

La cybersécurité doit demeurer une priorité en 2023

Publié le 6 décembre 2022

Christopher Gannatti, CFA

Global Head of Research

En ce début de 4ème trimestre 2022, il semble logique de se projeter pour identifier les opportunités potentielles qu'offriront les actions thématiques. L'année 2022 a été difficile en termes de performance du cours des actions pour nombre de ces stratégies, mais si l'on se projette au-delà de la période difficile des rendements, plusieurs moteurs de la demande se profilent à l'horizon. Selon nous, la cybersécurité constitue l'un des meilleurs moteurs.

Analyse de l'Univers thématique de WisdomTree pour les 3 premiers trimestres 2022

Même en prenant du recul et en reconnaissant les difficultés de l'environnement macroéconomique pour les investissements 'growth' sur les neuf premiers mois de 2022, nous pouvons quand même examiner les secteurs dans lesquels les investisseurs ont placé leur argent au sein d'une large gamme de plus de 40 thèmes distincts. L'analyse des 5 premiers et des 5 derniers thèmes en termes de flux est assez révélatrice1:

Top 5 des thématiques préférées des investisseurs européens dans les ETFs en termes de flux sur les 9 premiers mois de 2022

- Production d'énergie durable : USD 1 525 millions
- Égalité et diversité : USD 883 millions
- Cybersécurité : USD 761 millions
- Agriculture : USD 682 millions
- Semi-conducteurs : USD 277 millions

Les 5 thématiques les moins populaires auprès des investisseurs européens dans les ETF par flux sur les 9 premiers mois de 2022

- Robotique et automatisation : - USD 244 millions
- Plateformes : - USD 162 millions
- Santé numérique : - USD 156 millions
- Gestion durable des ressources : - USD 149 millions
- Vieillesse de la population : - USD 135 millions

Ainsi, et ce, même face à des performances très difficiles, la cybersécurité a été un des thèmes qui a le plus attiré les nouveaux investissements dans l'univers thématique de WisdomTree, qui compte plus de 40 thèmes distincts. Les cyberattaques et les incidents ne faiblissent pas

En 2021, l'attaque informatique par ransomware de Colonial Pipelines a eu un fort impact dans l'Est des États-Unis. Les hôpitaux ont été une autre cible majeure durant la pandémie. Le gestionnaire d'hôpitaux CommonSpirit Health a annoncé avoir été victime d'une cyberattaque en octobre 2022.

Le Bureau fédéral d'investigation (FBI) a tendance à répondre à de nombreuses cyberattaques. Son Centre de plainte contre les délits sur Internet (« Internet Crime Complaint Centre ») a indiqué avoir reçu un nombre record de 847 376 plaintes en 2021, avec des pertes potentielles estimées à plus de 6,9 milliards de dollars³.

Les responsables informatiques se déclarent prêts à augmenter leurs dépenses

Le cabinet de conseil Gartner publie des études importantes sur des sujets liés aux technologies de l'information. À la mi-octobre 2022, cette société a publié certaines conclusions issues de son enquête annuelle réalisée auprès de 2 200 responsables informatiques (« annual CIO survey »). 66 % des personnes interrogées ont déclaré envisager d'augmenter leurs investissements dans la cybersécurité⁴.

En réalité, la hausse des investissements dans la cybersécurité dépasse ceux dans 'l'intelligence économique et l'analyse', dans lesquelles 55 % des interrogés ont affirmé qu'ils augmenteraient leurs investissements⁵.

D'après Gartner, la taille totale du marché des dépenses de sécurité des informations et de gestion du risque sera supérieure à 188 milliards de dollars en 2023, ce qui devrait représenter une augmentation de plus de 11 % par rapport à 2022⁶.

Quelle part du budget est affectée à la cybersécurité ?

Il s'agit d'une question difficile. Il est toujours préférable de consulter directement les responsables informatiques afin de voir comment ils abordent les défis auxquels ils sont confrontés. Le responsable informatique de l'entreprise de produits alimentaires conditionnés Kellogg Co. a indiqué que la sécurité représente environ 15 % du total des dépenses de son entreprise dans les informations et les technologies⁷.

Ce niveau se situe probablement dans la fourchette haute des grandes entreprises, mais il dépend beaucoup du secteur. Les sociétés de services financiers engagent généralement des investissements conséquents dans la cybersécurité, contrairement aux entreprises de services publics et d'infrastructures essentielles, qui devraient dépenser davantage dans ce domaine, selon nous.

Le secteur de la cybersécurité est victime d'une pénurie de main-d'œuvre

La pénurie de talents dans le domaine de la cybersécurité aurait augmenté de 26,2 % au cours de l'année écoulée et il pourrait y avoir environ 3,4 millions d'emplois non pourvus dans le monde. La répartition

régionale indique une pénurie particulièrement conséquente dans la région d'Asie Pacifique. L'équivalent du manque de main d'œuvre par zone géographique est le suivant⁸:

- Amérique du Nord : 436 080
- Amérique latine : 515 879
- Europe, Moyen Orient et Afrique : 317 050
- Asie-Pacifique : 2 163 468

Les entreprises envisagent toutes les possibilités disponibles pour parvenir à pourvoir ces postes. Certaines d'entre elles investissent dans des programmes de formation à certaines compétences nécessaires et à destination des employés qui ont moins d'expérience. D'autres solutions peuvent inclure une meilleure utilisation des logiciels, de l'apprentissage automatique et de l'intelligence artificielle. S'il n'existe pas de solution simple et rapide, la cybersécurité est un secteur d'emploi en forte croissance et dont le rythme de croissance pourrait perdurer durant les années 2020.

La consolidation est une tendance clé parmi les entreprises de cybersécurité

En analysant les activités des entreprises de cybersécurité, nous avons constaté que les clients souhaitaient disposer de moins de programmes individuels. Même si chaque entreprise est unique, certains rapports ont indiqué qu'un responsable informatique peut parfois utiliser près de 70 outils de cybersécurité différents⁹.

Les clients souhaitent des solutions de haut niveau au sein des différents domaines techniques (à l'image de la protection des 'End points', de la sécurité du cloud, de la sécurité des emails, etc.), mais il existe un risque associé au fonctionnement simultané d'un grand nombre d'outils.

Durant les 9 premiers mois de l'année 2022, nous avons constaté des opérations de fusions-acquisitions pour un montant d'environ 111,5 milliards de dollars dans le secteur de la cybersécurité, contre 80,9 milliards de dollars en 2021, soit une accélération des opérations. Le chiffre de l'année 2022 correspond à 203 transactions individuelles alors que le chiffre de 2021 correspondait à 293 opérations individuelles¹⁰.

Quiconque s'intéresse au secteur de la cybersécurité a été témoin de l'activité de Thoma Bravo et Vista Equity Partners en 2022. Thoma Bravo a annoncé et conclu le rachat de ForgeRock (USD 2,3 milliards), Ping Identity Holding Corp. (USD 2,8 milliards) et SailPoint (USD 6,9 milliards) en 2022. Les grandes entreprises de cloud computing disposent généralement de liquidités et peuvent également conclure des transactions¹¹ :

- L'achat de Mandiant par Google Cloud pour un montant d'environ 5,4 milliards de dollars a fait l'objet de nombreux articles et reportages
- D'une manière plus discrète, Microsoft a acquis la société d'études spécialisée dans les menaces informatiques Miburo et la société de cybersécurité RiskIQ Inc.

L'expansion continue du nombre de cyberattaques signifie que la demande d'innovation en cybersécurité devrait se poursuivre activement. Mais reste à savoir si les clients obtiendront ces services auprès de

fournisseurs individuels, de plateformes de cyber-sécurité plus importantes que celles mises à disposition par des acteurs du capital-investissement, ou par le biais de fournisseurs de cloud computing avec qui ils sont en relation.

Conclusion : un thème intéressant pour la suite du cycle macroéconomique

Le cycle macroéconomique actuel, qui voit la plupart des grandes banques centrales se concentrer sur l'inflation et relever sensiblement les taux directeurs à chaque réunion, ne permet pas aux cours des actions des entreprises de cybersécurité d'augmenter durablement. Un grand nombre des entreprises dont l'activité nous semblent être la plus passionnante sont très jeunes et se développent assez vite, mais elles n'en sont pas encore au stade de générer de robustes bénéfices.

Les entreprises de croissance visant à développer leurs activités et préférant réinvestir plutôt que générer des bénéfices nets positifs n'ont pas été favorisées dans un environnement marqué par une inflation élevée et une hausse des taux d'intérêt. Toutefois, nous tenons à rappeler aux investisseurs que la Réserve fédérale américaine ne relèvera pas ses taux de 75 points de base à l'infini, réunion après réunion, et que l'inflation finira par diminuer tout comme lors des cycles précédents. Dans la mesure où de nombreuses sociétés de cybersécurité spécialisées dans les logiciels affichent des valorisations inférieures à 2021 et où la cybersécurité est un impératif essentiel au sein d'une entreprise, ces sociétés pourraient être idéalement positionnées le moment venu. Même si l'on ne sait jamais exactement quelles entreprises ou quels services produiront les meilleurs résultats, il sera important de se protéger contre les attaques informatiques, les piratages et les risques.

1 Sources : WisdomTree, Morningstar et Bloomberg. L'ensemble des données sont au 30 septembre 2022 et reposent sur la classification interne des fonds thématiques de WisdomTree. Au 30 septembre 2022, cette classification couvrait 42 thèmes distincts.

2 Source : Steven Rosenbush. « Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate. » Wall Street Journal. Le 17 octobre 2022.

3 Source : M. Rosenbush, le 17 octobre 2022.

4 Source : M. Rosenbush, le 17 octobre 2022.

5 Source : M. Rosenbush, le 17 octobre 2022.

6 Source : M. Rosenbush, le 17 octobre 2022.

7 Source : M. Rosenbush, le 17 octobre 2022.

8 Source : « (ISC)2 Cybersecurity Workforce Study. » 2022. <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>

9 Source : James Rundle. « Cyber M&A Expected to Remain Robust Into 2023. » Wall Street Journal. Le 19 octobre 2022.

10 Source : M. Rundle, le 19 octobre 2022.

11 Source : M. Rundle, le 19 octobre 2022.

Blogs associés

+ Dans un marché morose pour les valeurs de croissance, la cybersécurité pourrait générer de bons résultats futurs

Important Risks Related to this Article

Informations importantes

Communications commerciales publiées dans l'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 l'EEE 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 d'intérêts 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 d'ore d'achat de titres ou d'actions. Ce document ne doit pas être utilisé comme fondement d'une décision d'investissement. 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 d'investissement doit être fondée sur les informations figurant dans le prospectus approprié et sur des conseils indépendants en matière d'investissement, fiscaux et juridiques.

L'application 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 n'est pas et ne doit en aucun cas être interprété comme une publicité ou une ore publique d'actions ou de titres aux États-Unis ou dans toute province ou tout territoire des États-Unis. L'introduction, la transmission et la distribution (directes ou indirectes) de l'original ou d'une copie de ce document sont interdites aux États-Unis.

Bien que WisdomTree s'efforce d'assurer l'exactitude du contenu de ce document, WisdomTree ne peut en garantir l'exactitude. 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 l'activité du marché, ces opinions sont susceptibles de changer. WisdomTree, ses alliés et leurs dirigeants, directeurs, partenaires ou employés respectifs déclinent toute responsabilité pour toute perte directe ou indirecte découlant de l'utilisation de ce document ou de son contenu.