GARANTIR LA SÉCURITÉ DE TOUTES VOS APPLICATIONS

Adaptive Defense 360 est la première offre à combiner les capacités d'une protection EPP (Endpoint Protection Platform) et d'une solution EDR (Endpoint Detection & Response) dans une solution unique. La solution inclut un service EDR capable de classifier avec précision chaque application qui s'exécute dans votre entreprise, en autorisant uniquement l'exécution des programmes identifiés comme légitimes. Les capacités EDR s'appuient sur un modèle de sécurité reposant sur trois principes : la surveillance constante des applications qui fonctionnent sur les ordinateurs et serveurs d'une entreprise, la classification automatique par un apprentissage machine exploitant notre plate-forme Big Data sur le Cloud, et enfin, l'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 sytèmes de l'entreprise.

DEUX MODES D'ACTIONS

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'extérieur sont bloqués par défaut jusqu'à jusqu'à leur classification.
Le ***mode étendu*** permet uniquement l'exécution des logiciels catalogués inoffensifs après une longue phase d'apprentissage. Il est recommandé aux organisations qui souhaitent une approche « à risque zéro » de la sécurité.

45%

DES LOGICIELS MALVEILLANTS SONT DE PLUS EN PLUS SOPHISTIQUÉS

16%

EVOLUTION DES SOLUTIONS ANTIVIRUS TRADITIONNELLES

SYSTÈMES D'EXPLOITATION ET APPLICATION

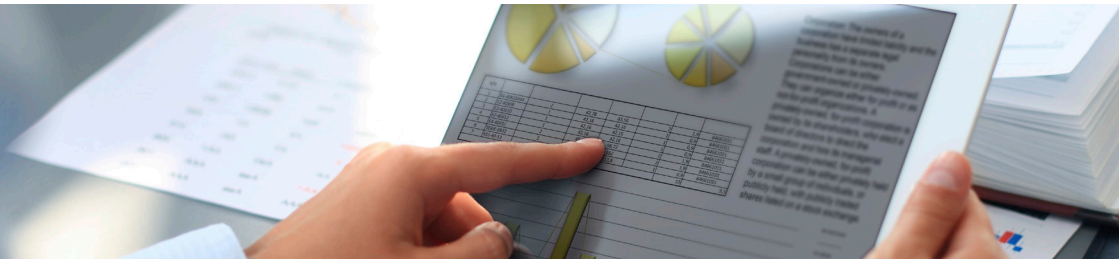
Les systèmes tels que Windows XP, qui ne sont plus supportés par leur éditeur, ne reçoivent plus de correctifs et sont donc vulnérables. Ils deviennent des proies faciles pour les menaces nouvelles zéro day et les attaques de nouvelle génération. En outre, les vulnérabilités dans les applications comme Java, Adobe, Microsoft Office et les navigateurs sont exploitées par 90% des logiciels malveillants. Ce module de protection contre les vulnérabilités utilise des règles contextuelles et comportementales pour permettre aux entreprises de travailler dans un environnement sécurisé.

31%

EVOLUTION DES ENVIRONNEMENTS INFORMATIQUES DES ENTREPRISES

RÉSULTAT D'ANALYSE

Les graphiques d'exécution donnent une vue claire de tous les événements provoqués par des logiciels malveillants. Bénéficiez, grâce à une cartographie complète, 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.



L'ÉTAT DU RÉSEAU EN TEMPS RÉEL

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. De plus, recevez des rapports par e-mail sur l'activité journalière du service.