

Panda Adaptive Defense 360

Plateforme EPP + EDR avec services de Threat Hunting et d'attestation 100%.

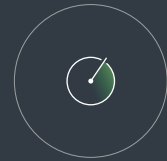
Panda Adaptive Defense 360 est une plateforme de sécurité intelligente associant une protection des terminaux (EPP), une technologie de détection et réponse sur le poste client (EDR) et des services gérés d'attestation, de traque et d'investigation approfondie des cybermenaces avancées.

Adaptive Defense 360 repose sur 4 principes :



Prévention, détection et réponse

aux attaques, avec ou sans malware, via un agent de protection unique



Visibilité instantanée et rétroactive

avec historiques détaillés de l'activité sur tous les terminaux



Classification de 100% des services et processus actifs

99.98% par apprentissage machine, 0.02% par les analystes en cybermenace de Panda



Traque et investigation approfondie des cyberattaques

assurés par les analystes de Panda Security ou par nos MSSPs

La combinaison de ces solutions et services administrés fournit un aperçu détaillé de l'activité sur chaque terminal, un contrôle total des processus en cours d'exécution, et une réduction de la surface d'attaque.

"Panda Security a été nommé Visionnaire dans le Gartner 2018 Magic Quadrant for Endpoint Protection Platforms¹."

Ian McShane, Eric Ouellet,
Avivah Litan, Prateek Bhajanka.

Gartner 2018 Magic Quadrant
for Endpoint Protection Platforms
Janvier 2018

"Une évolution nécessaire contre les menaces inconnues. Panda Adaptive Defense a une panoplie d'outils que nous n'avons pas vu dans les autres solutions."

Data and Analytics. Industry: Services
250M - 500 M USD. North America
December 2018

www.gartner.com/reviews/review/view/646718



4.6 ★★★★★
134 Avis vérifiés

92% 👍
Recommandations

Panda Adaptive Defense 360
Visibilité sans limite, Contrôle absolu



Réinventer la Cybersecurité

Le nouveau modèle de sécurité qui vous offre toute les réponses.

Panda Security dévoile un nouveau modèle de protection qui combine les dernières technologies en terme de prévention, de détection, de réaction et de remédiation.



Surveillance en continu de toutes les applications



Classification de 100% des processus actifs sur l'ensemble des terminaux



Protection automatisée par apprentissage machine et traitement I.A et Big Data



Analyse et investigation approfondie réalisée par des analystes en cas de nécessité



Prévention contre les malwares identifiés



Détection des cybermenaces avancées



Détection dynamique des exploitations de vulnérabilités



Détection basée sur de l'analyse comportementale et contextuelle

Découvrez tout ce que Panda Adaptive Defense 360 et ses modules peuvent faire pour votre sécurité :

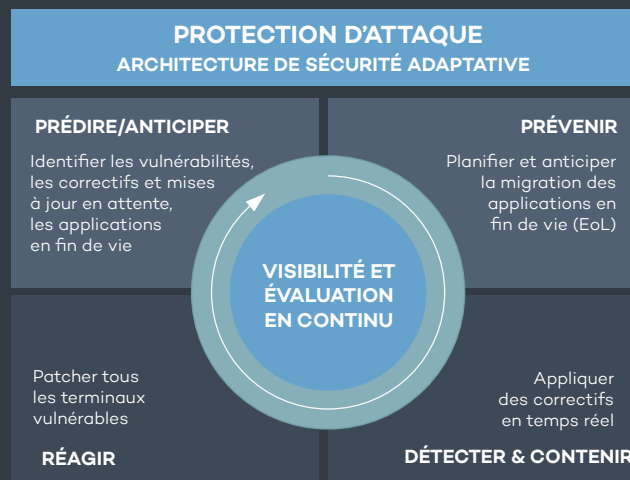
www.pandasecurity.com/business/adaptive-defense/

Panda Patch Management

Panda Patch Management est une solution conviviale pour la gestion des vulnérabilités des systèmes d'exploitation et des applications tierces sur les stations de travail et serveurs Windows. Il réduit les risques tout en renforçant les capacités de votre organisation en matière de prévention, de confinement et de réduction de la surface d'attaque. La solution ne nécessite pas le déploiement de nouveaux agents sur les postes ni de console de gestion additionnelle car elle est nativement intégrée à toutes les solutions Panda pour terminaux.

Panda Patch Management permet une visibilité centralisée et en temps réel sur l'état de sécurité des vulnérabilités logicielles, des correctifs manquants, des mises à jour et logiciels non pris en charge (EOL3), à l'intérieur et à l'extérieur du réseau de l'entreprise. Il offre également des outils faciles à utiliser pour l'ensemble du cycle de gestion des correctifs : De la découverte et de la planification à l'installation et à la surveillance.

- Découverte des ordinateurs vulnérables, des correctifs et mises à jour en attente.
- Application des correctifs et mise à jour des tâches de planification et d'installation
- Supervision des terminaux et des statuts de mise à jour
- Gestion granulaire basée sur des groupes et des rôles disposant d'autorisations différentes

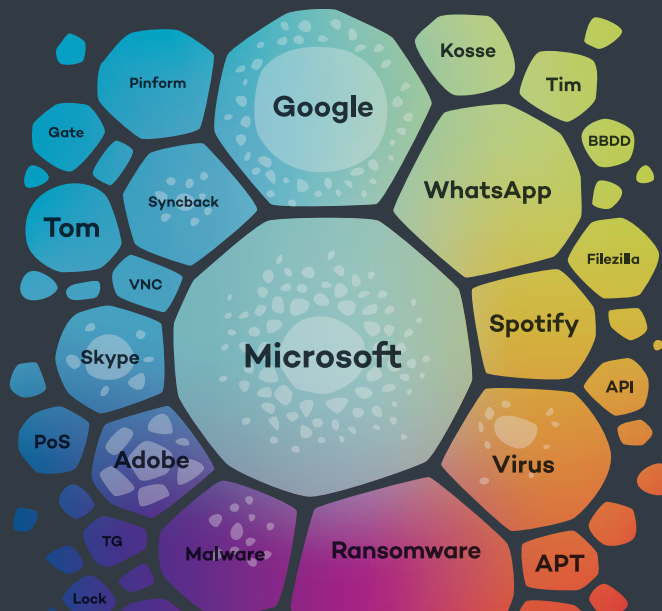


www.pandasecurity.com/business/solutions/#patchmanagement

Advanced Reporting Tool

Ce module agrège toutes les données reçues, en les corrélant et en les présentant en temps réel sous forme graphique pour offrir une visibilité granulaire de tout événement se produisant sur le réseau. Panda Advanced Reporting Tool est ainsi capable de générer automatiquement des informations sur la sécurité et de fournir les outils permettant à l'entreprise de localiser avec précision les attaques et les comportements inhabituels, d'où qu'ils viennent, ainsi que de détecter toute utilisation interne abusive des systèmes et ressources du réseau de l'entreprise.

- Représentation graphique paramétrable des analyses.
- Émission d'alertes avec indicateurs sur l'état de sécurité du réseau et de l'usage des ressources IT.
- Analyse approfondie et diagnostic de l'origine de la menace.
- Gain en visibilité sur la vulnérabilité des terminaux.
- Surveillance de l'usage inapproprié des ressources internes.



www.pandasecurity.com/business/modules/#ART

SIEM Feeder

Ce module génère de la valeur ajoutée et offre une plus grande visibilité sur tout ce qui se passe sur votre réseau en incorporant toutes les données collectées par Panda Adaptive Defense au sein de votre propre application SIEM.

Avec SIEM Feeder, vous pouvez désormais intégrer une nouvelle source d'information critique : les processus et programmes en cours d'exécution sur tous vos terminaux.

SIEM FEEDER VOUS PERMET DE DÉCOUVRIR

Quels nouveaux programmes sont exécutés alors qu'ils ne sont pas encore classifiés

Comment ces programmes ont pu accéder à votre réseau d'entreprise

Les éventuelles activités suspectes sur les appareils des utilisateurs

Quels sont les logiciels en cours d'utilisation présentant des vulnérabilités

Les processus qui accèdent à des données utilisateur et les transmettent à l'extérieur

Combien de ressources réseau sont consommées par chaque processus



www.pandasecurity.com/business/modules/#siem