Zero Trust pour l'IoT : la bonne approche

Sommaire

Introduction

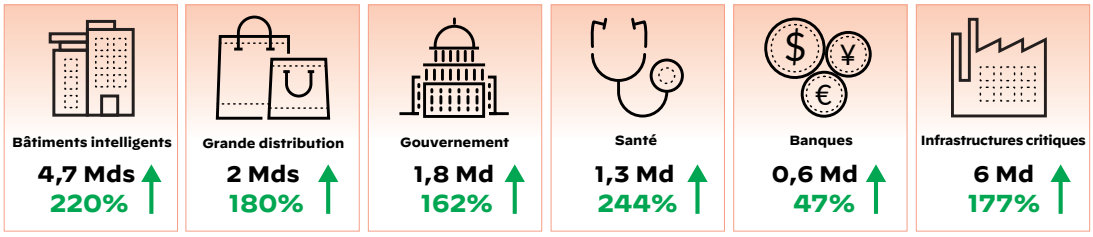
Les équipes réseau et sécurité s'appuient depuis toujours sur la protection périmétrique du réseau pour sécuriser l'ensemble de l'entreprise, le réseau interne étant traditionnellement jugé fiable et sécurisé. Jusqu'à présent, le périmètre réseau marquait la limite entre l'extérieur (« pollué ») et l'intérieur (« propre »), et aucune restriction n'était imposée au flux de trafic applicatif. Mais l'arrivée de nouveaux modèles d'organisation du travail bouscule la gestion traditionnelle du périmètre réseau de la sécurité.

Ainsi, trois tendances poussent les entreprises à revoir leur copie.

- **La transformation numérique :** l'engouement pour les appareils IoT génère un gain de valeur et de productivité pour les entreprises tout en réduisant les coûts.
- **La migration vers le cloud :** un nombre croissant d'appareils, gérés ou non, envoient de plus en plus de données en mode cloud ou multicloud.
- **Le travail hybride :** les collaborateurs sont libres d'utiliser le réseau de campus ou non, ce qui expose le réseau d'entreprise aux menaces externes.

Le périmètre réseau traditionnel n'est plus un sanctuaire protégé, preuve en est le volume croissant de menaces et d'attaques cyber lancées sur les organisations. Caméras de sécurité, systèmes CVC, éclairage intelligent, stores connectés, pompes à perfusion, imprimantes, cafetières connectées, smart TV, assistants virtuels, DAB, terminaux de point de vente... À l'ère de l'Internet des objets (Internet of Things, IoT), une multitude d'appareils informatiques, conventionnels ou non, sont connectés et accèdent au réseau d'entreprise. Dès lors, les niveaux de risque sont réduits au plus petit dénominateur commun et la surface d'attaque augmente considérablement, ce qui aggrave les risques de déplacements latéraux.

Dans son rapport 2020 sur les menaces de l'IoT portant sur 1,2 million de terminaux, l'équipe Unit 42 de Palo Alto Networks chiffre à 30 % le nombre d'appareils IoT dans les entreprises en 2020. En outre, la base de données Gartner Machina IoT estime à 13 % la croissance annuelle des appareils IoT entre 2020 et 2030.



10M de nouveaux appareils IoT se connectent au réseau chaque jour*

Plus de **30+%** des ressources de l'entreprise sont des appareils IoT*

* Nombre d'appareils attendus en 2030, et augmentation en pourcentage de 2020 à 2030.

Figure 1 : Perspectives de croissance pour l'IoT par secteur, d'après la base de données Gartner Machina

Dans les entreprises, la prolifération des appareils IoT soulève de nombreuses craintes liées à la sécurité. Ces objets connectés livrés avec des failles, difficiles à corriger et dépourvus de tout contrôle de sécurité bénéficient pourtant d'un accès illimité au réseau. La figure 2 donne un aperçu d'attaques IoT menées récemment contre des entreprises.

Voici les conclusions du rapport Unit 42 sur les menaces IoT de Palo Alto Networks.

- Principales menaces pesant sur les appareils IoT :
  - Exploit par analyse réseau (14 %)
  - Pratiques liées aux mots de passe utilisateur (13 %)
  - Vers (12 %)
  - Ransomware (8 %)
- 57 % des objets connectés sont vulnérables aux attaques de gravité moyenne à élevée
- 83 % des appareils d'imagerie médicale fonctionnent sous des systèmes d'exploitation en fin de support

La multiplication des appareils IoT et la progression des attaques dont ils font l'objet ont forcé les entreprises à repenser leur stratégie de gestion du risque et à se tourner vers une approche Zero Trust pour sécuriser ces équipements.

Figure 2 : Les attaques IoT touchent tous les secteurs

Qu'est-ce que la sécurité Zero Trust ?

À l'heure où le télétravail, le BYOD, le transfert des ressources d'entreprise dans le cloud et l'engouement pour les objets connectés effacent le périmètre réseau classique, et ce dans un contexte de recrudescence des cybermenaces, le Zero Trust s'impose plus que jamais au cœur de la stratégie de sécurité des entreprises. Palo Alto Networks définit le Zero Trust comme une stratégie de sécurité qui consiste à éliminer toute confiance implicite et à valider toutes les étapes des interactions numériques entre un utilisateur/appareil et une entreprise. Cette approche solidement encadrée de la sécurité offre aux entreprises la possibilité de moderniser et de recréer les réseaux, de poursuivre leur progression dans le cloud et de renforcer leurs opérations de sécurité.

Figure 3 : Principaux objectifs du Zero Trust

Palo Alto Networks structure son approche Zero Trust sur des principes clés de sorte que la sécurité des utilisateurs, des applications et de l'infrastructure d'une entreprise (voir Tableau 1 ci-après) repose sur les quatre piliers suivants : Identité, Appareil/Workload, Accès et Transaction.

Tableau 1 : Principales fonctionnalités du Zero Trust et validation en continu

	Identité	Appareil/Workload	Accès	Transaction
Zero Trust pour les utilisateurs	Validation des utilisateurs par authentification forte	Vérification de l'intégrité de l'appareil utilisateur	Application de l'accès utilisateur aux données et aux applications sur le principe du moindre privilège	Analyse de l'ensemble du contenu à la recherche d'activités malveillantes et de vols de données
Zero Trust pour les applications	Validation des développeurs, du DevOps et des administrateurs par authentification forte	Vérification de l'intégrité des workloads	Application de l'accès sur le principe du moindre privilège pour les workloads qui accèdent à d'autres workloads	Analyse de l'ensemble du contenu à la recherche d'activités malveillantes et de vols de données
Zero Trust pour l'infrastructure	Validation de l'ensemble des utilisateurs qui ont accès à l'infrastructure	Identification de tous les appareils, objets connectés inclus	Segmentation de l'accès suivant le principe du moindre privilège pour l'infrastructure native et tierce	Analyse de l'ensemble du contenu de l'infrastructure à la recherche d'activités malveillantes et de vols de données

La sécurisation des appareils IoT non gérés constitue un élément essentiel pour concrétiser l'approche Zero Trust pour l'infrastructure. Quant aux principes clés, ils leur assurent une sécurité Zero Trust actionnable.

Zero Trust pour l'IoT : la bonne approche

Dérivés des principes du Zero Trust pour l'infrastructure présentés dans la section précédente, des principes granulaires spécifiques permettent d'instaurer le Zero Trust pour les appareils IoT.
Le tableau suivant propose une idée de cadre Zero Trust pour la sécurisation des objets connectés.

Tableau 2 : Approche Zero Trust pour l'infrastructure étendue aux appareils IoT

Appareil/Workload	Accès	Transaction
Découverte de tous les appareils IoT	Recommandation du modèle Zero Trust	Surveillance en continu des appareils IoT
Évaluation du risque de sécurité IoT	Implémentation du modèle Zero Trust	Prévention des menaces connues et inconnues

De nombreuses solutions font la promotion du Zero Trust pour les appareils connectés sans parvenir toutefois à répondre aux besoins complexes de la sécurité IoT. Voici quelques problématiques soulevées par la mise en place du Zero Trust pour l'IoT.

Sécurité Zero Trust pour les appareils IoT : les problématiques

1. Découverte et identification complexes

- Les solutions traditionnelles de sécurité des terminaux basées sur des agents sont incapables de détecter et de gérer les objets connectés. La faible puissance de calcul et de processeur inhérente à la plupart de ces appareils est incompatible avec l'installation d'un agent sur le terminal.
- La plupart des technologies de détection IoT se contentent de détecter et de classifier les appareils connectés dont les signatures ont été prérépertoriées. Les approches basées sur l'empreinte digitale ou la signature ne permettent pas de repérer l'ensemble des appareils IoT. En cause ? Une grande diversité de protocoles et de normes, ainsi que l'émergence d'appareils nouvelle génération sur le réseau.

- Les appareils IoT, fabriqués par lots, sont rarement identifiés de manière unique (contrairement aux appareils IT). Faute d'être découverts, identifiés et intégrés à l'inventaire des équipes IT, la plupart échappent à la vigilance et contribuent au phénomène de shadow IoT.

2. Authentification, définition des politiques et segmentation ardues

- La majorité des appareils IoT ne prennent pas en charge les mécanismes classiques d'authentification et d'autorisation d'entreprise, par exemple 802.1X ou SSO. Il en va de même de la liste des adresses MAC (MAC Authentication Repository, MAR) qui ne fonctionne pas en raison de la classification imprécise des appareils. Les appareils IoT étant des leviers de croissance pour l'entreprise, les équipes réseau n'ont donc pas d'autre choix que de les intégrer manuellement, sans toutefois contrevenir totalement à leur stratégie de gestion des risques.
- La définition de règles et de politiques de segmentation s'avère chronophage et fastidieuse. Cette tâche manuelle, qui permet de bloquer les mouvements latéraux de menaces, est encore compliquée par le manque de visibilité sur les appareils non gérés.

3. Évaluation en continu difficile

- Les objets connectés restent hors de portée des analyses de vulnérabilité par manque de visibilité.
- Nombre d'appareils IoT et OT font partie de l'infrastructure critique ; leur analyse ou sondage actif pour évaluer les risques et les vulnérabilités peut de fait perturber le réseau.

4. Faible sécurité des solutions de sécurité IoT

- Les solutions de sécurité IoT n'ont ni la Threat Intelligence ni la capacité nécessaires pour recommander des politiques Zero Trust de réduction des risques. Il incombe donc aux équipes de sécurité de rassembler des informations et du contexte sur l'appareil et de mettre en œuvre manuellement des politiques Zero Trust. Un processus lent et propice aux erreurs.
- Les solutions actuelles sont basées sur des alertes et n'intègrent aucun mécanisme de prévention des menaces ni d'application des politiques de sécurité.

Mise en place du Zero Trust pour les appareils IoT

Palo Alto Networks IoT Security fait entrer les appareils IoT dans le modèle de la sécurité Zero Trust, basée sur 3 piliers – appareil/workload, accès et transaction – et sur les principes qui vont de pair. L'objectif est de minimiser les risques liés à la sécurité IoT et de protéger votre réseau des cyberattaques. Palo Alto Networks simplifie à l'extrême le Zero Trust pour les objets connectés et améliore la posture de sécurité globale des entreprises. Voyons en pratique comment les organisations peuvent mettre en place le Zero Trust avec IoT Security de Palo Alto Networks.

Principe numéro 1 du Zero Trust : appareil/workload

Identification de tous les appareils, objets connectés inclus

1. Découverte

On ne peut sécuriser que ce que l'on voit. D'où l'importance de ne pas se limiter aux utilisateurs et aux appareils IT standard. Au contraire, l'extension des principes du Zero Trust passe par l'inclusion de tous les appareils IoT non gérés du réseau. IoT Security de Palo Alto Networks est la seule solution de sécurité IoT sans agent qui s'appuie sur le machine learning (ML) et l'inspection approfondie des paquets (DPI) alliée à la télémétrie collaborative. Sa mission : découvrir et catégoriser tous les appareils IoT connectés du réseau, y compris ceux jusqu'alors invisibles. Le machine learning (ML) surpasse toutes les méthodes de découverte des appareils réactives, traditionnelles et basées sur la signature. Cette approche permet de découvrir et de catégoriser en temps réel, de façon rapide et précise, les appareils IoT arrivés sur le réseau à la faveur du modèle hybride de télétravail ou de protocoles sans fil nouvelle génération comme la 5G.

Notre solution IoT Security passe au crible 200 paramètres pour associer précisément l'adresse IP de chaque appareil avec son type, son fournisseur et son modèle et faire émerger plus de 50 attributs essentiels à leur catégorisation. Cette classification précise et granulaire en amont est indispensable pour distinguer les appareils IoT non gérés des ressources IT gérées. Cette méthode permet d'appliquer des politiques de sécurité Zero Trust n'autorisent que le trafic approuvé dans votre environnement IoT.

Le tableau suivant présente les principales catégories d'informations contextuelles d'IoT Security.

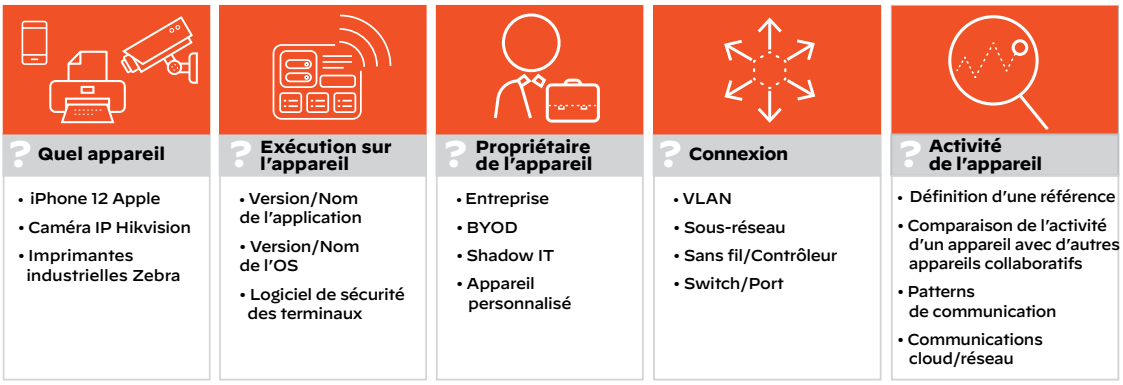


Figure 4 : IoT Security peut détecter 90 % des appareils en 48 heures, et plus par la suite

2. Évaluation du risque

Deuxième étape de la mise en œuvre du Zero Trust, l'évaluation du risque fournit une indication très précise du niveau de risque pour chaque appareil IoT. Or, la notion de « risque » est devenue assez floue et désigne indifféremment une menace ou une vulnérabilité. Une définition précise s'impose donc. Le risque est la vraisemblance qu'une menace exploite des vulnérabilités pour compromettre les actifs ou leur nuire (ici, les appareils IoT). Par conséquent, le risque lié aux appareils IoT se mesure à l'aune de trois vecteurs : les menaces, les vulnérabilités et le contexte des ressources. IoT Security de Palo Alto Networks détecte et évalue le risque en tenant compte de ces trois éléments. Pour ce faire, la solution s'appuie sur de multiples sources d'informations : données collaboratives de l'appareil, évaluation des anomalies comportementales des appareils établie par ML, travaux de recherche de l'équipe Unit 42, failles et vulnérabilités communes (CVE), systèmes de gestion des vulnérabilités tiers, etc.

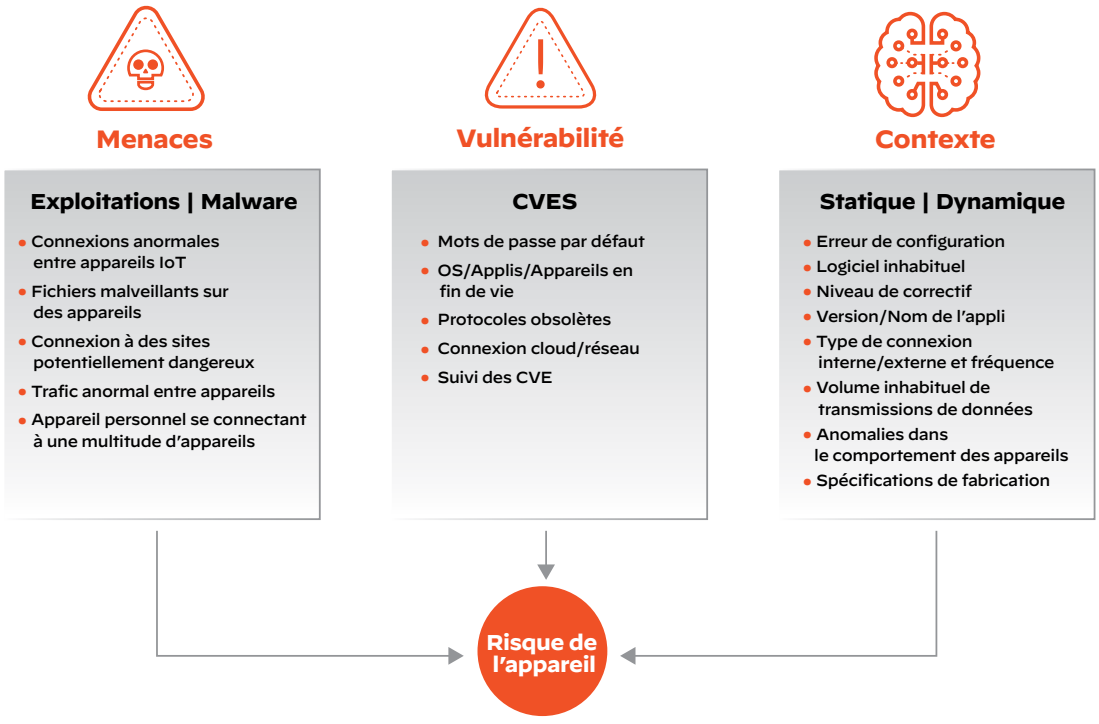


Figure 5 : Approche et évaluation complètes des risques

IoT Security mesure le risque et attribue une note pour chacun des 4 critères suivants :

1. Appareils IoT individuels
2. Profil de l'appareil
3. Site
4. Entreprise

Pour calculer les scores de risque des profils d'appareils, des sites et des entreprises, IoT Security intègre, outre les scores des appareils d'un groupe, le pourcentage d'appareils à risque calculé pour l'ensemble des appareils du groupe. Les différents scores sont un moyen simple de connaître le risque à différents points du réseau.

Découvrez comment réduire le temps de détection des vulnérabilités des appareils IoT du réseau de plus de trois semaines à quelques heures.

Principe numéro 2 du Zero Trust : accès

Segmentation suivant le principe du moindre privilège pour l'infrastructure native et tierce

3. Politique du moindre accès

La politique du moindre accès est un élément essentiel du Zero Trust. Intégrée à la sécurité IoT, elle restreint au minimum l'accès d'un appareil IoT au réseau. Les objets connectés, généralement dédiés et dotés d'un comportement prédictif, se prêtent bien à la mise en œuvre de la politique du moindre accès, notamment dans les cas suivants :

- **Création de politiques dynamiques (virtual patching) pour assurer le fonctionnement opérationnel des appareils IoT :** la politique du moindre accès autorise le fonctionnement d'appareils vulnérables, mais en bloquant ou en limitant leur accès à certaines ressources. Cette approche est très utile lorsque des appareils IoT/OT sont des leviers d'activité et doivent être opérationnels. C'est notamment le cas des appareils IoT critiques dans les établissements de santé ou sur des sites de production. Cette stratégie temporaire limite le risque d'exploitation d'une vulnérabilité avant qu'elle ne soit éliminée.
- **Politique de contrôle d'accès réseau :** la politique du moindre accès permet également de limiter ou de restreindre l'accès des appareils IoT à certaines ressources pour l'exécution de leurs tâches. Par exemple, une caméra de surveillance a besoin de communiquer uniquement avec le système de stockage vidéo et le site web du fournisseur pour les mises à jour du firmware.

Désormais, la définition et l'élaboration de politiques de réduction des risques par profil d'appareil s'avèrent extrêmement laborieuses. Inventaire des périphériques IoT, définition des profils d'appareils par type ou fonction, définition de comportements jugés normaux, mise au point de politiques qui n'interrompent pas les opérations, intégration avec d'autres technologies pour appliquer ces politiques… les étapes manuelles sont nombreuses.

La solution de Palo Alto Networks est la seule du marché à avoir fait évoluer l'évaluation du risque en proposant systématiquement des politiques d'accès Zero Trust basées sur le moindre accès pour réduire les risques. IoT Security compare les métadonnées de millions d'appareils IoT avec celles de votre réseau et utilise ses propres profils d'appareils pour déterminer des modèles de comportements considérés comme normaux. Chaque équipement et catégorie d'équipements IoT font ainsi l'objet de recommandations quant aux politiques à adopter pour restreindre ou autoriser les accès, accélérant l'implémentation des stratégies Zero Trust sans recourir à des processus manuels et chronophages. Pour chaque appareil, les équipes de sécurité gagnent de fait des heures précieuses qu'elles devraient normalement consacrer à la collecte de données sur les ports/protocoles, les connexions et l'utilisation des applications, pour ensuite définir elles-mêmes des politiques adaptées. Une fois validées, les politiques sont rapidement importées sur votre pare-feu nouvelle génération (NGFW) piloté par machine learning. Tout changement se répercutera automatiquement afin de réduire vos tâches d'administration au strict minimum.

IoT Security automatise la création de politiques pour vous faire gagner 20 fois plus de temps. Découvrez comment.

Politique de segmentation du réseau

Dans le droit fil du principe du Zero Trust « ne jamais faire confiance, toujours vérifier », la segmentation des appareils IoT peut être perçue comme une étape fondamentale vers cette approche. Par exemple, dans les établissements de santé, il serait peu judicieux de placer des moniteurs de fréquence cardiaque sur le même réseau que des systèmes d'imagerie. Une segmentation basée sur le profil des appareils et une variété de facteurs (type d'appareil, fonction, niveau de criticité, niveau de menace, etc.) permettent de mettre en place des pratiques d'isolement qui réduisent considérablement l'impact potentiel d'une infection croisée.

Déployé sur le pare-feu nouvelle génération de Palo Alto Networks, IoT Security adopte une approche granulaire de la segmentation basée sur le profil d'appareil, qui tient compte de ces facteurs pour activer la séquestration. L'impact potentiel d'une infection croisée entre les appareils IT et IoT est ainsi considérablement réduit. L'utilisation du pare-feu nouvelle génération de Palo Alto Networks (Next-Generation Firewall, NGFW) comme passerelle de segmentation permet de bénéficier de ses fonctionnalités réseau intrinsèques pour un déploiement fluide dans l'environnement. Elle favorise ainsi l'apport mesuré de contrôles de sécurité sur des appareils IoT non gérés sur le réseau.

Si vous préférez recourir à une solution NAC pour segmenter votre réseau, IoT Security s'intègre aussi en natif à Cisco ISE, Forescout® et Aruba ClearPass®. Sachez toutefois que le contrôle NAC ne voit que les appareils authentifiables ; qui dit appareils IoT non authentifiés, donc sans utilisateurs associés, dit angles morts. IoT Security fournit à la solution NAC des informations sur les appareils non gérés détectés, y compris des données contextuelles garantes d'une segmentation intelligente et efficace. Voici un exemple réel tiré de l'un de nos clients, qui illustre comment IoT Security élimine les angles morts de la solution NAC pour la visibilité et le contexte.

Tableau 3 : IoT Security élimine les angles morts de la solution NAC		
MAC	**Identité NAC**	**Identité IoT Security**
00:*0:7*:73:37:5*	Appareil AmbiCom	Station pour pompe à perfusion Carefusion
c8:2*:*4:56:27:06	Appareil Apple	Poste de travail médical
08:60:6*:*8:06:83	Appareil Asus	Poste de travail médical
00:08:74:*2:50:*5	Appareil Dell	Visionneuse DICOM
00:2*:5*:6*:06:72	Appareil HP	Imageur DICOM
00:09:6*:*6:60:7*	Appareil IBM	Poste de travail médical
00:*0:*4:2*:*0:94	Appareil technologique INSIDE	Poste de travail médical
Nbre total d'appareils	**5 958**	**12 012**

Tableau 4 : Appareils NAC et IoT Security détectés	
NAC	**IoT Security**
Appareils détectés = 5 698	Appareils détectés = 12 012
Contexte NAC =	Contexte Sécurité IoT =
Appareil-AmbiCom	Station pour pompe à perfusion AmbiCom Carefusion

Le partitionnement en contexte des appareils IoT leur assure un accès sur le principe du moindre privilège et restreint leur connexion aux applications requises. En outre, cette approche les isole des réseaux hôtes et d'entreprise et minimise les temps d'interruption de fonctionnement dans les infrastructures IoT critiques en neutralisant les problèmes d'incompatibilité qui surviennent entre systèmes.

4. Application de la politique

IoT Security peut appliquer les politiques de sécurité Zero Trust recommandées en natif avec sa passerelle NGFW ou par le biais de points de contrôle tiers. Voyons comment elles sont mises en œuvre :

- Appliquez les recommandations en un clic via la passerelle NGFW de Palo Alto Networks. Notre composant breveté Device-ID™ surveille un appareil sur le réseau et, à chaque alerte ou incident, fournit des informations détaillées en contexte sur la passerelle NGFW pilotée par machine learning, sans tenir compte des changements d'adresse IP ou d'emplacement de l'appareil. En outre, les règles de politique et les contrôles en couche L7 sont automatiquement mis à jour en cas de changement dans les emplacements et les risques identifiés. Le tableau 5 explique en quoi Device-ID est plus évolutif et plus rapide pour éliminer les menaces et y répondre.
- Appliquez les politiques recommandées via nos intégrations NAC avec Cisco ISE, Forescout ou Aruba ClearPass.

Tableau 5 : Device-ID : une solution de mise en œuvre rapide et précise des politiques pour les administrateurs	
Sans Device-ID	**Avec Device-ID**
Utiliser une adresse IP comme proxy pour l'identité de l'appareil manque de précision	L'identité de l'appareil est disponible dans la politique
Compter sur les utilisateurs, le réseau ou les administrateurs de l'appareil pour mettre un terme aux incidents de l'appareil est propice aux erreurs et aux exploits	Application uniforme d'une politique indépendamment du lieu de connexion et de la configuration de l'appareil
S'appuyer sur des systèmes externes de contrôle d'accès réseau (NAC) ou de gestion des ressources, par exemple, suppose des intégrations en natif et des mises à jour	Alimentation directe de Device-ID via IoT Security, sans intégration complexe
En cas de menaces ou d'incidents, le SOC doit explorer plusieurs systèmes pour trouver l'appareil impliqué.	Les alertes sont envoyées sur le SIEM avec des informations sur l'appareil

Principe numéro 3 du Zero Trust : transaction

Analyse de l'ensemble du contenu de l'infrastructure à la recherche d'activités malveillantes et de vols de données.

5. Surveillance en continu

La surveillance continue est la dernière étape, et non des moindres, de la mise en œuvre de la sécurité Zero Trust pour l'IoT. Même correctement profilé et placé dans le segment approprié, un appareil peut toujours être compromis en se connectant au réseau. Le cas échéant, l'accès aux ressources et au réseau de cet appareil doit être bloqué sans attendre.

Notre solution IoT Security pilotée par ML vérifie automatiquement l'identité de l'appareil et ses « comportements normaux ». Une fois les « comportements normaux » identifiés, la solution lance la détection des anomalies pour repérer et évaluer tout écart potentiel par rapport aux comportements de référence. Notre solution de machine learning crée un référentiel de comportements pour les appareils IoT de la Couche L7 et fournit deux types d'information :

- Grâce au ML, IoT Security compare les comportements avec des données collectives de référence pour entretenir constamment une base de référence et surveiller les écarts. Ces informations servent à automatiser la création de politiques Zero Trust.
- IoT Security surveille également les flux des appareils et les schémas de communication et les compare en continu avec ceux du VLAN. Objectif : simuler la microsegmentation appropriée, puis l'appliquer.

Les appareils IoT génèrent des patterns uniques et identifiables de comportement réseau. IoT Security conjugue machine learning et IA pour reconnaître ces comportements et identifier chaque appareil du réseau. La solution crée ainsi un inventaire contextuel complet, maintenu à jour en permanence de manière dynamique. Après avoir identifié un appareil et établi une base de référence de ses activités réseau normales, la solution surveille son activité réseau pour détecter tout comportement inhabituel symptomatique d'une attaque ou d'une faille. IoT Security envoie sur le portail des alertes de sécurité aux administrateurs et, suivant les préférences de chacun, signale les activités suspectes par e-mail et SMS. En outre, la solution bloque l'accès au réseau de l'appareil qui n'est pas conforme à la politique de sécurité et de conformité établie.

6. Prévention intégrée

IoT Security mise sur des technologies leaders de prévention des intrusions, d'analyse anti-malware, de filtrage web et de sécurité DNS pour surveiller tous les appareils IoT et bloquer toutes les menaces qui ciblent vos objets connectés. Parfaitement intégrés à IoT Security, nos services de sécurité dans le cloud coordonnent toute la Threat Intelligence afin de bloquer les menaces IT, OT, IoT et IoMT, sans surcharger vos équipes de sécurité. Pour réduire les temps de réponse, les objets connectés compromis peuvent être systématiquement isolés par nos pare-feu nouvelle génération pilotés par machine learning. Ainsi, vos équipes de sécurité disposent de tout le temps nécessaire pour élaborer un plan de remédiation sans risquer une propagation de l'infection.

Implémentation du Zero Trust sur toute l'infrastructure

Par le passé, la conduite à tenir consistait à sécuriser les utilisateurs, les applications et les appareils identifiables dans le périmètre du réseau. Seulement voilà, la donne a changé avec la recrudescence d'appareils IoT non gérés dans les entreprises conjuguée à la complexité nouvelle d'un périmètre de sécurité réseau qui semble s'étirer sans fin. D'où la nécessité pour les entreprises d'adopter une approche de la sécurité IoT nouvelle, simplifiée et axée sur les bonnes pratiques de la sécurité Zero Trust.

Demandez une démo gratuite de la solution de sécurité IoT la plus complète du marché et découvrez comment Palo Alto Networks IoT Security simplifie considérablement l'adoption du Zero Trust pour les appareils IoT non gérés.

paloalto NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam, Pays-Bas

Téléphone :
+31 20 888 1883
www.paloaltonetworks.fr