Il WisdomTree Cybersecurity si evolve per riflettere l'era dell'IA

Pubblicato il 26 ottobre 2026

Elvira Kuramshina
Associate Director, Quantitative Research

Punti chiave

- Una nuova era di rischi informatici: l'IA generativa ha già cambiato le dinamiche economiche della criminalità informatica, e i modelli di IA più avanzati stanno ora aprendo una nuova fase di rischi e domanda. Abbiamo aggiornato la metodologia del WisdomTree Team8 Cybersecurity UCITS Index per riflettere questo cambiamento.
- L'IA sta ridefinendo gli aspetti da proteggere: con la creazione di nuove superfici di attacco e nuove categorie di spesa per la sicurezza informatica, le fonti di crescita del settore stanno cambiando e i criteri di selezione e ponderazione delle società devono evolversi di conseguenza.
- Tre aggiornamenti alla metodologia: un punteggio di pertinenza tematica migliorato e basato su molteplici indicatori, un punteggio di crescita prospettico e una formula di ponderazione trasparente e modulare, tutti concepiti per cogliere le opportunità offerte dalla sicurezza informatica nell'era dell'IA.
- Stesse fondamenta, orientamenti più mirati: l'universo di partenza, il quadro di base e il partner specializzato, Team8, rimangono invariati, mentre le ponderazioni del portafoglio si spostano verso le società con un posizionamento più solido nel settore della sicurezza informatica e migliori prospettive di crescita.
- La sicurezza informatica come livello di base: con la crescente integrazione dell'IA nell'economia digitale, l'indice è concepito per tenere il passo con i segmenti caratterizzati dalla domanda più sostenuta.

La sicurezza informatica è da sempre una corsa tra aggressori e difensori e l'intelligenza artificiale (IA) sta cambiando il ritmo di tale competizione. Negli ultimi anni, l'IA generativa ha già ridefinito le dinamiche economiche della criminalità informatica, rendendo gli attacchi più rapidi e numerosi e fornendo al contempo ai difensori strumenti più potenti per rilevarli e contrastarli. Ora, i progressi dei modelli di IA più avanzati stanno inaugurando una nuova era. Con la crescente diffusione dell'IA nei sistemi aziendali, emergono nuovi elementi da proteggere, dai modelli ai dati di formazione, fino agli agenti autonomi e alle identità non umane. Le opportunità continuano a riguardare la sicurezza informatica, ma le fonti di crescita e di differenziazione al suo interno stanno cambiando. Insieme al nostro partner specializzato, Team8, analizziamo le implicazioni dei cambiamenti per il settore.

Negli ultimi anni, questo è stato caratterizzato dalla sicurezza nativa del cloud, incentrata sull'identità e potenziata dall'IA. Oggi si sta evolvendo in un contesto sempre più definito dalle capacità dei modelli più avanzati, dagli agenti autonomi, dalle identità non umane e dalle nuove superfici di attacco, con gli stessi sistemi di IA che necessitano di una protezione specifica. Per cogliere le opportunità derivanti da questa transizione è necessario un approccio in grado di adattarsi agli ambiti in cui l'IA sta creando la domanda futura più forte. La nostra risposta sul piano metodologico consiste nell'aggiornamento degli indicatori, sulla base di valutazioni più approfondite degli esperti per la selezione e la ponderazione delle società, mantenendo invariati l'universo di riferimento e la struttura metodologica di base.

Perché le opportunità nel settore della sicurezza informatica stanno cambiando

Il panorama delle minacce informatiche si sta intensificando contemporaneamente su più fronti. Il 2026 Global Threat Report di CrowdStrike ha rilevato che, nel caso più rapido, un criminale informatico è passato dall'accesso iniziale al movimento laterale in appena 27 secondi, a dimostrazione di quanto possa essere ridotto il margine di errore per chi si occupa della difesa. Anche il numero dei soggetti che compiono tali attacchi è in aumento, con una crescita del 49% su base annua dei gruppi di ransomware attivi. Nel frattempo, i costi di una protezione inefficace continuano a salire. Secondo le stime di IBM, il costo medio globale di una violazione dei dati ammonta a 4,99 milioni di dollari.

L'IA sta ora plasmando entrambi i fronti di questa battaglia. Da un lato, ha creato una nuova superficie di attacco. Una ricerca di Check Point ha rilevato che circa un prompt di IA generativa su 80 mette a rischio dati sensibili, mentre IBM stima che il costo medio di una violazione che coinvolge un attacco di inversione di un modello di IA sia pari a circa 6 milioni di dollari. Dall'altro lato, l'IA si sta dimostrando una risorsa preziosa per chi si occupa della difesa. L'analisi di IBM suggerisce che le organizzazioni che utilizzano ampiamente l'IA e l'automazione nelle proprie operazioni di sicurezza risparmiano in media 1,93 milioni di dollari per violazione. Questa duplice natura sta dando origine a una categoria distinta di spesa per la sicurezza, incentrata sulla protezione dei modelli, dei dati di formazione, degli agenti autonomi e delle identità non umane. Nessun altro sviluppo illustra meglio questo cambiamento della recente comparsa di modelli di IA più avanzati, dotati di capacità sofisticate nel campo della sicurezza informatica.

Figura 1: L'IA sta diventando una nuova superficie di attacco e un nuovo strumento sia per i criminali informatici che per i responsabili della relativa sicurezza

In oltre 90 organizzazioni	1 prompt di IA generativa su 80	6 milioni di dollari
Gli aggressori hanno sfruttato strumenti legittimi di IA generativa, inserendo prompt dannosi per generare comandi finalizzati al furto di credenziali e criptovalute (CrowdStrike).	espone dati sensibili agli aggressori (Check Point).	è il costo medio globale di una violazione dei dati causata da un attacco di inversione di un modello di IA, a dimostrazione della crescente difficoltà di proteggere i dati di formazione e le informazioni sensibili (IBM).

56%	Il 7,5% dei prompt di IA generativa	1,93 milioni di dollari
Di aumento degli attacchi basati sull'IA, trainato dalle impersonificazioni tramite deepfake generati dall'IA e dai malware potenziati dall'IA (IBM).	Contiene dati sensibili o informazioni private (Check Point).	è il risparmio sui costi derivante dall'ampio utilizzo dell'IA e dell'automazione nelle operazioni di sicurezza, rispetto alle organizzazioni che non ne fanno uso (IBM).

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

Il rilascio ad accesso controllato di Claude Mythos Preview di Anthropic e la successiva iniziativa Project Glasswing, che ha coinvolto circa 50 partner, hanno segnato un punto di svolta, dimostrando un nuovo livello di capacità dei modelli di IA più avanzati nell'individuazione delle vulnerabilità su larga scala. In un solo mese, i partner hanno rilevato oltre 10.000 vulnerabilità di gravità elevata o critica. L'AI Security Institute del Regno Unito, che ha valutato Mythos Preview nell'aprile 2026, ha descritto queste capacità come a duplice uso: pongono sfide concrete per la sicurezza, ma offrono anche il potenziale per miglioramenti radicali delle capacità di difesa. In vista dell'arrivo di modelli ancora più avanzati, l'istituto ha sottolineato quanto sia fondamentale investire fin da ora nella difesa informatica.

La risposta sul piano metodologico

La risposta metodologica all'evoluzione delle opportunità nel settore della sicurezza informatica si articola in tre aggiornamenti: un punteggio di pertinenza migliorato e basato su molteplici indicatori, un punteggio di crescita prospettico e una formula di ponderazione trasparente e modulare. Nel loro insieme, questi aggiornamenti mirano a individuare la direzione in cui si sta evolvendo la domanda di sicurezza informatica e le società che si prevede si trovino nella posizione migliore per beneficiarne.

Un punteggio di pertinenza migliorato e basato su molteplici indicatori

Punteggio di pertinenza = ampiezza dell'esposizione alla sicurezza informatica + leadership di prodotto + temi prioritari

In precedenza, il punteggio di pertinenza tematica si basava su un unico indicatore: la classificazione di una società come “pertinenza ampia” (Broad Focus) o “pertinenza ristretta” (Narrow Focus). Ora viene determinato dalla somma di tre indicatori complementari e interpretabili. Ciascuno di essi coglie una dimensione diversa del posizionamento di una società nel settore della sicurezza informatica.

- L’**ampiezza dell’esposizione alla sicurezza informatica (40%)** premia le società in grado di beneficiare della domanda in numerosi segmenti del mercato, anziché dipendere da una gamma ristretta di soluzioni. Una società è ritenuta di “pertinenza ampia” quando presenta un’elevata esposizione ad almeno la metà dei temi di sviluppo della sicurezza informatica. Le società di “pertinenza ristretta”, che presentano un’elevata esposizione ad almeno un tema, rimangono ammissibili, consentendo così anche agli operatori specializzati di rientrare nell’universo delle opportunità d’investimento.
- La **leadership di prodotto (30%)** riconosce non soltanto l’ampiezza, ma anche la profondità. Team8 valuta i prodotti di sicurezza informatica all’interno di specifiche categorie di soluzioni e identifica le società i cui prodotti sono leader nei rispettivi segmenti, anche quando la gamma complessiva degli stessi è più limitata. Questo consente alla strategia di allocare alle società in grado di cogliere la domanda emergente grazie a capacità differenziate.
- I **temi prioritari (20 o 30%)** consentono di orientarsi verso i segmenti nei quali si prevede un’accelerazione della domanda di sicurezza informatica. Una società ottiene un punteggio del 20% se almeno la metà della sua esposizione riguarda questi temi, che sale al 30% se è anche leader di prodotto. Gli attuali temi prioritari sono **Sicurezza dell’IA**, che comprende le soluzioni destinate a proteggere gli stessi sistemi di IA; **Sicurezza più intelligente**, che utilizza l’IA e l’automazione per rendere le risposte alle minacce più rapide e adattive; e **Mondo senza confini**, incentrato sulle identità e sugli accessi, sempre più cruciali man mano che gli agenti di IA creano un numero crescente di identità non umane. Questi temi non sono fissi e possono cambiare con l’evoluzione della tecnologia e dei vettori di attacco.

Un punteggio di crescita prospettico

Il punteggio di crescita aggiornato misura la capacità prevista di una società di tradurre la domanda di sicurezza informatica in ricavi, utilizzando come indicatore la crescita stimata del fatturato. Adotta un approccio prospettico laddove siano disponibili dati affidabili, seguendo un semplice ordine di preferenza: innanzitutto il tasso annuo di crescita composto (CAGR) del fatturato stimato su due anni, seguito dalla stima su un anno qualora non sia disponibile quella biennale e, infine, dalla crescita effettiva registrata negli ultimi dodici mesi qualora le stime siano elaborate da meno di cinque analisti.

Le società vengono quindi classificate rispetto alle altre società idonee dell’universo della sicurezza informatica, anziché sulla base di soglie di crescita fisse, in modo che le stesse si adattino alle condizioni di mercato e al ritmo del ciclo del settore. Il 20% delle società con i punteggi più bassi viene escluso, mentre quelle rimanenti sono suddivise in quattro gruppi, ciascuno con un proprio fattore di ponderazione:

- **crescita rapida e dimensioni significative (1,5x) -** società a crescita più rapida il cui fatturato recente figura tra i dieci più elevati del gruppo delle società a crescita più rapida ed è superiore alla mediana dell'universo. Il gruppo prevede un massimo di dieci società;
- **crescita rapida (1,2x) -** società con una crescita superiore alla mediana dell'universo;
- **crescita (1x) -** società con una crescita pari o inferiore alla mediana;
- **crescita in rallentamento (0,8x) -** società appartenenti al 40% inferiore in base al relativo punteggio, la cui crescita recente supera quella stimata dagli analisti, segnalando un rallentamento del momentum.

Un'unica formula di ponderazione trasparente

Ponderazione finale = stessa ponderazione × fattore di pertinenza × fattore di crescita

Ogni società parte dalla stessa ponderazione. Tale ponderazione iniziale viene quindi moltiplicata per due fattori, uno derivante dal punteggio di pertinenza e l'altro dal punteggio di crescita. I risultati vengono successivamente normalizzati affinché la somma delle ponderazioni del portafoglio sia pari al 100%.

Il **fattore di pertinenza** è pari a 1 più il punteggio di pertinenza della società. Ciascuno dei tre indicatori apporta una propria maggiorazione: fino al 40% per l'ampiezza, il 30% per la leadership di prodotto e il 20 o il 30% per l'esposizione ai temi prioritari. Una società può quindi essere sovraponderata di un valore pari al 100% prima dell'applicazione del fattore di crescita.

Il **fattore di crescita** adegua successivamente la ponderazione in base al gruppo di crescita a cui appartiene la società, passando da una sovraponderazione per le società del gruppo "crescita rapida e dimensioni significative", a una sottoponderazione per quelle del gruppo "crescita in rallentamento".

L'approccio è trasparente perché ogni orientamento della ponderazione è riconducibile a uno specifico indicatore, e modulare perché i fattori di pertinenza e di crescita operano indipendentemente e possono essere analizzati singolarmente. Le ponderazioni sono inoltre soggette alle regole dell'indice in materia di concentrazione, liquidità e capitalizzazione di mercato, che garantiscono la diversificazione del portafoglio e la sua effettiva investibilità.

La continuità del portafoglio rimane un elemento centrale

Per illustrare le differenze tra la metodologia aggiornata e il portafoglio precedente, confrontiamo il portafoglio target per il ribilanciamento di ottobre 2026, costruito secondo le nuove regole, con le precedenti ponderazioni dell'indice stabilite a marzo 2026.

La struttura principale del portafoglio rimane sostanzialmente invariata. Sette delle dieci maggiori partecipazioni del nuovo portafoglio figuravano già tra le prime dieci a marzo, mentre le prime tre, CrowdStrike,

Palo Alto Networks e Fortinet, presentano ciascuna la stessa ponderazione, pari al 7,68%. Complessivamente, le prime dieci rappresentano il 58,99% del portafoglio.

Figura 2: Prime 10 società della strategia migliorata dopo il ribilanciamento di ottobre 2026

Nome della società	Ponderazione	Classificazione di crescita	Fattore di ponderazione della pertinenza
CrowdStrike Holdings, Inc.	7,68%	Crescita rapida e dimensioni significative	2,00
Palo Alto Networks, Inc.	7,68%	Crescita rapida e dimensioni significative	2,00
Fortinet, Inc.	7,68%	Crescita rapida e dimensioni significative	2,00
Zscaler, Inc.	6,15%	Crescita rapida e dimensioni significative	1,60
Rubrik, Inc.	6,15%	Crescita rapida e dimensioni significative	1,60
Varonis Systems, Inc.	4,92%	Crescita rapida	1,60
Netskope, Inc.	4,92%	Crescita rapida	1,60
Cloudflare, Inc.	4,61%	Crescita rapida e dimensioni significative	1,20
Datadog, Inc.	4,61%	Crescita rapida e dimensioni significative	1,20
Elastic NV	4,61%	Crescita rapida e dimensioni significative	1,20
Top 10 total	**58,99%**		

Fonte: WisdomTree. Sulla base delle partecipazioni target predisposte per il ribilanciamento del WisdomTree Team8 Cybersecurity UCITS Index dopo la chiusura dei mercati del 23 ottobre 2026. **Non è possibile investire direttamente in un indice. La performance storica non è indicativa di quella futura e qualsiasi investimento può diminuire di valore.**

Il cambiamento più significativo riguarda la distribuzione delle ponderazioni. Il nuovo portafoglio attribuisce una maggiore ponderazione alle società con un posizionamento più solido nel settore della sicurezza informatica, aumentando il peso di tutti e tre i gruppi del punteggio di pertinenza, in particolare quelli relativi alla leadership di prodotto e ai temi prioritari. Sul fronte della crescita, una quota maggiore è allocata

alle società del gruppo “crescita rapida e dimensioni significative”, mentre non viene più attribuita alcuna ponderazione alle società dell’universo che si collocano nel 20% inferiore in base ai punteggi di crescita.

Figura 3: Confronto tra la nuova e la precedente strategia per gruppi di pertinenza e di crescita

Gruppi	Ponderazione nel nuovo WCBR	Ponderazione nel vecchio WCBR
Punteggio di pertinenza		
Ampiezza dell’esposizione alla sicurezza informatica	27,14%	24,33%
Leadership di prodotto	56,54%	49,03%
Temi prioritari	84,19%	76,42%
Punteggio di crescita		
Crescita rapida e dimensioni significative	49,16%	41,82%
Crescita rapida	25,03%	25,50%
Crescita	9,01%	20,54%
Crescita in rallentamento	16,80%	7,99%
20% inferiore	0%	4,15%

Fonte: WisdomTree. Le ponderazioni del nuovo WCBR si basano sulle partecipazioni target predisposte per il ribilanciamento del WisdomTree Team8 Cybersecurity UCITS Index dopo la chiusura dei mercati del 23 ottobre 2026. Le ponderazione nel vecchio WCBR rappresentano le ponderazioni target impostate per il precedente ribilanciamento di marzo 2026. **Non è possibile investire direttamente in un indice. La performance storica non è indicativa di quella futura e qualsiasi investimento può diminuire di valore.**

In sintesi

La sicurezza informatica sta diventando un elemento fondamentale dell’economia digitale e dell’IA, mentre la domanda che ne deriva viene ridefinita dai modelli di IA più avanzati. La metodologia aggiornata mantiene invariati l’universo di riferimento, il quadro di base e il partner specializzato, perfezionando al contempo i criteri di selezione e ponderazione delle società per seguire l’evoluzione della domanda.

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.

INFORMAZIONI IMPORTANTI

La presente documentazione è stata redatta da WisdomTree e dalle sue affiliate e non costituisce previsione, ricerca, consulenza di investimento, raccomandazione, offerta o sollecitazione ad acquistare o vendere titoli o ad adottare qualsivoglia strategia di investimento. Le opinioni espresse sono aggiornate alla data di redazione della documentazione e possono cambiare a seconda del variare delle condizioni. Le informazioni e le opinioni riportate nella presente documentazione derivano da fonti proprietarie e non proprietarie. Pertanto, WisdomTree, le sue affiliate o i suoi incaricati, dipendenti o agenti non garantiscono la correttezza e l'affidabilità delle stesse e declinano qualsiasi responsabilità derivante da errori e omissioni (ivi compresa la responsabilità nei confronti di qualunque persona per negligenza). Fare affidamento sulle informazioni nel presente materiale è ad esclusiva discrezione del lettore. **I rendimenti ottenuti nel passato non sono un'indicazione affidabile dei rendimenti futuri.**