Juillet 2022

RESEARCH
Influence and insight
through social media

ZTNA 2.0

Un impératif à l'ère du travail hybride

LIVRE BLANC

Rédigé par
Zeus Kerravala

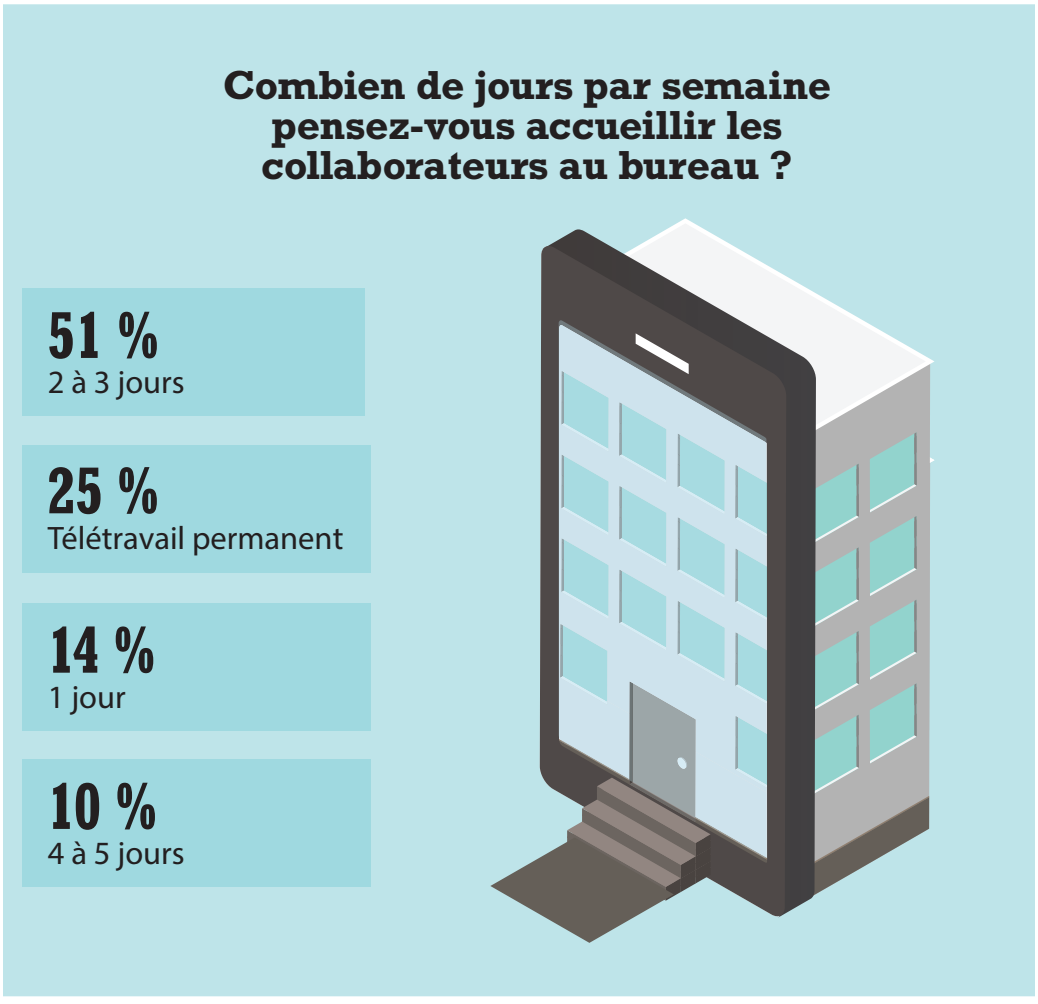
ZK Research
Une division de
Kerravala Consulting

INTRODUCTION : LE MODÈLE HYBRIDE EST DEVENU LA NORME

La pandémie de COVID-19 a provoqué des bouleversements majeurs à l'échelle mondiale, en particulier dans le monde du travail. Pour faire face à la situation d'urgence, les entreprises ont dû déployer en quelques mois des projets de transformation numérique qu'elles avaient à l'origine bâtis et planifiés sur plusieurs années. La plupart des salariés ont aujourd'hui basculé en télétravail, et cette tendance est bien partie pour s'inscrire dans la durée. C'est en tout cas ce qui ressort d'une étude menée en 2022 par ZK Research : alors que seuls 22 % des collaborateurs opéraient régulièrement en télétravail avant le début de la crise sanitaire, 51 % exerceront désormais leurs fonctions en distanciel entre deux et trois jours par semaine, et 14 % le feront sur la base d'un jour par semaine (figure 1). Toutes ces données indiquent que le nouveau monde du travail sera hybride.

Pour bon nombre d'entreprises, un retour en présentiel à temps plein n'est même pas du tout envisageable. Brent Hyder, président et Chief People Officer chez Salesforce, a confié à MarketWatch que l'éditeur de logiciels comptait moderniser ses locaux en se débarrassant de ses rangées de bureaux à l'ancienne. L'une des raisons invoquées est que 65 % de ses 54 000 employés devraient ne travailler en présentiel que trois jours par semaine (contre 40 % avant la pandémie). D'autres grands noms, comme Microsoft et Google, ont eux aussi adopté des modèles de travail hybride.

Figure 1 : Le nouveau monde du travail sera hybride



Étude ZK Research 2022 Work-from-Anywhere

À PROPOS DE L'AUTEUR

Zeus Kerravala est le fondateur et analyste en chef de ZK Research. Il fournit des conseils tactiques et un accompagnement stratégique à ses clients pour les aider à faire face au contexte actuel et à se projeter dans le plus long terme. Ses études et analyses offrent des éclairages aux acteurs de tous horizons : responsables IT et réseau, constructeurs de matériels informatiques, éditeurs de logiciels, entreprises de services du numérique (ESN) et toutes celles et ceux qui envisagent d'investir dans les secteurs couverts par ZK.

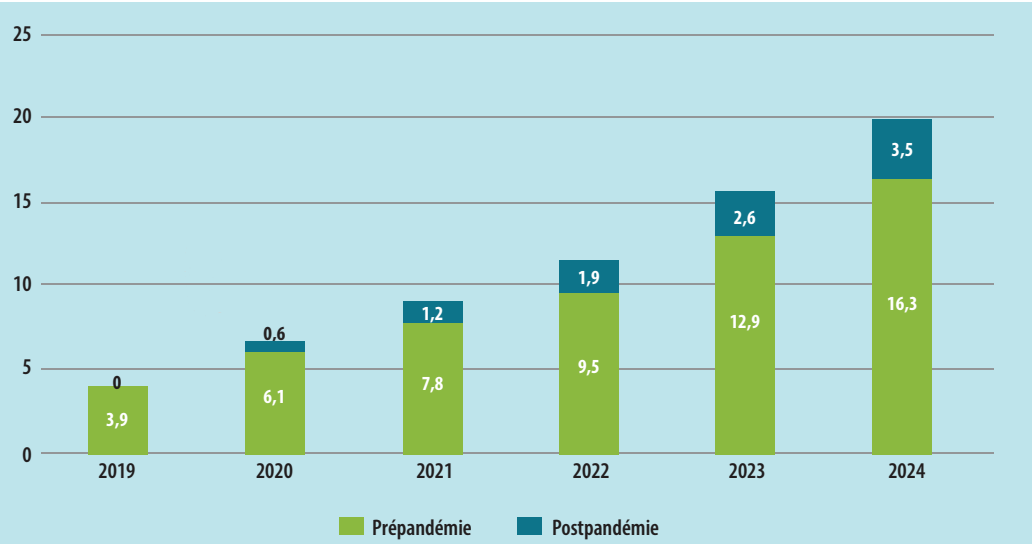
Ces nouveaux modes d'organisation ont été longuement repris et décortiqués dans les médias, notamment en ce qui concerne la façon dont ils transforment le rapport au travail – en particulier chez les professionnels pour qui la collaboration est essentielle. En revanche, ce dont on parle moins, c'est leur incidence sur l'IT d'entreprise, y compris les profonds changements induits au niveau de l'utilisation et du déploiement. Par exemple :

L'adoption du cloud s'accélère et son modèle évolue. Les réseaux cloud s'écartent du modèle centralisé au profit d'une infrastructure distribuée, où les workloads et les applications s'étendent à plusieurs clouds privés, publics et sites en périphérie, le fameux Edge. En faisant tomber les barrières physiques, les services cloud sont tout naturellement voués à donner l'impulsion aux modèles de travail hybride. L'état des lieux WFA (Work-From-Anywhere) 2022 dressé par ZK Research rapporte que 64 % des entreprises ont augmenté leurs dépenses consacrées au cloud public, tandis que 58 % ont revu à la hausse leurs budgets destinés aux clouds privés.

L'accès distant a besoin d'une refonte. Les entreprises doivent se préparer à gérer une majorité de télétravailleurs sur le long terme. Lorsque la pandémie a éclaté, les VPN (réseaux privés virtuels) ont fait office de solution de secours pour connecter les salariés à distance. Mais faute d'une sécurité (accès ouverts aux réseaux) et de performances (backhaul du trafic par le data center) suffisantes, ces outils ne forment pas une alternative viable dans la durée. C'est pourquoi les organisations cherchent à renforcer leur connectivité à l'aide de solutions SD-WAN (Software-Defined WAN) et SASE (Secure Access Service Edge) pour connecter et sécuriser l'environnement de télétravail. Ceci explique la croissance qu'enregistre le marché du SD-WAN depuis la pandémie (voir figure 2).

La DSI exerce un contrôle moins direct sur l'infrastructure. Il y a dix ans, les équipes informatiques dictaient encore quels appareils et applications les collaborateurs avaient le droit d'utiliser, où et quand ils pouvaient accéder aux ressources IT, et comment ils devaient se connecter au réseau privé de l'entreprise.

Figure 2 : Les dépenses dans le SD-WAN s'accélèrent



Rapport ZK Research 2021 SD-WAN Forecast

La sécurité des modes de travail hybrides requiert un nouveau paradigme Zero Trust : le ZTNA 2.0.

Mais aujourd'hui, cette maîtrise a périclité face à la prolifération du Shadow IT et du SaaS (Software as a Service), tandis que le SD-WAN a introduit l'accès Internet haut débit public et que le travail hybride a étendu le périmètre de l'entreprise au domicile des salariés. Les environnements informatiques, qui faisaient autrefois l'objet d'un contrôle resserré, sont devenus tout autant désorganisés qu'imprévisibles.

De toutes les disciplines de l'IT, la sécurité est peut-être la plus impactée par ces phénomènes. Désormais, les équipes SSI ont pour mission de protéger une surface d'attaque à la fois dynamique, distribuée et éphémère. Résultat, les programmes de sécurité traditionnels – bien que nécessaires – se révèlent insuffisants. Après des dizaines d'années de bons et loyaux services, les VPN sont devenus incapables de satisfaire aux nouvelles exigences de performance et de sécurité des collaborateurs. Pour répondre à ces problématiques, il est temps de mettre l'accès réseau à l'heure du Zero Trust. Toutefois, les entreprises doivent viser au-delà des solutions ZTNA (Zero-Trust Network Access) de première génération, qui ne sont ni plus ni moins que des outils d'accès classiques enrichis de quelques fonctionnalités. La sécurité du travail hybride requiert un nouveau paradigme Zero Trust : le ZTNA 2.0.

CHAPITRE I : LE ZTNA 1.0 EXPOSE LES ENTREPRISES À DES COMPROMISSIONS

Depuis quelques années, les solutions ZTNA ont connu un fort engouement par leur capacité à renforcer la sécurité en rétrécissant la surface d'attaque. Les réseaux IP, ouverts par nature, sont conçus de sorte que chaque terminal qui s'y connecte puisse communiquer avec le reste de l'infrastructure. Ce principe assure la fluidité et la rapidité d'Internet. Le problème est qu'en cas de compromission du réseau, l'attaquant obtient l'accès à l'ensemble des ressources de l'entreprise, n'hésitant pas à se tapir dans l'environnement pour agir incognito pendant des mois et causer un préjudice considérable à l'entreprise.

Le parti pris du ZTNA consiste à basculer vers un modèle axé sur le moindre privilège, où aucun dispositif ne peut communiquer avec un autre sans en avoir reçu l'autorisation explicite. Cette approche permet de réduire efficacement la surface d'attaque : en cas d'intrusion, le cybercriminel n'aura accès qu'à quelques autres systèmes – voire aucun –, limitant ainsi l'onde de choc de l'incident. Malheureusement, les solutions ZTNA de première génération présentent des lacunes qui les empêchent de concrétiser la vision initiale :

Le ZTNA 1.0 va à l'encontre de la stratégie du moindre privilège : clé de voûte du ZTNA, ce principe de sécurité ne peut être pleinement réalisé par des solutions réseau. Même si certains fournisseurs prétendent comprendre les applications ou le contrôle des accès au niveau applicatif, la plupart se cantonnent à des concepts liés au réseau (adresse IP, numéro de port, FQND [Fully Qualified Domain Names], etc.). Cette approche peut sembler relativement logique, puisque Internet repose sur ces mêmes éléments. Elle est toutefois restreinte par trois problèmes majeurs :

- **La surface d'attaque n'est pas optimisée.** La plupart des applications utilisent des ports et des adresses IP dynamiques. Par conséquent, les solutions ZTNA doivent octroyer l'accès à une vaste plage de ports et d'adresses, ce qui élargit et expose inutilement la surface d'attaque.
- **L'accès ne peut être restreint qu'au niveau applicatif.** La visibilité des solutions ZTNA 1.0 s'arrête au niveau de l'application. Autrement dit, elles ne sont pas en mesure d'en contrôler l'accès. Dans certains cas, il peut être judicieux de restreindre l'accès à des fonctions spécifiques. Pour ce faire, la solution ZTNA aurait besoin d'un accès au niveau sous-applicatif.

Les solutions de première génération n'offrent pas toutes les fonctionnalités requises pour concrétiser les promesses de sécurité du ZTNA.

- **L'environnement s'expose à des risques de latéralisation des malwares.** Les malwares écoutent souvent sur le même numéro de port ou la même adresse IP que les applications autorisées. Ils peuvent ainsi accéder à l'environnement puis se déplacer latéralement à travers l'infrastructure de l'entreprise.

La confiance est présumée dès qu'un accès est accordé : à partir du moment où un utilisateur ou une application est autorisé à accéder à l'environnement, cette communication est supposée fiable de façon implicite et permanente. C'est là l'une des principales failles du ZTNA 1.0, car toute compromission passe nécessairement par l'obtention d'un tel accès. Dès qu'un comportement devient suspect, les permissions associées doivent immédiatement être révoquées – ce que ne permet pas le ZTNA 1.0, qui repose sur le modèle « autoriser et ignorer ».

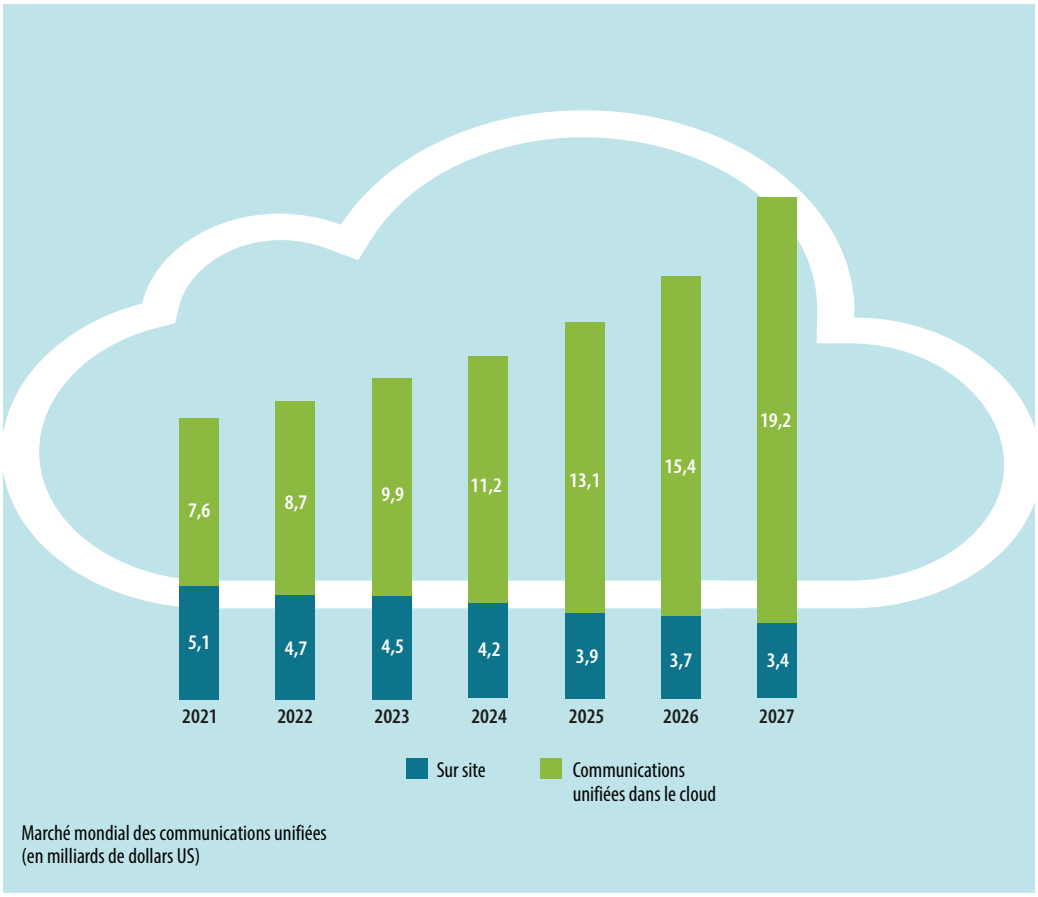
Absence d'inspection de sécurité permanente : le ZTNA 1.0 a été pensé comme un mécanisme de contrôle des accès. Ce modèle est donc incapable de détecter et d'empêcher l'intrusion de malwares, et encore moins leur latéralisation une fois qu'un utilisateur est autorisé à accéder à une application. Cette forme de sécurité par l'obscurité suppose que le trafic autorisé est exempt de tout malware ou d'autres menaces et vulnérabilités.

Aucune protection des données : les solutions ZTNA actuelles ont zéro visibilité et contrôle sur les données, ce qui expose les entreprises au risque d'exfiltration par des attaquants ou des acteurs malveillants en interne. Ce dernier cas de figure tend d'ailleurs à être sous-estimé dans les entreprises. Il représente pourtant une source considérable de perte de données : Le rapport d'enquête sur les compromissions de données (DBIR) 2021 de Verizon rapporte ainsi une hausse de 47 % de la fréquence d'attaques impliquant des acteurs internes entre 2018 et 2020, tout en soulignant que ces compromissions représentent 22 % de l'ensemble des incidents de sécurité.

Incapacité à sécuriser toutes les applications : les outils ZTNA traditionnels ne couvrent qu'un sous-ensemble d'applications privées utilisant des ports statiques. De plus, ces solutions ne sont pas en mesure de sécuriser les applications cloud-native basées sur les microservices ni celles qui emploient des ports dynamiques (applications voix et vidéo, par exemple) ou qui dépendent de connexions initiées par un serveur (helpdesk, systèmes de patching, etc.). Enfin, le ZTNA de première génération ne reconnaît tout simplement pas les applications SaaS, qui composent aujourd'hui la majorité du parc applicatif des entreprises et dont la proportion ne cesse d'augmenter. Le rapport ZK Research 2021 Global UC Forecast indique que les communications unifiées (UC) dans le cloud, qui incluent la voix et la vidéo, devraient connaître un taux de croissance annuel moyen de 21 % d'ici 2026 (figure 3). Ce segment en plein essor a mis au jour une faille béante du ZTNA 1.0.

Les solutions de première génération n'offrent pas toutes les fonctionnalités requises pour concrétiser les promesses de sécurité du ZTNA. Le modèle hybride a transformé le rapport au travail, l'utilisation des applications ainsi que l'accès à l'environnement de l'entreprise. En conséquence, le ZTNA doit lui aussi faire sa révolution.

Figure 3 : L'évolution des communications cloud est proportionnelle à l'essor du travail hybride



Rapport ZK Research 2022 Global UC Forecast

CHAPITRE II : DÉFINITION DU ZTNA 2.0

Le ZTNA 2.0 propose une refonte complète de la gestion des accès. Si les solutions de première génération s'apparentaient à une sorte de VPN évolué, les produits 2.0 ont quant à eux été spécialement conçus pour garantir en permanence l'application du moindre privilège sur toute l'infrastructure de l'entreprise. Voici les principes fondamentaux du ZTNA 2.0 :

Intervention sur la couche applicative : le ZTNA 2.0 réoriente le paradigme en passant du réseau (couche 3) à l'application (couche 7), ce qui permet de libérer le plein potentiel du Zero Trust. Ces nouvelles solutions exercent un contrôle des accès granulaire au niveau applicatif – et sous-applicatif – indépendamment des configurations réseau. Cette approche favorise ainsi la mise en œuvre concrète du principe du moindre privilège. Tout déplacement de l'utilisateur ou changement au niveau du réseau n'affecte aucunement la capacité du ZTNA 2.0 à appliquer ce principe.

Vérification continue du niveau de confiance : comme nous l'avons vu précédemment, la confiance peut être difficile, voire impossible à inscrire dans la durée. Une fois qu'un utilisateur obtient l'accès à une application, sa légitimité n'est plus jamais remise en question, ce qui permet à d'éventuelles compromissions ultérieures d'échapper aux mécanismes de détection. Le ZTNA 2.0 doit évaluer en permanence le niveau de confiance en s'appuyant sur différents critères tels que la posture de sécurité des équipements, le

Le ZTNA 2.0 assure un contrôle des données homogène sur l'ensemble du parc applicatif de l'entreprise.

comportement des utilisateurs et l'activité des applications. En cas d'anomalie, il révoque immédiatement l'accès incriminé. Par exemple, un utilisateur qui se connecte à l'autre bout du monde quelques minutes après avoir accédé localement à une application traduit un probable vol d'identifiants. De même, une application qui s'exécute soudainement sur un nouveau port peut être le signe d'un détournement.

Inspection de sécurité permanente : les solutions ZTNA 2.0 dignes de ce nom doivent assurer en permanence une inspection approfondie des paquets (DPI) sur la totalité du trafic, y compris les connexions préalablement autorisées. Cette démarche permet d'identifier et de bloquer rapidement les compromissions et les menaces zero-day. Une inspection constante de la sécurité constitue la meilleure forme de défense qui soit lorsque les identifiants d'un utilisateur légitime sont dérobés puis utilisés pour lancer des attaques contre les applications ou l'infrastructure.

Protection complète des données : le ZTNA 2.0 assure un contrôle des données homogène sur l'ensemble du parc applicatif de l'entreprise, sur site ou SaaS – rappelons que ces dernières ne sont pas reconnues par les solutions de première génération. Ces contrôles peuvent être effectués à l'aide d'une seule et même politique DLP (prévention des pertes de données), ce qui simplifie considérablement les opérations.

Protection complète des applications : programmes développés en interne, applicatifs privés, SaaS et cloud-native… le ZTNA 2.0 sécurise toutes les applications de l'entreprise. Sont également couvertes les applications utilisant des ports dynamiques ou dépendant de connexions initiées par un serveur.

CHAPITRE III : PALO ALTO NETWORKS FOURNIT DES SOLUTIONS ZTNA 2.0 COMPLÈTES

Situé en plein cœur de la Silicon Valley, Palo Alto Networks est le leader du marché de la cybersécurité, un statut que l'entreprise doit notamment à son vaste portefeuille de produits. Ces dernières années, sa plateforme Prisma Access s'est imposée comme la solution de facto pour la sécurisation et la connexion des télétravailleurs. Pionnier des solutions Zero Trust Network Access, Palo Alto figure parmi les Leaders du dernier rapport Forrester New Wave consacré au ZTNA.

Plus récemment, Prisma Access s'est enrichi de la première solution ZTNA 2.0 du marché, conçue autour d'un produit de sécurité à la fois simple et unifié qui protège les modes de travail hybrides tout en fournissant une expérience utilisateur optimale. Si de nombreux fournisseurs se targuent de proposer des produits de sécurité « cloud », la plupart sont en réalité bâtis sur des technologies traditionnelles migrées vers le cloud via une approche « lift and shift ». De son côté, Palo Alto offre une gamme de services de sécurité cloud-native modernes (passerelle web sécurisée [SWG], CASB [Cloud Access Security Broker] nouvelle génération, FWaaS [Firewall as a Service], DLP…) pour former une solution SSE inédite. Grâce à son référentiel de politiques commun et à sa gestion centralisée, Prisma Access répond idéalement aux exigences des nouveaux modes de travail hybrides, sans jamais compromettre la performance.

La plateforme de Palo Alto répond ainsi à l'ensemble des critères soulignés au chapitre III :

Accès basés sur le principe du moindre privilège : Prisma Access opère entre les couches 3 (réseau) et 7 (application) de la pile OSI (Open Systems Interconnection). Palo Alto utilise sa technologie

Prisma Access protège tous les utilisateurs ainsi que l'ensemble du parc applicatif de l'entreprise à l'aide d'un produit unifié.

brevetée App-ID pour garantir un contrôle granulaire au niveau applicatif et sous-applicatif. Cette approche lui permet notamment d'opérer un contrôle sur des fonctions spécifiques comme le chargement et le téléchargement.

Vérification continue du niveau de confiance : la solution signée Palo Alto Networks évalue continuellement le degré de confiance et de vérification grâce aux trois technologies brevetées décrites ci-après.

- **User-ID** fournit une visibilité approfondie sur les utilisateurs et surveille en permanence leur comportement afin de détecter toute activité suspecte.
- **Device-ID** offre une visibilité sur la posture de sécurité des équipements, ce qui permet de révoquer un dispositif dès que ce dernier enfreint les politiques de l'entreprise.
- **App-ID** vérifie que le trafic associé à un port donné correspond bien aux applications adéquates (par exemple, seulement des communications sécurisées sur le port 443).

Inspection de sécurité permanente : Prisma Access exploite le machine learning (ML) pour neutraliser 95 % des menaces inline, sans recourir à des signatures. En associant ces fonctionnalités innovantes aux services de sécurité cloud de Palo Alto, la plateforme bloque plus de 224 milliards de menaces par jour pour ses clients. Quant aux attaques qui ne peuvent être stoppées à l'aide d'une protection inline, elles font l'objet d'un traitement « single-pass » à travers d'autres services de sécurité en mode cloud :

- **Threat Prevention** neutralise les exploits, les communications CnC (commande et contrôle) et d'autres attaques réseau à travers toutes les applications et les protocoles.
- **WildFire** offre un vaste écosystème d'analyse antimalware qui assure une distribution rapide des signatures.
- **Advanced URL Filtering** est un outil de sécurité web qui bloque 24 % d'attaques de phishing en plus que les autres solutions du marché.
- **DNS Security** barre la route aux attaques DNS (Domain Name System).

Protection complète des données : contrairement aux solutions ZTNA 1.0, qui n'ont aucune visibilité sur l'exfiltration ou la perte de données, Prisma Access s'intègre à Enterprise DLP de Palo Alto Networks pour faire la lumière sur l'accès aux données dans toute l'entreprise. À partir d'une console unique et centralisée, les clients peuvent appliquer une politique DLP homogène à l'intégralité des données, peu importe qu'elles soient stockées au sein d'applicatifs traditionnels sur site, d'applis SaaS ou dans le cloud public.

Sécurisation de toutes les applications : Prisma Access protège l'ensemble des utilisateurs et des applications de l'entreprise à l'aide d'un produit unifié, peu importe que le collaborateur se connecte ou non par le biais d'un agent. Sa couverture s'étend à tous les applicatifs (sur site, cloud public, SaaS, propriétaires, cloud-native).

Prisma Access accorde une place centrale à l'expérience utilisateur, sur laquelle Palo Alto Networks s'engage par des accords de niveau de service (SLA) garantissant une disponibilité de 99,999 % et des temps de traitement sous la barre des 10 ms. ZK Research estime que Palo Alto Networks est le seul fournisseur

Figure 4 : L'architecture cloud-native de Prisma Access modernise le ZTNA

Palo Alto Networks et ZK Research, 2022

ZTNA 2.0 capable de garantir des engagements SLA de performance pour les applications SaaS tierces.

Certes, rien ne vous empêche de monter de toutes pièces une solution ZTNA 2.0 à l'aide de produits spécialisés migrés dans le cloud. Mais ce modèle présente de fortes lacunes par rapport aux fonctionnalités de la plateforme cloud-native Prisma Access de Palo Alto Networks. Le comparatif de la figure 4 devrait suffire à vous en convaincre.

CONCLUSION ET RECOMMANDATIONS

Le modèle hybride a changé à jamais le monde du travail, créant par là même de nouvelles exigences pour la connexion et la sécurité des collaborateurs. Les VPN et le ZTNA de première génération ont fait le job au moment du basculement en masse vers le télétravail, mais alors que le modèle hybride s'ancre sur la durée, l'heure est venue d'envisager une solution d'accès pour le long terme.

Face à ces nouveaux défis, le ZTNA 2.0 apparaît comme la seule voie à suivre. Les solutions d'ancienne génération étaient peut-être efficaces il y a dix ans, mais le fait est qu'elles n'ont jamais été pensées pour les infrastructures dynamiques et distribuées d'aujourd'hui. Le ZTNA 2.0 a été entièrement conçu pour s'adapter aux environnements cloud-first et multisites qui sont le lot d'une grande majorité d'entreprises aujourd'hui. Pour elles, le ZTNA 2.0 s'impose comme un véritable impératif. Voici les conseils de ZK Research pour migrer sereinement vers une solution ZTNA de deuxième génération :

Repensez la sécurité à l'ère du travail hybride. Le modèle de sécurité traditionnel, qui implique l'achat

de produits spécialisés, a peut-être fait ses preuves par le passé, lorsque la DSI maîtrisait l'environnement informatique de A à Z (applications et appareils autorisés, connexion réseau et même mode d'accès à ce dernier). Or, ce modèle est en inadéquation totale avec les nouveaux modes de travail, alors que les applications migrent vers le cloud, que les appareils sont devenus mobiles et que les salariés privilégient le télétravail. Cette nouvelle donne impose l'adoption d'une solution entièrement unifiée, à l'image de ce que propose Palo Alto Networks à travers sa plateforme Prisma Access.

Commencez par la principale difficulté de sécurité à résoudre. Si le ZTNA 2.0 se veut aujourd'hui incontournable pour les entreprises dans leur globalité, le point de départ variera en fonction des spécificités de chacune d'elles. ZK Research a identifié trois axes de transition vers le ZTNA :

- Sécurisation de l'accès aux applications privées, en lieu et place du VPN
- Sécurisation de l'accès Internet et SaaS, en remplacement de la passerelle web sécurisée (SWG)
- Déploiement d'une stratégie de sécurité des applications SaaS se substituant aux CASB et DLP

Choisissez un partenaire de sécurité cloud-native. On ne compte plus le nombre de solutions revendiquant une sécurité en mode cloud. Or, en tant que client, il faut bien comprendre que tous les clouds ne se valent pas, et qu'il existe souvent une différence notoire entre « cloud » et « cloud-native ». D'où l'importance pour les clients d'effectuer une étude détaillée en amont de façon à porter leur choix sur une véritable plateforme de sécurité cloud-native moderne, synonyme d'innovation et de résilience.

CONTACT

zeus@zkresearch.com

Mobile : +1 301-775-7447

Bureau : +1 978-252-5314