WildFire

Supprimer les risques liés aux malwares hautement évasifs

Chaque seconde compte : raisons de l'échec de l'analyse et du sandboxing traditionnels des malwares

Les adversaires d'aujourd'hui disposent d'un accès facile à l'infrastructure cloud légitime, ainsi qu'au machine learning pour distribuer rapidement des fichiers malveillants évasifs aux utilisateurs finaux. Les outils de sécurité cloisonnés ne peuvent tout simplement pas tenir le rythme des malwares actuels, qui prolifèrent à la vitesse de 1 000 nouvelles menaces toutes les cinq minutes, avec jusqu'à 10 000 variantes constatées au cours des cinq minutes suivantes.

Avantages pour l'entreprise

Ne soyez pas la première victime d'une toute nouvelle menace. La nouvelle prévention en ligne stoppe les menaces encore inconnues dans les types de fichiers courants sur le pare-feu nouvelle génération basé sur le machine learning, sans affecter la productivité.

Éliminez le risque généré par les temps d'arrêt. Réduisez le délai de réaction à une menace, initialement de quelques heures ou minutes, désormais à quelques secondes, grâce à l'exécution automatisée d'une protection coordonnée sur le réseau, le terminal et le cloud.

Réduisez les évènements exploitables et la charge de travail sur les opérations de sécurité. Les fonctionnalités de prévention en ligne sur le pare-feu nouvelle génération basé sur le ML arrêtent la menace initiale, fournissant moins d'évènements de détection sur lesquels enquêter et à contenir.

Réduisez le coût total de possession grâce à l'architecture basée sur le cloud. Supprimez les coûts de déploiement, de gestion, de correctifs et de maintenance des sandbox basées sur les appareils.

Gagnez une capacité d'analyse infinie sans aucun coût supplémentaire. Notre modèle de services assure le calcul et l'évolutivité dont vous avez besoin sans aucune charge basée sur la capacité.

Évitez les intégrations manuelles. Chaque renseignement créé est automatiquement réinvesti dans l'écosystème Palo Alto Networks, supprimant l'outillage ou l'intégration manuel(le).

Les organisations souffrant d'attaques de type « zero-day » ou de menaces persistantes avancées causant des brèches de données peuvent avoir à surmonter les obstacles suivants :

- **Risque de réputation**—Grande visibilité dans les médias et la presse créée par les exigences gouvernementales et industrielles en matière de rapports, aggravée par le volume et le type d'informations perdues.
- **Risque réglementaire**—Sanctions imposées par les organismes directeurs et exigences accrues en matière de conformité et d'évaluation, selon les actifs informationnels ciblés (par ex. renseignements nominatifs, informations de compte, propriété intellectuelle client ou professionnel).
- **Risque financier**—Perte de revenus potentielle associée à une baisse de confiance des acheteurs, ransomwares et réglementations accrues (par ex. temps d'arrêt, réduction des ventes, augmentation des exigences de conformité, coût de récupération des données).
- **Risque légal**—Responsabilité suite à des difficultés civiles et problèmes de diligence résultant de la perte de données client et de la conformité aux réglementations (par ex., HIPAA, RGPD, législation des États-Unis [CCPA, réglementation sur la cybersécurité du NYDFS, etc.], réglementation australienne de confidentialité des données).

Pour atténuer les risques associés aux attaques évasives, les organisations se tournent vers les solutions de sandboxing en réseau pour l'analyse des malwares. Malheureusement, toutes ces solutions traditionnelles affectent la productivité de l'utilisateur et fournissent lentement les verdicts, interrompant les processus en détenant des fichiers pour les analyser, faisant fuiter du contenu pendant l'analyse ou modifiant le contenu et rendant de nombreux fichiers impossibles à lire. Par ailleurs, ces solutions présentent une autre faille fatale : elles peuvent protéger contre les nouvelles menaces uniquement une fois que la première victime d'une organisation (le patient zéro) a déjà été identifiée ou compromise.

Prévention immédiate exécutée par une analyse cloud évolutive à l'infini

Le service de prévention des malwares WildFire® de Palo Alto Networks supprime la nécessité de faire un compromis sur la sécurité au profit de la performance et permet enfin aux organisations d'adopter une position donnant la priorité à la prévention. Moteur de prévention et d'analyse dans le cloud des malwares le plus sophistiqué du secteur, WildFire analyse chaque fichier inconnu à la recherche d'une intention malveillante, puis assure la prévention en un temps record afin de réduire le risque qu'une première victime apparaisse, et de chaque menace qui s'ensuit.

Contrairement aux solutions traditionnelles qui dépendent uniquement d'une analyse hors ligne ou retardée d'un malware inconnu, l'analyse et les informations de WildFire sont directement envoyées aux modèles de machine learning qui agissent localement, au niveau du pare-feu, pour stopper jusqu'à 95 % des nouvelles menaces en ligne. Pour le reste, WildFire utilise une approche multitechnique novatrice afin de distribuer des signatures à chaque pare-feu nouvelle génération en quelques secondes.

Aucun autre moteur d'analyse des malwares ne peut offrir des services de prévention sans affecter la productivité. WildFire combine des analyses statiques et dynamiques, des techniques novatrices de machine learning, une analyse récursive et un environnement d'analyse sur mesure révolutionnaire pour analyser, identifier et prévenir même les menaces les plus évasives et sophistiquées possible. Après l'analyse, WildFire prend toute sa mesure lors de l'automatisation : il applique une prévention rapide et cohérente en périphérie, dans votre data center, depuis le cloud, au sein des applications de type software-as-a-service (logiciel en tant que service - SaaS), et au niveau des terminaux.

Principales fonctionnalités

Empêcher les menaces inconnues au niveau du pare-feu grâce au machine learning en ligne

Alimenté par les modèles de menaces rectifiés en permanence dans le cloud, WildFire comprend un moteur de machine learning en ligne exécuté au sein de nos pare-feu nouvelle génération basés sur le ML matériels et virtuels. Cette fonctionnalité novatrice sans signature empêche la présence de contenu malveillant dans les types de fichiers courants, comme les fichiers portables exécutables et les attaques sans fichier émanant de PowerShell®, le tout totalement en ligne, sans nécessiter d'analyse cloud, sans endommager le contenu et sans aucune perte de productivité pour l'utilisateur. Qu'un fichier inconnu corresponde à une signature existante ou soit classé par un pare-feu nouvelle génération basé sur le ML, WildFire réalise toujours une analyse complète, extrayant des informations et des données précieuses afin de fournir du contexte aux analystes de la sécurité, de générer des mises à jour de formation pour les modèles de machine learning et de partager des informations sans aucun abonnement afin d'éviter d'autres vecteurs d'attaque.

Bénéficier d'une prévention internationale via l'écosystème WildFire, fournie en quelques secondes

Face aux menaces hautement personnalisées que sa prévention basée sur le machine learning ne peut pas stopper, WildFire applique une puissante analyse basée sur le cloud pour assurer la prévention sur les réseaux, les infrastructures cloud, les terminaux et où que soient déployés les capteurs activés par WildFire. Travaillant en

tandem avec les nouvelles fonctionnalités de PAN-OS®, WildFire génère et assure une prévention globale en quelques secondes via une analyse initiale pour la plupart des nouvelles menaces. Cette exécution novatrice dans le cloud de signatures résistant à l'évasion ferme la fenêtre au déploiement réussi de contenu malveillant par les adversaires.

Utiliser des signatures, non des empreintes

WildFire n'utilisant pas des empreintes, mais des signatures de contenu pour la prévention, il peut identifier davantage de malwares avec une seule signature. Par conséquent, par rapport aux systèmes principalement basés sur les empreintes qui nécessitent des rapports de 1:1, WildFire protège contre davantage d'attaques avec les mêmes ressources. Une seule signature WildFire peut protéger contre jusqu'à plusieurs millions de variantes polymorphiques d'un même malware.

Éradiquer le comportement malveillant dans l'intégralité du trafic

WildFire identifie les fichiers présentant des comportements malveillants potentiels, puis délivre des verdicts basés sur leurs actions en appliquant la threat intelligence, les analyses et la corrélation, en même temps que des fonctionnalités avancées :

- **La visibilité totale sur le comportement malveillant** identifie les menaces dans l'intégralité du trafic sur des centaines d'applications, y compris le trafic Web ; les protocoles de messagerie, comme SMTP, IMAP et POP ; et les protocoles de partage de fichiers, comme SMB et FTP, quels que soient les ports ou le chiffrement.
- **L'analyse d'un trafic réseau suspect** surveille toute l'activité réseau produite par un fichier suspect, y compris la création de portes dérobées, le téléchargement de malwares subséquents, la visite de domaines peu fréquentables, la reconnaissance de réseau, etc.
- **La détection d'attaques sans fichier/de scripts** identifie à quel moment des scripts potentiellement malveillants, comme JScript et PowerShell, traversent le réseau et les transfère à WildFire pour une analyse et une exécution.

Les puissantes fonctionnalités de découverte et d'analyse de WildFire sont intégrées de manière homogène dans de nombreux produits de la gamme Palo Alto Networks, ainsi que dans les solutions de pointe de partenaires sur des plateformes de messagerie et cloud.

Découvrir de nouvelles menaces avec une approche multitechnique résistante à l'évasion

WildFire va au-delà des approches traditionnelles de sandboxing utilisées pour détecter des menaces inconnues dans un environnement d'analyse sur le cloud, en combinant plusieurs techniques :

- **L'analyse dynamique** observe l'exécution des fichiers dans un environnement virtuel résistant à l'évasion et spécifiquement conçu, afin de permettre la détection de malwares jusqu'alors inconnus grâce à des centaines de caractéristiques comportementales.
- **Le machine learning** extrait des milliers de caractéristiques uniques de chaque fichier, formant un modèle de machine learning prédictif afin d'identifier de nouveaux malwares, ce qui n'est pas possible uniquement avec une analyse statique ou dynamique.
- **L'analyse statique** complète l'analyse dynamique avec une détection efficace des malwares, fournissant une identification instantanée de leurs variantes. L'analyse statique tire davantage parti de la décompression dynamique pour analyser les menaces tentant d'échapper à la détection grâce à l'utilisation d'un ensemble d'outils de compression.

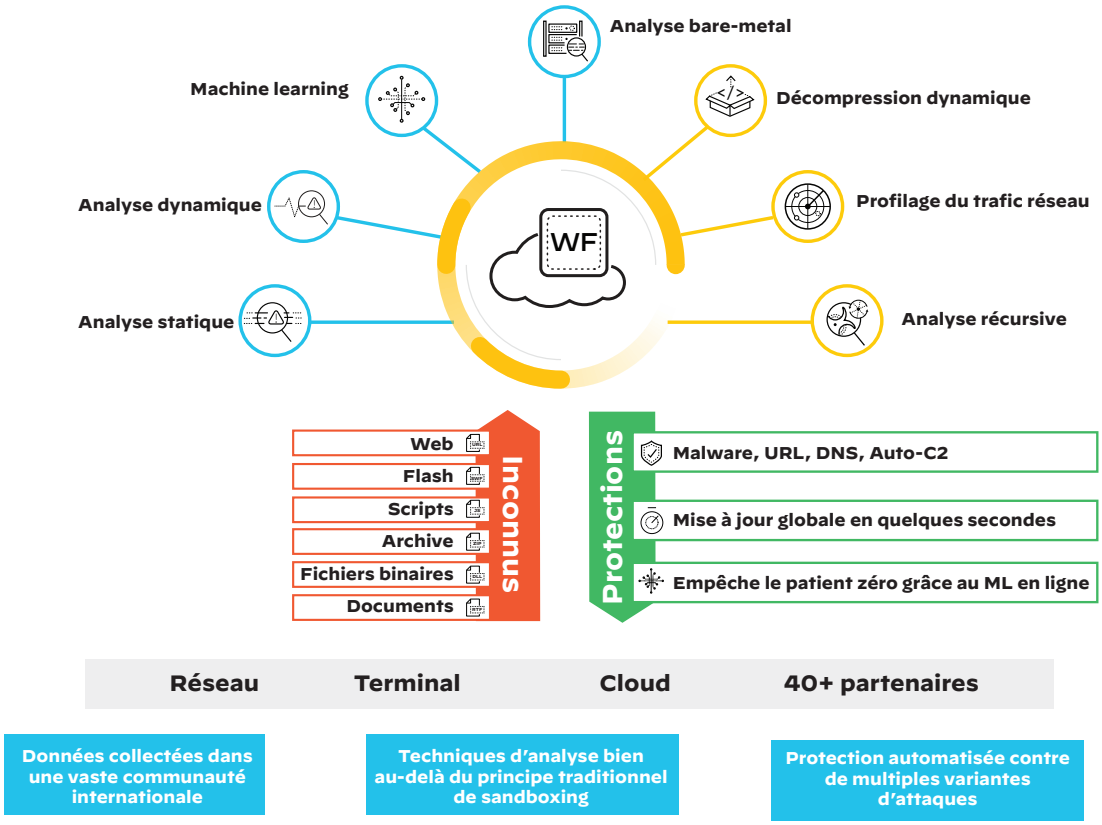

Figure 1 : WildFire : le centre nerveux global pour l'analyse des malwares

- **L'analyse bare-metal** exécute des menaces évasives dans un environnement matériel réel au sein duquel toute possibilité de déploiement de techniques d'analyse anti-VM par des adversaires est bloquée.
- **Un hyperviseur sur mesure** empêche les techniques d'évasion des pirates grâce à un hyperviseur propriétaire robuste qui ne dépend pas de projets en open source ou d'un logiciel propriétaire auxquels les pirates peuvent accéder.

Ensemble, ces techniques uniques permettent à WildFire d'analyser et de bloquer les malwares avec une grande efficacité et un taux de faux positifs proche de zéro.

Stopper les attaques complexes en plusieurs étapes

Les pirates informatiques continuent de faire évoluer les malwares afin qu'ils échappent aux techniques d'analyse existantes et ce, en divisant les attaques en composants et étapes distincts à l'aide de vecteurs d'exécutions simultanées multiples et en exploitant des services cloud fiables pour éviter d'être détectés. Ces stratégies rendent inutiles l'analyse traditionnelle de malwares à simple vecteur et en une seule étape.

En combinant la portée sur le cloud de WildFire avec l'analyse avancée de fichiers et l'indexation URL, l'analyse récursive multivectorielle (Multi-Vector Recursive Analysis (MVRA)) offre une solution unique et complète pour empêcher les attaques sophistiquées en plusieurs sauts et étapes des acteurs malveillants. Contrairement à d'autres solutions, WildFire peut suivre les multiples étapes d'une attaque depuis l'angle de l'analyse d'un fichier, même si l'exécution échoue lors d'une étape spécifique. Ce processus unifie les analyses dans les vecteurs d'attaque sur le Web et via un fichier, ce qui permet une vision holistique et unique d'une campagne en plusieurs étapes. Les attaquants ne peuvent plus masquer leur contenu malveillant derrière plusieurs étapes d'URL bénignes ou derrière des sites fiables de partage de documents.

Avantages opérationnels

- **Automatisation de la reprogrammation des contrôles de sécurité afin de bloquer les menaces inconnues :** les renseignements partagés en temps réel par plus de 35 000 abonnés sont automatiquement mis à jour et empêchent les menaces sur les réseaux, les terminaux et dans les infrastructures cloud.
- **Mise à disposition d'un contexte détaillé quant aux menaces analysées :** obtenez des rapports minutieux de chaque fichier malveillant envoyé à WildFire dans de multiples environnements de systèmes d'exploitation et versions d'applications.
- **Intégration homogène avec les outils de sécurité existants :** tirez parti de l'intégration d'une API ouverte avec SIEM, TIP, un système de tickets, SOAR ou des outils XDR afin de traiter les indicateurs de compromission.
- **Mise à profit de la threat intellignence concrète :** avec la threat intelligence contextuelle AutoFocus™, vous pouvez tcampagnes pour vous assurer que votre prochaine action est appropriée.

Déploiemtent dans une architecture cloud évolutive et sûre

L'architecture cloud de WildFire prend en charge l'analyse et la prévention de menaces inconnues à grande échelle sur les réseaux, les terminaux et les infrastructures cloud. Les fichiers sont soumis au cloud international WildFire, offrant grande portée et rapidité, et tout client de Palo Alto Networks peut rapidement activer le service, y compris les utilisateurs des pare-feu nouvelle génération virtuels et matériels basés sur le ML, des offres cloud publiques, des SaaS Prisma™ et des agents Cortex XDR™. Palo Alto Networks gère directement l'infrastructure WildFire, dans le respect des bonnes pratiques standard de l'industrie en matière de sécurité et de confidentialité, avec des audits réguliers de conformité à la norme SOC 2. Consultez la fiche technique de confidentialité de WildFire pour en savoir plus.

Afin que vous puissiez mieux gérer la souveraineté des données et les questions de confidentialité, nous conservons des infrastructures cloud WildFire régionales qui vous offrent davantage de contrôle sur l'emplacement de vos données. Fournissant les mêmes fonctionnalités de détection et de prévention que le cloud public WildFire, ces infrastructures cloud vous permettent d'ajuster les soumissions de manière à satisfaire aux questions de confidentialité des données localisées.

Journalisation, création de rapports et analyse détaillée intégrées

Les utilisateurs de WildFire reçoivent des journaux intégrés, des analyses et une visibilité sur les évènements malveillants via l'interface de gestion PAN-OS, la gestion de la sécurité du réseau Panorama™, AutoFocus, Cortex XDR, Cortex™ XSOAR, ou le portail WildFire, ce qui permet aux équipes d'enquêter rapidement et de mettre en relation des évènements observés dans leurs réseaux. Avec ces informations, les équipes de sécurité peuvent rapidement localiser et prendre des mesures concernant les données requises, pour des enquêtes et des réactions aux incidents rapides quelle que soit l'application utilisée.

La puissance des services de sécurité Palo Alto Networks

Le nombre et le degré de sophistication des cyberattaques ont augmenté. En effet, les attaquants utilisent désormais des techniques avancées pour contourner les équipements et les outils de sécurité réseau. Les organisations doivent donc trouver un moyen de protéger leurs réseaux sans alourdir la charge de travail de leurs équipes de sécurité ni impacter leur productivité. Parfaitement intégrés à la toute première plateforme de pare-feu nouvelle génération basée sur le machine learning, nos services de sécurité cloud coordonnent les renseignements et offrent une protection contre tous les vecteurs d'attaques grâce des fonctionnalités hors pair, tout en éliminant les failles de sécurité réseau créées par un trop grand nombre d'outils distincts. Profitez des meilleures fonctionnalités sur le marché sur une plateforme cohérente et protégez votre organisation des menaces les plus avancées et évasives. Tirez parti de WildFire ou de n'importe lequel de nos services de sécurité :

- **Threat Prevention :** oubliez les systèmes de prévention des intrusions (IPS) traditionnels pour désormais prévenir automatiquement toutes les menaces connues sur l'ensemble de votre trafic en une seule passe.
- **URL Filtering :** permettez l'utilisation sûre d'Internet en empêchant l'accès aux sites Web malveillants connus et inconnus avant que les utilisateurs ne puissent les consulter.
- **DNS Security :** contrez les attaques DNS visant à exfiltrer des données ou à prendre les commandes et le contrôle, sans modifier votre infrastructure.
- **IoT Security :** protégez les appareils IoT (Internet des objets) et OT dans l'ensemble de votre organisation grâce à la première solution de sécurité IoT clé en main sur le marché.
- **Sécurité réseau GlobalProtect™** pour les terminaux : étendez les fonctionnalités du pare-feu nouvelle génération basé sur le machine learning à vos utilisateurs distants pour une sécurité homogène dans tout votre environnement.

Tableau 1 : récapitulatif des caractéristiques et des licences	
Fonctionnalités activées avec l'abonnement WildFire	
Techniques avancées d'analyse, de prévention et anti-évasion	**Analyse statique**—Combine l'analyse de la mémoire, le machine learning et l'analyse des anomalies d'un fichier, des modèles malveillants et du code malveillant connu. **Prévention en ligne basée sur le ML (sur le pare-feu)** — Bloque les exécutables malveillants inconnus et les attaques PowerShell. **Analyse dynamique**—Inclut l'hyperviseur personnalisé, le score du comportement, le profilage du réseau et l'analyse multiversion. **MVRA**—Combine une analyse avancée des fichiers et une indexation des URL afin d'empêcher les attaques en plusieurs sauts et étapes. **Analyse bare metal**—Permet une analyse dynamique complète sur du matériel réel, sans environnement virtuel ni hyperviseur.
Systèmes d'exploitation pris en charge	macOS, Android, Windows XP/7/10
Fichiers pris en charge	Fichiers PE (EXE, DLL et autres), tous les types de fichiers Microsoft Office, fichiers Mac OS X, fichiers Linux (ELF), fichiers Android Package Kit (APK), fichiers Adobe Flash et PDF, fichiers d'archive (RAR et 7-Zip), fichiers de script (BAT, JS, VBS, PS1, Shell script et HTA), analyse des liens dans les e-mails et fichiers chiffrés (TLS/SSL).
Protocoles pris en charge	SMTP, POP3, SMB, FTP, IMAP, HTTP, HTTPS
Analyse de fichiers par jour	Élastique
Type de signature	• Basé sur les nouveaux malwares ou de type « zero day » découverts dans le trafic Web (HTTP/HTTPS), les protocoles de messagerie (SMTP, IMAP et POP) et le trafic FTP. • Généré sur la charge utile du malware de l'échantillon et testé en termes de précision et de sécurité
Mises à jour de la protection pour les malwares	• Quelques secondes, avec les signatures sans retard au pare-feu nouvelle génération connecté.*
Emplacements régionaux du cloud	• Amérique du Nord (2 ; international et régional), Amsterdam, Singapour et Japon.
Intégrations principales	• Avec Palo Alto Networks, y compris tous les services de sécurité via le cloud, AutoFocus, Cortex XDR et Prisma SaaS. • Avec les partenaires technologiques pour la détermination du verdict sur des services tiers dans l'API WildFire.
Gestion et création de rapports	Palo Alto Networks Panorama et interface utilisateur Web, API
Analyse détaillée	• 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 et le réseau. • Un accès à l'échantillon du malware d'origine à des fins d'ingénierie inverse, avec les PCAP complets des sessions d'analyse dynamique. • API ouverte pour l'intégration avec des outils de sécurité tiers, comme les systèmes de gestion des informations et des évènements de sécurité (SIEM).
Confiance et confidentialité	• Palo Alto Networks a mis en place des contrôles stricts en matière de confidentialité et de sécurité pour bloquer l'accès non autorisé aux informations sensibles ou identifiables. Nous appliquons les bonnes pratiques du secteur à des fins de sécurité et de confidentialité. Pour plus d'informations, consultez nos fiches techniques de confidentialité des données.

Tableau 1 : récapitulatif des caractéristiques et des licences (suite)	
Licences et exigences	
Exigences	Pour utiliser les services WildFire de Palo Alto Networks, les éléments suivants sont requis : • Pare-feu nouvelle génération de Palo Alto Networks exécutant PAN-OS • Une licence Prévention des menaces Palo Alto Networks
Licence WildFire complète	WildFire nécessite une licence spécifique, sous forme de service cloud intégré pour les pare-feu nouvelle génération Palo Alto Networks. La licence fait également partie des services Palo Alto Networks ELA, VM-Series ELA et Prisma Access.
Environnement recommandé	Des pare-feu nouvelle génération Palo Alto Networks déployés n'importe où, en tant que sources internes et externes, peuvent introduire dans le réseau des menaces basées sur des fichiers.
Licence WildFire basique	La fonctionnalité WildFire basique est incluse dans le pare-feu nouvelle génération Palo Alto Networks avec un ensemble limité de caractéristiques et permet uniquement les actions suivantes : • le transfert de fichiers de type EXE et DLL, y compris des contenus compressés et chiffrés (Windows XP/7 uniquement) pour l'analyse WildFire ; • la récupération de signatures WildFire via les mises à jour des antivirus et/ou de la prévention des menaces ; • les mises à jour automatiques toutes les 24–48 heures, selon les services de prévention des menaces actifs (prévention en ligne basée sur le machine learning et signatures sans retard non pris en charge).

* Nécessite PAN-OS 10.0.

paloalto NETWORKS

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

+31 20 888 1883

www.paloaltonetworks.com