NOMURA

Global Markets Research
18 September 2026

Global AI Trend Tracker – LLM in vertical industry

EQUITY: TECHNOLOGY

Is cybersecurity the next big thing for LLM adoption?

Quick Note

Research Analysts

China Technology

Bing Duan - NIHK
bing.duan1@nomura.com
+852 2252 2141

Joel Ying, CFA - NIHK
joel.ying@nomura.com
+852 2252 2153

Following our publication of the China AI value chain anchor report on 11 September (*China AI value chain - Eyeing a longer and durable AI adoption cycle*), a key question arose about the next "killer apps" for large language models (LLMs), and we also noted strong interest on cybersecurity software. Over the past weekend, we have noticed heated discussions on whether frontier model companies should slow down LLM development, and one key focus is the security weakness of LLM and Gen AI platforms. We think this may lead to more awareness about cybersecurity and information security in the AI cloud ecosystem. While certain cybersecurity players could see fundamental improvements due to the rising security demand on infra/network/application layers, we still caution that: 1) demand from a major customer segment, i.e., the government and enterprise market remains lackluster in China, while the competitive landscape in China's security software market remains suboptimal; and 2) LLM companies are tapping into the cybersecurity market through their coding agents and co-work agent tools, partially cannibalizing the traditional security software companies' security market. We think certain software security leaders, i.e., Sangfor (300454 CH, Neutral) with improved fundamentals may offer near-term trading opportunities; however, the China security software sector is yet to stage a full-swing recovery, and hence, we maintain our neutral view on the sector.

LLM players tapping into cybersecurity: Is it the next big thing for LLM monetization?

As the LLMs' intelligence grow meaningfully, they also bring greater risks to cybersecurity for both individuals and enterprises. Since the beginning of 2026, overseas LLM players such as Anthropic (unlisted), OpenAI (unlisted), and Meta (META US, Not rated) have reported several cybersecurity incidents where LLMs actively launched attacks. Therefore, LLM players have begun taking a series of measures to control cybersecurity incidents generated by LLMs, while leveraging LLM capabilities to strengthen the cybersecurity defenses of foundational software. On 7 April 2026, Anthropic announced that its latest model, Mythos Preview, demonstrated highly automated vulnerability detection and exploitation capabilities in internal testing.

We believe the potential benefits to adopt LLM in cybersecurity include: 1) improved efficiency: complex event analysis that previously took hours can be reduced to minutes with the help of AI agents, and AI can help automatically summarize events and generate structured reports; 2) improved accuracy: LLMs can significantly reduce false positive rates for alerts through semantic understanding, and they can also improve detection and prediction accuracy; and 3) quantifiable results: intelligent cybersecurity systems can quantify security effectiveness. For example, Anthropic's Project Glasswing helped partners discover over 10,000 high-risk vulnerabilities in the first month. Moreover, we think using LLM for security applications is a natural extension of coding capabilities of LLM: the code understanding, tooling, and multi-stage reasoning capabilities can be directly transferred to vulnerability discovery and verification capabilities. We think the continuous improvement of LLMs' complex programming capabilities may lead to a quantum leap in cybersecurity capabilities, which could be widely adopted in the enterprise market.

Production Complete: 2026-09-18 10:37 UTC

See Appendix A-1 for analyst certification, important disclosures and the status of non-US analysts.

Fig. 1: LLM players' actions on cybersecurity

Company name	Date	Project name	Details
Anthropic	2026.4.8	Claude Mythos Preview	Anthropic launched the Claude Mythos Preview LLM, demonstrating highly automated network bug discovery and exploitation capabilities.
		Project Glasswing	Anthropic primarily uses Claude Mythos Preview for a defensive cybersecurity project (Project Glasswing), with initial participants including AWS, Apple, Google, JPMorgan Chase, Microsoft, Nvidia, Palo Alto Networks, and the Linux Foundation, along with more than 40 organizations.
	2026.5.1	Claude Security	Anthropic is open to all Claude Enterprise users with the open beta of Claude Security. Claude Security reasons code like a human researcher, understanding component interactions and data flows to gain insights into complex bugs.
OpenAI	2026.3.6	Codex Security	Codex Security can identify cybersecurity vulnerabilities and propose solutions to fix them.
	2026.5.12	Project Daybreak	Project Daybreak is built on the GPT-5.5-Cyber model and Codex Security agent, integrating a security partner ecosystem including Cisco, CrowdStrike, Palo Alto Networks, Cloudflare, Oracle, and others, aiming to enhance enterprise software security defenses.
	2026.8.10	GPT-5.6-Cyber	OpenAI launched GPT-5.6-Cyber, open to Daybreak Red users. This model is built on GPT-5.6 Sol and is specifically designed to enhance capabilities and reduce rejection responses in certain specific cybersecurity tasks.
	2026.9.3	GPT-6 Security	OpenAI claims GPT-6's cybersecurity capabilities have reached the highest level of the OpenAI Preparedness Framework—Critical—for the first time.
Z.AI	2026.9	GLM-5.3 Cyber Co-work	Z.AI officially announced that cybersecurity became the first implementation scenario for GLM5.3, and 100 enterprises have already completed integration. GLM-5.3 mainly undertakes high-value tasks such as multi-agent vulnerability mining, real-world business security research, large-scale codebase audits, and security hardening for financial institutions; while GLM-5.3-Flash covers high-frequency tasks such as batch scanning, log processing, and alert analysis.

Source: Company data, Nomura research

Security software companies: new growth driver or cannibalization?

The cybersecurity industry can be divided into several segments: network and infrastructure defense, zero trust and secure workspace access, cloud security, a pplication and API security, identity and access management, data security, d etection/response and security operation, vulnerability and threat, assessment and compliance. For the AI industry chain (AI infra, AI network, LLM, AI application), we think security plays an important role in each layer.

LLMs and AI applications offer significant demand for cybersecurity, and some of them are unique to the Gen AI market. For instance, LLM requires jailbreak protection, hallucination governance, and content compliance review, making it a new security category unique to the Gen AI era. Moreover, AI agents were given excessive authorization or access rights to operate users' system and data, which make identity protection and permission governance (IAM for Agent) critical functions. Garner projects AI security market to reach USD4.8bn in 2027E, a 68.7% increase y-y, and further grow to USD7.7bn in 2028E. AI application security will remain the largest spending category in 2027E, and forecasted to reach USD851mn, followed by AI usage control at USD749mn, according to Gartner. IDC predicts that the market size for security agent-related applications in China will reach USD1.6bn by 2028E. Although AI security is still a small market at present, we believe there are strong growth potential in areas such as AI-driven event response and threat detection, AI cloud protection, AI governance, etc.

We note that many security software companies in China have launched AI security products. Meanwhile, LLM players are also entering the security sector, and may



potentially gain market shares from traditional security players, in our view. Moreover, AI application security products, such as LLM firewalls, are also being embedded by AI Cloud platforms into their MaaS solutions as an integral part. Users can purchase LLM services and related security products together on cloud platforms, thus bypassing third-party security software vendors. Meanwhile, traditional security software players own rich security data assets and industry knowhow, which help them deliver better customized solutions, in our view, and we think the security market is yet to consolidate in the near term.

Fig. 2: Cybersecurity industry chain and key players



Source: Nomura research

Fig. 3: AI security TAM by segment (USD mn), 2026-27E

Segment	2026 spending	2026 growth (%)	2027 spending	2027 growth (%)
AI Application Security	508	82.1%	851	67.5%
AI Usage Control	433	86.6%	749	73.0%
AI Governance Platforms	275	77.4%	462	68.0%
AI Gateway	251	80.6%	429	70.9%
Other Securing AI	1,368	83.9%	2,292	67.5%
Total	**2,835**	**83.0%**	**4,783**	**68.7%**

Source: Gartner, Nomura research

Fig. 4: AI security products from key Chinese players

Company name	Product	First launch date	Commercialization progress
Qi An Xin	QAX-GPT LLM	2023.8	Bundled sales with other products
Sangfor	Security GPT LLM	2023.5	Upgraded to 4.0 version and integrated with DeepSeek-R1
	AI computing gateway	2025.2	It has already been delivered in industries such as healthcare, manufacturing, and ISV
360	360zhinao LLM	2023.7	AI-related projects won over CNY300 million in October 2025
	360 Security LLM All-in-One Machine	2025.4	Sale price is CNY0.6mn+
DBAPP Security	Security LLM	2023.8	AI revenue exceed CNY58mn, up 230% y-y in 2025
	Security Agent Platform	2024	
Venustech	Panxiaogu Security LLM	2022	LLM application firewalls have already been implemented in specific projects in government, telecom operators, finance, energy, and other industries
	LLM application security proudct matrix	2025.2	
	Tianyue and Anxing Security Agent System	2025-2026	

Source: Company data, Nomura research