

Lumension® Intelligent Whitelisting™

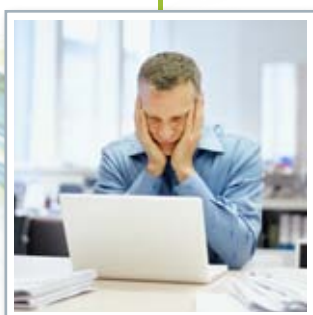


Une solution de sécurité des postes de travail plus efficace, flexible et facile à gérer qui réduit le risque lié aux programmes malveillants et le coût total de possession des postes de travail, sans nuire à la productivité de l'entreprise

Dans l'environnement dynamique des menaces actuelles, les entreprises sont de plus en plus vulnérables aux attaques de programmes malveillants ciblés et sophistiqués conçus par des cybercriminels motivés par l'argent.

Pour répondre aux exigences de ce nouvel environnement, les entreprises doivent s'assurer d'un meilleur contrôle centralisé sur les configurations des postes de travail afin d'améliorer leur état de sécurité, sans affecter la productivité des utilisateurs finaux.

Facteurs déterminants et difficultés de la sécurité des postes de travail



Dans l'environnement informatique décentralisé, mobile et connecté en permanence d'aujourd'hui, les postes de travail sont plus difficiles à gérer, sécuriser et contrôler que jamais, car les utilisateurs finaux bénéficient souvent de privilèges d'administrateur local dont ils se servent allégrement pour télécharger des applications tierces indésirables ou non autorisées sur les postes de travail. Les entreprises sont par ailleurs confrontées à la menace croissante d'un volume de plus en plus élevé de programmes malveillants ciblés et sophistiqués conçus pour contourner les défenses de sécurité traditionnelle telles que les produits antivirus. Il en résulte que les professionnels de l'informatique se sentent moins protégés aujourd'hui qu'il y a encore à peine un an.

La montée exponentielle incessante des programmes malveillants et l'inefficacité croissante des antivirus traditionnels ont conduit à une augmentation des coûts de résolution, de réponse aux incidents et de service d'assistance informatique, à l'heure où l'entreprise lambda signale aujourd'hui plus de 50 incidents par mois liés à des programmes malveillants qui affectent la productivité¹. Si l'antivirus continue de faire partie de l'arsenal de protection des postes de travail, il n'est plus efficace en tant que technologie autonome et accroît le coût total de possession du poste de travail.

- » L'antivirus ne peut pas suivre le rythme, avec près de 1,6 million de nouvelles instances de programmes malveillants identifiées par mois, et ne peut pas offrir une protection contre les menaces non répertoriées ou mixtes².
- » L'antivirus ne donne pas la visibilité nécessaire sur les applications tierces installées et exécutées sur les postes de travail, et n'aide pas à maintenir des configurations de sécurité centralisées.
- » L'antivirus ne peut pas contrôler les actions des utilisateurs disposant de privilèges d'administrateur local, ni empêcher l'introduction d'applications indésirables.

La liste blanche ou le contrôle des applications constitue une approche de sécurité des postes de travail éprouvée qui change la donne. Au lieu d'essayer d'identifier tous les programmes malveillants qui existent (une tâche impossible dans l'environnement des menaces actuel), la liste blanche des applications identifie les logiciels nécessaires aux opérations de l'entreprise et autorise uniquement les applications approuvées par le département informatique à s'exécuter sur le poste de travail. Toutefois, les technologies autonomes traditionnelles de liste blanche et de contrôle des applications ne peuvent pas offrir la flexibilité et l'efficacité opérationnelle requises par le département informatique pour gérer les postes de travail dans un environnement dynamique.

[Lumension® Intelligent Whitelisting™](#) combine l'efficacité de la sécurité renforcée de la liste blanche et du contrôle des applications avec la flexibilité des règles automatisées de gestion des changements basée sur la confiance. L'implémentation et la gestion sont ainsi facilitées pour le département informatique, tant dans les environnements dynamiques que verrouillés, tout en garantissant à l'entreprise productivité et agilité.

1. Ponemon Institute, État des lieux du risque pour les postes de travail (novembre 2010)
2. McAfee Labs, Rapport sur les menaces : troisième trimestre 2010 (novembre 2010)

Lumension® Intelligent Whitelisting™, qui fait partie de l'offre [Lumension® Endpoint Management and Security Suite](#), est la première solution de sécurité des postes de travail intelligente de l'industrie qui permet aux entreprises d'allier l'efficacité des solutions antivirus à l'efficacité opérationnelle et la sécurité optimisées de la gestion des correctifs logiciels, de la liste blanche et du contrôle des applications. En combinant [Lumension® AntiVirus](#), [Lumension® Application Control](#) et [Lumension® Patch and Remediation](#) dans un flux de travail unifié et entièrement intégré, Lumension permet au département informatique d'offrir une sécurité des postes de travail nettement renforcée sans nuire à la productivité opérationnelle.

Sécurité des postes de travail opérationnelle et efficace pour les environnements dynamiques

Avec *Lumension*® Intelligent Whitelisting™ :

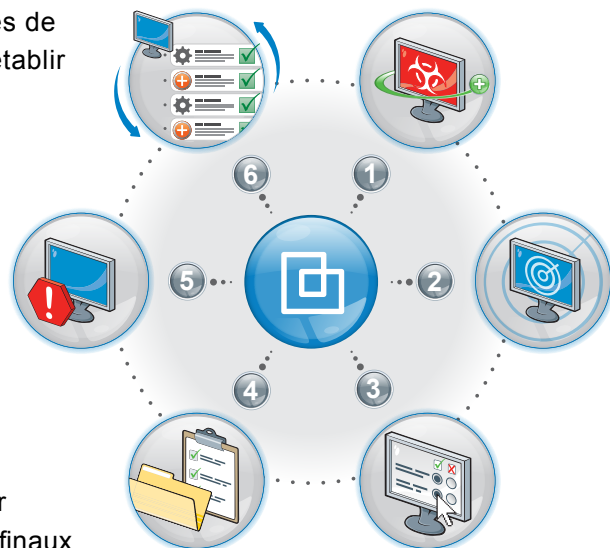
- » **Améliorez la sécurité de vos postes de travail** et bloquez les attaques ciblées et non répertoriées via une stratégie de défense approfondie qui n'autorise que les fichiers exécutables connus et sûrs à s'exécuter sur les postes de travail.
- » **Reprenez le contrôle de vos postes de travail** en réduisant le risque lié aux administrateurs locaux. Les utilisateurs finaux dotés de droits d'administrateur local peuvent en effet introduire des niveaux élevés de risque lié aux configurations, vulnérabilités et applications, et laisser des brèches que les attaques non répertoriées et autres programmes malveillants peuvent exploiter.
- » **Offrez un contrôle et une liste blanche des applications flexibles, efficaces et conviviaux.** Contrairement aux produits autonomes traditionnels de contrôle des applications, la solution de liste blanche intelligente intégrée de Lumension offre une flexibilité accrue en permettant au département informatique de gérer efficacement le changement basé sur la confiance au sein d'un environnement de postes de travail dynamique.
- » **Augmentez votre productivité organisationnelle** en éliminant les programmes malveillants et les conflits logiciels qui engendrent des temps d'arrêt non planifiés, en libérant des ressources informatiques pour qu'elles travaillent sur des initiatives plus stratégiques, en minimisant le temps d'arrêt des utilisateurs finaux dû à l'infection par des programmes malveillants, et en assurant une mise en vigueur granulaire des règles liées aux applications entre les différents rôles et utilisateurs.
- » **Réduisez le coût total de possession des postes de travail** en minimisant le nombre d'appels passés au service d'assistance informatique et de réponses aux incidents liés à des programmes malveillants et des problèmes causés par des conflits logiciels, ainsi qu'en réduisant la complexité de la gestion de plusieurs produits ponctuels différents et sans rapport entre eux.

Fonctionnement de *Lumension*® Intelligent Whitelisting™

Lumension® Intelligent Whitelisting™ offre un contrôle flexible de l'utilisation des applications sur le poste de travail. En établissant des règles sur la façon dont le changement peut être introduit, au lieu de se concentrer uniquement sur les types de changements qui doivent être bloqués, on obtient un modèle opérationnel de gestion de la sécurité des postes de travail plus efficace. Lumension offre cette capacité grâce à un flux de travail des solutions unifié, efficace et simple à gérer.

1. **Nettoyage** : analysez votre environnement de postes de travail à l'aide de *Lumension*® AntiVirus, ou d'autres produits anti-programmes malveillants, afin d'identifier et de supprimer automatiquement tous les programmes malveillants connus.
2. **Identification** : obtenez une visibilité inégalée sur les applications qui s'exécutent dans l'environnement des postes de travail. Identifiez les applications des postes de travail connues et inconnues, et déterminez rapidement le risque potentiel qu'elles présentent.

3. **Définition** : prenez un instantané de l'environnement des postes de travail pour définir rapidement les règles de base permettant d'établir la liste blanche des applications. Approuvez automatiquement les mises à jour logicielles des éditeurs, chemins d'accès et utilisateurs sûrs, et simplifiez la gestion de la liste blanche grâce au moteur de confiance flexible et basé sur des règles de Lumension. Les règles de liste blanche des applications sont mises à jour et déployées de manière transparente sur les postes de travail identifiés.
4. **Surveillance** : surveillez en permanence les règles de liste blanche en dehors de leur mise en vigueur et journalisez toutes les tentatives d'exécution. Évaluez l'impact potentiel des règles de liste blanche et ajustez les règles du moteur de confiance pour parvenir à l'équilibre optimal entre la productivité des utilisateurs finaux et une sécurité des postes de travail efficace.
5. **Mise en vigueur** : empêchez les applications inconnues et non autorisées de s'exécuter par défaut et bloquez automatiquement les attaques non répertoriées, avant que les dernières définitions d'antivirus ou les derniers correctifs de vulnérabilités soient déployés. Réduisez encore plus le risque informatique en étendant les règles de liste blanche aux utilisateurs finaux disposant de privilèges d'administrateur local.
6. **Gestion** : simplifiez la gestion de la liste blanche et réduisez les problèmes opérationnels informatiques grâce à l'intégration transparente à Lumension® Patch and Remediation ou d'autres outils d'application de correctifs logiciels tiers. Lumension® Intelligent Whitelisting™ met à jour automatiquement les règles de liste blanche des applications lorsque les dernières mises à jour logicielles et les derniers correctifs des vulnérabilités sont déployés. Des rapports détaillés fournissent une analyse supplémentaire de l'état de sécurité global de votre entreprise et de l'environnement sur liste blanche.



Principaux avantages

- » Réduit le risque lié aux programmes malveillants en stoppant tous les programmes malveillants connus et contribue à empêcher les attaques non répertoriées et autres applications malveillantes de pénétrer dans votre environnement informatique.
- » Réduit le risque lié aux applications tierces en offrant une visibilité sur toutes les applications exécutées à travers l'entreprise et en empêchant les applications indésirables ou non autorisées de s'exécuter.
- » Empêche les applications indésirables, non prises en charge ou sans licence d'être utilisées sur le poste de travail, n'autorisant que les logiciels nécessaires pour des raisons professionnelles et dont l'exécution est approuvée par le département informatique.
- » Offre une sécurité des postes de travail efficace sans sacrifier la productivité des utilisateurs finaux.
- » Réduit le coût total de possession de la gestion des postes de travail et les coûts liés aux programmes malveillants (par exemple, service d'assistance, régénération d'image) tout en rationalisant la gestion de la liste blanche des applications.
- » Contrôle les utilisateurs finaux disposant de privilèges d'administrateur local qui leur permettent d'installer et d'exécuter des applications sûres tout en limitant leurs actions conformément aux règles.
- » Prend en charge d'autres produits de sécurité et opérationnels tiers via une architecture ouverte.
- » Réduit la charge de gestion pour le département informatique en automatisant les règles de liste blanche pour les sources de changement sûres (par exemple, applications, éditeurs, programmes à mise à jour automatique, emplacement et autorisation locale).

Principales fonctionnalités

Liste blanche/contrôle des applications

Identifie automatiquement les logiciels sûrs qui sont autorisés à s'exécuter sur le poste de travail et empêche toutes les autres applications de s'exécuter, qu'elles soient malveillantes, indésirables ou simplement suspectes. Prend en charge tous les fichiers exécutables, dont les fichiers .EXE, .DLL, .COM, etc. Améliore la productivité pour les utilisateurs finaux comme pour le département informatique.

Moteur de confiance

Automatise les mises à jour de la liste blanche en fonction de règles de confiance pour garantir la flexibilité de la liste blanche et l'agilité de l'entreprise sans imposer un processus manuel gourmand en main-d'œuvre. Le moteur de confiance simplifie la gestion de la liste blanche dans les environnements dynamiques. Il inclut les fonctions suivantes.

- » **Éditeur sûr** : permet d'apporter des changements "à la volée" à la liste blanche lorsque ces changements sont accompagnés d'un certificat valide signé par le fournisseur d'applications. Ces changements sont approuvés automatiquement et ne nécessitent aucune intervention de l'administrateur.
- » **Outil de mise à jour sûr** : permet d'apporter des mises à jour automatisées à la liste blanche lorsque des changements sont apportés par des programmes expressément autorisés.
- » **Chemin d'accès sûr** : permet à la liste blanche d'être mise à jour automatiquement à mesure que des changements sont apportés à la bibliothèque d'applications connues acceptées.
- » **Autorisation locale** : permet aux utilisateurs finaux d'apporter des changements ad hoc avec la responsabilité et le contrôle nécessaires, en effectuant le suivi de ces changements et en permettant aux administrateurs de les annuler, le cas échéant. **(Disponible au troisième trimestre 2011.)**

Verrouillage rapide

Simplifie le processus d'établissement de la liste blanche pour appliquer immédiatement les règles et empêcher les changements non autorisés de se produire. Un instantané automatisé de chaque poste de travail est utilisé pour créer une liste blanche et démarrer la mise en vigueur des règles de liste blanche. Fournit une action immédiate contre les nouvelles menaces non répertoriées et autres attaques de programmes malveillants, réduisant la charge de travail pour le département informatique.

Audit simple

Permet aux administrateurs d'observer et d'auditer les règles de liste blanche pour veiller à ce que les considérations de sécurité et les besoins opérationnels soient respectés avant que les actions de mise en vigueur ne soient appliquées. Un instantané local de référence peut être établi et des mesures appropriées prises, sans s'appuyer sur une image de perfection absolue. Réduit la charge du département informatique en créant et en gérant une liste blanche des applications de confiance.

Flux de travail unifié

Garantit un processus transparent pour analyser l'environnement informatique, supprimer les menaces connues, verrouiller l'environnement informatique, gérer en souplesse les changements apportés à l'environnement et supprimer les frictions opérationnelles entre la sécurité et les opérations informatiques. Réduit les durées d'implémentation et de formation, avec un délai de protection plus rapide.



Prenez le contrôle de vos postes de travail et améliorez la productivité opérationnelle

Rationalisez la gestion des postes de travail et protégez votre entreprise des menaces ciblées et non répertoriées sans nuire aux opérations. Contactez votre représentant commercial ou votre revendeur Lumension, ou rendez-vous sur www.lumension.com.

Principales fonctionnalités (suite)

Antivirus intégré

Veillez à ce que les postes de travail soient dépourvus de programmes malveillants connus avant qu'ils ne soient verrouillés et mis sur liste blanche en utilisant le module produit Lumension AntiVirus entièrement intégré. L'identification basique des signatures de programmes malveillants, ajoutée aux capacités évoluées d'environnement protégé ("sandbox"), d'analyse comportementale et de mise en correspondance partielle de schémas, fournit une protection accrue en combinaison avec la liste blanche des applications. Automatise la suppression des programmes malveillants pour une meilleure productivité des utilisateurs finaux et du département informatique.

Gestion des correctifs logiciels intégrée

Gérez simultanément les configurations de sécurité et le risque lié aux vulnérabilités des applications et systèmes d'exploitation au sein du module Lumension Patch and Remediation entièrement intégré. Lorsque des changements opérationnels sont apportés pour atténuer le risque lié aux vulnérabilités, comme le déploiement de nouveaux logiciels et des changements aux configurations des systèmes, toutes les mises à jour appropriées des règles de liste blanche sont effectuées afin de garantir une mise en vigueur transparente sans perturber les utilisateurs finaux ni surcharger les administrateurs. Améliore la sécurité des postes de travail sans nuire à la productivité des utilisateurs finaux et du département informatique.

Lumension® Endpoint Management and Security Suite

Fournit l'architecture de plate-forme sous-jacente pour Lumension® Intelligent Whitelisting™, avec un agent et une console uniques. L'architecture extrêmement évolutive réduit le coût total de possession global et optimise les opérations informatiques et la visibilité de la sécurité.

Ressources en ligne

- » [Pour en savoir plus sur l'évolution de la liste blanche des applications, rendez-vous sur \[www.intelligentwhitelisting.com\]\(http://www.intelligentwhitelisting.com\)](#)
- » [Blog dédié à la protection des postes de travail](#)
- » [Outil d'analyse des applications](#)
- » [Livre blanc : Liste blanche intelligente : introduction à une sécurité des postes de travail plus efficace et efficiente](#)
- » [Podcast : Liste blanche de sécurité des applications: bloquer les intrus tout en accordant l'accès aux personnes autorisées](#)
- » [Podcast : Liste blanche de sécurité des applications: bloquer les intrus tout en accordant l'accès aux personnes autorisées](#)

Contacteur Lumension

- » Siège international
8660 E Hartford Dr., Suite 300
Scottsdale, AZ 85255
États-Unis
+1.480.970.1025
sales@lumension.com
- » Royaume-Uni
+44.0.1908.357.897
sales.uk@lumension.com
- » Europe
+352.265.364.11
sales-emea@lumension.com
- » Asie-Pacifique
+65.6725.6415
sales-apac@lumension.com