WildFire™

WildFire identifie les logiciels malveillants inconnus, les exploits zero day et les menaces persistantes avancées ou APT (Advanced Persistent Threats) grâce à une analyse dynamique dans un environnement virtuel évolutif basé sur le cloud. Il diffuse automatiquement des protections, presque en temps réel, pour aider les équipes de sécurité à réagir aux cyber-attaques avancées. WildFire repose sur une plateforme de sécurité d'entreprise qui classifie l'ensemble du trafic en natif, y compris les menaces et les applications qui les contiennent, indépendamment du port ou du chiffrement SSL.

- Identifie les logiciels malveillants inconnus et les exploits zero day à l'aide de techniques d'analyse statique et dynamique avancées.
- Allie la visibilité et le contrôle complets des applications et menaces connues à l'analyse dynamique basée sur le cloud des menaces inconnues pour garantir une analyse précise, sûre et évolutive des logiciels malveillants.
- Véritable blocage en ligne des fichiers dangereux et malveillants, ainsi que du trafic de commande et contrôle.

Les cyber-attaques avancées emploient des méthodes furtives et persistantes pour déjouer les mesures de sécurité traditionnelles. Pour contrer ces adversaires redoutables, les équipes de sécurité d'aujourd'hui doivent se rendre à l'évidence : les systèmes de prévention des intrusions, programmes antivirus et bacs à sable monofonctionnels traditionnels ne sont pas en mesure de vaincre les menaces persistantes avancées.

Plateforme de sécurité pour entreprise

WildFire repose sur la plateforme de sécurité leader du secteur offrant une visibilité totale sur le trafic réseau, y compris les tentatives furtives de déjouer les systèmes de détection comme les ports non standard ou le chiffrement SSL. Les menaces connues sont bloquées de manière proactive grâce à une prévention fournissant des défenses de base contre les exploits connus, les logiciels malveillants, les URL à haut risque et l'activité de commande et contrôle (C2). Les fichiers inconnus sont analysés par WildFire dans un environnement de bac à sable virtuel et évolutif dans lequel les nouvelles menaces sont identifiées et des protections sont automatiquement développées et transmises sous la forme de mises à jour. Il en résulte une approche unique en boucle fermée du contrôle des cyber-menaces, qui commence par des contrôles de sécurité positifs pour réduire la surface d'attaque, inspecte l'ensemble du trafic, des ports et des protocoles pour bloquer toutes les menaces connues, détecte rapidement les menaces inconnues en observant leur comportement dans un environnement d'exécution virtuel basé sur le cloud, puis met en œuvre automatiquement en première ligne de nouvelles protections pour garantir que les menaces précédemment inconnues sont désormais connues de tous et bloquées sur toute la chaîne d'élimination.

WildFire

WildFire est un environnement d'analyse des logiciels malveillants virtuel avancé, spécialement conçu pour l'émulation matérielle haute fidélité et qui analyse les échantillons suspects au fur et à mesure de leur exécution. Plutôt que de s'en remettre à des signatures préexistantes, ce service basé sur le cloud détecte et bloque les logiciels malveillants ciblés et inconnus, les exploits et l'activité C2 sortante en observant leur comportement. Outre le fait de porter rapidement à la connaissance de tous des menaces inconnues, WildFire génère des protections qui sont partagées à travers le monde en 15 minutes. Le service de sécurité s'intègre étroitement aux pare-feu nouvelle génération Palo Alto Networks®, permettant un contrôle complet du réseau tandis que les cyber-criminels tentent d'y introduire des logiciels malveillants ou de communiquer avec des systèmes infectés.

paloalto networks®

Mise au jour des cyber-menaces par l'étude des comportements

Pour détecter les logiciels malveillants et exploits inconnus, WildFire exécute le contenu suspect sous les systèmes d'exploitation Windows XP, Windows 7 et Android, avec une visibilité totale sur les types de fichiers courants, y compris les fichiers EXE, DLL, ZIP, les documents PDF, les documents Office, le contenu Java, les packages APK Android, les applets Adobe Flash et les pages Web, en incluant le contenu intégré à haut risque tel que le JavaScript, les fichiers Adobe Flash et les images.

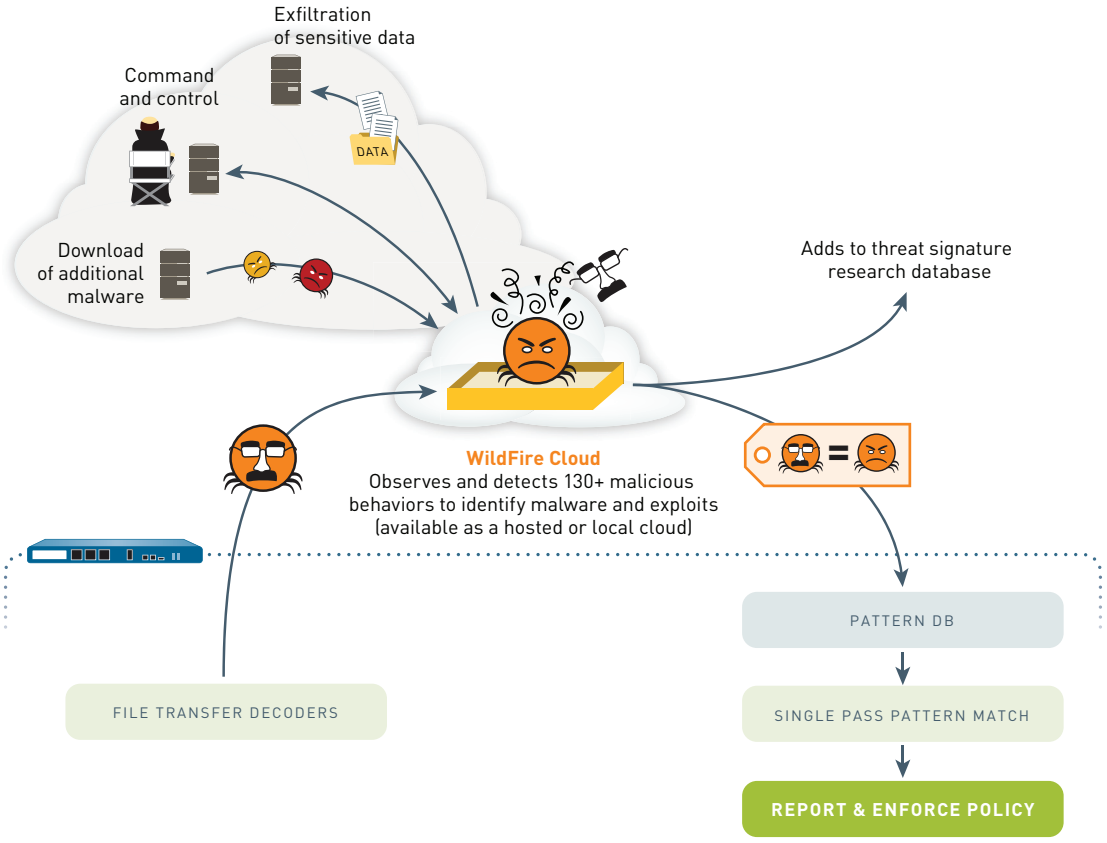
WildFire identifie plus de 200 comportements potentiellement malveillants pour déceler la vraie nature des fichiers malveillants selon leurs actions, notamment :

- **Changements apportés à l'hôte :** examen de tous les processus impliquant des modifications de l'hôte, y compris l'activité sur les fichiers et le registre, l'injection de code, les attaques par pulvérisation des segments de mémoire (exploits), l'ajout de programmes auto-exécutables, les exclusions mutuelles (mutexes), les services Windows et autres activités suspectes.
- **Trafic réseau suspect :** analyse de toute l'activité réseau produite par le fichier suspect, y compris la création de portes dérobées, le téléchargement de logiciels malveillants subséquents, la visite de domaines peu fréquentables, la reconnaissance de réseau, etc.
- **Détection des techniques anti-analyse :** surveillance des techniques utilisées par les logiciels malveillants avancés pour éviter l'analyse par machine virtuelle, comme la détection de débogueur, la détection d'hyperviseur, l'injection de code dans des processus de confiance, la désactivation des fonctions de sécurité basées sur l'hôte, etc.

Étendant la plateforme de pare-feu nouvelle génération qui classifie l'ensemble du trafic sur des centaines d'applications en natif, WildFire applique cette analyse de comportement indépendamment du port ou du chiffrement, avec une visibilité totale sur le trafic Web, les protocoles de messagerie (SMTP, IMAP, POP) et le protocole FTP.

Architecture de détection basée sur le cloud

ePour permettre une analyse anti-malware dynamique sur tout le réseau à grande échelle, WildFire repose sur une architecture basée sur le cloud qui peut être exploitée



Mode de fonctionnement de WildFire : WildFire est l'association logique d'un pare-feu matériel nouvelle génération et d'une analyse des logiciels malveillants basée sur le cloud et évolutive.

par votre pare-feu nouvelle génération Palo Alto Networks existant, sans matériel supplémentaire. Dans les cas où des contraintes règlementaires ou relatives à la confidentialité empêchent l'utilisation d'une infrastructure de cloud public, une solution de cloud privé peut être conçue sur site à l'aide de l'appareil WF-500. Dans les deux scénarios, WildFire offre la même visibilité de haut niveau et un déploiement simple et peu coûteux.

Prévention des menaces grâce au partage d'informations au niveau mondial

Lorsqu'une menace inconnue est découverte, WildFire génère automatiquement des protections pour la bloquer sur toute la cyber-chaîne d'élimination, partageant ces mises à jour avec tous les abonnés du monde entier en seulement 15 minutes. Ces mises à jour rapides sont en mesure de stopper rapidement la diffusion de logiciels malveillants, ainsi que d'identifier et de bloquer la prolifération de toutes les variantes futures sans action ni analyse supplémentaire. Le partage d'informations au niveau mondial par les clients de Palo Alto Networks contribue à l'éradication progressive des cyber-attaques.

En conjonction avec la protection contre les fichiers dangereux et malveillants, WildFire examine en profondeur les communications sortantes malveillantes, perturbant l'activité de commande et contrôle avec des signatures anti-C2 et des signatures de rappel basées sur DNS. Ces données alimentent également PAN-DB, où les URL malveillantes récemment découvertes sont automatiquement bloquées. Cette mise en corrélation des données et protections en ligne est essentielle à l'identification et au blocage des intrusions en cours ainsi que des futures attaques sur un réseau.

Journalisation, création de rapports et recherche de preuves intégrées

Les utilisateurs de WildFire bénéficient de journaux, d'analyses et d'une visibilité intégrés sur les évènements WildFire dans l'interface de gestion, Panorama ou le portail WildFire, ce qui permet aux équipes d'enquêter rapidement sur les évènements observés sur leurs réseaux et de les mettre en corrélation. Le personnel de sécurité peut ainsi localiser promptement les données nécessaires à des enquêtes immédiates et à la résolution des incidents. L'analyse des journaux et les signatures personnalisées permettent de réagir aux indicateurs de compromission basés sur l'hôte et basés sur le réseau.

Pour aider les équipes de sécurité et de réponse aux incidents dans la détection des hôtes infectés, WildFire fournit également les éléments suivants :

- Une analyse détaillée de chaque fichier malveillant envoyé à WildFire dans différents environnements de systèmes d'exploitation, y compris l'activité basée sur l'hôte comme sur le réseau.
- Les données de session associées à la diffusion du fichier malveillant, y compris la source, la destination, l'application, le User-ID™, l'URL, etc.
- Un accès à l'échantillon du logiciel malveillant d'origine à des fins d'ingénierie inverse et les PCAP complets des sessions d'analyse dynamique.
- Une API ouverte pour l'intégration aux meilleurs outils SEIM, tels que l'application Palo Alto Networks pour Splunk et les agents de terminaux leaders.

Cette analyse fournit une multitude d'indicateurs de compromission qui peuvent être appliqués sur toute la chaîne d'élimination des APT.

Préservation de la confidentialité de vos fichiers

WildFire met à profit un environnement de cloud public géré directement par Palo Alto Networks. Tous les fichiers suspects sont transférés de manière sécurisée entre le pare-feu et le centre de données WildFire via des connexions chiffrées, signées des deux côtés par Palo Alto Networks. Tout fichier identifié comme bénin est détruit, tandis que les fichiers malveillants sont archivés en vue d'une analyse approfondie.

Configuration requise pour WildFire :

- L'utilisation de WildFire nécessite PAN-OS™ 4.1+
- L'analyse de contenu PDF, Java, Office et APK nécessite PAN-OS 6.0+
- L'analyse de contenu Adobe Flash et de pages Web nécessite PAN-OS 6.1+

Informations de licence :

Les fonctionnalités WildFire de base sont disponibles en standard sur toutes les plateformes exécutant PAN-OS 4.1 ou une version supérieure.

- Images d'analyse Windows XP et Windows 7
- Types de fichiers EXE et DLL, y compris le contenu compressé (zip) et chiffré (SSL)
- Soumission automatique des fichiers suspects à WildFire
- Protections automatiques délivrées avec les mises à jour régulières de contenu de prévention des menaces (une licence de prévention des menaces est nécessaire) toutes les 24-48 heures

L'abonnement WildFire ajoute une protection presque en temps réel contre les menaces avancées, avec notamment ces fonctionnalités supplémentaires :

- Mises à jour automatiques des signatures WildFire toutes les 15 minutes pour tous les nouveaux logiciels malveillants détectés partout dans le monde.
- Prise en charge améliorée des types de fichiers, y compris : fichiers PE (EXE, DLL et autres), tous les types de fichiers Microsoft Office, fichiers Portable Document Format (PDF), applets Java (JAR et CLASS), packages APK Android, applets Adobe Flash (SWF et SWC) et pages Web.
- Prise en charge du WF-500.
- API WildFire pour la soumission par programme de jusqu'à 1 000 échantillons par jour et jusqu'à 10 000 requêtes de rapport par jour.

WF-500

Le WF-500 est une solution matérielle en option destinée aux clients qui choisissent de déployer WildFire en tant que cloud privé pour une confidentialité renforcée des données. Le WF-500 est dimensionné pour prendre en charge la plupart des réseaux de moyenne ou grande taille, avec la possibilité de déployer des appareils supplémentaires à mesure que les volumes de trafic augmentent ou pour les réseaux nécessitant une distribution géographique.

Caractéristiques techniques du WF-500

PROCESSEUR

- Processeur Intel Dual Core à 6 cœurs avec Hyper-Threading

MÉMOIRE

- 128 Go de RAM

DISQUE SYSTÈME

- SSD 120 Go

Caractéristiques matérielles

ENTRÉE/SORTIE

- 10/100/1 000 x 4
- Port série console DB9, USB

CAPACITÉ DE STOCKAGE

- RAID1 2 To : disque dur certifié RAID 1 To x 4 pour 2 To de stockage RAID

ALIMENTATION

- Alimentation double 920 W dans une configuration redondante échangeable à chaud

CONSOMMATION ÉLECTRIQUE MAXIMALE

- 510 Watts

EN RACK (DIMENSIONS)

- 2U, rack standard 19″ (8,89 cm (H) x 53,34 cm (P) x 44,45 cm (L))

BTU/H MAX.

- 1 740 BTU/h

TENSION D'ENTRÉE (FRÉQUENCE D'ENTRÉE)

- 100-240VCA (50-60Hz)

CONSOMMATION DE COURANT MAX.

- 11 A à 100 VCA

SÉCURITÉ

- UL, CSA, CB

EMI (POTENTIEL D'INTERFÉRENCE ÉLECTROMAGNÉTIQUE)

- FCC classe A, CE classe A, VCCI classe A

ENVIRONNEMENT

- Température de fonctionnement : 32 à 95 °F, 5 à 35 °C
- Température de non fonctionnement : -4 à 158 °F, -40 à 65 °C

Pour obtenir des informations supplémentaires sur les fonctions de sécurité du WF-500 et les capacités associées, visitez **www.paloaltonetworks.com/products**

paloalto networks
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054
Téléphone principal : +1.408.753.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087
www.paloaltonetworks.com

Copyright ©2014, Palo Alto Networks, Inc. Tous droits réservés. Palo Alto Networks, le logo Palo Alto Networks, PAN-OS, App-ID et Panorama sont des marques de fabrique de Palo Alto Networks, Inc. Les caractéristiques décrites dans ce document peuvent être modifiées sans préavis. Palo Alto Networks décline toute responsabilité quant aux éventuelles inexactitudes ou obligations de mise à jour du présent document. Palo Alto Networks se réserve le droit de changer, modifier, transférer ou réviser cette publication sans préavis. **PAN_DS_WF_101414**