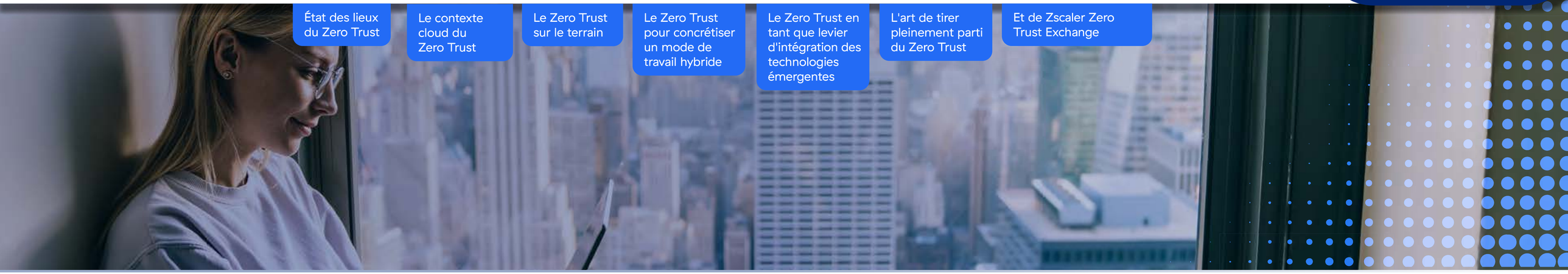
État des lieux 2023 du Zero Trust

DE LA PRÉVENTION À LA MISE EN ŒUVRE :
Tirer pleinement parti du Zero Trust pour les entreprises orientées mobilité et cloud.

Sommaire



Synthèse décisionnelle

Nathan Howe | VP, Technologies émergentes et 5G, Zscaler

Dans un contexte d'accélération de la transformation digitale, le Zero Trust s'est imposé pour sécuriser les utilisateurs, les instances et les dispositifs, au sein des entreprises multisites et orientées mobilité & cloud.

Les professionnels IT du monde entier en prennent conscience, à mesure que le Zero Trust se généralise et remet en question les principes traditionnels de la sécurité et du réseau, en vigueur depuis des décennies.

Plus de 90 % des professionnels IT qui ont initié leur migration vers le cloud ont déjà mis en œuvre une stratégie de sécurité Zero Trust ou sont en passe de le faire dans l'année à venir.

C'est ce que révèlent les résultats de notre dernière enquête mondiale, menée auprès de plus de 1 900 DSI, RSSI, CDO (Chief Data Officer), CTO et Directeurs en charge de l'infrastructure, tous évoluant au sein d'entreprises qui ont déjà entamé la migration d'applications et de services vers le cloud.

Ce chiffre est encourageant et optimiste quant au déploiement d'une architecture Zero Trust au-delà des 12 prochains mois.

22 %

Seuls 22 % des personnes interrogées sont convaincues que leur entreprise tire pleinement parti du potentiel de leur infrastructure cloud, un chiffre qui montre qu'il est nécessaire de penser au-delà de la sécurité simplement.

En effet, au fur et à mesure de la migration vers le cloud, les avantages du Zero Trust en matière de sécurité sont plus clairs. Plus des deux tiers (68 %) des responsables/décisionnaires IT conviennent que la transformation sécurisée du cloud est impossible avec une infrastructure de sécurité réseau traditionnelle. Ils estiment également que l'accès réseau Zero Trust présente des avantages évidents par rapport aux pare-feu et VPN traditionnels pour sécuriser l'accès à distance aux applications.

Mais avec seulement 22 % du panel qui affirme que leur entreprise exploite pleinement le potentiel de leur infrastructure cloud, il es important de ne pas s'arrêter à la sécurité. Dans une perspective IT globale, le Zero Trust crée de multiples opportunités dans le cade du processus global de digitalisation. Oui, cette discipline prévient les attaques de cybersécurité à grande échelle, mais peut en faire beaucoup plus : stimuler l'innovation, renforcer l'engagement des collaborateurs ou encore concrétiser des économies financières tangibles.

Alors que les entreprises s'efforcent d'offrir un nouvel environnement de travail moderne (hybride dans son approche et reposant sur une multitude de technologies émergentes telles que l'IoT/OT, la 5G, voire le métavers), elles doivent élargir leur vision du Zero Trust et de leur transformation digitale. Une plateforme Zero Trust a le pouvoir de redéfinir les exigences en matière d'infrastructure métier et organisationnelle : elle devient un moteur business qui permet aux entreprises d'offrir le modèle de travail hybride que leurs collaborateurs appellent de leurs vœux, mais aussi de devenir des entreprises digitalisées bénéficiant de nombreux avantages : agilité, productivité ou encore pérennité de leur infrastructure.

Nous avons commandité cette étude pour dresser un état des lieux de la transformation Zero Trust au sein des entreprises. Les résultats sont encourageants avec un taux de déploiement du Zero Trust élevé. Pour autant les objectifs de ces déploiements gagneraient à être plus ambitieux. Les responsables IT ont l'opportunité incroyable de sensibiliser les décisionnaires métiers aux principes du Zero Trust et de présenter cette discipline en tant que catalyseur business de valeur. Il s'agit du chaînon manquant qui aide les entreprises, dès à présent, à adopter et se préparer aux technologies futures.

ÉTAT DES LIEUX DU ZERO TRUST

90 % Plus de 90 % des entreprises qui ont initié leur migration vers le cloud disposent déjà d'une stratégie de sécurité Zero Trust en place, ou sont en passe de le faire dans les 12 prochains mois.

88 % Globalement, 88 % des responsables IT sont relativement convaincus que leur entreprise exploite au mieux le potentiel de leur infrastructure cloud, mais seuls 22 % d'entre eux en sont totalement convaincus.

AU NIVEAU RÉGIONAL, LA PART DE CEUX QUI SONT CERTAINS D'EXPLOITER TOUT LE POTENTIEL DU CLOUD EST COMME SUIT :

#1 Le ZTNA est la priorité n°1 des investissements en technologie Zero Trust au cours des 12 prochains mois, ce qui démontre l'importance de l'accès à distance pour accompagner un mode de travail hybride.

68 % Plus de deux tiers (68 %) des responsables IT conviennent qu'une adoption sécurisée du cloud est impossible avec une infrastructure de sécurité réseau traditionnelle. Il estiment également que l'accès réseau Zero Trust (ZTNA) présente des avantages évidents par rapport aux pare-feu et VPN traditionnels pour sécuriser l'accès distant aux applications.

54 % des responsables IT affirment qu'ils considèrent les VPN ou les pare-feu en périphérie de réseau inefficaces pour assurer une protection contre les cyberattaques ou pour fournir une visibilité sur le trafic des applications et sur les attaques.

LES PRINCIPAUX OBSTACLES À L'EXPLOITATION DU PLEIN POTENTIEL DU CLOUD :

45 % Difficultés à sécuriser les données dans le cloud et préoccupations relatives à la confidentialité des données

42 % Complexité du réseau et difficulté à faire évoluer les outils matériels de sécurité

40 % Accès tiers et à distance à l'IoT et OT

33 % Connectivité aléatoire expérience utilisateur médiocre pour les accès distants

EN DEHORS DE LA SÉCURITÉ, DE L'ACCÈS ET DE LA COMPLEXITÉ, LES PRINCIPALES RAISONS QUI INCITE,T À LA MISE EN ŒUVRE D'UNE ARCHITECTURE ZERO TRUST NE SONT PAS STRATÉGIQUES POUR LES ENTREPRISES :

65 % Améliorer la détection des menaces avancées ou des attaques sur applications Web et élargir la sécurité pour les données sensibles

44 % Sécuriser l'accès à distance pour les fournisseurs, les partenaires et les technologies industrielles OT

27 % Assurer une connectivité plus sécurisée pour les collaborateurs travaillant en mode hybride

24 % Maîtriser les coûts et la complexité de la sécurité réseau traditionnelle

Section I

Le contexte cloud de l'adoption du Zero Trust

Lorsque nous faisons référence au « cloud » dans le cadre de cette enquête, nous parlons d'applications, de données et d'instances fournies en tant que services à partir d'Internet, en lieu et place d'un data center local au sein d'un réseau d'entreprise. Il s'agit notamment du SaaS (Software-as-a-Service), de l'IaaS (Infrastructure-as-a-Service), du PaaS (Platform-as-a-Service) ou d'applications privées conçues ou hébergées dans le cloud.

Avant de nous pencher sur les spécificités du Zero Trust, nous souhaitions définir le contexte de son adoption, examiner les tendances de l'univers IT au sens large, et, plus précisément, où en sont les entreprises dans leur migration vers le cloud.

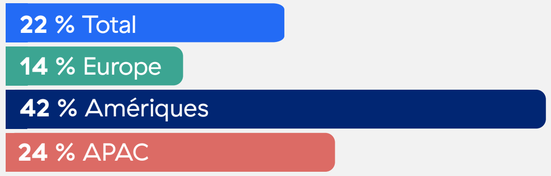
Il ne fait aucun doute que les événements de ces dernières années ont accéléré le passage au cloud.

Dans de nombreuses entreprises, le processus est déjà bien engagé, voire achevé.

Nous avons interrogé de plus de 1 900 DSI, RSSI, CDO, CTO et Directeurs en charge de l'infrastructure dans le monde entier, issus d'entreprises qui ont déjà migré des applications et services vers le cloud. Près de la moitié d'entre eux (46 %) a déclaré que le processus de migration était entièrement achevé.

Mais alors que 88 % des décisionnaires IT sont relativement convaincus de tirer le meilleur parti de leur migration vers le cloud, seuls 22 % sont tout à fait convaincus que leur entreprise exploite aujourd'hui le plein potentiel du cloud.

PERSONNES INTERROGÉES QUI SONT CONVAINCUES QUE LEUR ENTREPRISE EXPLOITE ACTUELLEMENT LE PLEIN POTENTIEL DE L'INFRASTRUCTURE CLOUD



% DES PERSONNES INTERROGÉES QUI DÉCLARENT ÊTRE TRÈS CONFIANTES QUE LEUR ENTREPRISE EXPLOITE ACTUELLEMENT LE PLEIN POTENTIEL DE L'INFRASTRUCTURE CLOUD

Survolez les pays pour plus d'infos.

Europe :

- 9 % Allemagne
- 11 % France
- 11 % Espagne
- 19 % Royaume-Uni

Région Amériques :

- 41 % États-Unis
- 51 % Brésil

APAC :

- 16 % Singapour
- 55 % Inde

Les disparités régionales révèlent que les décisionnaires IT européens sont ceux qui émettent le plus de doutes sur leur utilisation de l'infrastructure cloud, avec seulement 14 % d'entre eux exprimant une confiance totale. Sur les Amériques, ce chiffre grimpe à 42 %.

Bien qu'il n'existe aucune origine unique et claire à cette disparité, une des raisons potentielles pourrait tenir aux différences interculturelles dans la vitesse d'adoption des technologies innovantes, l'Europe adoptant traditionnellement une approche plus prudente et mettant davantage l'accent sur la confidentialité des données. De plus, compte tenu de l'infrastructure de connectivité bien établie de l'Europe et de sa forte orientation vers le secteur industriel, la volonté d'adopter immédiatement des innovations telles que la 5G est moindre et la modification des processus opérationnels en place prend plus de temps. Comme nous le découvrirons plus en détail dans une prochaine section, les entreprises de la zone Amériques ont plus d'appétence pour les technologies émergentes, telles que l'intelligence artificielle, l'apprentissage automatique et la réalité augmentée. Ceci laisse penser que des plans sont déjà en place pour que l'infrastructure cloud prenne en charge des cas d'utilisation plus sophistiqués.

Mais plus généralement, pourquoi les entreprises ont-elles eu du mal à exploiter le plein potentiel du cloud ?

À première vue, la sécurité apparaît comme le principal frein, les responsables IT ayant présenté deux raisons liées à la sécurité pour répondre à cette question :

PRINCIPAUX FREINS À L'EXPLOITATION DU PLEIN POTENTIEL DU CLOUD

45 % Inquiétudes concernant la confidentialité des données et difficultés à sécuriser les données dans le cloud

42 % Complexité d'adaptation du réseau et sécurité réseau peu évolutive

40 % Défis liés aux accès des tiers et l'accès à distance aux systèmes IoT et OT

33 % Connectivité aléatoire et expérience utilisateur médiocre pour les accès à distance

LES PRINCIPAUX OBSTACLES À L'EXPLOITATION DU PLEIN POTENTIEL DU CLOUD, PAR PAYS

Survolez les pays pour plus d'infos.

En Europe et dans la région APAC, les préoccupations relatives à la confidentialité des données dominent :

- 36 % Espagne
- 34 % Inde
- 33 % Italie
- 32 % Australie
- 28 % France

Sur le continent américain, les entreprises font face à des défis de sécurité des données dans le cloud :

- 44 % Brésil
- 30 % États-Unis

De leur côté, Singapour et le Japon peinent à faire évoluer le matériel de sécurité du réseau :

- 41 % Singapour
- 30 % Japon

Dans un environnement cloud, la surface d'attaque augmente de manière exponentielle : chaque service, utilisateur et appareil connecté à Internet devient un point d'entrée potentiel, une passerelle d'entrée vulnérable qui doit être sécurisée contre les menaces.

Et les entreprises ont de bonnes raisons de s'inquiéter. Dans un environnement cloud, la surface d'attaque augmente de manière exponentielle : chaque service, utilisateur et appareil connecté à Internet devient un point d'entrée potentiel, une passerelle d'entrée vulnérable qui doit être sécurisée contre les menaces. Nous reviendrons sur ce sujet dans la prochaine section.

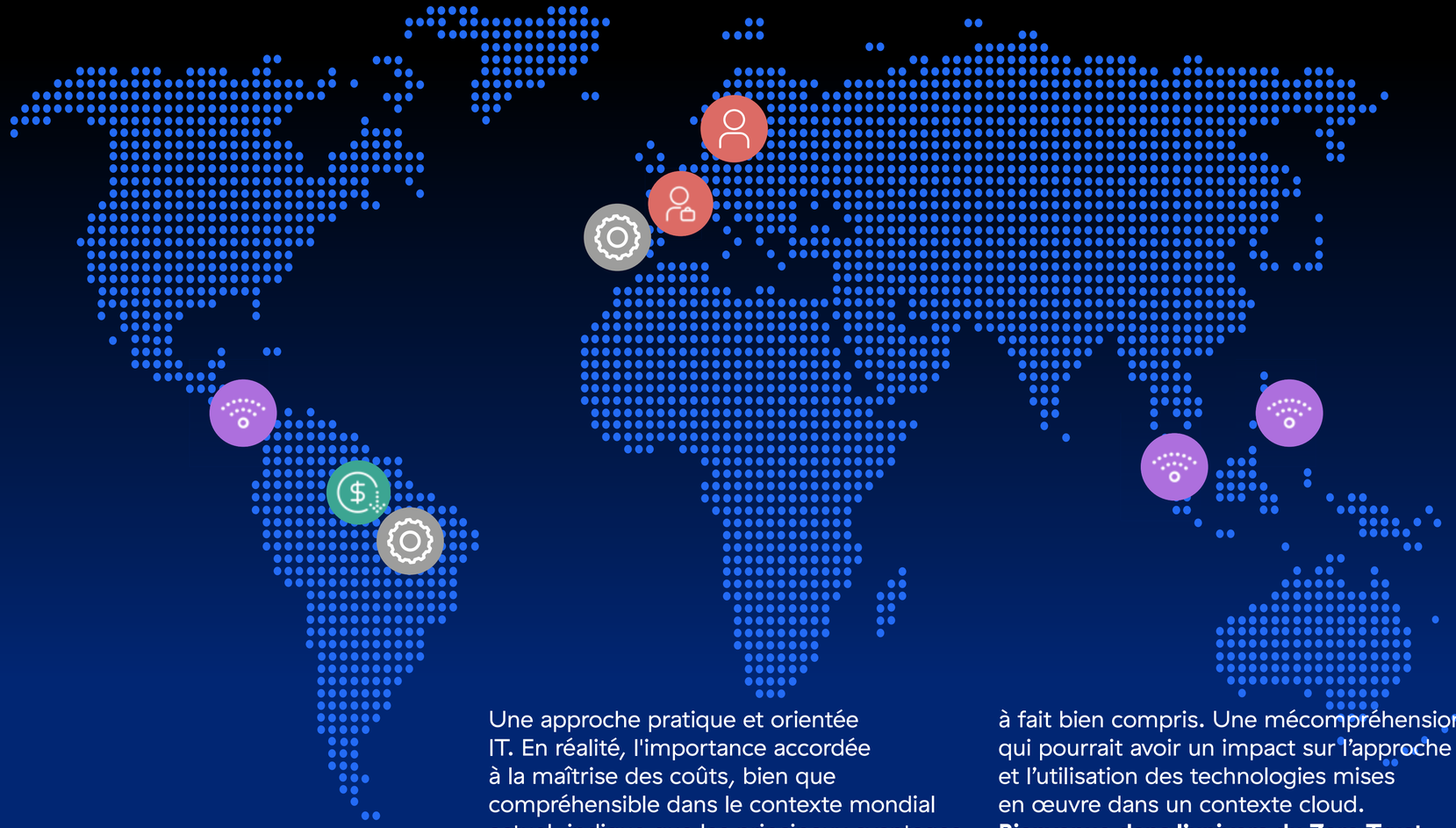
Cependant, un examen des motivations qui sous-tendent les migrations vers le cloud met en évidence un frein beaucoup plus fondamental dans la façon dont les responsables IT considèrent le cloud, un frein qui impacte sans doute l'efficacité de l'utilisation du cloud. Lorsque interrogés sur les principaux facteurs qui motivent les projets de transformation numérique au sein de leur entreprise, les décisionnaires IT mettent en exergue trois réponses : maîtriser les coûts, encourager l'innovation technologique et gérer les risques de cybersécurité.

PRINCIPAUX FACTEURS QUI MOTIVENT LES PROJETS DE TRANSFORMATION NUMÉRIQUE SELON LES RESPONSABLES IT :

- Réduire **les coûts de l'infrastructure** IT
- Encourager les innovations telles que **la 5G et l'Edge Computing**
- Maîtriser **les risques de** cybersécurité
- Gérer les **environnements multicloud**
- Améliorer la capacité à recruter et à fidéliser les **meilleurs talents**

LES PRINCIPAUX FACTEURS QUI MOTIVENT LES PROJETS DE TRANSFORMATION NUMÉRIQUE, PAR PAYS

Survolez les pays pour plus d'infos.



Le Brésil s'aligne sur le consensus mondial, la plupart des entreprises mentionnant la réduction des coûts d'infrastructure informatique comme un objectif principal.

En revanche, il en va autrement dans certains pays européens. En France, les entreprises sont principalement préoccupées par la mise en place d'un mode de travail hybride, tandis que la Suède a pour priorité l'expérience utilisateur.

Encourager les innovations à l'instar de la 5G et l'Edge Computing se révèle plus important dans les pays plus avant-gardistes que sont le Japon, le Mexique et Singapour. La croissance du chiffre d'affaires est tout autant une priorité à Singapour.

L'optimisation des processus métiers figure également dans le top 3 des priorités métiers au Brésil et en Espagne.

Une approche pratique et orientée IT. En réalité, l'importance accordée à la maîtrise des coûts, bien que compréhensible dans le contexte mondial actuel, indique que les principaux avantages du cloud ne sont peut-être encore tout à fait bien compris. Une mécompréhension qui pourrait avoir un impact sur l'approche et l'utilisation des technologies mises en œuvre dans un contexte cloud. **Bienvenue dans l'univers du Zero Trust.**


Il ne fait aucun doute
que les événements de
ces dernières années ont
accéléré l'adoption du cloud

Section II

Le Zero Trust sur le terrain

Zero Trust, une approche holistique de la sécurisation des entreprises modernes, repose sur 2 idées fondamentales : un accès basé sur le principe du moindre privilège et le principe selon lequel aucun utilisateur ou application ne devrait être intrinsèquement considéré comme étant de confiance. Le Zero Trust mise sur l'hypothèse que tout objet sur le réseau est malveillant. La confiance n'est accordée qu'en fonction de l'identité de l'utilisateur et du contexte d'accès. La politique de sécurité et ses règles régissent chaque étape du processus. Aux États-Unis, le National Institute of Standards and Technology (NIST) définit le principe directeur d'une architecture Zero Trust comme suit : « aucune confiance implicite accordée aux ressources ou aux comptes d'utilisateurs sur la seule base de leur emplacement physique ou de leur réseau (c'est-à-dire les réseaux locaux par opposition à Internet), ou sur la base de la propriété des ressources (ressource d'entreprise ou personnelle) ». Il s'agit donc de « Ne jamais faire confiance. Toujours vérifier ».

La sécurité, l'accès et la complexité étant les principales préoccupations des responsables IT en matière de cloud, il n'est guère surprenant que les entreprises soient toujours plus nombreuses à s'intéresser au Zero Trust en tant que lever ces freins. Les réponses à l'enquête indiquent que les entreprises ont une bonne compréhension de base des avantages de Zero Trust en matière de sécurité, par rapport aux approches plus traditionnelles dans ce nouvel environnement opérationnel.

Interrogés sur l'infrastructure traditionnelle de réseau et de sécurité, 54 % des responsables IT affirment qu'ils considèrent les VPN ou les pare-feu en périphérie de réseau comme peu efficaces pour assurer une protection contre les cyberattaques et fournir une visibilité sur le trafic des applications et les attaques. Par ailleurs, 68 % reconnaissent qu'en matière d'accès distant sécurisé aux applications, l'accès réseau Zero Trust (ZTNA) présente des avantages évidents par rapport aux pare-feu et VPN traditionnels, ou que la sécurisation du cloud ne peut être optimale avec une infrastructure de sécurité réseau traditionnelle.

Survolez les pays pour plus d'infos.

Personnes interrogées qui conviennent que la sécurisation du cloud est impossible avec une infrastructure de sécurité réseau traditionnelle et que l'accès réseau Zero Trust présente des avantages évidents par rapport aux pare-feu et VPN traditionnels en matière d'accès distant sécurisé aux applications.

- 85 % Inde
- 81 % États-Unis
- 75 % Brésil
- 75 % Singapour
- 73 % Suède

Personnes interrogées qui conviennent que les VPN ou les pare-feu de périmètre sont soit inefficaces pour assurer une protection contre les cyberattaques ou qu'ils peinent à fournir une visibilité sur le trafic des applications et les attaques :

- 72 % Inde
- 65 % Singapour
- 64 % Japon
- 57 % Allemagne
- 56 % États-Unis

Personnes interrogées qui conviennent qu'en plus de la sécurité, les équipes IT ont besoin d'outils intégrés pour analyser, dépanner et résoudre efficacement les problématiques d'expérience utilisateur :

- 70 % Inde
- 63 % Mexique
- 62 % États-Unis
- 56 % Singapour
- 51 % Espagne
- 50 % Japon

90 %

Plus de 90 % des personnes interrogées et ayant initié leur migration vers le cloud ont déjà mis en œuvre une stratégie de sécurité Zero Trust, ou sont en passe de le faire sur les 12 prochains mois.

Au-delà de cette prise de conscience, ils agissent en conséquence ce qui s'avère prometteur. Plus de 90 % des personnes interrogées et ayant initié leur migration vers le cloud ont déjà mis en œuvre une stratégie de sécurité Zero Trust, ou sont en passe de le faire sur les 12 prochains mois.

L'Italie et l'Inde sont en pole position dans la mise en œuvre d'une stratégie de sécurité Zero Trust. 97 % des entreprises italiennes et 96 % des entreprises indiennes confirment qu'elles disposent déjà d'une telle stratégie en place, ou qu'elles s'apprêtent à en déployer une.

Survolez les pays pour plus d'infos.

Part des entreprises qui ont dispose déjà d'une sécurité Zero Trust, qui sont en cours de déploiement ou qui sont en phase de planification stratégique pour la déployer :

- 97 % Italie
- 96 % Inde
- 95 % Royaume-Uni
- 95 % USA
- 94 % Japon
- 93 % Brésil
- 93 % Singapour
- 92 % Allemagne
- 91 % Mexique
- 90 % Pays-Bas
- 89 % Espagne
- 89 % France
- 88 % Australie
- 85 % Suède

Le Zero Trust est toujours essentiellement considéré comme une solution de sécurité cloisonnée… Sauf que le Zero Trust peut apporter bien plus aux entreprises.

Malheureusement, le fait d'avoir mis en place un système de sécurité Zero Trust ou d'avoir prévu d'en déployer un ne signifie certainement pas qu'il est exploité au maximum de son potentiel en tant qu'outil business.

En réalité, les résultats témoignent que le Zero Trust reste perçu comme une solution de sécurité IT cloisonnée : les problématiques immédiates de sécurité sont traitées, avec, à la clé, des avantages concrets. Sauf que le Zero Trust peut apporter bien plus aux entreprises.

PRINCIPALES RAISONS DE DÉPLOYER UNE ARCHITECTURE ZERO TRUST

65 % Améliorer la détection des menaces avancées ou des attaques sur applications Web et élargir la sécurité pour les données sensibles

44 % Sécuriser l'accès à distance pour les fournisseurs, les partenaires et les systèmes OT (operational technology)

27 % Assurer une connectivité plus sécurisée pour les collaborateurs travaillant en mode hybride

24 % Maîtriser les coûts et la complexité de la sécurité réseau traditionnelle

PRINCIPALES RAISONS DANS LE MONDE DE DÉPLOYER UNE ARCHITECTURE ZERO TRUST :

Survolez les pays pour plus d'infos.

Améliorer la détection des menaces avancées :

- 52 % Inde
- 42 % Singapour
- 41 % États-Unis
- 39 % Italie
- 35 % Espagne
- 30 % France
- 26 % Royaume-Uni

Améliorer la détection des attaques d'applications Web :

- 44 % Brésil
- 35 % Mexique

Élargir la sécurité pour protéger les données sensibles :

- 44 % Brésil

Fournir un accès à distance sécurisé aux fournisseurs, partenaires, sous-traitants :

- 33 % Australie
- 32 % Japon
- 24 % Pays-Bas

Cette approche au Zero Trust, qui consiste à n'utiliser le Zero-Trust qu'à des fins de sécurité au début d'un processus de transformation, limite considérablement son potentiel. Dommage, lorsqu'on sait à quel point il est important pour une entreprise d'assurer sa transformation digitale et d'innover, rapidement et à grande échelle.

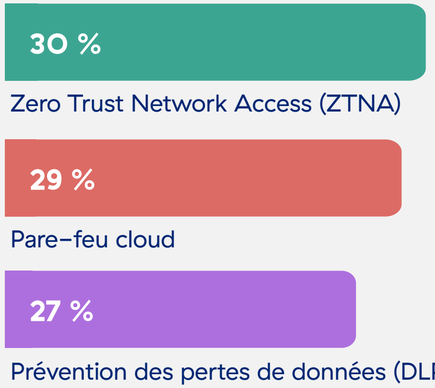
Lorsque le Zero Trust est appréhendé dans sa globalité, au-delà d'une simple technologie ou d'un simple produit, il permet aux entreprises de simplifier leur infrastructure, de repenser leur mode de fonctionnement et de se transformer grâce au digital. À titre d'exemple, les entreprises qui ont instauré le principe de Zero Trust disposent d'un inventaire complet et précis de l'ensemble de leurs applications et autres ressources au sein de leur entreprise. Sur la base de cet inventaire, elles sont en mesure de décider sur les moyens pour optimiser leurs processus, maîtriser leurs coûts, mettre au rebut leur matériel obsolète et renforcer leur productivité.

Mais pour bénéficier de ces avantages stratégiques, le message portant sur la notion de Zero Trust doit pouvoir être entendu des dirigeants et faire partie intégrante de la stratégie de l'entreprise au sens large. Aujourd'hui, les hésitations perdurent quant à la signification de Zero Trust et à son impact sur les entreprises. La pénurie de compétences sur ce sujet est également d'actualité.

Il devient urgent d'aider les dirigeants d'entreprise et les DSI à comprendre que l'objectif du Zero Trust est de simplifier leur infrastructure globale en supprimant l'administration fastidieuse du parc matériel IT. C'est à ce titre que le Zero-Trust permettra de concrétiser les résultats business des entreprises, tout en optimisant le niveau de sécurité.

L'examen des technologies Zero Trust dans lesquelles les entreprises investiront en priorité au cours des douze prochains mois permet de constater une évolution de leur compréhension des avantages métiers. Cette compréhension est varie sensiblement d'une région à une autre, tandis que la marge de progression reste importante.

PRINCIPALES TECHNOLOGIES ZERO TRUST DANS LESQUELLES LES ENTREPRISES INVESTISSENT



PERSPECTIVE RÉGIONALE : ZONE AMÉRIQUES

Amit Chaudhry, Directeur, Marketing produit

Les entreprises adoptent désormais le cloud, la mobilité, l'IA, l'IoT et les technologies OT pour doper leur agilité et leur compétitivité. Les utilisateurs sont disséminés, tout comme leurs données. Mais naturellement, pour une collaboration rapide et productive, ils réclament un accès direct aux applications, d'où qu'ils se trouvent et à tout moment.

Ce rythme effréné de la transformation digitale fournit aux acteurs malveillants une fenêtre d'opportunité pour pirater des architectures réseau et de sécurité datant parfois de plusieurs décennies. Le nombre d'attaques est sans précédent, avec notamment une forte prévalence du ransomware et des attaques sur la chaîne logistique. Et alors que ces attaques deviennent plus sophistiquées, une sécurité basée sur des VPN et pare-feu ne parvient pas à sécuriser le réseau et à offrir une expérience utilisateur de qualité.

Pour concrétiser la vision d'un environnement de travail hybride sécurisé, les entreprises abandonnent rapidement les pare-feu et les VPN au profit d'une architecture Zero Trust assurant un accès rapide, direct et sécurisé aux applications, depuis tout lieu et à tout moment. Fondé sur le principe d'un accès à moindre privilège, avec une connexion est établie sur la base de l'identité et du contexte, le Zero Trust est sans doute le levier le plus pertinent et simple pour protéger les données.

Aujourd’hui, les hésitations perdurent quant à la signification de Zero Trust et à son impact sur les entreprises. La pénurie de compétences sur ce sujet est également d'actualité.

Section III

Faire appel au Zero Trust pour accompagner des modes de travail hybrides

L'infrastructure de travail hybride fait référence à une infrastructure qui permet aux collaborateurs de changer d'environnement de travail de manière homogène entre des sites physiques et distants, sans limite, ni complexité administrative.

Lorsque les premiers confinements lors de la crise sanitaire ont obligé les entreprises à organiser le télétravail pour leurs équipes, nous étions loin de nous douter que cette « mesure temporaire » ouvrirait la porte à une toute nouvelle façon de travailler et qu'en réalité, la notion de travail elle-même ne serait plus jamais le même.

Au lieu de cela, le travailleur moderne a le choix : travailler à domicile, au bureau ou à tout autre endroit et il est essentiel de lui apporter les technologies nécessaires.

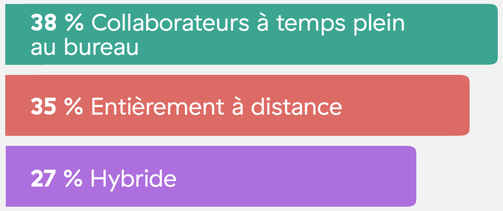
Les personnes interrogées anticipent, qu'au cours des 12 prochains mois, leurs collaborateurs continueront à pleinement tirer parti des différentes options qui s'offrent à eux : travailleurs au bureau à temps plein (38 %), les télétravailleurs (35 %) et travailleurs hybrides (27 %). Ces chiffres sont relativement homogènes à travers le monde.

Alors que près des deux tiers (62 %) des responsables IT déclarent que leur entreprise adopte le travail hybride ou offre à ses équipes toute la flexibilité nécessaire pour travailler à distance, le fait que plus d'un tiers des répondants (38 %) prédit que les collaborateurs vont revenir au bureau à plein temps est à la fois surprenant et inquiétant. Bien que cela puisse être compréhensible pour certains secteurs qui reposent sur des interactions en présentiel (tels que la santé et l'hôtellerie), dans des conditions de marché favorables, le retour au bureau à plein temps pourrait également freiner nombre d'entreprises dans leur volonté d'attirer et fidéliser les talents si elles ne sont pas en mesure d'offrir l'environnement de travail flexible auquel les employés se sont habitués ces dernières années.

19 %

Au niveau mondial, seuls 19 % des décideurs IT interrogés déclarent disposer d'une infrastructure basée sur le Zero Trust et adaptée au travail hybride.

PART DU PERSONNEL SUSCEPTIBLE DE TRAVAILLER À DISTANCE À TEMPS PLEIN, AU BUREAU À TEMPS PLEIN, OU DE FAÇON HYBRIDE, AU COURS DES 12 PROCHAINS MOIS



Au-delà de l'intention, s'assurer qu'une infrastructure IT et de sécurité est en place pour accompagner les différents modes de travail est une toute autre question. À l'échelle mondiale, seuls 19 % des décideurs informatiques interrogés déclarent disposer d'une infrastructure spécifique au travail hybride et basée sur le Zero Trust, ce qui confirme que les entreprises ne sont pas entièrement prêtes à gérer un environnement de travail fortement disséminé à grande échelle. Outre ceux qui ont déjà mis à jour leur infrastructure, 50 % sont en train de mettre en œuvre ou de planifier une stratégie de travail hybride basée sur Zero Trust.

Et parmi ceux qui proposent ou prévoient de proposer le Zero Trust pour un accès à distance sécurisé aux fournisseurs, partenaires, sous-traitants ou opérateurs en usine et d'équipement, c'est-à-dire ceux qui, par nature, évoluent dans un environnement hybride, tout indique que l'accès réseau Zero Trust constitue un domaine d'investissement prioritaire pour les 12 prochains mois. Cela laisse supposer une volonté de répondre aux défis immédiats imposés par les tendances liées au travail hybride.

Survolez les pays pour plus d'infos.

La mise en œuvre d'une stratégie hybride basée sur le Zero Trust est une priorité dans les pays suivants :

- 37 % Inde
- 36 % Singapour
- 33 % Japon
- 29 % Allemagne
- 29 % Pays-Bas

Parallèlement, les pays suivants en sont encore, en grande partie encore, au stade du projet :

- 34 % Mexique
- 27 % États-Unis
- 27 % France
- 25 % Suède

Dans l'ensemble, le Royaume-Uni semble être le plus réticent à adopter des stratégies de travail hybride basées sur le Zero Trust, 21 % des entreprises déclarant qu'elles n'ont actuellement aucun projet pour déployer une infrastructure hybride, et 20 % préférant s'en tenir à leurs technologies traditionnelles d'accès à distance.

La sécurité est bien entendu une préoccupation essentielle pour des entreprises plus nombreuses à évoluer dans un contexte hybride.

PRINCIPALES PRÉOCCUPATIONS DE SÉCURITÉ POUR LES ENTREPRISES QUI PROPOSENT UN MODE DE TRAVAIL HYBRIDE :

- **54 %** les systèmes industriels OT et l'accès à Internet.
- **53 %** Les applications privées sur site, ainsi que les applications privées et instances dans le cloud (sur IaaS, PaaS)
- **32 %** L'Internet des objets ainsi que l'accès Internet à distance

Mais il est important de souligner que ces résultats démontrent que la sécurité du travail hybride ne se résume pas à déjouer les menaces entrantes : il s'agit également de fournir un accès sécurisé à l'infrastructure à de nombreux utilisateurs, collaborateurs, fournisseurs et partenaires business.

Dans ce contexte, malgré l'accent mis sur la sécurité, les raisons invoquées par ceux qui disposent ou planifient une infrastructure de travail hybride basée sur le Zero Trust commencent également à évoquer l'impact business plus large des solutions Zero Trust, avec des implications sur l'expérience et la productivité des collaborateurs.

RAISONS MOTIVANT LA MISE EN ŒUVRE OU LA PLANIFICATION D'UNE INFRASTRUCTURE DE TRAVAIL HYBRIDE BASÉE SUR LE PRINCIPE DU ZERO TRUST

52 % Une expérience aléatoire pour les collaborateurs qui accèdent aux applications et aux données présentes sur site et dans le cloud

46 % Les collaborateurs accusent une perte de productivité en raison de problématiques d'accès au réseau

39 % Les collaborateurs ne sont pas en mesure d'accéder aux applications et aux données à partir de leurs dispositifs personnels

Survolez les pays pour plus d'infos.

Les pays faisant état du plus grand nombre d'expériences d'accès incohérent sont

- 70 % Japon
- 68 % Inde
- 64 % États-Unis
- 62 % Singapour

En Europe, seule la moitié environ des entreprises interrogées déclare subir ces accès aléatoires, avec

- 52 % Suède
- 49 % Pays-Bas
- 47 % France
- 45 % Allemagne

Les pertes de productivité dues aux problèmes d'accès au réseau ont été invoquées comme étant la raison dominante d'une migration vers une nouvelle infrastructure dans les pays suivants :

- 55 % Mexique
- 48 % Espagne
- 47 % Royaume-Uni

Les personnes interrogées et dont les entreprises disposent d'une infrastructure traditionnelle et basée sur VPN pour permettre le travail hybride, déclarent devoir gérer des problématiques plus fondamentales liées au télétravail.

L'expérience utilisateur est un moteur de productivité dans les environnements de travail hybrides : c'est l'un des principaux enseignements sur l'année dernière. Nos résultats révèlent que la réactivité varie selon les régions lorsqu'il s'agit de moderniser l'infrastructure d'entreprise pour répondre aux problématiques d'expérience observées à ce jour.

Pour proposer aux utilisateurs une expérience optimale dans un environnement d'entreprise de plus en plus disséminé, le trafic utilisateur doit être dirigé vers l'application via le chemin le plus court possible, pour éviter toute latence et congestion. Les entreprises doivent tenir compte de la mobilité de l'employé hybride qui doit avoir accès à l'application requise de manière dynamique, avec une bande passante optimale, qu'il travaille à domicile, au bureau ou qu'il soit en déplacement. Outre l'expérience, si un employé n'est pas satisfait de la performance de l'accès à ses applications professionnelles critiques, il pourrait être tenté de contourner les contrôles de sécurité, une attitude à risque.

En comparaison, les personnes interrogées dont les entreprises utilisent une infrastructure de travail hybride traditionnelle, basée sur un VPN, déclarent être toujours confrontées aux problématiques classiques associées au télétravail. Parmi celles-ci, l'administration complexe d'infrastructures de sécurité différentes pour les collaborateurs sur site et distants (47 %), les performances altérées des applications telles que ressenties par les utilisateurs (39 %) et la difficulté des équipes IT à surveiller et améliorer l'expérience utilisateur des utilisateurs distants (37 %).

Bien que le travail hybride suscite encore de nombreuses inquiétudes en matière de sécurité, des réponses comme celles-ci reflètent le défi beaucoup plus vaste que ce mode hybride pose aux entreprises : un défi qui intègre l'accès, l'expérience et les performances.

Le Zero Trust, lorsqu'il est correctement appréhendé, répond à tous ces défis, offrant une simplicité qui permet aux équipes IT de répondre aux attentes et exigences en évolution de leur entreprise.

PERSPECTIVES RÉGIONALES : RÉGION APAC

Heng Mok, RSSI, APJ

La région Asie-Pacifique (APAC) illustre parfaitement l'idée qu'une seule même solution ne vaut pas pour tous. Cette zone est un creuset de cultures et de styles de vie, et chaque marché de cette région possède sa propre approche au travail. Même avant la pandémie, nous avons observé des différences notables, avec des marchés comme le Japon et Singapour qui privilégiait une organisation plus hiérarchique du travail, tandis que le modèle de travail de l'Australie et de l'Inde se voulait plus relax.

La région APAC comprenant certaines des villes les plus confinées au monde, ces nuances sont encore plus prononcées aujourd'hui, alors que nous émergeons des confinements à répétitions. Parmi les personnes interrogées dans le cadre de l'enquête, la majorité des décideurs IT au Japon et sur Singapour s'attendent à ce que leurs équipes reviennent au bureau à plein temps, un contraste frappant avec les personnes interrogées en Australie et en Inde, qui s'attendent à une généralisation du télétravail.

Toutefois, nous pensons que les entreprises seront plus nombreuses à privilégieront des modèles de travail hybride à long terme. De nombreuses entreprises avec lesquelles j'ai discuté optent pour des pratiques hybrides afin d'en tirer parti pour attirer et fidéliser les talents. Avec une concurrence accrue pour un réservoir limité de talents, il n'est pas surprenant que nombre d'entreprises se mettent à l'heure de l'hybride et recherchent des solutions technologiques pour accompagner cette transition de manière transparente.

L’expérience utilisateur est un moteur de productivité dans les environnements de travail hybrides : c'est l'un des principaux enseignements sur l’année dernière.

Section IV

Adopter une approche Zero Trust pour intégrer les technologies émergentes

Les technologies émergentes font référence aux technologies nouvelles ou en rapide évolution, dont les applications pratiques sont encore largement sous-exploitées, mais qui devraient avoir un impact majeur sur les entreprises et générer un avantage concurrentiel.

Les solutions digitales permettant le télétravail ne sont bien sûr pas les seules technologies que les entreprises tentent d'exploiter. À l'ère du numérique, les technologies industrielles (ou OT pour Operational Technology) jouent un rôle toujours plus important. Ce périmètre, traditionnellement adossé à des systèmes et processus classiques, devrait se transformer fondamentalement grâce à des technologies émergentes. Chacune d'entre elles offrira un ensemble de possibilités passionnantes pour simplifier et automatiser davantage les processus opérationnels.

Les entreprises doivent toutefois penser encore plus loin, en anticipant également les innovations technologiques à venir, pour assurer la pérennité de leurs décisions en matière d'infrastructure. Les décideurs informatiques doivent prendre en compte les différentes directions que peut prendre leur entreprise en fonction des innovations, et faire preuve d'ouverture d'esprit quant à la manière dont les technologies émergentes peuvent accompagner leurs fonctions métiers. Le Zero Trust est sans doute le chaînon manquant, que les entreprises sont invitées à intégrer, pour se préparer aux technologies futures, dès aujourd'hui.

En accord avec les motivations d'une migration vers le cloud et la transformation digitale en général, nos résultats ont révélé que la volonté de se concentrer sur des résultats stratégiques plus larges semble faire défaut dans la manière dont les entreprises planifient leurs projets liés aux technologies émergentes.

Interrogés sur le volet le plus difficile de la mise en œuvre de projets liés à des technologies émergentes, 30 % des répondants citent une sécurité adéquate, suivie des besoins budgétaires d'une digitalisation plus poussée (23 %). En revanche, seuls 19 % citent la dépendance à l'égard des décisions stratégiques de l'entreprise comme étant un défi.

L'ASPECT LE PLUS DIFFICILE DE LA MISE EN ŒUVRE DES PROJETS DE TECHNOLOGIES ÉMERGENTES, PAR RÉGION

Survolez les pays pour plus d'infos.

La sécurité a constitué le plus grand défi pour les pays suivants :

- 54 % Brésil
- 41 % Japon
- 37 % Inde
- 37 % Italie
- 35 % Espagne
- 31 % États-Unis

En revanche, les pays suivants sont principalement préoccupés par les contraintes budgétaires :

- 27 % Singapour
- 27 % France
- 23 % Royaume-Uni

Le manque de vision semble être le principal obstacle qui se dresse entre les entreprises et les technologies émergentes.

- 24 % Pays-Bas

Le seul pays où la plupart des entreprises ont cité la dépendance à l'égard des décisions stratégiques d'entreprise comme étant le plus grand frein.

- 28 % Suède

Si les préoccupations budgétaires sont attendues, il est intéressant de constater l'accent mis sur la sécurisation du réseau, mais de manière dissociée par rapport à la stratégie d'entreprise. Les entreprises se concentrent sur la sécurité sans pleinement comprendre les avantages commerciaux qu'elle présente, une preuve supplémentaire que la notion de Zero Trust n'est pas encore perçue comme un catalyseur pour l'activité business.

Alors qu'elles planifient l'utilisation de technologies émergentes telles que la réalité augmentée, les jumeaux numériques et la construction virtuelle, un accès performant et à faible latence aux applications devient une préoccupation. Ceci est particulièrement vrai sur le continent américain, où l'intérêt pour les technologies émergentes dans les trois prochaines années est particulièrement marqué.

PERTINENCE D'UN ACCÈS PERFORMANT ET À FAIBLE LATENCE AUX APPLICATIONS SUR LES 3 PROCHAINES ANNÉES

55 % Europe

79 % Région Amériques

62 % APAC

TECHNOLOGIES PRIORITAIRES D'ICI 2025	MONDE	EUROPE	AMÉRIQUES	APAC
Accès via le cloud aux technologies OT et aux systèmes de contrôle industriel	34 %	29 %	40 %	38 %
Déploiement de la technologie 5G pour une meilleure connectivité	32 %	29 %	39 %	32 %
Réduction de l'empreinte carbone de l'entreprise	29 %	28 %	28 %	30 %
Déploiement de projets d'intelligence artificielle/ d'apprentissage automatique	27 %	22 %	39 %	28 %

Survolez les pays pour plus d'infos.

Entreprises se concentrant sur un accès cloud aux systèmes OT et de contrôle industriel :

- 46 % Mexique
- 45 % Inde
- 44 % Singapour
- 36 % Australie
- 33 % France

Entreprises qui privilégient le déploiement de technologies 5G :

- 47 % Brésil
- 45 % Inde
- 41 % Italie
- 36 % Espagne
- 28 % Royaume-Uni

Entreprises qui citent la réduction de l'empreinte carbone en tant que priorité n°1 :

- 41 % Italie
- 28 % Allemagne
- 32 % Suède

Seules les entreprises des Pays-Bas font de l'expansion de l'edge computing leur priorité principale (29 %), tandis que les États-Unis se concentrent essentiellement sur le déploiement de projets IA et de ML (43 %).

Nous voyons déjà dans quelle mesure ces technologies émergentes prioritaires pourraient mener à des résultats métiers plus larges. Cependant, nos résultats suggèrent toujours l'absence d'une vision plus globale au sein des entreprises. Les entreprises se doivent d'être plus conscientes des avantages concurrentiels que peuvent leur procurer les technologies émergentes, notamment, bien sûr, en matière de sécurité.

PERSPECTIVES RÉGIONALES : RÉGION EMEA

Nathan Howe, VP en charge des technologies émergentes

Les entreprises européennes sont moins susceptibles d'être les premières à adopter les technologies nouvelles ou émergentes. Même si l'Europe a été le berceau de la révolution industrielle et de ses inventions mécaniques, la région a été dépassée depuis longtemps en matière d'adoption des technologies digitales. La région Asie-Pacifique-Japon est devenue le pôle technologique de la fabrication de puces. D'auLa capacité d'innovation au sein de la Silicon Valley attire et fédère des personnes du monde entier pour imaginer les technologies de demain.

Dans ce contexte, il n'est pas surprenant que l'Asie ait déjà compris la puissance de la 5G, une norme qui devrait surperformer le Wi-Fi en matière de connectivité à l'heure du Digital. Alors que les Amériques se positionnent à mi-chemin, l'Europe s'interroge encore sur comment passer à la 5G dans le cadre de ses efforts de digitalisation. L'Europe est toutefois sur le point de connaître une croissance spectaculaire dans le domaine du cloud numérique et des technologies émergentes : en effet, de nouvelles tendances géopolitiques, comme la pénurie de composants électroniques et les problématiques de chaîne logistique, incitent les pays européens à établir des centres d'excellence au sein de leur région.

Section V

La voie pour exploiter le plein potentiel de Zero Trust

Sur la base de ces résultats, comment les entreprises doivent-elles aborder leur parcours vers le Zero Trust ?

Les défis associés aux architectures réseau et de sécurité traditionnelles restent d'actualité et invitent à repenser la manière dont la connectivité est assurée dans le monde moderne. C'est dans ce contexte que doit intervenir le Zero Trust, une architecture qui ne considère aucun utilisateur ni application comme étant de confiance par défaut. Le Zero Trust propose des accès sur la base du moindre privilège. La confiance n'est accordée qu'une fois que l'identité et le contexte ont été vérifiés et que les règles de la politique de sécurité ont été appliqués.

Cette approche considère toutes les communications réseau comme potentiellement malveillantes. Les communications entre les utilisateurs et les instances, ou entre les instances elles-mêmes, sont suspendues jusqu'à ce qu'elles soient validées par des politiques fondées sur l'identité. Cela empêche tout accès inopportun et déplacement en interne. Cette validation s'applique à tout environnement réseau et l'emplacement d'une entité sur le réseau n'est plus pris en compte et ne dépend pas d'une segmentation rigide du réseau.

À l'origine, le Zero Trust était une nouvelle façon de protéger les réseaux. Par la suite, ce principe s'est étendu au-delà des réseaux sur site, mais était toujours axé principalement sur la sécurisation du trafic des applications privées. Pendant trop longtemps, le trafic a été considéré en fonction de sa relation avec un réseau, au lieu d'être dissocié de ce dernier. Aujourd'hui, les entreprises doivent prendre conscience de potentiel entier du Zero Trust pour protéger les applications SaaS, le trafic vers et depuis les clouds publics, et même les utilisateurs lorsqu'ils accèdent à l'Internet public. Les initiateurs de ce trafic peuvent être tant des instances que des utilisateurs. L'accès peut être indépendant du transport, le trafic passant par n'importe quel routeur et empruntant n'importe quel réseau, filaires ou sans fil, 4G ou 5G, ainsi que les extensions futures.

Il est grand temps d'appliquer les principes de Zero Trust à tout le trafic, quelle que soit son origine et quelle que soit sa destination. Il s'agit désormais de ne plus s'interroger sur quelle entité se connecte à quel réseau, et d'utiliser le Zero Trust pour interconnecter toutes les entités directement en appliquant les politiques métiers. À l'ère du cloud, Internet est le nouveau réseau corporate, et tout le trafic est considéré comme équitable pour connecter en direct la bonne entité à l'entité de destination adéquate, avec application des politiques métiers.

Quelles mesures les entreprises peuvent-elles prendre dès aujourd'hui pour se transformer en entreprises sûres, agiles, flexibles et efficaces, pour composer avec les tendances macroéconomiques actuelles et les exigences des technologies émergentes ?

Il existe trois recommandations essentielles :

1

Les entreprises doivent reconsidérer la manière dont elles appréhendent la notion de Zero Trust, en en faire un moteur de transformation digitale sécurisée et un levier de performance business.

Avec sa visibilité et un contrôle renforcés, une architecture basée sur le Zero Trust devient un levier de simplicité pour les environnements IT actuels et permet aux entreprises de se concentrer sur les résultats qu'elles attendent de leur technologie, qu'il s'agisse de performances optimales, d'une expérience utilisateur renforcée ou de la maîtrise des coûts.

2

La sensibilisation reste un levier majeur pour dissiper les craintes, les incertitudes et les doutes sur le Zero Trust et son impact sur les entreprises.

Le DSI et le RSSI ont un rôle essentiel à jouer pour sensibiliser leurs dirigeants à la pertinence du Zero trust et à son adéquation par rapport à la stratégie d'entreprise.

3

Les technologies émergentes doivent être perçues en tant qu'avantage concurrentiel. Les infrastructures intégrant le Zero Trust établissent dès aujourd'hui les bases de l'avenir.

Le choix des technologies émergentes à adopter doit être motivé par une vision d'entreprise globale et par les besoins actuels et futurs d'entreprise, et non par les tendances du marché ou parce qu'une technologie fait le buzz. Le Zero Trust répond aux besoins d'une connectivité sécurisée et performante de ces technologies en devenir.

Lorsque les mentalités auront évolué et que le Zero Trust sera perçu en tant qu(outil business essentiel, les entreprises devront s'interroger sur comment déployer une architecture Zero Trust qui leur permettra d'atteindre leurs objectifs business ?

Zscaler a fait du Zero Trust la clé de voûte de sa solution Zero Trust Exchange et de son framework SSE. Le Zero Trust régit les utilisateurs accédant aux applications internes et externes, la connectivité IoT/OT et les instances accédant aux ressources en environnement multicloud ou sur Internet. Les principes du Zero Trust permettent d'inscrire le travail hybride dans la stratégie d'entreprise, invitant les collaborateurs, les partenaires business et les clients de travailler depuis le lieu de leur choix, celui qui les rend les plus productifs. Ce travail hybride assure la continuité des activités, favorise le recrutement de nouveaux talents et permet de déployer des environnements de travail hybrides.

Zscaler Zero Trust Exchange est un service cloud–native qui offre aux collaborateurs , partenaires et clients un accès rapide, direct et sécurisé aux applications externes et internes, quels que soient l'emplacement, l'appareil ou le réseau.

Il intègre également les sept éléments essentiels de l'architecture Zero Trust, qui sont regroupés dans les trois catégories suivantes :

Vérifier

L'architecture Zero Trust met d'abord fin à la connexion et détermine

1. Qui se connecte ?
2. Quel est le contexte de l'accès ?
3. Où va la connexion ?

Contrôle

L'architecture Zero Trust va ensuite :

4. Évaluer le risque
5. Prévenir toute compromission
6. Prévenir la perte de données

Appliquer

Avant d'enfin établir une connexion, l'architecture Zero Trust va :

7. Appliquer la politique de sécurité

C'est en gardant ces éléments à l'esprit que les entreprises adeptes du cloud accéléreront leur transformation numérique et seront prêtes à s'adapter à l'avenir, quel qu'il soit.

À propos de Zscaler et de Zscaler Zero Trust Exchange

Zscaler est reconnu en tant que leader du Zero Trust, disposant d'une plateforme Zero Trust pertinente, conviviale et mature.

Vous pouvez tirer parti de notre plateforme cloud-native Zscaler Zero Trust Exchange pour migrer vers le Zero Trust. Contrairement aux produits de sécurité et réseau traditionnels, Zero Trust Exchange est une plateforme conçue sur mesure pour le cloud. Sa sécurité commence par la fermeture de chaque connexion, ce qui permet une inspection approfondie du contenu et la vérification des droits d'accès en fonction de l'identité et du contexte.

Zero Trust Exchange opère sur 150 data centers dans le monde, garantissant à vos utilisateurs un service de proximité, étroitement interfacé avec les fournisseurs cloud et les applications auxquels ils accèdent, tels que Microsoft 365 et AWS. La solution offre le chemin le plus court entre vos utilisateurs et leurs destinations, avec une sécurité complète et une expérience utilisateur optimale.

Pour en savoir plus sur notre plateforme conviviale, cliquez ici.

Zero Trust Exchange fonctionne sur 150 data centers répartis dans le monde

Méthodologie

ATOMIK Research a interrogé 1 908 décideurs de haut niveau (DSI/RSSI/CDO/Responsable de l'architecture réseau) dans les régions EMEA (Royaume-Uni, Allemagne, France, Pays-Bas, Suède, Italie, Espagne), Amériques (États-Unis, Mexique, Brésil) et APAC (Japon, Inde, Australie, Singapour). L'étude a été menée entre le 31 mai et le 28 juin 2022. Le panel interrogé comprenait 43 % d'entreprises comptant jusqu'à 4 999 employés, 32 % comptant de 5 000 à 9 999 employés et 25 % avec un effectif de 10 000 employés ou plus.