



Maîtriser les cyber- risques et accélérer les opérations de fusions & acquisitions dans la finance

Introduction

La plateforme cloud-native de Zscaler est un hub d'interconnexion qui optimise l'expérience et la prise en charge des utilisateurs, simplifie les déploiements et l'opérationnel et protège les ressources contre les cybermenaces. Avec ces avantages, les opérations de fusions, acquisitions et cessions (M&A/D pour Mergers, Acquisitions and Divestitures) d'entreprise sont accélérées dans un contexte de confiance.

Défis des M&A/D dans le secteur des services financiers

Le secteur bancaire, des services financiers et des assurances (BFSI – banking, financial services and insurance) enregistre des évolutions de grande ampleur qui perturbent ses modèles économiques et, dans certains cas, vont jusqu'à le mettre en péril. L'atonie des taux d'intérêt, le contexte et les incertitudes en matière de politique monétaire, associés à des changements massifs induits par la transformation digitale (finance décentralisée et FinTech notamment), ont incité les entreprises du secteur BFSI à privilégier des stratégies de croissance externe, en particulier dans les cas de carences en compétences technologiques.

Les Fintechs dotées de modèles économiques matures sont de plus en plus actives dans les transactions. Dans le secteur BFSI, Huit domaines sont à prendre en compte pour les opérations de M&A/D :

- 1.** Le services bancaires numériques (par exemple, le rachat d'EVEN par MoneyLion pour 440 millions de dollars)
- 2.** Les paiements (par exemple, l'acquisition de nets par Mastercard pour 3,2 milliards de dollars)
- 3.** Le modèle de rachat immédiat avec règlement ultérieur (par exemple, l'acquisition d'Afterpay par Square pour 29 milliards de dollars)
- 4.** Les prêts (par exemple, l'acquisition de Truebill par Rocket Companies pour 1,3 milliard de dollars)
- 5.** La gestion de patrimoine (par exemple, l'acquisition de Nutmeg par JPMorgan Chase)
- 6.** Les assurances (par exemple, la prise de contrôle de Metromile par Lemonade pour 500 millions de dollars)
- 7.** Les plateformes Fintech (par exemple, Visa qui s'empare de Tink pour 2,2 milliards de dollars)
- 8.** La finance décentralisée (par exemple, le rachat de Blockrize par Gemini)
- 9.** La consolidation des banques régionales (par exemple, l'acquisition de First Midwest par Old National Bank pour 2,5 milliards de dollars)

Les raisons qui sous-tendent les transactions ci-dessus sont les suivantes :

- 1.** Un acteur majeur des BFSI qui acquiert une Fintech pour s'emparer des capacités de sa plateforme technologique (algorithme propriétaire, modèles de data science...)
- 2.** Une Fintech en pleine croissance qui s'empare d'une autre Fintech pour consolider sa position de leader

Pour que l'activité de fusion et d'acquisition aboutissent aux résultats escomptés, les négociateurs et les décideurs doivent aborder de manière proactive les domaines susceptibles de grever la création de valeur et les synergies escomptées.

Déséquilibre du stack technologique.

Les acteurs de la BFSI ont développé un mix complexe de technologies au cours des deux dernières décennies, ce qui a abouti une dette technique importante. De nombreuses entreprises ont adopté des technologies digitales sans se soucier de cette dette technique et fonctionnelle qui s'est amplifiée au fil du temps. Cette réalité peut générer des risques majeurs lors des fusions et acquisitions, compte tenu de la difficulté à évaluer la posture de risque de l'entreprise rachetée. En conséquence, les entreprises échouent trop souvent à concrétiser les synergies anticipées en matière de revenus et de coûts.

Les politiques de sécurité de l'information des grandes entreprises, établies pour des architectures de sécurité traditionnelles basées sur le périmètre du réseau, sont susceptibles d'être hors de propos pour les Fintechs qui sont nées dans l'ère du cloud. Par exemple, une institution financière nord-américaine majeure disposant d'une architecture de sécurité périmétrique (pare-feu et VPN) a eu du mal à intégrer la plateforme technologique cloud native issue de ses acquisitions de Fintech, ce qui a abouti à une expérience utilisateur médiocre.

Menaces de cybersécurité et de vulnérabilité des données :

Des problématiques de cybersécurité et de vulnérabilité des données surviennent souvent après l'annonce d'une opération de croissance externe. En effet, les acteurs malveillants cherchent à tirer profit de cette période incertaine de transition, au cours de laquelle les collaborateurs sont plus vulnérables. Pour les acteurs de la BFSI, la nécessité de sécuriser rapidement les données réglementées, les processus, ainsi que les écosystèmes des sites et des partenaires est primordiale pour pérenniser la conformité et éviter les mauvaises surprises. De plus, l'absence d'un processus de due diligence rigoureux pour comprendre la posture de risque des entreprises acquises peut donner lieu à un échec réglementaire. Par exemple, PayPal a dû suspendre les services de TIO Networks neuf mois après son

acquisition en raison d'une faille de sécurité massive qui n'a pas été détectée et signalée à temps.

Selon un rapport publié par Kroll, 13 % de toutes les cyberattaques (ransomware, ingénierie sociale et usurpation d'identité par email) visent le secteur BFSI.

Zscaler permet de sécuriser et d'accélérer les opérations de fusions & acquisitions

Zscaler réinvente les processus d'intégration suite à des fusions, acquisitions et cessions, sur la base du concept d'un hub Zero Trust, proposé en tant que service par une plateforme 100 % cloud. Zscaler Zero Trust Exchange connecte les utilisateurs de manière sécurisée aux systèmes, applications, dispositifs et entre eux, sans aucun lien avec le réseau de l'entreprise acheteuse ou rachetée. La plateforme offre un accès instantané aux données et garantit leur disponibilité, tout en protégeant le réseau de l'entreprise contre les cyber-risques et menaces potentiels. Il en résulte une sandbox évolutive, sécurisée et transparente, réutilisable à l'infini pour mener à bien les intégrations.

Un time-to-value en quelques semaines plutôt qu'en mois ou trimestres

Zscaler simplifie le processus d'intégration grâce à sa plateforme Zero Trust Exchange fournie depuis le cloud, permettant de simplifier quasi instantanément les architectures réseau et de normaliser la sécurité sur l'ensemble de l'environnement. Les entreprises qui s'adossent à Zscaler peuvent procéder aux intégrations à leur rythme. Elles ne sont pas obligées de tout intégrer par défaut et ne sont plus contraintes par ces facteurs de temps, de performances, de coût et d'expérience qui résultent généralement de la complexité technologique associée aux fusions-acquisitions. Le modèle de fourniture SaaS de Trust Exchange concrétise un réseau et une sécurité durables dès le premier jour. Entièrement opérationnel en quelques jours, Zscaler lève les obstacles à l'action, ce qui permet aux entreprises de concrétiser plus rapidement les synergies.

Maîtriser et contrôler les risques via une politique de sécurité commune.

La plateforme de Zscaler protège activement l'entreprise contre les cybermenaces connues et en évolution, tout en assurant une gestion des risques internes. Puisque l'intégralité du trafic transite via notre plateforme, les entreprises peuvent se concentrer sur la protection de leur trafic plutôt que sur la sécurité de leur périmètre. Zscaler offre une visibilité et un audit détaillés de tous les accès sur le périmètre organisationnel, au sein d'un plan de contrôle unique, tout en identifiant et en déjouant toutes les menaces issues du réseau.

Simplifier l'intégration et optimiser les coûts en administrant et non en concevant.

La plateforme permet aux opérationnels informatiques et de la sécurité de connecter de manière sécurisée n'importe quel appareil, application ou utilisateur, peu importe sa localisation ou la destination de son trafic. Tous les accès sont accordés presque sans effort. Grâce à des politiques orientées métier,

les entreprises contrôlent, connectent et auditent en toute sécurité les accès aux applications, aux utilisateurs et aux instances, sans recourir à un réseau privé ou à un SD-WAN. De plus, les entreprises exploitent la puissance d'Internet et du plus grand hub d'échange de données sécurisé au monde pour acheminer leur trafic et se dimensionner à la demande, en fonction de leur croissance et de leurs acquisitions, ou selon un modèle basé sur l'utilisateur/la consommation. Il n'y a aucune limite matérielle ni de possibilité de gestion autonome, non contrôlée.

Doper l'agilité et la flexibilité de l'entreprise

Parce que Zscaler élimine nombre d'opérations d'intégration technique complexes et chronophages, la plateforme transforme les transactions de fusion et d'acquisition en des processus reproductibles. Zscaler simplifie l'intégration en permettant aux administrateurs de sélectionner les systèmes nécessaires et peut aider à dissocier les ressources associées à une cession sans recourir à un clonage.

Comment Zscaler Zero Trust Exchange accélère en toute sécurité les transactions M&A/D

Zero Trust Exchange, clé de voûte de la plateforme de Zscaler, permet aux entreprises d'accélérer leur transformation digitale en toute sécurité. Zero Trust Exchange élargit les environnements informatiques afin que les collaborateurs puissent travailler de l'endroit de leur choix, tout en bénéficiant d'une sécurité totale. La solution permet une plus large connectivité et dissocie la sécurité du réseau.

Simplifier les transformations du réseau Exchange migre d'une topologie en étoile vers un modèle direct-to-cloud. Cette approche moderne et simple élimine la plupart des difficultés liées aux intégrations réseau, au matériel et à l'espace d'adressage. Elle offre un plan de contrôle unique pour tous les modèles cloud (hybride, multicloud, multi-entité, multi-VPC) et permet un accès direct aux applications, où qu'elles soient hébergées.

Transformer et moderniser la sécurité L'approche périmétrique traditionnelle, cloisonnée, est progressivement abandonnée au profit du modèle Zero Trust. Celui-ci offre une connexion sécurisée et directe qui réduit les vulnérabilités potentielles liées au stockage et au transfert de données (dans les SaaS et clouds publics) et s'applique à presque tous les profils de menaces de sécurité. Avec Zscaler, les menaces peuvent être restreintes dans leur capacité à se déplacer latéralement, tandis que l'évolutivité de la plateforme permet de réagir aux menaces nouvelles et évolutives en temps quasi réel.

Favoriser la mobilité des collaborateurs. Les collaborateurs sont nomades et déconnectés des espaces physiques. Zero Trust Exchange facilite cette mobilité en fournissant aux utilisateurs un accès basé sur des politiques, où qu'ils se trouvent. L'époque du tunnelling au sein des réseaux est révolue tandis que les problématiques sont résolues de manière proactive. La plateforme peut évoluer pour répondre aux nouvelles demandes des utilisateurs, quelles que soient leur localisation et leur méthode d'accès à Internet.

Zscaler, un vecteur moderne d'intégration

La capacité immédiate de partager des processus et des données de manière transparente et depuis n'importe où constitue une capacité différenciatrice que Zscaler apporte aux opérations de fusions et acquisitions dans le secteur BFSI. La simplicité de Zscaler permet de réaliser des intégrations beaucoup plus rapidement et avec un minimum de perturbations pour les utilisateurs. Zscaler permet aux entreprises de démarrer rapidement des activités génératrices de valeur tout en augmentant le volume des transactions issues des opérations de croissance externe. Contactez-nous dès aujourd'hui pour une [démonstration](#).



À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 160 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, constitue la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur zscaler.com/fr ou suivez-nous sur Twitter @zscaler.