Battere i benchmark più ampi nel 2025 con la sicurezza informatica

Pubblicato il 16 giugno 2025

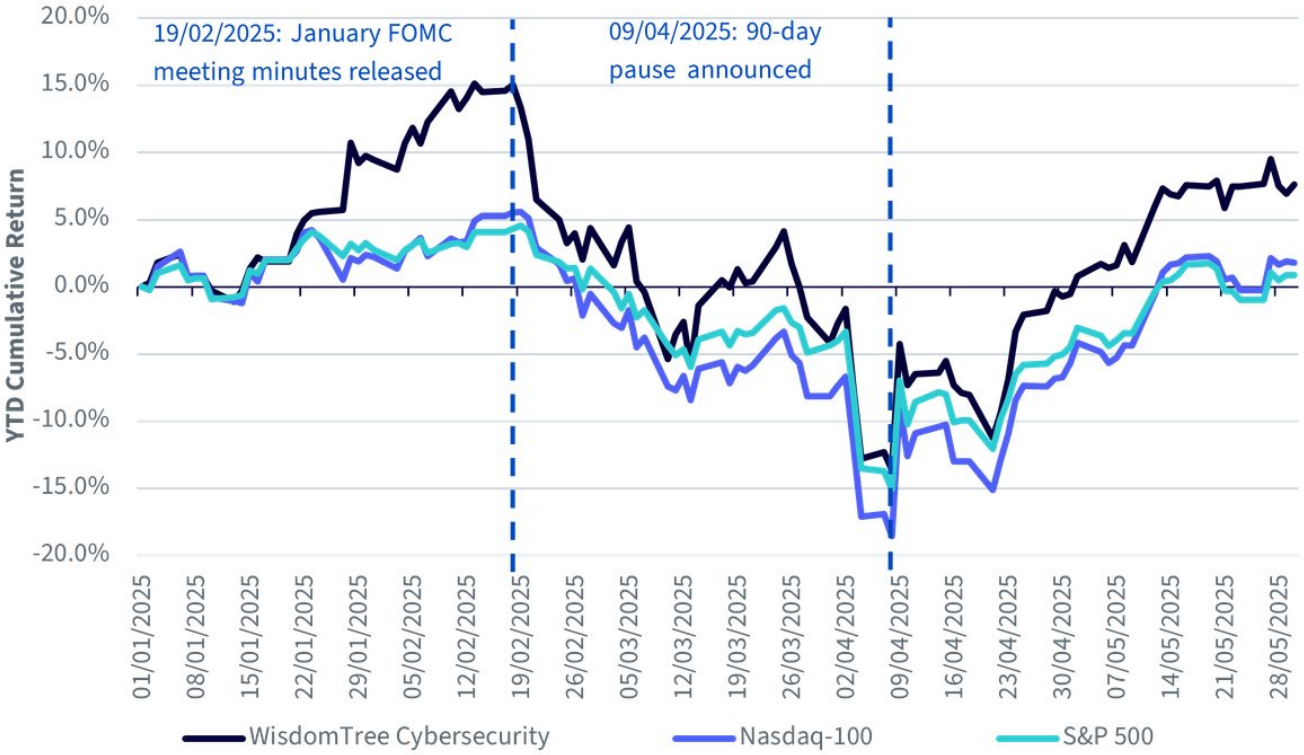
Elvira Kuramshina
Associate Director, Quantitative Research

Principali insegnamenti

- La sempre maggiore digitalizzazione a livello mondiale produce un aumento della domanda di soluzioni di sicurezza informatica. Ma oltre all'incessante ondata di digitalizzazione, a rafforzare ulteriormente il potenziale di crescita del settore sono molteplici fattori favorevoli.
- Mentre i timori relativi ai tassi di interesse e ai dazi contribuiscono ad aumentare la volatilità e a scuotere la fiducia delle imprese nella propria capacità di spesa, i fattori favorevoli di lungo periodo forniscono una base solida per investimenti duraturi nella sicurezza informatica.
- Il potenziale di differenziazione offerto dal WisdomTree Team8 Cybersecurity UCITS Index e la resilienza della domanda relativa alla sicurezza informatica lo rendono un investimento interessante a lungo termine, da affiancare alle esposizioni core tradizionali.
- Prodotti correlati WisdomTree Cybersecurity UCITS ETF – USD Acc Scopri di più

Il 2025 sta mettendo a dura prova la pazienza degli investitori. Dall'incertezza causata dai dazi all'aumento dei rischi geopolitici, fino all'accelerazione della proliferazione dell'IA, i mercati si trovano ad affrontare periodi di forte turbolenza e volatilità. In un contesto così complesso, il WisdomTree Team8 Cybersecurity UCITS Index si distingue per aver sovraperformato, da inizio anno, i benchmark tecnologici e azionari più ampi, a dimostrazione della sua resilienza nonostante l'indebolimento dell'economia e il cambiamento delle priorità e della spesa delle aziende (cfr. Figura 1). In questo post approfondiamo la resilienza della domanda di soluzioni di sicurezza informatica a lungo termine, evidenziamo i venti contrari a breve termine derivanti dall'incertezza macroeconomica e, infine, discutiamo di come un'allocazione satellite alla sicurezza informatica possa potenzialmente incrementare i rendimenti del portafoglio e portarli a superare quelli dei benchmark più ampi.

Figura 1: Da inizio anno, il WisdomTree Cybersecurity ha battuto il Nasdaq-100 e l'S&P 500



Fonte: WisdomTree, Bloomberg. Aggiornata al 30 maggio 2025. Il WisdomTree Cybersecurity è rappresentato dal WisdomTree Team8 Cybersecurity UCITS Index. Tutti i rendimenti si riferiscono a indici di tipo "net total return". **Non è possibile investire direttamente in un indice. La performance storica non è indicativa di quella futura e qualsiasi investimento può diminuire di valore.**

Resilienza della domanda di sicurezza informatica

In un mondo che diventa sempre più digitale, la sicurezza informatica assume un ruolo fondamentale per salvaguardare il nostro futuro. Ma oltre all'incessante ondata di digitalizzazione, a rafforzare ulteriormente il potenziale di crescita della sicurezza informatica sono molteplici fattori favorevoli:

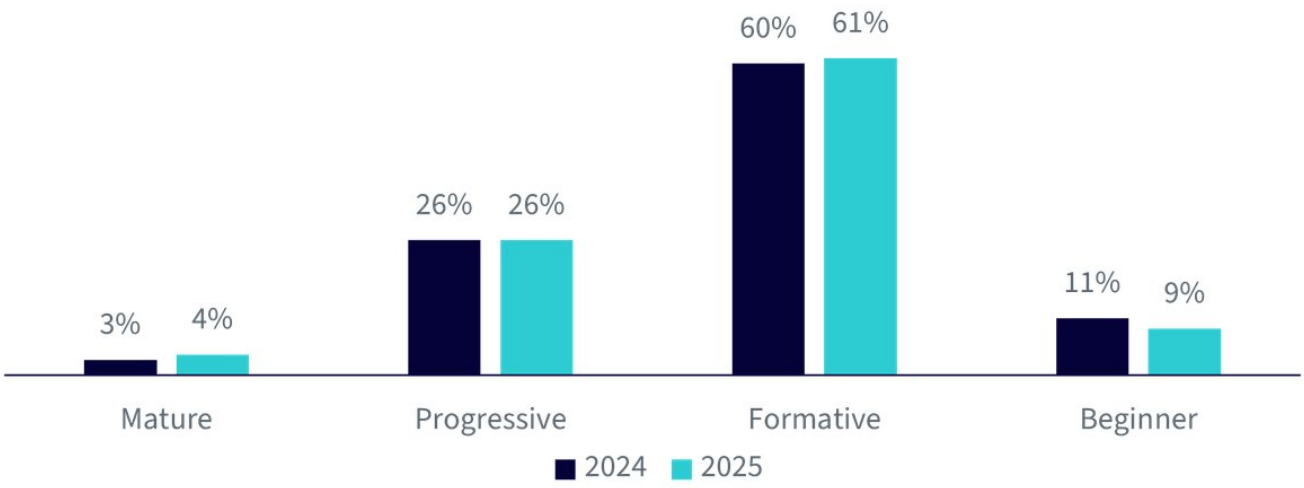
1. Ridefinizione della resilienza aziendale e competitiva

La digitalizzazione, già accelerata dalla pandemia globale, ha ricevuto un ulteriore impulso con la rivoluzione innescata dall'IA. Tuttavia, ogni livello aggiuntivo di infrastruttura digitale richiede misure di sicurezza solide e, nell'era digitale moderna, la sicurezza informatica diventa una questione di resilienza aziendale. Un recente incidente informatico ai danni di Marks & Spencer, uno dei maggiori rivenditori al dettaglio del Regno Unito, è un esempio di quanto, nella realtà moderna, gli attacchi informatici possano essere devastanti e costosi. Secondo le stime dell'azienda, le perdite in termini di profitti ammontano a 300 milioni di dollari e i disagi alle operazioni online dureranno fino a luglio[1].

L'incidente sottolinea l'importanza, per le aziende moderne, di disporre di soluzioni di sicurezza informatica adeguate, oltre a spiegare perché la relativa domanda rimane elevata anche in periodi di turbolenza economica. Allo stesso tempo, nel suo Cybersecurity Readiness Index 2025, Cisco riferisce che le aziende

faticano a stare al passo con l'evoluzione del panorama delle minacce: solo il 30% mostra uno stato di preparazione “maturo” o “progressivo” rispetto ai rischi odierni in materia di sicurezza informatica, con dinamiche pressoché invariate dal 2024 (cfr. Figura 2). A sua volta, questo dimostra il potenziale di crescita futura delle aziende del settore, dato che le imprese che cercano di rafforzare la propria resilienza competitiva inizieranno ad aumentare la spesa per la sicurezza informatica. Ad esempio, le aziende che dispongono di soluzioni di sicurezza informatica adeguate possono ottenere un vantaggio competitivo basato sulla fiducia e adottare in sicurezza nuove tecnologie per mantenerlo.

Figura 2: Preparazione globale rispetto ai rischi legati alla sicurezza informatica



Fonte: Cisco Cybersecurity Readiness Index 2025. Il Cisco Cybersecurity Readiness Index 2025 valuta il grado di preparazione delle aziende rispetto ai rischi odierni in materia di sicurezza informatica. Per farlo, utilizza cinque pilastri: Identity Intelligence, Machine Trustworthiness, Network Resilience, Cloud Reinforcement e Artificial Intelligence (AI) Fortification. La valutazione si basa su un sondaggio condotto in doppio cieco tra 8.000 aziende e leader del settore della sicurezza informatica in 30 mercati globali e in un'ampia gamma di settori del comparto privato.

2. Rischi geopolitici e venti favorevoli a livello politico

Inoltre, il parallelo aumento delle tensioni geopolitiche e degli attacchi informatici di alto profilo ha mantenuto la sicurezza informatica al centro dell'attenzione non solo delle aziende, ma anche dei governi. Il panorama delle minacce in rapida evoluzione, che include attori statali, ha portato a una serie di risposte normative e strategiche che stanno rafforzando la domanda di soluzioni di sicurezza informatica a lungo termine. Negli Stati Uniti, la National Cybersecurity Strategy (2023) ha sottolineato l'urgenza di adottare un approccio più intenzionale e coordinato alla difesa informatica, oltre a promuovere il riallineamento degli incentivi a sostegno di investimenti strategici a lungo termine nel ciberspazio. In Europa, la Legge dell'UE sulla cibersolidarietà mira a rafforzare la preparazione, il rilevamento e la risposta collettivi attraverso finanziamenti nell'ambito dell'obiettivo strategico della “Cibersicurezza” e di azioni congiunte di preparazione, consapevolezza della situazione e cooperazione transfrontaliera. Nel frattempo, anche la

NATO sta aumentando l'attenzione rivolta alla difesa informatica collettiva, adeguando la propria posizione difensiva in risposta al panorama in rapida evoluzione delle minacce.

3. Proliferazione dell'IA generativa

Dal lancio di ChatGPT il 30 novembre 2022, l'IA generativa ha conquistato il mondo. Se da un lato questa tecnologia offre alle aziende di sicurezza informatica funzionalità innovative, come l'automazione del rilevamento delle minacce e il miglioramento dell'analisi dei dati, dall'altro crea nuove vulnerabilità e favorisce l'evoluzione del panorama delle minacce. Con la sua rapida diffusione e i suoi continui progressi, la tecnologia è stata uno dei principali catalizzatori della crescita degli attacchi informatici. Dagli strumenti malevoli per generare deepfake e assumere un'identità diversa all'ingegneria sociale, fino all'avvelenamento dei dati dei modelli linguistici di grandi dimensioni (LLM) e al jailbreak degli stessi per migliorare la creazione di malware, gli autori delle minacce stanno sfruttando l'IA per diventare più efficienti e prolifici (e raggiungere più rapidamente i propri obiettivi).

Allo stesso tempo, le organizzazioni si trovano ad affrontare un aumento dei rischi di fuga dei dati causato dall'uso di modelli di IA. Nel suo primo "AI Security Report 2025", Check Point riferisce che 1 prompt su 13 generato dall'IA contiene dati sensibili o privati e 1 su 80 mette dati sensibili a disposizione degli aggressori. Allo stesso tempo, Check Point ha sottolineato che le aziende che non utilizzano l'IA potrebbero scoprire che i propri dipendenti sfruttano strumenti di IA senza autorizzazione, con conseguenti rischi aggiuntivi. Per rispondere a questa sfida, diverse aziende specializzate nella sicurezza informatica hanno già iniziato a offrire soluzioni su misura specificamente pensate per i rischi derivanti dall'uso aziendale degli LLM. Con la diffusione delle minacce informatiche basate sull'IA, la domanda di soluzioni di cibersicurezza è destinata ad aumentare.

Venti contrari macro a breve termine

Nonostante la forte domanda sottostante e l'interessante potenziale di crescita futura, le aziende specializzate nella sicurezza informatica non sono immuni dalle turbolenze macroeconomiche più ampie. Infatti, spesso rappresentano titoli tecnologici a più lunga duration in termini di sensibilità alle aspettative relative ai tassi di interesse. Il motivo risiede principalmente nel fatto che molte delle principali società di sicurezza informatica stanno crescendo rapidamente e gran parte dei flussi di cassa attesi sono proiettati nel futuro. Con l'aumento dei tassi di interesse, tali flussi di cassa futuri vengono scontati in misura maggiore, rendendo le valutazioni più sensibili alle variazioni delle aspettative relative ai tassi.

I recenti sviluppi della politica monetaria negli Stati Uniti, in un contesto di incertezza macroeconomica in seguito all'annuncio dei dazi, hanno portato a una maggiore volatilità dei mercati e a una revisione delle aspettative relative ai futuri tagli dei tassi, innescate dalla pubblicazione dei verbali della riunione del Federal Open Market Committee (FOMC) di gennaio. L'incertezza legata ai dazi ha contribuito a far aumentare i rischi di recessione sui mercati, soprattutto in un contesto caratterizzato dal rallentamento dell'economia e da una Fed che preferisce mantenere i tassi invariati piuttosto che rischiare un taglio troppo precoce.

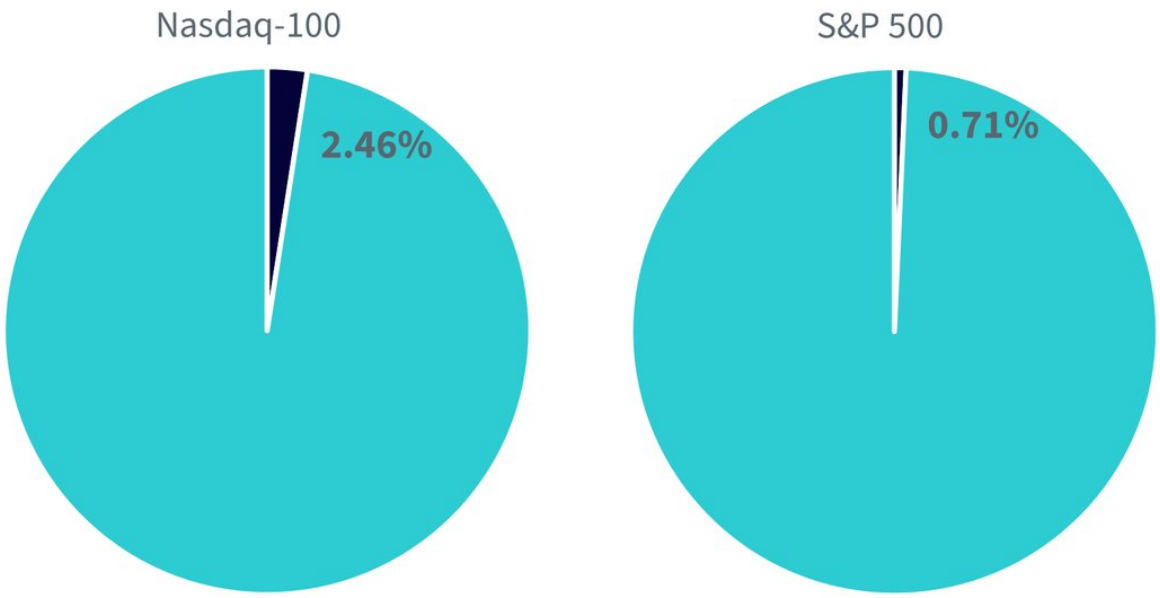
I dazi in programma hanno contribuito ad aumentare la volatilità e a ridurre la fiducia delle imprese nella loro capacità di spesa. In questo clima, le aziende valutano con maggiore cautela le prospettive a breve termine, con un conseguente rallentamento delle conclusioni delle trattative nel settore della sicurezza informatica. I dazi statunitensi potrebbero influire sulle società di sicurezza informatica anche attraverso i loro dispositivi hardware, ad esempio firewall, router sicuri, sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS). Alcune società potrebbero vendere i propri software in pacchetti che includono hardware di terzi e risultare quindi esposte a rischi derivanti dai propri partner. Le società di sicurezza informatica specializzate in software godono di una posizione migliore in questo contesto, ma potrebbero essere colpite indirettamente dai dazi. I servizi basati sul cloud si affidano all'hardware dei centri dati fisici e i fornitori di cloud pubblici potrebbero aumentare i prezzi se i loro costi salgono.

Sebbene i timori relativi ai tassi d'interesse e ai dazi potrebbero esercitare pressioni sulla spesa a breve termine, i fattori favorevoli di lungo periodo, dalla rapidità della digitalizzazione alla proliferazione dell'IA, fino all'evoluzione delle minacce geopolitiche, forniscono una base solida per investimenti sostenuti nella sicurezza informatica. Le prospettive di crescita a lungo termine del settore rimangono intatte e il mercato azionario sembra concordare, come si può dedurre dal forte rimbalzo del WisdomTree Team8 Cybersecurity UCITS Index dopo l'annuncio della sospensione di 90 giorni da parte del presidente Trump il 9 aprile, nonché dal differenziale di rendimento che la strategia ha registrato rispetto ai benchmark azionari e tecnologici più ampi nei primi tre mesi del 2025 (cfr. Figura 1).

Un satellite interessante per un core a lungo termine

Una delle principali opportunità di valore delle strategie tematiche risiede nella differenziazione che offrono rispetto alle esposizioni azionarie generali. Tale potenziale di differenziazione può variare da tema a tema. Nel caso delle società di sicurezza informatica, l'esposizione che gli investitori possono ottenere tramite benchmark azionari o tecnologici più ampi è minima, soprattutto a causa della scarsa ponderazione di tali società all'interno di questi ultimi. Ad esempio, al 30 maggio 2025, Palo Alto e CrowdStrike, due delle più grandi società per capitalizzazione di mercato specializzate nella sicurezza informatica, hanno una ponderazione nel Nasdaq-100 pari rispettivamente allo 0,79% e allo 0,68%. Se operiamo un confronto con il WisdomTree Team8 Cybersecurity UCITS Index, che attualmente include 25 società di sicurezza informatica, la sovrapposizione con il Nasdaq-100 e l'S&P 500 è rispettivamente inferiore al 2,5% e all'1% (cfr. Figura 3).

Figura 3: Sovrapposizione tra il WisdomTree Team8 Cybersecurity UCITS Index e i benchmark azionari e tecnologici più ampi



Fonte: WisdomTree, Bloomberg, MSCI, al 30 maggio 2025. Il WisdomTree Cybersecurity è rappresentato dal WisdomTree Team8 Cybersecurity UCITS Index (WTCBRUN). Il Nasdaq-100 è il NASDAQ 100 Index. L'S&P 500 è l'S&P 500 Index. La sovrapposizione dei titoli in comune rappresenta la somma di tutte le ponderazioni che si sovrappongono a quelle del WTCBRUN all'interno di un determinato indice. La sovrapposizione delle ponderazioni è calcolata prendendo la ponderazione minore di un titolo detenuto sia nel WTCBRUN che in un determinato indice. **Non è possibile investire direttamente in un indice. La performance storica non è indicativa di quella futura e qualsiasi investimento può diminuire di valore.**

Una sovrapposizione ridotta suggerisce che aggiungendo questo tipo di esposizione alla propria allocazione core a titoli tecnologici o azionari è possibile migliorare i rendimenti grazie ai vantaggi offerti dalla diversificazione. Inoltre, la resilienza della domanda relativa alla sicurezza informatica rende una strategia incentrata sulla stessa un investimento interessante nel lungo termine, da affiancare alle esposizioni core tradizionali.

[1] https://www.bbc.co.uk/news/articles/c93llkg4n51o

Important Risks Related to this Article

Informazioni importanti

Comunicazioni di marketing emesse all'interno dello Spazio economico europeo ("SEE"): Il presente documento è stato emesso e approvato da WisdomTree Ireland Limited, società autorizzata e regolamentata dalla Central Bank of Ireland.

Comunicazioni di marketing emesse in giurisdizioni non appartenenti al SEE: Il presente documento è stato emesso e approvato da WisdomTree UK Limited, società autorizzata e regolamentata dalla Financial Conduct Authority del Regno Unito.

Per fare riferimento a WisdomTree Ireland Limited e a WisdomTree UK Limited si utilizza per entrambe la denominazione "WisdomTree" (come applicabile). La nostra politica sui conflitti d'interesse e il nostro inventario sono disponibili su richiesta.

Solo per clienti professionali. Le informazioni contenute nel presente documento sono fornite a titolo meramente informativo e non costituiscono né un'offerta di vendita né una sollecitazione di un'offerta di acquisto di titoli o azioni. Il presente documento non deve essere utilizzato come base per una qualsiasi decisione d'investimento. Gli investimenti possono aumentare o diminuire di valore e si può perdere una parte o la totalità dell'importo investito. Le performance passate non sono necessariamente indicative di performance future. Qualsiasi decisione d'investimento deve essere basata sulle informazioni contenute nel Prospetto informativo di riferimento e deve essere presa dopo aver richiesto il parere di un consulente d'investimento, fiscale e legale indipendente.

L'applicazione di regolamenti e leggi fiscali può spesso portare a una serie di interpretazioni diverse. Eventuali punti di vista o opinioni espresse in questa comunicazione rappresentano le opinioni di WisdomTree e non devono essere interpretate come consulenza normativa, fiscale o legale. WisdomTree non fornisce alcuna garanzia o dichiarazione circa l'accuratezza di qualsiasi punto di vista o opinione espressa in questa comunicazione. Qualsiasi decisione di investimento dovrebbe essere basata sulle informazioni contenute nel prospetto appropriato e dopo aver richiesto una consulenza finanziaria, fiscale e legale indipendente.

Il presente documento non è, e in nessun caso deve essere interpretato come, una pubblicità o qualsiasi altro strumento di promozione di un'offerta pubblica di azioni o titoli negli Stati Uniti o in qualsiasi provincia o territorio degli Stati Uniti. Né il presente documento né alcuna copia dello stesso devono essere acquisiti, trasmessi o distribuiti (direttamente o indirettamente) negli Stati Uniti.

Benché WisdomTree si adoperi per garantire l'esattezza del contenuto del presente documento, WisdomTree non garantisce né assicura la sua esattezza o correttezza. Qualsiasi terzo fornitore di dati di cui ci si avvalga per reperire le informazioni contenute nel presente documento non rilascia alcuna garanzia o dichiarazione di sorta in relazione ai suddetti dati. Laddove WisdomTree abbia espresso dei pareri relativamente al prodotto o all'attività di mercato, si ricorda che tali pareri possono cambiare. Né WisdomTree, né alcuna consociata, né alcuno dei rispettivi funzionari, amministratori, partner o dipendenti,

accetta alcuna responsabilità per qualsiasi perdita, diretta o indiretta, derivante dall'utilizzo del presente documento o del suo contenuto.