Enterprise Strategy Group | Getting to the bigger truth.™

LIVRE BLANC ESG

L’évolution du ZTNA au service des stratégies Zero Trust

Par John Grady, Analyste senior d’ESG

Mai 2022

Ce livre blanc ESG a été rédigé pour Palo Alto Networks.
Il est diffusé sous licence de TechTarget, Inc.

Sommaire

Avant-propos

Pendant la pandémie, l'accès réseau Zero Trust (ZTNA) s'est avéré primordial pour permettre aux organisations d'autonomiser leurs télétravailleurs en offrant des solutions capables de renforcer la sécurité, l'évolutivité et la facilité de gestion, contrairement aux seuls réseaux privés virtuels. Le passage au travail hybride et à distance a eu un impact profond et durable, non seulement sur le lieu, mais aussi sur les modes de travail. Désormais, le travail ne désigne plus un endroit, mais bel et bien une activité. À l'heure où les entreprises s'adaptent à ce nouveau modèle hybride basé sur des utilisateurs et applications distribués, les équipes IT, réseau et de sécurité se heurtent à de nouvelles difficultés, à savoir un élargissement colossal de la surface d'attaque dû aux connexions « direct-to-app ».

Pour faire face à cette tendance, les organisations ont déployé des solutions ZTNA, modernisant ainsi leur infrastructure afin d'offrir les fonctionnalités réseau et de sécurité nécessaires dans un SASE en mode cloud. Résultat : des connexions « direct-to-app » au plus près des applications et des utilisateurs. Toutefois, à bien des égards, les solutions de première génération/ZTNA 1.0 ne permettent pas l'instauration d'un véritable modèle Zero Trust. De fait, elles octroient trop de droits d'accès. En outre, une fois ces droits accordés dans les solutions ZTNA 1.0, la connexion est implicitement et indéfiniment considérée comme sûre, ce qui ouvre une brèche au profit des menaces avancées et des activités et comportements malveillants.

Applications, menaces, travail hybride… Il est temps d'adopter une nouvelle approche du ZTNA, conçue de A à Z pour répondre aux problématiques actuelles. Vous découvrirez dans ce livre blanc les raisons d'être de cette approche novatrice et ses fonctionnalités indispensables (principe du moindre privilège, vérification permanente du niveau de confiance, etc.), basées sur les activités et comportements utilisateurs et sur le contexte global de l'entreprise – ainsi que les mesures d'inspection destinées à protéger les données et applications, où qu'elles se trouvent. Nous examinerons également la nouvelle approche du ZTNA qui sous-tend les solutions Palo Alto Networks Prisma Access en mode cloud. Enfin, les dirigeants y trouveront des conseils pour libérer tout le potentiel de la technologie ZTNA 2.0 afin de réduire les risques liés aux environnements de travail d'aujourd'hui.

Applications, menaces, travail hybride… Il est temps d'adopter une nouvelle approche du ZTNA, conçue de A à Z pour répondre aux problématiques actuelles.

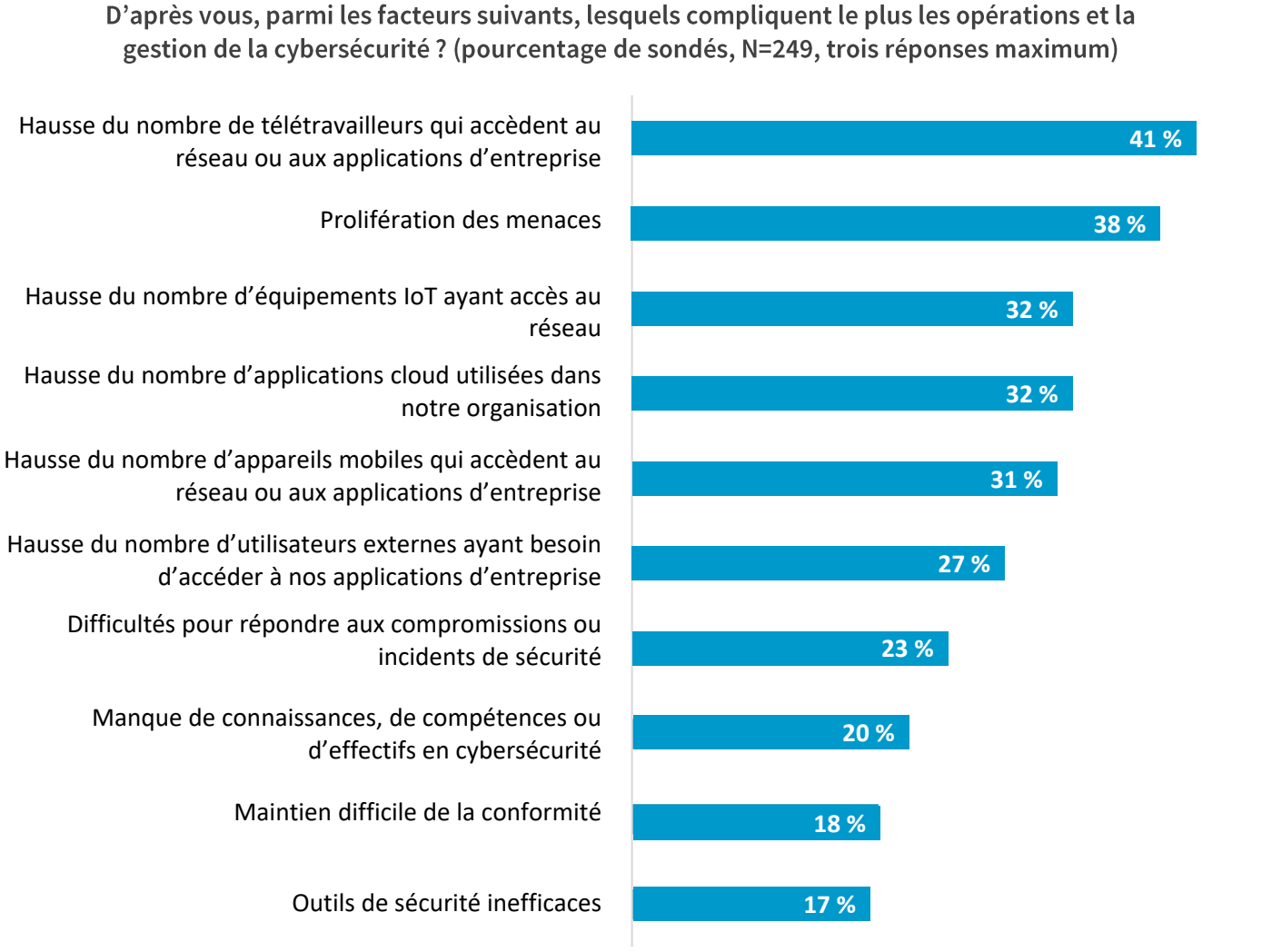
Problèmes d'accès dans les nouveaux environnements de travail

La pandémie a révélé que le travail hybride et à distance était non seulement possible, mais plébiscité par une grande proportion de collaborateurs. Ainsi, ce qui n'était au départ qu'un moyen de répondre à la crise sanitaire permet désormais aux entreprises de booster leur efficacité et leur productivité tout en satisfaisant les besoins de leurs employés. Toutefois, l'ampleur et la cadence de cette transition ont grandement compliqué la tâche des équipes IT, réseau et de sécurité. D'après une étude d'ESG, 59 % des dirigeants déclarent que la cybersécurité est devenue plus complexe ces deux dernières années.[1]

Pour les sondés, cette complexité croissante est due en majeure partie à une hausse du nombre de télétravailleurs qui accèdent au réseau et aux applications d'entreprise. Outre le problème des accès à distance, les dirigeants mentionnent des soucis liés à l'évolution des menaces, à l'augmentation du nombre d'applications cloud utilisées dans leur organisation et au besoin de connecter des utilisateurs externes aux ressources de leur entreprise (cf. figure 1).[2]

[1] Source : résultats d'une enquête d'ESG, *The State of Zero Trust Security Strategies,* mai 2021.
[2] Ibid.

Figure 1. Complexité de la cybersécurité : les facteurs d'influence

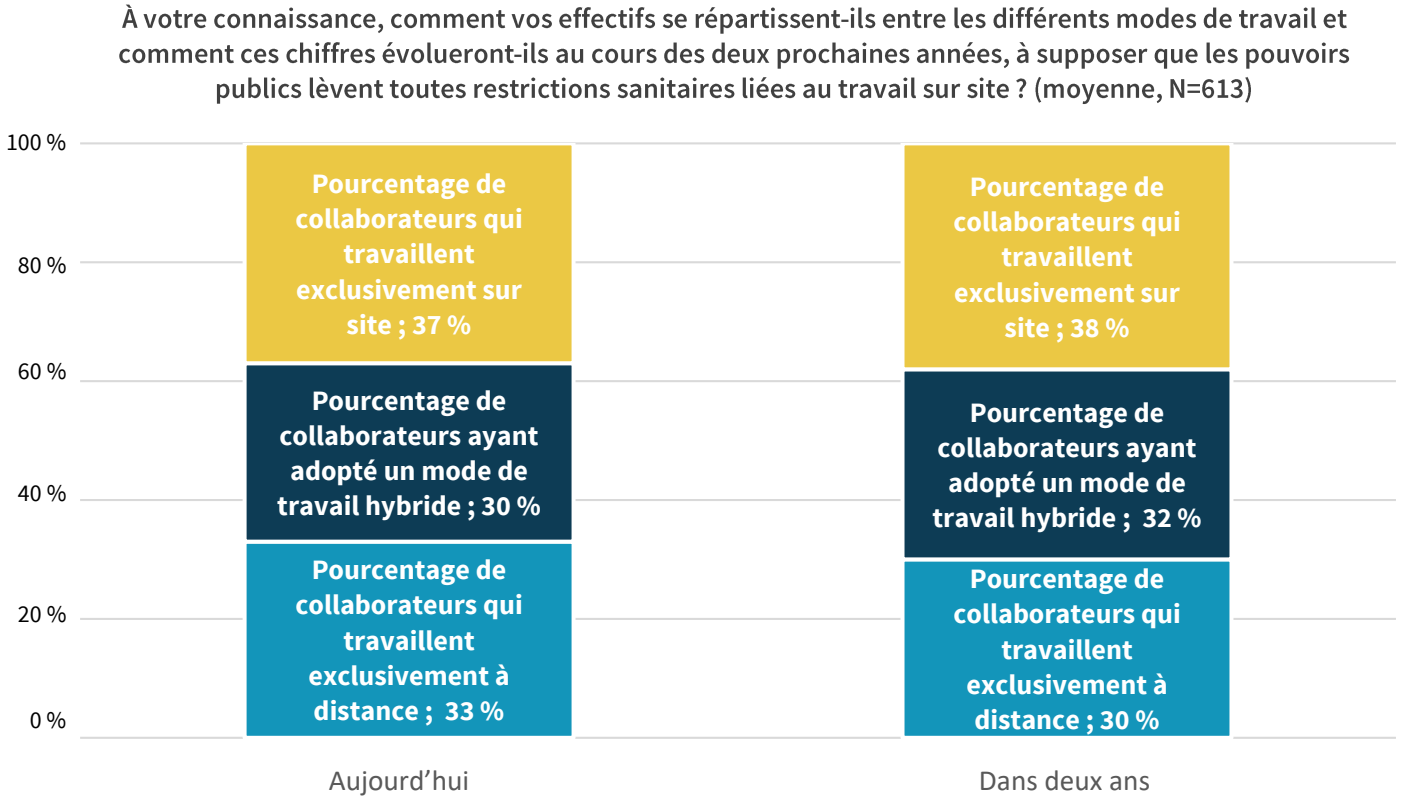


Source : ESG, une division de TechTarget, Inc.

Si les raisons qui sous-tendent l'adoption du télétravail ont changé, cette transition aura malgré tout un impact durable. D'abord simple solution transitoire à la crise, elle a donné naissance à de nouveaux modes de travail hybrides, que les collaborateurs attendent voire exigent dans de nombreux cas. Il ne serait ni réaliste ni viable de vouloir revenir en arrière. D'après une étude d'ESG, plus de 60 % des collaborateurs travaillent désormais dans un environnement hybride ou complètement à distance. Plus éloquent encore, ce chiffre devrait rester relativement stable au cours des deux prochaines années (cf. figure 2).[3]

[3] Source : intégralité des résultats de l'enquête d'ESG, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased*, décembre 2021.

Figure 2. De nouveaux modes de travail hybrides



Source : ESG, une division de TechTarget, Inc.

Dans ce monde du travail métamorphosé naissent de nouvelles problématiques liées à la sécurisation des télétravailleurs et à l'accès des utilisateurs au réseau d'entreprise et aux applications critiques. Outre une surface d'attaque bien plus vaste, le réacheminement du trafic vers un data center via le réseau d'entreprise (backhauling) laisse peu à peu la place à un modèle davantage basé sur les connexions « direct-to-app » et l'edge computing.

Dans le même temps, grâce à des moyens en hausse et, dans certains cas, au soutien des États, les assauts des cybercriminels se font de plus en plus sophistiqués. Pour couronner le tout, les attaquants se concentrent sur les failles exposées par les effectifs hybrides et à distance, ainsi que sur les points faibles inhérents aux solutions réseau et de sécurité existantes. En clair, une nouvelle approche s'impose dès maintenant.

Adoption du ZTNA et du modèle Zero Trust

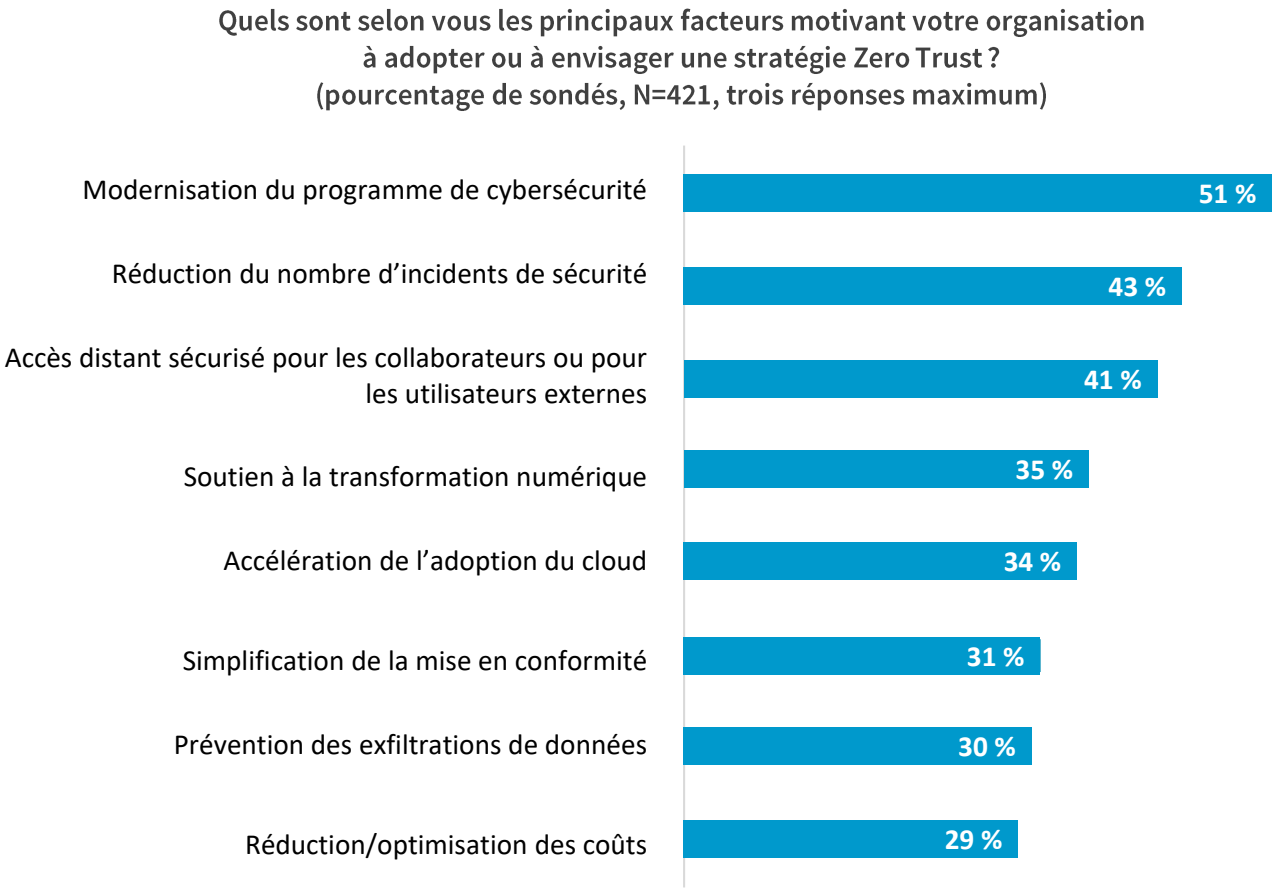
Compte tenu des problématiques en présence, il ne fait aucun doute que le ZTNA et le modèle Zero Trust constituent des éléments clés des approches réseau et de sécurité associées au monde du travail hybride. Lorsqu'il est correctement implémenté, le modèle Zero Trust réduit les risques de compromission, simplifie la gestion et l'application des politiques et renforce la sécurité des utilisateurs, des applications et des données. Toutefois, bien que le terme « Zero Trust » soit apparu dès 2010, ce modèle tarde à prendre racine au sein des entreprises. En effet, d'après une enquête d'ESG, 54 % des sondés déclarent que l'initiative Zero Trust de leur organisation date de moins de deux ans.[4]

Les entreprises envisagent d'implémenter une stratégie Zero Trust pour plusieurs raisons, notamment afin d'atteindre des objectifs IT généraux (transformation numérique, accélération de l'adoption du cloud, etc.). Parmi les motivations les plus

[4] Source : résultats d'une enquête d'ESG, *The State of Zero Trust Security Strategies*, mai 2021.

courantes figurent la modernisation de la cybersécurité et la sécurisation des accès distants des collaborateurs et des utilisateurs externes (cf. figure 3).[5]

Figure 3. Facteurs d'adoption du modèle Zero Trust



Source : ESG, une division de TechTarget, Inc.

L'expansion éclair du télétravail pendant la pandémie explique elle aussi l'intérêt accru pour le Zero Trust et les nouvelles attentes vis-à-vis de ce modèle. Manque d'évolutivité, dépendance matérielle, besoin du backhauling, droits d'accès excessifs… L'essor du travail à distance au cours de la crise sanitaire a révélé les nombreuses lacunes opérationnelles et de performance liées aux accès distants par VPN.

Ces lacunes ont grandement contribué à l'essor du modèle Zero Trust en tant que framework, mais aussi et surtout à celui de l'accès réseau Zero Trust comme alternative viable et plus sûre aux VPN. D'après une étude d'ESG, 69 % des entreprises utilisent le ZTNA et ont abandonné les VPN ou prévoient de s'en passer.[6] Le ZTNA offre d'autres avantages par rapport aux VPN :

- Les utilisateurs ne peuvent voir que les applications et services pour lesquels ils bénéficient d'un droit d'accès explicite.
- Les applications sont invisibles depuis l'Internet public.
- Dans la plupart des cas, les solutions ZTNA sont proposées en mode cloud.

[5] Ibid.
[6] Source : intégralité des résultats de l'enquête d'ESG, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased*, décembre 2021.

Toutefois, si les solutions ZTNA 1.0 existantes représentent un progrès indispensable par rapport aux VPN, l'essor constant du télétravail, des modes de travail hybrides et du cloud hybride, ainsi que l'explosion du nombre d'applications de nouvelle génération, révèlent les faiblesses de cette technologie qu'il convient de corriger.

Raisons d'être d'une nouvelle approche ZTNA

Les principales faiblesses des solutions ZTNA 1.0 existantes concernent les contrôles d'accès, le principe du moindre privilège, le manque de visibilité et un modèle basé sur la confiance, mais dans lequel les vérifications sont rares. En clair, ces solutions négligent certains principes du modèle Zero Trust. Parmi les points faibles des approches ZTNA 1.0 :

1. Principe du moindre privilège : les solutions ZTNA 1.0 sont conçues pour assurer un contrôle grossier des accès. Cela va à l'encontre du principe du moindre privilège puisqu'elles traitent les applications comme un bloc réseau des couches 3-4 (IP et port). Les utilisateurs bénéficient alors d'un accès trop vaste par rapport à leurs besoins. Ces solutions négligent également d'autres informations contextuelles sur les applications qui pourraient leur permettre de vérifier les utilisateurs et les appareils, y compris les applications utilisées, l'heure, la géolocalisation, etc.

2. « Autoriser et ignorer » : une fois l'accès à une application octroyé, les communications qui en résultent sont implicitement et définitivement considérées comme sûres. En clair, la solution ne remet plus jamais en cause le comportement de l'utilisateur et de l'application. Inadaptée à l'environnement actuel, cette stratégie dévie du modèle Zero Trust, car elle ne permet pas de prévenir les compromissions qui passeraient par des activités autorisées.

3. Pas d'inspection de sécurité : les solutions d'aujourd'hui supposent que le trafic est sécurisé, sans l'inspecter et sans pouvoir détecter et neutraliser les malwares et les déplacements latéraux d'une connexion à l'autre une fois qu'un utilisateur a accès à une application. Elles accordent des droits d'accès, mais ne disposent d'aucune visibilité ni d'aucun contrôle sur le trafic, ce qui accroît le risque de compromission de données.

4. Protection des données limitée, voire inexistante : les solutions actuelles offrent peu ou pas de visibilité et de contrôle sur les données sensibles. C'est pourquoi les entreprises ont souvent recours à d'autres solutions pour sécuriser les données sensibles des applications privées et SaaS ou Internet. Seulement voilà, elles créent alors des approches cloisonnées et disparates qui accroissent la complexité de leur environnement et les exposent au risque d'exfiltration de données par des attaquants ou des menaces internes. Les entreprises d'aujourd'hui doivent pouvoir contrôler leurs données sur toutes les applications, à partir d'une seule politique DLP.

5. Plateformes distinctes pour les applications cloud et sur site : d'après une enquête d'ESG, les organisations recherchent avant tout des technologies Zero Trust capables de couvrir à la fois leurs environnements cloud et sur site.[7] Or, de nombreuses solutions ZTNA sont conçues soit pour les applications sur site, soit pour les applications cloud, mais pas les deux. Une approche moderne doit tout englober afin de réduire les risques et la complexité.

Caractéristiques clés des solutions ZTNA modernes

Pour répondre aux problématiques des nouveaux environnements de travail, les solutions ZTNA doivent combler ces lacunes. Sans quoi les organisations investiront dans des solutions qui offrent un niveau de sécurité insuffisant pour notre époque. Outre la réduction des risques, les dirigeants doivent recourir à des produits qui tiennent compte de l'expérience utilisateur, des performances et de la facilité de gestion. Pour relever les défis liés au travail hybride, au cloud hybride et

[7] Source : résultats d'une enquête d'ESG, *The State of Zero Trust Security Strategies*, mai 2021.

aux applications modernes, la nouvelle génération de solutions ZTNA doit impérativement remplir un certain nombre de critères :

- Recentrage sur les applications : elles doivent se concentrer sur la couche 7, et non uniquement sur l'accès et les politiques réseau. Il sera alors possible d'opérer au niveau des couches 3 à 7 afin d'appliquer le principe du moindre privilège sans concession pour une granularité maximale du contrôle d'accès aux niveaux applicatifs et sous-applicatifs. Ainsi, les utilisateurs seront moins susceptibles d'avoir accès à trop de ressources.

- Évaluation continue basée sur les comportements : dans un modèle ZTNA 2.0, une fois l'accès à une application octroyé, ce droit est constamment réévalué sur la base de différents facteurs comme les activités et les comportements des utilisateurs et le contexte global de l'entreprise. En cas de détection d'activités suspectes ou d'exfiltration potentielle de données, il est possible de révoquer l'accès à une application en temps réel.

- Inspection de sécurité permanente : une fois la connexion établie, il est nécessaire d'inspecter constamment tout le trafic, même les connexions autorisées, afin de prévenir toutes les menaces, y compris les attaques zero-day. Cette fonctionnalité s'avère primordiale en cas de vol d'identifiants d'utilisateurs légitimes destiné à lancer des attaques contre des applications ou l'infrastructure.

- Protection de toutes les données : le modèle ZTNA 2.0 offre une visibilité et un contrôle complets et homogènes sur les données sensibles, quelle que soit l'application, et ce à partir d'une seule et même console de gestion et d'une politique unique. Mieux encore, ce nouveau modèle permet d'appliquer la DLP d'entreprise à toutes les données, où qu'elles se trouvent (anciennes applications sur site, cloud public ou SaaS).

- Couverture complète des applications : les solutions ZTNA 2.0 qui couvrent toutes les applications (publiques, privées/sur site et cloud) et tous les modèles d'accès aux données (à distance et hybride) permettent la mise en place d'un vrai modèle d'architecture Zero Trust au lieu de simples accès distants. Elles doivent également procéder à une inspection régulière et approfondie du trafic afin de veiller à sa sécurité. C'est ainsi qu'elles aident à stopper toutes les menaces à l'aide du machine learning, notamment par la prévention inline des menaces zero-day.

Pour combler les lacunes des solutions ZTNA 1.0 existantes, les dirigeants doivent également privilégier des produits qui non seulement résolvent les problèmes actuels, mais répondent aussi aux besoins de demain en matière de réduction des risques et d'expansion des environnements de travail hybrides. Lorsque le ZTNA fait partie intégrante d'une plateforme SASE plus vaste, les organisations peuvent bénéficier d'une gestion cohérente et simplifiée, ce qui favorise l'efficacité opérationnelle et garantit une application homogène des politiques et règles d'accès à toutes les applications et tous les utilisateurs de l'environnement. Dans le même temps, il est essentiel de préserver l'expérience utilisateur. À l'heure où les modèles hybrides deviennent la norme, les modes d'accès des collaborateurs à leurs applications professionnelles doivent rester sensiblement les mêmes où qu'ils se trouvent.

Palo Alto Networks Prisma Access : le ZTNA 2.0 en mode cloud

Récemment, Palo Alto Networks a apporté des améliorations à sa solution Prisma Access afin de répondre aux besoins d'accès distant/Zero Trust des environnements de travail hybrides. Cette solution en mode cloud offre une expérience d'accès réseau Zero Trust résolument 2.0. Parmi ses fonctionnalités clés :

- Contrôle granulaire des utilisateurs, des applications et des accès pour une sécurité intégrale. Prisma Access permet aux entreprises d'appliquer le principe du moindre privilège sans concession sur les couches 3 à 7, grâce à des contrôles déployés aux niveaux stratégiques : application, sous-application, fonctions et activités. Le principe s'applique alors indépendamment de l'utilisateur, de l'application et du lieu de la connexion.

- Vérification continue du niveau de confiance basée sur les comportements. En cas de comportement suspect ou d'exfiltration potentielle de données, il est possible de révoquer l'accès à une application en temps réel afin de réduire le risque et les dégâts éventuels. La vérification continue du niveau de confiance met ainsi fin à l'approche du ZTNA 1.0 qui consiste à ne jamais remettre en cause les droits d'accès.

- Inspection régulière et approfondie pour un trafic sécurisé. Grâce à un traitement du trafic « single-pass », Prisma Access recherche tous les types de menaces sans nuire aux performances et aux temps de latence. Les fonctionnalités de machine learning permettent de neutraliser les menaces inline, sans signatures. Dans le cadre d'une plateforme plus vaste, Prisma Access intègre entre autres la prévention des menaces, l'analyse des malwares, le filtrage d'URL avancé et la sécurité DNS.

- Sécurisation permanente de toutes les applications, quel que soit le mode d'accès. Le ZTNA 2.0 de Prisma Access prend en charge tous les utilisateurs et toutes les applications dans l'entreprise : sur site, cloud public, SaaS, ancienne génération et modernes/cloud-native. Les utilisateurs peuvent s'y connecter avec ou sans agent et bénéficier de la même protection quoi qu'il arrive.

- Protection des données où qu'elles se trouvent. Prisma Access contrôle les données de la même façon sur toutes les applications utilisées dans l'entreprise, conformément à une seule et même politique DLP. Résultat : les données et les accès sont sécurisés en toutes circonstances. Conçue dans le cloud, la solution de Palo Alto Networks s'appuie sur les niveaux d'élasticité et de disponibilité des géants du cloud public pour protéger les données à grande échelle.

- Gestion unifiée et expérience utilisateur homogène. La plateforme unifiée Prisma Access simplifie les tâches de gestion et de déploiement des équipes réseau et de sécurité tout en offrant une expérience utilisateur homogène, résiliente et ultraperformante, quels que soient l'application et l'appareil, et où qu'ils se trouvent. Son architecture permet un taux de disponibilité de 99,999 %, des temps de traitement de 10 ms et des niveaux de service élevés sur les applications SaaS. Prisma Access intègre également le module ADEM (Autonomous Digital Experience Management) en natif. Sa fonction : identifier les problèmes en amont, les isoler et les résoudre avant qu'ils n'impactent les utilisateurs.

Conclusion

Les organisations ont la lourde tâche d'autonomiser leurs télétravailleurs et leurs collaborateurs hybrides. À l'heure où les applications et les utilisateurs sont partout, une nouvelle architecture s'impose : il faut abandonner le backhauling au profit de connexions « direct-to-app ». Seulement voilà, cette transformation n'est pas sans conséquence pour la sécurité des entreprises, surtout face à des menaces de plus en plus sophistiquées qui ciblent les utilisateurs distants.

Si les solutions d'accès réseau Zero Trust ont temporairement permis aux organisations de s'adapter aux nouveaux modes de travail favorisés par la pandémie, le développement constant du télétravail et des environnements professionnels hybrides a révélé les lacunes de cette technologie. Il est indispensable de combler ces dernières afin de répondre aux exigences de flexibilité, de productivité et de sécurité des collaborateurs ayant adopté un mode de travail hybride.

Véritable pionnier de la sécurité des réseaux et des terminaux, du modèle Zero Trust et des accès distants, Palo Alto Networks a identifié les points faibles des solutions d'accès réseau Zero Trust 1.0 pour mieux les éliminer. Sa plateforme Prisma Access intègre le ZTNA 2.0 pour renforcer la sécurité des entreprises.Il s'agit de la première solution ZTNA à offrir de vraies fonctionnalités Zero Trust : accès selon le principe du moindre privilège, vérification continue du niveau de confiance basée sur les comportements, inspection de sécurité régulière et approfondie, ou encore contrôle cohérent des données sur toutes les applications. En outre, Prisma Access repose sur un modèle de gestion et de plateforme unifié, ce qui garantit des performances et des expériences utilisateur homogènes.

Enterprise Strategy Group est un cabinet intégré d'études et de stratégie dont les analyses, les enquêtes et les services de contenus « go-to-market » livrent des éclairages concrets à la communauté IT mondiale.

www.esg-global.com contact@esg-global.com +1 508 482 0188