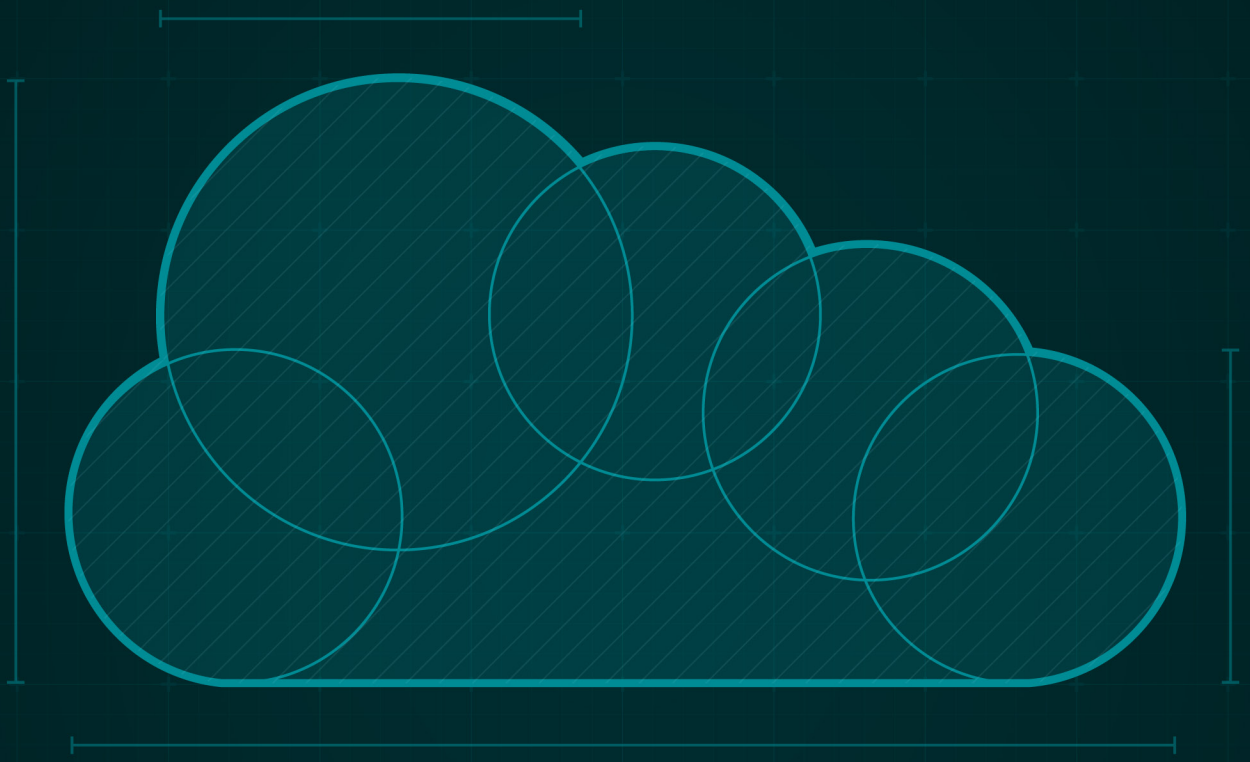
netskope

LIVRE BLANC



Déploiement du Zero Trust dans une architecture SASE

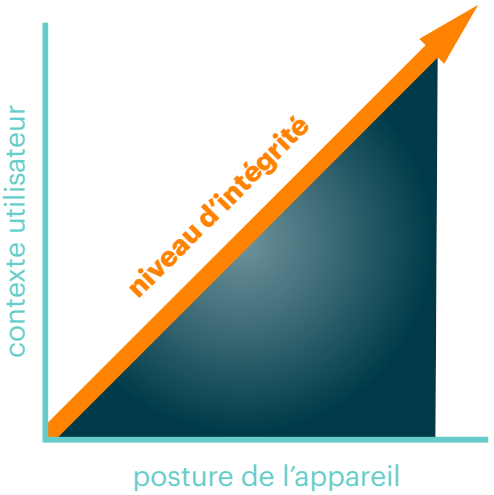
Confiance adaptative et continue : la clé pour réussir l'implémentation du Zero Trust et du SASE

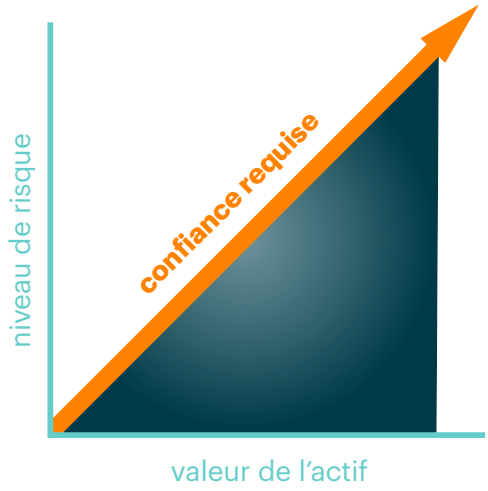
Pour un concept qui repose sur l'*absence* (de confiance), le Zero Trust est absolument *partout*. Pourtant, malgré l'effervescence qui entoure cette nouvelle approche, une chose semble encore manquer à sa compréhension : une description convaincante des objectifs du Zero Trust et des résultats visés. Jusqu'ici, les entreprises qui se sont aventurées dans des projets Zero Trust ont dû faire face à plusieurs défis d'envergure : incohérence des définitions, manque de clarté des critères de réussite ou encore incompatibilité de systèmes informatiques existants, souvent obsolètes. L'adoption du Cloud, la transition au télétravail et la transformation digitale sont des opportunités pour souligner l'importance des principes du Zero Trust pour les architectures Secure Access Service Edge (SASE) multi-cloud. Chez Netskope, nous pensons qu'une approche Zero Trust dans un environnement SASE ou hybride nécessite la mise en œuvre d'une confiance adaptive en continu pour l'ensemble des utilisateurs, appareils, réseaux, applications et données nous permettant de garantir une application véritablement universelle des politiques.

L'objectif premier du Zero Trust est de passer d'un modèle de confiance implicite (« *je fais confiance, mais je vérifie* ») à un modèle de confiance explicite (« *je vérifie avant de faire confiance* »). Dans ce schéma, les ressources n'accordent plus leur confiance de façon tacite (par le biais de l'adresse IP, par exemple) aux entités souhaitant se connecter. En évaluant plusieurs éléments contextuels (identité de l'utilisateur, identité du device et posture de sécurité, heure, géolocalisation, rôle au sein de l'entreprise, niveau de confidentialité des données et bien plus), la ressource peut déterminer *le niveau d'intégrité*, et donc de confiance, d'une interaction spécifique sur un appareil spécifique. À titre d'exemple, le niveau d'intégrité d'un utilisateur dont l'appareil est muni d'un agent capable de fournir des données de télémétrie sophistiquées, reflétant l'environnement de l'appareil, sera probablement plus élevé que celui associé à un utilisateur dont l'appareil ne fournit qu'une adresse MAC déjà enregistrée. Plus le niveau de fiabilité est élevé, plus la confiance accordée l'est également.

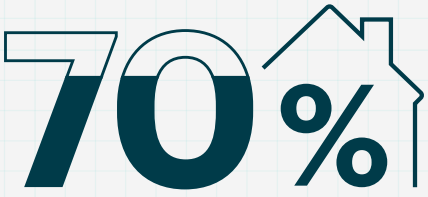
Mais évaluer le niveau de fiabilité d'une interaction au moment où elle est initiée n'est pas suffisant. Au cours de l'interaction, le contexte doit être réévalué *en continu*. Une évolution du contexte peut entraîner un *ajustement* (positif ou négatif) du niveau de confiance, ce qui en retour peut faire évoluer le type d'accès à la ressource.

En matière d'accès, les décisions binaires prônant le « tout ou rien » privent les entreprises de la souplesse qu'exigent les nouveaux modes de travail. Le recours à une application SaaS à haut risque nécessaire pour préserver la productivité d'un employé serait, par exemple, ingérable dans un modèle aussi simpliste. L'accès doit être corrélé au contexte et chercher l'équilibre entre confiance et risque. Dans les situations à haut



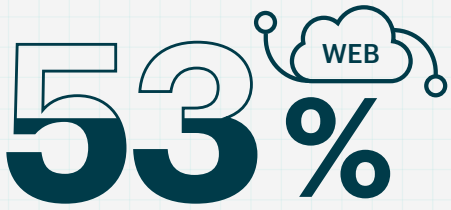


Mais en essence, une véritable approche Zero Trust vise surtout à réduire les risques et renforcer l'agilité opérationnelle, en écartant la confiance implicite et en évaluant continuellement la fiabilité des appareils et utilisateurs grâce à la gestion d'identités, l'accès adaptatif et des analyses complètes.



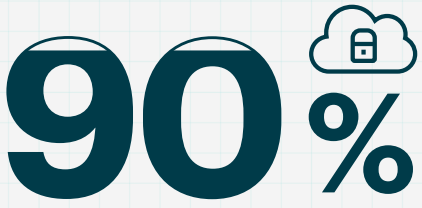
des utilisateurs ont continué de travailler à distance **durant le premier semestre 2021**

Plus de la moitié du trafic géré par la passerelle web relève d'un accès au Cloud



APPLICATIONS ET SERVICES CLOUD

90 % du trafic est crypté à l'aide de TLS*



CRYPTÉ À L'AIDE DE TLS

* Rapport Google HTTPS Transparency

risque, l'accès est restreint mais pas totalement bloqué, ce qui permet d'effectuer les tâches les plus pressantes. Dans des situations à risque modéré, l'accès est élargi, et certaines obligations (telles que l'authentification multifactorielle ou la nécessité d'un appareil managé) peuvent être allégées. Le modèle de confiance adaptative, les exigences en matière de fiabilité augmentent proportionnellement à la valeur du bien pour lequel l'accès est demandé. En analysant des signaux tels que les risques liés à l'application ou à l'activité, les risques utilisateurs, la sensibilité des données, la posture de l'appareil, l'emplacement des utilisateurs et d'autres attributs, l'approche adaptative permet de prendre en temps réel la décision d'autoriser, de refuser ou de restreindre l'accès, ou bien de rediriger ou de conseiller l'utilisateur. Et parce que l'approche adaptative aligne les politiques sur l'appétence au risque, une révocation d'accès peut même être envisagée si cela s'avérait nécessaire.

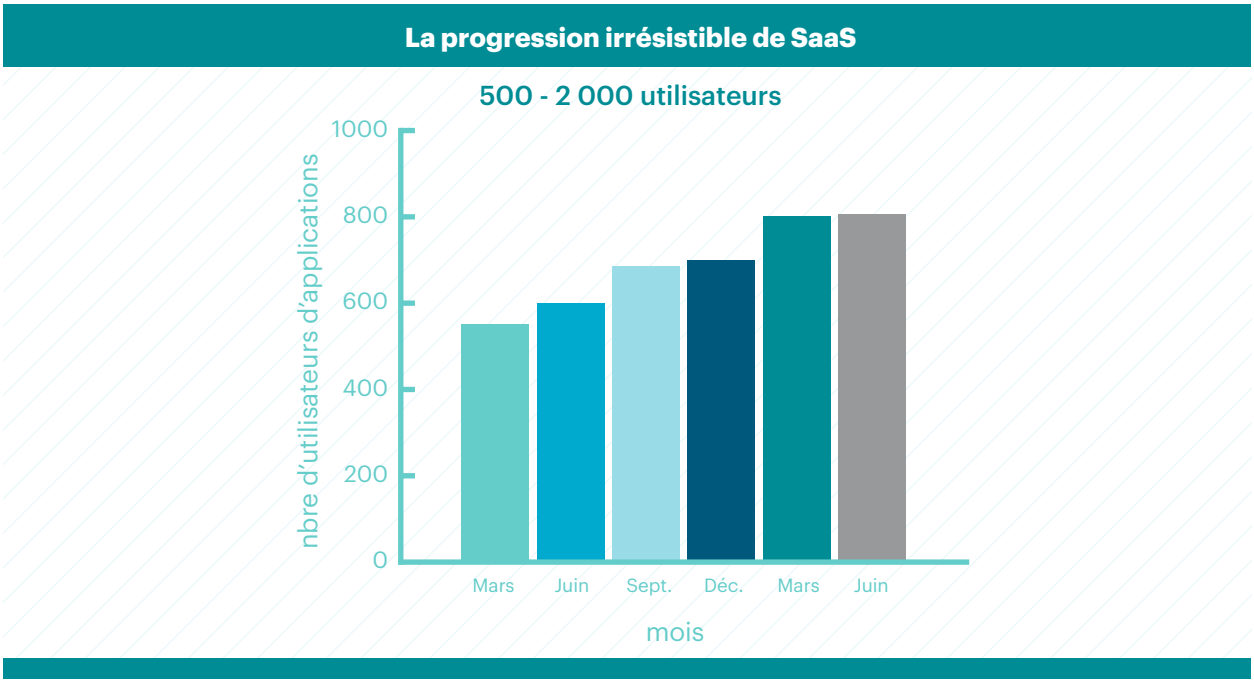
Un autre objectif de l'approche Zero Trust est de concevoir le dispositif de sécurité en supposant que l'environnement peut faire l'objet d'une violation à tout moment, et même que le cas s'est déjà présenté. Cette perspective plutôt inédite facilite le déploiement de schémas et de pratiques capables de réduire les surfaces d'attaque, limiter le rayon de propagation, restreindre les mouvements latéraux et répondre aux menaces plus rapidement et précisément.

Si, à première vue, le Zero Trust peut sembler n'être qu'une simple reformulation de deux principes de sécurité aussi courants qu'importants, le concept s'étend bien au-delà du principe du moindre privilège et de la dissimulation des ressources. Certes, les utilisateurs approuvés ne reçoivent que l'accès nécessaire aux ressources approuvées, et les ressources non-approuvées sont invisibles et donc inaccessibles aux utilisateurs non-approuvés. Mais en essence, une véritable approche Zero Trust vise surtout à réduire les risques et renforcer l'agilité opérationnelle, en écartant la confiance implicite et en évaluant continuellement la fiabilité des appareils et utilisateurs grâce à la gestion d'identités, l'accès adaptatif et des analyses complètes.

POURQUOI LE ZERO TRUST EST-IL IMPORTANT AUJOURD'HUI ?

Le modèle de réseau traditionnel date de l'époque où les employés de bureau accédaient aux applications d'entreprise dans des datacenters sur site. À l'image des dispositifs de sécurité physiques, les systèmes de protection des réseaux supposaient des menaces externes puisque quiconque se trouvant à l'intérieur était digne de confiance. Assurées d'être protégées contre les menaces externes, la plupart des entreprises considéraient le concept du Zero Trust comme une innovation sans trop y porter d'attention. Le périmètre était suffisant pour le moment, et des questions plus pressantes occupaient les services informatiques et équipes de sécurité.

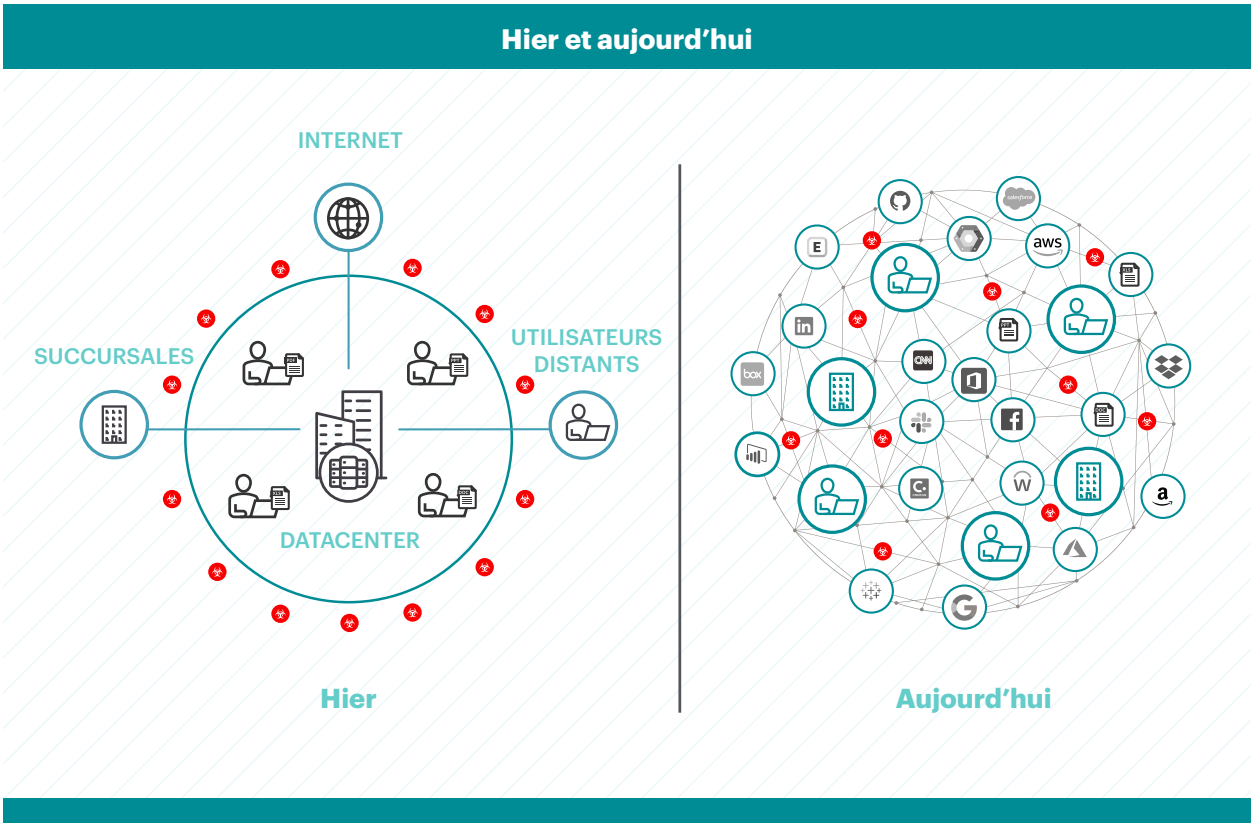
Et puis le monde a changé : les applications, les utilisateurs et les données ont migré à l'extérieur du périmètre. Attirées par la variété des options proposées et la simplicité de leur acquisition, les entreprises ont commencé à se tourner vers les applications Software-as-a-Service (SaaS) pour prendre en charge un nombre croissant de leurs processus opérationnels. Ainsi, même si certains processus requièrent toujours des solutions personnalisées, l'entreprise type de 500 à 2 000 utilisateurs serait désormais abonnée à plus de 805 *applications SaaS différentes !*



Source : Netskope Cloud and Threat Report – Juillet 2021

En parallèle, les entreprises ont aussi découvert que les Clouds publics de type Infrastructure-as-a-Service (IaaS) et Platform-as-a-Service (PaaS) offraient plus de souplesse que les datacenters traditionnels. Ces plateformes sont ainsi devenues la destination par défaut de la plupart des nouvelles applications. La plupart des entreprises adopte maintenant une stratégie multi-cloud, choisissant parmi plusieurs fournisseurs hyperscale en fonction des exigences des applications et de l'expertise des développeurs. (Le « *lift-and-shift* », processus permettant de migrer les applications existantes vers le Cloud public, a connu moins de succès, notamment parce que le Cloud amplifie les problèmes inhérents aux architectures défaillantes et aux mauvaises décisions de sécurité.)

En 2020, les entreprises ont démontré leur capacité de s'adapter à des changements aussi radicaux qu'un basculement généralisé vers le télétravail. Et s'il n'a pas été sans perturbations (et qu'il reste impraticable dans certains secteurs), le télétravail est aujourd'hui devenu la norme dans de nombreuses entreprises. De ce fait, les employés et leurs interlocuteurs doivent pouvoir accéder aux applications indépendamment de leur emplacement (sur site, SaaS, Cloud public) et de leur appareil (managé ou non-managé).



Dans ce contexte, le modèle Zero Trust constitue la solution idéale. Deux catégories de produits reposant sur ce modèle se sont ainsi imposées : le Zero Trust Network Access (ZTNA) et la segmentation basée sur l'identité (micro-segmentation).

Les produits du marché des ZTNA s'appuient sur les principes du Zero Trust pour gérer la mise à disposition des applications aux utilisateurs. Des utilisateurs spécifiques peuvent ainsi recevoir l'autorisation d'accès à des applications protégées, managées sur site ou dans le Cloud public, et à des applications SaaS, indépendamment du réseau sur lequel ils se connectent. Le degré d'accès est modulé en fonction du contexte entourant l'interaction, qui détermine lui-même le niveau de confiance. Ainsi, les utilisateurs d'appareils non-managés peuvent recevoir un plein accès aux applications managées traitant des données publiques, un accès en lecture seule aux applications managées traitant des données sensibles et aucun accès aux applications traitant des données confidentielles. En outre, les analyses qui combinent l'historique des comportements de l'utilisateur avec la compréhension d'une fonctionnalité spécifique de l'application sont capables de détecter et neutraliser les menaces en amont.

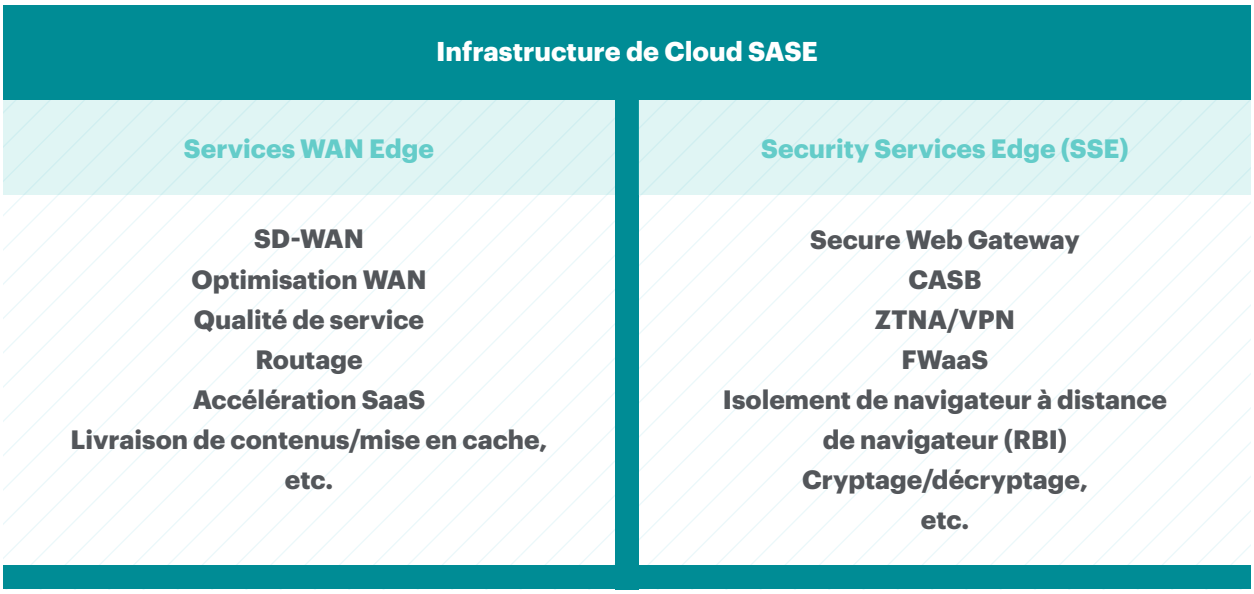
La segmentation basée sur l'identité (telle que définie par Gartner) est une nouvelle façon d'envisager la micro-segmentation. La micro-segmentation est une méthode permettant d'isoler les données grâce à une série de règles prédéterminées, qui définissent les ressources (ex. : appareil, charge de travail ou conteneur) autorisées à communiquer entre elles. La segmentation basée sur l'identité approfondit le concept, en ajoutant des règles dynamiques qui évaluent l'identité et d'autres attributs afin d'accorder ou de refuser l'accès. Les identités des ressources sont transférables et indépendantes du réseau utilisé. Associée à l'évaluation en temps réel d'éléments de contexte supplémentaires, la segmentation basée sur l'identité permet une plus grande agilité et une plus grande évolutivité du contrôle des politiques de segmentation.

Bien entendu, les modèles Zero Trust requièrent un degré supplémentaire de gestion. Les propriétaires de ressources (applications ou documents par exemple) sont responsables de bien évaluer et d'ajuster les utilisateurs autorisés à accéder à ces ressources. Ce processus est connu comme gestion des droits. Si cette gestion reste encore très manuelle, et donc propice aux erreurs, plusieurs technologies émergentes visent aujourd'hui à offrir l'automatisation tant attendue dans ce domaine. Au-delà de cette procédure de gestion, l'approche Zero Trust nécessite aussi de définir les attributs et les éléments contextuels qui détermineront ensemble le niveau de fiabilité nécessaire pour interagir avec les ressources. En effet, dans les environnements où des modèles traditionnels d'autorisation des accès ne peuvent être définis efficacement, l'ajout d'un contexte permet une évaluation plus précise de la confiance.

INTRODUCTION À L'ARCHITECTURE SASE

Les questions de sécurité sont nées avec les réseaux. Au fil des années, de nombreux outils spécialisés ont tenté de s'imposer dans les datacenters, rivalisant d'ingéniosité pour attirer l'attention des administrateurs. Et tant que les applications et les données restaient sur site et que les utilisateurs travaillaient dans des bureaux traditionnels, ils suffisaient. Certains de ces outils intégraient des mécanismes leur permettant de communiquer entre eux. Mais à mesure que les utilisateurs ont adopté le télétravail et les données et applications ont migré dans le Cloud, les outils traditionnels n'avaient plus assez de visibilité car tous supposaient que les applications, les données et les utilisateurs étaient statiques. Ce principe n'étant plus valide, les outils traditionnels ne sont désormais plus adaptés. Ils ne sont pas compatibles entre eux, sont rarement évolutifs, n'offrent pas une gestion unifiée et, c'est peut-être leur plus grand défaut, ne peuvent accomplir leur mission lorsque vos données sont stockées et traitées sur une infrastructure tierce.

L'architecture SASE, définie par Gartner en 2019, promet de surmonter les limites imposées par la multiplication des outils et des consoles. Le modèle SASE associe des fonctionnalités de réseau courantes (ex. : SD-WAN, optimisation de WAN, QoS, routage, CDN, et autres) à des fonctionnalités de sécurité courantes (ex. : SWG, CASB, ZTNA, VPN, FWaaS, RBI, et autres) dans une architecture consolidée et unifiée. Par le biais des politiques, l'ensemble des applications et services sont soumis à des contrôles d'accès, et la circulation des informations sensibles entre tous les utilisateurs et ressources est surveillée et contrôlée. SASE exécute les fonctionnalités de sécurité et de réseau à partir du Cloud, assurant une expérience homogène à tous les utilisateurs quels que soient leur emplacement et celui de leurs applications.



Source : Gartner, "2021 Strategic Roadmap for SASE Convergence," G00741491, https://www.gartner.com/document/3999828

Une bonne architecture SASE applique les principes du Zero Trust. Le modèle SASE consolide tous les modes d'accès aux ressources, sans tenir compte du mode d'autorisation des accès. Selon les principes du Zero Trust, l'autorisation d'accès et le suivi du niveau de fiabilité sont régis par un ensemble de conditions, sans tenir compte du type d'architecture technique. Lorsqu'ils sont associés, les concepts SASE et Zero Trust modifient en profondeur la façon dont les entreprises protègent leurs biens numériques. On peut considérer le SASE comme étant une excellente base pour développer un programme de Zero Trust efficace, qui englobe les environnements hybrides dans lesquels utilisateurs, applications et données peuvent être partout.

Plus globalement, et en fonction de l'éditeur, les entreprises qui adoptent une architecture SASE associée aux principes du Zero Trust devraient pouvoir :

- acquérir des connaissances sur les risques associés aux utilisateurs et applications leur permettant de déterminer le niveau de fiabilité nécessaire dans différentes conditions et d'adapter l'accès en fonction de ce facteur ;
- étendre les principes du Zero Trust au-delà des applications privées aux applications web et SaaS en fonction des connaissances acquises sur les risques, avec des politiques et des postures adaptatives ;
- exploiter les informations sur les risques au sein des applications afin de contrôler l'accès à des activités spécifiques (par exemple, un scénario à faible confiance qui permet la consultation et l'ajout de commentaires, mais interdit le partage et la suppression) ;
- activer des services de sécurité supplémentaires tels que l'isolement à distance du navigateur et la prévention optimisée des pertes de données en fonction du niveau de risque ou de confiance ;
- suivre constamment les changements de contexte qui nécessitent une réévaluation de la confiance (par exemple, réauthentification, authentification renforcée, modification des autorisations ou augmentation/réduction de l'accès) ; et
- réduire la surface d'attaque globale en écartant les protocoles et services de l'Internet public.

BÉNÉFICES POUR LES ENTREPRISES ET LES UTILISATEURS

Aujourd'hui, l'entreprise numérique ne peut se permettre d'attendre une autorisation. Pourtant, elle a de plus en plus recours à des applications et des données accessibles sur Internet (qui n'a certainement pas été conçu en pensant à la sécurité). Les entreprises peuvent atteindre leurs objectifs opérationnels sans compromettre leur sécurité en intégrant, dès le départ, les principes de la confiance adaptative et continue dans leurs programmes de sécurité et de gestion du risque, ainsi que dans leurs projets de transformation digitale.

Agilité au sein de l'entreprise

L'agilité exige un degré de souplesse des infrastructures et services, tant au niveau du volume et de sa localisation que de la diversité des nouveaux services et applications. Les résultats accessibles et probables lorsque les principes Zero Trust sont appliqués dans une architecture SASE et hybride incluent :

- Une expérience utilisateur homogène – l'accès est le même quel que soit l'emplacement de l'utilisateur et prévisible quel que soit le type d'appareil utilisé.
- Un accès indépendant de l'emplacement – l'accès aux applications est dissocié du réseau sous-jacent ; les applications peuvent être transférées (par exemple, du site au Cloud public) sans que les utilisateurs n'aient à changer leurs habitudes.
- Davantage d'opportunités d'offrir un certain degré d'accès – afin de réorienter la majorité des décisions de sécurité pour tendre vers un « oui, sous certaines conditions » plutôt qu'un « non ».
- Une collaboration renforcée avec les fournisseurs et partenaires sans avoir besoin de leur fournir de comptes d'utilisateurs locaux ni exercer de pression sur leur environnement informatique.
- Des opérations de sécurité proactives, conçues pour prendre en charge le nombre croissant d'applications et éviter d'avoir à autoriser l'accès en urgence, une fois les applications déjà déployées.

Réduction des risques

La gestion des risques cyber est une priorité pour la plupart des dirigeants. Chaque entreprise doit déterminer sa propre appétence et tolérance au risque, des éléments qui restent relativement constants au sein d'un même secteur. La gestion des risques est compliquée par la dépendance à l'égard de chaînes d'approvisionnement de plus en plus longues et opaques, la prolifération des services et applications cloud et un cadre réglementaire ambigu. Limiter les risques dans ce nouvel environnement impliquera d'adopter une approche Zero Trust dans laquelle :

- Les ressources passent d'un accès public à un accès privé, et sont de ce fait protégées des dangers d'Internet et invisibles à ceux qui ne disposent pas d'une habilitation robuste ou ne sont pas en mesure de démontrer un niveau suffisant de fiabilité.
- Les accès non autorisés sont contenus, de manière à réduire le rayon de propagation des comptes affectés.
- La visibilité sur les types des données sensibles, leurs emplacements et leurs mouvements est renforcée et constante.
- Les analyses offrent un panorama complet des politiques et comportements acceptables, faisant ainsi émerger plus rapidement les risques et les menaces (à la fois issues des activités anormales ou malveillantes) de manière à les contenir et les neutraliser rapidement.
- Le dispositif de sécurité global étant renforcé, les entreprises sont devenues des cibles moins attrayantes pour les hackers.

Processus optimisé de déploiement et de maintenance des produits

L'agilité et la réduction des risques nécessitent une architecture adaptée, y compris :

- Un service de sécurité cloud-native qui évolue selon les besoins de l'entreprise, en éliminant les difficultés de déploiement et les contraintes de capacité généralement associées aux appareils de sécurité.
- Une plateforme cloud unique, une inspection en un seul passage et un point unique d'application des politiques, contrôlés par un moteur de stratégie doublé d'une console d'administration en vue d'assurer l'homogénéité de la politique de sécurité sur tous les canaux.
- En travaillant avec un seul fournisseur, on élimine les retards qui accompagnent généralement le dépannage et la réparation de produits dont les caractéristiques d'interopérabilité n'ont pas été testées ou sont inconnues.

CINQ PHASES POUR INSTAURER UNE CONFIANCE ADAPTATIVE ET CONTINUE AVEC NETSKOPE

Netskope aide les entreprises à atteindre leurs objectifs en matière de stratégie de confiance adaptative et continue. Le processus ne sera pas forcément le même pour toutes les entreprises. Votre secteur, votre degré d'adoption du Cloud et vos systèmes existants détermineront non seulement le point de départ de ce processus, mais également les efforts nécessaires.

Quelques étapes simples peuvent cependant aider chaque entreprise à se préparer. Commencez par ces tâches :

- Imaginez une série d'utilisateurs types qui reflètent les divers rôles au sein de votre entreprise. Répertoriez les besoins d'accès généralement associés à chaque utilisateur type. Ignorez les définitions d'accès existantes pour chacun des postes et repartez de zéro.
- Répertoriez toutes les applications privées et applications SaaS. Cartographiez les interactions des applications et de leurs composants, aussi bien entre eux qu'avec des ressources externes à l'entreprise.
- Identifiez toutes les données : leurs emplacements, niveaux de sensibilité, fonctions opérationnelles et durées de vie prévues.

Pour être efficace, un projet de confiance adaptative et continue doit être accompagné d'un programme robuste de gestion des identités et des accès. Sans un système fiable et précis d'enregistrement des identités, il est impossible de déterminer ou présumer d'un niveau élevé de confiance. Chaque entité – qu'il s'agisse d'une personne, d'un appareil ou d'un objet – doit présenter une identité que toutes les autres entités peuvent valider. Heureusement, la plupart des entreprises ont déjà les bases d'un système de gestion des identités. Pour une approche Zero Trust, il est crucial que ce système soit compatible avec des protocoles standards tels que SAML, OIDC et OAuth, puisque cela correspond aux attentes de la plupart des organisations. La fédération d'identités établit un degré de confiance entre des domaines d'identités disparates, permettant aux utilisateurs d'un domaine d'accéder à des ressources autorisées d'autres domaines sans avoir à utiliser différentes identités.

Avec ces informations en main, vous pouvez commencer à planifier et exécuter les cinq phases détaillées sur la page suivante.

PHASE 0 — Avant de commencer

- Définir les utilisateurs types et assigner les privilèges d'accès
- Répertorier toutes les applications privées et SaaS
- Répertorier toutes les données

PHASE 1 — Accès Zero Trust

- Identifier une source fiable d'identités
- Cartographier les utilisateurs et les applications
- Supprimer les droits obsolètes ou non utilisés
- Orienter tous les accès vers un point d'application de la politique afin d'éliminer les risques d'accès direct

Établir un référentiel de confiance

PHASE 2 — Accès adaptatif

- Ajouter un contexte aux politiques d'accès
- Laisser le contexte signaler le besoin d'une authentification forte
- Prendre en compte le contexte pour le coaching
- Ajuster continuellement les politiques d'accès

Enrichir le référentiel de sécurité avec les autorisations dans les activités applicatives

PHASE 3 — Isolement à la demande

- Insérer un isolement à distance du navigateur pour l'accès aux sites web à haut risque et de mauvaise réputation
- Détecter les attaques de type « commande et contrôle » et autres comportements anormaux

Appliquer des contrôles de confiance explicite aux destinations

PHASE 4 — Protection des données en continu

- Distinguer les accès par des appareils managés et non-managés
- Adapter les politiques d'accès en fonction du contexte
- Veiller à la configuration optimale des ressources cloud
- Identifier les informations sensibles et contrôler leur diffusion
- Évaluer permissions de partage et intégrations A2A en continu

Examinez constamment les accès et supprimez ceux relevant d'un excès de confiance. Adoptez un modèle d'accès à privilèges minimums et appliquez-le en toutes circonstances.

PHASE 5 — Informer et ajuster grâce aux analyses en temps réel

- Conserver une bonne visibilité sur les applications et les risques
- Inspecter l'activité cloud et web afin d'évaluer et d'ajuster les politiques au mieux
- Créer des visualisations adaptées aux différentes parties prenantes
- Peaufiner les politiques en boucle fermée

Renforcez votre posture de sécurité et de confiance avec un examen des politiques en circuit fermé.

PHASE 1

Accès Zero Trust : proscrivez les accès anonymes

Commencez à établir le contexte dès le premier point d'accès. Pour cela, consolidez la gestion des accès et des identités (y compris les rôles et leurs affiliations), la détection d'applications privées, et une liste des catégories de sites web et applications SaaS approuvées. Réduisez les possibilités de mouvements latéraux et protégez vos applications contre le *fingerprinting*, le balayage des ports et la recherche de vulnérabilités. Mettez en place un processus d'authentification unique (SSO) avec authentification multifactorielle (MFA).

Netskope Security Cloud permet de mettre en place une SSO fédérée avec des contrôles d'accès adaptatifs aux sites web, applications privées, et milliers d'applications SaaS, y compris celles relevant du Shadow IT adoptées par les différentes unités opérationnelles. Netskope Private Access dispose de fonctionnalités complètes de ZTNA, de la détection des applications privées à l'accès applicatif pour les utilisateurs managés ou les contractants, sans compter les cas de fusion-acquisition. En tant que point de contrôle d'accès au Web et aux applications SaaS, la solution Next Generation Secure Web Gateway (NG SWG) de Netskope peut neutraliser les attaques de type phishing ou autre en vérifiant les identifiants pour les applications SaaS, le webmail et le stockage cloud, soit les principales sources de menaces pour les entreprises d'aujourd'hui.

Tâches spécifiques à cette phase :

- Identifiez une source fiable pour la vérification des identités et déterminez les autres sources d'identité avec lesquelles la fédération est possible.
- Déterminez lorsqu'une authentification renforcée est nécessaire.
- Constituez et entretenez une base de données qui mappe les utilisateurs (employés et tiers) aux applications. Des entretiens réguliers avec les unités opérationnelles seront nécessaires. Désignez un groupe d'individus auxquels confier cette responsabilité.
- Rationalisez l'accès aux applications en supprimant les privilèges (d'employés ou de tiers) devenus superflus du fait de changements de postes, départs, résiliations de contrats, etc.
- Supprimez la connectivité directe en orientant tous les accès vers un point d'application des politiques pour chaque application privée ou interne (ZTNA) et pour chaque accès aux applications SaaS et au Web (CASB, SWG).
- Créez des graphiques et un tableau de bord actualisés en temps réel des applications et utilisateurs. Déterminez les accès recommandés pour chaque utilisateur sur chaque application et service.

PHASE 2

Accès adaptatif : maintenez un modèle de confiance explicite

Ajoutez des éléments contextuels supplémentaires pour renforcer l'adaptabilité des contrôles en vue de maintenir un modèle de confiance explicite. Évaluez les signaux dans les évaluations de risques applicatifs, les évaluations de risques utilisateurs, les contrôles de posture aux terminaux, ainsi que les emplacements des utilisateurs, applications et données. Mettez en place des politiques adaptatives qui déclenchent l'authentification par étapes, alertent l'utilisateur pour qu'il indique s'il souhaite poursuivre ou annuler l'activité d'une application, justifient la poursuite de l'activité ou l'orientent en temps réel vers des applications autorisées.

Netskope Security Cloud donne un contexte riche pour l'ensemble du trafic cloud et web inspecté, et affiche des informations en temps réel sur les risques applicatifs, les scores d'évaluation des risques utilisateurs et des informations de l'analyse UEBA, dans le temps et basé sur le comportement utilisateur. Ces scores activent différentes actions adaptatives en temps réel, telles que l'authentification renforcée, la cessation des processus et bien plus, en fonction des politiques souhaitées pour les utilisateurs, les données ou les applications.

Tâches spécifiques à cette phase :

- Définissez comment déterminer si un appareil est managé.
- Ajoutez des éléments contextuels aux politiques d'accès (bloquer, autoriser en lecture seule ou autoriser certaines activités en fonction de plusieurs conditions).
- Utilisez davantage l'authentification forte lorsque le risque environnemental est élevé (par exemple, pour tous les accès à distance aux applications privées et aux SaaS afin de supprimer le contenu) et diminuez son utilisation lorsque le risque est faible (par exemple, les appareils managés accédant aux applications locales en lecture seule).
- Évaluez le risque utilisateur, orientez certaines catégories d'utilisateurs vers des catégories d'applications spécifiques.
- Ajustez continuellement les politiques afin de refléter les nouvelles exigences opérationnelles à mesure que les applications évoluent, apparaissent ou disparaissent.
- Établissez un référentiel de confiance pour les autorisations au sein des activités applicatives.

PHASE 3

Isolement à la demande : contenez le rayon de propagation

Dissociez les navigateurs des applications et appliquez les contrôles au trafic sortant. Déployez un dispositif d'isolement de navigateur à distance (RBI) afin de limiter la fonctionnalité du navigateur à celle d'un dispositif d'affichage. Activez un pare-feu sur appareil pour limiter les destinations auxquelles l'appareil peut se connecter.

La solution d'isolement de navigateur à distance (RBI) de Netskope est native, fonctionne en un seul passage et s'intègre aux capacités de protection des données et de neutralisation des menaces existantes. En outre, elle offre un niveau de performance supérieur aux produits RBI traditionnels, dont la chaîne de services est liée à des proxys ou des passerelles. Toujours dans l'optique d'abolir la confiance implicite, l'accès direct aux ressources à risque sur le Web doit être minimisé, notamment lorsque les utilisateurs interagissent simultanément avec des applications managées.

L'isolement à la demande – soit un isolement qui s'insère automatiquement en cas de conditions de risque élevé – limite le rayon de propagation des utilisateurs affectés et des sites web à risque. En outre, Netskope Cloud Firewall est un mécanisme de pare-feu extrêmement performant, qui permet de neutraliser les tentatives de communication avec les nœuds « commande et contrôle » détenus par le hacker.

Tâches spécifiques à cette phase :

- Insérez automatiquement un isolement à distance du navigateur dans le chemin d'accès vers les sites web à haut risque ayant mauvaise réputation.
- Configurez un isolement à distance du navigateur pour les accès aux applications privées à partir d'appareils non-managés.
- Envisagez un dispositif d'isolement à distance du navigateur en tant qu'alternative au proxy inverse CASB pour les applications SaaS au comportement défectueux lors de la réécriture d'URL.
- Surveillez les tableaux de bord des menaces et utilisateurs actualisés en temps réel afin de détecter les anomalies et les attaques de type « commande et contrôle » (C2).

PHASE 4

Protection des données en continu : mettez en place des politiques de protection des données en un seul passage

Gagnez en visibilité en matière d'emplacement et de diffusion des données sensibles. Surveillez et contrôlez le mouvement des informations sensibles par le biais d'applications SaaS approuvées et non-approuvées, sites web, stockage dans le Cloud public, applications personnalisées dans le Cloud public et e-mails sortants. Appliquez des politiques de protection des données en un seul passage à travers l'ensemble du trafic inspecté dans le Cloud, les e-mails et le Web pour les données en mouvement, et par le biais des API pour les données inactives.

Netskope Security Cloud permet de maîtriser les déplacements de données accidentels et non approuvés, et délivre une analyse complète de l'activité des données inspectées. Les systèmes de défense traditionnels ne sont pas en mesure de décoder le trafic cloud et, de ce fait, sont incapables de protéger les données correctement, notamment pour les instances personnelles d'applications approuvées ou non-approuvées. Netskope Cloud Firewall-as-a-Service (FWaaS) assure un contrôle d'accès sur tous les ports et protocoles du réseau sortant pour les utilisateurs distants et les succursales, atténuant le risque d'attaques de type « commande et contrôle » et l'exfiltration de données.

Tâches spécifiques à cette phase :

- Définissez une stratégie globale de différentiation pour l'accès aux données à partir d'appareils managés et non-managés.
- Ajoutez des éléments adaptatifs à votre politique afin d'autoriser l'accès au contenu en fonction du contexte (par exemple, plein accès au contenu public sur les appareils non-managés, accès en lecture seule au contenu sensible sur les appareils non-managés, accès bloqué au contenu confidentiel sur les appareils non-managés).
- Mettez en place une solution de gestion de la posture de sécurité du cloud (CSPM) pour évaluer en permanence les configurations des services de cloud public afin de protéger les données et de respecter les règles de conformité.
- Évaluez l'utilisation des politiques et règles DLP inline pour le Web, les applications SaaS managées, le Shadow IT, les services de Cloud public et les e-mails de manière à protéger vos données et satisfaire aux exigences de conformité.
- Définissez les politiques et règles DLP applicables aux données inactives dans les environnements IaaS et SaaS managés, notamment les permissions de partage de fichiers pour le stockage d'objets dans le Cloud et les intégrations d'application à application (A2A) permettant le partage et le déplacement de données.
- Affinez les politiques en ajoutant éventuellement des attributs d'utilisateurs ou de groupes.
- Examinez constamment les accès et supprimez ceux relevant d'un excès de confiance. Adoptez un modèle d'accès à privilèges minimums et appliquez-le en toutes circonstances.

PHASE 5

Visualisations et analyses en temps réel : maintenez une posture de confiance et de sécurité robuste

Enrichissez et affinez les politiques en temps réel. Évaluez la pertinence et l'efficacité des politiques existantes en fonction des tendances utilisateurs, des anomalies d'accès, des modifications aux applications et de l'évolution de la sensibilité des données. Ajustez les politiques en conséquence, de façon à tolérer l'exposition aux risques tout en restant dans les limites.

Les fonctionnalités de visualisation et d'analyse en temps réel de Netskope donnent un aperçu des activités du Netskope Security Cloud, en identifiant les utilisateurs qui devraient être autorisés (ou non) à travailler sur les données de l'entreprise dans un ensemble donné d'applications. Ces fonctionnalités travaillent à l'unisson avec les équipes de sécurité opérationnelle, de réseau et d'intelligence des menaces, et permettent d'expliquer clairement les résultats du programme de sécurité aux décideurs et parties prenantes des applications. Les informations dérivées des analyses aident les organisations à planifier leur programme de sécurité, anticiper les évolutions et prévoir les étapes à mettre en place.

Tâches spécifiques à cette phase :

- Conservez une visibilité des applications et services qu'utilise l'entreprise, et des niveaux de risque associés.
- Déterminez qui aura accès aux ressources privées et réduisez-en l'accès au minimum afin de limiter l'exposition aux risques.
- Gagnez en visibilité et en compréhension quant à l'activité de vos utilisateurs sur le Cloud et le Web, de manière à ajuster continuellement et à monitorer les politiques des données et menaces.
- Identifiez les principales parties prenantes au sein de votre programme de gestion des risques et de la sécurité (CISO/CIO, service juridique, CFO, SecOps, etc.) et créez des graphiques qui sont faciles à comprendre.
- Créez des tableaux de bord pour gagner en visibilité sur ces points : site, application, instance, utilisateur, activité, fichier source/destination et plus.
- Assurez-vous de pouvoir importer et exporter les tableaux de bord afin de collaborer avec d'autres équipes de sécurité.
- Renforcez votre posture de sécurité et de confiance avec un examen des politiques en circuit fermé.

La transformation numérique a été accélérée par les événements de 2020, poussant les entreprises à envisager de restructurer leurs programmes et leurs infrastructures de réseau et sécurité afin de répondre aux besoins actuels. Une nouvelle approche est clairement nécessaire pour assurer une expérience rapide et fluide aux utilisateurs, avec des contrôles de gestion des risques simples et efficaces à travers les architectures hybrides et multi-cloud.

Avec Netskope, les utilisateurs sont connectés à Internet, à toutes leurs applications et à leur infrastructure, rapidement et en toute sécurité, depuis n'importe quel appareil, dans ou hors du réseau. Grâce à notre technologie brevetée et le CASB, le proxy et le ZTNA intégrés au sein d'une seule plateforme, Netskope Security Cloud donne le contexte le plus spécifique. Il fournit un accès conditionnel et favorise la sensibilisation des utilisateurs tout en appliquant les principes Zero Trust aux solutions de protection des données et de prévention des menaces et ce à tous les niveaux. Le Cloud privé de sécurité globale de Netskope offre des capacités de calcul complètes à la périphérie du réseau, afin de construire un réseau global fiable à haute performance et extrêmement sécurisé.