KASPERSKY ENDPOINT SECURITY FOR BUSINESS : LA SEULE VÉRITABLE PLATE-FORME DE PROTECTION DES TERMINAUX

10 AVANTAGES

QUE SEULE UNE PLATE-FORME DE SÉCURITÉ INTÉGRÉE EST EN MESURE DE VOUS FOURNIR

KASPERSKY lab

Le rapport sur les risques mondiaux liés à la sécurité informatique de Kaspersky Lab révèle que 94 % des entreprises déclarent avoir été victimes d'un incident de sécurité extérieur au cours des 12 derniers mois[1].

Le volume et la sophistication des menaces évoluent de manière exponentielle. C'est la raison pour laquelle les entreprises de toutes tailles cherchent à mieux comprendre les risques liés à la sécurité informatique, notamment les attaques ciblées ainsi que les mesures qu'elles doivent prendre pour se protéger contre des menaces spécifiques plutôt que d'adopter une approche aléatoire et générale de la notion généralisée de « programmes malveillants ».

Il est regrettable de constater que de nombreux éditeurs de solutions de sécurité informatique continuent de s'appuyer sur cette approche en acquérant des nouvelles technologies et en juxtaposant des codes disparates, souvent incompatibles, sources de complexité et de nombreux problèmes à résoudre.

[1] Rapport sur les risques mondiaux liés à la sécurité informatique 2014.

L'utilisation des solutions classiques de sécurité des terminaux, de protection contre les programmes malveillants, de chiffrement et de contrôle des appareils et des réseaux touche à sa fin. Les plates-formes de protection des terminaux comportant des technologies de sécurité étroitement intégrées, représentent la nouvelle tendance en termes de protection avancée des données contre les menaces.

Mais la différence entre intégration et plate-forme au sens strict est de taille. Et en termes d'intégration, il existe différents degrés d'exhaustivité. Pour de nombreux fournisseurs, l'intégration est simplement devenue synonyme de compatibilité.

Et pour d'autres, la compatibilité se traduit par la juxtaposition de solutions préassemblées, pouvant atteindre 40 produits qui doivent fonctionner avec leur propre code.

Les fournisseurs promettant des solutions intégrées sont multiples, mais en approfondissant vos recherches, vous découvrirez qu'il y a une différence considérable entre un simple fonctionnement correct des produits et une réelle synergie prévue dès leur développement. Certains fournisseurs ont du mal à intégrer leurs produits, mais prétendent pourtant proposer des plates-formes véritablement intégrées.

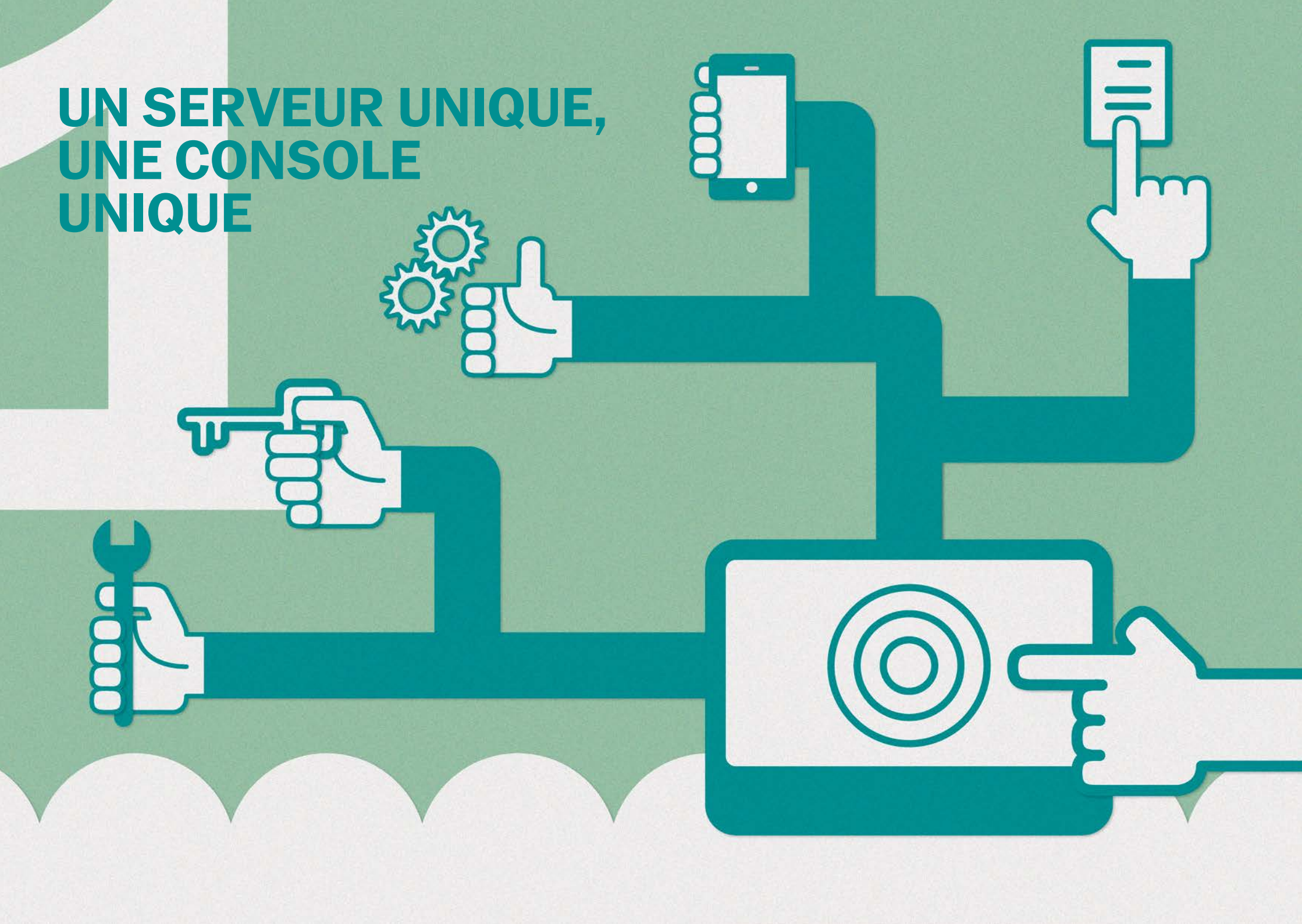
L'achat de ce qui paraît être la prochaine nouveauté ne permet pas de bénéficier de la même vision exhaustive ou protection.

Voici quelques-uns des avantages que seule une solution de plate-forme véritablement intégrée peut apporter : Kaspersky Endpoint Security for Business est en mesure d'offrir les avantages suivants aux administrateurs informatiques :

1. Un serveur unique, une console unique
2. Un agent unique*, une installation simplifiée
3. Une politique unique
4. Un effet de synergie qui va au-delà de la simple somme de ses composants
5. Une gestion des droits d'administration unifiée : capacité d'audit et de contrôle avancée, centralisée sur une seule console
6. Structure et présentation communes : rapidité et simplicité des rapports
7. Une meilleure visibilité des données — tableaux de bord et rapports intégrés
8. Gestion et contrôle unifiés des licences : optimisation des performances et maîtrise
9. Un code unique, conçu en interne pour favoriser une intégration plus avancée
10. Un modèle d'achat intégré : un seul achat permet de bénéficier de l'ensemble des fonctionnalités dont vous avez besoin

* Architecture d'agent unique pour chaque plate-forme (Windows, Linux, Mac).

UN SERVEUR UNIQUE, UNE CONSOLE UNIQUE



1 UN SERVEUR UNIQUE, UNE CONSOLE UNIQUE

Kaspersky Security Center, la solution de Kaspersky Lab, est unique en ce sens où elle permet de bénéficier d'un serveur de gestion et d'une console d'administration uniques étroitement intégrés pour couvrir tous les aspects de la sécurité des terminaux, de la protection contre les programmes malveillants à la protection des données en passant par la gestion de flotte mobile (MDM) et la gestion des systèmes.

La gestion des politiques de sécurité et des rapports est centralisée sur une console unique, intégrée à des ressources externes telles que des annuaires LDAP et Microsoft Exchange. Les bases de données des inventaires logiciels et matériels ainsi que les vulnérabilités/mises à jour logicielles sont également incluses, ce qui favorise les possibilités d'intégration et de synergie, car les mêmes données peuvent être utilisées dans des fonctions multiples. Il n'est pas nécessaire d'effectuer une synchronisation avec différents serveurs ou jeux de données : l'ensemble des composants n'est installé qu'une seule fois sur le même serveur et géré par la même console.

Ces capacités d'intégration et de synergie avancées offrent un avantage différent par rapport aux solutions concurrentes, dont la plupart comprennent des technologies issues de croissance externe, composées de bases de données multiples et distinctes qui sont tout simplement incapables d'offrir la même profondeur d'intégration que la plate-forme de Kaspersky Lab.

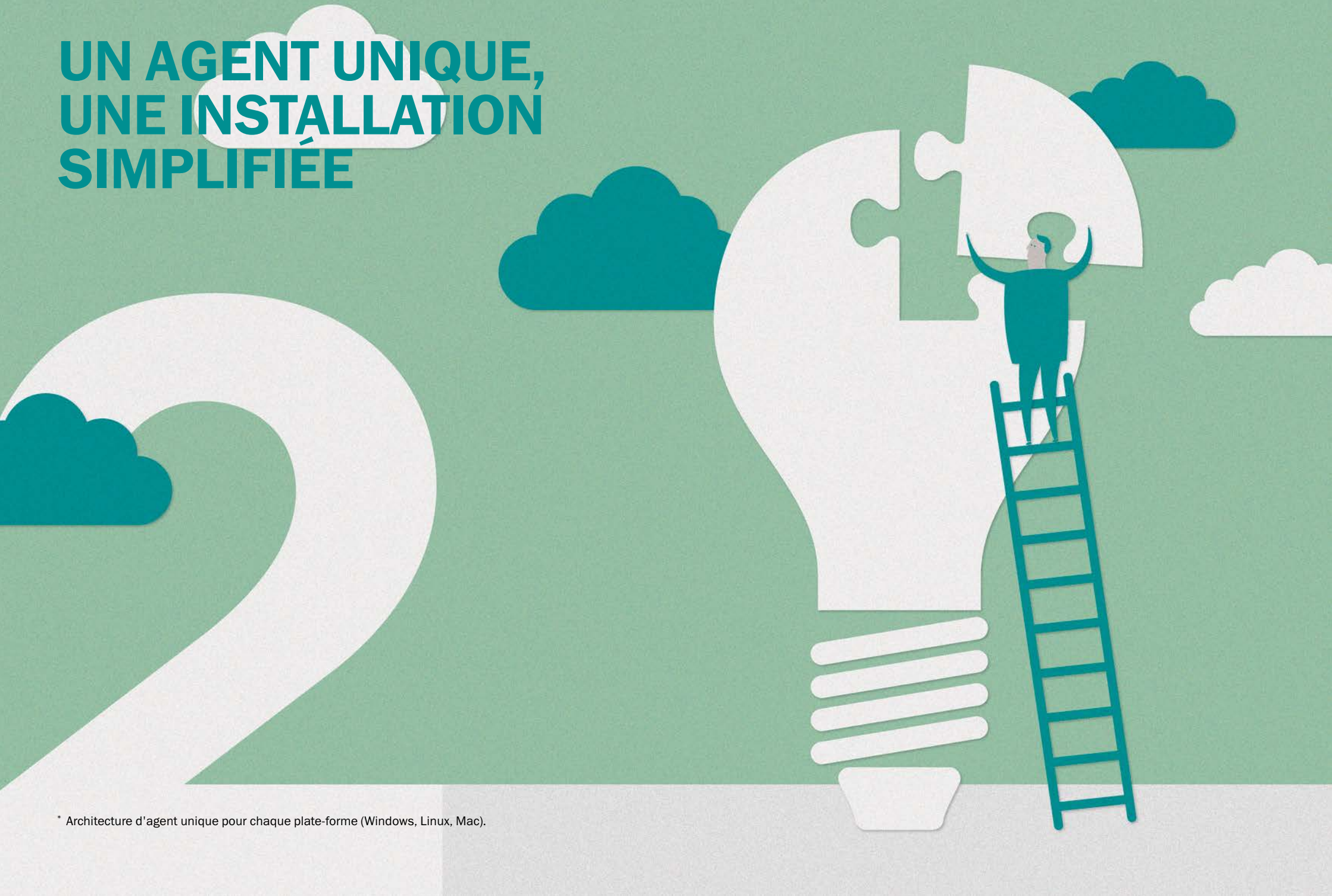
Avantages :

- **Rapidité et facilité du déploiement :** le serveur de gestion, l'installation de la console et le processus de configuration permettent de bénéficier d'une fonctionnalité complètement intégrée, prête à l'emploi.

- **Un unique serveur physique de gestion :** vous n'avez plus à gérer différents matériels, systèmes ou composants supplémentaires pour chaque serveur et console d'administration. La solution Kaspersky Lab ne requiert qu'un serveur UNIQUE pour la majorité des déploiements.

- **Un unique logiciel de gestion :** facilité de gestion de l'infrastructure pour les petites entreprises tout en offrant la possibilité de procéder à des déploiements à plus grande échelle.
  — Certains produits nécessitent l'installation d'autres packages suite au déploiement initial pour ne proposer, au final, que des fonctionnalités similaires à celles de Kaspersky Lab.
  — Pour davantage de confort, la plate-forme Kaspersky Lab intègre des applications supplémentaires (par ex. celles requises dans un environnement Microsoft) dans le cadre du processus d'installation et d'auto-installation, ce qui permet de gagner du temps et d'éviter les problèmes. Cela fonctionne, tout simplement.

UN AGENT UNIQUE, UNE INSTALLATION SIMPLIFIÉE



* Architecture d'agent unique pour chaque plate-forme (Windows, Linux, Mac).

2 UN AGENT UNIQUE, UNE INSTALLATION SIMPLIFIÉE

La solution de Kaspersky Lab est unique car elle propose un agent au niveau des terminaux qui tire parti de l'intégration de code avancée afin de garantir une compatibilité et une synergie totales et simples sur des configurations matérielles et logicielles.

Les véritables plates-formes de protection des terminaux disposent d'une architecture simple, permettant ainsi de réduire la complexité et d'approfondir l'intégration en utilisant un minimum d'agents pour exécuter les tâches. Les fonctions connexes telles que l'analyse des vulnérabilités, les mises à jour d'applications et les correctifs ainsi que les modules de protection contre les programmes malveillants et de chiffrement bénéficient d'une architecture d'agent unique rationalisant ainsi les performances tout en réduisant vos activités de gestion.

De nombreuses offres concurrentes nécessitent plusieurs agents sur la même machine pour gérer les fonctions telles que l'application des correctifs, le contrôle ou le chiffrement des applications, engendrant ainsi des risques de problèmes liés à la compatibilité des agents et des tests complémentaires.

* Architecture d'agent unique pour chaque plate-forme (Windows, Linux, Mac).

Avantages :

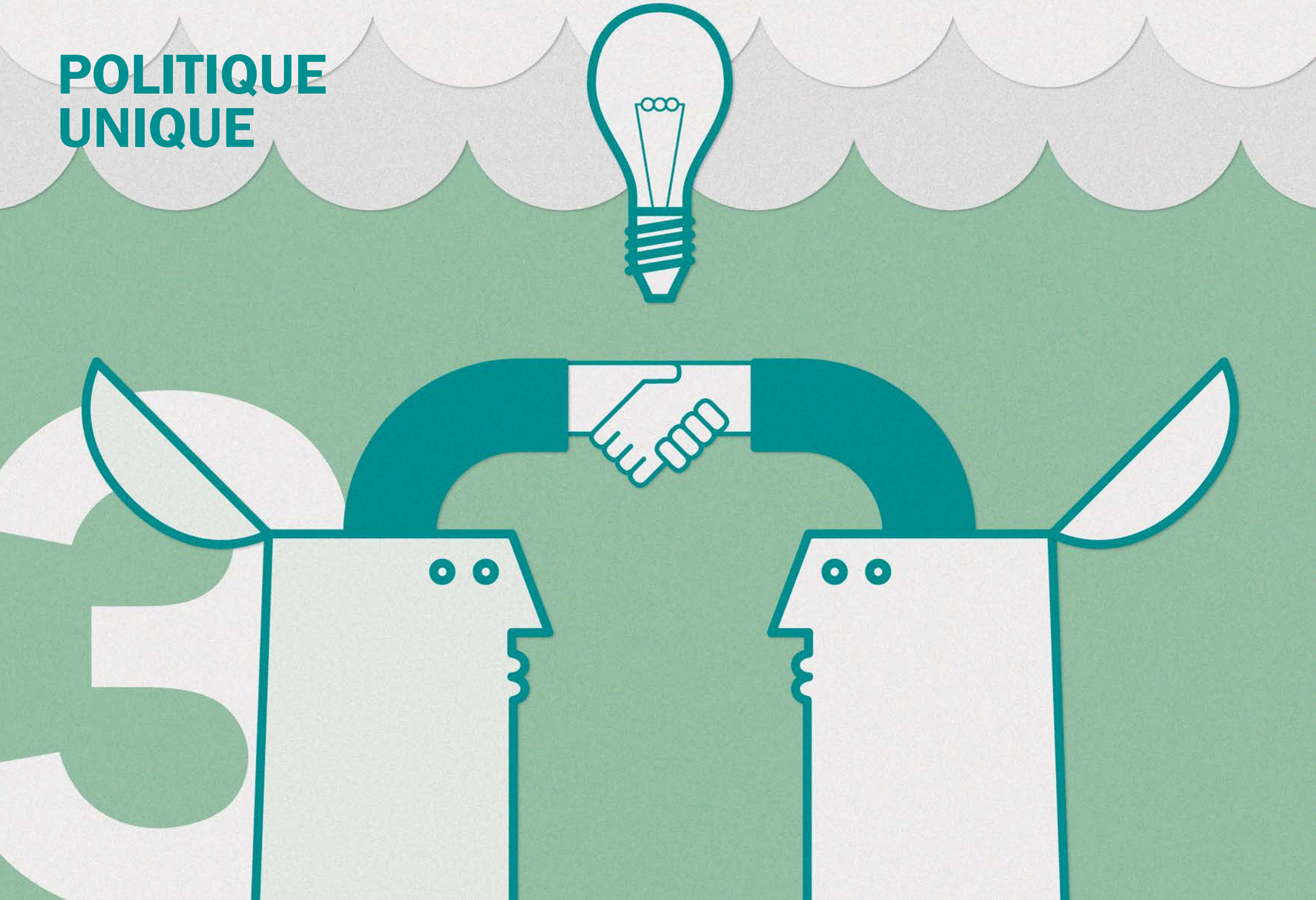
- **Gain de temps sur le déploiement initial et les mises à jour :** il suffit d'une simple installation pour les contrôler, sans aucune dépendance, ni obligation de lancer de nombreux redémarrages.

- **Plus de préoccupation quant à la configuration requise :** nul n'ignore que la croissance reposant sur des acquisitions de produits génère des problèmes de compatibilité logicielle. Outre le logiciel fourni, une fonctionnalité préassemblée peut nécessiter une prise en charge nouvelle et distincte. Il est dommage que vous n'ayez découvert cela qu'au début du déploiement... Seule une approche de développement intégrée et organique peut garantir une parfaite compatibilité des différents composants logiciels en matière de plates-formes de terminaux/d'appareils gérés. Cela se traduit également par moins de tests de compatibilité pour le client.

- **Impact réduit :** sur les performances système et la gestion.

- **Développement de nouvelles synergies :** l'intégration avancée favorise la flexibilité et des fonctionnalités supplémentaires. Développez vos capacités sans augmenter vos ressources.

POLITIQUE UNIQUE



3 POLITIQUE UNIQUE

La complexité est l'ennemi de la sécurité, mais gérer tous les aspects de la sécurité de l'information au sein d'une organisation implique généralement la gestion de solutions multiples très différentes. Plus vous simplifiez les processus de gestion, plus vous bénéficiez de visibilité et réduisez les risques.

Une véritable plate-forme de protection des terminaux contrôle la détection, le déploiement, la configuration de la politique et la mise à jour des terminaux dans l'ensemble de l'infrastructure de l'entreprise. L'agent unique dédié à chaque plate-forme de la solution Kaspersky Endpoint Security permet aux administrateurs de définir une politique active pour un groupe géré couvrant tous les composants requis mais sans avoir à vérifier ou à mettre en relation plusieurs politiques.

Network Agent connecte le terminal au serveur d'administration en exécutant des tâches de gestion des systèmes (par ex. inventaire logiciel et matériel, analyse des vulnérabilités et gestion des correctifs), offrant ainsi flexibilité et synergie réelles entre les fonctions.

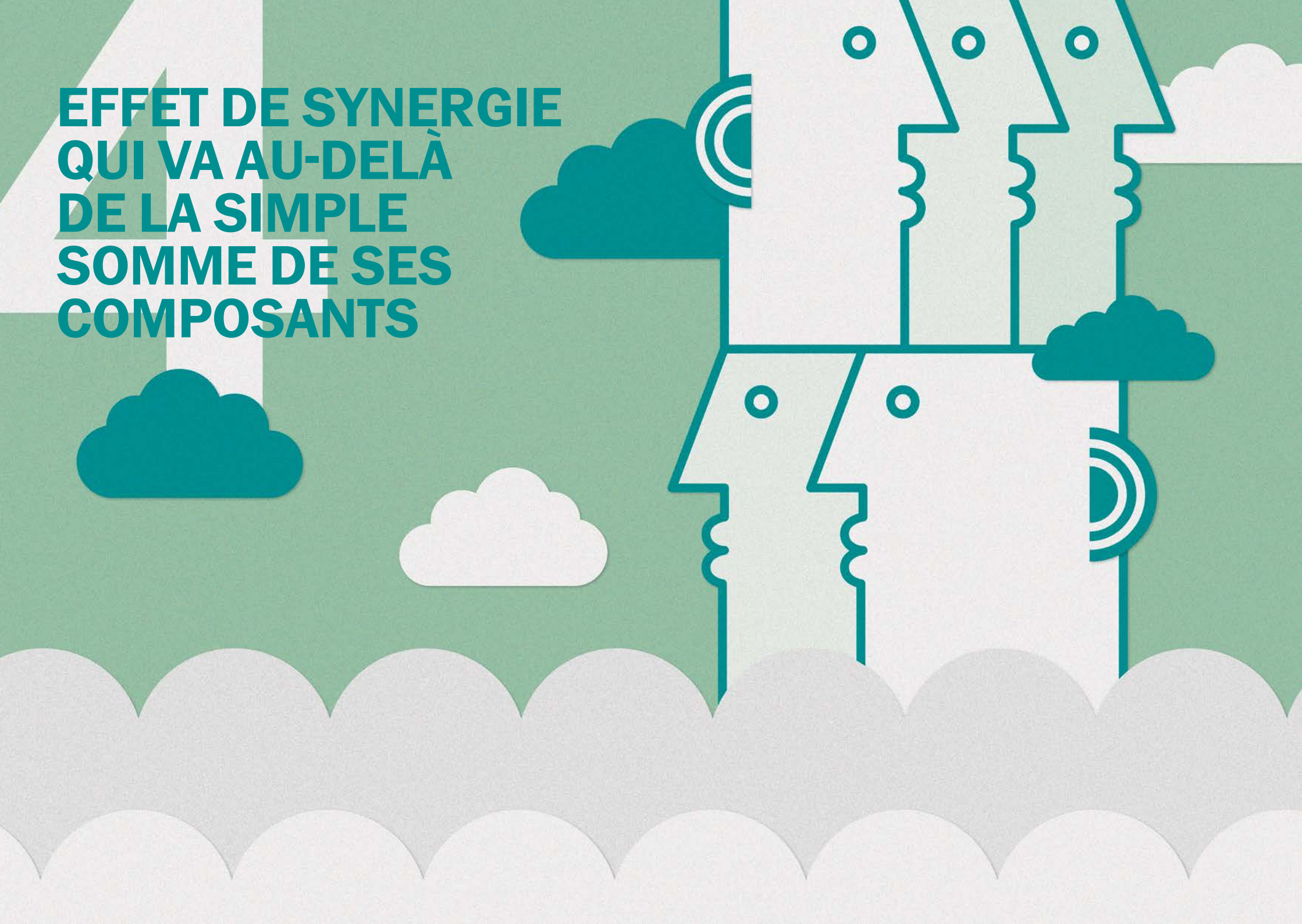
Avantages :

- **Gestion simplifiée de la politique et des tâches :** un seul ensemble de paramètres et de conditions communes (groupes gérés, paramètres de déploiement et notifications) permet d'optimiser la mise en œuvre de la politique, éliminant ainsi les processus et les tâches redondantes pour l'administrateur informatique.

- **Contrôle de la politique et de la mise en œuvre en toute simplicité :** un tableau de bord unique et des rapports relatifs au déploiement et à l'exécution permettent d'obtenir un aperçu complet et synthétique de l'état de la politique et de la conformité sur l'ensemble du réseau.

- **Simplicité des modifications de la politique et des tâches :** les modifications sont réalisées en une seule étape. L'attribution automatique de la politique peut couvrir plusieurs paramètres de sécurité en une seule fois, de la protection au contrôle des applications, des appareils et du Web, ainsi que les politiques de chiffrement.

EFFET DE SYNERGIE QUI VA AU-DELÀ DE LA SIMPLE SOMME DE SES COMPOSANTS



4 EFFET DE SYNERGIE QUI VA AU-DELÀ DE LA SIMPLE SOMME DE SES COMPOSANTS

Les fonctionnalités intégrées de la solution de protection des terminaux sont au cœur de la plate-forme de protection des terminaux de Kaspersky Lab. Elles permettent de faciliter la mise en œuvre de scénarios de sécurité avancés, voire complexes. Une intégration réelle offre une sécurité qui va au-delà des composants de chaque fonctionnalité, par exemple :

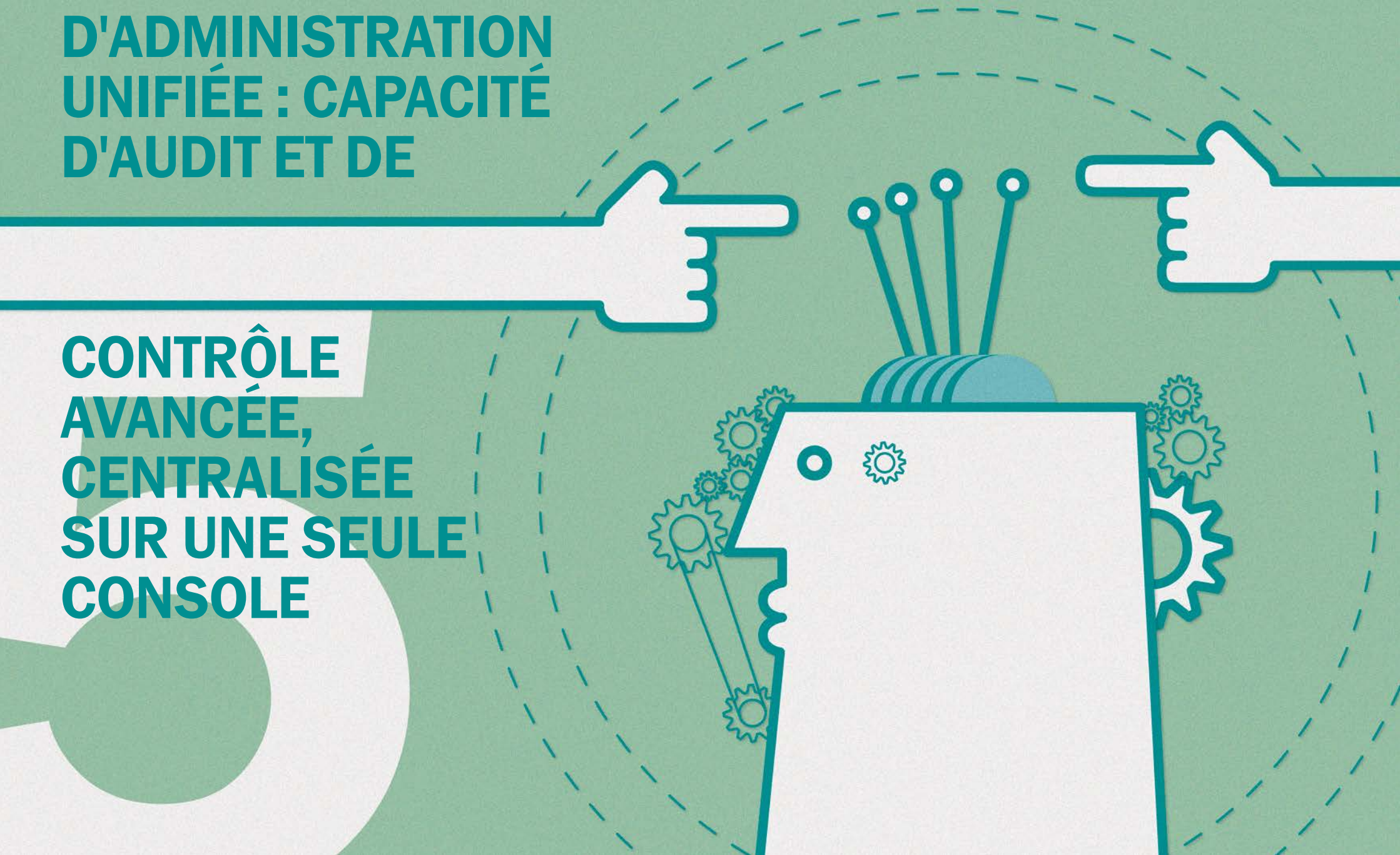
Pour mettre en œuvre une protection intégrale contre les cyber-menaces tout en analysant le trafic Web et les fichiers téléchargés, une entreprise peut s'appuyer sur la fonctionnalité de contrôle des applications de Kaspersky Lab pour imposer l'utilisation d'un seul navigateur approuvé par le service informatique.
Ce navigateur peut, à son tour, être davantage sécurisé, en appliquant automatiquement des correctifs de vulnérabilité de haute priorité, et protégé contre les attaques zero-day grâce à la prévention automatique des failles d'exploitation. Les fonctionnalités intégrées de Kaspersky Lab permettent ainsi de bénéficier d'une couche de sécurité contre un vecteur d'attaque très large. C'est que nous entendons par effet de synergie.

Avantages :

- **Partage des pratiques en matière de gestion de la sécurité et d'informations recueillies à partir de fonctions différentes, notamment :**
  — des informations relatives aux appareils mobiles sont utilisées pour contrôler et chiffrer les appareils ;
  — des informations relatives aux applications contribuent à leur contrôle et aux politiques de chiffrement ;
  — gestion des appareils mobiles (MDM) intégrée à la sécurité des données sur les appareils ;
  — les décisions en matière de gestion des correctifs peuvent être basées sur l'évaluation des vulnérabilités.

L'effet de synergie ne se limite pas aux scénarios décrits ci-dessus. L'intégration des codes avancée garantit une compatibilité et une synergie totales et simples sur des configurations matérielles et logicielles. Grâce à la plate-forme de Kaspersky Lab, la sécurité va au-delà des composants de chacune des fonctionnalités.

GESTION DES DROITS D'ADMINISTRATION UNIFIÉE : CAPACITÉ D'AUDIT ET DE CONTRÔLE AVANCÉE, CENTRALISÉE SUR UNE SEULE CONSOLE



5 GESTION DES DROITS D'ADMINISTRATION UNIFIÉE : CAPACITÉ D'AUDIT ET DE CONTRÔLE AVANCÉE, CENTRALISÉE SUR UNE SEULE CONSOLE

Le manque de personnel dans les services informatiques est un problème courant pour de nombreuses PME et entreprises. Le ralentissement économique et l'informatique toujours plus complexe contraignent les administrateurs informatiques à exécuter davantage de tâches en moins de temps.

La plate-forme de protection des terminaux de Kaspersky Lab offre une solution à cette problématique en fournissant des outils de gestion unifiés pour les tâches de sécurité quotidiennes. L'intégration avancée permet de contrôler les privilèges et de gérer les journaux à partir d'une seule et même console. Un journal enregistre toutes les activités, contrairement aux produits concurrents qui doivent la plupart du temps extraire des données de consoles et de serveurs distincts.

La gestion des droits et la journalisation unifiée permettent de contrôler plus efficacement et de bénéficier d'une meilleure visibilité des activités du personnel, contribuant ainsi à une gestion plus performante des autorisations. Résultat : sécurité et contrôle renforcés des opérations et de la gestion informatiques à partir d'une seule et même console.

Avantages :

- **Simplicité pour définir et contrôler les autorisations :** dans une PME classique où l'expert en informatique s'occupe de tout, l'exécution des tâches liées à la sécurité doit être simple, y compris définir les autorisations en matière de lecture/modification, d'accès, etc.

- **Intervention rapide face aux incidents et historique des activités unifié :** après tout, les administrateurs informatiques sont des êtres humains et l'erreur est également humaine. Aussi, en cas d'incident de sécurité, il est essentiel de réagir dans les plus brefs délais. Une fonctionnalité permettant de modifier ou de bloquer rapidement des accès est indispensable, outre la capacité à suivre ces changements. Avec des solutions distinctes, des incidents complexes peuvent nécessiter la création de processus d'analyse multiples. Kaspersky Lab simplifie cette tâche en gérant l'ensemble des modifications apportées à la sécurité des terminaux, aux politiques et aux activités de gestion dans un seul et même fichier journal et ce, à partir d'une console de gestion unique.

STRUCTURE ET PRÉSENTATION COMMUNES : RAPIDITÉ ET SIMPLICITÉ DES RAPPORTS

6 STRUCTURE ET PRÉSENTATION COMMUNES : RAPIDITÉ ET SIMPLICITÉ DES RAPPORTS

Les administrateurs sous pression saisiront toutes les opportunités qui se présenteront pour gagner du temps ou simplifier l'exécution d'une tâche. Les plates-formes de protection des terminaux disposant de fonctionnalités intégrées et unifiées ainsi que d'une interface commune facilitent la gestion des rapports, des analyses et des incidents : Kaspersky Security Center génère une structure de rapports similaire, présentés dans un format courant.

La journée de travail d'un administrateur informatique se traduit généralement par une grande quantité de tâches routinières mais vitales, qui doivent toutes être contrôlées et faire l'objet de rapports. Dans un environnement de solutions mixtes, cela implique un nombre varié de tableaux de bord générant des rapports dans différents formats : PDF, HTML ou email. Qui a le temps de tous les consulter ET de s'assurer que tout fonctionne correctement ?

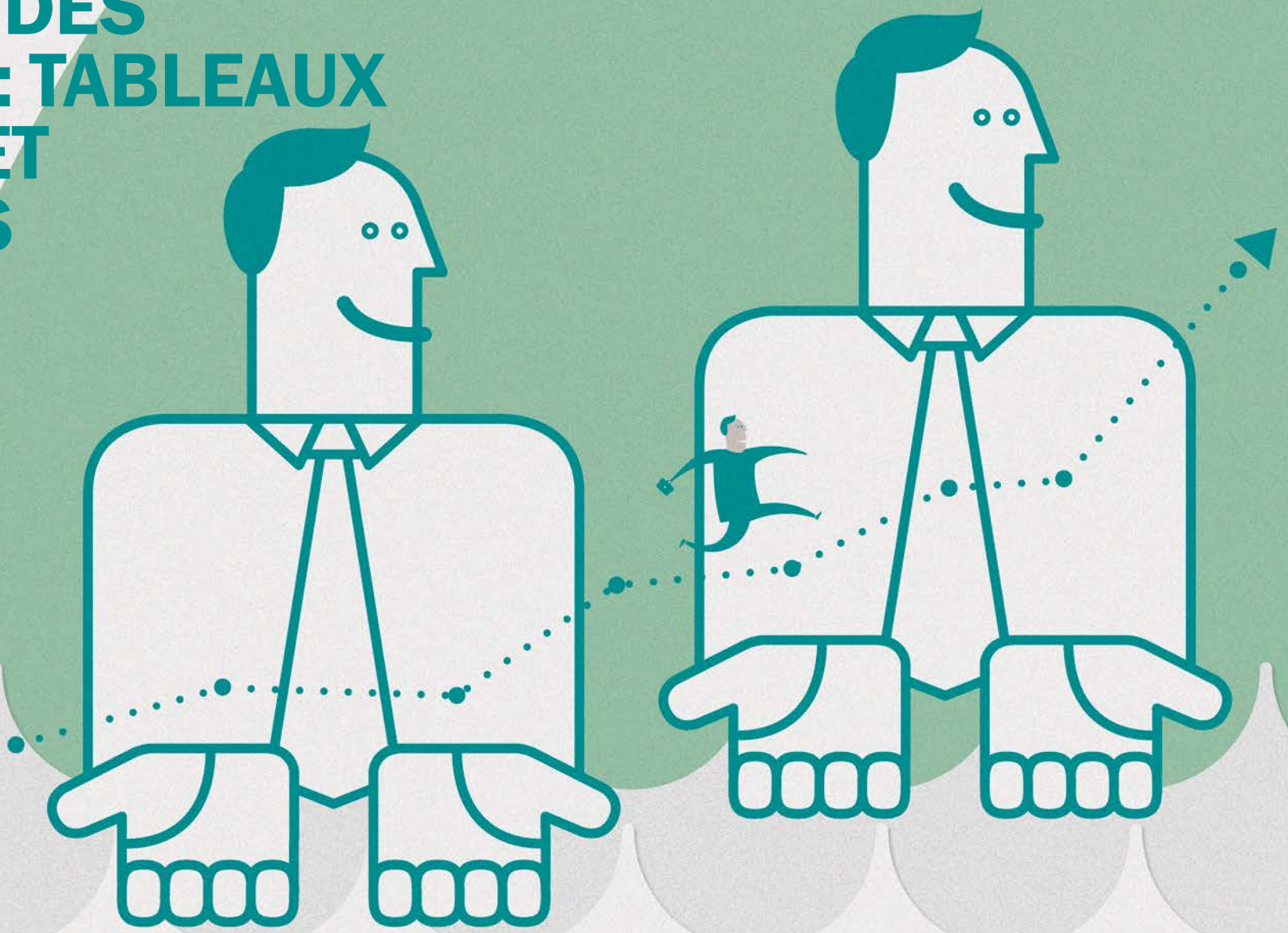
Dans cet environnement, même l'amélioration la plus infime en termes de convivialité ou d'efficacité permet de gagner beaucoup de temps et de réduire la charge de travail des administrateurs de la sécurité informatique déjà débordés. Des rapports présentés dans un format courant peuvent faciliter l'analyse et l'évaluation, améliorant ainsi la gestion des incidents tout en favorisant une approche proactive de la sécurité informatique.

Avantages :

- **Plus de simplicité et de rapidité dans l'analyse des rapports :** les modèles de rapport utilisent la même terminologie et structure. Ordinateur, PC, nœud, machine sont tous assimilés au même terminal et indifféremment utilisés dans la documentation produits et fournisseurs. Le simple fait d'ajouter d'autres produits risque de compliquer la situation. Que se passerait-il si chacun des composants de sécurité de votre environnement de solutions mixtes avait le même problème de langage ? Que se passerait-il si tous les paramètres de chacun de ces composants avaient des noms similaires simplement différents ? Dans un tel environnement complexe, l'évaluation des menaces ou d'autres incidents devient beaucoup plus compliquée que nécessaire, même pour des administrateurs habitués à cette configuration. Pour ces derniers, il ne suffit pas d'accepter la complexité. Qu'en est-il en cas d'intervention d'auditeurs ou de régulateurs externes ? Leur présenter une vue d'ensemble confuse de votre infrastructure risque de donner une mauvaise impression.

- **Gestion simplifiée des incidents :** identifiez facilement des incidents similaires dans différents nœuds de l'infrastructure informatique tels que des programmes malveillants ou des violations de politique.

MEILLEURE VISIBILITÉ DES DONNÉES : TABLEAUX DE BORD ET RAPPORTS INTÉGRÉS



7 MEILLEURE VISIBILITÉ DES DONNÉES : TABLEAUX DE BORD ET RAPPORTS INTÉGRÉS

Les plates-formes de protection des terminaux doivent offrir une approche globale des tableaux de bord et des rapports. Une véritable intégration va au-delà de l'interface. Par exemple, cliquer sur un onglet unique de type « propriétés des terminaux » dans une console d'administration doit permettre d'obtenir des informations relatives à tous les aspects de la sécurité du client géré, notamment les politiques mises en œuvre, les mises à jour des statuts et les incidents.

Les tableaux de bord et les rapports doivent également faciliter le processus d'enquête et fournir une meilleure visibilité du terminal. L'intégration permet de recueillir des informations sur plusieurs composants, et ce en toute simplicité.

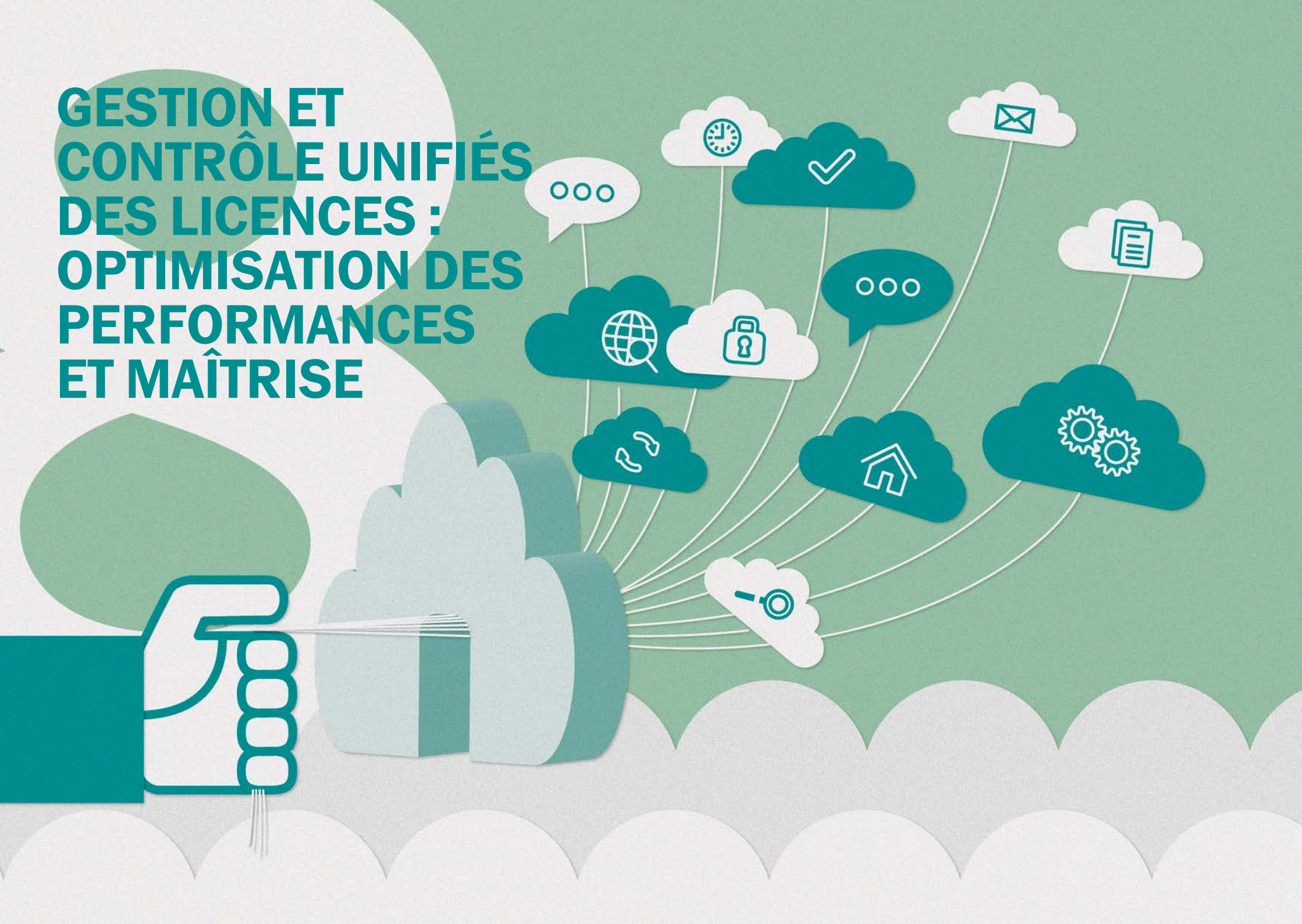
Avantages :

- **Centralisation de tous les composants de sécurité des terminaux :** un tableau de bord synthétique et immédiatement accessible inclut les principales informations relatives à l'état des terminaux gérés, à l'exécution des tâches de déploiement et au contrôle des licences ainsi qu'aux événements et incidents majeurs liés à la sécurité.

- **Simplicité de l'examen et de l'analyse :** explorez des rapports interdépendants afin d'analyser et de recueillir des données sous différents angles, notamment la gestion des terminaux, l'évaluation des vulnérabilités, l'application des correctifs, l'inventaire matériel et des applications ainsi que les comptes d'utilisateurs créés. Bénéficiez d'une visibilité de l'état de la protection et des incidents, y compris en matière de détection des programmes malveillants et d'état du chiffrement des données. Ceci facilitera le processus d'analyse et d'évaluation de la sécurité.

- **Rapports analytiques prêts à l'emploi :** les rapports analytiques sont un élément clé des responsabilités d'un administrateur de la sécurité informatique. Générer des rapports complets à partir de plusieurs consoles et jeux de données prend du temps et représente un vrai casse-tête. C'est la raison pour laquelle la plate-forme de sécurité des terminaux de Kaspersky Lab propose des rapports analytiques clés en main. Plus besoin d'utiliser des rapports personnalisés à l'aide d'outils tiers. Vous disposez ainsi de davantage de temps pour d'autres projets.

GESTION ET CONTRÔLE UNIFIÉS DES LICENCES : OPTIMISATION DES PERFORMANCES ET MAÎTRISE



8 GESTION ET CONTRÔLE UNIFIÉS DES LICENCES : OPTIMISATION DES PERFORMANCES ET MAÎTRISE

La gestion des licences pour toutes les solutions de sécurité installées sur l'ensemble du réseau d'entreprise n'a jamais été aussi simple. Grâce à Kaspersky Lab, une seule licence permet d'activer toutes les fonctionnalités, sans exception : sécurité des terminaux, protection des données, gestion des appareils mobiles et des systèmes.

Cette licence unique est facilement distribuée vers l'ensemble des terminaux d'entreprise, indépendamment de l'état ou du site : machines virtuelles ou physiques sur tous les réseaux, fixes ou mobiles. La fonctionnalité de gestion des licences intégrée de Kaspersky Lab vous permet d'utiliser plus efficacement ce que vous achetez tout en contrôlant plus strictement la validité des licences.

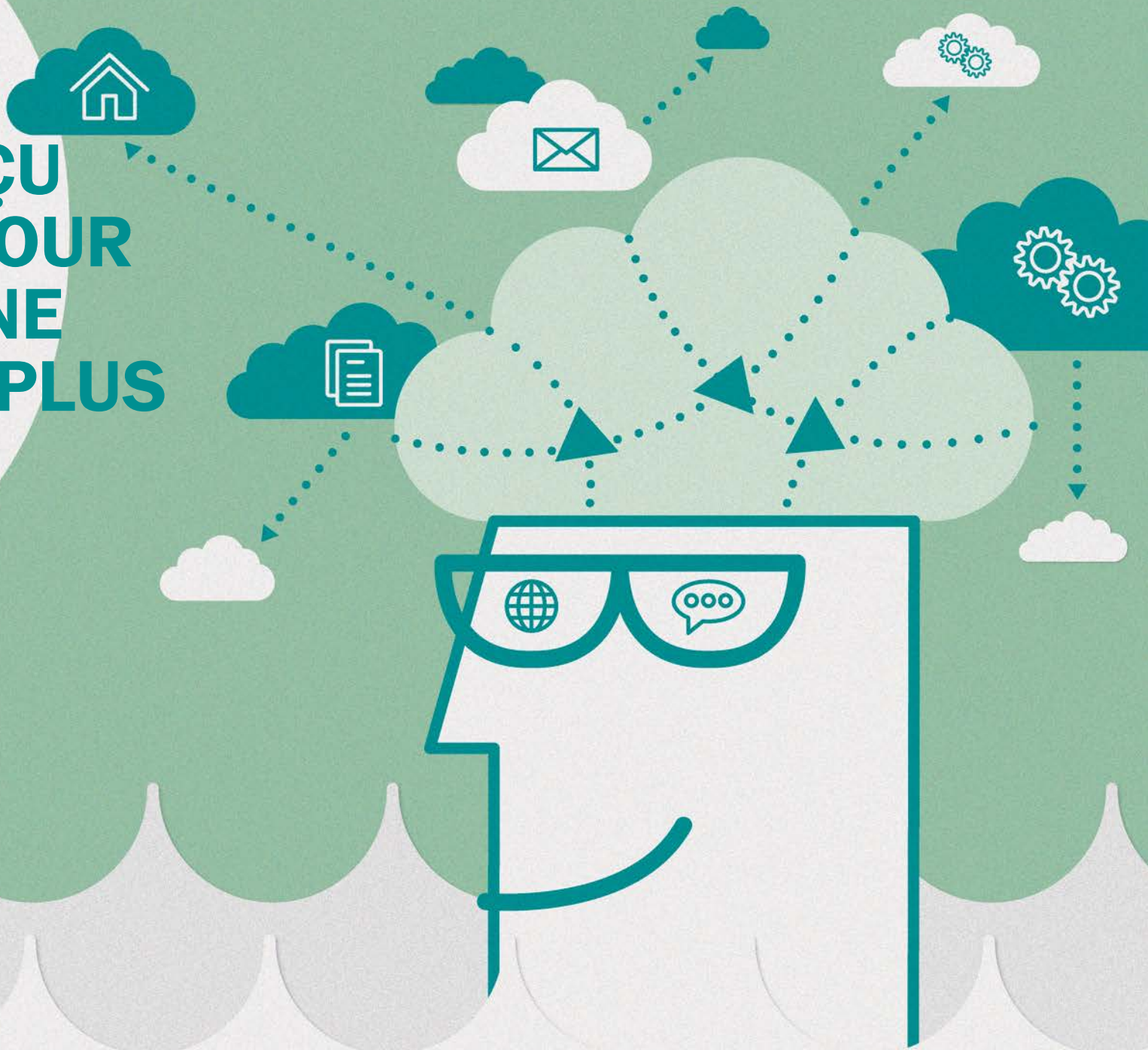
Avantages :

- **Centralisation de l'audit des licences :** il n'est plus nécessaire de s'appuyer sur des outils de contrôle des licences différents pour surveiller et vérifier leur état.

- **Efficacité d'utilisation des licences :** réduisez les coûts en distribuant les licences de manière souple vers votre environnement informatique à mesure qu'il évolue. Par exemple, lors de la migration des PC et ordinateurs portables traditionnels vers des appareils mobiles à l'aide d'une fonctionnalité simultanée.

- **Simplicité de mise à niveau de votre solution de sécurité :** la plate-forme de protection des terminaux de Kaspersky Lab permet de renforcer la sécurité selon vos besoins. Commencez par la sécurité des terminaux, puis activez les fonctionnalités telles que le chiffrement ou la gestion des systèmes en ajoutant une nouvelle licence.

UN CODE UNIQUE, CONÇU EN INTERNE POUR FAVORISER UNE INTÉGRATION PLUS AVANCÉE



9 UN CODE UNIQUE, CONÇU EN INTERNE POUR FAVORISER UNE INTÉGRATION PLUS AVANCÉE

Le code unique de Kaspersky Lab, conçu et géré en interne, est au cœur de notre plate-forme de protection des terminaux intégrée.

Alors que d'autres fournisseurs adoptent des stratégies d'acquisition pour accroître leur offre produits face à l'évolution rapide des menaces, Kaspersky Lab est le seul à développer et à gérer le tout en interne. Contrairement à d'autres fournisseurs, ceci permet de prendre en charge une intégration avancée à partir du code, permettant ainsi de vous faire bénéficier des nombreux avantages mentionnés précédemment dans ce document.

Avantages :

- Serveur de gestion et console d'administration uniques ;
- Architecture client-terminal unique ;
- Politiques uniques et gestion unifiée ;
- Effet de synergie de la fonctionnalité intégrée ;
- Tableaux de bord et rapports intégrés.

Le même code et processus de développement accélère les mises à jour ainsi que l'application des correctifs. Ainsi, les utilisateurs de Kaspersky Lab sont en mesure de mettre à jour une seule et même application (ainsi que ses composants) alors que d'autres produits concurrents requièrent cette opération sur une ou plusieurs applications.

MODÈLE D'ACHAT INTÉGRÉ : UN SEUL ACHAT PERMET DE BÉNÉFICIER DE L'ENSEMBLE DES FONCTIONNALITÉS DONT VOUS AVEZ BESOIN

10 MODÈLE D'ACHAT INTÉGRÉ : UN SEUL ACHAT PERMET DE BÉNÉFICIER DE L'ENSEMBLE DES FONCTIONNALITÉS DONT VOUS AVEZ BESOIN

Une seule commande couvre l'ensemble de vos besoins en matière de sécurité et de fonctionnalités. Une licence unique active le tout.

Avantages :

- **Un package unique pour répondre à des besoins différents :** un seul pack de licence permet aux utilisateurs de Kaspersky Lab de bénéficier de niveaux et de variantes différentes en termes de fonctionnalités intégrées pour répondre ainsi à leurs besoins. C'est exceptionnel.

RÉSULTAT...

Grâce à Kaspersky Lab, les utilisateurs bénéficient d'une véritable plate-forme de protection des terminaux développée de bout en bout en s'appuyant sur le même code et la même R&D. Nos technologies intégrées en matière de protection contre les programmes malveillants et les vulnérabilités logicielles sont élaborées par notre groupe de recherche interne et dédié qui étudie en permanence comment les nouvelles menaces pénètrent les systèmes afin de développer une protection plus efficace.

Le groupe de recherche des vulnérabilités et de liste blanche de Kaspersky Lab gère notre écosystème de partenaires et de fournisseurs, offrant ainsi une base de données de logiciels légitimes constamment mise à jour tout en fournissant les informations les plus récentes sur les correctifs disponibles.

La convergence de la sécurité des terminaux et de la technologie de gestion des systèmes/clients est une tendance qui ne cesse d'évoluer. Grâce à son code et son processus de développement internes, Kaspersky Lab est en mesure d'exploiter les synergies évidentes entre les fonctions de sécurité et celles traditionnellement considérées comme des composantes de la gestion des systèmes.

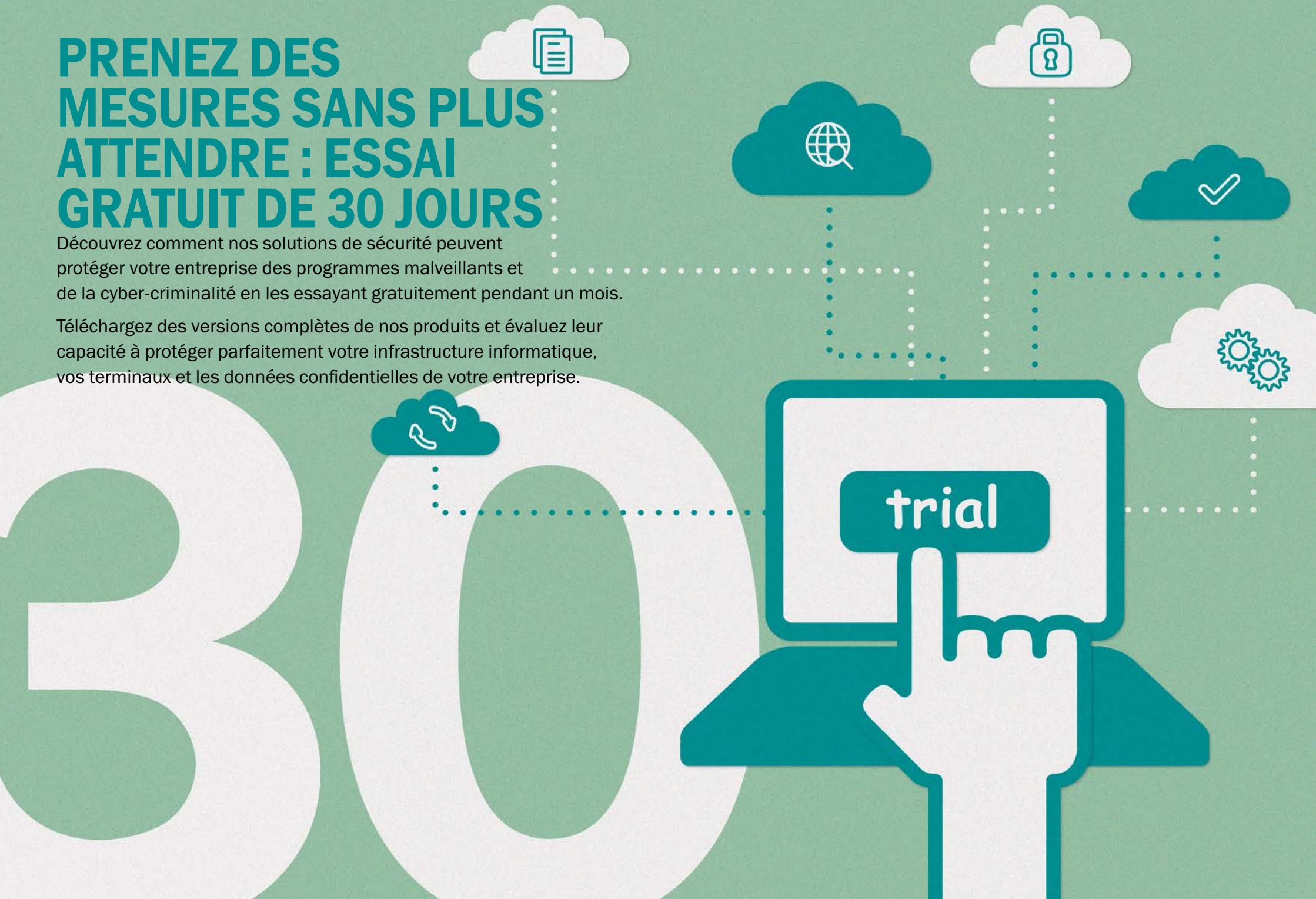
L'intégration de Kaspersky Lab propose une véritable plate-forme de protection des terminaux. La protection doit être optimale et pas facultative.

En savoir plus sur **http://www.kaspersky.com/fr/business-security**

PRENEZ DES MESURES SANS PLUS ATTENDRE : ESSAI GRATUIT DE 30 JOURS

Découvrez comment nos solutions de sécurité peuvent protéger votre entreprise des programmes malveillants et de la cyber-criminalité en les essayant gratuitement pendant un mois.

Téléchargez des versions complètes de nos produits et évaluez leur capacité à protéger parfaitement votre infrastructure informatique, vos terminaux et les données confidentielles de votre entreprise.



À PROPOS DE KASPERSKY LAB

Kaspersky Lab est le plus grand éditeur privé mondial de solutions de protection des terminaux. La société fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité pour utilisateurs de terminaux informatiques*. Depuis plus de 17 ans, Kaspersky Lab fait figure de précurseur dans le domaine de la sécurité informatique, fournissant des solutions de sécurité numérique efficaces aux grandes entreprises, PME et particuliers. Kaspersky Lab, dont la holding est enregistrée au Royaume-Uni, opère actuellement dans près de 200 pays et territoires du monde entier et offre une protection à plus de 300 millions d'utilisateurs.
Plus d'informations sur **www.kaspersky.com**.

* L'entreprise est classée quatrième fournisseur mondial de solution de sécurité des terminaux, en termes de chiffre d'affaires, par IDC en 2012. Ce classement a été publié dans le rapport IDC « Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares » (Sécurité des terminaux dans le monde : prévisions pour 2013-2017 et parts de marché des fournisseurs en 2012), document numéro 242618, août 2013. Ce rapport classait les éditeurs de logiciels selon leurs revenus provenant des ventes de solutions de sécurité des terminaux en 2012.

RETROUVEZ-NOUS SUR LES RÉSEAUX SOCIAUX

#securebiz

Visionnez nos vidéos sur YouTube	Découvrez nos présentations sur Slideshare	Rejoignez nos fans sur Facebook	Découvrez notre blog	Suivez-nous sur Twitter	Rejoignez-nous sur LinkedIn

KASPERSKY lab