‘AI Security’ emerges as the next cybersecurity theme

Veröffentlicht am 20. März 2026

Team8
Global venture group

Elvira Kuramshina
Associate Director, Quantitative Research

Wichtige Erkenntnisse

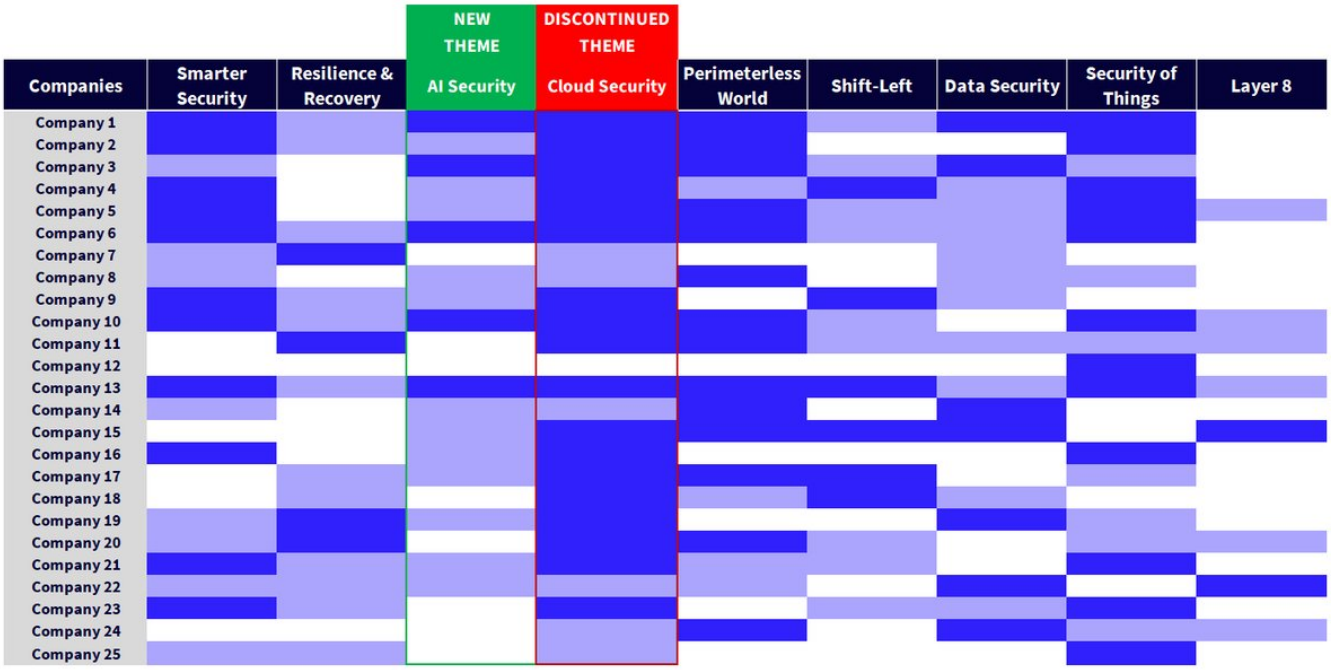
- The WisdomTree Team8 Cybersecurity Index dynamically evolves its key cyber themes to remain aligned with structural shifts in the cybersecurity landscape.
- Cloud security is no longer a differentiator, as capabilities are now embedded across most cybersecurity platforms.
- The Cloud Security theme is retired to better reflect the maturity and ubiquity of cloud protection.
- AI adoption is creating new attack surfaces, including model manipulation, data poisoning, and sensitive data leakage.
- AI Security is emerging as a distinct, high-growth category, driven by new risks and specialized solutions.

Cybersecurity is evolving rapidly as new technologies, threat vectors and enterprise architectures reshape how organisations defend their systems and data. The WisdomTree Team8 Cybersecurity Index was designed to track how these developments are shaping the future of cybersecurity through key cybersecurity themes. As cybersecurity innovation continues to accelerate, periodic updates to these themes help ensure the Index remains aligned with how modern cybersecurity is being built, deployed and adopted across the industry.

This is not the first time we have adjusted; for example, in 2023, we introduced the Layer 8 theme focused on human risk. Today, to reflect the latest developments in the cybersecurity landscape, particularly the maturation of cloud security and the rapid rise of artificial intelligence, we are again making updates to the index’s key cybersecurity themes (Figure 1 and Table 1).

Figure 1: Exposure of companies across cyber themes in the WisdomTree Team8 Cybersecurity Index

Exposure to each theme is presented from darker blue (high exposure) to white (no product in the space).



Companies	Smarter Security	Resilience & Recovery	NEW THEME AI Security	DISCONTINUED THEME Cloud Security	Perimeterless World	Shift-Left	Data Security	Security of Things	Layer 8
Company 1									
Company 2									
Company 3									
Company 4									
Company 5									
Company 6									
Company 7									
Company 8									
Company 9									
Company 10									
Company 11									
Company 12									
Company 13									
Company 14									
Company 15									
Company 16									
Company 17									
Company 18									
Company 19									
Company 20									
Company 21									
Company 22									
Company 23									
Company 24									
Company 25									

Source: WisdomTree, Team8. The classification presented will take effect after the close of business on 20 March 2026. **You cannot invest directly in an index. Historical performance is not an indication of future performance and any investments may go down in value.**

Table 1: Description of cyber themes in the WisdomTree Team8 Cybersecurity Index

Cyber theme	Rationale
Smarter Security	Response capacity is stretched to its limits as organizations face immense security complexity – dozens of products that aren't integrated, an expanding enterprise network, a cyber talent shortage, and an adversary leveraging increasingly sophisticated capabilities. Smarter security can plug the
Resilience & Recovery	Digital infrastructure is now business critical, and therefore recovery from cyberattacks is now a core tenet of risk mitigation and business continuity. Any sound security strategy necessitates capabilities that enable rapid recovery and reconstitution of assets and capabilities.
Cloud Security	**DISCONTINUED THEME**
AI Security	**NEW THEME**
Perimeterless World	The enterprise perimeter is nearly extinct and the shift to remote work during the pandemic is accelerating its demise. Identity and zero trust architectures will become increasingly important in governing access management.
Shift-Left	Developing and managing software is becoming more agile and faster than ever. Security can't come after the fact, but needs to be shifted-left to the developers, embedding security considerations from the start in a DevSecOps model.
Data Security	Globalization and growth of the digital economy are colliding with emerging privacy regulations and consumer preferences, providing users with more control over their data. Architectural design and business processes must accommodate new privacy- and zero trust-driven strategies.
Security of Things	IoT device connectivity unlocks new business value in the industrial economy. But as IT networks and operational technology (OT) networks converge, the attack surface expands, and adversaries can move from stealing data to threatening health and safety.
Layer 8	No matter how much money a company invests in security controls, humans will always defeat them. Layer 8 is all about how we train humans, how we empower them, how we monitor them, or in certain instances, how we take them out of the loop.

Source: Team8, WisdomTree. You cannot invest directly in an index. **Historical performance is not an indication of future performance and any investments may go down in value.**

Retiring the Cloud Security theme

The Cloud Security theme was originally designed to capture companies focused on protecting cloud infrastructure and environments. This included technologies such as Cloud Workload Protection Platforms (CWPP), Cloud Infrastructure Entitlement Management (CIEM), Cloud Security Posture Management (CSPM), SaaS Security Posture Management (SSPM), Cloud-Native Application Protection Platforms (CNAPP), Container Security, and Cloud Access Security Brokers (CASB).

However, as cloud adoption has become universal across enterprises, cloud security capabilities have also become widely embedded across the cybersecurity landscape. Today, most cybersecurity vendors offer products that address cloud environments in some capacity. As a result, in our view, cloud security is no longer a meaningful differentiator between cybersecurity vendors, nor does it serve as a strong proxy for identifying companies aligned with emerging cybersecurity growth themes. Reflecting this shift, the Cloud Security theme is being retired as a distinct category within the index.

While the Cloud Security theme is being discontinued, the Index is introducing Artificial Intelligence (AI) Security as the next cybersecurity theme, driven by the rapid adoption of AI systems, the expansion of the AI attack surface, and the emergence of specialised AI security solutions.

Introducing AI Security as a distinct cybersecurity theme

Artificial intelligence is rapidly becoming embedded across enterprise software, infrastructure and workflows. While AI is transforming productivity and enabling new capabilities spanning industries, it is also introducing new security risks and attack surfaces that create unique opportunities for attackers. Several major drivers are accelerating the evolution of the AI security market:

Explosion in the adoption of AI systems

Enterprises are rapidly deploying AI tools across software development, knowledge management, customer support and internal workflows. What began as experimentation with generative AI is increasingly moving into production environments and becoming embedded in core enterprise software systems. Organisations are also deploying AI agents that autonomously interact with applications, data sources and external systems, further expanding the operational role of AI within enterprise environments.

New attack surfaces in AI infrastructure

Since AI systems rely on data pipelines, training environments, model repositories, and inference infrastructure, each component represents a potential entry point for attackers. Moreover, the growing use of AI agents introduces new security considerations that make them attractive targets. As a result, security teams are increasingly confronting risks that did not exist until recently. These risks include manipulation attacks, where adversaries craft malicious inputs to bypass safeguards or produce unintended outputs; infection attacks, where attackers poison training data or manipulate model behaviour to influence system outputs; and exfiltration attacks, which attempt to extract sensitive information such as training data, model parameters, or proprietary algorithms from AI systems.

Rapid emergence of specialised AI security solutions

Over the past year, a new generation of security companies has emerged, focused specifically on the unique security needs of AI systems and AI-native environments. These solutions are designed to secure AI models and training environments, protect data pipelines and model supply chains, monitor and control AI system behaviour, detect vulnerabilities and misuse in AI applications, and enforce governance, compliance, and security controls for enterprise AI deployments.

As these risks and technologies continue to evolve, the cybersecurity market is beginning to recognise AI Security as a distinct category within the broader cybersecurity ecosystem, and for these reasons, the WisdomTree Team8 Cybersecurity Index will now formally recognise AI Security as its own dedicated theme.

Positioning the Index for the future

The WisdomTree Team8 Cybersecurity Index was designed to track key cybersecurity themes emerging across the industry, and as the industry evolves, so do key themes shaping its future. By retiring the Cloud Security theme and introducing the AI Security theme, the index continues to reflect key structural

developments in the cybersecurity market, helping ensure it remains aligned with the technologies and themes shaping the future of cybersecurity.

Team8 disclaimer:

This Article represents the opinions of Team8 Labs Inc. (“Team8”) and is for informational purposes only. You should not treat any opinion expressed by Team8 as a specific inducement to make an investment in any security, but only as an expression of Team8’s opinions. Team8’s statements and opinions are subject to change without notice. Team8 is not registered as an investment adviser under the Investment Advisers Act of 1940, as amended (the “Advisers Act”), and relies upon the “publishers’ exclusion” from the definition of investment adviser under Section 202(a)(11) of the Advisers Act. As such, the information contained in this Article does not take into account any particular investment objectives, financial situation or needs and is not intended to be, and should not be construed in any manner whatsoever as, personalized investment advice. The information in this Article is provided for informational and discussion purposes only and is not intended to be, and shall not be regarded or construed as, a recommendation for a transaction or investment or financial, tax, investment or other advice of any kind by Team8. You should determine on your own whether you agree with the information contained in this Article. Certain of the securities referenced in this Article may currently, or from time to time, be constituents of an index developed and maintained by WisdomTree Investments, Inc. using data provided by Team8, which has been or will be licensed for a fee to one or more investment funds. In addition, certain officers or employees of Team8 or funds or other persons or entities affiliated or associated with Team8 may hold shares of, be officers or directors of, or otherwise be associated with some or all of the issuers of the securities referenced in this Article or included in such index. Team8 expressly disclaims all liability with respect to any act or omission taken based on, and makes no warranty or representation regarding, any of the information included in this Article.

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can offen lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.