

# Visibilité sans limite, Contrôle absolu

## Panda Adaptive Defense 360

### Protection, Detection, Response & Remediation

Organisations still being compromised: Despite layers of next-gen security, hackers, zero-day and targeted attacks are still causing havoc.

Panda Adaptive Defense 360 is the only Endpoint Protection solution to provide 100% process classification service as standard.

## Panda Patch Management

### Simplifiez la gestion de correctif pour réduire la surface d'attaque de votre réseau

Panda Patch Management est une solution pour gérer les mises à jour et les correctifs, à la fois pour les systèmes d'exploitation et pour des centaines d'applications tierces. Elle renforce les capacités de prévention, de confinement et de correction des menaces, réduisant la surface d'attaque sur les serveurs et les postes de travail sous Windows.

Patch Management fournit une visibilité en temps réel sur l'état de santé des terminaux, en termes de vulnérabilités, de correctifs, de mises à jour en attente et de logiciels non pris en charge (EoL). Découvrez, planifiez, installez et surveillez.

## Panda Data Control

### Sécurité, visibilité et contrôle des données en temps réel

Des violations massives de données se produisent encore trop souvent : l'accès non contrôlé aux données personnelles (PII) et sensibles (IP) de l'entreprise est une menace quotidienne pouvant entraîner de graves pertes financières et des atteintes à la réputation.

Panda Data Control aide les organisations à se conformer aux réglementations de protection des données, à identifier et à protéger leurs données personnelles et sensibles, en temps réel et tout au long de leurs cycles de vie sur les terminaux et les serveurs.

## Panda Full Encryption

### Renforcez la sécurité des accès non autorisés de manière centralisée

L'un des moyens les plus efficaces de minimiser l'exposition de vos données consiste à chiffrer automatiquement les disques durs des ordinateurs de bureau, des ordinateurs portables et des serveurs, afin de garantir que l'accès à vos données est sécurisé et conforme aux mécanismes d'authentification mis en œuvre.

Panda Full Encryption utilise BitLocker, une technologie Microsoft éprouvée et stable, pour chiffrer et déchiffrer les disques sans affecter les utilisateurs et fournir aux organisations la capacité de contrôler et de gérer de manière centralisée les clés de récupération stockées sur Aether, notre nouvelle plateforme de gestion cloud.

## Advanced Reporting Tool

### A partir de vos données, des informations directement exploitables pour votre sécurité et votre IT.

Personnel informatique dépassé : l'augmentation des volumes de données et les attaques avancées entraînent la négligence de détails vitaux, compromettant la sécurité de l'ensemble du système.

Panda Advanced Reporting Tool corréle les données pour générer automatiquement des informations de



Protection traditionnelle (EPP)    Protection avancée (EDR)    Gestion d'infrastructure    Gestion/protection d'infrastructure    Protection avancée (modules optionnels)    Email hébergés

Panda Endpoint Protection   
 Panda Endpoint Protection Plus   
 Panda Adaptive Defense   
 Panda Adaptive Defense 360   
 Panda Systems Management   
 Panda Fusion   
 Panda Fusion 360   
 Panda Patch Management   
 Panda Full Encryption   
 Advanced Reporting Tool   
 Panda Data Control   
 Panda Email Protection

**Comparatif des solutions professionnelles Panda Security**

Gestion centralisée à partir d'une console cloud unique	● 1	● 1	● 1	● 1	● 2	● 3	● 3	● 1	● 1	● 1	● 1	● 4
Un seul agent léger sur les terminaux	●	●	●	●	●	2 agents	2 agents	●	●	●	●	
Protection contre les applications malveillantes (malware, phishing, ransomware, Trojans, etc.)	●	●		●		●	●					●
Protection contre les scripts et les macros malveillantes dans les fichiers Office, etc.	●	●	●	●		●	●					
Protection contre les attaques ciblées (APT) dans leurs phases de pre-execution et d'exécution			●	●			●					
Détection des exploits inconnus basée sur le comportement des processus compromis en mémoire			●	●			●					
Application virtuelle des correctifs pour les systèmes non pris en charge			●	●		●	●					
Détection des indicateurs d'attaque (IoAs) dans la phase de pré-exécution	●	●	●	●		●	●					
Détection comportementale et contextuelle des IoAs en phase d'exécution			●	●		●	●					
Surveillance de l'activité sur les systèmes Windows, macOS and Linux			●	●			●					
Apprentissage automatique et approfondi basé sur les attributs statiques, dynamiques et contextuels			●	●			●					
Service d'attestation à 100% pour prévenir l'exécution de logiciels malveillants			●	●			●					
Service administré de traque et d'analyse des menaces pour détecter les activités suspectes des pirates et des employés indéliants			●	●			●					
Pare-feu personnel et administré	●	●		●		●	●					
IDS/HIPS*	●	●		●		●	●					
Protection anti-tamper	●	●	●	●		●	●					
Contrôle des périphériques	●	●		●		●	●					
Filtrage d'URL par catégorie		●		●		●	●					
Surveillance de la navigation Web		●		●		●	●					
Intégration avec les systèmes SIEM existants (optionnel)			●	●			●					
Protection du courrier électronique contre le phishing, les logiciels malveillants et les menaces avancées		Exchange		Exchange		Exchange	Exchange					●
Protection anti-spam		Exchange		Exchange		Exchange	Exchange					●
Désinfection et remédiation	●	●	●	●		●	●					
Fichiers mis en quarantaine accessibles depuis la liste des détections	●	●	●	●		●	●					
Graphiques calendaires d'exécution et expertise détaillée des attaques			●	●			●					
Confinement via la console: Isolation des terminaux de manière contrôlée			●	●		●	●					
Confinement via la console : Redémarrage des terminaux de manière contrôlée	●	●	●	●		●	●					
Déploiement en temps réel des politiques de sécurité et des mises à jour	●	●	●	●		●	●	●	●			
Identification des périphériques non gérés	●	●	●	●		●	●	●	●			
Tableaux de bord, rapports et alertes personnalisables en temps réel	●	●	●	●		●	●	●	●	●		●
Inventaire des actifs matériels et logiciels	●	●	●	●	●	●	●					
Antivol - alarme à distance (Android)	●	●		●		●	●					
Cliché et localisation du voleur (Android)	●	●		●		●	●					
Surveillance de périphériques sans agents					●	●	●					
Installation centralisée du logiciel et contrôle des licences installées					●	●	●					
Scripting et automatisation des tâches					●	●	●					
ComStore - Bibliothèque de composants					●	●	●					



Protection traditionnelle (EPP)

Protection avancée (EDR)

Gestion d'infrastructure

Gestion/protection d'infrastructure

Protection avancée (modules optionnels)

Email hébergés

**Comparatif des solutions professionnelles Panda Security**

	Panda Endpoint Protection	Panda Endpoint Protection Plus	Panda Adaptive Defense	Panda Adaptive Defense 360	Panda Systems Management	Panda Fusion	Panda Fusion 360	Panda Patch Management	Panda Full Encryption	Advanced Reporting Tool	Panda Data Control	Panda Email Protection
--	---------------------------	--------------------------------	------------------------	----------------------------	--------------------------	--------------	------------------	------------------------	-----------------------	-------------------------	--------------------	------------------------

Ticketing d'incident/Help Desk/Chat					●	●	●						
Support MDM pour smartphones et tablettes Android / iOS					●	●	●						
Contrôle à distance					●	●	●						
Surveillance des ordinateurs et des serveurs (Processeur, mémoire, VMI, journaux d'événements, etc.)					●	●	●						
Gestion des correctifs et des services packs pour les systèmes d'exploitation Windows et les applications tierces					Only SO	Only SO	Only SO	●					
Gestion des applications en fin de vie								●					
Restauration de correctifs								●					
Possibilité de désactiver Windows Update de manière centralisée								●					
Patching en temps réel ou programmé								●					
Chiffrement / déchiffrement intégral du disque à l'aide de BitLocker									●				
Gestion centralisée et récupération des clés de cryptage									●				
Application centralisée des stratégies de chiffrement									●				
Tableaux de bord, widgets et rapports de chiffrement									●				
Tableau de bord, widget et requêtes prédéfinies pour les KPI de sécurité										●			
KPIs sur les applications vulnérables, installées et exécutées										●			
KPIs sur l'accès aux données des terminaux										●			
KPIs sur les application shadow IT en cours d'exécution										●			
Inventaire et classification des fichiers PII <sup>6</sup>											●		
Surveillance des fichiers PII (données dormantes, utilisées et en mouvement)**											●		
Recherches guidées définies par l'utilisateur pour les fichiers PII <sup>6</sup> et non-PII											●		
Possibilité de supprimer les fichiers PII <sup>6</sup>											●		
Consoles utilisateur et administrateur												●	
Techniques anti-phishing avancées (anti-spoofing, SPF, DKIM et DMARC, etc.)												●	
Technologie anti-spam propriétaire												●	
Quarantaine centralisée gérée par l'administrateur ou l'utilisateur local												●	
Communication sécurisée obligatoire (TLS) pour les destinataires sélectionnés												●	
Sauvegarde des emails entrants												●	
Notificateur d'emails sur les terminaux												●	
Validation stricte de l'expéditeur												●	
Compatible Windows	●	●	●	●	●	●	●	●	●	●	●	●	Périmétrique
Compatible Exchange		●		●	●	●	●				●	●	Périmétrique
Compatible macOS X	●	●		●	●	●	●				●	●	Périmétrique
Compatible Linux	●	●		●	●	●	●				●	●	Périmétrique
Compatible avec les systèmes virtualisés	●	●	●	●		●	●				●	●	Périmétrique
Compatible Android	●	●		●	●	●	●				●	●	Périmétrique
Compatible iOS					●	●	●						Périmétrique

Les modules **Panda Advanced Reporting** et **Panda Data Control** sont disponibles uniquement avec **Panda Adaptive Defense** et **Panda Adaptive Defense 360**. Les modules **Panda Patch Management** et **Panda Full Encryption** sont disponibles avec **Panda Endpoint Protection & Panda Endpoint Protection Plus**, **Panda Fusion**, **Panda Adaptive Defense** et **Panda Adaptive Défense 360**.

Pour plus d'informations ou pour un essai gratuit de nos solutions, rendez-vous sur [www.pandasecurity.com](http://www.pandasecurity.com)

<sup>\*</sup> Console cloud unique : Gestion centralisée accessible à tout moment. Réduit les coûts d'infrastructure et de maintenance  
<sup>1</sup> Gestion cloud par la console Aether de l'ensemble des solutions et des modules Panda Security pour terminaux  
<sup>2</sup> Console cloud Panda Cloud Systems Management  
<sup>3</sup> Meta-console cloud Panda donnant accès aux interfaces de gestion des produits Panda Cloud System Management, Panda Endpoint Protection Plus & Panda Adaptive Defense 360  
<sup>4</sup> Console cloud Panda Email Protection  
<sup>5</sup> Intrusion Detection System/Host-Based Intrusion Prevention System : Système de détection d'intrusion/ Système de prévention des intrusions sur l'hôte  
<sup>6</sup> Personally Identifiable Information : Informations personnelles identifiables  
 \*\* Données dormantes, actions prises (données en cours d'utilisation) et données en mouvement.