F-Secure Software Updater

Un outil unique pour protéger votre entreprise

F-Secure

Vue d'ensemble

Ce document décrit Software Updater, ses fonctionnalités, son fonctionnement, ce qui est corrigé et comment. Il précise également les logiciels et les versions mis à jour.

Fonctionnalités clés

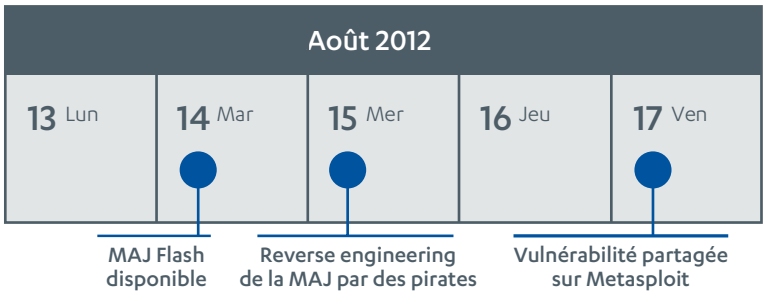
- Détection et Classification des mises à jour de sécurité
- Déploiement automatique des mises à jour de sécurité avec des possibilités d'exclusion et de déploiement manuel
- Installation des mises à jour manquantes
- Gestion des correctifs pour Windows et logiciels tiers
- Administration intégrée ne nécessitant aucune infrastructure séparée

Avantages

- Possibilité de déployer facilement et automatiquement des mises à jour de sécurité pour des logiciels tiers
- Protection automatique contre les menaces connues pour une protection sans faille
- Avec 85% des vulnérabilités provenant de logiciels tiers, la gestion des correctifs de ces logiciels est essentielle
- Software Updater est intégré aux solutions de sécurité de F-Secure, pour une meilleure détection, des mises à jour automatiques et une administration intégrée à un prix abordable

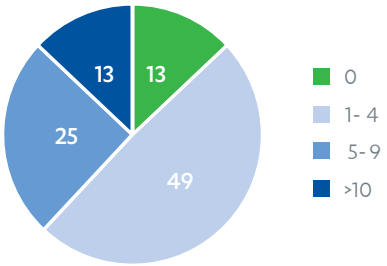
L'importance des mises à jour logicielles automatiques

Les logiciels malveillants les plus récents exploitent les vulnérabilités connues des logiciels pour infecter les systèmes informatiques. De nouvelles tentatives d'exploitation de vulnérabilités voient le jour immédiatement après la publication de correctifs.



Dès que les vulnérabilités sont corrigées, les mises à jour sont analysées pour déterminer les vulnérabilités qu'elles corrigent. Tous les ordinateurs non corrigés deviennent alors des cibles de choix au bout de quelques jours seulement !

La plupart des infections pourraient être évitées par l'application immédiate des correctifs de sécurité. En fait, 83% des logiciels malveillants pourraient être bloqués grâce à des logiciels à jour, mais la plupart des postes des entreprises ne disposent pas des mises à jour critiques.



87% des ordinateurs des entreprises ne disposent pas des mises à jour de sécurité critiques.
Source : étude F-Secure de mars 2013.

Les administrateurs n'ont actuellement pas de visibilité sur les logiciels tiers installés sur les postes qu'ils gèrent, sauf lorsque des restrictions utilisateur strictes sont appliquées.

Déterminer les mises à jour de sécurité disponibles et les rechercher, les tester et les déployer, prend beaucoup de temps, d'autant plus que le nombre de logiciels différents utilisés augmente. Cela signifie que les administrateurs ne peuvent, en général, que mettre en place les mises à jour des logiciels majeurs, laissant les autres de côté.

Une fois que tout est corrigé, les administrateurs doivent recommencer le processus dès que de nouvelles mises à jour de sécurité sont disponibles.

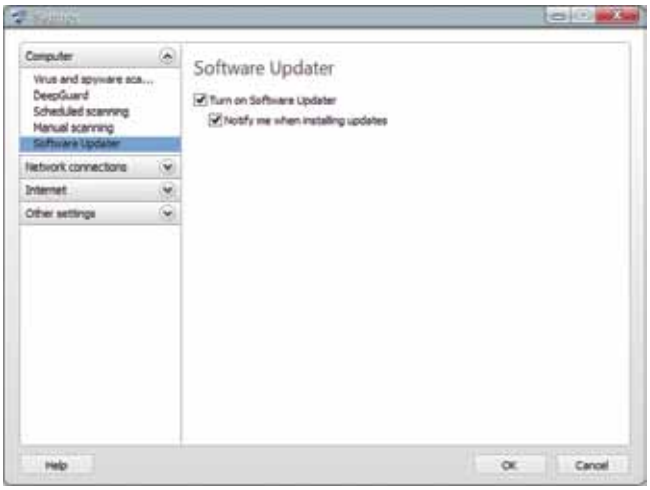
Qu’est-ce que Software Updater ?

F-Secure Software Updater analyse et documente les mises à jour manquantes des logiciels tiers, puis déploie automatiquement les mises à jour de sécurité. Il s'agit des mises à jour Microsoft pour le système d'exploitation et les applications MS, ainsi que de nombreuses applications tierces telles qu'Adobe Flash, Java, OpenOffice, des gestionnaires d'archives, des lecteurs multimédias, des logiciels de visualisation/modification d'images et autres, qui sont communs et sujets aux vulnérabilités, et donc aux failles de sécurité.

Software Updater télécharge périodiquement des fichiers de définition comprenant des informations sur les mises à jour de logiciels, leurs versions, les références des bulletins de sécurité, les liens vers des articles des bases de connaissances et l'emplacement des packages d'installation, puis compare ces informations avec les logiciels installés pour identifier les mises à jour manquantes.

Software Updater est intégré à PSB et à nos solutions Premium

Software Updater est intégré à PSB et aux solutions Premium de F-Secure. Par conséquent, il n'est pas nécessaire d'installer d'agent distinct, de serveur d'administration ou de console. Tout est intégré pour une meilleure détection, des mises à jour automatiques et une administration centralisée. Software Updater est à la fois abordable d'un point de vue financier et facile à utiliser.



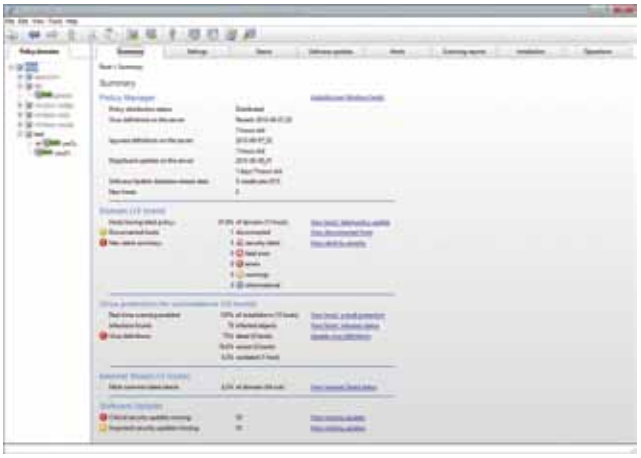
Les mises à jour de sécurité "critiques" et "importantes" sont des mises à niveau mineures des logiciels. Cela signifie qu'elles peuvent être installées automatiquement car elles sont très peu susceptibles d'entraîner des problèmes de compatibilité, de provoquer des problèmes de fonctionnement ou d'entraîner d'autres effets indésirables.

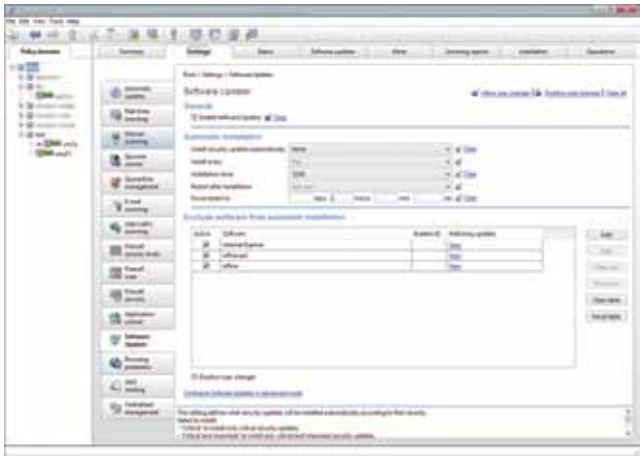
Les Service Packs sont toujours exclus du mode automatique car ils sont susceptibles de modifier le comportement des produits et entraîner des problèmes de compatibilité. C'est pourquoi les administrateurs doivent décider de l'installation de ces mises à jour.

Les administrateurs peuvent définir des exclusions pour le mode automatique en fonction des noms des logiciels ou des références des bulletins, et les masquer de l'interface de la console pour éviter de l'encombrer. C'est particulièrement important pour les entreprises ayant besoin des versions précises de logiciels pour garantir le fonctionnement d'applications métiers, comme par exemple Java Runtime. En outre, puisque les mises à jour de certains logiciels sélectionnés (par exemple Microsoft) peuvent être prises en charge par d'autres produits, les exclusions permettent d'éviter les chevauchements avec Software Updater.

Fonctionnement de Software Updater

La recherche des mises à jour manquantes se produit au démarrage du système, lorsque de nouvelles définitions de mises à jour de logiciels sont téléchargées, ou au moins une fois par jour si aucun de ces évènents ne se produit. La liste des mises à jour manquantes est communiquée au serveur Policy Manager et le nombre cumulé de mises à jour manquantes est présenté dans l'écran des statistiques du client.





L'état de l'installation est visible dans la console Policy Manager et les éventuels échecs d'installation sont signalés afin qu'ils puissent être étudiés.

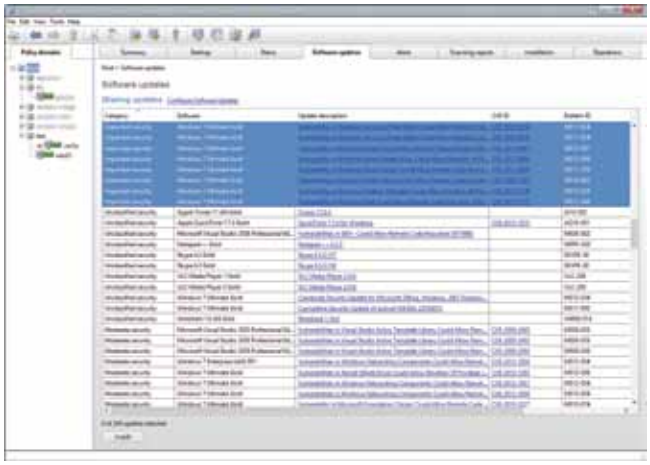
Un redémarrage n'est pas effectué lorsque les applications n'en ont pas besoin. Mais si plusieurs applications nécessitant un redémarrage sont mises à jour en même temps, le redémarrage n'est effectué qu'une seule fois pour ne pas perturber les utilisateurs.

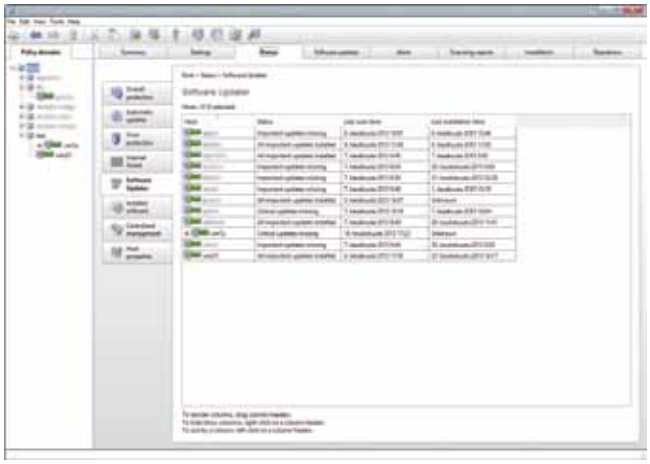
Les clients téléchargent les mises à jour directement depuis les sites des éditeurs concernés et les installent silencieusement en arrière-plan. Il n'est pas nécessaire de mettre en place des points de distribution internes.

Les mises à jour peuvent être mises en cache via des proxys transparents, comme pour le trafic web normal des postes, si ces proxys sont utilisés. Les mises à jour installées sont indiquées dans les rapports web de Policy Manager.

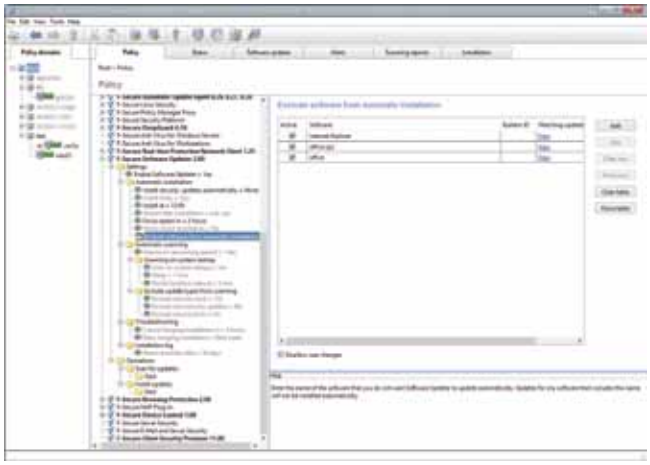
Les administrateurs ont le contrôle

Les administrateurs peuvent consulter les mises à jour manquantes pour l'ensemble de l'environnement et pour des postes spécifiques dans la console Policy Manager et les rapports web.





Les administrateurs peuvent affecter des mises à jour spécifiques à certains postes, certains domaines ou à l'ensemble de l'environnement en sélectionnant et en déclenchant la commande d'installation dans la console Policy Manager.



Les administrateurs peuvent également préciser si l'installation des mises à jour de sécurité doit se faire automatiquement, et indiquer le niveau de criticité des mises à jour à installer.

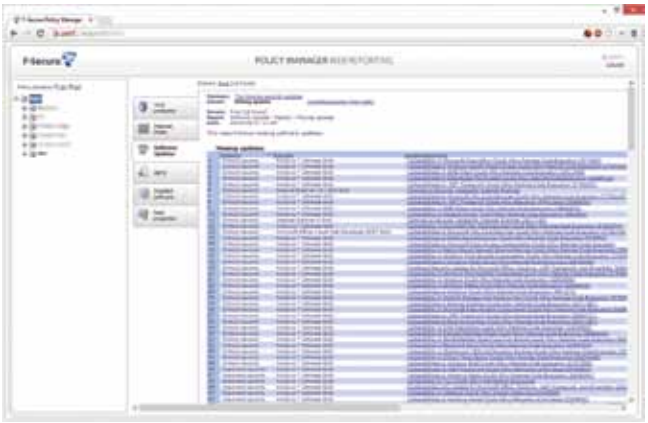
Le système permet aux administrateurs de garder le contrôle de l'environnement quand cela est nécessaire, car aucune intervention des utilisateurs finaux n'est requise pour finaliser les mises à jour. Les administrateurs peuvent empêcher les utilisateurs finaux de modifier les paramètres pour éviter les erreurs humaines. Les installations sont également effectuées avec les droits utilisateurs des postes ; les utilisateurs finaux n'ont donc pas besoin de valider de demandes de mise à niveau.

Les administrateurs peuvent également définir le jour et l'heure des installations pour le mode automatique, forcer le redémarrage et préciser le délai de grâce avant de forcer un redémarrage après installation

Des rapports web en toute clarté

Un portail web clair et facile à utiliser permet aux administrateurs d'administrer la solution à tout moment, en tout lieu et depuis n'importe quel appareil.

Les administrateurs peuvent consulter les détails des mises à jour manquantes. Les rapports des mises à jour logicielles manquantes, indiquant leur niveau d'importance et le nombre d'hôtes affectés, sont facilement accessibles avec un navigateur web.



Software Updater est également intégré à Protection Service for Business

F-Secure Protection Service for Business (PSB) intègre également la fonctionnalité Software Updater. PSB propose une protection complète contre toutes sortes de menaces ciblant votre entreprise, pour les ordinateurs portables, les ordinateurs de bureau, les appareils mobiles, les serveurs de messagerie et les serveurs de fichiers.

F-Secure - Protège l'irremplaçable

L'innovation, la fiabilité et la réactivité font de F-Secure l'un des principaux fournisseurs en matière de sécurité informatique depuis sa création en 1988. Nos solutions moult fois récompensées sont aujourd'hui utilisées par des millions de foyers et d'entreprises dans le monde. Nous fournissons une protection de haut niveau en temps réel permettant aux utilisateurs d'ordinateurs et de smartphones de profiter pleinement de leurs activités en ligne.
La société F-Secure est cotée sur le NASDAQ OMX Helsinki Ltd.

F-Secure SARL
38/44 rue Jean Mermoz
78600 Maisons Laffitte
France
Tél. +33 (0)8 20 00 07 59

© 2013 F-Secure Corporation. Tous droits réservés. F-Secure et le triangle F-Secure sont des marques déposées de F-Secure Corporation. Les noms des solutions F-Secure et leurs logos ou symboles sont des marques ou des marques déposées de F-Secure Corporation. Les autres produits et les noms de sociétés mentionnés dans ce document appartiennent à leurs propriétaires respectifs.