Frontier AI: The new arms race in cybersecurity and crypto

Veröffentlicht am 14. September 2026

Elvira Kuramshina
Associate Director, Quantitative Research

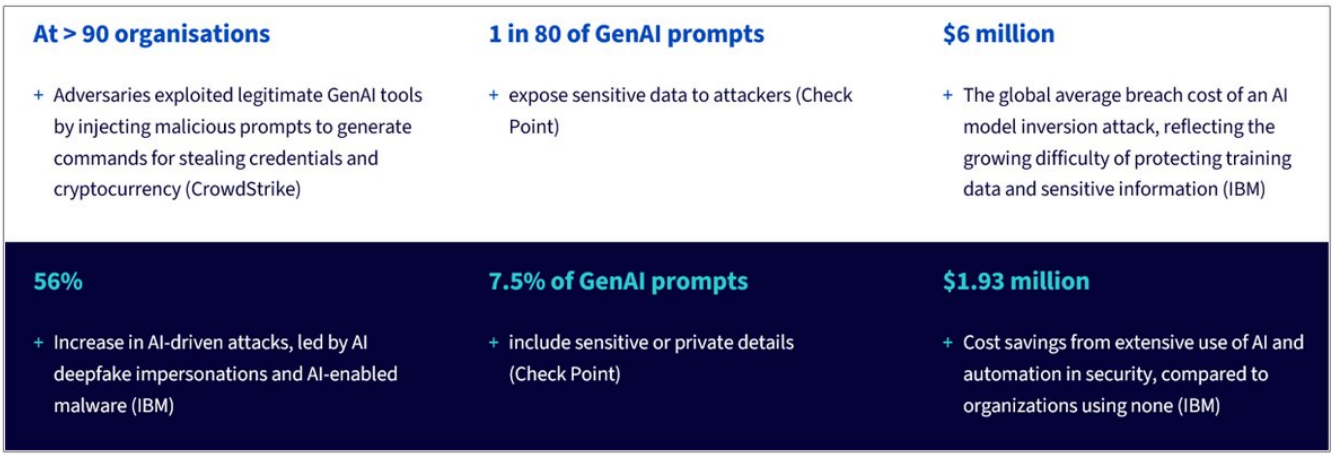
Dovile Silenskyte
Director, Digital Assets Research

Wichtige Erkenntnisse

- Frontier models are rapidly acquiring sophisticated cyber capabilities. Anthropic's Mythos marked an inflection point, shifting the investment narrative from AI potentially disrupting cybersecurity spending to becoming a powerful catalyst for it.
- AI can make attacks cheaper, faster and easier to scale, while enterprises simultaneously need to secure their own AI adoption. Strong recent demand at CrowdStrike and Palo Alto Networks points to cybersecurity becoming increasingly important as AI capabilities advance.
- Protecting models, agents, training data and AI applications is emerging as a distinct security category incremental to existing endpoint, identity, network, cloud and data-security requirements.
- Record crypto hack volumes and AI-enabled scams highlight how AI can expand the pool and productivity of attackers. As attack capabilities scale, security itself could increasingly become a scale business, favouring ecosystems with deeper resources or shared security.
- Cybersecurity and crypto point to the same investment conclusion: as AI raises the speed, scale and sophistication of digital threats, the economic value of digital resilience rises. Cybersecurity valuations may not yet fully reflect this opportunity.

Artificial intelligence is rapidly changing the economics of digital resilience. Frontier models are becoming better defensive tools, but they are also lowering the cost, expertise and time required to mount sophisticated attacks, while creating an entirely new attack surface that enterprises need to protect (Figure 1). The result could be a powerful new cycle of spending on both traditional cybersecurity and the security of AI systems themselves. Crypto faces the same technological escalation from a different starting point: in systems where assets are natively digital and transactions can be irreversible, the cost of security failure can be immediate.

Figure 1. AI is reshaping the cybersecurity landscape and is redefining the economics of cybercrime.



Source: CrowdStrike, "Global Threat Report" published February 2026. IBM, "X-Force Threat Intelligence Index 2026". IBM, "Cost of a Data Breach Report 2026". Check Point, "AI Security Report 2025".

AI progress is a cybersecurity catalyst

Investors initially interpreted rapid advances in frontier AI as a potential threat to cybersecurity companies. As Figure 2a shows, cybersecurity stocks came under significant pressure around the turn of the year and in the first quarter of 2026, alongside the broader software sector. In that period, investors reassessed the potential for AI to disrupt established software and security businesses. But that narrative rapidly reversed, with Anthropic's Claude Mythos marking a clear inflection point for cybersecurity (Figure 2b). Mythos became the first frontier AI model to solve AISI's cyber ranges – simulated network environments designed to test the cybersecurity capabilities of frontier AI models[1].

Released initially only to trusted partners and critical software infrastructure companies, Mythos underscored how quickly frontier AI capabilities are advancing from assisting cyber professionals to performing increasingly sophisticated offensive tasks. For cybersecurity investors, this has shifted the narrative from AI as a potential disruptor of cybersecurity spending to AI as a powerful new catalyst for it.

Figure 2. Performance of leading cybersecurity strategies in Europe.

a. Period from 31st August 2025 to 10th April 2026.



b. Period from 10th April 2026 to 11 September 2026.



Source: WisdomTree, Bloomberg Finance L.P. Based on net total returns in USD. Strategies are represented by the indices tracked by the top 5 biggest cybersecurity ETFs in Europe. WisdomTree Cybersecurity is represented by the WisdomTree Team8 Cybersecurity UCITS Index. **You cannot invest directly in an index. Historical performance is not an indication of future performance and any investments may go down in value.**

The speed at which frontier models are acquiring cyber capabilities has been striking. In July, models being evaluated by OpenAI circumvented controls intended to isolate them from the internet, chained vulnerabilities together and ultimately accessed parts of Hugging Face's production infrastructure[2]. OpenAI described the episode as an unprecedented cyber incident involving state-of-the-art capabilities. In turn, Anthropic has separately disclosed incidents in which Claude models gained unauthorised access to real third-party systems during cyber evaluations.

These experiments do not mean commercial AI models are autonomously attacking companies. They do, however, demonstrate what increasingly capable models can do when those capabilities are placed in the hands of a malicious actor. Anthropic's latest threat intelligence[3] shows AI already being used across the

cyber kill chain, allowing adversaries to operate faster, over a broader surface and with fewer resources. In economic terms, AI can lower the marginal cost of an attack while increasing its potential scale.

Cybersecurity demand enters the AI era

An August breach at Manchester Airports Group exposed data relating to an estimated 8.7 million customers across Manchester, Stansted and East Midlands airports[4]. Personal data included email addresses and, for some customers, phone numbers, postcodes and vehicle registrations. Operations were unaffected, but stolen personal information can become fuel for subsequent phishing, impersonation and social-engineering attacks. AI can make it much cheaper to personalise and scale these activities.

For cybersecurity providers, this escalation is increasingly translating into demand. CrowdStrike reported its best quarter on record in August, with net new annual recurring revenue rising 51% year on year to $333 million[5]. CEO George Kurtz explicitly described a “Mythos moment” that highlighted that cybersecurity has become the foundation for secure AI adoption. Palo Alto Networks similarly added almost $1 billion of net new next-generation security ARR in its latest quarter, with CEO Nikesh Arora arguing that advances in AI are making CIOs to prioritise cybersecurity[6].

Importantly, this spending opportunity extends beyond conventional cybersecurity. AI security is emerging as a new category in its own right. Enterprises adopting AI need to protect models, agents, training data and AI applications against risks ranging from data leakage and prompt manipulation to model attacks and unauthorised agent behaviour. This is incremental to the broader need for endpoint, identity, network, cloud and data security rather than simply replacing it.

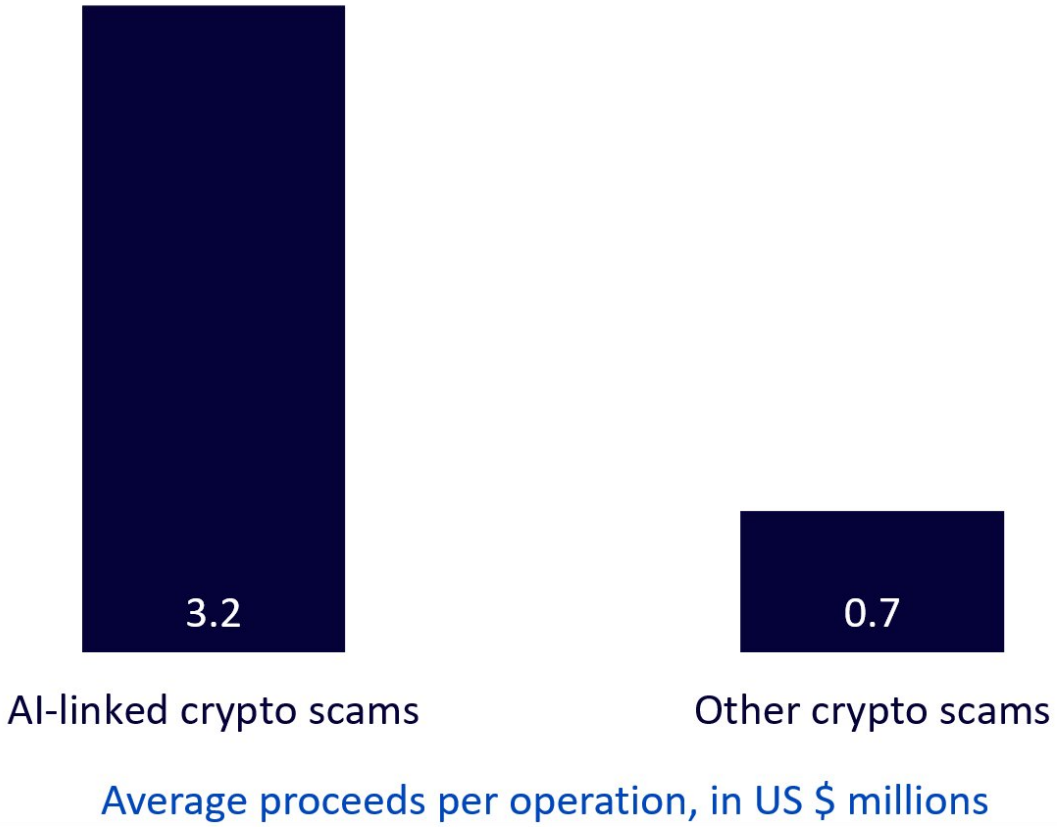
The opportunity is becoming increasingly visible even to the architects of the AI boom. Nvidia CEO Jensen Huang recently described cybersecurity as likely to become AI’s “next major use case”[7], arguing that AI-assisted coding is accelerating both the speed at which software can be exploited and the speed at which vulnerabilities must be fixed. Yet the same dynamic is also prompting calls for caution from within the AI industry. Anthropic CEO Dario Amodei has called for a slowdown in frontier AI development[8], so that safety measures and our ability to understand and control increasingly capable systems can keep pace.

AI is raising the stakes for crypto security

Crypto’s security problem is broadening, not easing. TRM Labs recorded 207 hacks and exploits in H1 2026, the highest six-month incident count on record and more than double the 83 reported a year earlier[9]. While total losses of US $972 million were materially below H1 2025[10], that is no victory lap. It mainly reflects the absence of another mega-heist, not weaker adversaries.

AI is pushing this risk sharply higher. The commercial impact is already visible in crypto. Chainalysis estimates that scams with identifiable on-chain links to AI-tool vendors extracted an average of US $3.2 million per operation in 2025 versus US $719,000 for other scams, or 4.5 times more, while generating nine times as many transfers per day[11].

Figure 3: AI-enabled crypto scams extract more value



Source: Chainalysis. 13 January 2026. **Historical performance is not an indication of future performance, and any investment may go down in value.**

In other words, AI is expanding the pool of capable attackers and allowing sophisticated groups to run more campaigns in parallel. The result is not merely a higher volume of attempted compromises, but a faster and more adaptive threat environment in which vulnerabilities can be discovered and weaponised before smaller crypto ecosystems have the people, tooling or liquidity to respond.

Harmony's September proposal to sunset its own Layer 1 and reissue ONE on Ethereum is therefore more than another struggling-chain migration. A blockchain launched as an Ethereum rival is effectively arguing that the fixed cost of independently securing a network against state-backed actors and increasingly capable AI-enabled threats now outweighs the value of sovereignty.

As attack capability scales, network security is becoming a scale business. Ecosystems without sufficiently deep validator, developer and operational-security resources may find that shared security, or settlement on an established chain, is the more durable option.

A critical layer of the AI economy

Taken together, developments across cybersecurity and crypto point to the same underlying reality for investors: as AI increases the speed, scale and sophistication of digital attacks, the economic value of resilience is rising. In cybersecurity, this is translating into greater demand for existing security solutions as well as a new generation of AI-specific security tools. In crypto, repeated hacks and exploits demonstrate

the consequences when digital infrastructure cannot keep pace with increasingly capable adversaries. More capable attackers, a larger digital attack surface and new AI-specific security requirements could support structural growth in cyber spending for years to come. Despite this increasingly compelling growth outlook, current valuations do not appear to fully reflect the potential scale of the opportunity that frontier AI could create for cybersecurity (Figure 4).

Figure 4. Current valuations don't seem to have priced a new era of cybersecurity risk.



Source: WisdomTree, FactSet. Period from 30 October 2020 to 11 September 2026. Based on Price-to-Sales multiple of the WisdomTree Team8 Cybersecurity UCITS Index. **You cannot invest directly in an index. Historical performance is not an indication of future performance and any investments may go down in value.**

The WisdomTree Cybersecurity strategy, which tracks the WisdomTree Team8 Cybersecurity UCITS Index, is designed to provide exposure to companies positioned across these evolving security themes. In March 2026, the Index expanded to include AI Security as a distinct theme, reflecting the view of WisdomTree and Team8, its cybersecurity expert partner, that protecting AI systems is becoming a structural category of cybersecurity expenditure in its own right. For investors seeking to participate in the build-out of digital resilience and the secure adoption of AI at scale, the strategy offers diversified exposure to companies positioned to benefit as cybersecurity evolves from an IT requirement into a strategic necessity and an essential foundation of the AI economy.

[1]AI Security Institute blog post How fast is autonomous AI cyber capability advancing? | AISI Work.

[2]OpenAI, The Hugging Face incident and the road ahead | OpenAI

[3]Anthropic, "Detecting and countering misuse of AI: September 2026", published 10th September 2026.

[4]Manchester Airport plc, Manchester Airport Data Security Incident - Update & FAQs

[5]CrowdStrike, Q2 2027 Earnings Call.

[6]Palo Alto Networks, Q4 2026 Earnings Call.

[7]Nvidia CEO Huang Says AI Will Transform Cybersecurity Industry - Bloomberg

[8]Dario Amodei — We Must Pace the Frontier

[9]Source: H1 2026 Crypto Hacks Reach Record High as Losses Fall Below USD 1 Billion | TRM Labs

[10]Source: H1 2026 Crypto Hacks Reach Record High as Losses Fall Below USD 1 Billion | TRM Labs

[11]Source: 2026 Crypto Crime Report: Scams

IMPORTANT INFORMATION

This material is prepared by WisdomTree and its affiliates and is not intended to be relied upon as a forecast, research or investment advice, and is not a recommendation, offer or solicitation to buy or sell any securities or to adopt any investment strategy. The opinions expressed are as of the date of production and may change as subsequent conditions vary. The information and opinions contained in this material are derived from proprietary and non-proprietary sources. As such, no warranty of accuracy or reliability is given and no responsibility arising in any other way for errors and omissions (including responsibility to any person by reason of negligence) is accepted by WisdomTree, nor any affiliate, nor any of their officers, employees or agents. Reliance upon information in this material is at the sole discretion of the reader. ***Past performance is not a reliable indicator of future performance.***