Mettez un terme aux cybermenaces

Panda Adaptive Defense 360

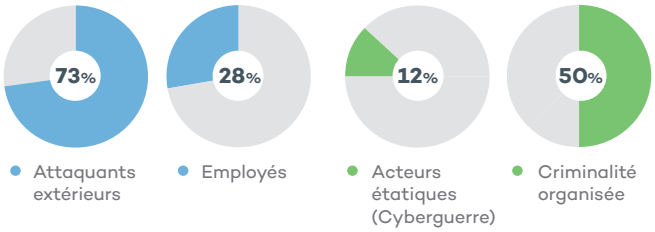
Une sécurité de pointe automatisée et centralisée

panda

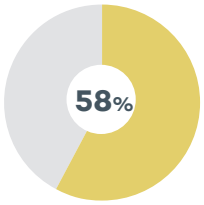
pandasecurity.com

CYBERSECURITÉ DES ENTREPRISES

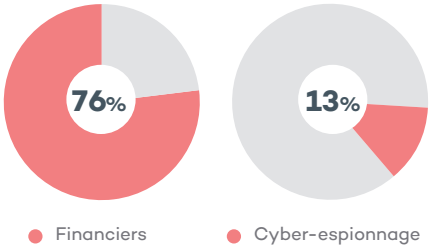
Qui se cache derrière les cybermenaces ?[1]



Qui sont les victimes ?



Quels sont les motifs ?[1]



Les terminaux constituent le nouveau périmètre cible.

La mobilité, le traitement et le stockage dans le cloud ont révolutionné les environnements d'entreprise. **Les postes clients constituent le nouveau périmètre** à défendre. Les solutions de sécurité sur les postes clients doivent être **avancées**, **adaptatives et automatisées**. Elles doivent offrir les niveaux les plus élevés de prévention et de détection des attaquants, lesquels réussiront tôt ou tard à contourner les mesures préventives. De telles solutions doivent aussi proposer des outils agiles permettant de réagir rapidement, de réduire au maximum les dommages et de diminuer la surface d'attaque.

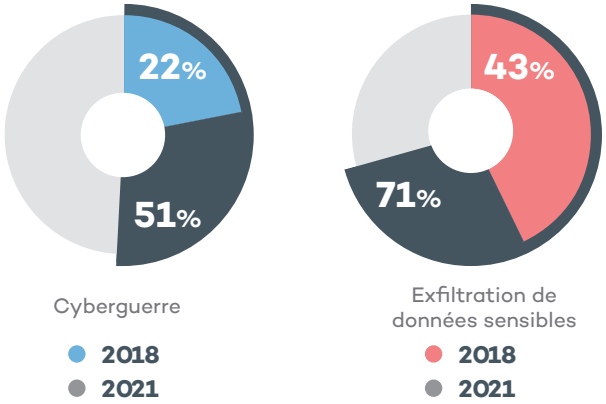
Professionnalisation des cybercriminels

Les techniques des pirates deviennent **de plus en plus sophistiquées**, conséquence de la démocratisation des technologies et des fuites répétées en matière de cyber-intelligence.

Quel coût pour les entreprises ?

- **Coût global :** 600,000 million $[2]
- **Coût d'une violation de données :** 3.86 million $[3]

Perception d'un risque élevé par les entreprises[4].



Dans 60% des cas, les attaques visant les nations sont des actions de **cyberguerre**.

Les cybermenaces de prochaine génération sont conçues pour se glisser au travers des **solutions traditionnelles** sans être détectées.

Cyberdefense dans les organisations

Les pirates ciblent les ordinateurs et serveurs, car ces derniers hébergent les actifs les plus précieux des entreprises et **leur défense par les équipes de sécurité est très difficile à assurer**. Les applications de détection et réponse sur le poste client (**EDR**), loin d'être la seule solution, **augmentent les charges de travail**, car la prévention, la détection et le confinement des menaces, ainsi que la réponse à celles-ci ne sont pas automatisés. **L'amélioration de la posture de sécurité** de votre entreprise **sans augmenter les coûts d'exploitation** passe inévitablement par **l'automatisation des capacités de prévention, de détection et de réponse** sur les postes clients.

SOLUTIONS DE DÉTECTION ET RÉPONSE SUR LE POSTE CLIENT (EDR)

Les solutions EDR surveillent, consignent et stockent les détails de l'activité des postes clients, notamment les événements utilisateurs, les processus, les modifications en base de registre, ainsi que les usages mémoire et réseau. Cette visibilité met au jour des menaces qui resteraient autrement inaperçues.

Quels sont les problèmes cachés des solutions EDR ?

Des techniques et outils multiples sont employés pour détecter des anomalies de sécurité dans les événements et confirmer ou rejeter les alertes. Tous ces éléments nécessitent une intervention humaine.

Les solutions EDR requièrent une supervision 24 h/24, 7 jours/7 et une réponse rapide de la part de personnels hautement qualifiés.

Toutefois, de telles ressources sont onéreuses et difficiles à trouver. Les entreprises en sous-effectifs et aux budgets réduits ne sont pas préparées pour tirer pleinement parti des avantages des solutions EDR. Le personnel est alors soumis à une charge de travail plus forte du fait de la mise en œuvre et de l'utilisation de ces solutions au lieu d'être épaulé dans son rôle essentiel : l'amélioration de la démarche sécurité de son entreprise.

1 "2018 Data Breach Investigation report". Verizon
2 "2018 Economic Impact of Cybercrime — No Slowing Down". CSIC/McAfee
3 "2018 study on global megatrends in cybersecurity". Ponemon Institute
4 "2018 Cost of Data Breach Study: Global Overview". Ponemon Institute/IBM Security

Panda Adaptive Defense 360

Panda Adaptive Defense 360 est une solution de cybersécurité innovante basée sur le cloud pour les ordinateurs de bureau, les ordinateurs portables et les serveurs. Cette solution **automatise la prévention, la détection, le confinement et la réponse** concernant les attaques avancées présentes ou futures, les malwares « zero-day », les rançongiciels, le phishing, les exploitations en mémoire et les attaques sans logiciel malveillant, à l'intérieur et à l'extérieur du réseau d'entreprise.

Elle diffère d'autres solutions en combinant le plus large éventail de technologies de protection (**EPP**) **avec des fonctions EDR automatisées**, grâce à deux services gérés par des experts Panda Security, et fournis en tant que fonctionnalités de la solution :

- **Service d'attestation 100%.**
- **Service de traque et d'investigation sur les menaces (THIS).**

Grâce à son architecture de type cloud, l'**agent est léger** et n'influe pas sur les performances des postes clients, lesquels sont gérés via une **console cloud unique**, même en l'absence de connexion Internet.

Panda Adaptive Defense 360 intègre la plate-forme de protection cloud et de gestion (Aether), qui optimise la prévention, la détection et la réponse automatisée ne nécessitant qu'un effort minimal de la part de l'utilisateur.

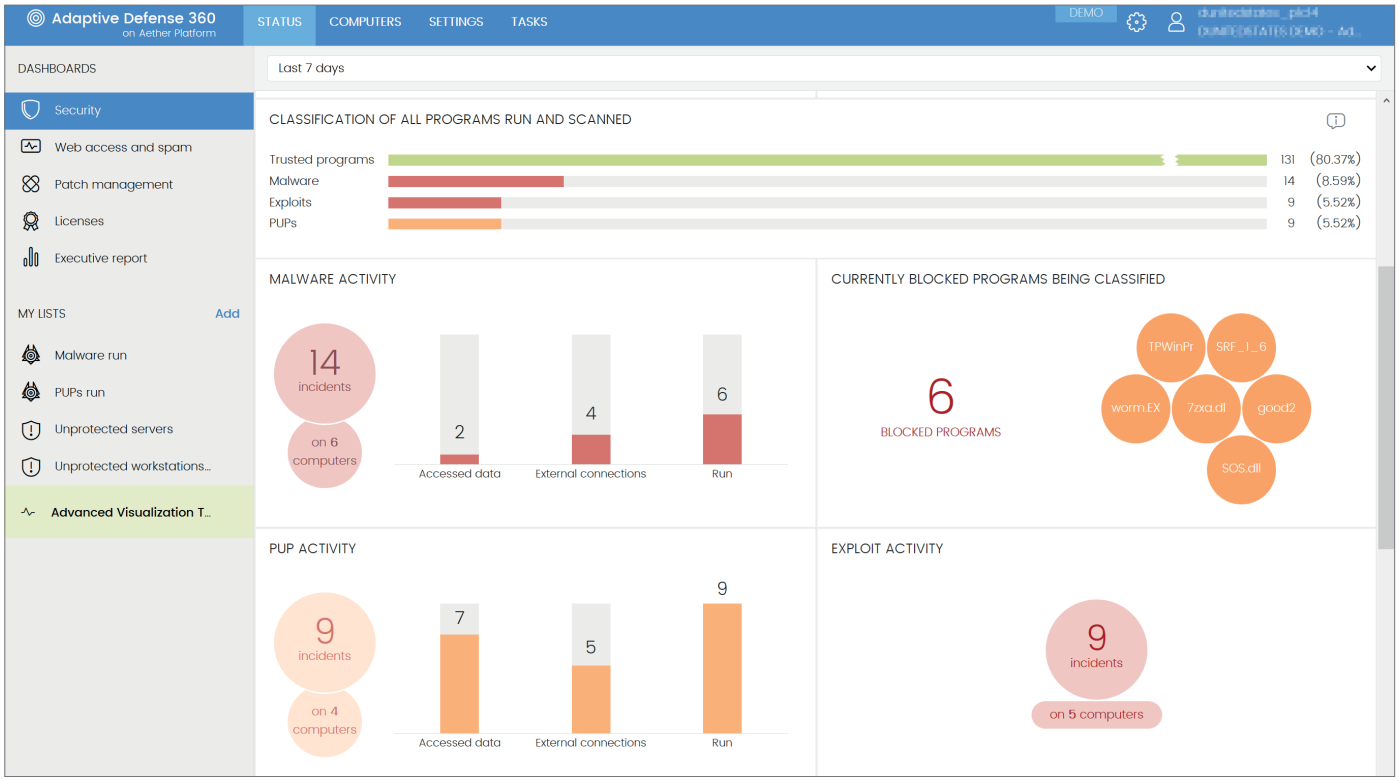


Figure 1 : Le tableau de bord offre une vue globale et une gestion consolidée, capable de prioriser les menaces détectées

AVANTAGES

Panda Adaptive Defense 360

Simplifie et réduit au maximum le coût d'une sécurité avancée et adaptative

- Ses services gérés tirent automatiquement les enseignements des menaces et réduisent les coûts en personnel spécialisé. Il n'y a pas de fausses alarmes, de délégation de responsabilité ni de temps perdu en paramétrage manuel.
- La prévention au niveau des postes clients est maximale. Les coûts d'exploitation sont pratiquement réduits à zéro.
- Aucune installation, configuration ou maintenance d'une infrastructure de gestion n'est nécessaire.
- Les performances des postes clients ne sont pas impactées, car l'approche utilise un client léger et une architecture de type cloud.

Automatise et réduit les délais de détection et d'exposition (Dwell Time)

- Prévient l'exécution des cybermenaces, de malwares type zero-day, de rançongiciels et des tentatives de phishing.
- Détecte et bloque les activités malveillantes en mémoire (exploits), avant qu'elles ne provoquent des dommages ainsi que les techniques et procédures de piratage.
- Détecte les processus malveillants qui échappent aux mesures préventives.

Automatise et réduit les délais de réponse et d'analyse

- Résolution automatique et transparente.
- Récupération de l'activité sur le terminal – restauration immédiate de l'activité normale.
- Données exploitables concernant les attaquants et leur activité, ce qui accélère l'analyse a posteriori.
- Contribue à réduire la surface d'attaque et à améliorer la maturité en matière de politique de sécurité.

PLATEFORME CLOUD DE PROTECTION ADAPTATIVE

Des experts et des machines pour piloter une sécurité adaptative de pointe.

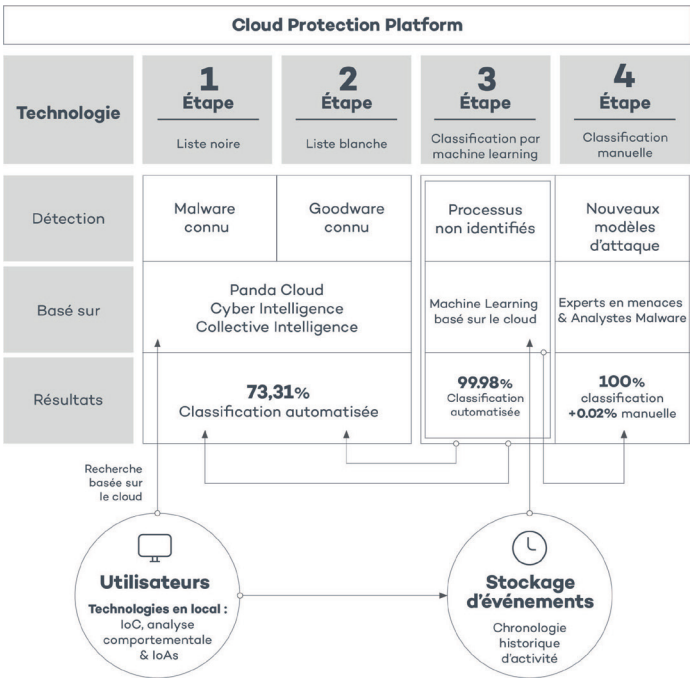
SERVICE D'ATTESTATION À 100%

Le service d'attestation à 100 % surveille et empêche l'exécution d'applications et de processus malveillants sur les terminaux. Pour chaque exécution, il génère une **classification en temps réel d'éléments malveillants ou légitimes, sans aucune incertitude**, et sans délégation au niveau du client. Tout cela est possible grâce à la vitesse, à la capacité, à la flexibilité et à l'évolutivité de l'intelligence artificielle (IA) et du traitement cloud.

Le service associe le **Big Data** et l'**apprentissage machine** multi-niveaux, y compris l'**apprentissage approfondi** (Deep Learning), le résultat de la supervision continue et de l'automatisation de **l'expérience, des renseignements et des connaissances accumulées par les experts** en cyber menaces de Panda Security.

Le Service d'attestation à 100 % est, à la différence des autres solution du marché, capable de libérer les entreprises du risque d'exécution de logiciels malveillants sur les terminaux situés à l'intérieur et à l'extérieur de leur réseau informatique.

Figure 2 : Processus de traitement du service géré de classification



SERVICE GÉRÉ DE TRAQUE ET D'INVESTIGATION SUR LES MENACES

Il existera toujours des menaces en mesure de franchir les contrôles de sécurité déployés

La traque des menaces est le processus consistant à identifier de nouvelles menaces avancées et leurs TTP*, au-delà de ce que peuvent faire les systèmes actuels de détection des menaces, avant que des dégâts importants ne soient occasionnés dans l'entreprise.

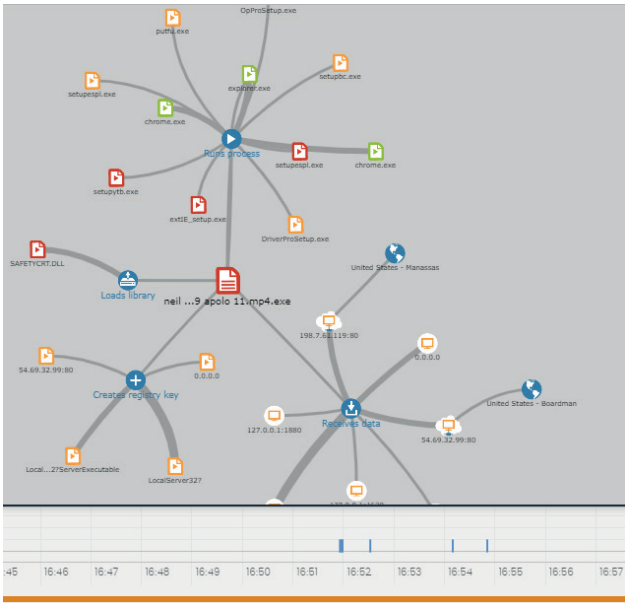
La traque des menaces part du principe que les entreprises sont dans un **état de risque permanent.**

Elle offre, entre autres, les avantages suivants :

- Détection accrue des nouvelles menaces.
- Amélioration de la réponse aux incidents.
- Diminution de la surface d'attaque.

Le service géré de **traque et d'investigation sur les menaces** (Threat Hunting and Investigation) de Panda Security est piloté par des experts en cybersécurité hautement qualifiés, dotés de capacités de profilage, d'analyse et de corrélation d'événements via des outils d'analyse en temps réel et a posteriori, afin d'identifier de nouvelles techniques de piratage et de dissimulation.

Figure 3 : La chronologie des incidents dans la console Panda Adaptive Defense 360 permet des analyses a posteriori (forensics) : la date de première survenance sur le réseau, les noms et le nombre des postes clients affectés, les changements de paramètres et les auteurs des flux de communication suspects.



* TTP: Tactiques, techniques et procédures utilisées par les pirates

AETHER : LA PLATE-FORME CLOUD DE SUPERVISION

Sécurité, visibilité et contrôle de prochaine génération avec une approche complète et évolutive via le cloud, qui apporte une valeur immédiate à votre activité.

La plate-forme Aether avec sa console cloud, commune à toutes les solutions pour terminaux de Panda Security, optimise la gestion de la sécurité adaptative et avancée à l'intérieur et à l'extérieur du réseau de l'entreprise.

Conçue pour que les équipes de sécurité puissent se focaliser uniquement sur la gestion de la démarche cybersécurité de l'entreprise, cette approche réduit au maximum la complexité et optimise la flexibilité, la granularité et l'évolutivité au quotidien.

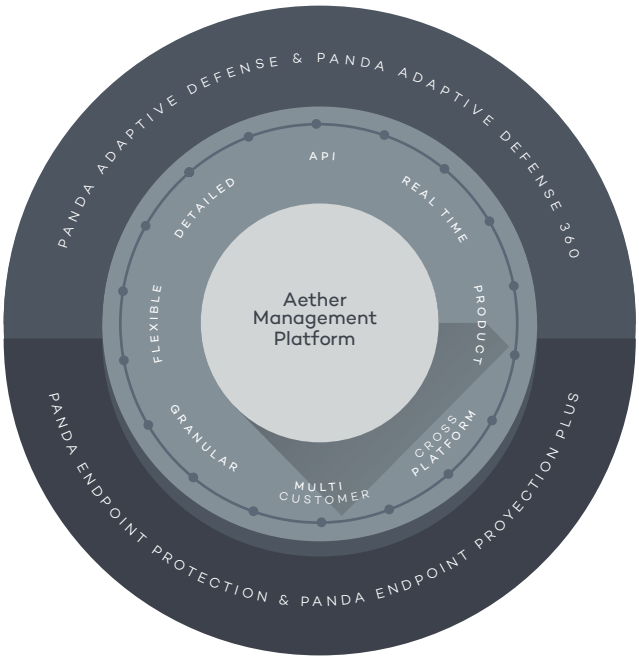


Figure 3: Aether, la plate-forme cloud de gestion unifiée

LES AVANTAGES D'AETHER AVEC

Panda Adaptive Defense 360

Facile à implémenter et offrant une visibilité immédiate sur votre niveau de sécurité

- Déploiement, installation et configuration en l'espace de quelques minutes.
- Un agent de communication léger, multiproduit, multi-modules et multi-plateforme (Windows, Mac, Linux, Android).
- Détection automatique des terminaux non protégés. Installation à distance.
- Technologie proxy propriétaire, pour déploiement sur les ordinateurs sans connexion Web.
- Technologie propriétaire de repository/cache pour une optimisation du trafic.

Simple d'utilisation, et s'adaptant à votre organisation

- Console Web intuitive, flexible et modulaire.
- Rôles prédéfinis et personnalisés.
- Audit détaillé des actions sur la console.
- Utilisateurs disposant d'autorisations et d'une visibilité totales ou restreintes.
- Politiques de sécurité personnalisables par groupes d'utilisateurs.
- Fichiers journaux des inventaires et des modifications au niveau matériel et logiciel.

Facilite la supervision et accélère la réponse

- Indicateurs clés priorisés et tableaux de bord.
- Alertes priorisées et confirmées dans votre workflow.
- Historique complet exploitable des incidents : processus concernés, source, durée de séjour, prévalence, etc.
- Action par simple clic sur les postes clients : redémarrage, confinement, application de patchs et analyse pour une réponse accélérée.

SÉCURITÉ AVANCÉE ET AUTOMATISÉE POUR LES TERMINAUX

Panda Adaptive Defense 360 intègre, dans une même solution, les technologies préventives traditionnelles et des technologies innovantes pour la prévention, la détection et la réponse automatisée contre les cybermenaces sophistiquées.

Technologies préventives traditionnelles

- Firewall personnel ou administré. IDS.
- Contrôle des périphériques.
- Analyses antimalveillance multivecteur, à la demande ou permanente.
- Listes noires/blanches administrées. Intelligence collective.
- Analyses heuristiques avant exécution.
- Contrôle des accès Web.
- Antispam & Antiphishing.
- Anti-tampering. (controleur d'intégrité contre les accès et manipulations non autorisés)
- Filtrage de contenu messagerie.
- Remédiation et rollback.

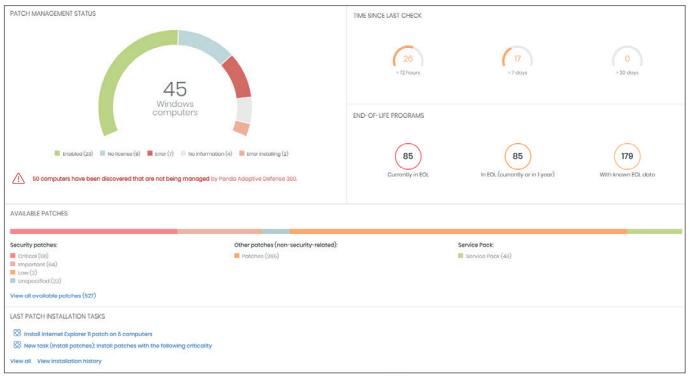
Technologies de cybersécurité avancées

- EDR: surveillance constante de l'activité des postes clients.
- Prévention de l'exécution de processus inconnus.
- Apprentissage machine des comportement, permettant de classer 100 % des processus inconnus (menaces persistantes avancées, logiciels de rançon, rootkits, etc.)
- Confinement (Sandboxing) par le cloud dans les environnements réels.
- Analyse comportementale et détection d'IoA (scripts, macros, etc.).
- Détection et réponse automatique aux exploits en mémoire.
- Traque gérée des menaces pour parer les attaques sans logiciels malveillants (fileless attacks).

MODULES EN OPTION

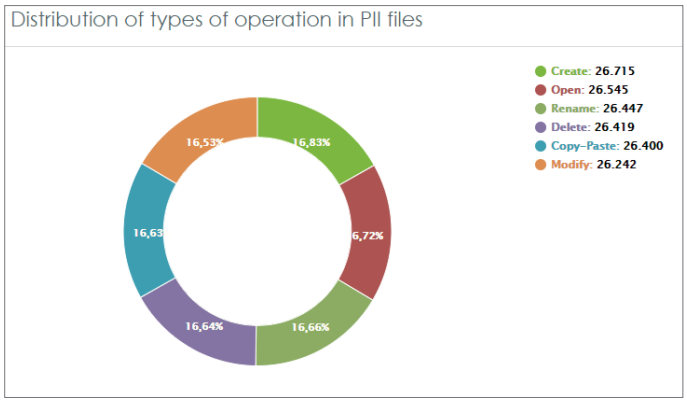
Panda Patch Management

Panda Patch Management est une solution intuitive pour gérer les vulnérabilités des systèmes d'exploitation et des applications tierces sur les postes clients et les serveurs Windows. Le résultat est une surface d'attaque réduite, un renforcement des capacités préventives et un confinement des incidents.



Panda Data Control

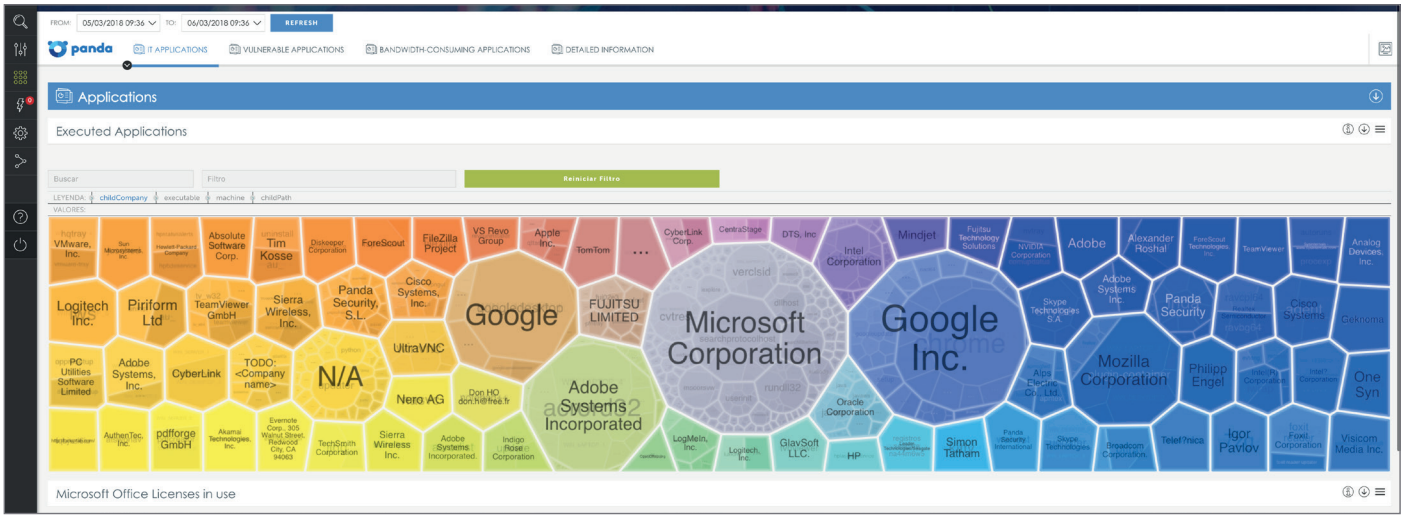
Panda Data Control identifie, audite et surveille les données personnelles ou sensibles non structurées présentes sur les postes clients : aussi bien les données statiques que celles en circulation ou en exploitation.



Panda Advanced Reporting Tool

La plate-forme de reporting automatise la mise en corrélation des informations générées par l'exécution des processus et applications sur les postes clients avec leur contexte, que Panda Adaptive Defense 360 collecte et enrichit dans la plate-forme de protection cloud.

Panda Advanced Reporting Tool génère automatiquement de l'information au niveau de l'activité de l'entreprise et permet la recherche, la mise en corrélation et la configuration d'alertes en matière d'événements.



Le module **SIEMFeeder** envoie en temps réel aux organisations les événements collectés sur les terminaux et enrichis d'information de sécurité provenant de la plate-forme de protection cloud, afin de les intégrer dans la solution SIEM de l'entreprise.

Pour en savoir plus : www.pandasecurity.com/business/solutions

CERTIFICATIONS ET RÉCOMPENSES

Panda Security obtient régulièrement des récompenses en matière de protection et de performances, décernées par les organismes Virus Bulletin, AV-Comparatives, AV-Test et NSSLabs.

Panda Adaptive Defense a obtenu la certification EAL2+ dans son évaluation des Critères Communs.

Panda Security est identifié comme 'Visionnaire' dans le Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) 2018.

AV-Comparatives valide Adaptive Defense 360 "Comme cette solution classe tous les processus exécutés, elle ne peut pas passer à côté d'un logiciel malveillant"

"L'anticipation est notre meilleure alliée pour la définition de nos besoins futurs et pour la prévention des risques. Adaptive Defense 360 nous donne la visibilité nécessaire à cette anticipation."

Jean-Yves Andreoletti

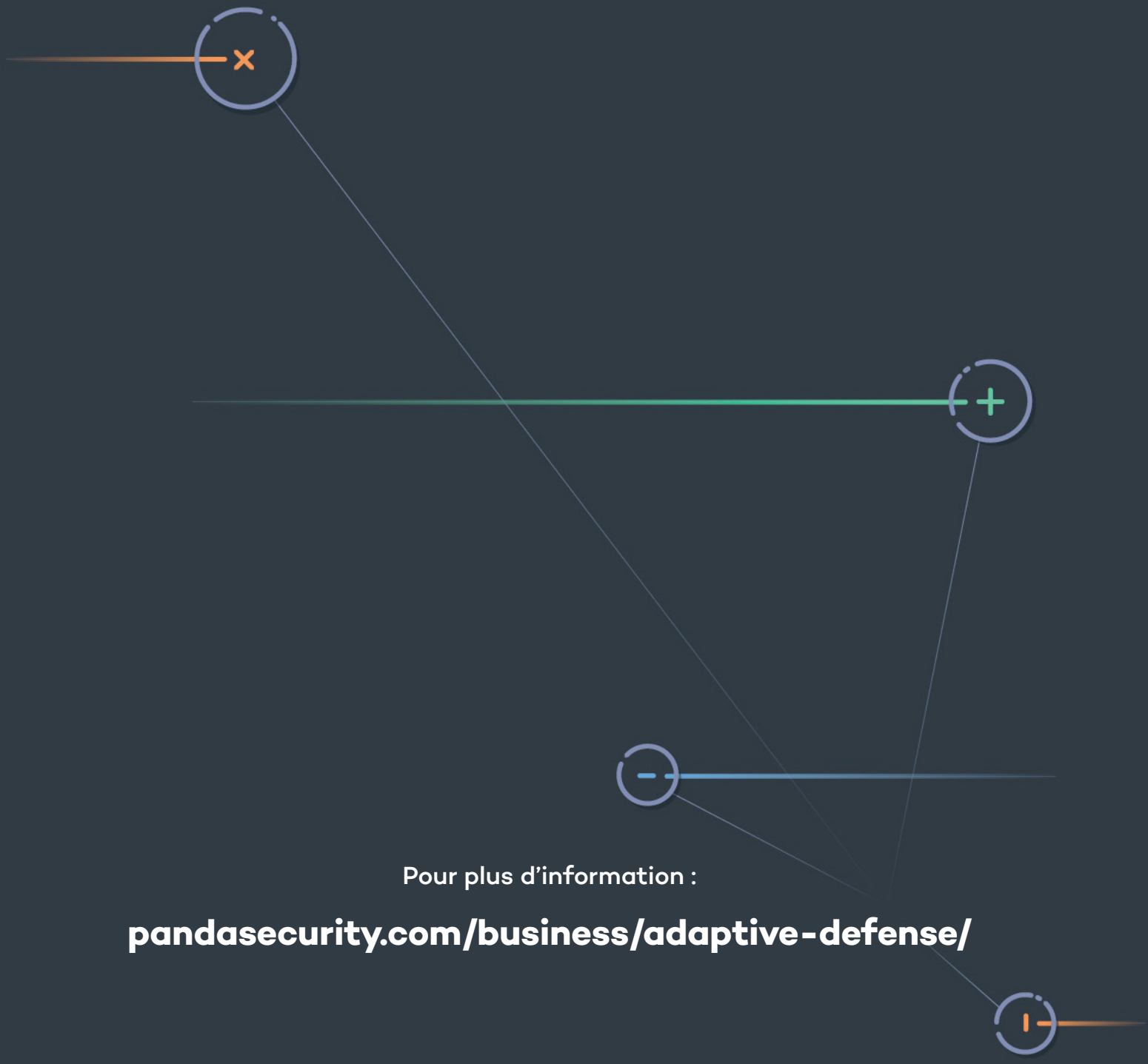
Ingénieur systèmes et réseaux des plates-formes d'intégration, validation et maintenance

Plateformes prises en charge et configuration système requise

Les plates-formes prises en charge évoluent en permanence afin de fournir la couverture maximale possible aux systèmes d'exploitation les plus récents. Accédez à l'aide en ligne de chacun de nos produits avec les liens suivants:

Postes de travail & Serveurs Windows : http://go.pandasecurity.com/endpoint-windows/requirements
Terminaux Mac OS : http://go.pandasecurity.com/endpoint-macos/requirements
Postes de travail & Serveurs Linux : http://go.pandasecurity.com/endpoint-linux/requirements
Téléphones & terminaux Android : http://go.pandasecurity.com/endpoint-android/requirements

Panda Patch Management : http://go.pandasecurity.com/patch-management/requirements
Panda Data Control : http://go.pandasecurity.com/data-control/requirements
Panda Cloud Systems Management : http://go.pandasecurity.com/systems-management/requirements



Pour plus d'information :

pandasecurity.com/business/adaptive-defense/