

从微软 GPT 安全去理解数据解析与安全大脑的战略意义

2023 年 03 月 31 日



分析师：吕伟

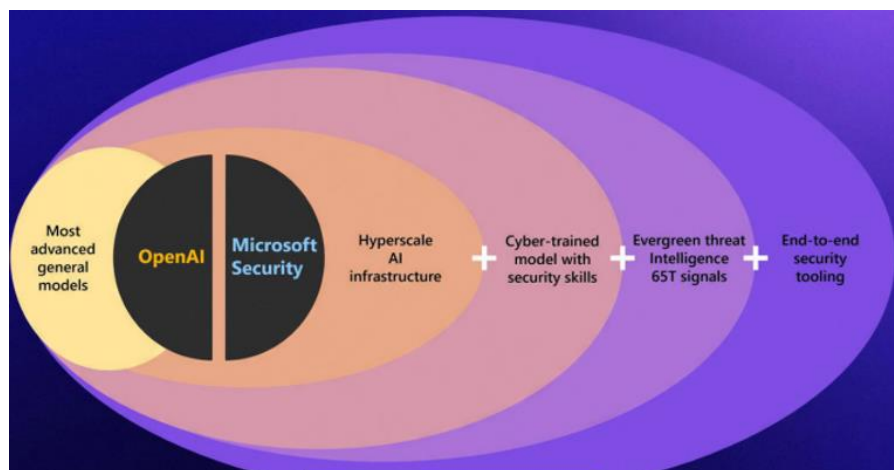
执业证号：S0100521110003

电话：021-80508288

邮箱：lvwei_yj@mszq.com

➤ **3 月 28 日，微软举办基于 GPT 模型的安全发布会。**微软提到，基于 GPT4 大模型以及微软安全团队每日搜集超 65 亿网络威胁情报，微软安全 Copilot 试图通过 AI 逆向追溯工程黑客们的意图、潜在方法等，将安全策略集成在云端一键部署；此外，微软安全 Copilot 支持多模态交互、团队协作和根据意见自动优化等特点。

图1：基于 OPENAI 的安全视图



资料来源：微软，民生证券研究院

➤ **天平之上的抉择，微软 Security Copilot 旨在平衡用户的控制权与隐私安全。**GPT 模型在通过海量数据训练自身理解能力的同时，不可避免的会让人疑惑是否会涉及到个人及企业的专有数据，而此次微软通过 Security Copilot 提出在 AI 模型下的安全三要素：

- 1) 您的数据总是您的数据；
- 2) 您的数据将保留在自身的组织架构内，并不用于训练基础模型；
- 3) 微软通过业界最全面的企业合规和安全控制来保护您的数据和人工智能模型

推荐

维持评级

相关研究

1. 计算机行业动态报告：详解 ChatGPT 插件如何开启 AI 操作系统-2023/03/28
2. 计算机周报 20230325：ChatGPT 已具备颠覆操作系统雏形-2023/03/25
3. 计算机行业点评：华为卓越大模型技术持续创新-2023/03/24
4. 医疗信息化行业事件点评：医疗数据要素重磅政策带来大机遇-2023/03/23
5. 计算机行业事件点评：AI 应用之低代码平台：软件开发的革命-2023/03/19

图2：微软的 security copilot



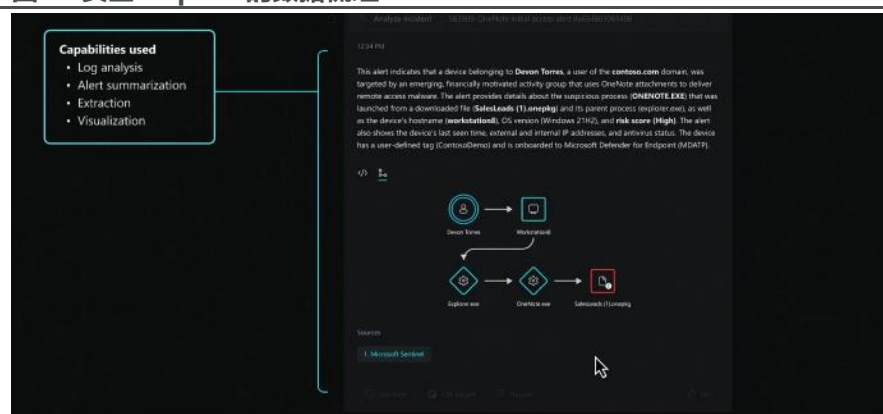
资料来源：微软，民生证券研究院

在三要素的基础上，微软通过每天汇总的 65 万亿信号包括身份安全、遵从性、设备管理和隐私等多维度信息，从而实现超前判断攻击者的意愿。Security copilot 通过赋能安全产品具备 AI 的理解能力，从根本上加速抵御威胁的防御能力，实现按需提醒和提前预测两大功能。作为首个生成式人工智能安全产品的微软安全 Copilot，本身建立在 GPT-4 AI 全功能的基础上，不断地从微软构建的全球威胁情报、安全数据和技能中持续学习，以提供量身定制的见解、强化的防御和更快的反应。

➤ **数据梳理与安全大脑或将成为微软 Security copilot 的“矛与盾”。**微软于本次发布会上重点举例在勒索软件上的攻与防：

- 1) 数据梳理：安全 Copilot 将大量复杂的调查工作在短短几个步骤中迅速整合，乃至形成可视化化的图形。在传统模式下，通常需要花费超过数月的时间，而通过微软安全 copilot 的模式仅需几分钟；

图3：安全 Copilot 的数据梳理



资料来源：微软，民生证券研究院

- 2) 安全大脑：安全 Copilot 的预警系统打破语言、数据获取和培训等障碍。在微软的演示中，微软安全 Copilot 建立在大型语言模型的创新之上，并利用微软的安全专业知识、智能和技术的基础力量进一步演化，实现为特定的安全用例提供量身定制的功能。通过提问或提示符发出相关命令，结合微软的 65 万亿信号实现直接到洞察，乃至端到端微软安全产品组合，形成学习循环的安全大脑模式。

图4：安全 Copilot 的数据梳理



资料来源：微软，民生证券研究院

➤ **投资建议：**信息安全一直是每次技术进步的难点，而此次 GPT 带来的 AI 浪潮中，安全问题更引人深思，从模型的本身-面向的领域-数据的使用-具体的应用等多维度中均带来全新的考验。本次 ChatGPT 故障导致数据泄露敲响了新技术带来新安全问题的警钟，此次微软 Security Copilot 带来基于 GPT 模型的安全模型，我们判断对于网络安全的业态将带来重构的冲击，具体如下：

微软的 65 万亿的信号来源于海量的 Raw Data，针对性对数据进行解析并实现归纳总结乃至溯源的功能是网络可视化能力的缩影，建议关注长久深耕网络可视化前端与后端的相关产业链：**浩瀚深度、中新赛克、美亚柏科、太极股份、迪普科技、恒为科技等；**

通过 AI 大模型深度理解能力实现前瞻判断威胁来源，真正实现主动消灭威胁隐患的安全新业态，建议关注**具备 AI 大模型+安全大脑的核心标的-三六零；**

同时建议关注态势感知以及安全运营的相关公司：**启明星辰、安恒信息、奇安信、深信服等。**

➤ **风险提示：**技术落地不及预期，竞争格局加剧。

分析师承诺

本报告署名分析师具有中国证券业协会授予的证券投资咨询执业资格并登记为注册分析师，基于认真审慎的工作态度、专业严谨的研究方法与分析逻辑得出研究结论，独立、客观地出具本报告，并对本报告的内容和观点负责。本报告清晰准确地反映了研究人员的研究观点，结论不受任何第三方的授意、影响，研究人员不曾因、不因、也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

评级说明

投资建议评级标准		评级	说明
以报告发布日后的 12 个月内公司股价(或行业指数)相对同期基准指数的涨跌幅为基准。其中：A 股以沪深 300 指数为基准；新三板以三板成指或三板做市指数为基准；港股以恒生指数为基准；美股以纳斯达克综合指数或标普 500 指数为基准。	公司评级	推荐	相对基准指数涨幅 15%以上
		谨慎推荐	相对基准指数涨幅 5% ~ 15%之间
		中性	相对基准指数涨幅-5% ~ 5%之间
		回避	相对基准指数跌幅 5%以上
	行业评级	推荐	相对基准指数涨幅 5%以上
		中性	相对基准指数涨幅-5% ~ 5%之间
		回避	相对基准指数跌幅 5%以上

免责声明

民生证券股份有限公司（以下简称“本公司”）具有中国证监会许可的证券投资咨询业务资格。

本报告仅供本公司境内客户使用。本公司不会因接收人收到本报告而视其为客户。本报告仅为参考之用，并不构成对客户的投资建议，不应被视为买卖任何证券、金融工具的要约或要约邀请。本报告所包含的观点及建议并未考虑个别客户的特殊状况、目标或需要，客户应当充分考虑自身特定状况，不应单纯依靠本报告所载的内容而取代个人的独立判断。在任何情况下，本公司不对任何人因使用本报告中的任何内容而导致的任何可能的损失负任何责任。

本报告是基于已公开信息撰写，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、意见及预测仅反映本公司于发布本报告当日的判断，且预测方法及结果存在一定程度局限性。在不同时期，本公司可发出与本报告所刊载的意见、预测不一致的报告，但本公司没有义务和责任及时更新本报告所涉及的内容并通知客户。

在法律允许的情况下，本公司及其附属机构可能持有报告中提及的公司所发行证券的头寸并进行交易，也可能为这些公司提供或正在争取提供投资银行、财务顾问、咨询服务等相关服务，本公司的员工可能担任本报告所提及的公司的董事。客户应充分考虑可能存在的利益冲突，勿将本报告作为投资决策的唯一参考依据。

若本公司以外的金融机构发送本报告，则由该金融机构独自为此发送行为负责。该机构的客户应联系该机构以交易本报告提及的证券或要求获悉更详细的信息。本报告不构成本公司向发送本报告金融机构之客户提供的投资建议。本公司不会因任何机构或个人从其他机构获得本报告而将其视为本公司客户。

本报告的版权仅归本公司所有，未经书面许可，任何机构或个人不得以任何形式、任何目的进行翻版、转载、发表、篡改或引用。所有在本报告中使用的商标、服务标识及标记，除非另有说明，均为本公司的商标、服务标识及标记。本公司版权所有并保留一切权利。

民生证券研究院：

上海：上海市浦东新区浦明路 8 号财富金融广场 1 幢 5F； 200120

北京：北京市东城区建国门内大街 28 号民生金融中心 A 座 18 层； 100005

深圳：广东省深圳市福田区益田路 6001 号太平金融大厦 32 层 05 单元； 518026