F-SECURE BUSINESS SUITE

Descriptif de la solution

F-Secure

SOMMAIRE

AVERTISSEMENT : Le présent document donne un aperçu détaillé des principaux composants de sécurité de Business Suite.

F-Secure améliore constamment ses services. F-Secure se réserve le droit de modifier les caractéristiques ou les fonctionnalités du logiciel, conformément à ses pratiques en matière de cycle de vie des produits.

1. RÉSUMÉ

La cyber sécurité est un processus qui débute par la prédiction : il faut comprendre les risques, connaître sa propre surface d'attaque et identifier ses points faibles. Un modèle de sécurité à plusieurs niveaux permet de minimiser la surface d'attaque et de prévenir les cyber incidents.

La cyber sécurité est donc désormais structurée par couches qui stoppent les cyber attaques à différents stades de la chaîne de piratage. Cette sécurité multi-niveaux, également appelée « défense en profondeur », protège votre infrastructure et assure une réponse rapide et économiquement pertinente lorsque survient un cyber incident. La sécurisation via les endpoints est un élément-clé de la cyber sécurité actuelle : elle protège le cloud public, les cloud privés, les infrastructures locales et les flux de travail on-premise.

Business Suite offre la meilleure protection pour les entreprises de toutes tailles. Le succès que remporte cette solution, année après année, dans des tests indépendants, atteste de son efficacité. Les fonctionnalités avancées et automatisées de Business Suite sont conçues pour monitorer efficacement les environnements informatiques complexes et évolutifs des entreprises.

Avec Business Suite, les administrateurs sont en mesure de gérer les autorisations au sein du réseau, sur les clouds privés et les clouds publics. Les outils automatisés permettent de gagner du temps en facilitant la gestion quotidienne de la sécurité. Nos partenaires certifiés offrent une assistance et des services à des clients partout dans le monde. Avec eux, nous proposons des modèles de licence flexibles et transparents pour répondre aux besoins de votre entreprise.

L'endpoint, au cœur de la cyber sécurité

Les entreprises n'ont plus un contrôle total sur le périmètre de leur environnement informatique. L'endpoint fait désormais office de périmètre et les utilisateurs sont devenus le maillon faible de la cyber sécurité des entreprises. Voilà pourquoi la protection des endpoints est aujourd'hui la pierre angulaire de la cyber sécurité.

La sécurité des entreprises doit être assurée à tout moment, jour après jour, mois après mois, année après année.

F-Secure est la seule entreprise à avoir remporté à six reprises l'award Best Protection décerné par l'AV-Test Institute, depuis la création de ce prix il y a huit ans. Aucune autre entreprise ne s'approche d'une telle performance.

Notre solution offre un haut-niveau de protection tout en restant intéressante sur le plan économique. Ses technologies intégrées protègent les ressources de votre entreprise, à partir des endpoints. Par exemple, les données de réputation des fichiers et des contenus permettent de contrôler l'utilisation du web ou de bloquer certains contenus nuisibles. Des outils automatisés et intégrés, tels que Software Updater, contribuent à sécuriser votre environnement informatique en mettant automatiquement à jour tous les logiciels tiers utilisés par votre entreprise. Grâce à l'intégration de plusieurs technologies de pointe, vos utilisateurs n'entrent pas en contact avec la plupart des menaces. Vous réduisez ainsi les risques liés à la plus grande faiblesse des entreprises : l'erreur humaine.

Nos solutions de sécurité professionnelles mobilisent plusieurs couches de protection qui se renforcent mutuellement, pour offrir la meilleure protection possible. Depuis début 2014, nous obtenons le score de 6 sur 6 dans les évaluations indépendantes AV-Test pour les produits de sécurité des entreprises. Aucun fournisseur ne serait en mesure d'atteindre un tel résultat aujourd'hui en utilisant uniquement les technologies anti-malware traditionnelles. Pour obtenir une sécurité efficace, vous devez choisir une solution qui a fait ses preuves en matière de détection et de protection contre les malware et autres menaces.

La protection préventive est la clé pour stopper les ransomware et autres logiciels malveillants. Vous avez besoin d'une solution offrant constamment les meilleurs niveaux de protection du marché . Parallèlement, celle-ci doit rester intuitive, préserver les performances systèmes et gérer automatiquement les mises à jour.

Des technologies de pointe conçues par une entreprise experte en cyber sécurité

F-Secure, entreprise européenne de cyber sécurité, possède des décennies d'expérience dans la défense des entreprises contre toutes les cyber attaques, qu'il s'agisse de ransomware opportunistes ou de cyber attaques avancées. Notre gamme complète de services et de produits récompensés s'appuie sur les innovations de sécurité brevetées de F-Secure et sur des renseignements de pointe sur les menaces pour protéger des dizaines de milliers d'entreprises et des millions d'individus.

Les experts en sécurité de F-Secure ont participé à plus d'enquêtes cyber criminelles européennes que n'importe quelle autre entreprise sur le marché. Nos produits sont vendus dans le monde entier, par des milliers de revendeurs et des centaines d'opérateurs.

Ransomware : Comment prévenir, prévoir, détecter et répondre
https://blog-assets.f-secure.com/wp-content/uploads/2019/11/20112058/ransomware_ppdr_2019.pdf

2. BUSINESS SUITE, UNE PARFAITE MAÎTRISE DE LA SÉCURITÉ

Business Suite est une solution offrant en continu la meilleure protection aux entreprises. Celle-ci couvre les éléments essentiels de la sécurité. Elle protège contre les vulnérabilités connues mais aussi contre les nouvelles menaces émergentes. Business Suite est une offre de protection complète pour les organisations de toutes tailles, avec des fonctions de contrôle avancées. Elle prend en charge les environnements physiques et virtuels, les clouds privés et les clouds publics, le tout via un outil de gestion centralisée. Business Suite est conçu pour répondre aux besoins de sécurité exigeants des entreprises d'aujourd'hui. Elle assure leur sécurité, depuis les serveurs jusqu'aux endpoints.

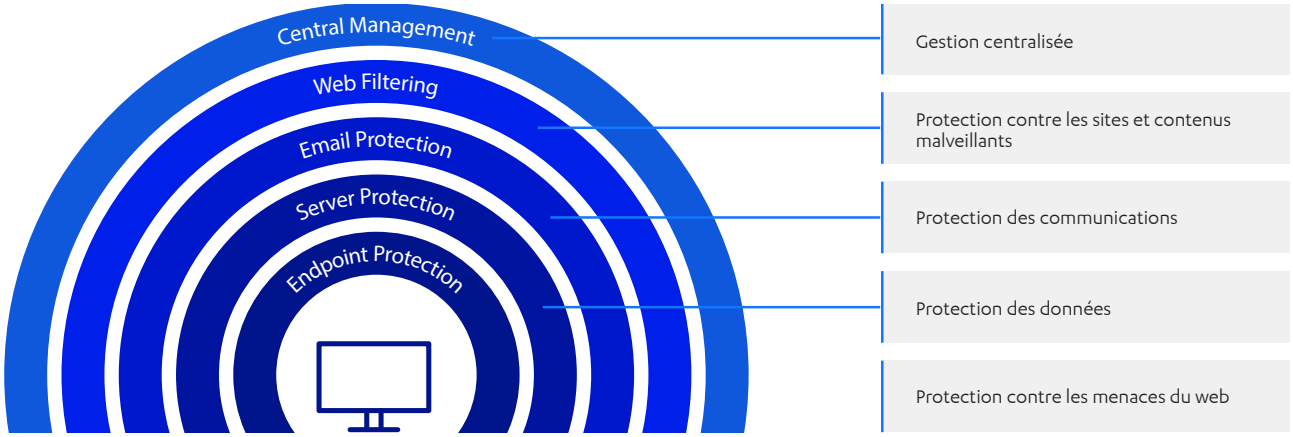
Business Suite en bref

- Contrôlez l'ensemble de votre environnement informatique, grâce à un seul outil polyvalent.
- Des fonctionnalités de gestion avancées, adaptées aux environnements complexes
- Une sécurité complète et sans compromis pour assurer la sécurité de votre entreprise
- Performances et évolutivité pour les entreprises de toutes tailles et de différentes structures
- Une protection fiable et une totale tranquillité d'esprit, pour vous focaliser sur votre cœur de métier
- Des performances optimisées pour les environnements virtuels et cloud, grâce au déchargement (offloading) des analyses
- La meilleure des protections pour votre entreprise, reconnue année après année.
- Un impact minimal sur les performances système.
- Une solution intuitive ; un achat simplifié ; des mises à jour facilitées

La réponse aux enjeux de sécurisation de votre environnement informatique

Une bonne gestion est la clé d'une sécurité efficace. La gestion centralisée vous offre un contrôle total sur les actifs informatiques de votre entreprise. Elle vous permet d'optimiser votre protection, tout en permettant à vos employés de travailler avec souplesse. En disposant d'une visibilité et d'une transparence totale sur vos systèmes, vous pouvez également vous assurer que votre entreprise est bien protégée contre toutes les cyber menaces.

Business Suite est la solution idéale pour toutes les entreprises ayant des besoins de sécurité exigeants, à la fois en termes de fonctionnalités, de contrôle et d'intégration. La meilleure façon de stopper les cyber attaques est de les arrêter avant qu'elles n'accèdent au réseau de votre entreprise. Pour y parvenir, Business Suite offre une protection multi-niveaux.



Une protection complète pour les entreprises, en un seul pack

Protection	Business Suite Standard	Business Suite Premium
Postes de travail Windows	•	•
Postes de travail Linux	•	•
Postes de travail Mac	•	•
Serveurs Microsoft Windows	•	•
Serveurs Microsoft Exchange	•	•
Serveurs Microsoft SharePoint	•	•
Serveurs Linux	•	•
Protection des serveurs et bureaux virtuels	•	•
Protection des charges de travail en cloud privés et publics	•	•
Serveurs Microsoft Terminal	•	•
Serveurs Citrix	•	•
Serveurs EMC Storage (CAVA/ICAP)	ICAP	CAVA & ICAP
F-Secure Proxy	•	•

Fnctionnalités	Business Suite Standard	Business Suite Premium
DeepGuard	•	•
Analyse du trafic web	•	•
Protection de la navigation	•	•
Botnet Blocker	•	•
Filtre anti-spams	•	•
Advanced Protection	•	•
DataGuard		•
Application Control		•
Software Updater		•
Web Content Control		•
Connection Control		•
Agent de déchargement des analyses pour les tâches en environnements virtuels et cloud		•

Business Suite offre une protection complète pour les entreprises. La version Premium inclut toutes les fonctionnalités avancées dans un pack clair et transparent.

Business Suite est adaptée aux hautes exigences en matière de sécurité. Elle comprend des fonctions de gestion avancées pour les environnements informatiques les plus complexes.

Les atouts de Business Suite

- Des fonctions de gestion avancées, adaptées aux environnements les plus complexes
- Un contrôle simplifié sur tous les actifs informatiques, pour une sécurité renforcée
- Administration simplifiée grâce à l'automatisation des opérations quotidiennes
- Optimisation des performances en environnements virtuels via le déchargement (offloading) des analyses
- Évolutivité, pour répondre aux exigences des grandes entreprises

Fonctionnalités Business Suite Premium

- Contrôle avancé des applications, pour gérer les logiciels installés et l'accès aux fichiers
- Gestion automatisée des correctifs - Software Updater - pour sécuriser votre entreprise contre les cyber menaces répertoriées
- Amélioration de la productivité et de la sécurité grâce à l'outil Web Content Control
- Sécurisation des connexions aux sites de confiance et protection des données critiques avec Connection Control
- Protection optimisée des performances en environnements virtuels et cloud

3. GESTION INTELLIGENTE ON-SITE DE LA SÉCURITÉ, VIA LES ENDPOINTS

Business Suite intègre les meilleures fonctions de sécurité, pour ne laisser aucune place aux vulnérabilités. Policy Manager, le centre de contrôle évolutif de Business Suite, gère toutes les applications de sécurité depuis une unique interface. Il offre un contrôle optimal, propose des fonctions d'automatisation synonymes de gain de temps et permet une gestion avancée des politiques en environnements physiques et virtuels, pour les clouds privés et publics.

Policy Manager vous aide à définir et à distribuer des politiques de sécurité et à surveiller la sécurité globale de votre entreprise. Un logiciel de sécurité optimal doit assurer une protection par couches. Il doit être facile à gérer et à contrôler. Vous pouvez automatiser toutes les tâches de sécurité quotidiennes et maintenir un contrôle accru sur les autorisations accordées à chaque utilisateur. Policy Manager vous aide à :

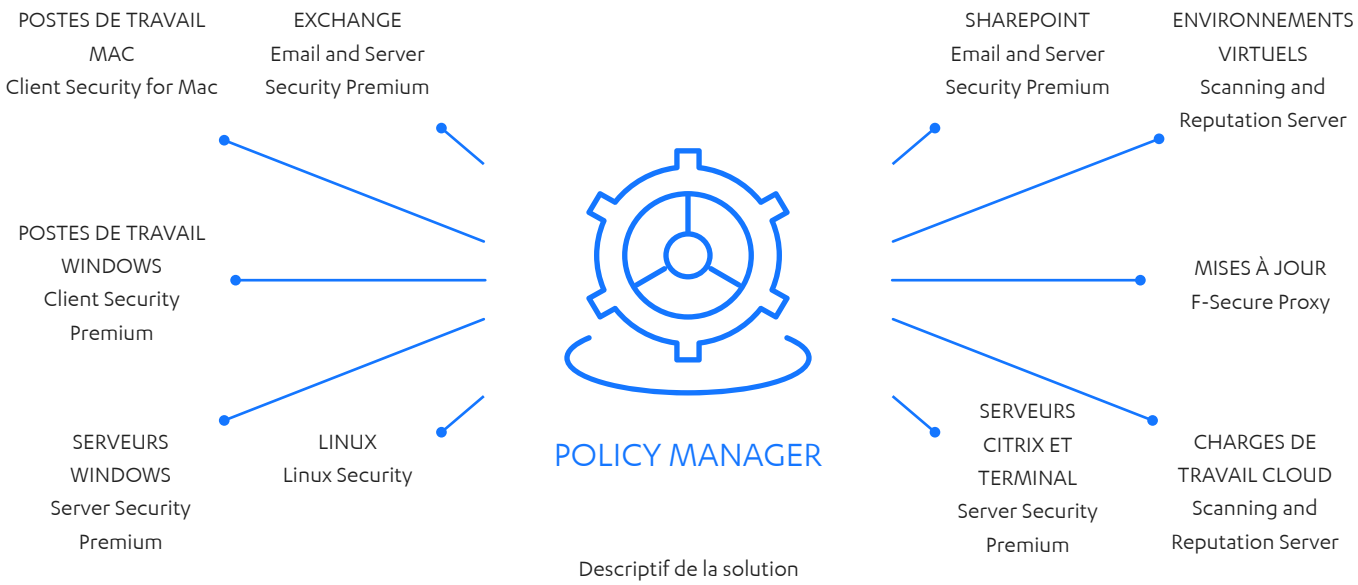
- obtenir une vue centralisée du statut de sécurité des endpoints et des alertes,
- définir et distribuer des politiques de sécurité,
- installer et mettre à jour des logiciels de sécurité sur des systèmes distants,
- mettre à jour des logiciels tiers utilisés sur votre réseau,
- créer facilement des rapports, et
- surveiller les activités de tous les systèmes, pour assurer leur conformité avec les politiques de l'entreprise.

Une fois la solution installée, vous pouvez visualiser les informations concernant l'ensemble de l'infrastructure, depuis une seule interface. Vous pouvez alors facilement vous assurer que l'ensemble de l'environnement informatique est protégé et que cette protection est à jour. Vous pouvez adapter les paramètres de protection si nécessaire, et restreindre les modifications que les utilisateurs peuvent apporter à ces paramètres.

Un contrôle complet sur la sécurité de votre entreprise

F-Secure Policy Manager vous donne un contrôle total sur tous les aspects de la sécurité réseau. Vous pouvez tout gérer, qu'il s'agisse de la sécurité des endpoints, de l'accès aux serveurs e-mails, de la navigation ou encore des mises à jour des logiciels. Vous pouvez mettre en place des contrôles automatisés et personnalisés, et définir les politiques de sécurité adaptées. Et vous bénéficiez de fonctions de gestion avancées pour les environnements complexes.

Policy Manager vous permet de simplifier le monitoring de l'environnement à l'aide de politiques de sécurité : cet ensemble de règles bien définies permettent de gérer la manière dont les informations sensibles et les autres ressources sont traitées, protégées et distribuées. Le logiciel F-Secure utilise des politiques configurées par l'administrateur de manière centralisée, pour un contrôle optimal.



Console de gestion Policy Manager

La console de gestion Policy Manager fournit une interface de gestion centralisée pour la sécurité des hôtes gérés sur le réseau. Policy Manager peut être exécuté sur Windows et Linux. Cet outil centralisé permet d'organiser le réseau en unités logiques pour partager des politiques de sécurité, installer des logiciels de sécurité et distribuer les politiques définies aux hôtes gérés.

Une gestion optimale et simplifiée

Une fois le système configuré, vous pouvez visualiser le statut de l'ensemble du domaine à partir de Policy Manager. Grâce à ce panneau de contrôle unique, vous pouvez vous assurer que le domaine entier est protégé, et pouvez modifier les paramètres de protection selon vos besoins. Le paramétrages de la sécurité est intuitif. Vous pouvez définir tous les paramètres nécessaires pour une protection optimale de tous les clients de votre réseau.
Dans l'onglet « Paramètres », vous pouvez empêcher les utilisateurs de modifier les paramètres de sécurité, et grâce à l'agent de mise à jour automatique Automatic Update Agent, vous avez la certitude que la protection des hôtes est à jour.

Policy Manager assure les fonctionnalités suivantes :

- Gestion centralisée
- Mises à jour automatiques
- Analyses en temps réel
- Analyses manuelles
- Contrôle des logiciels espions
- Gestion de la quarantaine
- Analyse e-mails
- Niveaux de sécurité du firewall
- Règles de firewall
- Services firewall
- Contrôle des applications
- Contrôle des périphériques
- Mise à jour des logiciels
- Analyse du trafic web
- Protection de la navigation
- Contrôle du contenu web
- Envoi d'alertes

L'onglet « Statut », un aperçu clair de l'état du réseau

Dans l'onglet « Statut » de la console, vous pouvez consulter l'état des mises à jour serveur pour les bases de données des malware, des logiciels espions et des définitions DeepGuard.

Vous pouvez vérifier l'état de ces variables à tout moment :

- Protection globale
- Mises à jour automatiques
- Protection antivirus
- Bouclier internet
- Mise à jour des logiciels (Software Updater)
- Logiciels installés
- Gestion centralisée
- Propriétés de l'hôte Software Updater
- Configuration et gestion des mises à jour de logiciels tiers

Software Updater - Configuration et gestion des mises à jour de logiciels tiers

Les programmes présentant des vulnérabilités connues et non-corrigées jouent un rôle dans près de 85 % des cyber incidents. Les attaques exploitant ces failles continuent de causer la majorité des violations réseau et des fuites de données sensibles.

Pourtant, 70 % des entreprises ne disposent d'aucune solution de gestion des correctifs. Selon le rapport 2015 *State of Application Security Report* de l'Institut SANS, 26 % des équipes de sécurité interne mettent 2 à 7 jours à déployer des correctifs sur leurs applications critiques et 22 % mettent 8 à 30 jours.

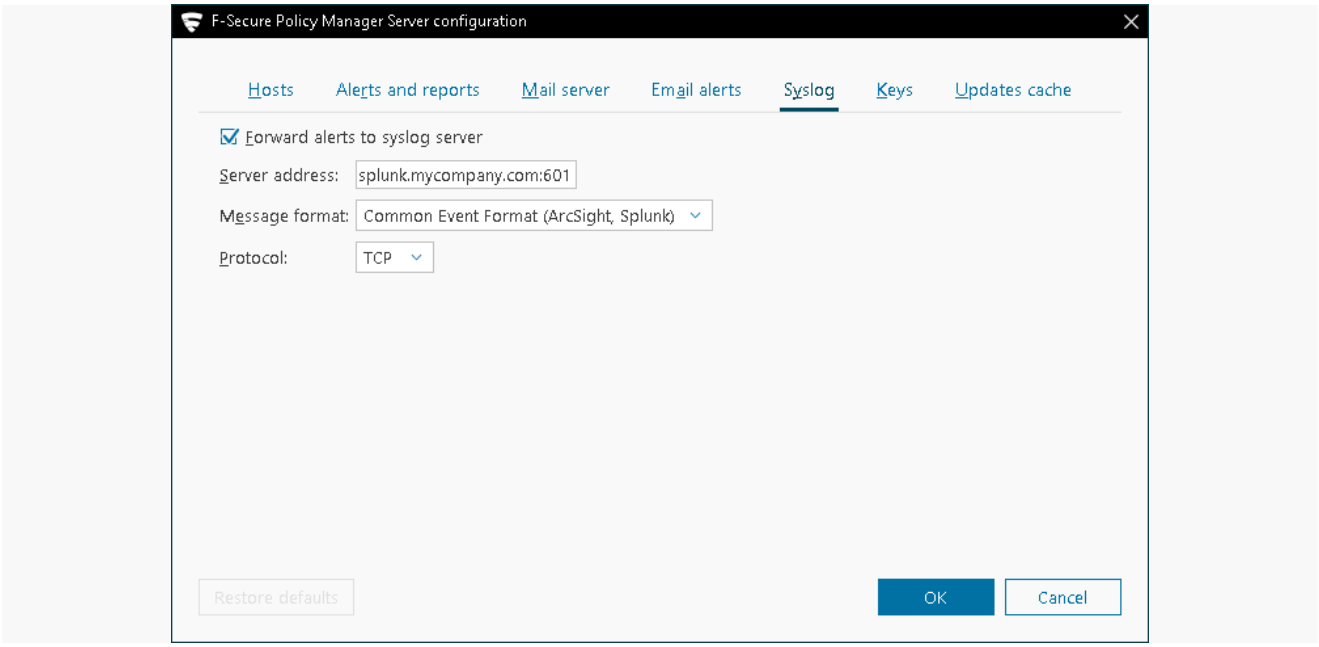
Business Suite Premium et Policy Manager simplifient la gestion des mises à jour logicielles pour tous les hôtes ayant installé Software Updater. Avec Policy Manager, vous pouvez vérifier l'état de toutes les mises à jour logicielles sur le réseau et les installer automatiquement sur les ordinateurs et serveurs Windows. Vous pouvez également désactiver l'installation automatique pour certaines de ces mises à jour, afin de les réaliser manuellement pour des cas spécifiques nécessitant une attention particulière.

Alertes - Visibilité et gain de temps dans la résolution des problèmes

Réglez tout type de problème rapidement et sans complications. L'interface Policy Manager vous donne une vue d'ensemble sur toutes les alertes provenant du réseau ou bien d'un serveur/poste de travail spécifique. Vous pouvez configurer ces alertes pour qu'elles soient transmises par e-mail ou au serveur Syslog de votre entreprise.

Transfert d'alertes pour une intégration SIEM facile

Avec Policy Manager, vous pouvez transférer des alertes de sécurité pour intégrer la protection Business Suite aux SIEM (systèmes de gestion des informations et des événements de sécurité) existants de votre entreprise. Vous obtenez ainsi des informations immédiates sur la sécurité de votre réseau géré, avec un impact minimal sur votre configuration actuelle.



Active Directory - La gestion réseau est simplifiée grâce à la synchronisation

Active Directory, le service d'annuaire de Microsoft, est largement utilisé comme système centralisé pour l'automatisation de la gestion réseau des données des utilisateurs et des ressources distribuées. Vous disposez de plusieurs options pour interconnecter votre Policy Manager et votre structure Active Directory existante :

- Si vous souhaitez répliquer entièrement votre arborescence Active Directory dans Policy Manager et la synchroniser automatiquement, vous pouvez créer une règle de synchronisation mettant automatiquement à jour Policy Manager avec toutes les modifications d'Active Directory.
- Si vous souhaitez répliquer votre Active Directory dans Policy Manager mais ne pas le synchroniser automatiquement, vous pouvez créer une règle de notification vous informant de tout nouvel hôte non-géré, que vous pouvez ensuite ajouter manuellement à l'arborescence Policy Manager. Cette option vous permet de surveiller le réseau pour détecter les hôtes non-protégés.
- Si vous souhaitez uniquement importer l'arborescence Active Directory sans synchronisation ni surveillance des modifications futures, vous pouvez importer la structure Active Directory de manière ponctuelle.

Opérations - mises à jour des définitions de malware et exécution d'analyses

Dans l'onglet « Opérations », vous pouvez lancer à distance des analyses malware pour des hôtes ou des domaines. Vous pouvez également vérifier le statut des dernières définitions de malware et les diffuser sur votre réseau. L'outil de diagnostic de F-Secure peut être exécuté à distance sur n'importe quel hôte. Le module de diagnostic est automatiquement disponible dans Policy Manager. Vous pouvez isoler les hôtes problématiques ou suspects, afin de pouvoir les examiner plus en détail, avant qu'ils ne constituent une menace à l'échelle de votre réseau.

Proxy de Policy Manager

Le Proxy de Policy Manager offre une solution aux problèmes de bande passante dans les installations distribuées de produits F-Secure. Cet outil réduit considérablement la charge des réseaux aux connexions lentes en récupérant les mises à jour des bases de données à partir d'un dépôt de mises à jour local plutôt qu'à partir du serveur F-Secure Policy Manager. Le proxy de F-Secure Policy Manager réside sur un ordinateur du réseau distant. Ce proxy doit être installé pour tous les réseaux connectés à des lignes réseau lentes, pour récupérer les mises à jour de la base de données à partir de F-Secure Policy Manager Server, et ensuite les distribuer localement aux postes de travail. Les postes de travail des bureaux distants communiquent aussi directement avec le serveur Policy Manager du bureau principal, mais cette communication est limitée à la gestion et à l'alerte à distance. Les lourdes mises à jour de la base de données sont redirigées vers le serveur mandataire de Policy Manager du même réseau local.

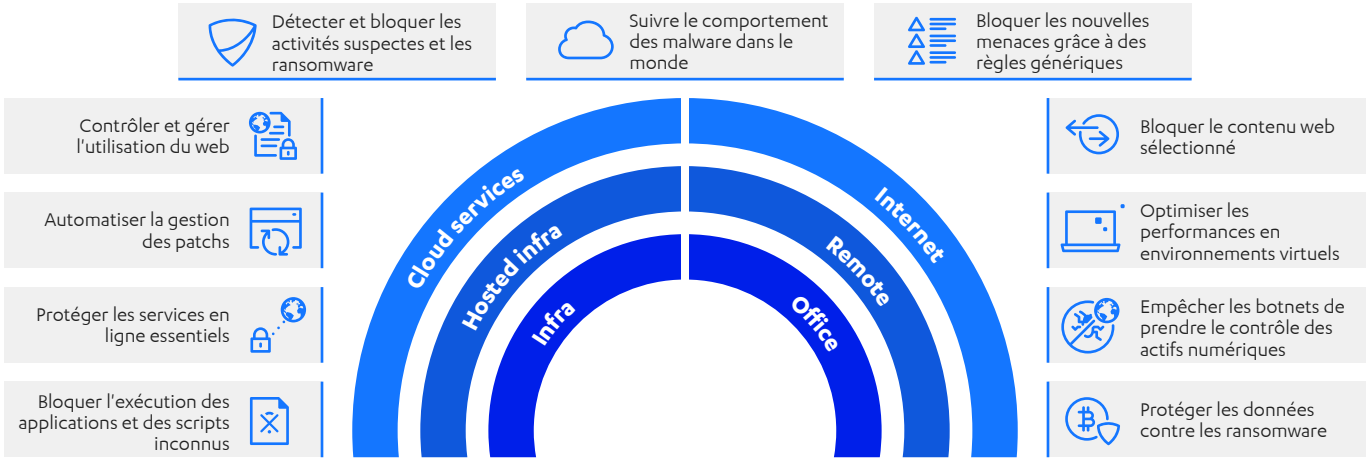
Proxy nouvelle-génération de Policy Manager

Le Proxy de Policy Manager est un outil de Policy Manager Server : il transmet certaines requêtes à un serveur maître tout en distribuant localement les mises à jour logicielles. Le serveur maître est alors déchargé d'une partie substantielle du trafic, et peut optimiser un trafic coûteux et à forte latence. Des connexions sécurisées sont utilisées à la fois entre les hôtes et le proxy, et entre le proxy et le serveur maître. Les certificats des nœuds de proxy doivent être préconfigurés à cette fin.

Résumé

Policy Manager vous donne un contrôle total sur tous les aspects de la sécurité réseau. Il vous suffit de procéder au déploiement. Vous pouvez tout gérer, qu'il s'agisse de la sécurité des endpoints, de l'accès aux serveurs e-mails, de la navigation ou encore des mises à jour de logiciels. Vous pouvez mettre en place des contrôles automatisés et personnalisés, et définir les politiques de sécurité adaptées.

4. PROTECTION DES CLIENTS ET DES ENDPOINTS



Conçu pour les environnements physiques, virtuels et cloud, F-Secure Client Security offre une sécurité de pointe pour tous les postes de travail Windows, qu'il s'agisse d'ordinateurs de bureau ou d'ordinateurs portables. Ses nombreuses couches de protection, ses technologies innovantes et ses fonctionnalités à valeur ajoutée confère aux entreprises une protection sans précédent. Avec Client Security, vous évitez les interruptions d'activité, vous gagnez du temps grâce à la gestion automatique des correctifs et vous renforcez votre productivité grâce aux contrôles des contenus web. Client Security assure une protection totale des endpoints, pour empêcher les malware d'atteindre votre réseau.

F-Secure Client Security est disponible en versions Standard et Premium. Cet outil comprend un haut-niveau de protection, une sécurité renforcée pour les activités sensibles comme les opérations bancaires, des patchs logiciels automatisés pour plus de 2 500 applications indépendantes, et bien plus encore.

Protection endpoint multi-niveaux

La réalité informatique devient plus complexe et les cyber menaces évoluent plus rapidement. Les moteurs d'analyse de fichiers ne représentent plus désormais qu'un simple niveau de sécurité, dans une approche devenue multi-couches. La vérification de la réputation des fichiers et des sites web sur le cloud, l'analyse comportementale et les systèmes de prévention des intrusions basé sur l'hôte (HIPS) constituent désormais des éléments à part entière des systèmes actuels de protection pro-active.

L'approche multi-niveaux de F-Secure comprend les modules suivants, chacun étant conçu pour traiter un aspect particulier de l'écosystème des cyber menaces. Tous ces outils travaillent ensemble pour fournir une solution intégrale :

Software Updater
Mise à jour automatique des applications Microsoft et de plus de 2500 logiciels tiers.

DeepGuard
Moteur anti-malware intelligent et heuristique offrant une capacité de détection 0-day.

F-Secure DeepGuard
Lire le livre blanc

Web content control
Améliorez la sécurité et la productivité de votre entreprise grâce à un accès contrôlé aux sites web. Bloquez l'accès à certains sites en fonction de leur catégorie.

Connection control

Sécurité supplémentaire pour les transactions sensibles telles que les opérations bancaires en ligne.

Real-time protection

F-Secure Security Cloud protège contre les nouveaux malware. Cet outil exploite des données sur les menaces relevées par d'autres ordinateurs protégés, pour permettre une réponse beaucoup plus efficace.

Anti-malware multi-moteurs

Protection inégalée grâce à un anti-malware multi-moteurs très avancé.

Firewall

Règles et fonctionnalités de gestion supplémentaires, intégrées au firewall Windows.

Protection de la navigation

Empêchez les employés d'accéder à des sites nuisibles contenant des liens ou des contenus malveillants.

Device control

Contrôle de l'accès aux périphériques USB.

Botnet Blocker

Stoppez les hackers qui cherchent à contrôler vos actifs informatiques en bloquant la communication avec les domaines Command & Control.

DataGuard

Protection supplémentaire contre les ransomware, pour éviter la destruction et l'altération des données.

Application Control

Blocage des applications et des scripts selon les règles créées par nos testeurs d'intrusion ou par l'administrateur.

Renforcez votre sécurité - Contrôlez l'utilisation du web

Comme nous l'avons déjà mentionné, la plupart des attaques et des téléchargements de malware ont lieu sur internet. Toute protection efficace doit donc intervenir avant que l'ordinateur ne soit atteint, en neutralisant les points d'infection possibles. C'est là que Browsing Protection entre en jeu.

La protection de la navigation web empêche les utilisateurs de visiter par inadvertance des sites légitimes piratés ou des sites malveillants. Pour ce faire, elle fournit une évaluation critique de la sécurité des sites web. Si le site est connu pour être malveillant, ou s'il contient des caractéristiques qui le rendent suspect, l'utilisateur est mis en garde. Or, les sites internet se comptent par millions et ils évoluent sans cesse : pour rester efficace, la protection de la navigation envoie des requêtes au Security Cloud de F-Secure. Ce cloud de sécurité abrite une base de données répertoriant les sites/fichiers sûrs et malveillants connus. Ces données sont mises à jour automatiquement, en temps réel, grâce à des systèmes de machine learning et d'intelligence artificielle conçus par les laboratoires F-Secure.

Web Traffic Scanning - Analyse du trafic web

Certaines technologies, telles que Java, Flash, Windows, Silverlight, les fichiers exécutables et les composants Active X sont des cibles typiques pour les kits d'exploitation. En 2015, Flash représentait plus de 80 % (100 % selon certaines sources) des 10 premiers exploits utilisés par les différents kits d'exploitation. Aujourd'hui, les pirates informatiques continuent à cibler des composants populaires.

Protection avancée

En bloquant ces contenus, vous protégez les utilisateurs de votre entreprise contre les vulnérabilités typiques des sites web. Vous stoppez ainsi de facto un grand nombre d'incidents. La protection avancée de Web Traffic Scanning permet de bloquer les contenus ne disposant pas de données de réputation fiables ainsi que les sites classés comme suspects par F-Secure. Les administrateurs peuvent également établir une liste blanche de certains sites web de confiance.

Botnet Blocker

La plupart des attaques de malware reposent sur des botnets. Ces botnets doivent communiquer entre eux, ce qu'ils font généralement par l'intermédiaire des domaines Command & Control. Ces domaines sont souvent utilisés par les cyber criminels pour s'établir sur les réseaux.Les botnets sont comme des portes dérobées automatisées donnant accès au réseau de l'entreprise. Il arrive que ces portes puissent même être louées par les pirates informatiques, à des prix abordables.

Une fois actifs, les botnets effectuent diverses tâches, comme la collecte de données, la surveillance des actions de l'utilisateur, etc. Botnet Blocker vous permet de bloquer efficacement ces réseaux de bots et les ransomware, en ajoutant une couche de protection permettant d'intercepter les malware à différents stades. Botnet Blocker empêche les agents botnets de communiquer avec leurs serveurs Command & Control. Il bloque les requêtes DNS pour les domaines ayant une réputation malveillante. Les botnets se retrouvent alors dans l'incapacité d'agir. Par ailleurs, la majorité des pirates informatiques utilisent des domaines jetables dans leur chaîne d'infection. Botnet Blocker empêche la résolution de ces domaines uniques, pour éviter toute infection en premier lieu.

Web Content Control

Jusqu'à 89 % des salariés admettent gaspiller du temps chaque jour au travail, 4 % d'entre eux consacrent même jusqu'à la moitié de leur journée de travail aux réseaux sociaux et à d'autres questions non liées au travail. L'accès illimité à internet a des répercussions sur la productivité. Avec Web Content Control, vous pouvez limiter l'utilisation d'internet pour n'autoriser que les contenus pertinents et éliminer une grande partie de la surface d'attaque. Cet outil catégorise les sites web en fonction de leurs contenus, par exemple « jeux d'argent » ou « divertissement ». Vous pouvez ensuite bloquer de manière sélective ceux dont vous jugez le contenu indésirable. Lorsque les utilisateurs tentent d'accéder à un site dont le contenu est interdit, ils voient dans leur navigateur une page indiquant que le site a été bloqué par le service informatique.

Connection Control

À quelques exceptions près, presque tous les malware bancaires nécessitent une connexion internet active en temps réel à leur serveur de Command & Control (C&C). Via cette connexion, ces malware peuvent recevoir des commandes de la part des hackers et recevoir des instructions pour leur transmettre les données volées. Cette connexion en temps réel est vitale pour le malware bancaire, car toute connexion fixe encodée dans les fichiers binaires serait très facile à retrouver et à fermer. Connection Control protège les transactions bancaires ou paiements en ligne sécurisés en bloquant toutes les connexions non-pertinentes. Toutes les données transmises pendant la transaction sont ainsi protégées contre l'interception et le vol.

5. GESTION DU SERVEUR

En moyenne, 90 % des attaques de malware sont stoppées par les solutions anti-malware traditionnelles. Mais les logiciels malveillants deviennent de plus en plus sophistiqués et résistent activement.

75 % des attaques sont opportunistes. Chacun est, de ce fait, une cible potentielle. Les serveurs et systèmes de courrier électronique font encore couramment l'objet de cyber attaques. Une intrusion informatique peut avoir des conséquences extrêmement graves et mettre en danger toute l'entreprise. Il est donc crucial de stopper les attaques avant qu'elles n'atteignent votre réseau.

F-Secure Server Security est une solution serveur. Elle protège vos serveurs sur site, vos serveurs virtuels et cloud contre les malware et les vulnérabilités logicielles, sans ralentir vos systèmes.

Server Security offre une protection en temps réel améliorée contre les virus, les logiciels espions et les logiciels à risque. Cette technologie permet une détection pro-active comportementale des nouvelles menaces, grâce à la technologie récompensée DeepGuard de F-Secure. Grâce à sa fonctionnalité de mise à jour des logiciels, Email and Server Security maintient le système d'exploitation et les logiciels serveur à jour, pour les protéger contre les cyber menaces ciblant les vulnérabilités.

Avec Policy Manager et Server Security, vous disposez d'une solution puissante et centralisée pour protéger vos serveurs, vos services de messagerie et vos systèmes de collaboration. Vous pouvez monitorer l'ensemble de votre environnement informatique, physique ou virtuel, et en assurer le bon fonctionnement. Server Security est disponible en deux versions : Standard et Premium. La version Premium comprend Software Updater, une solution clé-en-main mettant automatiquement à jour les logiciels tiers installés sur les serveurs.

Fnctionnalités	**F-Secure Server Security**	**F-Secure Server Security Premium**	**F-Secure Email and Server Security Standard**	**F-Secure Email and Server Security Premium**	**F-Secure Linux Server Security**
Protection anti-malware et spyware	•	•	•	•	•
DeepGuard™	•	•	•	•	
Web traffic scanning	•	•	•	•	•
Protection de la navigation	•	•	•	•	
Offload Scanning Agent for Virtual environments and cloud workloads	•	•	•	•	
Spam Control			•	•	
Email Quarantine Manager			•	•	
Software Updater		•		•	
Integrity checking					•
Firewall	•	•	•	•	•
Anti-Malware for Microsoft® Exchange			•	•	
Anti-Malware for Microsoft® SharePoint			•	•	
EMC CAVA support				•	

F-Secure Email and Server Security comprend les fonctionnalités suivantes :

Protection contre les malware et les logiciels espions

Protégez votre ordinateur contre les virus, les chevaux de Troie, les logiciels espions, les rootkits et les autres malware.

DeepGuard™

Une protection pro-active et instantanée contre les cyber menaces inconnues. Elle surveille le comportement des applications et bloque en temps réel les activités potentiellement dangereuses.

DeepGuard - Protection proactive, depuis l'hôte, contre les cyber menaces nouvelles et émergentes

https://www.f-secure.com/documents/996508/1030745/deepguard_whitepaper.pdf

Analyse du trafic web

Détection et blocage des contenus malveillants du trafic web (protocole HTTP), pour une protection supplémentaire contre les malware

Protection de la navigation

Protection des utilisateurs contre les exploits ciblant les navigateurs web et les sites web malveillants

Offload Scanning Agent pour les environnements virtuels et les charges de travail cloud

Déchargement (offloading) de la recherche de malware sur le serveur d'analyse et de réputation F-Secure, en environnements virtuels et cloud

Contrôle anti-spams

Détection et filtrage anti-spam provenant du trafic e-mails grâce à une protection en temps réel contre tous les types de spams, quels que soient leur contenu, leur format ou leur langue.

Email Quarantine Manager

Outil permettant aux utilisateurs autorisés de gérer les e-mails en quarantaine. Possibilité de relâcher, retraiter ou supprimer les e-mails ou pièces jointes placés en quarantaine.

Software Updater

Pour maintenir votre système et vos applications à jour en installant les correctifs, à mesure qu'ils sont publiés par les fournisseurs.

Integrity Checking

Protection des serveurs Linux contre les modifications non-autorisées.

Firewall

Protection des serveurs et des ordinateurs contre les tentatives de connexion non-autorisées.

Protection for Microsoft® Exchange

Protection du trafic de courrier entrant, sortant et interne. Protection des dossiers publics Exchange contre les malware et les autres cyber menaces. Filtrage du contenu et des pièces jointes.

Protection for Microsoft® SharePoint

Protection en temps réel des serveurs Microsoft® SharePoint. Analyse du contenu téléchargé en amont et en aval, pour détecter les malware et les autres menaces de sécurité.

Citrix® XenAPP

Protection anti-malware en environnement Citrix® XenAPP.

Prise en charge Isilon & EMC CAVA

Protection anti-malware pour les serveurs de stockage EMC via la prise en charge Isilon ou Celerra Anti Virus Agent.

6. MICROSOFT® EXCHANGE, MICROSOFT® SHAREPOINT ET CITRIX® SECURITY

F-Secure Email and Server Security est une solution puissante et complète conçue pour protéger les serveurs de messagerie et groupware de votre entreprise. Cette solution protège le réseau contre tout code malveillant transitant par HTTP ou SMTP. Elle protège également le réseau contre les spams.

Email and Server Security constitue la première ligne de défense contre les menaces 0-day et les vulnérabilités connues.

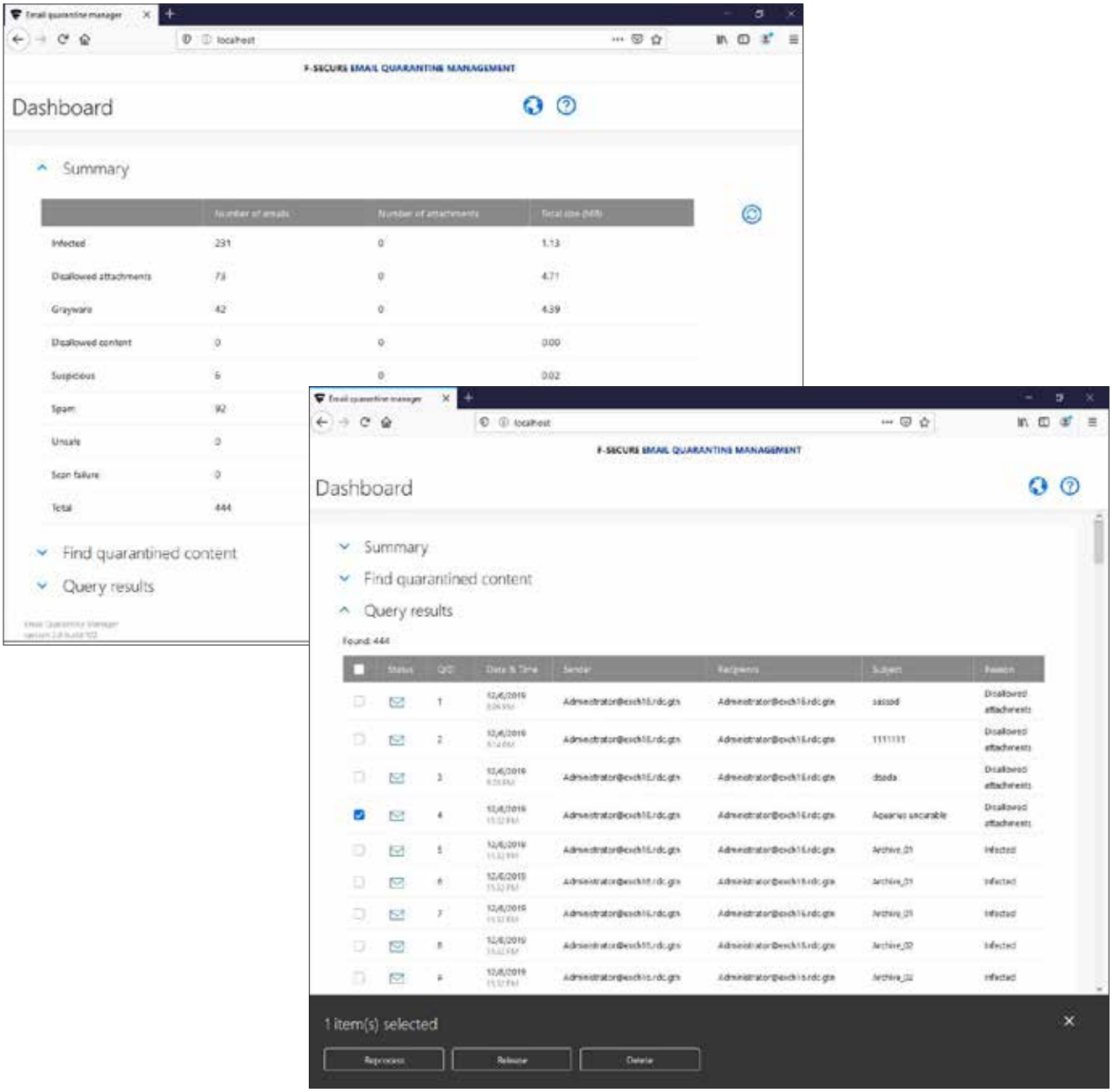
Email and Server Security contient un anti-malware et un anti-spam pour les serveurs de messagerie Microsoft® Exchange, un anti-malware pour les serveurs Microsoft® Terminal Servers et Citrix®, Microsoft® SharePoint et prend en charge EMC CAVA.

Utilisé sur un serveur de messagerie Exchange, Email and Server Security analyse les pièces jointes et le corps des messages à la recherche de codes malveillants. Email and Server Security est installé directement sur un serveur Microsoft® Exchange. Il intercepte les messages à destination et en provenance des boîtes mails, ainsi que les dossiers publics. Si le courrier intercepté contient un code malveillant, Email and Server Security peut être configuré pour désinfecter ou supprimer le contenu. Les pièces jointes et codes malveillants peuvent être placés en quarantaine, pour une analyse plus poussée. Email and Server Security peut également être configuré pour supprimer certaines pièces jointes en fonction du nom ou de l'extension des fichiers.

7. EMAIL QUARANTINE MANAGEMENT

F-Secure Email Quarantine Manager permet au personnel non-administrateur de traiter les messages et les pièces jointes placés en quarantaine par Email and Server Security. Cette quarantaine sert de base sécurisée où peuvent être conservés les fichiers potentiellement dangereux. Une fois mis en quarantaine, les logiciels malveillants, espions ou à risque sont dans l'incapacité de se propager ou de causer des dommages. Si vous devez autoriser l'accès à des applications, des fichiers ou des messages électroniques mis en quarantaine, il est possible de les restaurer.

Email Quarantine Manager vous permet de répartir les responsabilités liées au traitement des contenus mis en quarantaine. Par exemple, il devient possible de permettre aux équipes d'assistance de gérer la quarantaine, sans pour autant attribuer de droits de niveau administrateur ou donner accès à la totalité des paramètres de Email and Server Security.



8. LINUX SECURITY

Linux Security peut être utilisé pour protéger à la fois les serveurs et les postes de travail Linux. Policy Manager permet une gestion centralisée (une gestion autonome est également possible, via une interface utilisateur web locale).

L'analyse en temps réel vous offre une protection continue contre les virus et les applications potentiellement indésirables, à mesure que les fichiers sont ouverts, copiés et téléchargés sur le web.

L'analyse en temps réel fonctionne en arrière-plan, en recherchant les virus chaque fois que vous accédez à des fichiers sur le disque dur, les supports amovibles ou les lecteurs réseau. Si vous tentez d'accéder à un fichier infecté, la protection en temps réel bloque automatiquement l'exécution du virus. L'analyse en temps réel est destinée à analyser des ensembles limités de fichiers.

L'analyse manuelle, quant à elle, peut être utilisée pour analyser le système au complet. Vous pouvez également utiliser l'analyse programmée pour analyser l'ensemble du système à intervalles réguliers.

Les mises à jour automatiques permettent de garder les définitions de virus à jour, à tout moment. Les bases de données de définitions de virus sont mises à jour automatiquement après l'installation. Les mises à jour des définitions de virus sont assurées par F-Secure.

Le système de prévention des intrusions sur l'hôte (HIPS) détecte toute activité malveillante au niveau de l'hôte, pour protéger le système sur plusieurs niveaux.

Integrity Checking protège le système contre les modifications non-autorisées. Cet outil fonctionne selon le principe de la « bonne configuration a priori » : il doit être installé avant que l'ordinateur ne soit connecté au réseau, pour que le système possède d'emblée la configuration adéquate. Vous pouvez créer une liste des fichiers système à protéger et bloquer l'utilisation d'éventuels fichiers modifiés.

Notre Firewall filtre les paquets de manière dynamique en s'appuyant sur Netfilter et iptables. Il protège les ordinateurs contre les tentatives de connexion non-autorisées. Des profils de sécurité pré-définis, adaptés aux cas d'utilisation courants, permettent de définir le trafic autorisé/refusé.

Si un pirate informatique obtient un accès shell au système et tente d'ajouter un compte utilisateur, le système de prévention des intrusions sur l'hôte (HIPS) détectera les fichiers système modifiés et alertera l'administrateur. S'il accède au système et tente d'installer un rootkit sur un espace utilisateur en remplaçant divers utilitaires-système, le HIPS détectera également les fichiers système modifiés et, de la même manière, l'utilisateur sera alerté.

Fonctionnalités-clés et avantages

Protection supérieure contre les virus et les vers

Analyse des fichiers sur tous les systèmes compatibles Linux. Il s'agit de la solution idéale pour les ordinateurs exécutant plusieurs systèmes d'exploitation différents via un utilitaire multiboot.

Invisibilité

L'outil est totalement invisible pour les utilisateurs finaux.

Protection des fichiers système critiques

Les informations critiques contenues dans les fichiers système sont stockées et automatiquement vérifiées avant qu'un accès n'y soit autorisé.

Déploiement et gestion faciles

Les paramètres par défaut s'appliquent à la plupart des systèmes et cet outil peut être mis en service sans aucune configuration supplémentaire.

Options d'alerte avancées

Cet outil dispose de fonctions de surveillance et d'alerte étendues pouvant être utilisées pour notifier les contenus infectés à un administrateur réseau.

Adapté au cloud

Prise en charge d'un large éventail de distributions Linux, notamment Amazon Linux.

9. SÉCURITÉ VIRTUELLE ET PROTECTION DES CHARGES DE TRAVAIL CLOUD

La virtualisation offre de nombreux avantages, tels que la flexibilité, l'optimisation des ressources et l'efficacité opérationnelle. Mais elle crée de nouveaux défis liés aux capacités hardware limitées et aux utilisations partagées. Ces problématiques ont un impact sur la virtualisation des postes de travail et des serveurs.

Il appartient à la fois aux fournisseurs de services de cloud public et à leurs clients d'assurer la sécurité du cloud public et le respect des réglementations. C'est une responsabilité partagée. Malgré le transfert des charges de travail vers le cloud, c'est au client qu'il incombe de gérer les vulnérabilités, les exploits et la protection contre les logiciels malveillants.

La sécurité virtuelle et la protection des charges de travail sur le cloud permettent de décharger les opérations d'analyse consommatrices de ressources vers des serveurs d'analyse et de réputation (SRS) dédiés. Ce type de procédé réduit les besoins en processeur et en mémoire pour les machines virtuelles et les charges de travail sur le cloud.

F-Secure Virtual Security est disponible pour les plateformes de virtualisation les plus populaires : VMware, Citrix®, Hyper-V et KVM. La solution est un hyperviseur-agnostique et peut donc être déployée en cloud privé ou public.

Les machines virtuelles sont sécurisées par les installations standard de F-Secure Client Security (postes de travail), Server Security (serveurs de fichiers) ou Email and Server Security. Pour de meilleures performances, la solution utilise l'agent d'analyse de déchargement (OSA) pour déplacer les tâches d'analyse consommatrices de ressources vers un serveur d'analyse et de réputation (Scanning and Reputation Server) dédié.

Vous pouvez ainsi effectuer des analyses complètes sur les hôtes virtuels, sans craindre les pics d'utilisation de la mémoire et du processeur à l'échelle du cluster.

Un seul serveur F-Secure Scanning and Reputation Server (SRS) peut gérer la charge d'analyse pour un maximum de 130 machines virtuelles.

La sécurité virtuelle peut être déployée sur un seul hôte physique ou sur un cluster.

- Un seul hôte physique : la configuration la plus simple de F-Secure Virtual Security repose sur un seul ordinateur hôte physique qui exécute un certain nombre de postes de travail Windows virtuels.
- Clustering : plusieurs hôtes physiques se comportent comme un seul ordinateur. Un hôte physique ou un cluster peut faire fonctionner plus d'un groupe isolé de machines virtuelles.

Avantages

- Hyperviseur-agnostique, peut être déployé dans n'importe quel environnement de virtualisation (VI ou VDI)
- Déchargement (offloading) des opérations d'analyse consommatrices de performances sur un serveur dédié à l'analyse et à la réputation
- Protection pro-active, comportementale, contre les malware, les exploits, le phishing et les attaques réseau
- Réduction de la consommation de mémoire, de processeur et d'espace disque des machines virtuelles, pour réaliser des économies pour les environnements informatiques étendus
- Un modèle de tarification simple et un coût total abordable, avec un seul forfait couvrant les environnements clouds physiques, virtuels, privés et publics

RÉFÉRENCES

1. DeepGuard - Protection proactive sur l'hôte contre les menaces nouvelles et émergentes| https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163346/F-Secure_DeepGuard.pdf

2. F-Secure Security Cloud – Objectif, fonctions et avantages | https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163353/F-Secure_Security_Cloud.pdf

3. Ransomware : Prévenir, prévoir, détecter et réondre | https://blog-assets.f-secure.com/wp-content/uploads/2019/11/20112058/ransomware_ppdr_2019.pdf

À PROPOS DE F-SECURE

Fondée en 1988, F-Secure est une entreprise finlandaise spécialisée en cyber sécurité, cotée au NASDAQ OMX Helsinki Ltd. Depuis plus de trente ans, nous protégeons des dizaines de milliers d'entreprises et des millions de particuliers grâce à notre réseau de partenaires de distribution, et plus de 200 fournisseurs de services.
Des solutions de protection des postes de travail à la détection et réponses aux menaces avancées, nous veillons à ce que nos utilisateurs puissent compter sur une cyber sécurité de haut-niveau. L'alliance unique de l'expertise humaine, de solutions logicielles et d'intelligence artificielle nous permet d'être reconnu comme un acteur incontournable du marché européen.

f-secure.com/fr_FR/ | **twitter.com/fsecurefrance** | **facebook.com/f-secure**

F-Secure