Avez-vous été témoin d’un ‘excès de logiciels’ dans le domaine de la cybersécurité ?

Publié le 12 octobre 2022

Christopher Gannatti, CFA
Global Head of Research

Il faut bien reconnaître que nos lecteurs sont diverses et qu’ils se composent probablement de chefs d’entreprises, de salariés de grandes groupes, d’employés de petites entreprises et même peut-être de retraités ou de personnes entre deux emplois.

Quelle que soit votre situation, avec combien de nombreux outils différents de cybersécurité avez-vous été en interaction ? Un gestionnaire de mots de passe ? Une interface unique d’authentification ? Un outil spécialisé dans les emails ? Un autre outil spécialisé dans l’accès à une infrastructure d’informatique dans le cloud ?

Le fait est que plus vous vous y connaissez en cybersécurité, plus vous êtes conscient de l’existence d’un grand nombre de fournisseurs spécialisés dans différentes catégories de protection. Le terme ‘tool sprawl’ a été utilisé pour décrire le panorama de la cybersécurité en 2022, même s’il fournit un portrait informatif1.

Combien d’outils les clients utilisent-ils ?

Les entreprises gèrent parfois des portefeuilles de 60 à 80 outils. Au maximum, certains en utilisent jusqu’à 1402. Imaginez le temps qu’il faut pour gérer l’ensemble de ces logiciels durant une activité normale.

L’une des raisons pour lesquelles l’environnement actuel est caractérisé par un si grand nombre d’outils tient à l’évolution du poste de chef de la sécurité informatique. Il y a 10 ans, un bon chef de la sécurité informatique se définissait comme quelqu’un qui achetait et déployait des logiciels. En 2022, cette fonction est beaucoup plus une priorité essentielle pour le conseil d’administration et l’équipe de direction. Aujourd’hui, un bon chef de la sécurité informatique est évalué sur la base de ses résultats plutôt que sur le déploiement d’outils3.

Une enquête réalisée par Gartner a montré que 88 % des Conseils d’administration considéraient la cybersécurité comme un ‘risque opérationnel’ plutôt que comme un ‘risque technologique4.’

Bien entendu, la surface d’attaque en 2022 s'est également fortement étendue et il est fréquent que les entreprises soient créées sur la base de nouvelles techniques d’intelligence artificielle et d’apprentissage automatique ou machine learning.

Un décollage des transactions dès 2022

Jusqu’au 18 août 2022, les fonds de capital-investissement et leurs entreprises en portefeuille ont financé 162 opérations dans la cybersécurité à l’échelle mondiale pour un montant évalué à 34,9 milliards de

dollars. Si ce rythme se poursuit, il pourrait dépasser les 36,4 milliards de dollars atteints en 2021 pour un total de 308 transactions5.

Un facteur : les valorisations. L'année 2020 et la plupart de l'année 2021 ont été témoins du plus grand nombre de cotations en bourse de sociétés spécialisées dans la cybersécurité. Nombre d'entre elles étaient spécialisées dans le cloud et enregistrent une expansion exceptionnelle de leurs multiples et donc de leurs valorisations. Leur croissance a été soutenue, mais leurs cours de bourse n'étaient pas bon marché dans un environnement où le coût du capital a été très faible pendant très longtemps.

Avec la hausse de l'inflation et le changement de politique monétaire de nombreuses banques centrales qui a fait suite à des mesures expansionnistes de soutien à la croissance, nombre de ces entreprises ont enregistré une forte compression de leurs multiples. De ce fait, les acteurs du capital-investissement désireux de constituer un portefeuille consolidé d'entreprises ont sélectionné les plus attractives à des cours sensiblement inférieurs.

Thoma Bravo est l'un de ces acteurs plutôt actifs. Sur le seul segment de l'identification, Thoma a acquis Ping Identity pour un montant de 2,8 milliards de dollars et SailPoint pour 6,9 milliards6.

La consolidation est une envie profonde de la clientèle, probablement en réponse à l'« excès de logiciels » mentionné précédemment. Le marché a l'impression que le nombre d'entreprises du secteur est peut-être excessif. Il ne s'agit plus non seulement de se contenter de davantage d'innovation, mais également de construire des plateformes intégrées afin que les clients obtiennent plus de services auprès d'un seul fournisseur.

Option3 est un exemple d'entreprise qui est passé du financement de nouvelles entreprises à l'acquisition d'entreprises de taille intermédiaire en dernière phase dans le cadre de stratégies « buy-and-build ». Ce groupe envisage de lever 250 millions de dollars pour constituer un fonds LBO dédié à une stratégie d'acquisition de plateformes7.

Les sociétés de capital-investissement sont attirées pour de nombreuses raisons par les entreprises spécialisées dans la cybersécurité, et il convient de noter qu'elles ont enregistré des taux d'attrition inférieurs à ceux d'autres éditeurs de logiciels en tant que service (« Software-as-a-Service » ou SaaS). En outre, elles ont généralement généré des marges élevées.

Qu'en est-il du ralentissement économique ?

Comme c'est le cas dans de nombreux domaines, les comparaisons historiques ne peuvent que nous en apprendre davantage. En prenant le cas de la cybersécurité en 2007-2009, période englobant la « Grande Récession », la situation était totalement différente. Les budgets de cybersécurité sont très différents en 2022 qu'ils ne l'étaient en 2007 avant un ralentissement économique significatif8.

Il ne faut pas chercher très loin pour trouver des déclarations d'experts qui affirment que même si les dépenses dans la cybersécurité peuvent pâtir d'un ralentissement économique, il est très probable qu'elles ne seront pas autant impactées que d'autres domaines. De nombreuses dépenses sont exigées par la

réglementation ou sont considérées comme des paris sur l'exploitation continue des entreprises, ce qui les rend beaucoup plus difficiles à réduire.

Dans le même temps, les autorités de tutelle renforcent leurs cadres législatifs. La commission américaine des valeurs boursières (« Securities and Exchange Commission » ou SEC) aux États-Unis a exploré une règle qui imposerait la communication d'un 'incidence majeur de cybersécurité' dans un document public. Cette divulgation devrait également être effectuée assez rapidement après l'évènement, ce qui est peut-être une réponse à certains types d'attaques et de violations, à l'image de celles dont a été victime SolarWinds, où des mois après l'attaque l'ampleur des dommages potentiels ne faisait que progresser9.

Même si les autorités de tutelle n'imposent pas de dépenses accrues dans la cybersécurité, leur adoption de certains types de règles aura probablement un impact.

Conclusion : une mégatendance profitable en toute saison ?

Norges Bank Investment Management, le premier fonds souverain au monde dont les encours s'élèvent à 1 200 milliards de dollars, a récemment indiqué que la cybersécurité était leur principale préoccupation actuelle, affirmant que son institution faisait face à une moyenne de 3 attaques sérieuses par jour. Le fonds a enregistré environ 100 000 attaques par an et en classe environ 1 000 dans la catégorie des attaques sérieuses10.

Les entreprises exerçant dans le secteur financier sont de plus en plus visées et celles exerçant dans les pays nordiques ressentent assez concrètement leur proximité avec la Russie durant le conflit en Ukraine.

Si de nombreux thèmes d'investissement peuvent être quelque peu discrétionnaires ou en retard dans un contexte marqué par un ralentissement de l'économie, la cybersécurité fait exception. Même si nous ne connaissons peut-être pas les entreprises ou les services qui enregistreront la plus forte croissance à l'avenir, il n'est pas souhaitable de faire machine arrière dans le domaine de la sécurité.

1 Source : Kyle Alspach. « Thanks to the economy, cybersecurity consolidation is coming. CISOs are more than ready. » Protocol. Le 17 juin 2022.

2 Source : M. Alspach, le 17 juin 2022.

3 Source : M. Alspach, le 17 juin 2022.

4 Source : « Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as a Business Risk. » Gartner. Communiqué de presse. Le 18 novembre 2021.

5 Source : Madeline Shi. « PE dealmaking thrives in cybersecurity sector. » Pitchbook. Le 23 août 2022.

6 Source : Mme Shi, 23 août 2022.

7 Source : Mme Shi, 23 août 2022.

8 Source : Kyle Alspach. « Cybersecurity spending isn't recession-proof. But it's pretty close. » Protocol. Le 6 juin 2022.

9 Source : Kyle Alspach. « ’Game-changer’: SEC rules on cyber disclosure would boost security planning, spending. » VentureBeat. Le 10 mars 2022.

10 Source : Adrienne Klasa et Robin Wigglesworth Financial Times. Le 22 août 2022..

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.