Surperformer les indices larges en 2025 grâce à la cybersécurité

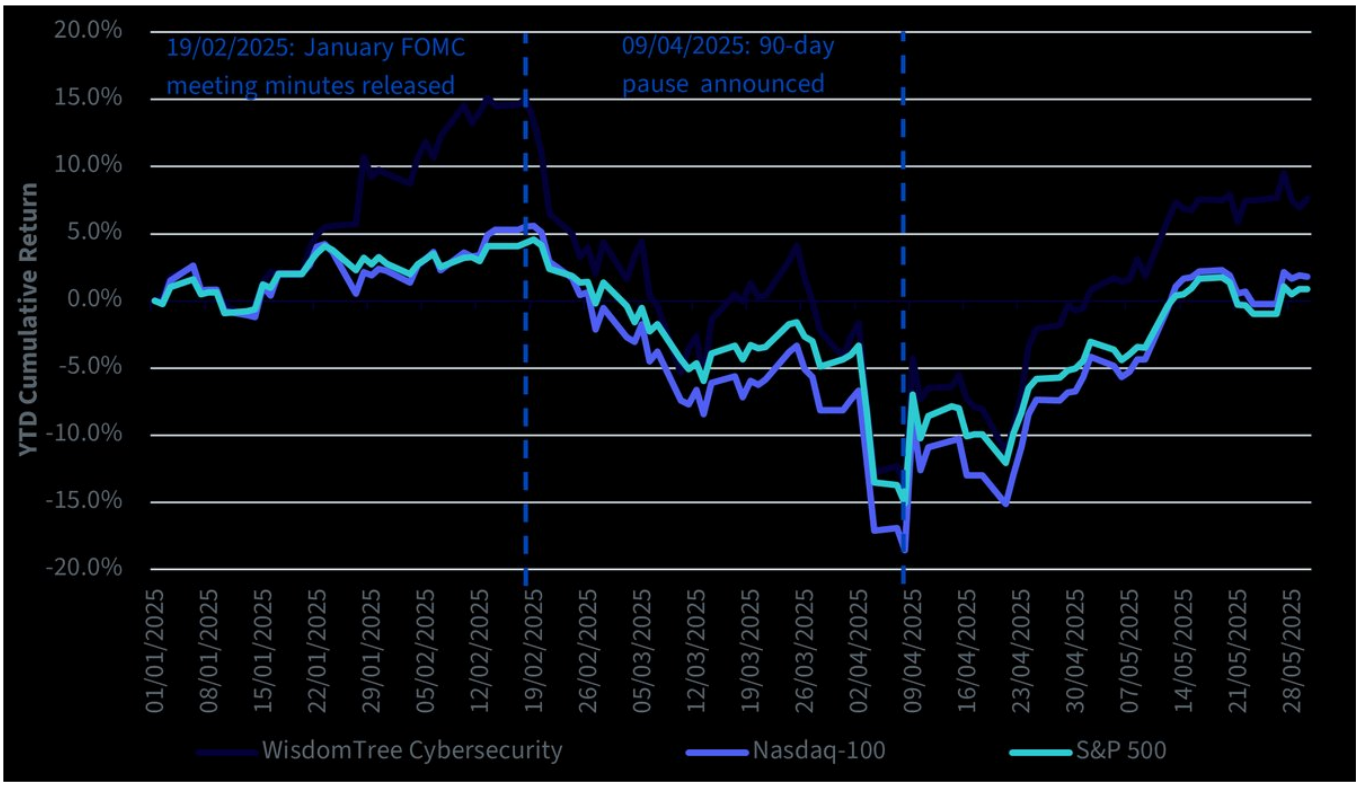
Publié le 16 juin 2025

Elvira Kuramshina
Associate Director, Quantitative Research

- Alors que le monde poursuit sa transformation digitale, la demande en matière de cybersécurité augmente en parallèle. Toutefois, parallèlement à la vague de numérisation actuelle, le potentiel de croissance de la cybersécurité se voit renforcé par une multitude de facteurs favorables.
- Alors que les préoccupations relatives aux taux d'intérêt et aux tarifs douaniers contribuent à une plus grande volatilité et à une baisse de la confiance dans les dépenses des entreprises, les vents favorables structurels offrent une base solide et durable pour les investissements dans la cybersécurité.
- Le potentiel de différenciation offert par l'indice WisdomTree Team8 Cybersecurity UCITS et la résilience de la demande en matière de cybersécurité en font un investissement à long terme convaincant, parallèlement aux expositions stratégiques traditionnelles.
- Produits associés WisdomTree Cybersecurity UCITS ETF – USD Acc En savoir plus

L'année 2025 met à rude épreuve la patience des investisseurs. De l'incertitude liée aux tarifs douaniers à l'augmentation des risques géopolitiques, en passant par la propagation rapide de l'IA, les marchés ont connu des turbulences et une volatilité importantes. Dans ce contexte difficile, l'indice WisdomTree Team8 Cybersecurity UCITS se démarque par sa surperformance depuis le début de l'année par rapport aux grands indices actions et technologiques, soulignant sa résilience malgré un environnement macroéconomique affaibli et l'évolution des priorités et des dépenses des entreprises (voir illustration 1). Dans cet article, nous analysons en détail la résilience de la demande à long terme en matière de cybersécurité, nous soulignons les vents contraires à court terme liés à l'incertitude macroéconomique et, enfin, nous abordons la manière dont une exposition ciblée à la cybersécurité peut accroître les rendements de votre portefeuille par rapport aux indices larges.

Illustration 1. L'indice cybersécurité de WisdomTree surpasse le Nasdaq-100 et le S&P 500 depuis le début de l'année.



Source : WisdomTree, Bloomberg. Au 30 mai 2025. L'indice cybersécurité de WisdomTree est représenté par l'indice WisdomTree Team8 Cybersecurity UCITS. Tous les rendements correspondent aux indices de rendement total net en USD. **Vous ne pouvez pas investir directement dans un indice. Les performances historiques ne garantissent pas les performances futures, et tout investissement est susceptible de perdre de la valeur.**

Résilience de la demande en matière de cybersécurité

Alors que le monde poursuit sa transformation digitale, la cybersécurité apparaît comme la mégatendance clé pour sécuriser notre avenir. Toutefois, parallèlement à la vague de numérisation actuelle, le potentiel de croissance de la cybersécurité se voit renforcé par une multitude de facteurs favorables :

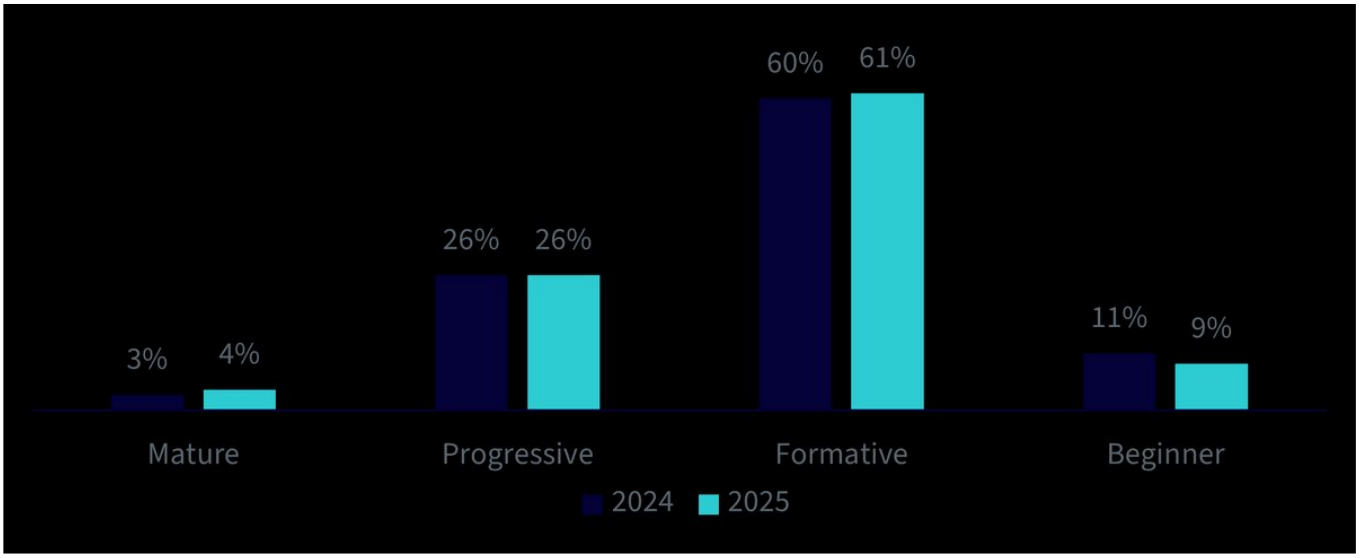
1. Redéfinition de la résilience commerciale et concurrentielle

La numérisation, déjà fortement accélérée par la pandémie mondiale, connaît un nouvel élan grâce à la révolution actuelle de l'IA. Chaque nouvelle couche d'infrastructure numérique nécessite des mesures de sécurité robustes et, à l'ère numérique moderne, la cybersécurité s'impose comme un enjeu crucial de la résilience des entreprise. Le récent incident de cybersécurité chez Marks & Spencer, l'un des plus grands distributeurs du Royaume-Uni, illustre à quel point une cyberattaque peut être paralysante et onéreuse dans le monde d'aujourd'hui. L'entreprise prévoit un impact de 300 millions de dollars sur ses bénéfices, tandis que ses activités en ligne resteront perturbées jusqu'au mois de juillet1.

Cet incident met en lumière la nécessité cruciale de disposer de solutions de cybersécurité adéquates pour toute entreprise moderne, ce qui explique la résilience de la demande malgré les difficultés économiques.

Dans le même temps, Cisco, dans son Indice Cybersecurity Readiness 2025, révèle que les entreprises ne parviennent pas à s'adapter au paysage des menaces en constante évolution : seules 30 % affichent une préparation qualifiée de « mature » ou « progressive » face aux risques actuels en matière de cybersécurité, avec une dynamique quasi inchangée depuis 2024 (voir illustration 2). Ceci démontre le potentiel de croissance des spécialistes de la cybersécurité, dans un contexte où les entreprises cherchent à accroître leur résilience concurrentielle en intensifiant leurs dépenses dans ce domaine. À titre d'exemple, les entreprises disposant de solutions de cybersécurité adéquates sont susceptibles de créer un fossé concurrentiel fondé sur la confiance et peuvent adopter en toute sécurité de nouvelles technologies pour rester compétitives.

Illustration 2. État de préparation à l'échelle mondiale face aux risques liés à la cybersécurité



Source : Indice Cisco Cybersecurity Readiness 2025. L'indice Cisco Cybersecurity Readiness 2025 évalue la capacité des entreprises à faire face aux risques actuels en matière de cybersécurité en s'appuyant sur cinq piliers : intelligence des identités, fiabilité des machines, résilience des réseaux, renforcement du cloud et fortification de l'intelligence artificielle (IA). L'évaluation se fonde sur une enquête en double aveugle menée auprès de 8 000 entreprises et leaders du secteur de la cybersécurité, sur trente marchés mondiaux, dans un large éventail d'industries du secteur privé.

2. Risques géopolitiques et dynamique politique favorable

L'augmentation simultanée des tensions géopolitiques et des cyberattaques de grande envergure maintient en outre la cybersécurité au cœur des préoccupations, non seulement pour les entreprises, mais également pour les gouvernements. L'évolution rapide du paysage des menaces, qui comprend les acteurs étatiques, a conduit à une vague de réponses réglementaires et stratégiques qui renforcent la demande à long terme de solutions de cybersécurité. Aux États-Unis, la Stratégie nationale de cybersécurité (2023) a souligné l'urgence d'adopter une approche plus intentionnelle et coordonnée en matière de cyberdéfense, ainsi que la nécessité de réaligner les mesures incitatives en vue de soutenir les investissements stratégiques à long terme dans le cyberespace. En Europe, le règlement de l'UE sur la cybersolidarité

vise à renforcer la préparation, la détection et la réponse collectives grâce à des financements relevant de l'objectif stratégique « Cybersécurité », ainsi qu'à travers des actions conjointes de préparation, de veille stratégique et de coopération transfrontalière. Parallèlement, l'OTAN se concentre davantage sur la cyberdéfense collective et adapte sa posture de défense en réponse à l'évolution rapide du paysage des menaces.

3. L'essor de l'IA générative

Depuis la sortie de ChatGPT le 30 novembre 2022, l'IA générative a chamboulé le monde. Alors que l'IA permet aux entreprises de cybersécurité de développer des capacités toujours plus innovantes, telles que l'automatisation de la détection des menaces et l'amélioration de l'analyse des données, elle crée également de nouvelles vulnérabilités et contribue à transformer le paysage des risques. Avec sa prolifération rapide et ses progrès constants, la technologie est l'un des principaux catalyseurs de la recrudescence des cyberattaques. Des outils malveillants permettant de générer des deepfakes pour l'usurpation d'identité et l'ingénierie sociale, jusqu'à l'empoisonnement des données des grands modèles de langage (LLM) et le contournement de leurs protections pour faciliter la création de logiciels malveillants, les cybercriminels exploitent l'IA pour gagner en efficacité, en rapidité et en volume dans la réalisation de leurs objectifs.

Dans le même temps, les organisations sont confrontées à des risques accrus de fuite de données en raison de l'utilisation de modèles d'IA. Dans la première édition de son « Rapport sur la sécurité de l'IA 2025 », Check Point révèle qu'une requête sur treize adressée à une IA générative comporte des données sensibles ou privées, tandis qu'une sur quatre-vingts expose ces données aux attaquants. Dans le même temps, Check Point souligne que les entreprises qui n'utilisent pas l'IA risquent de voir leurs employés se servir d'outils d'IA sans autorisation, s'exposant ainsi à de nouveaux risques. En réponse, plusieurs entreprises de cybersécurité ont d'ores et déjà commencé à proposer des solutions spécifiquement adaptées aux risques découlant de l'utilisation des LLM à des fins professionnelles. Alors que les cybermenaces alimentées par l'IA deviennent de plus en plus répandues, la demande de solutions de cybersécurité est appelée à augmenter au même rythme.

Des vents contraires macroéconomiques à court terme

Malgré une demande solide et un potentiel de croissance convaincant, les entreprises de cybersécurité ne sont pas à l'abri de turbulences macroéconomiques plus larges. En réalité, du point de vue de leur sensibilité aux taux d'intérêt, elles sont souvent assimilables à des actions technologiques à échéance longue. Cela s'explique principalement par le fait que de nombreuses entreprises de cybersécurité de premier plan connaissent une croissance rapide, et que la majeure partie de leurs flux de trésorerie prévisionnels est projetée sur le long terme. À mesure que les taux d'intérêt augmentent, ces flux de trésorerie futurs sont actualisés de manière plus importante, ce qui rend les valorisations plus sensibles aux évolutions des prévisions de taux.

L'évolution récente de la politique monétaire américaine, dans un contexte d'incertitude macroéconomique provoquée par l'annonce des nouveaux tarifs douaniers, a conduit à une volatilité accrue des marchés ainsi qu'à une réévaluation des attentes concernant les futures baisses de taux d'intérêt, qui a débuté par

la publication du compte rendu de la réunion de janvier du Comité fédéral des marchés ouverts (Federal Open Market Committee, FOMC). L'incertitude liée aux tarifs douaniers a contribué à ce que les marchés évaluent les risques de récession à la hausse, en particulier face à une économie au ralenti ainsi qu'à la volonté de la Fed de maintenir les taux stables plutôt que de risquer une baisse prématurée.

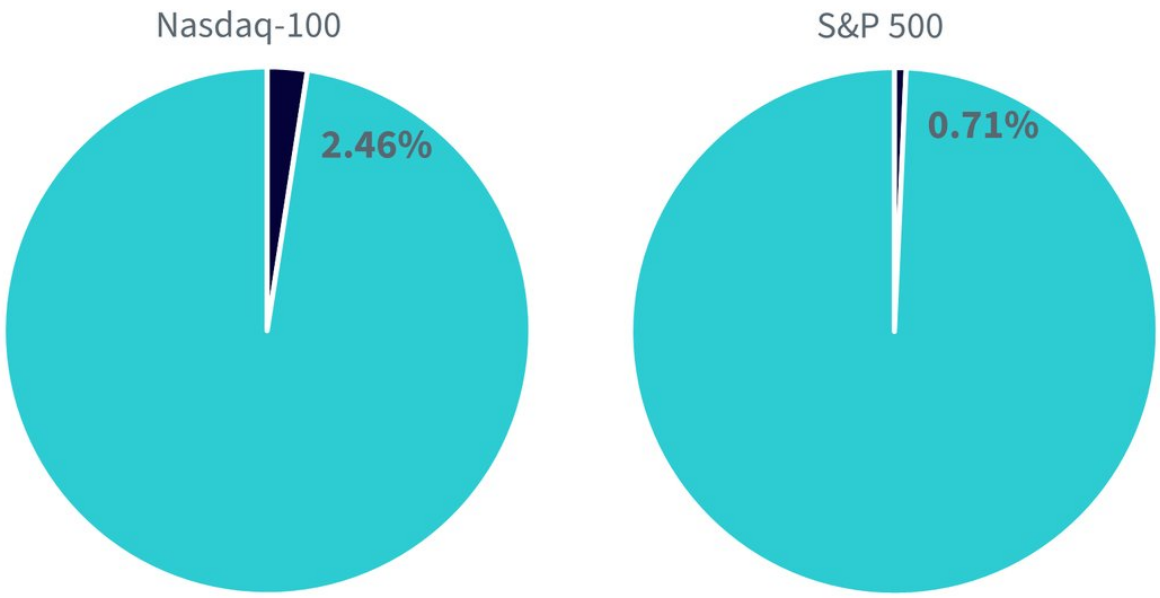
Les tarifs douaniers annoncés ont accentué la volatilité et réduit la confiance des entreprises quant à leurs dépenses. Dans ce climat, le secteur de la cybersécurité pourrait connaître un ralentissement des transactions, les entreprises évaluant les perspectives à court terme. Une autre manière dont les droits de douane américains pourraient impacter les entreprises de cybersécurité concerne leurs équipements matériels, tels que les pare-feux, les routeurs sécurisés ou les systèmes de détection et de prévention des intrusions (IDS/IPS). Certaines entreprises pourraient intégrer leur logiciel à du matériel tiers, et être impactées via leurs partenaires. Bien que les entreprises de cybersécurité axées sur les logiciels soient mieux positionnées dans cet environnement, elles peuvent également être exposées indirectement aux tarifs douaniers. Les services cloud dépendent de l'infrastructure physique des centres de données, et les prestataires de cloud public pourraient répercuter la hausse des coûts sur leurs prix.

Alors que les préoccupations en matière de taux d'intérêt et de tarifs douaniers pourraient exercer une pression sur les dépenses à court terme, les vents favorables structurels, qu'il s'agisse de l'accélération de la numérisation, de la propagation de l'IA ou de l'évolution des menaces géopolitiques, offrent une base solide et durable pour les investissements dans la cybersécurité. La perspective de croissance à long terme du secteur demeure intacte, et le marché actions semble s'y rallier. Cela se manifeste par le fort rebond de l'indice WisdomTree Team8 Cybersecurity UCITS après l'annonce d'une trêve tarifaire de 90 jours par le président Trump le 9 avril, ainsi que par la surperformance de la stratégie face aux principaux indices technologiques et actions durant le premier trimestre 2025 (voir illustration 1).

Un complément convaincant à un cœur d'investissement à long terme

L'une des principales propositions de valeur des stratégies thématiques réside dans la différenciation qu'elles offrent par rapport aux expositions larges sur les marchés actions. Ce potentiel de différenciation peut varier d'un thème à l'autre. Lorsqu'il s'agit d'entreprises de cybersécurité, l'exposition que les investisseurs peuvent obtenir sur le thème via les grands indices actions et technologiques est minime, notamment en raison de la faible pondération de ces entreprises dans les indices larges. À titre d'exemple, Palo Alto et CrowdStrike, qui figurent parmi les plus grandes entreprises de cybersécurité pure play par capitalisation boursière, ne représentent respectivement que 0,79 % et 0,68 % du Nasdaq-100 au 30 mai 2025. L'analyse du chevauchement avec l'indice WisdomTree Team8 Cybersecurity UCITS, qui comprend actuellement 25 entreprises de cybersécurité, révèle un chevauchement de moins de 2,5 % et de moins de 1 % avec le Nasdaq-100 et le S&P 500 respectivement (voir illustration 3).

Illustration 3. Chevauchement entre l'indice WisdomTree Team8 Cybersecurity UCITS et les grands indices actions et technologiques



Source : WisdomTree, Bloomberg, MSCI. Au 30 mai 2025. L'indice cybersécurité de WisdomTree est représenté par l'indice WisdomTree Team8 Cybersecurity UCITS (WTCBRUN). Le Nasdaq-100 désigne l'indice NASDAQ 100. Le S&P 500 désigne l'indice S&P 500. Le chevauchement des titres ordinaires correspond à la somme de toutes les pondérations qui se chevauchent avec l'indice WTCBRUN dans un indice donné. La pondération de chevauchement correspond à la pondération minimale d'un titre présent à la fois dans l'indice WTCBRUN et dans un autre indice donné. **Vous ne pouvez pas investir directement dans un indice. Les performances historiques ne garantissent pas les performances futures, et tout investissement est susceptible de perdre de la valeur.**

Un faible chevauchement suggère que l'ajout de ce type d'exposition à votre allocation principale en actions technologiques et en actions diversifiées pourrait améliorer les rendements grâce aux avantages de la diversification. En outre, la résilience de la demande en matière de cybersécurité fait de la stratégie cybersécurité un investissement à long terme convaincant parallèlement aux expositions stratégiques traditionnelles.

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

Important Risks Related to this Article

Informations importantes

Communications commerciales publiées dans l¼Espace économique européen (« EEE ») Ce document est publié et approuvé par WisdomTree Ireland Limited, une société autorisée et réglementée par la Central Bank of Ireland.

Communications commerciales émises dans des juridictions en dehors de l¼EEE Ce document est publié et approuvé par WisdomTree UK Limited, une société autorisée et réglementée par la Financial Conduct Authority du Royaume-Uni.

WisdomTree Ireland Limited et WisdomTree UK Limited sont toutes les deux désignées comme « WisdomTree » (le cas échéant). Notre Politique sur les conflits d¼intérêts et notre Inventaire sont disponibles sur demande.

Réservé aux clients professionnels uniquement. Les informations figurant dans ce document sont fournies à titre informatif et ne constituent pas une ore de vente, ou une sollicitation d¼ore d¼achat de titres ou d¼actions. Ce document ne doit pas être utilisé comme fondement d¼une décision d¼investissement. La valeur des investissements peut fluctuer et vous êtes susceptible de perte tout ou partie du montant investi. La performance passée ne constitue pas nécessairement une indication des performances futures. Toute décision d¼investissement doit être fondée sur les informations figurant dans le prospectus approprié et sur des conseils indépendants en matière d¼investissement, fiscaux et juridiques.

L¼application des réglementations et lois fiscales peut souvent conduire à des interprétations diérentes. Tous les points de vue ou opinions exprimés dans cette communication représentent les points de vue de WisdomTree et ne doivent pas être interprétés comme des conseils réglementaires, fiscaux ou juridiques. WisdomTree ne donne aucune garantie ou représentation quant à l'exactitude des vues ou opinions exprimées dans cette communication. Toute décision d'investissement doit être fondée sur les informations contenues dans le prospectus approprié et après avoir sollicité des conseils indépendants en matière d'investissement, fiscaux et juridiques. Ce document n¼est pas et ne doit en aucun cas être interprété comme une publicité ou une ore publique d¼actions ou de titres aux États-Unis ou dans toute province ou tout territoire des États-Unis. L¼introduction, la transmission et la distribution (directes ou indirectes) de l¼original ou d¼une copie de ce document sont interdites aux États-Unis.

Bien que WisdomTree s¼eorce d¼assurer l¼exactitude du contenu de ce document, WisdomTree ne peut en garantir l¼exactitude. Les fournisseurs de données tiers sollicités pour obtenir les informations contenues dans le présent document ne donnent aucune garantie ou représentation de quelque sorte en rapport avec ces données. Lorsque WisdomTree exprime ses propres opinions concernant le produit ou l¼activité du marché, ces opinions sont susceptibles de changer. WisdomTree, ses ailiés et leurs dirigeants, directeurs, partenaires ou employés respectifs déclinent toute responsabilité pour toute perte directe ou indirecte découlant de l¼utilisation de ce document ou de son contenu.