LA RGPD

Et comment la plate-forme de sécurité nouvelle génération peut vous aider à vous y conformer

Qu'est ce que la RGPD

Définition

Le règlement général sur la protection des données, ou RGPD, est la règlementation Européenne concernant la **protection des données personnelles** qui remplace la Directive sur la Protection des Données de 1995, à partir du 25 mai 2018. La but de la RGPD est d'apporter aux Européens une meilleure visibilité sur la manière dont sont collectées et managées leurs données personnelles.

Les sanctions

La RGPD introduit aussi des amendes administratives. Les conséquences d'une non-conformité sont sévères : concernant la sécurité ou la notification d'une brèche, l'amende peut s'élever à **2% du chiffre d'affaires annuel** (ou 10 000 000€ plafonné). L'amende peut s'élever au-delà en cas de non-respect des règles sur la collecte, le traitement et les obligations administratives (comme celle d'avoir le consentement, ou de nommer un Responsable de la Protection de la Donnée), **à 4% du chiffre d'affaires annuel** ou 40 000 000€.

Qui est concerné ?

La RGPD s'applique à **toutes les entités qui contrôlent ou traitent des données personnelles des résidents de l'UE**. Dans la loi, les données personnelles incluent les données permettant d'identifier ou pouvant être utilisées pour contacter quelqu'un (ex : nom, e-mail, date de naissance) ; les données qui identifient un équipement unique potentiellement utilisée par une seule personne (ex : adresse IP) ; ou les données qui peuvent être associées à l'activité ou le comportement d'une personne (ex : localisation, application téléchargée sur un équipement, site internet visité) (RGPD Article 4.1)

Les exigences

La RGPD a des dispositions dédiées au management de la donnée, notamment sur la **collecte ou le traitement**. La **sécurité des données** est aussi un pilier de la RGPD. En plus des exigences de sécurité, la loi introduit l'obligation de **notifier les brèches** impliquant la perte ou le vol de données personnelles dans les 72 heures après la découverte de celle-ci.

La RGPD est une loi complexe de protection de la donnée qui comprend de nombreuses obligations concernant le management de la donnée. **Palo Alto Networks peut contribuer aux efforts globaux pour être en conformité avec la RGPD** – en particulier concernant **la sécurité de la donnée et la protection**. Palo Alto Networks ne revendique pas d'adresser tous les aspects pour la conformité à la RGPD, mais la plateforme de sécurité nouvelle génération peut être positionnée comme un élément essentiel à la conformité à la RGPD.

Qu'est-ce que cela signifie pour les entreprises ?

Les entreprises doivent se mettre en conformité avec la RGPD en Mai 2018. Il y a plusieurs engagements, comme celui de notifier lorsqu'on collecte de la donnée personnelle, des interdictions sur du traitement non autorisé de données, et un devoir de recruter un Responsable de la Protection de la Donnée selon les cas. Sur un point de vue sécurité, les entreprises doivent particulièrement :

MIEL

Distribution. Formation. Assistance. Appelez le 01 60 19 34 52

D'un point de vue sécurité, les entreprises doivent particulièrement :

- Implémenter les mesures appropriées sur le plan technique et organisationnel pour assurer un niveau de sécurité en phase avec le risque.

Ces mesures sont centrées sur la collecte et le traitement de la donnée, et doivent tenir compte de l'état de l'art.

- Informer les autorités de supervision si de la donnée personnelle est perdue, volée ou compromise, 72 heures maximum après avoir été informées de la brèche.

Comment Palo Alto Networks contribue à la conformité à la RGPD ?

1) Sécuriser la donnée personnelle

La plateforme Palo Alto Networks sécurise la donnée à tous les niveaux (application, réseau, terminal, comme sur le cloud) en combinant la sécurité réseau et des terminaux à une base de données d'intelligence de la menace dans le Cloud, pour apporter une protection automatisée et prévenir les cyber-attaques (pas seulement les détecter).
Elle assemble toutes les fonctionnalités clés de sécurité – comprenant le firewall, le filtrage URL, l'IDS/IPS et la protection avancée des terminaux. Parce que ces fonctions sont intégrées nativement dans la solution avec la prévention des cyber-menaces en but premier, et partagent nativement l'information, la plateforme de sécurité Palo ALto Networks garantit une meilleure sécurité que les firewalls et antivirus traditionnels ou que tout autre produit de détection de menaces.

La RGPD demande des mesures de sécurité techniques et organisationnelles qui tiennent compte de l'état de l'art. Les menaces évoluent constamment, l'état de l'art des technologies doit évoluer en parallèle.

Avec la plateforme Palo Alto Networks, les entreprises peuvent valider et sécuriser l'utilisation de toutes les applications critiques, poursuivre avec confiance de nouvelles initiatives technologiques, et se protéger contre toutes les attaques même les plus sophistiquées.
Palo Alto Networks aide les responsables informatiques qui veulent pouvoir affirmer qu'ils sont conformes à l'état de l'art.

2) Empêcher les fuites/violation des données

La plateforme Palo Alto Networks est basée sur 4 principes clés :

- Apporter une visibilité complète
- Réduire la surface d'attaque
- Prévenir les menaces connues
- Prévenir les menaces inconnues

Ces principes de prévention fonctionnent avec le moteur d'analyse de la menace WildFire, l'outil le plus avancé du marché permettant la protection contre les malwares et exploits « zero-day » évasifs. Le service Cloud emploie une approche multi-techniques qui combine l'analyse dynamique et statique, des techniques de "machine learning" et une analyse encore plus profonde des terminaux réels (bare metal) pour détecter et prévenir les menaces les plus avancées.

Par ailleurs, la plateforme de sécurité peut aussi prévenir les fuites de données intentionnelles ou accidentelles par les collaborateurs internes à travers toute l'infrastructure. Cela peut se faire de plusieurs façons :

- **Sécurité réseau**. Pour protéger la donnée dans l'entreprise, les profils de filtrage de données intégrés dans le firewall nouvelle génération aident à prévenir la fuite de donnée accidentelle au niveau réseau.

- **Sécurité dans le cloud**. La plateforme utilise le firewall nouvelle génération et Aperture (Api de sécurisation) pour contrôler l'accès aux services SaaS.
  Le firewall nouvelle génération analyse le trafic depuis le réseau jusqu'aux applications SaaS et vice versa.
  Aperture agit en complément en utilisant des API SaaS pour se connecter directement aux applications cloud.
  Le data center Européen d'Aperture est basé à Francfort pour garantir une conformité totale avec la RGPD.

- **Sécurité des terminaux**. La protection avancée de Traps utilise une approche multi-méthodes pour bloquer les menaces connues et inconnues, dont les menaces « zéro day », sur les terminaux en utilisant un minimum de ressources.

- **Sécurité des identifiants** (stopper le vol d'identifiants). Palo Alto Networks donne la capacité d'arrêter les attaques par vol d'identifiants à différents niveaux de la chaine d'attaque d'un réseau, et de stopper la fuite d'identifiants en empêchant les utilisateurs de soumettre leurs identifiants sur des sites internet inconnus et non autorisés.

3) Notification d'une violation des données

Même si la solution n'a pas été développée dans ce sens, elle peut aider à la création de rapport pour modifier les violations de données.

- **Le management de la sécurité réseau Panorama** : une console depuis laquelle les firewalls nouvelle génération et les terminaux peuvent être managés. Panorama stocke tous ces logs qui pourront être utilisés pour la remédiation et la notification de brèches.

- **Le service d'intelligence de la menace contextuel Autofocus** : Autofocus peut apporter les analyses nécessaires à la remédiation, en aidant à comprendre l'utilisateur, la menace, l'impact et le niveau de risque, tout ce qui peut aider pour les exigences de notification.

Pour en savoir plus !

Un livre blanc en anglais est disponible en téléchargement via ce lien : https://goo.gl/jSnrPY.

Il inclut une liste complète des produits proposés par Palo Alto Networks et détaille les fonctionnalités qui vous aideront dans la mise en conformité de votre entreprise à la RGPD.

MIEL

Pour en savoir plus : http://www.miel.fr/palo-alto-networks

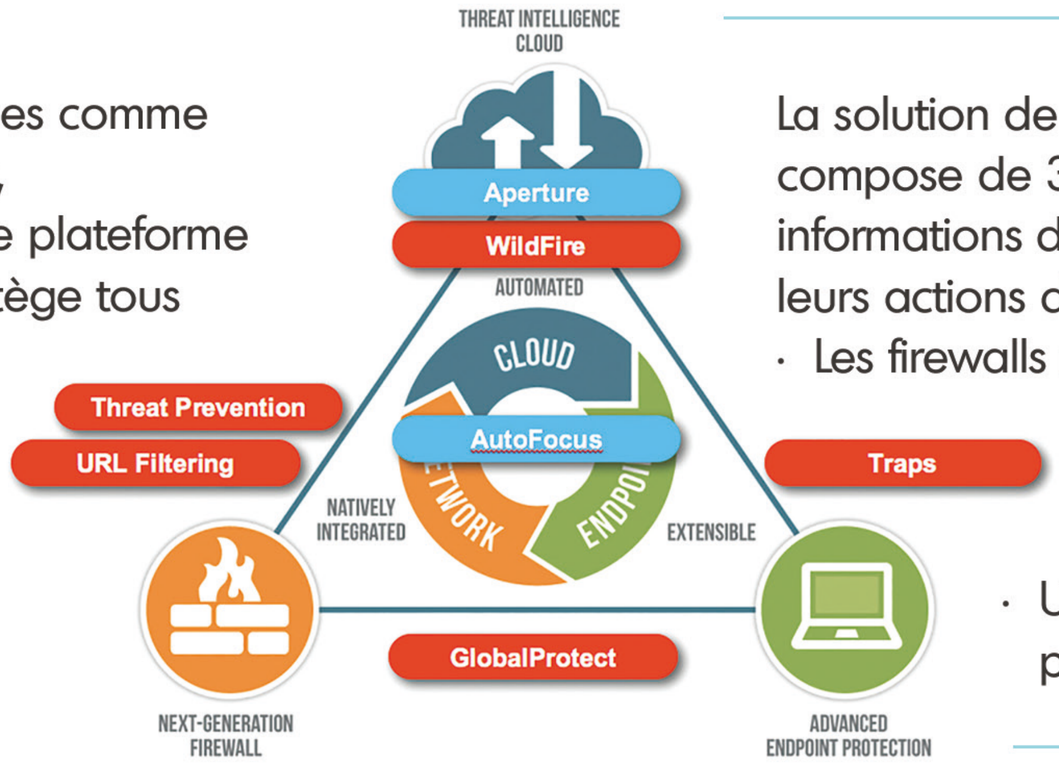
Palo Alto Networks :

Plateforme de sécurité

Nouvelle génération

Une plateforme de sécurité intégrée réseau, cloud et endpoint

Avec des partenaires stratégiques comme VMware, Citrix, Arista ou Splunk, Palo Alto Networks propose une plateforme de sécurité d'entreprise qui protège tous les utilisateurs, tous les devices, sur tous les points du réseau et du data center.



La solution de Palo Alto Networks se compose de 3 éléments qui corrèlent leurs informations de détection et coordonnent leurs actions de protection :

- Les firewalls nouvelle génération
- Une intelligence dans le cloud, de renseignement sur les menaces
- Une protection avancée du poste client

Palo Alto Networks leader sur le marché des pare-feux pour réseaux d'entreprise pour la sixième année consécutive

Le 10 juillet 2017, Gartner a dévoilé son nouveau Magic Quadrant orienté pare-feux pour réseaux d'entreprise.

Palo Alto Networks est positionné leader sur ce marché par le cabinet d'études pour ses capacités d'éxecution et de visibilité.

Palo Alto Networks a récemment lancé la version 8.0 de son système d'exploitation (PAN-OS), comprenant des améliorations sur WildFire et Panorama, et de nouvelles fonctionnalités de protection des utilisateurs de SaaS. L'entreprise a également publié un nouveau modèle de matériel d'entrée de gamme (PA-220), deux nouveaux appareils intermédiaires (série PA-800) et a actualisé sa série 5000, disponible depuis 2011, avec les modèles 5220, 5250 et 5260.

Téléchargez le rapport complet du Gartner ici :
https://goo.gl/9ZC4xL

ou flashez ce code

MiEL

Pour en savoir plus : http://www.miel.fr/palo-alto-networks