Rapport spécial

Juin 2023

Le SASE permet un réseau Zero Trust, améliore l'agilité de l'entreprise, réduit les coûts et rationalise les transformations numériques

Commandé par

verizon

S&P Global
Market Intelligence

Table des matières

Table des matières

Résumé

Un changement radical bouleverse les organisations et leur façon de sécuriser leurs périmètres réseau, leurs utilisateurs, leurs applications et leurs données. Les approches précédentes, basées sur des silos discrets de contrôles de réseau et de sécurité, avec un accès à distance fourni via des réseaux privés virtuels (VPN), sont rapidement remplacées par des architectures de SASE (Secure Access Service Edge) et de ZTNA (Zero Trust Network Access). Ce document résume les facteurs d'entreprise du SASE, les critères de prise de décision, les modalités d'achat, les approches de déploiement, la valeur commerciale et les données d'expérience grâce à des données qualitatives issues d'entretiens approfondis et d'un forum de discussion virtuel de dirigeants, combinés à des données quantitatives issues de la recherche de S&P Global Market Intelligence. Veuillez noter que le présent document se concentre principalement sur le SASE, car les méthodologies du ZTNA sont déployées parallèlement et en fonction du SASE.

Réussite

Commençons par l'étude d'un cas de mise en œuvre de SASE réussi, partagé par l'un des participants à l'étude. Nous avons mené un entretien approfondi avec le directeur de la technologie (Chief Technology Officer, CTO) d'une grande organisation de services britannique qui gère l'éducation, les routes et les transports, les bibliothèques, la santé, le recrutement et la sécurité publique pour près d'un million de personnes. L'expérience de cette organisation fournit un aperçu utile d'un parcours SASE.

Les principaux moteurs de cette organisation étaient les suivants :

- Prise en charge du travail à distance. Ce qui a commencé par un changement rapide pendant la pandémie de COVID-19 se poursuit aujourd'hui.
- Réduction des coûts. L'organisation a progressivement éliminé un fournisseur de services réseau traditionnel qui n'était plus nécessaire après le SASE, économisant ainsi entre 500 000 £ et 1 000 000 £ par an.
- Flexibilité croissante. Avant le SASE, lorsque l'organisation ouvrait de nouveaux bureaux, elle devait établir des connexions réseau point à point sécurisées, généralement via VPN, avant que les employés puissent commencer à travailler, un processus qui pouvait prendre des semaines ou des mois. Depuis la mise en œuvre du SASE, seul un service Internet de base via Wi-Fi est requis, ce qui permet une utilisation presque immédiate des nouvelles installations.

« Le SASE est un catalyseur. Il permet à nos employés, où qu'ils soient, de se connecter au Wi-Fi et de travailler, tout simplement. C'est important, surtout lorsque des employés doivent entrer chez les gens, se retrouvent en première ligne dans un hôpital ou travaillent avec la police et les pompiers. Le SASE a également entraîné une réduction de 30 % des appels d'assistance et nous pensons que d'ici la fin de l'année, elle atteindra 50 %. »

– CTO, services, de 5 001 à 10 000 employés, Royaume-Uni

Introduction au SASE

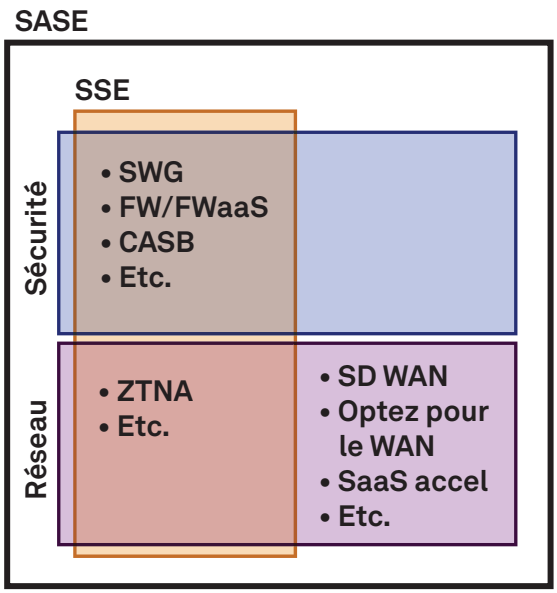
Au cours des dernières années, des événements importants ont fondamentalement changé les exigences d'accès à distance des organisations. Il s'agissait notamment de migrations massives vers le cloud, de transformation numérique et de passage au travail à distance. Il s'agissait également de mettre l'accent sur la réduction des coûts et l'amélioration de l'expérience utilisateur.

Les architectures réseau traditionnelles, construites autour de concepts de défense en profondeur qui supposaient un périmètre réseau relativement statique et reposaient fortement sur la sécurité à la périphérie du réseau, ont disparu. Les applications, les données et les utilisateurs peuvent désormais se trouver n'importe où, ce qui entraîne une expansion et une modification constantes des surfaces d'attaque. Par nécessité, l'authentification de sécurité doit désormais être appliquée au niveau de l'entité (par exemple un utilisateur ou un appareil), et les mécanismes utilisés pour vérifier et attribuer la confiance ont suivi, incarnant le cœur des principes de confiance zéro, ou Zero Trust : « Ne jamais faire confiance, toujours vérifier. »

La définition du SASE est un point à éclaircir. Le SASE est un modèle et un cadre de déploiement basés sur cinq technologies principales, incluant des composants réseau et sécurité :

- Pare-feu en tant que service (Firewall as a Service, FWaaS). Il s'agit d'un pare-feu de nouvelle génération fourni sous la forme d'un service centralisé basé sur le cloud.
- Passerelle Web sécurisée (Secure Web Gateway, SWG). Également connue sous le nom de « filtre Internet », la SWG applique les politiques de sécurité Web et contrôle l'accès au contenu Internet au niveau de l'application.
- Courtier de sécurité d'accès au cloud (Cloud Access Security Broker, CASB). Situés entre les utilisateurs et les fournisseurs de services cloud, les CASB contrôlent l'accès des utilisateurs et appliquent des politiques de sécurité telles que l'authentification et l'autorisation.
- Réseau étendu défini par logiciel (Software-Defined Wide-Area Network, SD-WAN). Le SD-WAN permet aux organisations de créer des WAN hautement performants sur Internet, améliorant ainsi la flexibilité et réduisant les coûts engendrés par les connexions MPLS traditionnelles.
- Accès réseau Zero Trust (Zero-Trust Network Access, ZTNA). Il limite l'accès aux applications à un ensemble d'utilisateurs ou d'entités autorisés et établit une limite sécurisée autour des applications, nécessitant une vérification de l'identité, du contexte et du respect des politiques avant d'accorder l'accès. Les applications deviennent pratiquement invisibles pour les utilisateurs non autorisés. Le ZTNA est un catalyseur clé des principes de confiance zéro.

Graphique 1 : Composants du SASE avec services de sécurité et réseau convergents



Source : S&P Global Market Intelligence, 2023.

Le SASE se définit comme un ensemble d'offres cloud natives, gérées de manière centralisée par le personnel informatique d'une entreprise, un fournisseur de services ou une combinaison des deux. Cependant, alors que les fournisseurs de SASE ont tendance à promouvoir l'idée d'une suite complète fournie et gérée par un seul fournisseur, cela semble rarement être le cas. De nombreuses organisations ont déployé des composants de SASE avant que le SASE n'apparaisse en tant que concept, et il est logique, au niveau de l'entreprise, de choisir les meilleurs composants de SASE, quel que soit le fournisseur. Nos données renforcent cela. Selon l'étude « 451 Research's Voice of the Enterprise: Information Security, Technology Roadmap 2023 », plusieurs composants SASE de base ont déjà été mis en œuvre, notamment la SWG (65 % des répondants) et le ZTNA (isolation réseau et micro segmentation [51 %] et périmètre défini par logiciel [57 %]). L'étude montre également que près des deux tiers des répondants (62 %) prévoient d'augmenter les investissements en SASE en 2023.

Ce rapport se compose de quatre parties qui correspondent à un cycle de déploiement de SASE typique. Tout d'abord, la planification initiale, le choix des fournisseurs et le processus de prise de décision, suivis des spécificités du déploiement, notamment les étapes de mise en œuvre, les niveaux de maturité, l'état de la transformation numérique, la participation de tiers et les indicateurs de performance clés (KPI) du projet. La troisième partie est une discussion sur les obstacles au projet, les réalités vécues par rapport aux attentes et les enseignements tirés, notamment les conseils des participants qui se sont impliqués activement au déploiement de ces projets dans le monde réel. Ce rapport se termine par une discussion sur les facteurs importants que les organisations doivent prendre en compte avant de passer au SASE.

Problème, solution, identification des fournisseurs et prise de décision

Nous avons découvert des besoins impérieux qui poussent les organisations à adopter les solutions de SASE. Les organisations plus matures et techniquement sophistiquées sont davantage motivées par les besoins de transformation commerciale et numérique que par les exigences techniques. Les grandes organisations (généralement plus de 10 000 employés) souffrent d'une dette technique et de systèmes hérités incompatibles qui ralentissent et compliquent les déploiements. Les petites organisations ont tendance à adopter des solutions plus rapidement et peuvent souvent s'approvisionner dans l'ensemble de la pile SASE auprès d'un seul fournisseur, alors qu'auparavant, les grandes organisations étaient nombreuses à déployer des parties de la pile SASE, en particulier le SD-WAN. Les fournisseurs ont répondu en proposant un service de sécurité en périphérie (Secure Service Edge, SSE – soit SASE moins le composant « accès ») conçus pour répondre à des cas d'utilisation spécifiques liés à l'élimination de l'infrastructure VPN et des coûts de licence. Le SASE et le SSE présentent des caractéristiques, des problèmes et des défis architecturaux similaires. Dans le cadre de l'étude, le SASE était la seule solution proposée, mais comme le SSE est considéré comme un dérivé du SASE, il est probable que les organisations utilisant le SSE le considéraient comme tel lors de la formulation des réponses à l'enquête.

Identification des problèmes

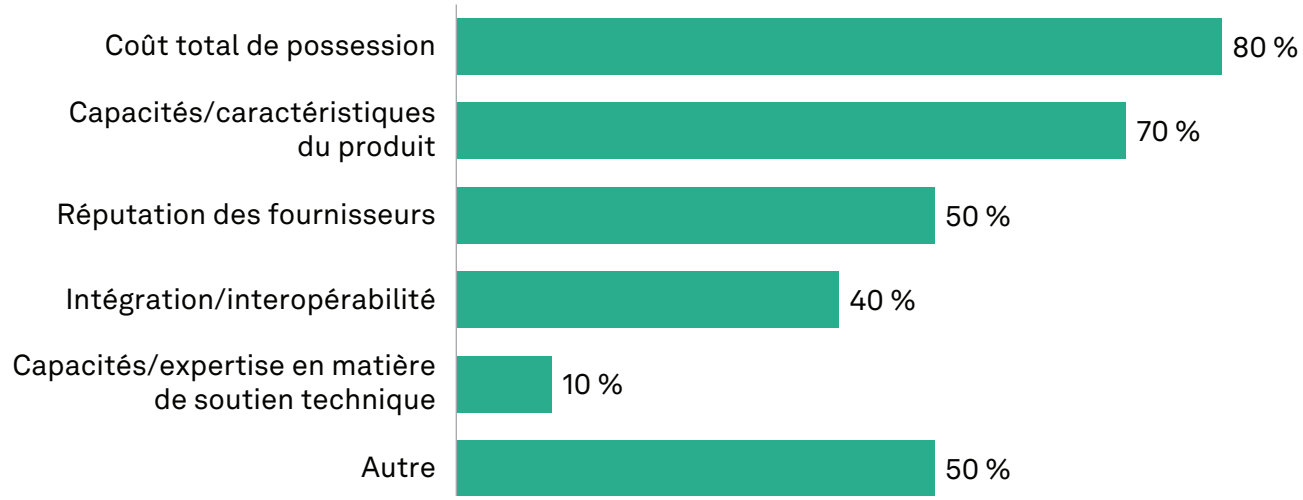
Les participants à l'étude présentaient de nombreux points communs qui les ont poussés à lancer un projet de SASE. Du point de vue de l'entreprise, l'amélioration de l'agilité, la réduction des coûts, la prise en charge du travail hybride (bureaux et travailleurs à distance), l'amélioration de l'expérience de l'utilisateur final, la réduction du risque et de l'impact des menaces, l'amélioration de la conformité et la pression de la concurrence ont tous été pris en compte dans la décision. D'un point de vue technique, le réseau, la sécurité, la modernisation et la simplification du système informatique et la gestion simplifiée des réseaux en croissance rapide étaient tous des facteurs clés. Et bien qu'il faille des mois ou des années à certaines organisations pour réaliser pleinement la vision d'une sécurité de bout en bout et sans frontières, la plupart des organisations ont constaté des « effets rapides » tels que la réduction ou l'élimination de l'infrastructure VPN et WAN et des coûts de licence, l'amélioration de l'expérience utilisateur et la prise en charge de lieux de travail flexibles.

Analyse des solutions, identification des fournisseurs et prise de décision

Nous avons analysé les ressources et les processus utilisés par les participants à l'étude pour dresser une « liste restreinte » et un fournisseur final du SASE. Dans la plupart des cas, les organisations interrogées ne se sont pas écartées des processus d'approvisionnement traditionnels, menant des recherches à l'aide de sites Web de fournisseurs, d'analystes du secteur, de conseillers de confiance et de pairs du secteur. Certaines organisations ont eu recours à des services externes lorsqu'elles manquaient d'expertise en interne. L'élaboration d'une liste restreinte de fournisseurs était un défi commun, car il existe au moins vingt offres SASE sur le marché.

Alors qu'au départ certaines organisations évaluaient jusqu'à dix fournisseurs, les listes restreintes se composaient généralement d'un fournisseur en place et de deux ou trois fournisseurs réputés. Elles ont mené des essais et des preuves de concept en utilisant des ressources internes et des fournisseurs et en mettant l'accent sur la preuve des exigences techniques. Les exigences en matière de justifications approfondies pour l'entreprise ont souvent été assouplies en raison de besoins urgents tels que des transitions rapides vers le travail à distance et des niveaux de risque supérieurs. Cependant, dans environ 40 % des cas, les cycles de vente ont pris plus d'un an entre le début de la recherche et la signature du contrat, probablement en raison de la complexité du processus d'achat et des parties prenantes impliquées. Les principaux décideurs étaient généralement le responsable de la sécurité des systèmes d'information (CISO), le directeur des systèmes d'information (CIO) ou d'autres hauts responsables techniques. Les petites organisations avaient tendance à prendre une décision finale plus rapidement que les grandes.

Graphique 2 : Principaux facteurs lors du choix d'un fournisseur de SASE



Q. Quels étaient les trois principaux facteurs et attributs des fournisseurs/partenaires que vous avez choisis ?
Base : Répondants de la zone EMEA (n = 10).
Source : Étude du SASE de S&P Global Market Intelligence, mars 2023.

« L'informatique non autorisée et fantôme – la consumérisation du SaaS permet à une unité commerciale de créer très facilement une instance d'un service et de l'utiliser avec des données commerciales. Nous avons besoin de visibilité et de contrôle, mais sans étouffer l'agilité et la collaboration. Les réseaux non corporatifs (maison, cafés, etc.) – nous n'avons pas une visibilité complète des réseaux en dehors de notre infrastructure traditionnelle. Nous devons être perspicaces et en mesure d'établir la confiance, le cas échéant, sur la base de l'identité. »

– Responsable de la sécurité de l'information, des risques et de la conformité, soins de santé, de 5 001 à 10 000 employés, Royaume-Uni

Déploiement du SASE

L'étude a révélé les informations principales du déploiement, notamment l'approche globale, l'état et la durée de la mise en œuvre, la relation avec les projets plus vastes de transformation du réseau et de transformation numérique, et les organisations internes qui ont dirigé le projet. L'étude a également comparé l'utilisation de ressources tierces et de ressources internes, les avantages les plus importants, l'état de transformation numérique et la sélection d'un ou plusieurs fournisseurs.

Approche de déploiement

Les participants ont indiqué diverses approches de déploiement. Aucun n'a déclaré se lancer dans une mise en œuvre « de choc » : certaines organisations ont d'abord déployé le SASE pour les utilisateurs et les applications à haut risque, tandis que d'autres ont choisi des utilisateurs et des applications à faible risque. Par exemple, certaines organisations fortement exposées aux risques à court terme, tels que le potentiel de violations ou d'échecs d'audits de conformité, ont d'abord choisi de résoudre le problème pour ces groupes. D'autres, moins préoccupées par le risque à court terme, ont adopté une approche plus conservatrice, telle que le déploiement auprès du personnel utilisant déjà des applications cloud modernes.

« Effets rapides, le plus risqué d'abord, un plus grand impact commercial. »

– CIO, ingénierie, de 1 001 à 5 000 employés, France

« Nous adoptons d'abord un déploiement pour les utilisateurs qui présentent le moins de risques et adoptons un déploiement plus frileux dans les domaines clés des opérations où les temps d'arrêt auraient un impact significatif et un préjudice potentiel sur les patients. »

– CTO, soins de santé, de 1 001 à 5 000 employés, Royaume-Uni

État d'avancement de la mise en œuvre et durée du projet

En ce qui concerne le processus de déploiement, 25 % des participants en étaient à l'étape de l'évaluation, de la demande de propositions et de la preuve de concept, 50 % étaient à mi-parcours de la mise en œuvre et 25 % avaient terminé ou presque terminé. Il est intéressant de noter l'absence de véritable tendance derrière la maturité du déploiement. La durée globale du projet (de l'approbation initiale à la production) variait de 6-12 mois à plus de 3 ans. Près de la moitié (45 %) des répondants ont indiqué des durées de 12 mois ou moins, 45 % se situaient dans l'intervalle de 13 à 36 mois, et les 10 % restants ont indiqué plus de 3 ans.

Participation plus importante au projet

En Europe, les trois quarts des participants ont déclaré avoir déployé le SASE dans le cadre d'une initiative de transformation numérique, contre seulement un tiers dans la région Asie-Pacifique (APAC). Environ deux tiers des répondants ont indiqué que la transformation du réseau avait été menée en même temps que le déploiement du SASE, environ 30 % ont indiqué que la transformation du réseau était terminée avant le projet SASE, et un seul répondant a indiqué que la transformation du réseau avait été mise en œuvre après le projet SASE. La transformation du réseau apparaît clairement comme un élément essentiel de la plupart des projets SASE.

Équipes/organisations impliquées

Étant donné que le SASE touche les équipes réseau et sécurité, l'étude a cherché à déterminer quelles équipes internes ont dirigé le projet. Dans la plupart des cas, le projet a été mené conjointement par les équipes réseau et sécurité (70 %) et seulement 15 % des projets ont été dirigés par l'équipe de sécurité seule. Dans aucun des exemples que nous avons évalués l'équipe réseau n'a dirigé le projet seule, et le reste des projets a été dirigé par une autre combinaison d'équipes.

Assistance de tiers

Davantage d'organisations ont eu recours à des tiers pour le déploiement que pour l'évaluation. En Europe, cette assistance provenait le plus souvent d'intégrateurs de systèmes (SI) plutôt que de revendeurs à valeur ajoutée et de fournisseurs de solutions, tandis qu'en Asie-Pacifique, la plupart des supports tiers étaient fournis par des fournisseurs de solutions, tandis que les SI étaient principalement utilisés comme conseillers. Les différences entre les régions EMEA et APAC sont probablement culturelles, car de nombreuses organisations de la région APAC entretiennent des relations étroites avec les fournisseurs de solutions et préfèrent compter sur eux pour les services après-vente.

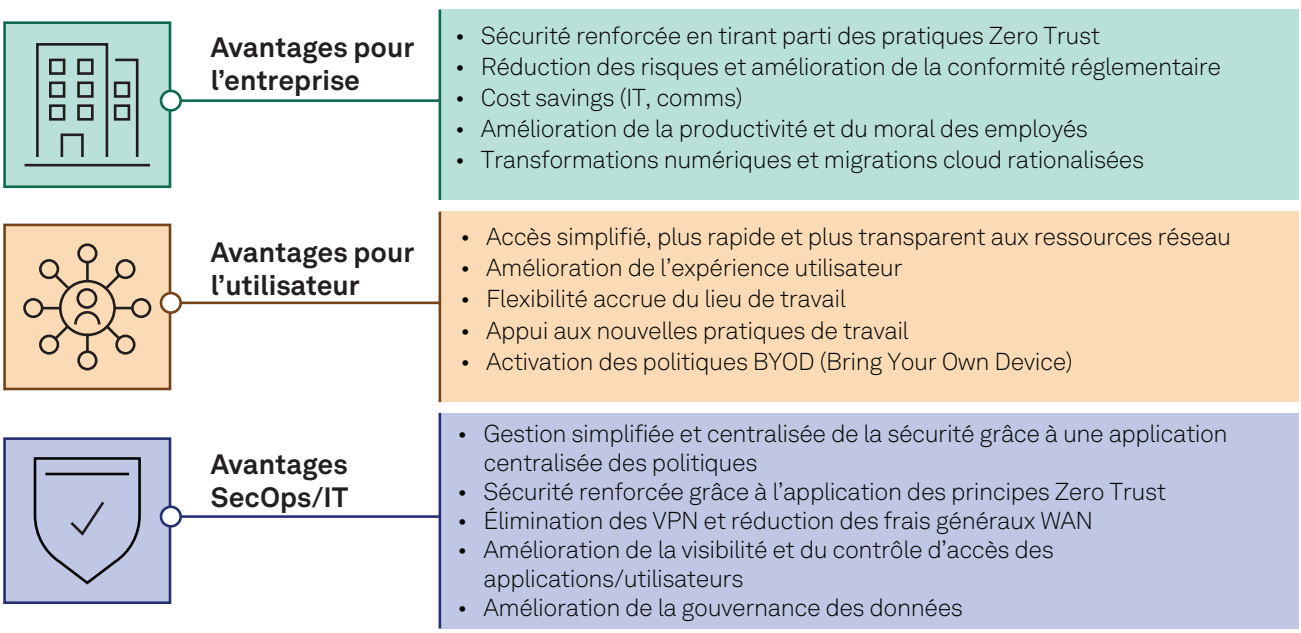
Principaux avantages du SASE

Les participants à l'étude ont mentionné de nombreux avantages spécifiques à leur déploiement de SASE. Nous les avons divisés en trois catégories de prestations : entreprise, utilisateur et sécurité des opérations/informatique (SecOps/IT).

Du point de vue de la sécurité de l'entreprise et de l'informatique, les répondants ont déclaré que les principaux avantages du SASE étaient la réduction des risques d'attaques et de violations ainsi que la réduction de la surface d'attaque et des vulnérabilités. Les avantages pour les utilisateurs comprenaient un accès à distance simplifié, une expérience utilisateur améliorée, une meilleure flexibilité du lieu de travail et la possibilité de prendre en charge le BYOD.

En outre, de nombreux participants à l'étude ont cité les avantages d'une architecture réseau Zero Trust grâce à la micro-segmentation du réseau, qui réduit considérablement la surface d'attaque et le « rayon d'impact » potentiel des violations.

Graphique 3 : Principaux avantages de la mise en œuvre du SASE



Source : Étude du SASE de S&P Global Market Intelligence, mars 2023.

« C'est aussi une question de réduction de la surface d'attaque. Nous donner la possibilité de restreindre les mouvements sur le réseau réduit considérablement le risque de réussite d'une attaque externe. L'amélioration du contrôle d'accès réduit également le risque de perte accidentelle. »

– CISO, services de données, de 1 001 à 5 000 employés, Royaume-Uni

État de la transformation numérique

Pour les besoins de cette étude, nous avons défini la « transformation numérique » comme le pourcentage d'applications modernisées ou cloud natives en production. Un quart des répondants ont déclaré que leurs organisations étaient en mode « rattrapage », c'est-à-dire qu'elles passaient rapidement à un état plus mature, tandis que les autres ont déclaré être dans un état presque ou complètement mature. Les principaux moteurs de la transformation numérique comprennent les pressions du marché pour améliorer la rentabilité et réduire les délais de mise sur le marché pour contrer les menaces de la concurrence. L'étude montre que si la plupart des répondants ont aligné les projets SASE sur des efforts de transformation numérique plus importants, les projets n'ont généralement pas été gérés ensemble : le financement, les délais et les autres facteurs de mise en œuvre du SASE étaient indépendants des initiatives plus larges de transformation numérique.

Fournisseurs uniques ou multiples et forces perçues

Malgré les affirmations des fournisseurs concernant la fourniture de tous les composants du SASE, la moitié des répondants à l'étude ont indiqué qu'ils utilisaient plus d'un fournisseur. Bien que les participants aient nommé dix-huit fournisseurs, quatre ont été plus fréquemment mentionnés. Il s'agit, par ordre alphabétique, de Fortinet, Netskope, Palo Alto Networks et zScaler. Le marché n'en est qu'à ses débuts, et le grand nombre de déploiements multifournisseurs indique que de nombreuses organisations continuent probablement à utiliser des fournisseurs en place pour certaines capacités et choisissent potentiellement de meilleures capacités technologiques chez d'autres.

Résultats du SASE, obstacles et données d'expérience

La phase finale de l'étude s'est concentrée sur les obstacles au projet SASE, les résultats et les données d'expérience. Il s'agit notamment de découvrir les différences entre les attentes et la réalité, l'effet du SASE sur la transformation numérique, les KPI utilisés, la manière de surmonter les obstacles et de recueillir les conseils des participants sur les principales leçons qu'ils ont tirées.

Attentes du projet et résultats

Il est intéressant d'analyser les différences entre les résultats attendus d'un projet et la réalité. Pour le SASE, les attentes comprenaient la réduction des risques, la réduction des coûts et l'amélioration de la productivité et de l'expérience utilisateur. Parmi les participants qui avaient terminé ou presque terminé leurs projets SASE, la plupart ont déclaré avoir atteint les résultats escomptés, voire des résultats supplémentaires. Voici une liste complète des résultats attendus créée par un participant, le CIO d'une grande organisation d'assurance au Royaume-Uni :

- Réduire la surface d'attaque grâce à la micro-segmentation et à la mise en œuvre des niveaux de confiance
- Sécuriser toutes les communications, quel que soit le réseau, via un accès dynamique basé sur le risques
- Accélérer et automatiser la réponse grâce à la détection et à l'analyse proactives des menaces à partir d'une surveillance contextuelle en temps réel
- Simplifier les contrôles de conformité grâce à des contrôles simplifiés, une meilleure automatisation et une standardisation accrue
- Sécuriser l'accès flexible aux ressources grâce à des politiques dynamiques
- Améliorer la productivité et l'expérience utilisateur
- Prendre en charge des produits et des services numériques prêts pour Internet
- Mettre en œuvre des solutions de sécurité plus rapides et plus agiles
- Réaliser des économies durables
- Activer des processus et un approvisionnement simplifiés

Les participants ont indiqué des résultats réels et positifs, même si beaucoup étaient à mi-déploiement et n'avaient pas encore pleinement constaté les avantages potentiels de la mise en œuvre. La plupart des résultats ont été qualifiés de « non tangibles », difficiles à quantifier, l'évaluation des avantages tangibles étant prévue plus tard, en raison de l'urgence du déploiement.

Indicateurs de performance clés

Les KPI sont généralement difficiles à définir et à quantifier dans les projets qui sont basés sur une technologie relativement nouvelle et qui sont encore en cours. Dans cette étude, un tiers des participants n'ont défini aucun KPI, un tiers ont défini des KPI « tangibles » et un tiers ont défini des KPI « non tangibles ». Certains répondants ont signalé un mélange de KPI tangibles et non tangibles.

« Un environnement plus sûr, un utilisateur malveillant contrecarré et un comportement antagoniste… Une gestion plus rapide des problèmes et une disponibilité accrue. »

– CIO, soins de santé, plus de 10 000 employés, Suède

« [Le SASE] a simplifié l'intégration des nouveaux employés et la nécessité de changer les mots de passe plus souvent. »

– CIO, hôtellerie, de 1 001 à 5 000 employés, Royaume-Uni

« [Le SASE] a permis de simplifier la mise en œuvre de nouveaux sites et secteurs d'activité. Grâce aux stratégies définies par logiciel à la périphérie, [le SASE] a apporté de la valeur grâce à la rapidité du déploiement. »

– CTO, soins de santé, de 1 001 à 5 000 employés, Royaume-Uni

« Un des avantages inattendus d'une architecture SASE, c'est de voir des synergies et une convergence d'intérêts entre l'infra/le réseau et la sécurité, domaine où on assiste généralement à une lutte entre les contraintes de performance et d'expérience utilisateur et les contraintes de sécurité (ce qui est assez rare pour être souligné !). Nous avons trouvé un terrain d'entente où concilier les deux. »

– Directeur des applications et de la sécurité des données, mines et métaux, plus de 10 000 employés, Singapour

Effets du SASE sur le parcours global de transformation numérique

La plupart des organisations ne considéraient pas le déploiement du SASE comme partie intégrante d'une initiative de transformation numérique plus large, mais le géraient de manière indépendante. Cela est probablement dû au fait que les projets de transformation numérique ont commencé avant les implémentations de SASE et se poursuivront longtemps après. Cela peut également être lié à des facteurs à court terme qui ont nécessité un déploiement rapide du SASE. Les répondants avaient des avis partagés lorsqu'on leur a demandé si le SASE était bénéfique à l'effort de transformation numérique. Certains ont déclaré que le SASE avait contribué à leur projet global de transformation numérique en réduisant les risques et en simplifiant l'expérience utilisateur, tandis que d'autres ont déclaré qu'il ralentissait le processus de transformation. Ce dernier point de vue est probablement lié aux obstacles à la dette technique qui ont dû être éliminés avant que le projet puisse se poursuivre.

« Cela nous a également donné la flexibilité de cibler les fusions-acquisitions avec peu d'efforts supplémentaires. En outre, nous pouvons répondre à l'évolution des opérations de notre entreprise.

– Responsable des solutions numériques, services publics, de 5 001 à 10 000 employés, Hong Kong

« En termes d'accélération du parcours [de transformation numérique], je serais un peu plus réservé sur le fait que cela a/aura un impact. »

– Directeur des applications et de la sécurité des données, mines et métaux, plus de 10 000 employés, Singapour

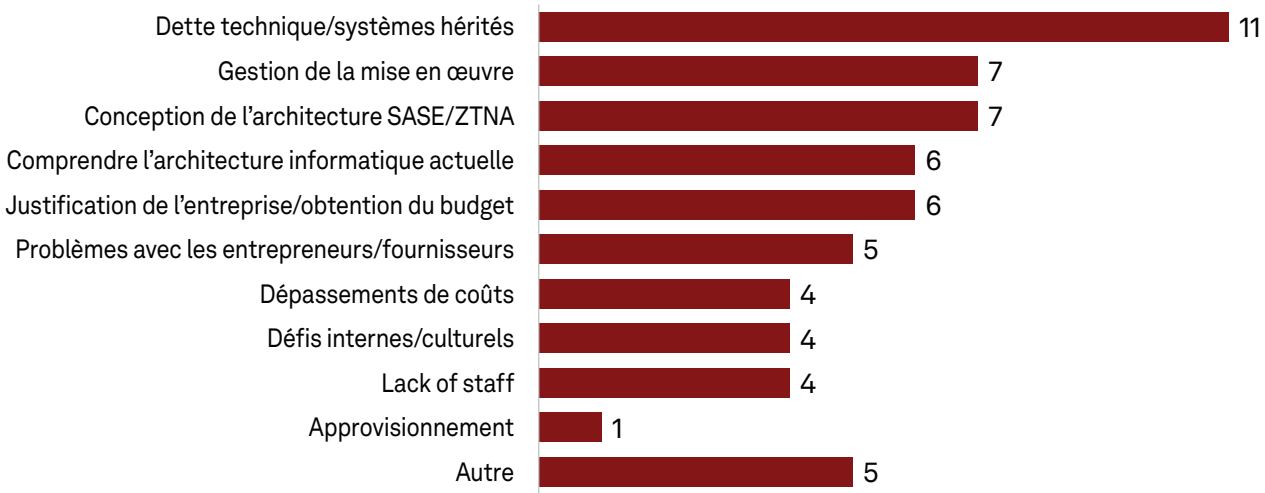
« Nous avons commencé par rationaliser la connectivité et les efforts qui ont mené les identités connexes et les projets de gestion des accès prennent désormais en charge presque toutes les autres applications. Donc, oui, il y a eu un effet d'accélération dans notre parcours DX. »

– Responsable régional de la sécurité de l'information, services informatiques, de 5 001 à 10 000 employés, Australie

Obstacles à la mise en œuvre du SASE

Plusieurs thèmes ont été évoqués, concernant les obstacles que les participants ont rencontrés ou s'attendaient à rencontrer lors de la mise en œuvre du SASE.

Graphique 4 : Principaux obstacles au déploiement du SASE



Q. Veuillez sélectionner les trois principaux obstacles que vous avez rencontrés ou que vous pensez rencontrer pendant le projet SASE.
Base : Tous les répondants (n = 20).
Source : Étude du SASE de S&P Global Market Intelligence, mars 2023.

« Le plus gros obstacle que nous rencontrerons dans notre mise en œuvre sera la dette technique que nous devrons rembourser avant de pouvoir achever le projet. Cela impliquera non seulement de mettre à jour de nombreux systèmes anciens et éprouvés, mais aussi de changer l'état d'esprit des personnes qui sont opposées au cloud parce qu'elles n'ont actuellement pas les connaissances requises pour réussir le déploiement de leurs systèmes dans le cloud et, par conséquent, bloquent activement les efforts visant à passer de nos centres de données physiques à Azure, AWS, etc. »

– CISO, services juridiques, de 5 001 à 10 000 employés, Allemagne

Données d'expérience

Dans la dernière partie de l'étude, nous avons recueilli les connaissances acquises par les participants tout au long du cycle de vie de leur projet SASE. Nous les divisons en quatre catégories : évaluation des besoins ; amélioration des compétences, planification et préparation ; choix des fournisseurs/partenaires SASE ; planification du déploiement.

Évaluation des besoins

Les participants ont souligné la nécessité d'établir un cadre d'exigences solide et d'élaborer une analyse de rentabilité avant de lancer le projet. Ils ont recommandé d'adopter une approche de type « la sécurité d'abord » et ont conseillé aux implémenteurs potentiels de ne pas exécuter la mise en œuvre du SASE comme un remplacement d'infrastructure réseau. Ils ont également souligné l'importance d'être réellement soutenus par les principaux intervenants et d'établir de solides structures de gouvernance.

« Si vous n'en êtes qu'au début, décidez comment vous allez quantifier le niveau de risque actuel sans Zero Trust, puis identifiez clairement comment vous allez démontrer la valeur lorsque la nouvelle solution sera en place. »

– CISO, services de données, de 1 001 à 5 000 employés, Royaume-Uni

Perfectionnement, planification et préparation

En progressant dans la planification et la préparation du projet, les participants ont souligné la nécessité de perfectionner les compétences et les ressources internes bien à l'avance. Un sujet commun était l'importance de bien comprendre les données, les applications et les actifs des appareils impliqués ou affectés par le SASE. La plupart des participants ont indiqué qu'ils disposaient déjà d'inventaires détaillés d'actifs de type « nomenclature logicielle » provenant de projets de transformation numérique et de processus de gouvernance, de risque et de conformité, ce qui leur donnait une longueur d'avance. Les participants ont également souligné la nécessité d'« aller plus loin » en matière de planification, d'analyse comparative et de KPI, ainsi que l'importance de la planification d'urgence et de communications internes solides.

« Incluez un architecte dans l'équipe de votre intégrateur et assurez-vous qu'il travaille avec vos propres architectes. Déployez en fonction des risques. »

– CISO, services de données, de 1 001 à 5 000 employés, Royaume-Uni

Choix des fournisseurs/partenaires SASE

Les participants à l'étude ont recommandé de se concentrer d'abord sur les compétences des fournisseurs, d'approfondir les exigences spécifiques du SASE et de comparer les revendications des fournisseurs aux compétences réelles, bien qu'ils aient souligné que c'était difficile. Les participants ont également mentionné l'importance de faire appel à un partenaire éprouvé et d'établir de solides relations avec les fournisseurs et les partenaires.

« La complexité de l'environnement (entités clients, entités fournisseurs, etc.) nécessite la collaboration avec des fournisseurs qui pourraient soutenir nos objectifs : s'appuyer sur les PMV, assurer la durabilité et l'évolutivité Zero Trust, améliorer l'orientation client (interne et externe), sécuriser notre entreprise, permettre l'avenir de l'activité, réduire la complexité et gérer la réglementation et la conformité. Bien que nous ayons eu recours à plusieurs fournisseurs et à plusieurs solutions basées sur une approche de pointe, nous avons également essayé de concilier une approche standardisée par domaine (par exemple, identité, appareils, etc.).

– CIO, assurance, plus de 10 000 employés, Royaume-Uni

Planification du déploiement

Au moment du déploiement, les répondants ont souligné l'importance d'utiliser un modèle de déploiement standardisé, ainsi que de planifier et de programmer minutieusement le déploiement. Certains ont recommandé de commencer à petite échelle, d'obtenir des effets rapides et de tirer très tôt des leçons avant d'étendre le projet.

« Définir les principes du programme et l'architecture cible et s'y engager, par exemple en commençant à petite échelle et en évoluant avec des cas d'utilisation, construire dans un format réutilisable, donner la priorité aux applications SaaS prêtes pour le cloud, se concentrer sur des solutions à l'épreuve du temps, renforcer les capacités fondamentales, etc. »

– CIO, assurance, plus de 10 000 employés, Royaume-Uni

Conclusions

L'étude a permis de tirer de nombreuses conclusions essentielles. Pour la plupart des organisations, le SASE est très logique au niveau de l'entreprise en termes de réduction des risques de cybersécurité, d'amélioration de l'expérience utilisateur, de travail à distance et hybride, et d'amélioration de la conformité aux réglementations et aux politiques internes. Il est également de plus en plus important en termes de facilitation et de sécurisation des efforts de transformation numérique.

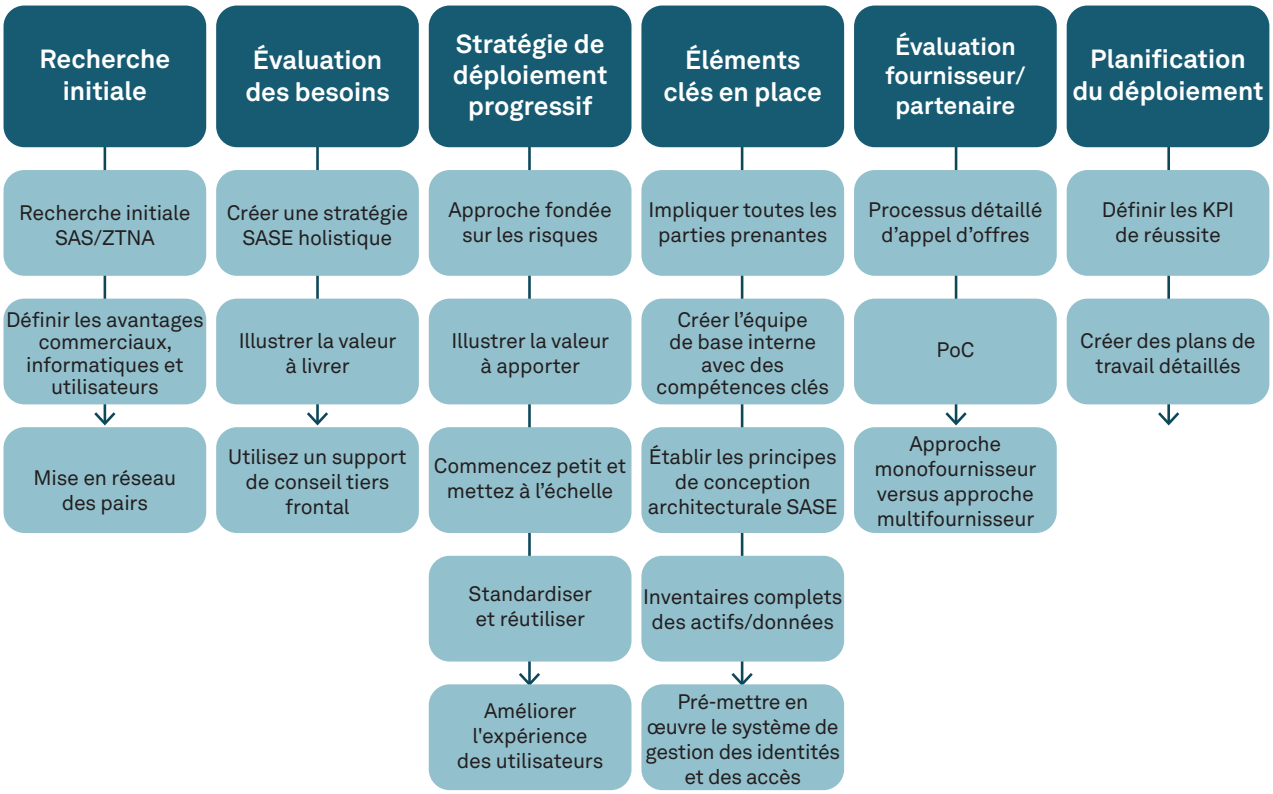
Comme tout projet technologique majeur, le parcours doit être soigneusement défini, planifié et exécuté, en ayant recours aux fournisseurs, technologies et partenaires appropriés. Les participants à l'étude ont souligné l'importance de bien comprendre les données, les applications, les utilisateurs et les appareils qui seront affectés et, bien que la plupart aient également indiqué que ces informations sont disponibles en raison des exigences de conformité et de transformation numérique, l'obtention des données pourrait être difficile et prendre beaucoup de temps. Les participants ont principalement mené des recherches initiales sur les solutions SASE à l'interne, à l'aide des sites Web des fournisseurs, d'analystes du secteur, de conversations avec les pairs du secteur et, dans certains cas, de conseillers de confiance tiers.

Certaines organisations ont commencé par un petit projet dans le but de voir des effets rapides pour montrer une valeur commerciale rapide aux parties prenantes, tandis que d'autres ont été obligées d'agir rapidement et à plus grande échelle pour réduire les risques ou soutenir des changements massifs en termes de lieux de travail. Il est essentiel d'impliquer très tôt les parties prenantes à ce processus, pour déterminer l'appétit pour le risque et l'approche de déploiement ultime. Contrairement à de nombreux investissements informatiques et de sécurité, la justification commerciale n'était pas une préoccupation majeure pour de nombreux participants à l'étude en termes d'obtention de budget, car il semble que de nombreuses organisations comprenaient que le SASE était une composante nécessaire des efforts de modernisation et étaient prêtes à engager les coûts et à accepter les risques associés.

Quel que soit le plan de mise en œuvre, le processus de sélection des fournisseurs et des partenaires est difficile en raison du nombre important de fournisseurs. Les participants préféraient les fournisseurs de sécurité ou de réseau déjà en place, bien que la plupart en aient évalué d'autres en fonction des recommandations de pairs ou de sources fiables. Les participants ont souvent mentionné la nécessité de tester pleinement les solutions au moyen de démonstrations approfondies et de preuves de concept, et la moitié des participants ont indiqué qu'ils ne trouvaient pas toutes les fonctionnalités requises auprès d'un seul fournisseur. Les grandes organisations ont indiqué que la planification de la mise en œuvre était plus difficile en raison de la dette technique et des systèmes hérités qui nécessitaient un rééquipement et une modernisation approfondis avant de devenir « compatibles SASE ». Le recours à des tiers variait, les fournisseurs de solutions et les SI étant le choix le plus populaire. Les organisations ont eu du mal à identifier des KPI quantifiables, et la plupart ont indiqué que l'utilisation de KPI « tangibles » n'était pas une priorité lors de la mise en œuvre. La durée des projets variait de six mois à plus de trois ans.

Les participants à l'étude ont fourni beaucoup de conseils sur la façon de surmonter les obstacles. Le graphique suivant résume leurs conseils.

Graphique 5 : Conseils des répondants pour surmonter les obstacles à la mise en œuvre du SASE



Source : Étude du SASE de S&P Global Market Intelligence, mars 2023.

Aujourd'hui, pour la plupart des organisations, le SASE est clairement la voie à suivre pour accroître la sécurité, réduire les risques et soutenir la transformation numérique. Le marché du SASE se développe rapidement, avec plus de vingt fournisseurs en lice, bien que quatre fournisseurs aient été mentionnés à plusieurs reprises dans l'étude. Une certaine consolidation du marché devrait se produire à mesure que les grands fournisseurs font des acquisitions stratégiques pour gagner des parts de marché et combler les lacunes, ce qui leur permet de fournir une pile de solutions SASE complète.

Méthodologie

Ce rapport est basé sur dix entretiens approfondis de trente à quarante minutes menés à la fin de l'année 2022 et sur un forum de discussion en ligne de vingt participants, qui s'est déroulé sur trois jours en mars 2023. Les participants à l'étude étaient également répartis entre l'Europe (France, Allemagne, Suède et Royaume-Uni) et l'Asie-Pacifique (Australie, Hong Kong, Inde et Singapour). Les participants travaillent dans une grande variété de secteurs, pour des organisations de plus de 1 000 employés en Europe et plus de 5 000 employés en Asie-Pacifique, et ils dirigent ou sont impliqués dans la gestion et/ou la mise en œuvre des achats de technologie SASE. Les répondants ont en moyenne vingt ans d'expérience dans le domaine de la sécurité de l'information et leurs fonctions incluent les titres de CISO, CIO, CTO et responsable régional de la sécurité. En raison de l'échantillon réduit de l'étude, les résultats doivent être interprétés de façon anecdotique.

À propos de l'auteur

Mark Ehr

Analyste-conseil principal

Mark Ehr est analyste consultant principal pour S&P au sein de l'équipe mondiale des TMT basée à Denver, Colorado, États-Unis. Avant de rejoindre S&P, il a travaillé 12 ans chez IBM où il a occupé des postes tels que l'aide à la vente de sécurité à l'échelle mondiale et la gestion des produits QRadar SIEM.

Auparavant, il a travaillé pour BigFix, Cabletron, Enterprise Management Associates, Ping Identity, Polarsoft, Siebel Systems et Sybase, et a occupé des postes tels que consultant, entrepreneur, analyste industriel, spécialiste du marketing de produits, développeur de logiciels et vendeur de technologies.

Mark est titulaire d'une licence en informatique de la Metropolitan State University de Denver.

À propos de S&P Global Market Intelligence

La recherche sur la technologie, les médias et les télécommunications (TMT Research) de S&P Global Market Intelligence fournit des éléments essentiels sur le rythme et l'ampleur de la transformation numérique dans le paysage mondial des TMT. Grâce aux produits de 451 Research et de Kagan, TMT Research offre des informations et des données différenciées sur l'adoption, l'innovation et la perturbation des marchés des télécommunications, des médias et de la technologie, avec l'appui d'une équipe mondiale d'experts du secteur et par le biais d'une gamme d'études multiclients, de services de conseil et de mise sur le marché, ainsi que d'événements en direct.

CONTACTS

Amériques : +1 800 447 2273
Japon : +81 3 6262 1887
Asie-Pacifique : +60 4 291 3600
Europe, Moyen-Orient, Afrique : +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html