PROTÉGEZ-VOUS CONTRE LES MENACES SANS JAMAIS BAISSER LA GARDE

Pour être réellement efficace, une solution de protection pour poste client doit désormais pouvoir offrir des fonctionnalités de prévention, de détection, de visibilité et d'intelligence adaptative, avant, pendant et même après une cyber-attaque.

Adaptive Defense intègre tous ces éléments dans une solution EDR offrant une protection performante et légère pour vos terminaux et serveurs, avec en outre une capacité de traitement étendue et évolutive

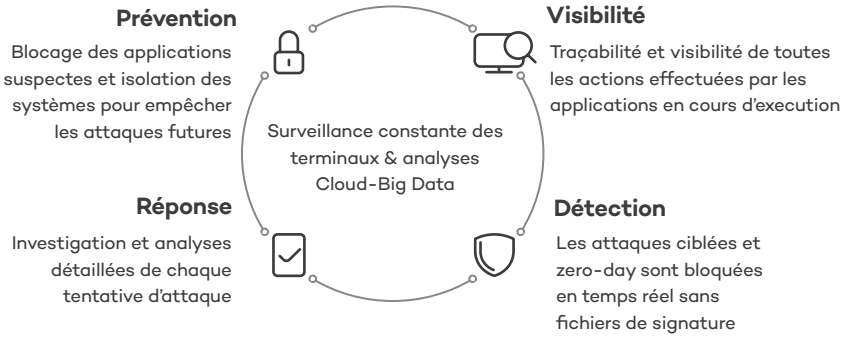
Adaptive Defense 360

Les solutions antivirus traditionnelles sont efficaces pour bloquer les logiciels malveillants connus au moyen de techniques de détection basées sur des index de signatures et des algorithmes heuristiques. Toutefois, elles sont inefficaces contre les attaques ciblées et « zero-day », lesquelles sont conçues pour exploiter la « fenêtre d'opportunités » du malware au moyen d'outils, de tactiques, de techniques et de processus malveillants (TTP).

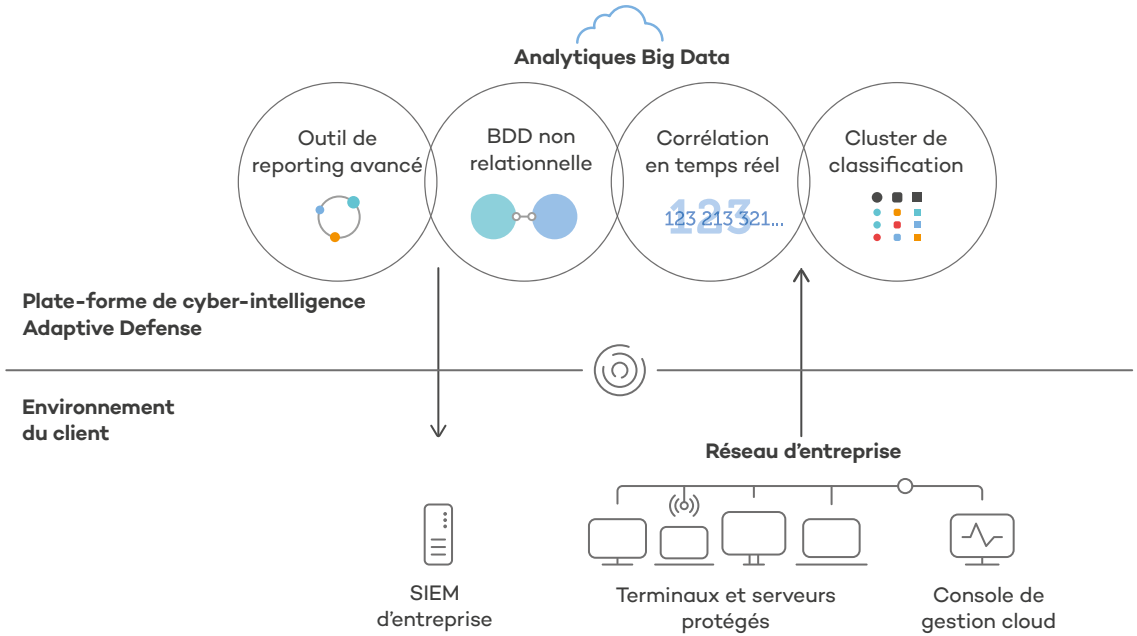
La fenêtre d'opportunités s'élargit et les pirates en tirent parti pour infecter les entreprises avec des virus, des logiciels de rançon, des chevaux de Troie et d'autres types de logiciels malveillants avancés et d'attaques ciblées.

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

La gamme Adaptive Defense est la solution de Panda Security à ces types d'attaques. Adaptive Defense propose un service de détection et de réponse pour les postes clients (EDR), capable d'auditer et de cataloguer avec précision chaque applicatif, processus et services système s'exécutant dans l'entreprise, afin d'autoriser uniquement les actions diagnostiquées comme fiables.



Panda Adaptive Defense s'appuie sur un modèle de sécurité basé sur trois principes : surveillance continue de toutes les applications sur les serveurs et postes de travail de l'entreprise, classification automatique des processus des postes clients au moyen de techniques d'analyse Big Data et d'apprentissage machine sur une plate-forme cloud, et possibilité pour un technicien expert du PandaLabs d'analyser le comportement en profondeur si un processus ne peut pas être classé automatiquement.



Les véritables solutions de sécurité devraient associer des technologies informatiques sophistiquées avec de l'intelligence humaine. En d'autres termes, il faut combiner les capacités actuelles d' apprentissage machine à l'expertise des analystes. Pour être prise au sérieux, une solution de sécurité doit offrir le type de prévention, de détection, de visibilité et d'intelligence capable d'arrêter en permanence et de façon autonome n'importe quel type de cyber-attaque, identifié ou pas.

Nous sommes convaincus que les décideurs doivent désormais prendre en compte les aspects clés suivants au moment de choisir une solution de cybersécurité pour terminaux :

- **Surveillance continue**, grâce à l'enregistrement et à la surveillance de toutes les activités des processus en cours afin d'empêcher le démarrage de logiciels non fiables au moment de l'exécution, de détecter les menaces avancées en temps réel, de réagir en quelques secondes et de rétablir le fonctionnement normal instantanément.
- **Détection de l'exécution de fichiers non fiables**, afin de réduire le périmètre des attaques menées contre l'entreprise. Vous devez vous assurer que la solution de sécurité sélectionnée puisse identifier comme fiables ou malveillantes la totalité des applications executées sur vos postes clients, serveurs et terminaux mobiles.
- **Détection intelligente des menaces.** Une cybermenace sera toujours plus rapide que n'importe quel appareil que vous souhaitez protéger. Par conséquent, ce n'est pas à l'utilisateur de s'occuper de la surveillance et de la réponse à donner en cas d'incident. Des solutions de sécurité pertinentes doivent être capables de fonctionner en autonomie et de s'adapter automatiquement à l'environnement d'exploitation spécifique à votre entreprise.
- **Réponse rapide et automatisée.** Les organisations sont saturées par le volume d'événements et d'alertes générés par leurs systèmes, mais une fois le cybercriminel infiltré, quelques secondes peuvent lui suffire pour dérober des informations. Par conséquent, la solution de sécurité choisie doit être capable d'identifier rapidement une attaque en cours, de prendre des mesures pour éviter des dommages et d'alléger la charge de travail des systèmes. Ainsi, vous pouvez réduire les coûts

Capacités de protection des postes clients critiques

● traitement complet
◒ traitement partiel

	Adaptive Defense	Anti virus	Anti exploit	Anti ransom	Sand boxing
PROTECTION CONTRE LA DYNAMIQUE D'ATTAQUES TELLES QUE :					
Logiciels malveillants connus et inconnus, attaques « zero-day », y compris tout nouveau crypto-ransomware et ses variantes	●	◒			◒
Menaces persistantes avancées (APT's), attaques ciblées et cyber-espionnage	●				
Attaques au moyen d'exploitations de vulnérabilités connues et inconnues, y compris lles attaques sans logiciels malveillants	●		●		
Attaques DDOS par botnet transformant les ordinateurs en machines "zombie" contrôlées par des serveurs C&C	●				◒
PROTECTION DE POSTES CLIENTS DE PROCHAINE GÉNÉRATION (NGEP)					
Prévention des logiciels malveillants, détection des attaques pendant leur exécution et prévention des tentatives répétées	●	◒	◒	◒	
Surveillance continue des processus actifs, classification de toutes les applications et arrêt de leur exécution si elles ne sont pas fiables	●				
Adaptation continue à la nouvelle dynamique des attaques au moyen de techniques de machine learning en environnement Big Data	●	◒			◒
Surveillance à long terme de l'attaque, outils de détection et de blocage dynamique, tactiques, techniques et processus malveillants (TTP)	●				
DÉTECTION, CONFINEMENT ET RÉSOLUTION					
Si quelque chose n'est pas normal ou si un comportement suspect est bloqué, vous serez alerté en temps réel	●				
Fournit des informations en temps réel sur les activités d'un pirate : origine de l'attaque, cause, actifs impactés et actions mises en place	●				
Résolution automatique, suppression des fichiers malveillants, réparation des dommages causés et arrêt des processus compromis	●	◒	◒	●	◒
Propose des informations d'exploitation sur les tâches effectuées après l'événement et les mesures prises contre de futures attaques	●				
SERVICE DE SÉCURITÉ ADMINISTRÉE					
Automatisation des processus afin de réduire la charge de travail des équipes de sécurité et le délai entre la détection et la réponse	●				
Des analystes experts dans le domaine de la découverte de nouvelles attaques (« chasseurs de menaces ») renforcent le service automatisé	●	◒			
Surveillance et analyse des activités des pirates 24 h/24, 7 j/7, 365 jours par an	●	◒			◒
OUTILS D'ANALYSE DES INCIDENTS					
Fournissent la chronologie d'une attaque (fichiers, logs, pilotes, etc.) et son impact sur l'activité (par ex., actifs affectés, machines zombies)	●				
Accès à des informations granulaires basées sur l'utilisateur, pour préserver la confidentialité	●				
Intégration complète avec d'autres outils d'analyse, et en particulier les solutions de type SIEM	●				
INTELLIGENCE DE GESTION DES RISQUE					
Visibilité complète sur tous les systèmes : logiciels en cours d'exécution, applications vulnérables, comportement des utilisateurs, trafic, etc.	●				
Outils de recherche d'anomalies provoquées par des attaques externes ou par une utilisation inappropriée des ressources de l'entreprise	●				
Outils basés sur une plate-forme Big Data en mode Cloud, qui réduit au minimum les coûts d'exploitation et les délais de réponse	●				
SIMPLICITÉ DE DÉPLOIEMENT ET DE GESTION					
Simplicité de déploiement, de mise à jour et de gestion à partir du cloud, pour la protection optimale des systèmes distants	●	●	●	●	◒
Déploiement à grande échelle, sans interruption du service, avec un auto-apprentissage et une adaptation à l' entreprise de manière transparente	●				
Plusieurs technologies parfaitement intégrées, afin d'éviter une consommation inutile de ressources et d'améliorer les synergies entre elles	●	●			
Impact minimum sur le réseau et sur les appareils protégés, avec un impact maximum de 5 % sur les performances du système	●	◒	◒	◒	
Gêne minimale pour les utilisateurs finaux. Reduction de la surcharge de travail pour les équipes d'exploitation dans l'analyse des données	●	◒	◒	◒	
CAPACITÉ DE TRAITEMENT EN TEMPS RÉEL					
Technologie d'apprentissage machine et d'analyse contextuelle comme méthode exclusive de classification	●				
Traitement cloud et Big Data permettant la diffusion, le partage et la croissance exponentielle des connaissances, en temps réel	●	◒			
Utilisation cloud et data mining sans limitation de calcul pour réduire la complexité des systèmes et optimiser la gestion des risques	●	◒			