

COMBLER LA BRÈCHE DANS LA DÉTECTION DES MALWARES ET DES ATTAQUES CIBLÉES

BOUSCULER ET DÉPASSER LES LIMITES DES
PROCESSUS DE DÉTECTION TRADITIONNELS



Adaptive Defense 360 : Résumé

L'approche novatrice d'Adaptive Defense 360 marque une rupture avec le « processus de prévention » qui prévaut depuis toujours dans le domaine de la sécurité en général et celui des logiciels de sécurité en particulier. Dans le cadre de ce processus, entreprises de sécurité et créateurs de logiciels malveillants se livrent à une course pour arracher un avantage temporaire, une « fenêtre de détection » qui sera ensuite refermée par de nouvelles techniques de dissimulation. Les investissements et les ressources mobilisés pour simplement maintenir une apparence de « stabilisation de ce front » augmentent jour après jour.

La nouvelle approche, basée sur la confiance, repose sur trois principes : la surveillance constante du comportement de tous les programmes s'exécutant sur les postes clients ; une classification et une évaluation des risques en

temps réel ou quasi temps réel grâce à un processus Big Data associé au besoin à une expertise par des analystes, et enfin une transparence/commodité maximale, afin qu'aucune intervention d'un utilisateur final ou d'un administrateur ne soit nécessaire pour faire fonctionner le service.

Même si la protection absolue n'existe pas, cette nouvelle approche complique grandement la tâche des logiciels malveillants qui chercheraient à demeurer invisibles et à percer des défenses de sécurité existantes. Cependant, comme de nouveaux incidents surviendront inévitablement, Adaptive Defense 360 offre aussi les capacités d'analyse a posteriori nécessaires pour y répondre, afin de déterminer quand le logiciel malveillant a infiltré le système, qui a été affecté, ce qui était ciblé et comment le logiciel malveillant est parvenu jusque-là.



Introduction

Malgré des investissements en sécurité sans cesse croissants (selon Gartner, les entreprises ont dépensé en 2013 plus de 13 milliards de dollars en firewalls, systèmes de prévention d'intrusions, plates-formes de protection des postes clients et passerelles Web sécurisées), il est clair que la bataille contre les logiciels malveillants est loin d'être gagnée.

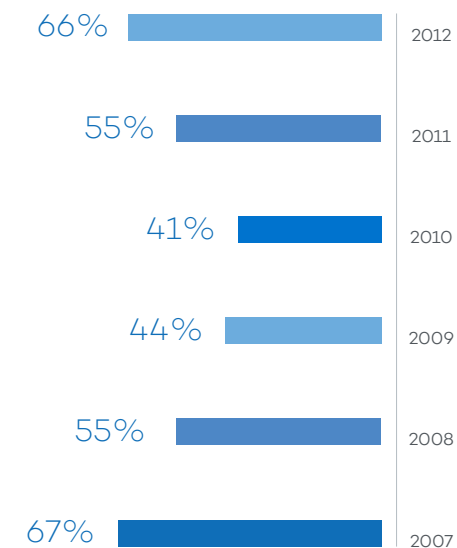
Bien au contraire, des violations de données très médiatisées et surtout des révélations particulièrement marquantes sur les activités d'espionnage d'état ont continué d'entretenir la perception d'un risque général très élevé et de réseaux perméables et impossibles à défendre.

Comme le déclare Gartner, « toutes les entreprises devraient maintenant assumer qu'elles sont dans un état de risque permanent ». Selon le Rapport d'enquête de Verizon sur les compromissions de données, 85 % des attaques n'ont été détectées qu'au bout de plusieurs semaines, et 92 % des attaques n'ont pas été détectées par les entreprises elles-mêmes. Il est très vraisemblable que le risque global soit resté aux mêmes niveaux que par le passé.

Comme l'avait déclaré l'ancien secrétaire à la Défense américain Donald Rumsfeld, « il y a des choses dont nous ne savons pas que nous ne les savons pas ».



Pourcentage de violations qui demeurent non découvertes pendant des mois



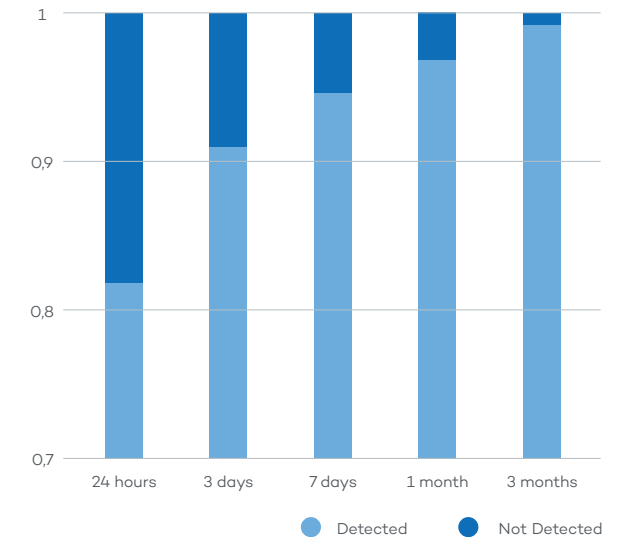
Source : Rapport d'enquête 2013 de Verizon sur les compromissions de données.

Les lacunes de la détection

Dans le cadre d'une étude interne menée par PandaLabs entre les mois de janvier et de juin 2013, tous les échantillons de logiciels malveillants recueillis quotidiennement ont été testés avec un grand nombre de produits antimalware. Un pourcentage relativement élevé de logiciels malveillants diffusés ne sont pas interceptés à temps. En fait, même un an après l'apparition d'un logiciel malveillant, près de 1 % des échantillons n'étaient toujours pas détectés (ce qui représente plus de 70 000 échantillons). Ces résultats montrent les lacunes qui persistent dans les produits focalisés sur la détection.



Logiciels malveillants non détectés par les éditeurs d'antivirus

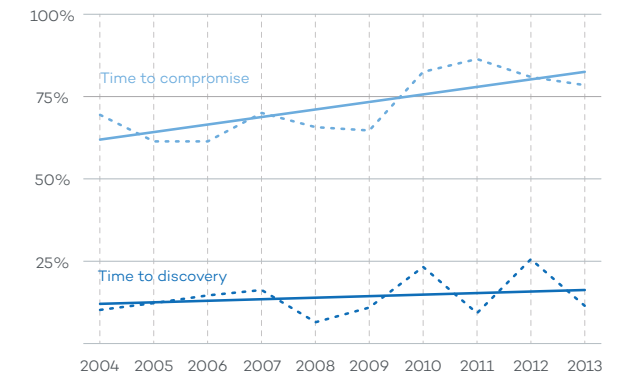


Graphique. Retard de détection des produits antimalware.



Rapport d'enquête 2014 de Verizon sur les compromissions de données. Les pirates améliorent leurs techniques de compromission des systèmes plus rapidement que les éditeurs de logiciels de sécurité ne sont capables de découvrir les compromissions.

Pourcentage de violations pour lesquelles le délai de compromission / délai de découverte n'a pas dépassé quelques jours



Qu'est-ce qu'Adaptive Defense 360 ?

Adaptive Defense 360 est une solution de sécurité capable de valider 100 % des applications qui s'exécutent au sein d'une entreprise. Elle se compose d'un agent ultra-léger installé sur le poste client et une infrastructure basée sur le Cloud, avec une assistance permanente de la part des analystes de PandaLabs.

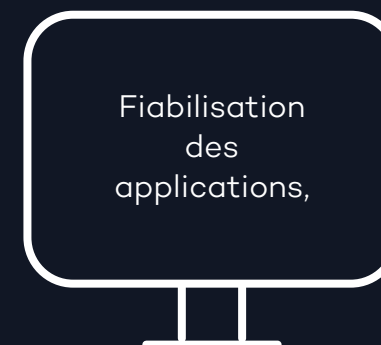
Adaptive Defense 360 classe de façon transparente tous les programmes exécutables (fichiers PE) qui s'exécutent sur le poste client, avec une précision garantie proche de 100 % (99,999 %). Il fiabilise aussi les applications, les données et le système d'exploitation (définition de comportement) afin de garantir que les applications les plus courantes ne seront pas exploitées du fait de vulnérabilités existantes et que les zones sensibles du système d'exploitation ne seront pas utilisées de façon anormale.

Il offre également une traçabilité en cas d'incident (afin de répondre aux questions quoi, quand, qui et comment relativement aux attaques).

Adaptive Defense 360 est capable de bloquer du code exécutable avant qu'il ne soit autorisé à s'exécuter, ou juste après (mode étendu-mode de blocage de base). Adaptive Defense peut aussi nettoyer automatiquement les infections en cas d'incident, en fonction de l'ensemble de services acheté par le client.



**ANALYSES CONTINUES
BASÉES SUR LE CLOUD**



**SURVEILLANCE CONSTANTE
DES POSTES CLIENTS**



Principes : Adaptive Defense 360 repose sur 3 principes

Surveillance constante

Tous les événements d'exécution sont enregistrés et classifiés à des fins d'avertissement préalable, de traçabilité et d'analyse postérieure. Tous les journaux d'événements sont accessibles à l'administrateur. Les recherches y sont également possibles, ce qui permet de savoir facilement comment se comportent exactement les applications, comment elles sont utilisées, par qui, quelles connexions sont établies, avec quels pays, quand, etc.

Classification continue des exécutables en cours de fonctionnement

Tous les exécutables fonctionnant en mémoire sont classifiés avec une précision garantie proche de 100 %, à l'aide de systèmes locaux et basés sur le Cloud corrélés avec des données collectées localement, mais aussi avec d'autres données contextuelles, des systèmes tiers et notre moteur d'analyse Big Data. Une classification assistée par un intervenant humain a aussi lieu dans des cas exceptionnels, particulièrement pendant la phase de déploiement initial.

Les programmes doivent en outre se comporter de manière à conserver leur niveau de confiance. Les calculs de probabilités pour déterminer le niveau de confiance reposent sur une technologie de regroupement propriétaire ainsi que sur les données empiriques et historiques de tous les fichiers (malveillants et non malveillants) déjà consultés et classifiés par Panda. Les probabilités sont continuellement recalculées à mesure de l'arrivée de nouvelles informations, et une analyse rétrospective de toutes les classifications précédentes a également lieu.

Transparence/Commodité

Aucune intervention manuelle de l'administrateur ou de l'utilisateur final (création de listes blanches, configuration de paramètres, etc.) n'est nécessaire pour faire fonctionner le service Adaptive Defense 360.

Une fois déployé, l'agent détectera, analysera et classifiera les fichiers exécutables de lui-même et en coordination avec le système sur le Cloud. Étant donné qu'Adaptive Defense est un service géré proposé par Panda et non un produit autonome, il élimine les tâches récurrentes que

les administrateurs doivent effectuer lors de l'utilisation d'autres solutions de sécurité contre des menaces évoluées, comme la priorisation et la gestion des alertes d'activité suspecte produites par la surveillance d'indicateurs de compromission. Adaptive Defense 360 ne produit pas ce genre d'alertes. Toutes les alertes indiquent la présence d'un logiciel malveillant avéré, et les suspicions sont entièrement prises en charge par le service d'une manière transparente pour les administrateurs.

Adaptive Defense 360 évite aussi d'avoir à utiliser des applications de listes blanches et à définir des processus d'exception et d'approbation, car tous les exécutables qui tentent de s'exécuter sont classifiés par le système.

...et toutes les capacités d'une solution EPP

Adaptive Defense 360 intègre Panda Endpoint Protection Plus, la solution EPP la plus complète de Panda avec une surveillance et des rapports de sécurité en temps réel, des outils correctifs et curatifs, une protection par profil d'utilisateur, le contrôle centralisé des appareils mobiles connectés, la surveillance et le filtrage Web.

Principaux avantages

Comment Adaptive Defense 360 aide les entreprises à résoudre le problème d'une protection inadéquate.

01

Élimine le retard de détection présenté par les produits traditionnels de protection des postes clients.

02

Réduction drastique du temps passé en investigations lors d'incidents de sécurité. Toutes les alertes émises par Adaptive Defense sont déjà confirmées.

03

Réduit au maximum les coûts de résolution en cas d'incident. Désinfection automatisée.

04

Répond aux questions auxquelles un produit traditionnel n'est pas en mesure de répondre : le quoi, le qui, le quand et le comment des incidents de sécurité.

05

Réduit les coûts de gestion de la sécurité des postes clients.

Avantages supplémentaires d'Adaptive Defense 360.



Offre une visibilité en temps réel de toute l'activité du poste client, en permettant aux administrateurs d'intercepter facilement les événements « à risque » ou les violations des règles.



Requiert beaucoup moins d'attention que les autres produits de protection des postes clients.



Ne nécessite pas d'infrastructure de gestion.



N'impose pas de désinstaller les défenses de sécurité existantes.



Protection à hautes performances pour les environnements de bureau virtualisés

Technologie

Sources d'informations d'Adaptive Defense 360 :

- Menaces - Externes.
- Ensemble des utilisateurs.
- Menaces - Internes (PandaLabs).
- Informations de vulnérabilités.
- Contexte.
- Référentiel de logiciels.

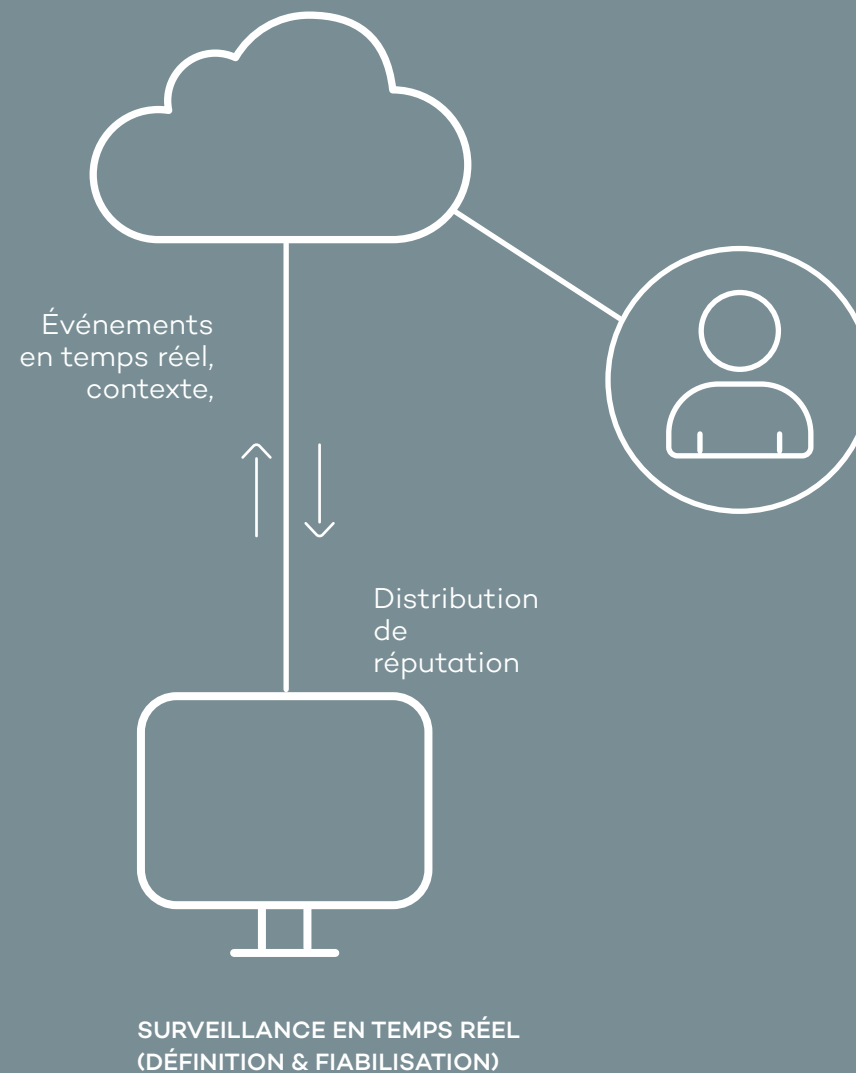
Surveillance en temps réel des événements sur les postes clients :

- Processus, services, PE.
- Communications.
- Registre.
- Téléchargements.
- Connexions.
- etc.

Fonctions d'administration :

- Alertes de logiciels malveillants.
- Rapports d'analyse post-incident.
- Recherche d'événement.

SYSTÈME D'ANALYSE & DE CLASSIFICATION BIG DATA



Capacités de détection

Les logiciels malveillants actuels utilisent de nombreuses astuces pour échapper à toute détection par les produits de sécurité. Ils se cachent sous des apparences inoffensives, en n'effectuant pas d'actions manifestes de façon immédiate, mais lentement au fil des jours ou des semaines. C'est pourquoi il devient nécessaire de surveiller constamment toutes les actions de tous les exécutables. La première classification d'un exécutable, à l'issue de sa première exécution, peut ne pas révéler sa nature malveillante. Les logiciels malveillants peuvent attendre de recevoir des instructions ou de rencontrer certaines conditions contextuelles pour commencer à montrer un comportement ou un objectif malveillant. En outre, les programmes légitimes peuvent aussi contenir des vulnérabilités qui peuvent être exploitées et leur faire effectuer des actions malveillantes.

Adaptive Defense 360 surveille tous les événements d'exécution de tous les exécutables. Tout nouveau comportement ou toute anomalie dans le profil d'exécution d'exécutables déjà classifiés déclenche une reclassification, qui prend en compte non seulement les traces comportementales mais aussi les contextes dynamiques et statiques de l'exécutable (processus père, chemin, etc.).

Dans le cadre du service, les clients

reçoivent uniquement des alertes sur les incidents de logiciels malveillants confirmés. Toute activité ou tout exécutable suspect est toujours traité entièrement par Panda avant sa mise hors de cause ou sa confirmation. Cela génère des économies importantes pour les services de sécurité qui doivent habituellement passer au crible un grand nombre d'alertes d'incidents « potentiels »

Capacités de « réponse ».

Lorsqu'un incident de logiciel malveillant est confirmé, une alerte est envoyée à l'administrateur avec toutes les informations fournies par l'analyse, notamment le temps pendant lequel l'exécutable est resté présent dans les systèmes avant d'être classifié comme malveillant, les machines/utilisateurs affectés, les actions de l'exécutable et le moment où elles ont eu lieu, la manière dont il a infiltré le système, les vulnérabilités qui étaient présentes dans les applications fonctionnant sur le poste client, ainsi que les données qui ont été lues lors de l'attaque et le moment où elles ont été lues. Des services de résolution complète des incidents sont également accessibles aux clients sous la forme de services professionnels.

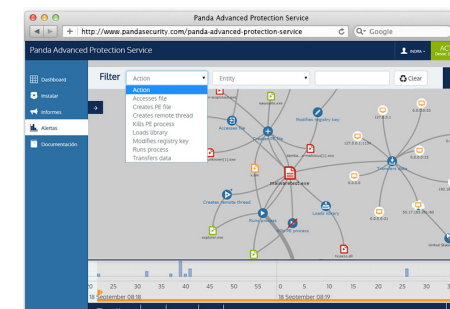
Rapports et alertes.

Des alertes sont envoyées à l'administrateur et sont également

disponibles dans une console Web, avec le rapport d'analyse associé. Pour chaque incident, une représentation visuelle de l'attaque est fournie, qui montre les entités, les communications et les actions effectuées, ainsi que la chronologie des événements.

Recherche avancée.

Toutes les informations d'activités recueillies et traitées par Adaptive Defense 360, pour tous les exécutables, peuvent faire l'objet de recherches et de filtrages ou être représentées graphiquement dans des schémas et des graphiques. La visibilité et la granularité des événements autorisent d'autres scénarios d'utilisation, comme la découverte ou l'identification en temps réel des applications en cours de fonctionnement, les informations d'utilisation (quels programmes sont utilisés, par qui et quand), la géolocalisation des communications, la mauvaise utilisation potentielle des données.



Comment fonctionne Adaptive Defense 360

Prévoir

- Exposition proactive
- Analyse
- Prévoir les attaques
- Systèmes de référence

Empêcher

- Résoudre/
Apporter un
changement
- Concevoir/
Modéliser le
changement
- Rechercher/

**SURVEILLANCE
ET ANALYSE
CONTINUES**

Détecter

- Détecter les incidents
- Confirmer & prioriser le
risque
- Contenir les incidents

Répondre

- Fiabiliser et isoler
les systèmes
- Mettre en échec les agresseurs
- Prévenir les incidents

Comment fonctionne Adaptive Defense 360

Déploiement de l'agent :

Après le choix de la configuration de proxy, l'agent (MSI ou exe) doit idéalement être déployé sur toutes les machines du réseau, si possible au moyen de stratégies Active Directory, bien qu'il puisse être déployé par d'autres moyens avec les permissions d'administration appropriées.

Une fois installé, l'agent Adaptive Defense 360 commence à recueillir des informations générales sur la machine et s'enregistre auprès du service, pour permettre une association unique de la machine avec le client et les événements collectés.

Surveillance des événements et profilage des applications :

Après s'être enregistré, l'agent commence à surveiller l'activité de tous les exécutables en cours de fonctionnement. Les événements collectés incluent : Téléchargements de fichiers, installations de logiciels, URL vers un téléchargement de fichier, modification du fichier hosts, changement de date de fichier, création de pilote, attachement/détachement de fenêtre, communications par processus (IP, ports, protocoles), création de PE, modification, chargement de DLL, création de service, mappage de PE, suppression/renommage de fichier,

création de dossier, création/ouverture d'archive, création/modification de clé du Registre, création de thread sur un processus distant, kill de processus, accès SAM, accès à des données (plus de 200 formats de fichiers), etc.

Tous les exécutables en cours de fonctionnement sont profilés et classifiés. La classification repose sur une base de connaissances constamment remise à jour des logiciels légitimes et des logiciels malveillants, ainsi que sur l'analyse des comportements statiques et dynamiques (comportements observés localement et chez l'ensemble des utilisateurs) et les informations contextuelles de chaque fichier exécutable.

Capacités préventives :

3.1. Les logiciels malveillants connus sont immédiatement bloqués, grâce à l'association de l'agent et de l'intelligence basée sur le Cloud.

3.2. Les applications les plus courantes comme Java, Adobe, Microsoft Office et les navigateurs sont protégées de façon générique contre les attaques basées sur des exploits, grâce à des règles contextuelles et comportementales.

3.3. Les données et certaines zones sensibles du système d'exploitation sont protégées contre les accès non

autorisés de la part d'applications tierces, en autorisant l'accès de la part des applications légitimes profilées et classifiées pendant la phase de déploiement.

Tous les exécutables sont classifiés avec une précision de pratiquement 100 % (99,999). Les exécutables classifiés comme logiciels malveillants sont automatiquement bloqués. Les applications peuvent être bloquées avant ou après leur exécution, selon la stratégie choisie par l'administrateur. Ainsi, avec une stratégie de blocage avant l'exécution (« blocage étendu »), les exécutables non classifiés au moment de l'exécution seront bloqués jusqu'à leur classification. Avec une stratégie de blocage après l'exécution (« blocage de base »), les exécutables non classifiés au moment de l'exécution seront autorisés à s'exécuter jusqu'à leur classification, et ils ne seront bloqués que si leur statut de logiciel malveillant est confirmé. La classification prend habituellement de quelques secondes à quelques minutes allant exceptionnellement jusqu'à quelques heures.

3.4. Les programmes légitimes peuvent aussi être bloqués sur la base d'une liste noire spécifiée par l'administrateur, pour des raisons de productivité ou d'autres raisons.

