



Microsoft Forefront « Stirling » (nom provisoire)

La sécurité dynamique de votre infrastructure.

Découvrez le nouveau système de sécurité complet, intégré, simple à gérer et à superviser

Une caractéristique remarquable : la réponse dynamique

La réponse dynamique est une fonctionnalité importante de « Stirling ». Les logiciels qui composent « Stirling » échangent des informations afin de répondre dynamiquement à toute nouvelle menace apparaissant dans l'entreprise.

Supposons qu'un cheval de Troie s'installe dans le PC d'un employé et ouvre des centaines de connexions sur Internet.

La plupart des solutions actuelles se contenteraient de signaler le problème et l'administrateur réseau devrait consulter le fichier journal du pare-feu pour identifier le PC suspect. Il transmettrait ensuite l'information à l'administrateur système qui tenterait de résoudre le problème, peut-être en isolant le PC infecté. Ce processus peut prendre des heures pendant lesquelles l'entreprise court un risque.

Avec « Stirling », la réponse est dynamique, coordonnée et automatique. Dans notre exemple, Forefront Threat Management Gateway détecte les nombreuses connexions ouvertes sur Internet. Il transmet cette information aux autres composants logiciels. Forefront Client Security déclenche alors une analyse sur le PC concerné pour rechercher un éventuel virus. En fonction du résultat, la protection d'accès réseau (NAP) peut décider de mettre le PC en quarantaine et de bloquer ses courriels. Toute cette procédure est automatique et ne prend que quelques minutes.

Par ce partage des informations de sécurité, « Stirling » et la réponse dynamique font gagner un temps précieux et sécurisent avec anticipation l'environnement informatique.

Forefront™ « Stirling » (nom provisoire) est un système de sécurité intégré qui assure une protection complète et coordonnée pour les points terminaux et les serveurs de messagerie et de collaboration, jusqu'au réseau de l'entreprise. « Stirling » est simple à gérer et à contrôler.

Par sa simplicité et par son affichage des menaces, des vulnérabilités et des risques de configuration, « Stirling » vous aide à réduire les coûts et vous donne l'état en temps réel de la sécurité de votre informatique.

Une protection complète et coordonnée

« Stirling » fournit une protection complète en coordonnant ses différents composants. Il apporte des réponses dynamiques à de nouvelles menaces qui pourraient viser les points terminaux, les serveurs de messagerie et de collaboration, et le réseau de l'entreprise.

Identification automatique des menaces et réponse dynamique

Les technologies de « Stirling » échangent entre elles des informations sur la sécurité informatique de l'entreprise. Ces informations couvrent les points terminaux et les serveurs de collaboration et de messagerie, au réseau. En fonction de l'importance du risque, le système répond dynamiquement en protégeant l'entreprise à différents niveaux. « Stirling » fait gagner du temps aux administrateurs tout en sécurisant l'environnement par anticipation.

Intégration des technologies de protection

Contrairement aux approches traditionnellement fragmentées, « Stirling » opte pour l'intégration des différents mécanismes de protection : détection des logiciels malveillants, pare-feu, anti-spam, filtrage du contenu, plusieurs moteurs d'analyse pour la messagerie et la collaboration, protection à la frontière du réseau, etc.

Microsoft « Stirling » : Un système de sécurité intégré



Dans sa version finale, « Stirling » inclura :

- Une console de gestion centralisée et un tableau de bord pour la configuration et la visibilité de la sécurité de toute l'infrastructure informatique.
- Les prochaines versions de Forefront Client Security, Forefront Security for Exchange Server, Forefront Security for SharePoint et Internet Security & Acceleration Server (qui sera renommé Forefront Threat Management Gateway).

En regroupant les signatures, les approches heuristiques et comportementales, et les listes de réputation en provenance de différentes sources, « Stirling » fournit une protection de haut niveau contre des menaces complexes.

Analyses et réponses en provenance du monde entier

« Stirling » exploite les informations en provenance du Microsoft Malware Protection Center, un centre mondial d'analyse et de réponse aux logiciels malveillants. Ce centre fournit du code et des mises à jour de signatures pour les logiciels de sécurité Microsoft. Ce centre se compose de plusieurs sites, répartis dans le monde entier, et d'ingénieurs experts dans l'analyse des menaces. Le Malware Protection Center est étroitement couplé avec le service Support de Microsoft afin de fournir le plus rapidement possible des réponses à toute nouvelle menace, 365 jours par an.

Gestion simplifiée

« Stirling » simplifie la gestion de la sécurité en proposant une console de gestion unique pour configurer la sécurité des points terminaux, des serveurs de messagerie et de collaboration. Il gère aussi la sécurité du réseau et s'intègre parfaitement à l'infrastructure existante.

Console de gestion centralisée

« Stirling » propose une console unique de gestion. Depuis ce point, les administrateurs surveillent et configurent toute la sécurité. Ils génèrent des rapports, mettent à jour les signatures et surveillent les alertes. La console respectant les rôles, chaque administrateur peut effectuer son travail sans interférer avec celui des autres. « Stirling » permet de gérer la sécurité à partir d'un point central, ce qui fait gagner du temps aux administrateurs.

Optimisation de la stratégie de sécurité

Contrairement à l'approche traditionnelle qui se concentre sur la configuration des produits et des technologies de sécurité, « Stirling »

définit des stratégies de sécurité sur des groupes d'ordinateurs et d'utilisateurs. Cette approche par stratégie est plus simple pour gérer les nombreux paramètres et produit moins d'erreurs de configuration.

Intégration dans l'infrastructure existante

« Stirling » a été conçu pour s'intégrer parfaitement à l'infrastructure Microsoft. Il reprend des éléments de System Center Operations Manager 2007 et SQL Server™. Le déploiement des signatures et des agents fonctionne parfaitement avec Windows Server Update Services (WSUS) et System Center Configuration Manager. « Stirling » sait aussi exploiter les groupes définis dans Active Directory® pour déployer des stratégies. Étroitement lié à la protection d'accès réseau (NAP), « Stirling » garantit que seuls les points terminaux conformes à la politique de sécurité de l'entreprise, pourront se connecter au réseau. En s'intégrant parfaitement dans l'infrastructure existante, « Stirling » réduit la complexité de la gestion de la sécurité.

Visibilité sur la sécurité

Via son tableau de bord, « Stirling » fournit une visibilité en temps réel, des rapports détaillés et des remèdes contre les menaces, les vulnérabilités et les risques liés à une mauvaise configuration.

État de la sécurité

Dans son tableau de bord, « Stirling » fournit des informations en temps réel sur l'état de la sécurité informatique. « Stirling » recoupe des informations à différents niveaux pour détecter des éventuelles menaces et vulnérabilités. Il

en déduit des analyses et des rapports en temps réel. Ainsi, les administrateurs comprennent instantanément si l'environnement informatique est sûr ou non.

Rapports détaillés

« Stirling » établit des priorités et signale les points importants. Les administrateurs peuvent personnaliser le tableau de bord pour l'adapter à leurs besoins spécifiques. Le tableau de bord regroupe un historique et des tendances pour mettre en évidence des menaces émergentes. Cela permet aux administrateurs de mieux comprendre l'évolution de leur environnement à moyen terme.



Investigation et remède

Le tableau de bord de « Stirling » contient des liens hypertextes pointant vers des sources d'informations complémentaires et des remèdes proposés. Il permet aussi de lancer l'édition de nombreux rapports afin que les administrateurs puissent affiner leurs investigations si nécessaire. « Stirling » facilite la résolution des problèmes de sécurité. En quelques clics, les administrateurs corrigent un problème de sécurité. « Stirling » leur apporte un meilleur contrôle de leur environnement informatique.

Microsoft Forefront « Stirling » est disponible en version bêta.
Pour télécharger ou pour obtenir d'autres informations, visitez
www.microsoft.com/france/forefront/Stirling.