天”大模型深度合作，提供安全语料与测评靶场，未来收入模式将从项目制向业务分成演进。

Q&A

如何看待人工智能时代网络安全行业的发展趋势？

人工智能为网络安全行业带来了机遇与挑战，但整体而言机遇大于挑战。从机遇来看，人工智能赋能网络攻击比赋能安全防护更为直接，降低了实施高强度攻击的技术门槛。过去只有具备高战略价值的机构才会成为专业 APT 组织的目标，而现在普通中小企业也可能遭受同等强度的网络攻击，这使得全社会对网络安全的需求进一步增强。从挑战来看，模型厂商基于大模型的安全能力可直接提供部分安全服务，如代码审计、漏洞挖掘等，这在一定程度上会挤占传统网络安全行业的市场空间。然而，一套完整的网络安全防御体系不仅依赖大模型的智能，也依赖安全产品对智能的利用能力和安全策略的执行能力，二者缺一不可。美国网络安全板块在 Cloud Code Security 刚推出时虽经历短暂的恐慌性下跌，但后续头部安全企业的营收与市值均实现大幅增长，这直观地反映了人工智能带来的机遇大于挑战。 在人工智能时代，网络安全行业的核心逻辑将从被动防御模式转向智能防御和体验增强的新模式。传统安全依赖边界防守、特征规则和人工响应，

足以应对传统攻击。但在人工智能时代，攻击者借助 AI 发起的攻击强度和频度均大幅增强，从漏洞发现到形成可利用攻击载荷的时间窗口也显著缩短，这使得以人为主的响应方式难以应对，必须构建由 AI 驱动的智能感知、研判和处置闭环。此外，传统安全建设重合规而轻用户体验，用户难以清晰感知所部署安全设备的价值与短板。在人工智能时代，通过 AI 驱动的渗透测试，可以持续、主动、常态化地对安全防护体系进行模拟攻击，从而精准评估防护效果和隐性风险，真正实现安全防御体系的可验证、可度量、可迭代，进而增强用户的安全获得感。

关于公司推出的“安心智能体”矩阵及“安心数字人”安全服务，目前用户的需求和接受程度如何？这部分业务的客户预算是否挤占了其它的安全投入？另外，通过数字人进行交付的模式，能否提升公司的客单价或毛利率水平？

目前，“安心数字人”主要以人机协同的模式应用，并非完全自主运行，而是由专业人员进行规范和限制以确保服务成果的确定性。其主要工作集中在告警研判、漏洞核查、合规巡查等重复性、高频次的安全服务与运营任务上，而重大的风险研判和深度的业务处置等复杂工作仍由安全服务专家承担。当前客户覆盖党政机构、运营商和金融等行业，这些行业普遍存在人力缺口较大、对降本增效及 7x24 小时常态化安全运营有强烈需求的特点。数字人的应用有效支持了全天候运营，因为若完全依赖人力，通常需要四倍的人员配置实行轮班制。 尽管应用效果显著，目前数字人服务仍处于从标杆案例向规模化复制发展的阶段，使用者多为对新技术接受度较高的前卫客户。在预算方面，2026 年采购数字人的客户资金基本源于对其他现有安全预算的挤占。由于客户普遍实行年度预算制，他们在 2025 年制定预算时并未为数字人设立专项资金。因此，当前的采购通常是从原有的安全运营服务等人力采购预算中调剂而来，这也部分解决了甲乙双方在服务价格上的分歧。预计从 2027 年开始，部分行业可能会出现针对安全数字人的专项采购预算，尤其是在我们现有的众多驻场安全运维客户中，已观察到此种预算倾向。未来，针对安全数字人的大规模集中采购有望在 2027 至 2028 年间出现。 关于盈利能力，现阶段该服务形态尚处推广落地期，其规模化后的客单价与毛利率水平尚需时间观察。从单价来看，数字人按“人天”计算的单价低于真实服务人员，但其部署数量和使用时长（如 7x24 小时、多点部署）会远超真人，使得总“人天”消耗量大幅增加。因此，单个项目的客单价是上升还是下降，仍有待市场磨合后确定。 总体而言，由技术驱动的安全交付形态结构性变革，对专业的网络安全服务商是利好趋势。AI 技术对行业乙方的冲击主要来自大模型厂商直接提供安全服务，以及甲方利用开源大模型自建安全能力。然而，高质量安全数字人的推出，依赖于专业安全厂商深厚的行业知识（know-how），这是大模型厂商和甲方难以替代的。因此，这种结合了安全与 AI 能力的交付模式，将成为公司的核心竞争力，也是我们持续投入和探索的方向。

半年报披露的大模型应用防火墙产品收入增速较快，请问该产品的具体定价模式是怎样的？在实际部署中，例如一个数据中心通常会配置多少台？此外，在 AI 安全领域，是否观察到客户有其他明确的需求和相应的产品布局？

自 2025 年以来，公司快速推出了大模型应用安全“三件套”，包括服务端的大模型应用防火墙、访问侧的大模型安全访问代理以及用于评估的 MAVAS。其中，MAFW 的收入增长尤为迅速，这主要源于其刚性需求。随着大量机构开始对外提供大模型服务，相关主管机关也提出了合规性要求，使得应用防火墙成为保障服务安全运行的必需品。尽管我们认为 MASB 和 MAVAS 这类产品从长期看同样具有巨大潜力，但目前市场需求最先在 MAFW 上得到确认和释放。 关于 MAFW 的定价，其模式与传统的 Web 应用防火墙非常相似。由于基础功能逐渐趋同，定价主要依据性能指标而非功能差异。关键的参考指标包括客户算力中心的建设规模、业务峰值的 QPS（每秒查询率），或是以每秒处理的 Token 数量来衡量。这些性能参数是决定价格的核心依据。在部署数量方面，由于 MAFW 通常用于保障对外服务，客户为确保业务的高可用性，典型的部署方式是采用双机热备模式，以配合其高可靠的集群环境。因此，双机部署是目前较为常见的配置方案。

MAFW（大模型应用防火墙）作为一种新兴的安全产品，其部署形态和应用场景未来可能呈现怎样的发展趋势？除了 MAFW，AI 安全领域还涌现出哪些新的产品形态和市场需求？

当前，在大型数据中心或智算中心部署 MAFW 以提供大模型服务时，通常采用的是单一逻辑大防火墙的形态，即便存在双机或集群部署，其逻辑上仍是一个整体。然而，市场已出现新的需求趋势，部分客户开始根据大模型访问者和访问内容，在语义层实施分域服务，类似于网络层的分域管理。这种应用层分域模式的出现，源于模型服务的复杂性增加。 为适应这一变化，MAFW 产品需要进行前向拓展，依据语义或应用的分域进行相应配置。这意味着，在语义层和智能应用层的网关正从单一形态向复杂分域环境演变。这一趋势对 MAFW 的提供商而言是积极信号，标志着其应用场景和空间正在扩大，与大模型应用的发展紧密相连，预示着产品生命周期的良好前景。 在 AI 安全的其他方向，除了以 MAFW 为代表的服务侧安全，访问侧和终端侧也涌现出新的产品形态。具体需求点包括：AI 的可观测性、智能体认证与鉴权、智能体行为监管、AI 全链路审计，以及终端侧的智能体安全（有时被称为 AIDR）和智能体行为审计等。尽管这些点状需求已出现，但其市场共识度和规模性尚未达到 MAFW 的水平。从长期看，随着 ToB 机构内部智能体和大模型应用的日益复杂，必然会产生更多刚性的安全需求。因此，公司将持续在这些方向进行技术和解决方案的投入，预计这将成为未来重要的业务增长点。

公司2026年上半年安全运营与服务业务实现了近30%的增长，收入占比接近50%，请问该业务增长主要由哪些领域驱动？未来能否成为公司业绩增长的主要动力？此外，关于安全服务数字人的进展可否提供一些更新？

2026 年上半年，公司安全运营与服务业务实现收入 6.14 亿元，同比增长 28%，占公司总营收的比重从 2025 年同期的 42%提升至近 50%，成为支撑上半年整体收入增长的重要力量。 该业务的增长主要源于以下几个因素： 首先，与中国移动的深化协同带来了移动云安全收入的快速增长。公司将安全能力融入移动云，在公有云、专有云和云资源池等方面的市场拓展成果显著，收入实现明显提升。 其次，关键基础设施行业客户的安全服务需求稳定增长，构成了业务的坚实基本盘。在政府、运营商、金融、电力等重点行业，客户需求正从单一的安全产品采购转向监测、托管运营和应急响应等综合性服务，公司持续拓展这些领域的安全运营业务。 最后，AI 技术的应用提升了产品服务能力和交付效率。通过 Agent SOC（AI SOC）、安心数字员工及专业安全智能体，承担了大量日志分析、报警过滤和威胁研判等人力工作，实现了降本增效，在客户场景中获得认可，并带动了相关产品的收入增长。 展望未来，公司将坚持“产品+平台+运营服务”的发展模式，协同发展安全产品与运营服务，以扩大收入规模，并持续提升业务质量和盈利能力。安全运营与服务业务是公司未来发展的核心动力之一。

公司第二季度毛利率同比下降 7.6 个百分点至 54%，半年报中提及原材料价格上涨。请问该因素对毛利率影响的具体幅度如何？公司是否考虑提价以应对成本压力，以及客户对提价的接受程度如何？

上半年公司面临的原材料价格上涨主要集中在存储类硬件，部分品类的价格较去年同期涨幅达到 3 倍以上。然而，由于这部分原材料成本仅占总成本的一小部分，其价格变动是否会直接传导至产品售价，需要结合当前行业市场竞争状况以及 AI 赋能带来的整体效率提升等因素进行综合评估。 为积极应对原材料价格波动，公司正持续强化供应链的集中统一规范化管理，通过扩大集采谈判优势和加强产供销计划联动来努力控制成本。这一过程也在一定程度上促进了内部全品类和产线范围内的能力优化。总体来看，当前这轮价格上涨对具备规模优势和完整供应链管理体系的公司而言，可能带来相对性的利好。

公司 2026 年上半年研发费用有所下降，这是否得益于 AI 辅助编程或数字员工等技术提升了效率？费用的下降是否会影响公司未来的研发投入力度？

公司内部正在积极推进数字化转型和智能化升级，在研发、销售、管理等多个环节引入大模型、智能体及 AI 辅助编程等工具，整体运营效率确有提升。过去一些投入人力较多、重复性高的工作正逐渐由智能工具承接。 研发费用的下降，主要原因是公司从 2025 年延续至 2026 年上半年对员工规模进行了小幅优化。需要强调的是，此次人员调整并未削弱公司的整体研发实力和技术投入。核心团队保持稳定，各部门核心职能运转及项目推进均处于良性状态，更多是通过工智能来提升企业综合效率。 面对当前行业的发展机遇，公司坚定持续

发的战略。这包括布局具有差异化竞争优势的科技创新和战略性新技术。从下半年来看，研发费用将趋于平稳。由于人员调整主要从 2025 年下半年开始，因此 2026 年上半年同比降幅较为明显，但下半年的同比变动幅度将显著减小。公司将围绕既定战略，聚焦前沿技术和核心业务，采取“有抓有放”的投入策略，在关键技术领域的领先性和前瞻性布局上会投入巨大力度。

请详细介绍公司与中国移动“九天”大模型的具体合作内容，以及在这种合作模式下，公司的收费模式是怎样的，预计将在哪些方面产生收入？

公司与中国移动“九天”大模型的合作属于体系内的“专专合作”，即两个专业子公司在不同方向上的融合。合作主要体现在以下几个方面： 第一，共同承担国家级及部委的研发项目。在这类项目中，“九天”负责模型训练开发，公司则负责安全场景的示范应用建设。具体工作包括为“九天”的基础大模型训练提供安全语料，并为模型服务的外围应用架构提供安全设计、保障及安全装置部署，例如为大模型前端配置 WAF 或进行分语境应用的安全定制开发。 第二，合作开发网络安全领域的基础大模型。此项合作对标国外相关模型，“九天”提供模型底座、训练资源、训练经验和算力，公司则提供安全领域的专业能力，包括长期积累的安全数据作为安全语料、独立的测评数据集（确保测评的公正性，避免训练数据污染），以及负责模型的安全能力评估。 总的来说，公司提供安全相关的全部能力、数据、场景和测评靶场等资源，而“九天”提供基础模型架构、算力及训练支持。 关于收费模式与预期收入，目前双方的合作仍以项目制收费为主，且项目量有较大提升。中国移动已将业务发展方向重新定位为通信网、算力网、智能网“三网三业”，而“九天”大模型是其智能网业务的核心引擎，也是 MaaS 等新业务模式的突破口。公司与“九天”的合作是全方位的，安全能力以内生或外生保护的方式融入大模型及其迭代过程。未来，随着“九天”新业务的推广，将会出现分成收入的模式。但这部分收入体现在公司财务数据中会有一定滞后性，需要等待相关新业务形成规模化后才能成为公司稳定的收入板块。 此外，“九天”不仅为公司带来了业务增长潜力，还提供了强大的算力支持，这为公司在当前发展阶段提供了坚实的底气。