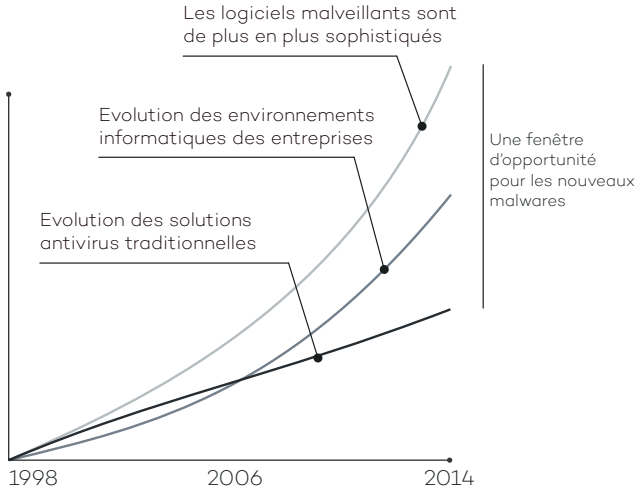
Adaptive Defense
Fermez la porte aux menaces évoluées

ÊTES-VOUS SÛR QUE VOTRE ENTREPRISE EST PROTÉGÉE CONTRE LES NOUVELLES MENACES ET LES ATTAQUES CIBLÉES ?

Le volume et la sophistication des logiciels malveillants et des outils de sécurité informatique ont beaucoup évolué. Le nombre de virus en circulation a connu une croissance exponentielle (près de 200 000 nouveaux virus apparaissent en moyenne chaque jour), et les nouvelles techniques utilisées pour percer les défenses et dissimuler des logiciels malveillants permettent aux menaces de demeurer longtemps dans les réseaux d'entreprise.



Dans le même temps, la complexité grandissante des environnements informatiques les rend plus difficiles à gérer et accroît la vulnérabilité des systèmes.

Les solutions antivirus traditionnelles sont de moins en moins en phase avec la réalité. Leur évolution linéaire continue de privilégier des techniques de détection basées sur des fichiers de signatures et des algorithmes heuristiques. Ces techniques produisent des résultats peu fiables, certains logiciels étant identifiés à tort comme malveillants alors que de véritables logiciels malveillants demeurent ignorés.

Ce défaut a conduit à ce que l'on nomme habituellement la '**fenêtre d'opportunités des logiciels malveillants**', c'est-à-dire le temps qui s'écoule entre l'apparition d'un nouveau virus et la publication de son antidote par les éditeurs de solutions de sécurité. Ce temps de plus en plus long est exploité par les pirates pour introduire des virus, des logiciels de rançon, des chevaux de Troie et d'autres types de logiciels malveillants dans les réseaux des entreprises. Ces menaces, de plus en plus courantes, sont capables de crypter des documents confidentiels puis de réclamer une rançon, ou de recueillir simplement des données sensibles à des fins d'espionnage industriel.

Les administrations, les banques et les autres grandes entreprises subissent désormais de plein fouet des attaques que les antivirus traditionnels ne détectent tout simplement pas à temps. Notre Département de recherche PandaLabs a analysé des millions d'échantillons de virus ainsi que les meilleurs produits antivirus du marché pour constater que 18 % des logiciels malveillants ne sont pas détectés dans les 24 heures qui suivent leur diffusion, et que dans les trois mois qui suivent, 2% des codes malveillants restent indétectés par les solutions traditionnelles.

Une solution existe : il s'agit d' **Adaptive Defense**. Ce service de Panda Security est capable de classifier avec précision chaque application qui s'exécute dans votre entreprise, en autorisant seulement l'exécution des programmes légitimes. Pour parvenir à ce résultat, nous avons travaillé cinq années durant sur un **nouveau modèle de sécurité** reposant sur trois principes : surveillance constante des applications qui fonctionnent sur les ordinateurs et les serveurs d'une entreprise, classification automatique par un apprentissage machine exploitant notre plate-forme Big Data sur le Cloud, et enfin, analyse par nos experts techniques des applications n'ayant pas été classifiées automatiquement afin de déterminer avec certitude le comportement de tout ce qui s'exécute sur les systèmes de l'entreprise.

LA SEULE SOLUTION POUR GARANTIR LA SÉCURITÉ DE TOUTES LES APPLICATIONS EN FONCTIONNEMENT

GARANTIE D'UNE PROTECTION FIABLE ET COMPLÈTE

Panda Adaptive Defense propose deux modes d'action :

• **Le mode standard** autorise, après une phase d'audit, l'exécution de toutes les applications cataloguées comme inoffensives ainsi que les systèmes automatisés. Les processus inconnus ou en provenance de l'exterieur sont bloqués par défaut jusqu'à la fin de leur classification.

• **Le mode étendu** permet uniquement l'exécution des logiciels catalogués inoffensifs apres une longue phase d'apprentissage. Il est recommandé aux organisations qui souhaitent une approche 'à risque zéro' de la sécurité.

RÉSULTATS D'ANALYSE A POSTERIORI

• Les **graphiques des événements d'exécution** donnent une vue claire de tous les événements provoqués par des logiciels malveillants.

• Bénéficiez, grâce aux **cartes de températures,** d'informations visuelles sur la source géographique des connexions de logiciels malveillants, des fichiers créés, etc.

• Localisez les logiciels installés sur votre réseau et comportant des vulnérabilités connues.

COMPATIBLE AVEC LES SOLUTIONS ANTIVIRUS TRADITIONNELLES

Adaptive Defense peut coexister avec les solutions antivirus traditionnelles, et agir comme **un outil d'entreprise complémentaire capable de bloquer tous les types de logiciels malveillants, notamment les attaques ciblées et les nouvelles menaces éclair** que les solutions traditionnelles ne sont pas en mesure de détecter.

PROTECTION POUR LES SYSTÈMES D'EXPLOITATION ET LES APPLICATIONS VULNÉRABLES

Les systèmes tels que Windows XP, qui ne sont plus supportés par leur éditeur, ne reçoivent plus de correctifs et sont donc vulnérables ; ils deviennent des proies faciles pour les menaces nouvelles (zero-days) et les attaques de nouvelle génération.

En outre, les vulnérabilités dans les applications comme Java, Adobe, Microsoft Office et les navigateurs sont exploitées par 90 % des logiciels malveillants.

Le module de protection contre les vulnérabilités d' **Adaptive Defense** utilise des règles contextuelles et comportementales pour permettre aux entreprises de travailler dans un environnement sécurisé même avec des systèmes qui n'ont pas été mis à jour.

INFORMATIONS EN TEMPS RÉEL SUR L'ÉTAT DU RÉSEAU

• Bénéficiez d'alertes immédiates dès qu'un logiciel malveillant est identifié dans le réseau, avec un rapport complet détaillant l'emplacement, les ordinateurs infectés et l'action entreprise par le logiciel malveillant.

• Recevez des rapports par e-mail sur l'activité journalière du service.

ACCESSIBLE AUX SYSTÈMES SIEM

Adaptive Defense s'intègre à des solutions SIEM pour fournir des informations détaillées sur l'activité de toutes les applications qui s'exécutent sur vos systèmes.

Pour les clients sans SIEM, **Adaptive Defense** inclut son propre système de stockage et de gestion des événements de sécurité afin d'analyser toutes les informations. collectées en temps réel.

SERVICE GÉRÉ À 100%

Vous n'aurez plus à investir dans du personnel technique pour traiter les fichiers suspects ou placés en quarantaine ou bien pour désinfecter et restaurer les ordinateurs infectés. **Adaptive Defense** classifie automatiquement toutes les applications grâce à son apprentissage machine dans nos environnements Big Data sous la supervision constante des experts de PandaLabs.

CONFIGURATION MINIMALE REQUISE

Console Web (surveillance uniquement)

- Connexion Internet
- Internet Explorer 7.0 ou ultérieur
- Firefox 3.0 ou ultérieur
- Google Chrome 2.0 ou ultérieur

Agent

- Systèmes d'exploitation (postes de travail): Windows XP SP2 et ultérieurs, Vista, Windows 7, 8 & 8.1
- Systèmes d'exploitation (serveurs): Windows 2003 Server, Windows Server 2008, Windows Server 2012
- Connexion Internet (directe ou via proxy)