LIVRE BLANC

L'importance du ZTNA pour les nouveaux sites distants

Les cybercriminels ne cessent de perfectionner leurs tactiques d'attaque, avec pour conséquence une prolifération des compromissions de sécurité. Selon un rapport de notre équipe Unit 42, 65 % des attaques sont dues à l'exposition de données utilisateurs par des applications, des services cloud/Internet et du trafic IoT (98 % de ce trafic n'est pas chiffré). Pour cette raison, une politique de sécurité Zero Trust, intégrée en natif à une solution SD-WAN, peut constituer la meilleure ligne de défense pour protéger les utilisateurs, les applications et les appareils IoT.

PRISMA® SD-WAN
BY PALO ALTO NETWORKS

sdxcentral®

Introduction

Aujourd'hui, l'entreprise n'a d'autre choix que de s'inscrire dans un processus continu de transformation numérique pour rester compétitive, répondre aux attentes des clients, développer de nouvelles synergies et proposer des produits de pointe. Mais sur le plan de la sécurité, plusieurs facteurs ont considérablement élargi la surface d'attaque : essor du travail hybride, appareils et utilisateurs toujours plus distribués, prolifération des objets connectés (IoT), etc.

Pour l'entreprise actuelle, le constat est simple. Toutes les ressources sont exposées à un risque, des données aux identifiants, en passant par les machines et les réseaux. Et les sites distants traditionnels n'offrent pas le type d'architecture de sécurité nécessaire pour protéger les salariés, la diversité d'applications distribuées et la hausse fulgurante des appareils IoT.

C'est pourquoi les entreprises doivent prendre des mesures stratégiques ciblées pour sécuriser leurs sites distants, leurs utilisateurs et leurs ressources. Comment ? Au travers d'une approche Zero Trust intégrant directement le principe du moindre privilège au SD-WAN, dans le cadre d'une solution SASE (Secure Access Service Edge).

Explorons plus en détail l'environnement des menaces en constante évolution, les insuffisances des solutions d'ancienne génération et les arguments imparables en faveur d'une approche Zero Trust.

Prolifération des cyberattaques

Chaque jour, voire plusieurs fois par jour, les médias se font l'écho de compromissions de sécurité de grande ampleur. Petites et grandes entreprises, systèmes de santé, institutions financières, établissements d'enseignement, supply chain logicielle… les attaques n'épargnent personne.

Quelques exemples récents :

En septembre 2022, une attaque par ingénierie sociale menée par un jeune hacker touche Uber. L'adolescent a pu accéder aux services de gestion des privilèges d'accès et à plusieurs systèmes de l'entreprise, notamment AWS, Duo, GSuite, Slack, VMware et Windows.

Début janvier, une banque d'adresses e-mail d'environ 200 millions d'abonnés Twitter est proposée sur le dark web au prix imbattable de 2 dollars. Cette révélation fait suite à des signalements selon lesquels des données d'abonnés Twitter ont été régulièrement achetées et vendues sur le dark web tout au long de l'année 2022.

Côté IoT, des hackers se sont introduits en mars 2021 dans une base de données contenant les flux vidéo de caméras de sécurité recueillis par la startup Verkada, Inc. Cette base de données contenait les flux en direct de 150 000 caméras de surveillance à l'intérieur d'hôpitaux, d'entreprises, de commissariats, de centres pénitentiaires et d'établissements scolaires. Tesla et Cloudflare comptent parmi les entreprises exposées.

Le géant de la téléphonie mobile T-Mobile a été touché plusieurs fois au cours des 12 derniers mois. L'opérateur a signalé en avril 2023 sa deuxième compromission de l'année. La nature des informations volées variait en fonction des clients et pouvait inclure : nom complet, coordonnées, numéro de compte et numéros de téléphone associés, code PIN du compte, numéro de sécurité sociale, numéros de pièces d'identité, date de naissance et solde débiteur.

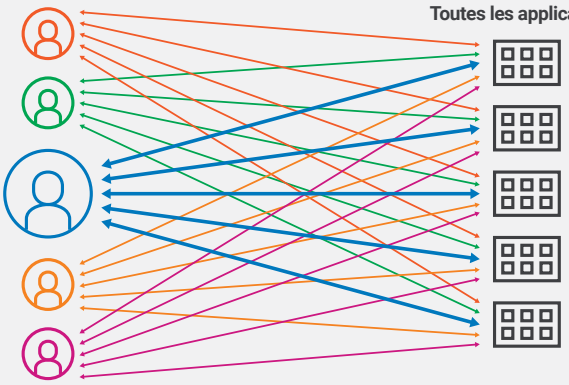
Et ceci n'est qu'un aperçu.

Les cyberattaques et le ransomware sont des phénomènes endémiques : les adversaires cherchent constamment à subtiliser des données d'entreprise, des informations de propriété intellectuelle et des données à caractère personnel, soit pour les exploiter directement, soit comme monnaie d'échange contre rançon. En chiffres, la situation est préoccupante : plus de 80 % des entreprises des États-Unis admettent que leurs systèmes ont été piratés à des fins de vol, de falsification ou de divulgation de données importantes.

D'autres statistiques tout aussi alarmantes :

- Le coût moyen d'une compromission de données s'établit désormais à 4,35 millions de dollars.
- 82 % des compromissions de données impliquent le facteur humain, notamment l'ingénierie sociale, des erreurs et des utilisations incorrectes.
- En 2022, 71 % des entreprises à l'échelle mondiale ont été touchées par les ransomwares et environ 72 % d'entre elles ont payé une rançon.

La situation se tend encore du fait de la hausse exponentielle des objets connectés. Les prévisions tablent sur un quasi-triplement de leur nombre, soit plus de 29 milliards en 2030. Globalement, le cabinet d'études de marché IoT Analytics prévoit qu'environ 27 milliards d'objets connectés seront en service dans les entreprises d'ici 2025. Pour remettre ce chiffre en perspective, les appareils qui se connectent aux réseaux d'entreprise seront plus de quatre fois plus nombreux que les utilisateurs dans quelques années.



Surface d'attaque plus large = multiplication des attaques

92 %

des responsables IT rapportent que leur entreprise a été victime d'une cyberattaque au cours des 12 derniers mois.

(Forrester, 2021)

Un nouvel outil pour chaque nouvelle menace

76

Nombre d'outils de sécurité qu'utilise en moyenne une entreprise (64 il y a deux ans, soit une augmentation de 19 %).

(Panaseer, 2022)

Figure 1. La surface d'attaque s'est considérablement élargie

Les appareils connectés ont incontestablement accompagné et accéléré la transformation numérique. Mais en parallèle, ils ont clairement exposé les entreprises et leurs sites distants à de nouvelles menaces. Le rapport Unit 42 sur les menaces IoT publié par Palo Alto Networks dégage les constats suivants :

- **57 %** des appareils IoT sont très vulnérables
- **98 %** du trafic IoT n'est pas chiffré
- **83 %** des objets connectés fonctionnent sous un OS en fin de support

Pour ne rien arranger, de plus en plus d'applications sont largement distribuées sur les sites distants et les réseaux hybrides, tandis que le tout-cloud se démocratise à vitesse grand V. Au final, l'exploitation des vulnérabilités va se poursuivre, mais à un rythme encore plus soutenu.

Trop d'outils, pas assez de visibilité

La cybersécurité évolue elle aussi à bon rythme avec l'élargissement de la surface d'attaque des entreprises. La transition quasi-immédiate au télétravail pendant la pandémie de Covid-19 n'est pas étrangère à cette accélération, tout comme la probable pérennisation du mode de travail hybride. Des enquêtes récentes indiquent notamment que 74 % des entreprises américaines appliquent un modèle permanent de travail hybride ou prévoient de le faire.

Mais l'élargissement de la surface d'attaque ne concerne pas que les entreprises. La supply chain logicielle, majoritairement composée de code open-source vulnérable, y est également confrontée.

Dans le même temps, les cybercriminels gagnent en sophistication et exploitent tous les points d'entrée possibles. Ils convertissent d'ailleurs leurs outils de ransomware en produits de consommation, sous la dénomination RaaS (Ransomware-as-a-Service). Ainsi, des novices sans compétences en code ou en piratage peuvent acquérir des kits RaaS à des tarifs planchers de 100 dollars.

Pour les entreprises, le problème réside dans la nature généralement rudimentaire de leurs outils de sécurité. Pour sécuriser une grande diversité de sites, d'utilisateurs et d'applications, les entreprises s'efforcent de déployer une série hétéroclite de produits spécialisés (outils de monitoring, mécanismes d'alerte, environnements sandbox, etc.) en se basant sur un inventaire basique de ce dont elles disposent et ce qu'elles peuvent protéger.

D'après Panaseer, société spécialisée en gestion de la posture de sécurité, les grandes entreprises déploient en moyenne 76 outils de sécurité dans leurs environnements. Pourtant, 82 % des responsables de la sécurité ont été pris de cours par un évènement de sécurité, un incident ou une compromission ayant échappé à un contrôle qu'ils pensaient suffisamment efficace.

Cette proportion révèle à quel point les dirigeants d'entreprise manquent souvent de visibilité ou de connaissances sur ce qui se passe sur leur réseau, d'où l'impossibilité de le sécuriser de bout en bout.

La situation se complique encore lorsque ces outils disparates résident dans les data centers d'entreprise. Les données doivent alors transiter du site distant jusqu'au data center, avec des conséquences défavorables sur les performances et l'expérience utilisateur.

Aujourd'hui pourtant, les applications sont partout, tout comme les sites distants. L'acheminement de toutes les données jusqu'au data center n'est donc plus praticable et s'avère même contre-productif, sous l'angle de l'optimisation du trafic. Certes, dans un data center autonome, les équipes de sécurité peuvent installer un ou plusieurs pare-feu. Mais cette méthode se révèle coûteuse et laborieuse si l'entreprise possède plusieurs sites distants dans différents pays ou régions. Elle brouille également la visibilité, car les entreprises peinent à déterminer le parcours des données et doivent composer avec des milliers, voire des millions de points de données pour en déduire des analyses essentielles.

Un réseau distribué devrait, en toute logique, bénéficier d'une sécurité distribuée, avec accessibilité totale et interconnectivité à l'échelle mondiale. Comme les utilisateurs se connectent où qu'ils soient, tous les terminaux doivent intégrer une sécurité de nouvelle génération.

Plus important encore, les entreprises ne peuvent pas simplement déduire des expériences passées qu'elles ont une visibilité sur les utilisateurs, les appareils et les comportements réseau. Car dans l'environnement actuel, il est extrêmement difficile de savoir si un utilisateur est vraiment celui qu'il prétend être, depuis quel terminal il se connecte et à quelles ressources il accède.

Place au Zero Trust et cap sur le Zero Trust 2.0

Les entreprises doivent aujourd'hui vérifier toutes les transactions numériques avant de les approuver. La nouvelle approche du Zero Trust pousse la logique encore plus loin : vérifier pour approuver, puis revérifier pour approuver de nouveau, etc.

L'expression « Zero Trust » a été employée pour la première fois en 2010 par John Kindervag, analyste chez Forrester Research. Elle résume l'hypothèse selon laquelle le risque est un facteur intrinsèque, aussi bien sur le réseau qu'à l'extérieur du réseau.

Les dirigeants d'entreprise connaissent pour la plupart l'expression et son concept. Et la hausse des compromissions et la transition vers le travail hybride font du Zero Trust une solution incontournable, aussi bien pour l'équipe informatique que l'équipe de direction.

Les premières versions du Zero Trust étaient simplistes et rudimentaires : en général, les utilisateurs étaient vérifiés une seule fois, et peut-être de temps à autre par la suite, puis vaquaient librement à leurs activités sur un appareil ou un réseau.

Mais aujourd'hui, les entreprises doivent franchir un nouveau cap au travers d'une vérification constante et continue du niveau de confiance, basée sur le principe du moindre privilège. Chaque demande d'accès doit faire l'objet d'une validation et d'une inspection, suivies de l'application de la politique de sécurité correcte, puis d'une authentification double et triple, et ce, en permanence tout au long de la connexion.

Explorez notre solution Zero Trust Network Access (ZTNA) 2.0 pour en savoir plus.

Imaginez le concept du Zero Trust 2.0 comme un aéroport post-11 septembre : lorsqu'un voyageur pénètre dans l'aéroport, il passe d'abord par un portique de détection de métaux, puis dans la file d'enregistrement/contrôle des bagages, puis par les contrôles de sécurité, avant d'arriver à sa porte d'embarquement et de monter à bord de l'avion. À chacune de ces étapes, il doit présenter les preuves de son identité.

Avec le Zero Trust 1.0, ce même voyageur pourrait se rendre au même aéroport le lendemain et contourner tous ces points de contrôle, car il a déjà été vérifié et autorisé à passer.

Ensemble, une solution ZTNA et une solution SASE (avec SD-WAN intégré à des solutions de sécurité réseau et proposé sous forme de service cloud unifié) peuvent former une ligne de défense extrêmement robuste et compléter plusieurs autres fonctionnalités essentielles :

- Réseau élastique grâce à une architecture basée sur un contrôleur centralisé qui simplifie la connectivité par des mises à jour automatiques de la topologie réseau et automatise les changements de listes d'accès par des opérations sans routage
- Architecture app-to-app directe vers toutes les applications (SaaS, cloud, Internet et privées) pour garantir les performances
- Automatisation des opérations IT complexes grâce à l'intelligence artificielle (IA)/machine learning (ML).

Choisir le bon outil

Il reste néanmoins à intégrer correctement le Zero Trust. Selon Gartner, 60 % des entreprises vont s'approprier le Zero Trust comme solution de base à leur programme de sécurité d'ici à 2025, mais plus de la moitié ne parviendront pas à en exploiter les avantages.

Pour en tirer le maximum, l'outil Zero Trust idéal doit fournir depuis le cloud des services de sécurité intégrés aux sites distants, où qu'ils soient.

La sécurité doit être granulaire, ou de couche 7, qui est considérée comme le niveau de sécurité le plus élevé sur la couche applicative, car les informations sont évaluées d'après l'application en cours d'utilisation. Cette granularité permet d'appliquer véritablement le principe du moindre privilège pour les accès et garantit que seules les personnes habilitées ont accès aux informations et ressources correspondantes, et ce, uniquement au moment et à l'endroit où elles en ont réellement besoin.

Un outil optimal doit également donner de la visibilité sur toutes les ressources, notamment les appareils IoT toujours plus nombreux, pour s'assurer que les contrôles et politiques corrects sont appliqués à l'ensemble du réseau.

De même, l'outil doit inclure des fonctionnalités IA, ML et d'automatisation pour simplifier le processus et fournir des données, analyses et éclairages précieux, exploitables en temps réel et déclinables en politiques et protocoles futurs.

L'avantage Prisma SD-WAN

Prisma SD-WAN de Palo Alto Networks simplifie les opérations en fusionnant les fonctionnalités réseau et sécurité en un service unifié permettant d'activer l'accès Zero Trust d'un seul clic.

Les utilisateurs et leur terminal SD-WAN se connectent automatiquement au nœud Prisma Access disponible le plus proche, après quoi le système détecte et protège les applications automatiquement. Le processus a lieu en continu dans tous les sites distants, avec des centaines ou des dizaines de milliers d'appareils connectés aux nœuds les plus proches.

Le principe du moindre privilège s'applique par une inspection continue de sécurité et une vérification permanente du niveau de confiance des ID des utilisateurs, des applications et des appareils. Cette méthode protège tous les utilisateurs et garantit une sécurisation homogène de l'ensemble des applications utilisées dans l'entreprise (cloud-native, privées sur site, SaaS, etc.). Elle est disponible à l'échelle mondiale : les sites distants appliquent le même principe d'approbation et de sécurité, quels que soient leur situation géographique et le lieu ou le mode de connexion de leurs utilisateurs.

Prisma SD-WAN offre une visibilité sur la couche 7, une sécurité hautement distribuée, ainsi qu'une vérification continue du niveau de confiance et une inspection constante du trafic. Sécurité, performance et visibilité sont étendues à tous les appareils, y compris l'IoT, qu'importe leur fabricant ou leur système d'exploitation. De plus, les fonctionnalités IA/ML automatisent les processus et les politiques, surveillent le réseau en continu, détectent les tentatives d'intrusion ou les compromissions réelles et recommandent de bonnes pratiques.

Avantages métiers d'un SD-WAN/SASE intégré

Prisma SD-WAN offre aux entreprises trois bénéfices distincts :

- Sécurité « best-of-breed » pour les utilisateurs, les applications et les appareils IoT
- Outil de gestion centralisé qui simplifie les opérations au quotidien
- Expérience utilisateur améliorée : le système connecte toujours les utilisateurs au nœud le plus proche, qu'ils se trouvent à Paris ou à Sydney

Pour produire ces bénéfices, plusieurs éléments interviennent :

- Contrôle des accès au niveau sous-applicatif. Prisma SD-WAN peut identifier, prioriser et réguler (ingénierie du trafic) de nombreuses applications SaaS et cloud critiques à l'entreprise.
- Accès actif/actif aux applications. La plateforme établit des tunnels overlay propriétaires entièrement automatiques jusqu'à Prisma Access, permettant ainsi de l'utiliser dans les connexions actives-actives et actives-veille.
- Intégration simplifiée à l'architecture CloudBlade basée sur des API sans perturbation de service. Cette configuration assure une connectivité automatique à pleine échelle au réseau mondial de Prisma Access.
- Rotation des clés de sécurité. La rotation et le renouvellement réguliers des tunnels overlay chiffrés depuis le contrôleur cloud renforcent la sécurité du trafic applicatif des sites distants vers le cloud.
- Gestion unifiée. Prisma SASE et Prisma Access sont accessibles sur une même console unifiée et gérés sur la même interface. Cette centralisation offre une visibilité sur le champ des menaces, les alertes de sécurité et les évènements réseau critiques.
- Data lake unifié regroupant l'ensemble des données/métriques, en particulier du réseau, de la sécurité et de l'expérience. La plateforme peut ainsi directement corréler les données, croiser les identifiants d'utilisateurs et d'applications, et recueillir des informations de sécurité.

Prisma SD-WAN réunit tout le nécessaire sous un seul et même service. Les opérations sont simplifiées sur un réseau sécurisé et hautement visible. Le déploiement en un clic protège les utilisateurs, les applications, le réseau et les appareils IoT. Les fonctionnalités IA/ML et d'automatisation analysent en permanence toute activité suspecte et révèlent des éclairages essentiels.

Les sites distants évoluent. Votre SD-WAN doit s'adapter.

L'entreprise d'aujourd'hui et de demain doit être intégrée, connectée, visible et « digital-first ».

Mais avant tout, elle doit être protégée.

Face à l'évolution permanente du champ des menaces, les entreprises n'ont pas d'autre choix que d'appliquer en continu l'approche Zero Trust pour les utilisateurs, les applications et les objets connectés. Cette solution est particulièrement efficace lorsqu'elle est associée au SD-WAN et au SASE dans une solution intégrée de bout en bout.

Découvrez comment Prisma SD-WAN peut sécuriser dès aujourd'hui vos sites distants de demain.

PRISMA® SD-WAN
BY PALO ALTO NETWORKS

À propos de Prisma SD-WAN

Prisma SASE de Palo Alto Networks incarne le site distant du futur, hybride, numérisé et sécurisé avec un SD-WAN de nouvelle génération. Contrairement à la solution SD-WAN de première génération, cette approche offre une connectivité flexible et résiliente, respectueuse des SLA relatifs à n'importe quelle application et liaison WAN. De plus, elle applique une sécurité Zero Trust pour les utilisateurs, les applications et les appareils IoT, tout en automatisant les opérations post-déploiement avec l'AIOps. Ainsi, les entreprises peuvent fournir en toute transparence une expérience utilisateur d'exception, sécuriser leur réseau (y compris l'IoT) de manière holistique et simplifier les opérations IT complexes.

www.paloaltonetworks.fr/sase/sd-wan

sdxcentral®

À propos de SDxCentral

SDxCentral est un acteur B2B des médias et du MarTech. Côté médias, nous capitalisons sur notre expertise pour donner aux professionnels IT les moyens de mieux conseiller leur entreprise et de faire progresser leur carrière. Nos contenus instruisent et renseignent les professionnels du cloud, des réseaux et de la sécurité qui occupent des postes opérationnels, de développement et de direction dans de grandes entreprises, y compris des fournisseurs de services majeurs. Côté MarTech, nous nous basons sur l'engagement des acheteurs pour cerner et prédire leurs intentions, et nous connectons nos clients avec les professionnels IT intéressés. Associées à notre contenu personnalisé étayé par des données, nos solutions de technologies marketing permettent aux spécialistes du marketing d'entreprise ou des ventes d'orienter les acheteurs de produits et solutions IT pour les convertir en clients.

www.sdxcentral.com