

L'application whitelisting fonctionne-t-elle ?

Qu'est-ce que l'Application Whitelisting ?

L'application whitelisting est un concept dans lequel vous disposez d'une liste de programmes autorisés à fonctionner, et tout le reste n'est pas autorisé à fonctionner.

Les technologies de liste blanche d'applications les plus avancées combineront un certain type de logique de source et de destination. Par exemple, une liste blanche d'applications peut indiquer : « Le Bloc-notes Windows est autorisé à accéder au dossier Taxes de mon bureau, mais pas Microsoft Word. »

Nous approfondirons ce point, mais de manière générale, les stratégies défensives de liste blanche d'applications reposent fortement sur ces deux variables :

1. Les attaquants acceptent de suivre les règles que vous avez établies pour eux concernant votre outil de cybersécurité de liste blanche d'applications.
2. Votre environnement est très petit, avec peu d'applications qui restent assez stables, et sans exploits.

Inconvénients des technologies de liste blanche d'applications

Complexité

Les réseaux informatiques sont comme des organismes complexes

Même les petits réseaux informatiques sont des entités en constante évolution, avec une myriade de comportements. Les applications sont constamment ajoutées et supprimées par les utilisateurs. Les modules à l'intérieur des applications sont constamment ajoutés et supprimés par les créateurs de programmes, en particulier lors des mises à jour. Enfin, les comportements des applications, en plus des changements de code entraînant des modifications de comportement, sont utilisés de différentes manières par différents utilisateurs à différents moments. Imaginez maintenant l'équipe qui devrait assurer le suivi constant de tout cela, ainsi que les tickets d'assistance informatique qui devraient constamment être ouverts.

En réalité, le seul environnement informatique stable est celui piloté par des kiosques, dans lesquels les programmes sont installés sans possibilité de mise à niveau, d'ajout ou de suppression, et où les utilisateurs sont strictement autorisés à effectuer une ou deux fonctions seulement. Peut-être un kiosque d'impression de photos ou quelque chose de similaire. Dans ce cas, la liste blanche d'applications ne devrait être mise à jour qu'à chaque mise à niveau du terminal du kiosque, disons deux fois par an.

Des listes blanches d'applications plus avancées signifient plus de complexité

Les listes blanches d'applications les plus simples se limitent à des listes de programmes autorisés à exister sur le système d'un utilisateur.

Cela peut déjà être difficile à gérer en soi, mais cela conduit à une variété d'améliorations potentielles.

Par exemple, ce n'est pas parce que le service de paie dispose d'une application pour interagir avec le système de paie de l'entreprise qu'il ne devrait pas y avoir un ensemble de règles distinct pour l'équipe de l'entrepôt, qui utilise des applications différentes (non liées à la paie) ?

Ainsi, des améliorations concernant les divisions ou les utilisateurs pouvant exécuter quelles applications constituent une amélioration évidente. Une amélioration qui a désormais créé une complexité supplémentaire, en plus du simple suivi du nombre, du type et des versions des programmes présents sur votre réseau.

Maintenant, supposons que nous ayons besoin d'un autre ensemble d'améliorations : nous devons décider quel utilisateur a accès à quelle application, pour quel ensemble de données.

Cela aussi a parfaitement du sens, n'est-ce pas ? Vous ne voulez pas que votre équipe de l'entrepôt ait accès aux dossiers RH, et l'équipe RH n'a probablement pas besoin d'accéder aux données opérationnelles de l'équipe de livraison de l'entrepôt.

Il s'agit d'un ensemble de combinaisons ridiculement complexe à suivre, maintenant que l'emplacement des données a été ajouté comme variable.

Ainsi, avec chaque amélioration nécessaire pour rendre les technologies de liste blanche d'applications efficaces, la gestion, la configuration et le support continu (sans doute sans fin, toujours croissant) nécessaire pour la maintenir fonctionnelle rend la technologie inutilisable. Le résultat est généralement que de grands groupes d'utilisateurs se voient accorder l'accès à de grands groupes d'applications, et probablement à la quasi-totalité des données. Il en résulte donc une configuration de la technologie presque inutile, car aucune entreprise ne dispose des ressources nécessaires pour la gérer correctement.

Les applications interagissent entre elles

Il est courant dans les systèmes d'exploitation modernes que les applications interagissent avec d'autres applications. Parfois, cette interaction est due à une intégration entre deux applications, qui améliore l'expérience utilisateur, comme un document Word ouvrant Microsoft Photos. À d'autres moments (cela est très courant), il existe des appels entre programmes qui sont effectués d'une manière généralement invisible pour l'utilisateur final.

Revision #1

Created 2026-07-24 06:48:01 UTC by Dennis Underwood

Updated 2026-07-24 06:48:01 UTC by Dennis Underwood