Collaborateurs plus autonomes : comment les DSI et les DSSI se préparent au travail en mode hybride

Ce rapport d'étude détaillé vous fera découvrir des techniques efficaces pour migrer d'une infrastructure traditionnelle à risque vers une stratégie Zero Trust efficace.

RAPPORT D'ÉTUDE DE HMG STRATEGY COMMANDITÉ PAR ZSCALER

HMG STRATEGY

zscaler™

NOTE DE SYNTHÈSE

Alors que nous entrons dans une nouvelle phase de la pandémie mondiale, de nombreuses entreprises s'interrogent sur la manière de faire revenir leurs collaborateurs après plus de deux années d'absence régulière de leur bureau physique. De nombreuses enquêtes révèlent que la plupart des collaborateurs souhaitent des conditions de travail hybrides, un mix entre travail au bureau et à distance. Ils vont jusqu'à démissionner de leur emploi pour saisir de nouvelles opportunités s'ils n'ont pas la liberté de décider quand et où ils peuvent travailler.

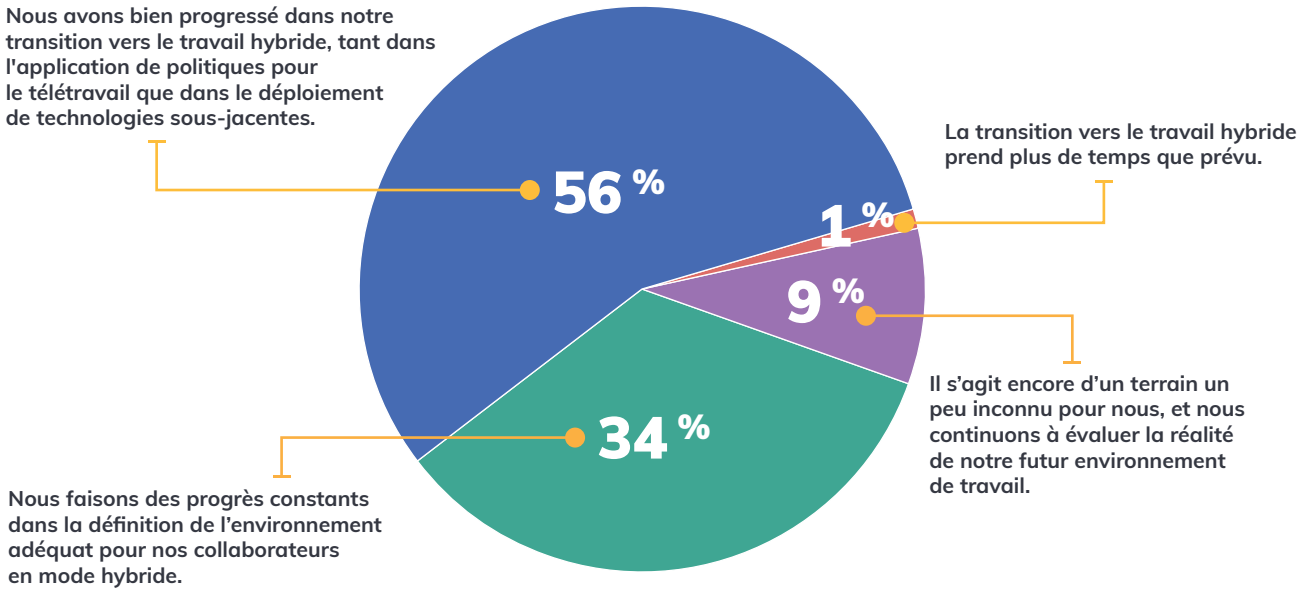
Dans ce contexte, comment réussir la transition de l'entreprise vers un mode de hybride ? Et comment les DSI et les DSSI peuvent-ils collaborer en bonne entente avec leur direction générale pour déployer un environnement de travail agile et productif tout en protégeant efficacement leur entreprise ?

Une récente enquête menée par HMG Strategy et commanditée par Zscaler, auprès de 138 DSI, DSSI et professionnels des technologies en entreprise, révèle que si 56 % des personnes interrogées déclarent que leur entreprise a« bien avancé » dans sa transition vers un environnement de travail hybride (définition de politiques de télétravail et déploiement des technologies sous-jacentes), près de la moitié (44 %) du panel estime que la transition de leur entreprise vers un environnement de travail hybride est toujours en cours.

Parmi ces 44 %, près d'une personne interrogée sur cinq déclare que la transition vers un environnement de travail hybride « est encore un terrain méconnu pour nous et nous continuons à évaluer à quoi ressemblera notre environnement futur de travail. »

S'adapter à un mode de travail hybride

Comment caractériseriez-vous la transition de votre entreprise du télétravail vers travail hybride ?



Source : Enquête 2022 sur les environnements de travail hybride et sécurisé de HMG Strategy, auprès de 138 DSI, DSSI et professionnels de la technologie, réalisée aux deuxième et troisième trimestres 2022.

« La plupart des entreprises sont en phase de transition du télétravail vers le travail hybride, mais elles n'y arrivent pas forcement », observe **Bryan Green**, DSSI, zone Amériques chez Zscaler. Par exemple, depuis le début de la pandémie, la plupart des entreprises ont réalisé des investissements temporaires et à court terme pour étendre l'utilisation des technologies VPN ou recourir à des applications sensibles à haut débit, à l'instar des systèmes de vidéoconférence utilisés pour accompagner le basculement vers le télétravail. « Mais elles ne prennent pas nécessairement les bonnes décisions en matière de sécurité sur le long terme », précise Bryan Green.

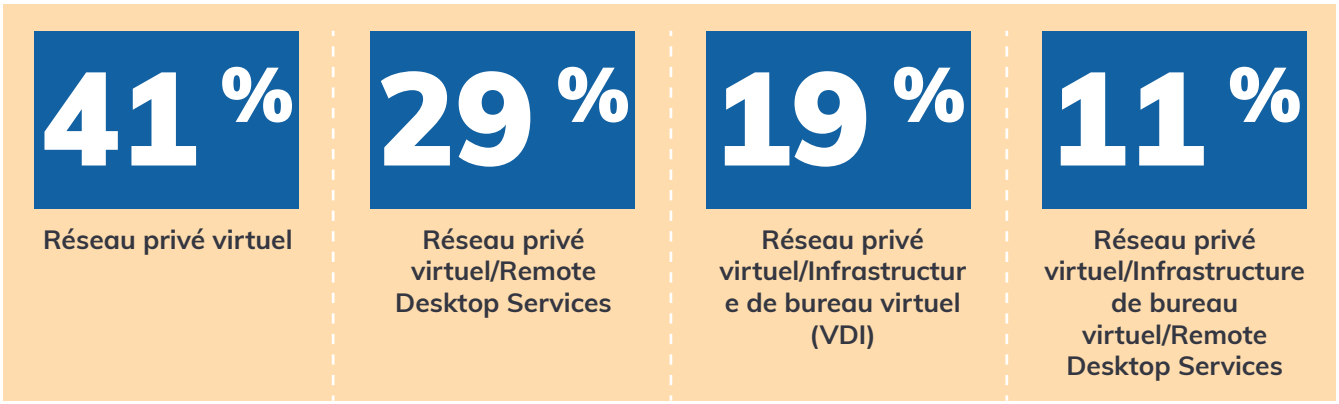
Véritables leviers du changement lors de la pandémie, les professionnels de la technologie sont bien positionnés pour aider leur entreprise à faire évoluer son environnement de travail, en veillant à déployer les technologies adaptées aux besoins des travailleurs hybrides et en créant un environnement flexible, productif et sécurisé pour les travailleurs au bureau et distants. Mais comme le suggère l'enquête, il reste énormément de travail à accomplir pour concrétiser ce concept.

HMG Strategy s'est associé à Zscaler pour mieux comprendre les défis et les opportunités qui se présentent aux entreprises lors de leur transition vers un environnement de travail hybride, y compris les freins technologiques et culturels à la mise en œuvre d'un environnement de travail hybride, sécurisé et flexible. Vous découvrirez dans ce rapport de recherche :

- Les difficultés techniques liées à au déploiement d'un environnement de travail hybride, sécurisé et flexible, notamment les carences des infrastructures existantes telles que les VPN ;
- Les risques auxquels les entreprises sont confrontées pour sécuriser l'accès aux applications pour leurs équipes hybrides ;
- Les défis de sécurité des accès aux applications privées pour les collaborateurs à distance et au bureau ;
- Une architecture robuste, basée sur le Zero Trust, comme solution aux problématiques de sécurité de l'environnement de travail hybride.

Moyens d'accès aux applications

Quelles formes de technologies d'accès aux applications utilisez-vous actuellement ?



Source : Enquête 2022 sur les environnements de travail hybride et sécurisé de HMG Strategy, auprès de 138 DSI, DSSI et professionnels de la technologie, réalisée aux deuxième et troisième trimestres 2022.

« La plupart des entreprises sont dans une transition du télétravail vers le travail hybride, mais le succès n'est pas toujours au rendez-vous. »

BRYAN GREEN
DSSI, zone Amériques
Zscaler

Surmonter les obstacles à la création d'un environnement de travail hybride, sécurisé et flexible

Si les entreprises ont adopté le SaaS et les services de cloud public au cours des dernières années, nombre d'entre elles en sont encore dans un processus de migration vers le cloud. Selon une étude de Foundry, 63 % des sociétés prévoient de transférer la plupart ou la totalité de leur infrastructure informatique vers le cloud au cours de l'année prochaine, par rapport à 41 % actuellement.

Et bien que l'adoption du cloud évolue rapidement, les entreprises investissent encore massivement dans les data centers et infrastructures sur site.

« AWS propose une infrastructure de cloud public et privé depuis 16 ans, mais c'est la COVID qui a accéléré l'adoption massive vers le télétravail il y a deux ans », pointe Bryan Green. « Par conséquent, de nombreuses entreprises doivent encore relever les défis de complexité liés aux personnes, aux processus et aux technologies. »

La dynamique du leadership constitue un autre enjeu complexe associé à l'adoption du travail hybride. Étant donné les investissements immobiliers majeurs que les sociétés ont engagés dans des bureaux leur appartenant ou qu'elles louent, de nombreux cadres supérieurs veulent s'assurer que l'espace de bureau est utilisé de manière rentable. Dans certains cas, les dirigeants d'entreprise exigent que les collaborateurs travaillent deux ou trois jours par semaine dans un bureau dédié, bien que de nombreux collaborateurs n'aient pas adhéré à la consigne.

Au cours de la première semaine suivant le Labor Day de 2022, la fréquentation des bureaux dans 10 grandes zones métropolitaines des États-Unis n'était que de 50 % de la fréquentation en 2020, avant la pandémie, selon une étude réalisée par Kastle Systems, un acteur des services managés de sécurité pour piloter les accès physiques dans les immeubles de bureaux. La fréquentation des bureaux reste inférieure à ce qu'elle était avant la pandémie, bien que diverses études font état d'une progression au cours des derniers mois.

« Les dirigeants de nombreuses entreprises sont conscients d'avoir lourdement investi dans l'immobilier », indique Bryan Green. « Elles souhaitent que leurs employés reviennent travailler au bureau. Il s'agit là d'une véritable problématique. »

Relever les défis de la cybersécurité

Lorsque les entreprises ont basculé vers le télétravail en mars 2020, leur stratégie de monitoring et de protection des télétravailleurs a présenté un certain nombre de lacunes. Pour commencer, de nombreuses entreprises ont fait appel aux réseaux privés virtuels (VPN) pour permettre aux collaborateurs d'envoyer et de recevoir des données via des réseaux partagés ou publics. Ceci à mis en évidence un certain nombre de vulnérabilités liées aux VPN :

- Chaque passerelle VPN possède un module d'écoute des flux entrants qui est en fait un vecteur potentiel d'attaque.
- La passerelle VPN devient alors un point de départ pour des attaques plus sophistiquées menées par des hackers.
- Le VPN est intrinsèquement ouvert, ce qui oblige les équipes de sécurité à bloquer explicitement l'accès des collaborateurs aux applications et systèmes pour lesquels ils n'ont pas ou ne devraient pas avoir de droits d'accès.

Modernisation de l'environnement de travail hybride

Bon nombre des défis associés à la conception d'un environnement de travail hybride, sécurisé et agile sont liés à une infrastructure obsolète et à une carence d'outils nécessaires pour prévenir les pertes de données et l'accès non autorisé aux applications.

Principaux freins à la création d'un environnement de travail hybride, sécurisé et flexible

30 %

Même si nous accompagnons activement le BYOD (utilisation de dispositifs personnels dans un cadre professionnel), nous ne disposons pas des outils nécessaires pour maîtriser le risque de perte de données et d'accès non autorisé aux ressources internes.

20 %

Notre infrastructure VPN ralentit sensiblement la connectivité Internet et a un impact négatif sur la productivité des collaborateurs.

22 %

Notre entreprise fait appel à des intervenants et partenaires externes, mais leur fournir un accès sécurisé aux applications internes représente un véritable défi.

16 %

La latence sur notre réseau VDI frustre les collaborateurs et rend les tâches les plus simples irréalisables sur les postes de travail virtuels.

7 %

Même si nous accompagnons activement le BYOD (utilisation de dispositifs personnels dans un cadre professionnel), nous ne disposons pas des outils nécessaires pour minimiser le risque de perte de données et d'accès non autorisé aux ressources internes. Notre entreprise fait appel à des intervenants et partenaires externes, mais leur fournir un accès sécurisé aux applications internes représente un véritable défi.

5 %

La latence sur notre réseau VDI frustre les employés et rend les tâches les plus simples irréalisables sur les postes de travail virtuels. Notre entreprise fait appel à des intervenants et partenaires externes, mais leur fournir un accès sécurisé aux applications internes représente un véritable défi.

Source : Enquête 2022 sur les environnements de travail hybride et sécurisé de HMG Strategy, auprès de 138 DSI, DSSI et professionnels de la technologie, réalisée aux deuxième et troisième trimestres 2022.

« Si vous disposez de VPN d'accès à distance et de VPN de site à site, vous vous retrouvez avec une vaste surface d'attaque qui permet à vos utilisateurs, ou à des acteurs malveillants, de potentiellement connaître les modules de votre infrastructure. »

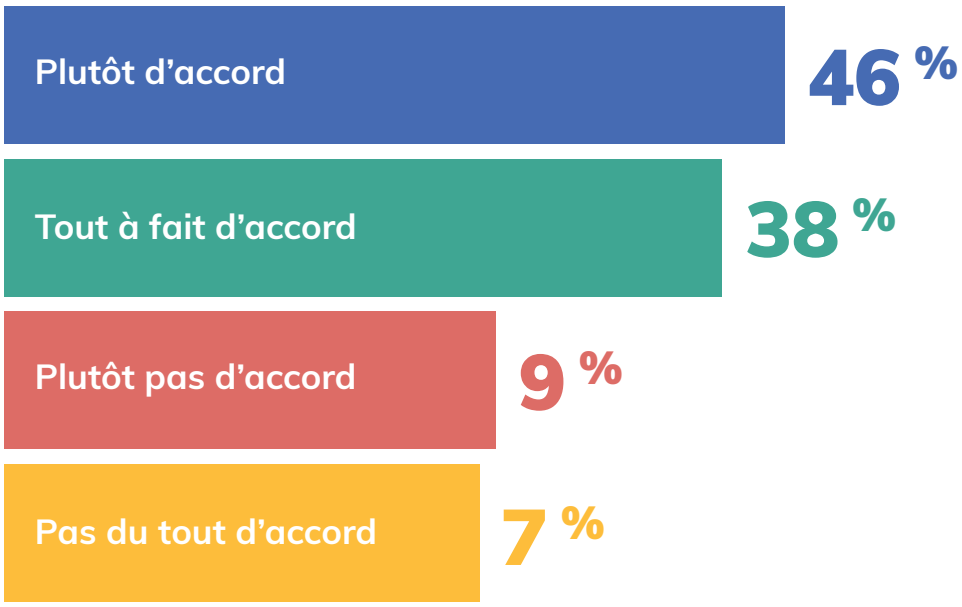
BRYAN GREEN
DSSI Amériques
Zscaler

« Lorsque vous créez une connexion VPN, c'est le réseau d'entreprise qui s'entend vers différents points », explique le DSSI de Zcaler, qui a travaillé sur les concentrateurs VPN de Cisco à partir de 2003. « Si vous disposez de VPN d'accès à distance et de VPN de site à site, vous vous retrouvez avec une vaste surface d'attaque qui permet à vos utilisateurs, ou à des acteurs malveillants, de potentiellement identifier les composantes de votre infrastructure. À moins d'avoir déployé certains types de pare-feu ou certaines méthodes de segmentation, les assaillants disposent d'un accès illimité à votre infrastructure. »

Un impact sur la productivité

L'utilisation des accès à distance et des VPN de site à site ne fait pas qu'étendre de manière exponentielle la surface d'attaque d'une entreprise .D'autre part, c'est la productivité des collaborateurs hybrides qui est impactée.

Dans quelle mesure êtes-vous d'accord pour dire que les performances médiocres et frustrantes des VPN pèsent sur la productivité des collaborateurs travaillant en mode hybride ?



Source : Enquête 2022 sur les environnements de travail hybride et sécurisé de HMG Strategy, auprès de 138 DSI, DSSI et professionnels de la technologie, réalisée aux deuxième et troisième trimestres 2022.

Les vulnérabilités inhérentes aux VPN ne sont que quelques-unes des raisons pour lesquelles les entreprises devraient passer à une architecture Zero Trust pour protéger leurs environnements de travail hybride. Une architecture Zero Trust peut non seulement protéger les entreprises contre les violations coûteuses, mais également réduire la complexité, renforcer la protection des données et améliorer l'expérience des employés tout en éliminant la surface d'attaque.

Dans les prochaines sections du rapport, nous nous pencherons sur les défis de sécurité associés aux accès à privilèges trop élevés, ainsi que sur les avantages opérationnels et business d'une stratégie Zero Trust.

Supprimer les accès bénéficiant de privilèges trop élevés pour mieux sécuriser l'environnement hybride

Si de nombreuses entreprises avaient déjà fait un premier pas timide vers le télétravail, le virage numérique généralisé que les entreprises ont été contraintes d'effectuer en mars 2020 a étendu de manière exponentielle leur empreinte numérique, de même que leur surface d'attaque.

Alors que les entreprises poursuivent leur adoption du cloud public, elle subissent parallèlement le risque d'offrir des accès à privilèges trop élevés et d'exposer leurs données critiques.

Exposition aux risques et travail hybride

Les infrastructures traditionnelles appliquées à un environnement de travail hybride sont source de risques pour les équipes de sécurité. Parmi ces risques, un accès à privilèges trop élevés aux applications pour les collaborateurs et les sous-traitants, ainsi qu'un accès par des utilisateurs compromis aux ressources du réseau.

À quels risques vous exposez-vous lorsque vous sécurisez l'accès aux applications pour vos collaborateurs hybrides ?

31 %

Accès avec des privilèges trop élevés pour les collaborateurs et les prestataires externes

26 %

Utilisateurs compromis accédant aux ressources du réseau

18 %

Perte de données accidentelle et/ou malveillante

15 %

Dispositifs à haut risque accédant aux ressources du réseau (par ex., inconnus, non conformes)

10 %

Attaques visant les applications (par ex. déni de service, cross-site scripting, injection)

Source : Enquête 2022 sur les environnements de travail hybride et sécurisé de HMG Strategy, auprès de 138 DSI, DSSI et professionnels de la technologie, réalisée aux deuxième et troisième trimestres 2022.

« Le surdimensionnement des privilèges d'accès est une problématique majeure de sécurité à laquelle nous sommes confrontés, et que nous avons eu du mal à traiter », observe Bryan Green. Il fait, à ce sujet, une analogie avec une agence bancaire qui interagit avec ses clients. Dans une agence bancaire, un client ne donne pas à chaque guichet ou employé de banque une clé de son coffre-fort. Mais lorsqu'il s'agit de fournir aux utilisateurs un accès logique à différents types d'applications en fonction de leurs rôles, « cet objectif se révèle beaucoup plus difficile à mettre en œuvre par rapport à un accès physique », poursuit Bryan Green.

Heureusement, les outils modernes de gestion des droits d'accès à l'infrastructure cloud (CIEM) répondent aux risques associés aux privilèges trop élevés, grâce à une visibilité approfondie sur les droits et les risques d'accès au cloud et la possibilité pour les entreprises d'adopter une stratégie basée sur le principe du moindre privilège.

Dans la dernière section de ce rapport d'étude, nous présentons les facteurs qui incitent les professionnels de la sécurité et des technologies à adopter un modèle de sécurité Zero Trust, ainsi que les avantages opérationnels et métiers de ce modèle.

Manque de confiance dans les outils de sécurité en place

Un tiers seulement des professionnels des technologies et de la sécurité se disent très confiants quant à la capacité des outils de sécurité en place dans leur entreprise à identifier un utilisateur compromis ou une menace interne accédant aux ressources du réseau.

Dans quelle mesure êtes-vous convaincu que vos outils de sécurité actuels sont capables d'identifier un utilisateur compromis ou une menace interne accédant aux ressources de votre réseau ?

34 %

Très confiant

62 %

Assez confiant

4 %

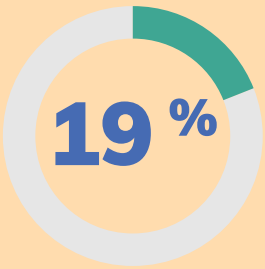
Pas du tout confiant

Source : Enquête 2022 sur les environnements de travail hybride et sécurisé de HMG Strategy, auprès de 138 DSI, DSSI et professionnels de la technologie, réalisée aux deuxième et troisième trimestres 2022.

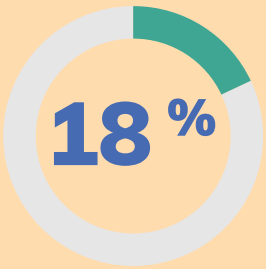
Lacunes de sécurité de l'accès aux applications privées

Les applications publiques ne sont pas les seules à être exposées aux vulnérabilités. Les applications privées accessibles via des passerelles Internet peuvent également être vulnérables aux attaques.

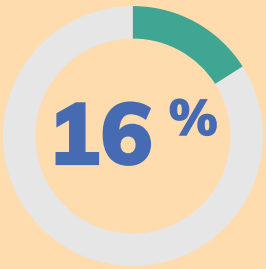
Lequel des scénarios suivants avez-vous rencontré en fournissant un accès à des applications privées pour des travailleurs distants et au bureau ?



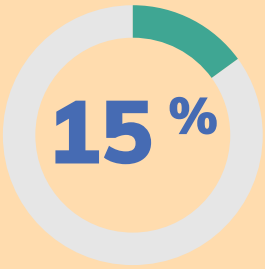
Les utilisateurs sont frustrés en raison de politiques d'accès incohérentes et d'une connectivité médiocre.



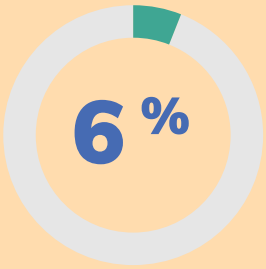
Les applications privées sont exposées à Internet pour être accessibles, ce qui les rend vulnérables aux attaques.



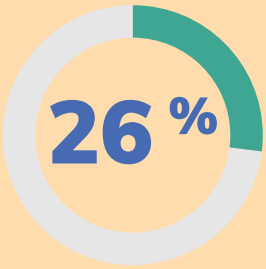
Les collaborateurs et les utilisateurs externes ont un accès intégral au réseau de l'entreprise, ce qui accentue le risque de propagation de menaces en interne.



Nous effectuons un backhauling du trafic des utilisateurs distants vers nos data centers pour leur permettre d'accéder aux applications privées, ce qui ralentit leur connexion Internet.



Nous connectons les utilisateurs présents au bureau ou sur les sites distants à nos data centers pour leur permettre d'accéder à des applications privées, ce qui freine les performances.



Nous n'avons été confrontés à aucun de ces scénarios.

Source : Enquête 2022 sur les environnements de travail hybride et sécurisé de HMG Strategy, auprès de 138 DSI, DSSI et professionnels de la technologie, réalisée aux deuxième et troisième trimestres 2022.

Vers une stratégie Zero Trust

Avec les risques de sécurité associés aux dispositifs personnels non gérés et utilisés dans le cadre du télétravail, l'utilisation des réseaux privés virtuels (VPN) a vulnérabilisé de nombreuses entreprises. En y associant les vulnérabilités résultant d'un accès à privilèges trop importants aux applications, et il est clair que l'infrastructure traditionnelle mise en place par de nombreuses entreprises pour accompagner les collaborateurs hybrides n'est tout simplement plus viable.

Ce ne sont là que quelques-unes des raisons pour lesquelles la majorité des DSSI et professionnels de la sécurité adoptent des architectures modernes Zero Trust pour renforcer leur ligne de défense et protéger les entreprises de bout en bout.

« Avant tout, une solution d'accès réseau Zero Trust améliore les performances de sécurité en réduisant la surface d'attaque », souligne Bryan Green. « De plus, le ZTNA améliore radicalement l'expérience des utilisateurs et les performances. »

Face à la généralisation du travail hybride, les décisionnaires IT envisagent sérieusement des alternatives à une architecture traditionnelle de sécurité. Renforcer la sécurité tout en dopant la productivité a été le facteur qui a incité la majorité des entreprises à adopter ZTNA. Toutes les entreprises qui ont adopté le Zero Trust ont constaté une réduction considérable des coûts et de la complexité, ce qui leur permet de se recentrer davantage sur leur cœur de métier.

Éléments qui favorisent l'adoption du Zero Trust

Plus de 35 % des personnes interrogées envisagent de privilégier le Zero Trust par rapport aux solutions traditionnelles pour protéger leur parc technologique et leurs collaborateurs dans un environnement de travail hybride.

Qu'est-ce qui a incité votre entreprise à adopter une stratégie de sécurité Zero Trust ?

29 %

Nous envisageons d'adopter une sécurité Zero Trust mais n'avons pas encore pris de décision.

Nous avons compris que les pare-feu et les VPN traditionnels sont plus facilement contournés par les assaillants et leur permettent de se déplacer librement en interne.	21 %
Nous sommes passés à une stratégie Zero Trust pour permettre une connectivité sécurisée et flexible des collaborateurs hybrides.	20 %
Nous avons compris que les pare-feu et les VPN traditionnels élargissaient la surface d'attaque.	15 %
Nous ne prévoyons pas, pour l'instant, d'adopter une stratégie de sécurité Zero Trust.	15 %

Source : Enquête 2022 sur les environnements de travail hybride et sécurisé de HMG Strategy, auprès de 138 DSI, DSSI et professionnels de la technologie, réalisée aux deuxième et troisième trimestres 2022.

« Imaginons qu'un acteur malveillant s'introduise ou pirate une partie de l'infrastructure de votre environnement. Pour neutraliser l'attaque, vous devez vous assurer que l'assaillant ne peut pas se mouvoir au sein de votre entreprise », explique Bryan Green. « Plus important, vous devez vous assurer qu'il n'est pas en mesure d'exfiltrer des données de votre environnement et détourner vos éléments de propriété intellectuelle, vos informations confidentielles ou vos données clients. Je pense que ces trois éléments constituent l'une des raisons les plus convaincantes pour adopter une solution Zero Trust pour sécuriser les accès. »

Une stratégie Zero Trust offre également des avantages supplémentaires sur un marché du travail concurrentiel. **84 %** des décisionnaires technologiques qui ont participé à l'étude de HMG Strategy pensent que le fait de promouvoir un modèle de travail hybride flexible et sécurisé contribue à la capacité de leur entreprise à attirer et fidéliser les talents.

« Je pense que le pourcentage élevé de décisionnaires qui font ce lien reflète la flexibilité et la liberté avec lesquelles les collaborateurs choisissent de travailler », conclut Bryan Green.

55 % des personnes interrogées dans le cadre de l'étude de HMG Strategy affirment que le passage au travail hybride a incité leur entreprise à réévaluer son infrastructure traditionnelle d'accès à distance.

Entre-temps, alors que de nombreuses équipes de direction se sont concentrées sur les coûts, la transition des fonctions traditionnelles, obsolètes et coûteuses, vers une infrastructure moderne Zero Trust, permet aux entreprises de répondre de manière rapide et flexible à la versatilité des conditions du marché, tout en maîtrisant les coûts et les risques auxquels elles sont exposées.

En se substituant à des fonctionnalités hétérogènes de sécurité, une architecture Zero Trust permet aux équipes de sécurité de simplifier et de gérer plus efficacement leur panel fonctionnel. « Évoluer vers un modèle Zero Trust permet de consolider les fonctions de sécurité et vous pouvez déployer et piloter nombre d'entre elles à partir d'une interface unique », fait remarquer Bryan Green.

Depuis le basculement vers un mode de travail digital en mars 2020, les collaborateurs ont démontré à quel point ils peuvent être productifs en mode télétravail et à quel point ils aspirent à plus de flexibilité entre vie personnelle et professionnelle. Il est devenu de plus en plus évident que l'environnement de bureau traditionnel, basé sur huit heures par jour, appartient au passé. Il est clair que les technologies traditionnelles telles que les VPN n'offrent pas la flexibilité et la protection nécessaires pour sécuriser les données sensibles dans un environnement de travail hybride. Une nouvelle approche, plus efficace, est nécessaire.

Selon notre expert, « le Zero Trust constitue pour les entreprises une opportunité exceptionnelle d'améliorer leur mode de fonctionnement dans un environnement de travail hybride ».

Les technologies Zero Trust qui sécurisent le travail hybride

Parmi les technologies Zero Trust suivantes, quelles sont celles que votre entreprise utilise actuellement pour sécuriser le travail hybride ?

19 %
Authentification multifacteur

16 %
Sécurité des terminaux (endpoints)

14 %
Pare-feu cloud

10 %
Protection contre la perte de données

9 %
Passerelle Web sécurisée

32 %
Autres

Source : Enquête 2022 sur les environnements de travail hybride et sécurisé de HMG Strategy, auprès de 138 DSI, DSSI et professionnels de la technologie, réalisée aux deuxième et troisième trimestres 2022.

À propos de HMG Strategy

HMG Strategy est une plateforme digitale mondiale qui permet aux décisionnaires technologiques de repenser leur entreprise et de remodeler le monde des affaires. Le réseau mondial de HMG Strategy est composé de plus de 400 000 DSI, CTO, DSSI, CDO, professionnels des technologies, de la recherche et du capital-risque, ainsi que d'experts métiers et de leaders d'opinion de renommée mondiale.

À propos de Zscaler

Zscaler accélère la transformation digitale de ses clients pour qu'ils gagnent en agilité, en efficacité, en résilience et en sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quelle que soit leur localisation. Adossée à plus de 150 data centers dans le monde, Zero Trust Exchange, basée sur le SASE, est la plus grande plateforme de sécurité cloud opérant en mode inline.