Zero Trust : Never Trust, Always Verify

L'identité comme nouveau périmètre de sécurité ?

Par Greg Young, VP Cybersecurity, Trend Micro et
William Malik, VP Infrastructure Strategies, Trend Micro

SOMMAIRE

1. AVANT-PROPOS : HISTORIQUE DU ZERO TRUST

UNE IDÉE QUI FAIT SON CHEMIN DEPUIS 10 ANS

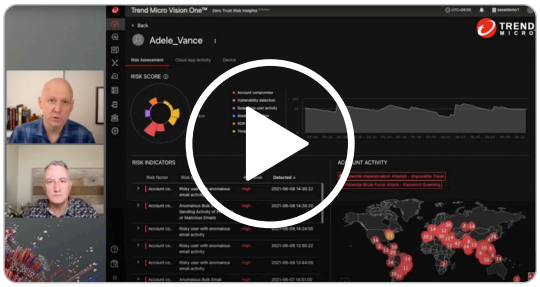
Le Zero Trust (ZT) peut s'apparenter à une nouveauté. Cependant, son approche stratégique et nombre de facteurs de son évolution existent déjà depuis le début des années 2010. L'informatique d'entreprise s'est transformée au cours de la décennie écoulée, mais les fondamentaux de la sécurité sont restés les mêmes. Le cloud, la transformation digitale, le télétravail et les services SaaS font partie de ces tendances qui revisitent la façon dont les entreprises voient la technologie. La sécurité, en revanche, n'a pas forcément su accompagner ces tendances pour les protéger. Elle reste donc trop souvent classique face à des entreprises qui, elles, ont su innover.

UNE TENTATIVE POUR FAIRE ÉVOLUER LA SÉCURITÉ TRADITIONNELLE

Les réseaux classiques sont très ouverts. Si vous êtes sur un VPN ou dans un bureau, vous pouvez accéder au réseau d'entreprise après authentification grâce à un identifiant et un mot de passe. La sécurité a tenté d'adapter cette approche en dissociant le réseau en zones plus restreintes. Cette réduction d'échelle reste, au final, basée sur les mêmes fondamentaux de sécurité. En revanche, elle alimente de nouveaux défis en matière de gestion et de visibilité, ce qui, paradoxalement, crée de nouvelles opportunités pour les assaillants. L'IoT (Internet des objets) a introduit des dispositifs semi-intelligents, considérés comme étant de confiance, tandis que la pratique du Shadow IT a restreint la visibilité des entreprises sur les modalités d'utilisation des données et des applications.

IDENTITÉ

Les fondamentaux en matière d'identité et de paire identifiant/mot de passe n'ont pas changé. Faire évoluer la sécurité traditionnelle n'a pas apporté une réponse satisfaisante, compte tenu de la multiplicité des identités et de règles complexes pour les mots de passe. Ces nombreuses identités et les réinitialisations régulières des mots de passe n'ont pas porté leurs fruits. En piratant les identifiants d'un utilisateur, un assaillant peut se mouvoir en interne sur le réseau pour tenter de propager un ransomware, s'octroyer des privilèges supplémentaires, exfiltrer des données ou espionner. C'est à cette problématique que répond l'authentification multi-factorielle (MFA), un net progrès en matière de processus d'authentification. Pour autant, la notion de « multi » se résume à rajouter un canal d'authentification. La confiance est binaire. Vous êtes considéré comme étant de confiance si vous êtes authentifié... Et rien de plus. Ainsi, la confiance est basée essentiellement sur l'authentification, et éventuellement sur quelques leviers de maîtrise des risques comme la géolocalisation. Et cette confiance reste d'actualité jusqu'à la déconnexion.



LES PERSPECTIVES DE TREND MICRO SUR LE ZERO TRUST

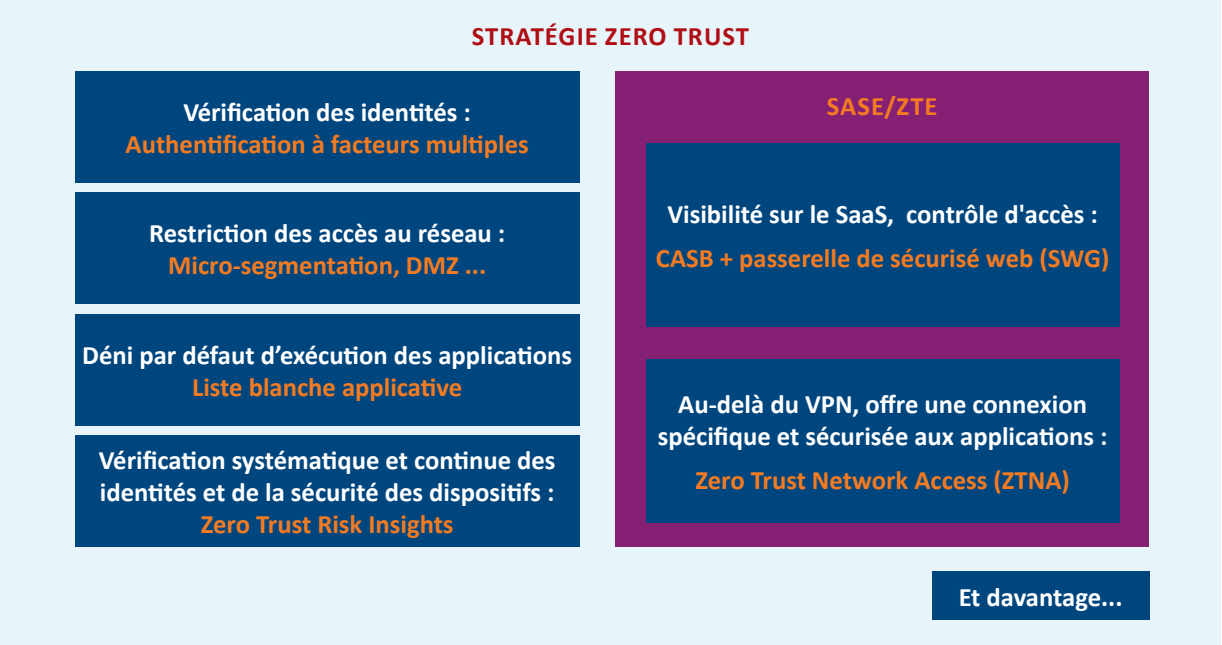
2. ZERO TRUST : DÉFINITION

Le ZT est à la fois une architecture et un objectif basés sur l'idée que chaque transaction ou entité n'est considérée comme étant de confiance que si cette dernière est effectivement validée et pérenne. L'attitude Zero Trust doit être tenue en dépit des évolutions de l'infrastructure et des activités métiers.

Dans ce contexte, les projets ZT s'articulent autour de piliers essentiels, parmi lesquels :

- La vérification des identités
- La restriction des accès au réseau
- Le déni d'exécution, par défaut, d'une application
- Une visibilité qui permet un processus permanent d'évaluation

DIFFÉRENTES VOIES POSSIBLES VERS LE ZERO TRUST...



Si chaque pilier est lié à une tâche de sécurité (MFA pour la gestion des identités, micro-segmentation pour la restriction des accès réseau, etc.), la visibilité nécessaire à une évaluation permanente reste le pilier le plus important. Sans visibilité, le niveau général du ZT engendre de la complexité, ce qui remet en cause les efforts entrepris.

Trois principes sont essentiels pour le ZT :

1. *Posture* 2. *Évaluation continue* 3. *Présomption d'une compromission*

La ***posture***, l'équivalent du bilan de santé chez un individu, est d'ordre qualitatif. Elle se veut précise et se réfère à la qualité de tous les dispositifs/utilisateurs et des identités. Le ZT pour une identité implique une authentification et l'évaluation de la posture de sécurité de cette identité. Avant le ZT, l'évaluation de la sécurité des identités était peu fréquente ou binaire. Avec cette notion de posture, il s'agit désormais d'évaluer les identités, les dispositifs, les applications et l'usage des données pour pointer les risques potentiels et réels. Ceci est basé sur le niveau de risque des menaces potentielles et sur les menaces réellement détectées et prises en charge. Sur un endpoint, une vulnérabilité non patchée constitue un risque potentiel, tandis que la détection d'une infection qui se propage en interne est un risque réel. Pour une identité, une erreur d'attribution de privilèges d'administration est un risque potentiel. Et un risque réel résulte d'un comportement d'authentification suspect ou de la détection d'emails de phishing provenant de cette identité.

Une ***évaluation continue***, contrairement à une évaluation périodique ou planifiée, couvre toutes les transactions. Un contrôle NAC d'accès au réseau s'impose, même s'il présente des limites. Le ZT tire parti des concepts du NAC, de son périmètre d'application et de son côté continu. Mais le NAC n'est pas équivalent au ZT. En effet, avec le NAC, la confiance est accordée après une vérification sur un nombre limité de critères. En revanche, une architecture ZT traite toutes les tentatives d'accès. Toutes les transactions sont vérifiées et toutes les entités disposent d'une posture de confiance.

La ***présomption d'une compromission*** reflète le principe que la confiance n'est accordée qu'après vérification. Les équipes de sécurité opèrent déjà selon ce principe : avant toute investigation, l'hypothèse est que tout se passe bien au sein de l'architecture tant qu'aucune alerte n'est émise. Avec le ZT, la confiance n'est pas accordée sans un feu vert inconditionnel : on ne se base donc plus sur les alertes. La présomption de compromission s'applique à toutes les entités, et notamment les identités et identifiants de connexion.

Ces trois principes remettent en cause ceux de la sécurité traditionnelle : ces principes sont intégrés à l'architecture ZT, tandis que les décisions de neutralisation des menaces et de prévention sont prises selon le niveau de risque. Les menaces sont jugulées avant de donner lieu à des attaques, et avant que les équipes de sécurité ne mènent leurs investigations. Ces équipes peuvent ainsi enquêter sur les incidents les plus graves et permettre aux équipes opérationnelles de traiter les risques associés aux menaces neutralisées.

3. CE QUE LE ZERO TRUST N'EST PAS

Le ZT n'est ni une norme, ni une certification. Il existe bien un document du NIST sur le ZT, une « Special Publication » (SP) et non un « Federal Information Processing Standard » (FIPS). Le document NIST SP 800-207 décrit des objectifs d'architecture, mais il n'existe aucune certification de conformité au NIST SP 800-207.

Le ZT n'est pas un produit. Si des produits peuvent s'associer pour définir une architecture ZT, il n'est néanmoins pas possible d'acheter un produit d'architecture ZT. Le déploiement d'un outil de micro-segmentation peut constituer une stratégie efficace, mais seulement s'il est réalisé selon les objectifs et principes de l'architecture ZT.

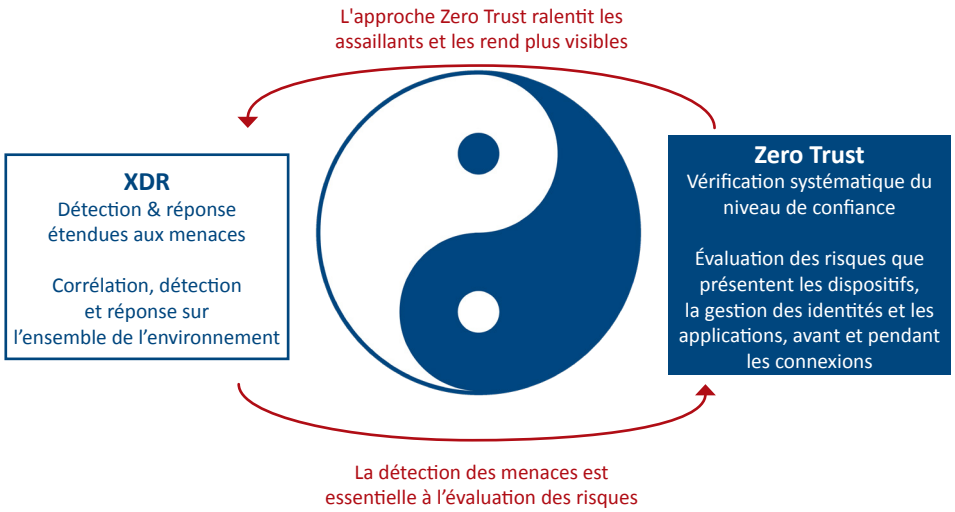
Certains éditeurs n'hésitent pas à accorder à leurs produits existants le label ZT, sans pour autant les avoir fait évoluer. Cette fioriture marketing vise à capitaliser sur la confusion potentielle autour du ZT pour tenter de positionner des produits en tant que solution tout-en-un. Les produits hérités peuvent faire partie d'une architecture ZT, mais ils doivent être déployés de manière spécifique, pour atteindre un objectif ZT. Une architecture ZT doit être déployée progressivement et être opérationnelle en permanence. La mise en œuvre complète du ZT peut courir sur plusieurs années et faire l'objet de différents projets autour de chaque pilier du ZT.

4. XDR ET ZERO TRUST

XDR (eXtended Detection and Response) constitue une nouvelle approche de sécurité qui se concentre sur les menaces. En tant qu'extension de l'EDR (Endpoint Detection and Response), XDR recueille des volumes importants d'indicateurs à partir de différentes sources de sécurité de données d'une organisation. Cette solution recherche des preuves sur l'ensemble du périmètre d'une entreprise pour identifier et traiter davantage de menaces. XDR, en tant que technologie pertinente pour neutraliser les menaces, est généralement déployé pour sécuriser une infrastructure existante et non pour la transformer immédiatement. Les équipes de sécurité utilisent la télémétrie XDR pour identifier les faiblesses d'une architecture qui donneront lieu à des changements tactiques au sein d'architectures sans ZT. Les entreprises ayant déployé XDR sont les plus susceptibles d'adopter une stratégie ZT.

XDR présente deux atouts essentiels pour concrétiser une architecture ZT : des fonctions robustes pour contrôler les endpoints et des indicateurs provenant de l'ensemble du périmètre IT d'une entreprise. Un endpoint doté d'une sécurité forte facilite le processus d'attribution du niveau de confiance. En effet, les équipes de sécurité peuvent déterminer si un endpoint est dépourvu de tout malware, connaître les transactions auquel il participe , obtenir des informations de valeur sur sa posture et s'assurer qu'un agent unique est déployé avec des fonctions ZT comme le ZTNA (Zero Trust Network Access). Les indicateurs issus du data lake XDR sont sources de visibilité, ce qui est essentiel pour le ZT. Ces indicateurs révèlent la posture des éléments autres que les endpoints, notamment au sein d'environnements cloisonnés présentant des failles susceptibles d'être exploitées par les assaillants. Les décisions ZT peuvent aboutir à des détections XDR lorsque l'accès est accordé à des ressources, tandis que ces données recueillies constituent une première source pour mener l'évaluation permanente.

Si le ZT tire parti de XDR pour améliorer l'infrastructure, c'est également XDR qui gagne en efficacité grâce au ZT. Une architecture robuste de sécurité empêche les assaillants de se mouvoir en interne, d'accéder à des ressources. Ces assaillants vont ainsi créer davantage de bruit, ce qui facilite leur détection. Le ZT restaure nombre de carences à l'origine d'incidents et ces derniers sont ainsi détectés et neutralisés par XDR. En supprimant de nombreuses vulnérabilités grâce à une architecture bénéficiant du ZT, XDR et les équipes de sécurité peuvent se focaliser sur les attaques les plus sophistiquées ou sur des domaines qui ne sont pas encore passés au ZT.



5. MIGRATION VERS LE ZERO TRUST

GESTION DES IDENTITÉS ET DES ACCÈS (IAM)

L'IAM (Identity and Access Management) régit l'identification des utilisateurs. Les utilisateurs préfèrent ne pas avoir à s'authentifier de manière répétée et privilégient le single sign-on. Les administrateurs souhaitent gérer tous les droits d'accès et requêtes d'un utilisateur et préfèrent une gestion consolidée des utilisateurs. Ces deux objectifs, ensemble, constituent le socle technique de l'IAM. Un projet IAM est, en lui-même, un projet d'envergure.

Les utilisateurs, ainsi que les dispositifs et services clés, doivent s'authentifier pour avoir accès aux ressources d'entreprise. Dans cette perspective, il s'agit d'identifier les utilisateurs qui accèdent à des ressources spécifiques et d'assurer leur provisioning via le service IAM, avec autant d'informations sur leur profil d'utilisateur que nécessaire. Les ressources sensibles doivent utiliser le MFA, ce processus étant de loin supérieur à l'utilisation d'un mot de passe statique.

GESTION DES ACCÈS PRIVILÉGIÉS (PAM)

Pour les ressources les plus sensibles, les outils PAM (privileged access management), à l'instar de ceux de CyberArk, BeyondTrust ou Thycotic présentent un réel intérêt. L'activité des comptes privilégiés est ainsi mise en log, ce qui renforce l'authentification et permet des investigations post-incident plus détaillées.

MOTS DE PASSE

Le National Institute of Standards and Technology a récemment revu ses recommandations en matière de gestion des mots de passe. Cet organisme, après analyse mathématique de la robustesse des mots de passe, a identifié qu'un mot de passe plus long est préférable à un mot de passe associant des caractères spéciaux, des chiffres et des lettres majuscules/minuscules. Plus un mot de passe est long, plus il est robuste. Pour les utilisateurs, un mot de passe long constitué de mots connus est plus simple à retenir qu'une chaîne de caractères complexe et dépourvue de sens. Si le changement fréquent de mot de passe est souvent recommandé, notons que cette pratique présente une valeur limitée en matière de cybersécurité. Lorsqu'un mot de passe est piraté, il est souvent utilisé en l'espace de quelques heures. Ainsi, changer son mot de passe tous les 90 jours ne présente qu'un intérêt modéré pour la gestion des risques. Le MFA est à privilégier à une authentification par simple mot de passe.

ÉVALUATION PERMANENTE DU NIVEAU DE SÉCURITÉ

L'intégrité d'un environnement IT dans la durée est un pilier de la sécurité des informations. Dans le cadre de cette mission, l'entreprise surveille des éléments clés, à la recherche d'incidents potentiels et d'indicateurs de compromission (IoC).

6. ZERO TRUST ET RÉSEAUX

MICRO-SEGMENTATION

Les réseaux à plat présentent le risque majeur de malware qui peuvent s'y mouvoir facilement. C'est la segmentation qui permet de rendre le réseau prêt à accueillir le ZT. L'objectif est de savoir arbitrer entre le degré d'isolement des sous-réseaux segmentés et la complexité à gérer les profils de chacun d'entre eux. Il est important de comprendre où se situent les données nécessaires aux processus critiques pour déterminer les zones, les délimiter et maîtriser le trafic indésirable.

CONFINEMENT DES TECHNOLOGIES VULNÉRABLES

Il est recommandé d'isoler toutes les technologies impactées par une vulnérabilité précise, à l'image des dispositifs IT disposant d'un même OS ne pouvant être patché. En effet, les constructeurs de certains dispositifs industriels (robots industriels, équipements médicaux, etc.) utilisent généralement une version d'OS précise. La modification de cet OS via une mise à jour ou à niveau est susceptible d'annuler la garantie et la certification du dispositif. Ces derniers doivent bénéficier de règles sévères pour maîtriser le risque d'intrusion.

Il est aussi préconisé de limiter les accès distants et physiques aux zones sensibles. Il s'agit notamment de définir une DMZ pour filtrer les accès distants des constructeurs de dispositifs ou des produits SaaS.

OUTILLER LES SEGMENTS DU RÉSEAU

Les sous-réseaux doivent bénéficier d'outils de sécurité pour détecter et neutraliser les malware et leurs dommages : cryptomining, chiffrement indésirable, exfiltration de données, programmes prohibés et outils malveillants de DDoS ou de spam email. Les alertes et les logs sont corrélés à des fins d'analyse et d'action, via une console consolidée.

Ensemble, ces mesures définissent et sécurisent votre topologie réseau.

ZERO TRUST NETWORK ACCESS (ZTNA)

Au fur et à mesure que les architectures ZT se généralisent, il est possible d'identifier des éléments récurrents que les entreprises déploient. Notamment un degré moindre de confiance dans les communications au niveau de l'edge, pour les connexions VPN entrantes et les requêtes sortantes vers des logiciels SaaS, instances cloud et serveurs web. Secure Access Service Edge (SASE) ou Zero Trust Edge (ZTE) sont deux labels qui s'appliquent à cette famille de services, disponibles sur l'edge et pour lesquels la mobilité des collaborateurs est un vrai défi.

Avant le ZT, nous faisions appel aux VPN, au CASB (cloud access security broker) et à une passerelle de sécurité web (SWG). Mais les VPN étaient contraints par leur terminaison au niveau du edge. Les connexions étaient de confiance, mais pas capables d'associer la sécurité et les réseaux SDN. Les SWG n'étaient pas toujours disponibles pour les collaborateurs distants tandis que le CASB était relativement statique. Les réseaux ont progressivement migré vers le software-defined, les entités sont devenues mobiles et la sécurité s'est gravée dans le marbre. Les endpoints non gérés, les services SaaS non contrôlés, les SD-WAN et l'accompagnement des télétravailleurs durant la crise du COVID-19 sont autant de facteurs qui ont pesé sur les architectures de sécurité pré-ZT et ont alimenté le besoin pour le SASE. Le SASE fait parti du ZT et emploie ses principes pour des segments spécifiques de l'entreprise. Le troisième niveau de cette solution est le ZTNA, qui est intégré dans le SASE et qui constitue la base sur laquelle s'adossent tous les autres services de sécurité SASE. Un ZTNA est un VPN intelligent qui reprend les principes du ZT. Si les connexions ZTNA intègrent la posture, l'évaluation permanente et la présomption d'une compromission, elles doivent néanmoins lier l'entité requérante à l'entité cible et être notifiées de tout changement résultant de leur nature software-defined, au niveau des entités et du routage. Prenons l'exemple d'un collaborateur distant se connectant à un serveur. Sa requête de connexion à une application SaaS via ZTNA permet de réduire la surface d'attaque.

Plus d'informations sur le ZTNA et le SASE ici :

https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-

https://en.wikipedia.org/wiki/Secure_Access_Service_Edge

À noter que ces définitions évoluent.

DÉPLOIEMENT D'UN RÉSEAU ZERO TRUST

Les VPN traditionnels constituent une solution certes simple, mais qui ne résout en rien le problème central. Un VPN crée un chemin chiffré à partir du dispositif de l'utilisateur vers le pare-feu situé sur l'edge du réseau corporate. L'ensemble du trafic utilisant ce chemin est chiffré (ceci ne s'applique qu'aux VPN d'entreprise. Les VPN de tiers chiffrent le trafic entre le dispositif de l'utilisateur et le pare-feu du tiers. À sa sortie, le trafic acheminé vers sa destination finale n'est plus chiffré). Avec cette approche, tout utilisateur, une fois connecté, accède à toutes les ressources en aval du pare-feu. Le VPN existe pour créer un périmètre.

Si la machine de l'utilisateur héberge un malware, celui-ci peut, lui aussi, accéder à toutes les ressources en aval du pare-feu. Ceci illustre les carences d'une sécurité basée sur un périmètre.

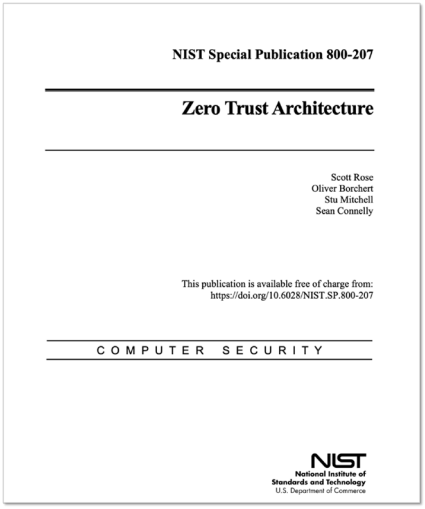
Le ZTNA peut se substituer au VPN conventionnel pour établir un environnement ZT, identifier les ressources de protection qu'offre le pare-feu et envisager des solutions pour gagner en précision. À titre d'exemple, plutôt que de centraliser tous les emails sur un serveur situé en aval du pare-feu, vous pouvez sécuriser chaque compte utilisateur avec une authentification à facteurs multiples et n'accorder l'accès au serveur email qu'aux utilisateurs authentifiés.

7. LES FRAMEWORKS ZERO TRUST

Plusieurs approches permettent de comprendre ou de décrire le ZT. Cependant, il n'existe aucune certification ou norme. Ceci peut être frustrant, puisque de nombreux domaines de la sécurité bénéficient de normes ISO et de frameworks de conformité. À cette frustration, s'ajoute une certaine confusion, lorsque certains produits affirment être certifiés « Zero Trust » ou se prétendent « conformes NIST (National Institute of Standards and Technology) ». Cependant, il existe des approches pertinentes pour comprendre et planifier votre stratégie ZT.

NIST SP-800-207

La publication spéciale du NIST intitulée « Zero Trust Architecture » souligne l'importance des stratégies ZT et illustre comment certains programmes du gouvernement fédéral américain s'adaptent pour employer le ZT, ainsi que pour définir les technologies qui peuvent être utiles. Contrairement au FIPS (Federal Information Processing Standards), cette publication ne constitue pas une norme. Elle vise à offrir des recommandations à l'intention des instances fédérales américaines.


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

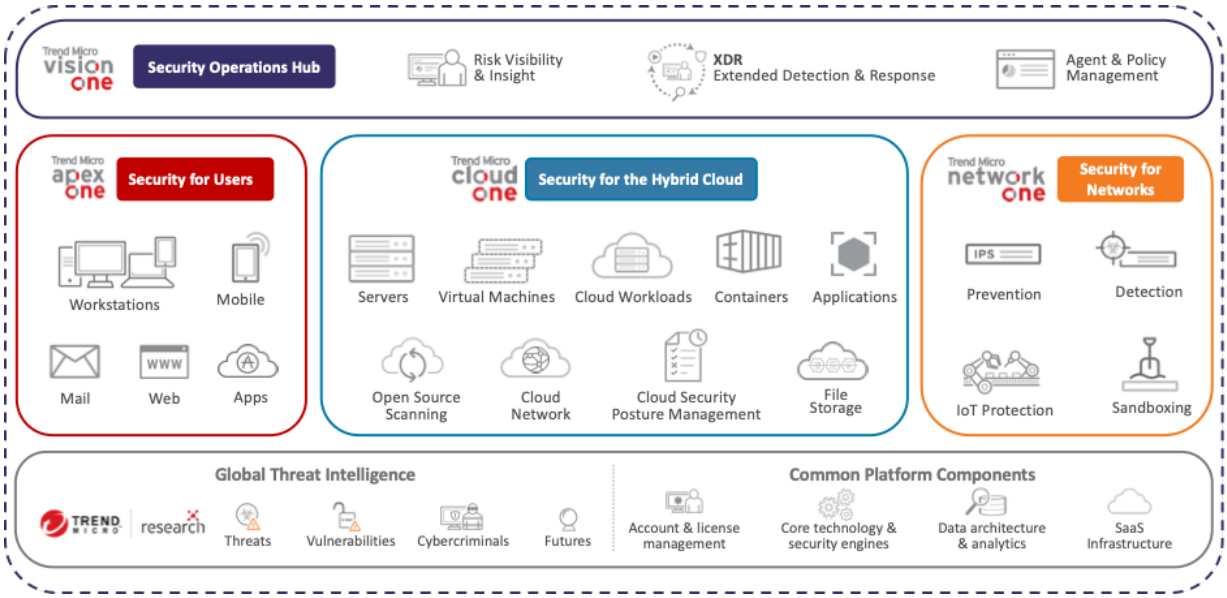
COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

L'OPINION DES ANALYSTES

Les préconisations et explications des analystes constituent une réelle aide pour comprendre les principes du ZT. Forrester, Gartner, IDC, ESG et autres firmes d'analystes ont fait converger leurs définitions et frameworks du ZT. Il n'y a pas de différence radicale entre leurs approches, mais force est de constater quelques divergences en matière de terminologie, notamment sur le périmètre du Zero Trust et des sous-domaines associés.

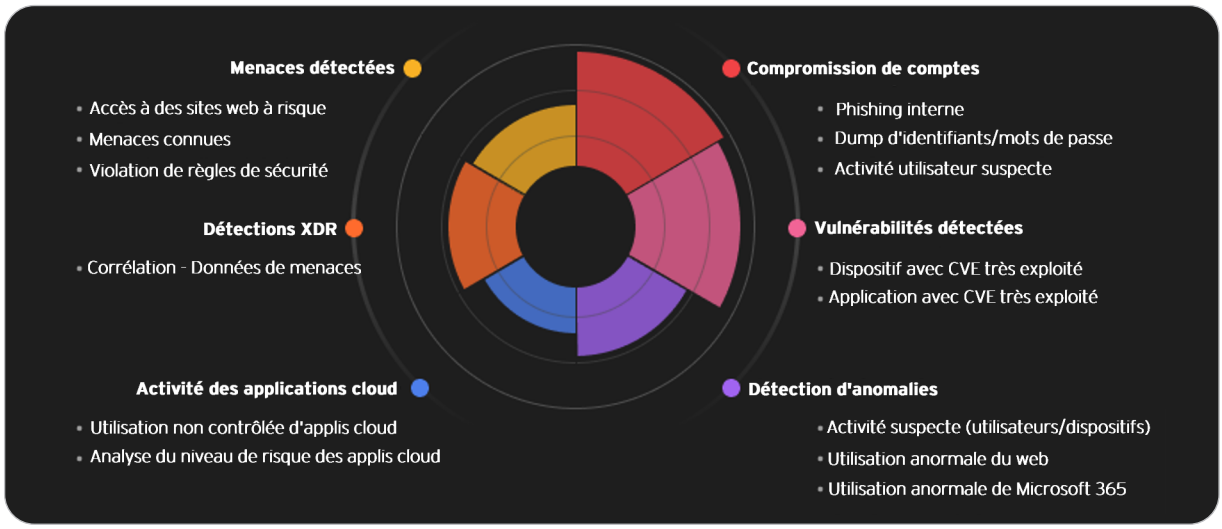
Gartner, Forrester, ESG, IDC et la majorité des autres analystes utilisent le terme Zero Trust. Pour qualifier l'association du CASB, d'une passerelle de sécurité web et d'un VPN compatible Zero Trust, Gartner utilise le terme de SASE (Secure Access Service Edge) tandis que Forrester y fait référence sous le label de ZTE (Zero Trust Edge). Tous les analystes s'accordent à penser que le ZT est compatible à un environnement SD-WAN. Cependant, il existe des divergences sur le fait que le SD-WAN et le réseau en lui-même font partie de la solution de sécurité ou pas. Il est probable que les analystes s'accorderont sur l'idée que le réseau est la cible. Une définition plus précise devrait émerger, qui reconnaît le rôle du SASE/ZTE pour sécuriser le SD-WAN et les sites distants. Pour autant, les équipements et applications réseau n'ont pas à être fournis par le fournisseur de sécurité. Au final, les analystes proposent des perspectives intéressantes, mais ils ne recommanderont pas une architecture de référence précise, ni de norme détaillée. Chaque projet ZT et SASE/ZTE est ainsi personnalisé aux besoins de l'entreprise utilisatrice.



8. ADOPTION DU ZERO TRUST : TREND MICRO VOUS ACCOMPAGNE

ÉVALUATION PERMANENTE DE LA SÉCURITÉ ET DE LA POSTURE

Dans le cadre d'une stratégie ZT, il est essentiel d'évaluer en permanence les risques liés aux identités, dispositifs, applications et données. Ceci est possible grâce à des indicateurs provenant d'endpoints, de l'email, de services d'annuaire, de XDR et d'autres sources. Au sein de Trend Micro Vision One™, l'application Zero Trust Risk Insights évalue le niveau de maîtrise des risques, prioritise les problématiques et suit la posture globale de l'entreprise dans la durée. Cette évaluation des risques en temps réel permet d'alimenter, via des API, une prise de décision automatisée sur les autres composantes de l'architecture ZT, parmi lesquelles le ZTNA, le SASE, la micro-segmentation et l'identité.



Facteurs utilisés par Zero Trust Risk Insights pour évaluer en continu les risques des utilisateurs/dispositifs

EXTENDED DETECTION AND RESPONSE (XDR)

Les fonctions XDR de Trend Micro Vision One recueillent la télémétrie à partir des endpoints, de l'email, des réseaux et du cloud, pour détecter et répondre plus rapidement aux attaques. Elles utilisent des modèles de détection multi-couche pour agréger des indices liés à l'activité des assaillants, apportant ainsi aux entreprises une visibilité sur les actions de remédiation possibles. Le service managé de détection et de réponse aux incidents (Trend Micro™ Managed XDR) propose une identification et une investigation expertes des menaces.

SÉCURITÉ ROBUSTE DES ENDPOINTS ET DES INSTANCES DANS LE CLOUD HYBRIDE

La sécurité robuste des endpoints est la clé de voûte de la protection des dispositifs et des instances dans le cloud hybride. Cette sécurité doit être basée sur différentes fonctions : contrôle applicatif pour ne permettre que l'utilisation d'applications de confiance, protection contre les malware inconnus, prévention d'intrusion, etc. Un seul agent de protection endpoint peut être utilisé pour la protection, EDR/XDR et pour fournir la télémétrie et les informations de risque à Zero Trust Risk Insights. Dans le futur, l'agent assurera également les fonctions de ZTNA et de SASE.

SÉCURITÉ RÉSEAU POUR LES ENVIRONNEMENTS SUR SITE, IOT ET CLOUD

La sécurité réseau aide à segmenter et protéger les réseaux. Des produits optimisés sécurisent les environnements sur site, IoT et cloud. En capitalisant sur les recherches sur les vulnérabilités qu'offre Trend Micro™ Zero Day Initiative™ (ZDI), les solutions de cybersécurité peuvent juguler les vulnérabilités non divulguées bien avant la disponibilité officielle d'un patch.

SÉCURITÉ DU CLOUD

De nombreuses fonctions de sécurité cloud permettent de mettre en œuvre le ZT. Au-delà de la sécurité des réseaux cloud et de la protection des instances réseau et instances cloud, la sécurité des conteneurs, du stockage de fichiers dans le cloud et des vulnérabilités open-source est également proposée, ainsi que la gestion de la posture de sécurité du cloud.

SOLUTIONS SASE FUTURES

Trend Micro™ Zero Trust Secure Access assure la sécurité des connexions entre les utilisateurs et les applications privées/publiques. Des fonctions CASB et ZTNA neutralisent automatiquement les connexions sur la base du Machine Learning, de règles personnalisées et des scores de risque fournis par Zero Trust Risk Insights.

9. CONCLUSION

Sur la décennie écoulée, la cybersécurité s'est focalisée sur la protection d'architectures vulnérables et complexes. Le secteur a innové pour mieux identifier et neutraliser les assaillants. Mais tout comme des pompiers qui luttent pour éteindre un incendie dans un immeuble dépourvu de systèmes retardant la propagation du feu, la conception de la sécurité de nos infrastructures IT doit évoluer si nous souhaitons prendre l'avantage sur l'adversaire. Le ZT propose une sécurité pertinente et la maîtrise des risques, pour ainsi doper l'efficacité des investissements et activités de sécurité.

TREND MICRO™

Securing Your Connected World

Trend Micro Incorporated, un leader mondial des solutions de cybersécurité, a pour mission de sécuriser les échanges d'informations numériques. Fort de décennies d'expérience en sécurité, de travaux de recherche sur les menaces à l'échelle mondiale et d'une innovation permanente, notre plateforme de cybersécurité protège des centaines de milliers d'entreprises et des millions d'individus contre les risques associés au cloud, aux réseaux, aux équipements et aux endpoints. Avec plus de 7 000 collaborateurs présents sur 65 pays et une activité de veille et de recherche parmi les plus sophistiquées au monde, Trend Micro permet aux entreprises de sécuriser leur univers connecté. www.trendmicro.com.

TREND MICRO FRANCE
85 Av. Albert 1er,
92500 Rueil-Malmaison
Téléphone : 01 76 68 65 00