# F-Secure Total - Internet Security module

## Device Protection

Votre sécurité repose sur une base solide. La protection de votre appareil est au cœur de F-Secure Total Protection : le socle indispensable qui protège votre appareil, vos données et vos activités en ligne. Sans cette protection, rien n'est vraiment fiable.

La protection de l'appareil vous protège là où les menaces frappent souvent en premier : les sites web qui tentent de voler vos informations personnelles, les logiciels malveillants qui ciblent votre appareil, les risques pour la vie privée invisibles et les vulnérabilités fondamentales qui laissent votre appareil sans défense. La protection contre le phishing lors de la navigation, l'antivirus, les conseils de confidentialité, la vérification du verrouillage de l'appareil et la vérification de la version du système d'exploitation fonctionnent ensemble comme une première ligne de défense, offrant ainsi une base solide pour le reste de la protection.

## Virus Protection

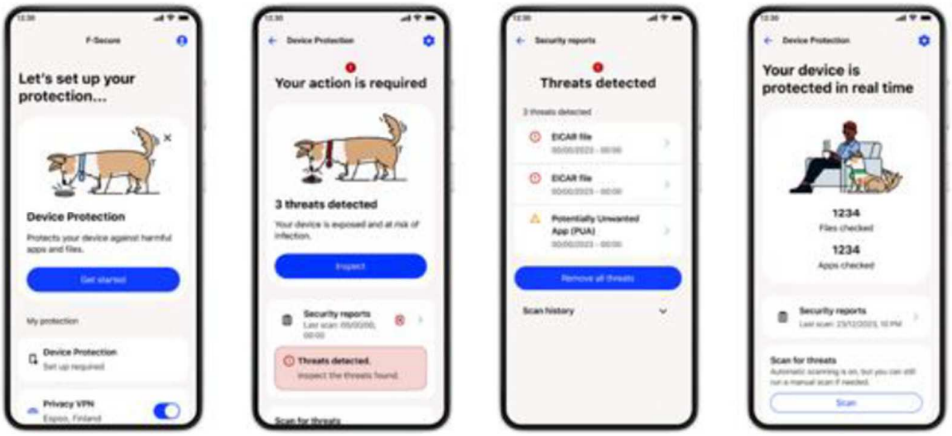
**Aperçu**

La protection antivirus est un élément essentiel de la sécurité de F-Secure Total. F-Secure Total offre une protection contre les logiciels malveillants sur tous les systèmes d'exploitation ouverts, tels que Windows, macOS et Android, particulièrement vulnérables à cette menace. En raison des restrictions d'Apple, cette protection n'est pas disponible pour iOS.

La protection antivirus protège vos clients contre les logiciels malveillants tels que les virus, les chevaux de Troie, les logiciels espions, les rançongiciels et les voleurs d'informations. Ces logiciels malveillants peuvent collecter et diffuser des informations personnelles, espionner les activités en ligne, voire verrouiller toutes leurs données personnelles et exiger une rançon pour les déverrouiller. Les infections par des logiciels malveillants (voleurs d'informations) figurent parmi les incidents de sécurité les plus courants, conduisant à l'usurpation d'identité et à diverses formes de fraude. F-Secure Total protège vos clients en prévenant ces incidents.

Pour prévenir les infections par des logiciels malveillants, tous les fichiers et applications sont analysés automatiquement. Outre les fichiers ou applications manifestement malveillants, Total recherche également les applications potentiellement indésirables susceptibles d'avoir un comportement inapproprié sur l'appareil, comme les outils de marketing agressifs. Les fichiers sont analysés en temps réel, à la demande (analyse manuelle) ou suite à des événements spécifiques, comme l'installation d'une application. Dès qu'un logiciel malveillant ou une application potentiellement indésirable (API) est détecté, l'utilisateur est immédiatement invité à la supprimer. La logique d'analyse dépend du système d'exploitation sous-jacent.

Attention ! La protection antivirus se trouve désormais dans la section « Protection de l'appareil ». Voir les images de Total Android ci-dessous.




**Sécurité du cloud et de l'IA**

En plus des analyses classiques effectuées directement sur l'appareil, F-Secure utilise des technologies d'analyse cloud avancées basées sur l'IA. La réputation des fichiers est vérifiée depuis le cloud, tout comme le moteur d'analyse traditionnel par empreinte digitale le fait depuis la base de données locale. Grâce à la gestion de la réputation dans le cloud, les modifications apportées à la réputation des fichiers sont dynamiques et instantanées. Toute modification est immédiatement appliquée à tous les utilisateurs, garantissant ainsi à chacun un accès permanent à la base de données la plus récente. Les technologies de détection cloud sont disponibles sur toutes les plateformes prises en charge.

Une logique intelligente basée sur le cloud détermine les applications à analyser afin d'optimiser l'utilisation des ressources de l'appareil. Les fichiers d'applications inconnus sont téléchargés et analysés dans le cloud à l'aide de diverses technologies, dont l'IA et l'apprentissage automatique. Les résultats d'analyse sont automatiquement transmis aux autres systèmes, permettant ainsi d'identifier immédiatement le fichier infecté et évitant de devoir prélever le même échantillon auprès d'autres utilisateurs. Les moteurs d'analyse et les bases de données étant gérés dans le cloud, toutes les modifications sont appliquées immédiatement à tous les utilisateurs.

**Détection comportementale**

Le détecteur de détection observe la détection d'une application pour déterminer les actions potentielles les plus diverses qui succèdent au voltooïde. Les détections basées sur la base de données ont dépassé les limites cruciales de la première version de nouveaux logiciels malveillants au moment où une détection s'est produite pour le mot de passe uitgegeven. Grâce à la mise au point de la structure des fonctions identifiées par un échantillon, vous pouvez identifier le programme de détection et les blocs d'activités schadelijke uitvoeren, vous-mêmes avant qu'un échantillon d'œuvres d'art soit détecté et pris en charge.

La détection est également disponible pour Mac. Pour les plus grands utilisateurs de Mac, les fonctionnalités sont pratiques et faciles à utiliser dans les logiciels vertrouwde créés. Telkens veut qu'une application soit examinée par un document, la détection automatique de l'application est contrôlée par un lecteur vert. Alors qu'une application en cours est la meilleure et qu'elle est testée pour vous, le mot du gebruiker om bevraagd avant l'application voir plus loin.

**Protection ransomware**

F-Secure Total PC est un logiciel de ransomware robuste qui s'attaque également aux virus de la fonction de base. Les mots intégrés de recherche de ransomwares ne sont pas à la portée des systèmes de surveillance backend pour une meilleure efficacité. Cela vous amène à utiliser une technologie de détection avancée pour acquérir des ransomwares afin de vous identifier et de vous bloquer pour que vous puissiez les utiliser. Vous souhaitez exécuter une activité contrôlée, bloquée et totalement automatisée dans le processus de planification en toute sécurité.

**Mode Gaming**

F-Secure Total prend en charge le mode de jeu et assure la gestion des jeux sur PC. Le mode de jeu a fait l'objet de très nombreux aménagements, d'installations et de fonctionnalités Windows pour une géooptimisation d'un jeu en cours d'exécution. Dans le mode de jeu, les mises à jour totales génèrent la bande passante et la durée de vie du processeur, des invites écrites, des combinaisons et des notifications (Windows Toasts) ne sont pas générées et des analyses antivirus automatiques ne démarrent pas. F-Secure Total PC est optimisé pour les meilleurs jeux. Les spécifications de votre ordinateur en cours de route avec d'autres produits de surveillance comme Microsoft Defender.

F-Secure Total Mac offre un mode de jeu « léger ». Les utilisateurs effectuent des analyses antivirus pour une période d'indisponibilité des ressources afin d'éviter tout jeu d'autres activités gourmandes en ressources.

| **Protection contre le virus** | **Windows** | **Mac** | **Android** | **iOS** |
|---|---|---|---|---|
| Protection contre le virus | Oui | Oui | Oui | -* |
| Scanners manuels<br><br>*De gebruiker kan een scan op aanvraag uitvoeren* | Oui | Oui | Oui | - |
| Analyse programmée<br><br>*Analyse automatisée de l'intervalle d'acquisition* | Oui | - | Oui | - |
| Scanning en temps réel<br><br>*Analyse les fichiers en continu en arrière-plan.* | Oui | Oui | - | - |
| Analyser les applications pendant | Oui | Oui | Oui | - |

| | | | | |
|---|---|---|---|---|
| l'installation<br>*Analyse les applications dès leur installation sur l'appareil.* | Real-time scanning | Real-time scanning | | |
| Analyse dans le cloud<br>*Vérifie la réputation des fichiers stockés dans le cloud.* | Oui | Oui | Oui | - |
| Protection comportementale<br>*Avertit en cas de comportement risqué de l'application* | Oui<br>Dans l'app + Cloud | Oui<br>Dans l'app + Cloud | Oui<br>Cloud | - |
| Protection contre les ransomwares<br>*Surveille et bloque les comportements suspects des ransomwares* | Oui | Oui | - | - |
| Protection antibot<br>*Détection et suppression des réseaux de bots* | Oui | - | - | - |
| Mode Pause/Analyse<br>*Suspendre les interruptions pendant le jeu.* | Oui | Oui<br>Durée de l'utilisateur | - | - |
| Exemple de soumission | Oui | Oui | Oui | - |

Attention ! Il est impossible d'offrir une protection antivirus pour la plateforme iOS en raison des directives d'Apple. Selon Apple, iOS ne contient aucun logiciel malveillant ; par conséquent, toute fonctionnalité prétendant protéger les utilisateurs contre les logiciels malveillants est une fausse promesse et n'est pas autorisée sur l'App Store.

# Protection contre browsing et phishing

### Aperçu

Une part toujours plus importante de nos activités quotidiennes se déroule en ligne : opérations bancaires, achats, recherche d'informations, réservations, rendez-vous, loisirs, communication, divertissement, etc. La Protection de navigation est conçue pour assurer la sécurité de vos clients sur Internet. Elle protège leur sécurité et leur vie privée et les aide à se prémunir contre les arnaques en les éloignant des pages web visant à collecter des informations personnelles ou à diffuser des contenus malveillants tels que des logiciels malveillants et des exploits.

En interceptant les requêtes de pages web et en vérifiant la réputation des pages web grâce au service de réputation web de F-Secure, la Protection de navigation garantit à vos clients une navigation sécurisée.

## Services de réputation de F-Secure

La Protection du navigateur est un service de réputation qui classe les pages web comme sûres ou non. Les sites non sûrs sont généralement des sites d'hameçonnage ou contenant des logiciels malveillants. La réputation des pages est vérifiée discrètement en arrière-plan pendant la navigation. Ces vérifications sont optimisées pour une expérience de navigation optimale. L'accès aux sites sûrs se fait normalement et sans interruption. L'accès aux sites non sûrs est simplement bloqué par une boîte de dialogue. La Protection du navigateur protège également vos clients contre les fraudes par e-mail ou SMS renvoyant vers de faux sites bancaires, par exemple, à condition qu'ils utilisent un navigateur sécurisé par cette protection.

## Sécurité bancaire

La Sécurité bancaire ajoute une couche de protection supplémentaire à la sécurité de navigation et à la protection antivirus. Tandis que la sécurité de navigation bloque l'accès aux sites web non sécurisés, tels que les faux sites bancaires ou les sites d'hameçonnage connus, la Sécurité bancaire améliore la visibilité et la sécurité lors de la consultation d'un site bancaire sécurisé. La Sécurité de navigation assure une protection discrète en arrière-plan, sans perturber votre navigation. Elle est conçue pour rendre la sécurité plus visible et tangible.

La Sécurité bancaire est l'une des fonctionnalités les plus appréciées des consommateurs en raison du sentiment de sécurité qu'elle procure lors des achats et des opérations bancaires en ligne. Cette fonctionnalité répond également à la principale préoccupation des consommateurs concernant Internet : les pertes d'argent lors d'achats et de transactions bancaires en ligne. Compte tenu de sa grande valeur pour le consommateur, ce composant est constamment amélioré, notamment en optimisant l'ergonomie et le sentiment de sécurité.

La Sécurité bancaire affiche un indicateur (bannière, cadre ou notification) dans le navigateur lorsque l'utilisateur consulte un site bancaire sécurisé et que la connexion est sécurisée (https). La Sécurité de navigation bloque automatiquement l'accès aux sites d'hameçonnage ou aux faux sites bancaires. F-Secure Total pour Windows Protection bancaire empêche également l'établissement d'autres connexions pendant que vous êtes sur un site bancaire sécurisé. Seules les applications de confiance sont autorisées à ouvrir de nouvelles connexions. Concrètement, cela se produit car, lorsqu'une session de Protection bancaire est lancée, toutes les connexions Internet provenant de processus non fiables sont interrompues. Toutes les connexions provenant de processus de confiance sont également vérifiées. Si des processus de confiance se connectent à des adresses IP non fiables ou inconnues, les connexions sont automatiquement bloquées. La Protection bancaire autorise les nouveaux processus de confiance à communiquer avec Internet.

La possibilité de bloquer les connexions non fiables empêche le détournement des sessions bancaires : votre argent est en sécurité. Total pour Windows ferme automatiquement la Protection bancaire une fois votre session bancaire terminée. La Protection bancaire redémarre lorsque vous consultez un autre site bancaire.

La protection contre les outils d'accès à distance (RAT) empêche l'utilisation de ces outils pendant une session bancaire (lorsque la Protection bancaire est activée). Cela empêche les fraudeurs d'utiliser des logiciels d'accès à distance pour commettre des vols sur votre compte bancaire en ligne, par exemple.

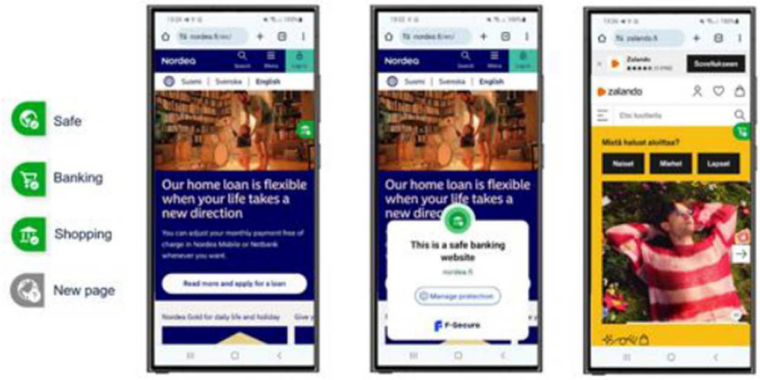
**Protection Safari et Chrome**

Safari Protection ajoute des fonctionnalités de protection de navigation au navigateur Safari natif des iPhone et iPad. De même, Chrome Protection protège le navigateur natif des téléphones et tablettes Android. Les fonctionnalités prises en charge incluent la protection de la navigation, la protection bancaire et la protection des achats (intégrée au module de protection contre la fraude).

Safari Protection et Chrome Protection nécessitent une configuration utilisateur. L'installation se fait via une tâche intelligente dans l'application. L'utilisateur est guidé tout au long du processus. Une fois activée, la navigation sur Internet avec le navigateur natif est protégée contre les sites web dangereux, tels que les sites contenant des logiciels malveillants connus et les sites d'hameçonnage.

Différents indicateurs s'affichent selon le type de page consultée. Les pages sécurisées sont marquées en vert. Les sites web sécurisés pour les achats et les opérations bancaires sont signalés séparément.

Safari Protection (voir images ci-dessous) affiche un indicateur de réputation de la page directement dans les résultats de recherche, permettant d'éviter facilement les pages non sécurisées. Un clic sur l'indicateur permet d'afficher plus de détails. L'accès aux pages non sécurisées est bloqué si l'utilisateur clique accidentellement sur un lien malveillant.




Les protections Safari et Chrome (voir images ci-dessus) affichent un indicateur de réputation de la page en surimpression pendant la navigation. L'utilisateur peut déplacer cet indicateur à l'écran sans perturber sa navigation. L'indicateur indique immédiatement le type de page web : sécurisée, bancaire, d'achat ou nouvelle/non analysée. En cliquant dessus, l'utilisateur peut consulter plus de détails. L'accès aux pages non sécurisées est bloqué.

Remarque ! La protection contre les achats fait partie de la fonctionnalité « Protection contre les arnaques ». Consultez la section « Protection contre les arnaques » de ce document pour plus d'informations.

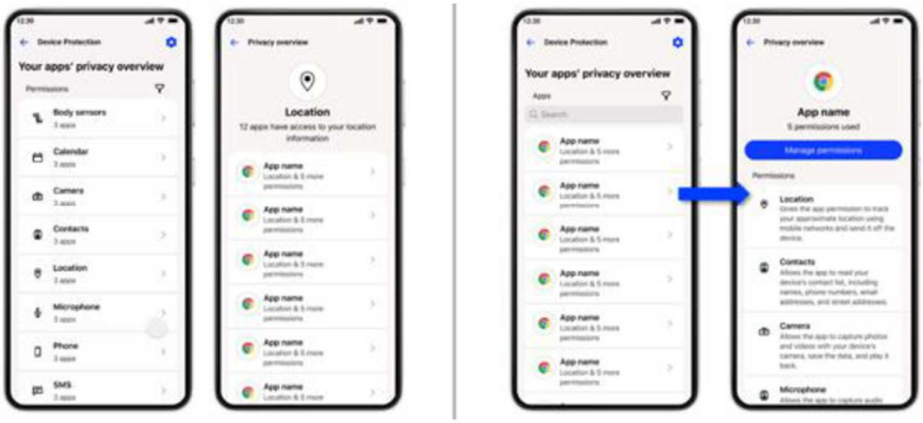
| **Protection contre la navigation indésirable et l'hameçonnage** | **Windows** | **Mac** | **Android** | **iOS** |
|---|---|---|---|---|
| La sécurité du navigateur<br><br>*vérifie la réputation des sites web* | Oui | Oui | Oui | Oui |
| Navigateurs compatibles<br><br>*Navigateurs compatibles avec cette fonctionnalité* | Edge, Chrome, and Firefox | Safari, Edge, Chrome, et Firefox | Chrome, | Safari |
| Bloque l'accès aux sites web dangereux<br><br>*Bloque les sites web d'hameçonnage et de logiciels malveillants* | Oui | Oui | Oui | Oui |
| Indicateur d'environnement bancaire sécurisé<br><br>*Indique si vous vous trouvez dans un environnement bancaire sécurisé et que la connexion est sécurisée (protocole HTTPS utilisé).* | Oui | Oui | Oui | Oui |
| Sécurité bancaire activée automatiquement<br><br>*Activation automatique lors de la consultation du site web de votre banque* | Oui | Oui | Oui<br><br>Accès unique | Oui<br><br>Accès unique |

| | | | | |
|---|---|---|---|---|
| Bloque les processus inconnus<br><br>*Bloque les connexions provenant de processus non fiables lorsque la protection bancaire est activée* | Oui | - | - | - |
| Bloque les connexions inconnues<br><br>*Bloque les connexions inconnues provenant de processus de confiance lorsque la sécurité bancaire est activée* | Oui | - | - | - |
| Bloque les outils d'accès à distance<br><br>*Bloque les outils d'accès à distance lorsque la sécurité bancaire est activée* | Oui | - | - | - |

Attention ! Safe Browser (mobile) sera progressivement supprimé fin 2025, car la protection est activée dans les navigateurs mobiles standard Safari et Chrome.

## Conseiller en matière de confidentialité

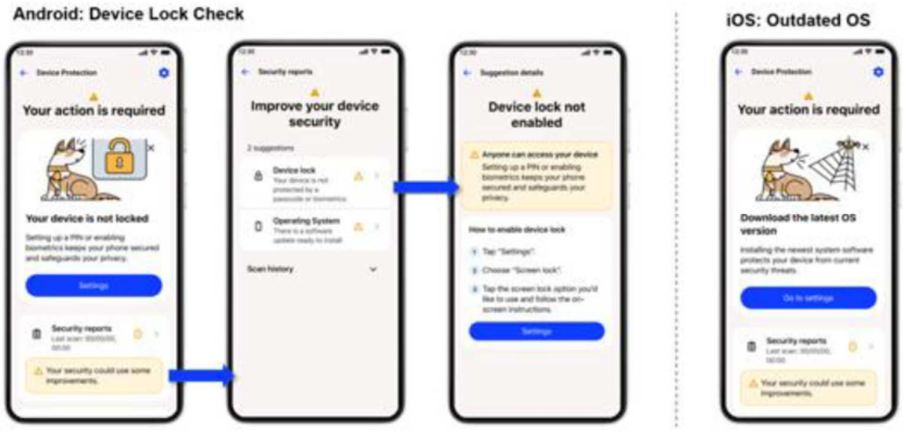
Zelfs veilige and betrouwbare apps kunnen Zeer uitgebreide machtigingen op the apparaat van de gebruiker aanvragen. Privacy Advisor est une nouvelle fonction de F-Secure Total pour Android, qui vous permet de contrôler les applications d'utilisation de vos appareils. Le marché est spécialisé dans l'utilisation de critères de localisation, de contacts, de photos, etc., pour garantir la protection de la vie privée des utilisateurs dans le cadre de leurs activités. La manière dont les applications sont filtrées sur la base de l'usinage aide les utilisateurs à se rendre de l'application en même temps est en mesure de les utiliser.




## Vérifier le verrouillage de l'appareil

Le verrouillage de l'écran est probablement la fonction de sécurité la plus importante d'un téléphone. Il empêche tout accès non autorisé à l'appareil, aux données de l'utilisateur et à toutes les applications et services. C'est particulièrement important pour les appareils mobiles, car ils peuvent facilement être perdus ou volés.

La fonction de verrouillage vérifie si l'utilisateur a activé le verrouillage de l'écran. Si ce n'est pas le cas, elle signale ce risque de sécurité et guide l'utilisateur pour le configurer dans les paramètres de l'appareil. Une fois la configuration effectuée, l'utilisateur n'a plus à s'en soucier.



### Vérifiez si votre système d'exploitation est obsolète

Les appareils mobiles donnent souvent une fausse impression de sécurité. De nombreuses activités paraissent moins sérieuses lorsqu'elles sont effectuées sur un téléphone ou une tablette, et les menaces semblent moins probables et moins graves. L'un des symptômes de ce phénomène est le défaut de mise à jour des applications et du système d'exploitation.

Quelle que soit la plateforme, des mises à jour du système d'exploitation sont régulièrement publiées afin d'introduire de nouvelles fonctionnalités, d'améliorer l'ergonomie et de corriger les bugs et les failles de sécurité. Du point de vue de la sécurité, un système d'exploitation obsolète représente un risque majeur pour la sécurité et la confidentialité des utilisateurs. Les cybercriminels recherchent constamment de nouvelles façons d'accéder à des informations personnelles sensibles, telles que les données bancaires. Un système d'exploitation non mis à jour leur permet d'utiliser même les techniques les plus anciennes. La vérification des systèmes d'exploitation obsolètes compare la version du système d'exploitation de l'utilisateur à la dernière version disponible. Il est conseillé à l'utilisateur de mettre à jour son système d'exploitation si une version plus récente est disponible.

| **Sécurité des appareils** | **Windows** | **Mac** | **Android** | **iOS** |
|---|---|---|---|---|
| Le conseiller en confidentialité i*nsiste sur l'utilisation des autorisations essentielles.* | - | - | Oui | - |
| Vérification du verrouillage de l'appareil<br><br>*Guide l'utilisateur pour activer le verrouillage de l'écran.* | - | - | Oui | Oui |
| Vérifiez si votre système d'exploitation est obsolète : *il est conseillé aux utilisateurs de mettre à jour leur système d'exploitation.* | - | - | - | Oui |

# Fonctionnalités du firewall

### Aperçu

Le pare-feu est un composant de sécurité essentiel qui filtre le trafic réseau indésirable (entrant et sortant) et empêche les tentatives d'intrusion sur vos appareils. F-Secure s'efforce d'offrir la

meilleure protection pare-feu et une interopérabilité optimale aux utilisateurs, quel que soit leur système d'exploitation.

Pour les fonctionnalités de base telles que la gestion du trafic TCP/IP et des ports ouverts, F-Secure Total PC et Mac utilise par défaut le pare-feu intégré au système d'exploitation. Ceci garantit une interopérabilité optimale, car la quasi-totalité des applications (jeux, utilitaires, applications réseau, multimédias, etc.) sont testées par rapport au pare-feu du système d'exploitation.

**Gestion au niveau applicatif**

En plus de la couche pare-feu TCP/IP, F-Secure Total Windows ajoute une fonctionnalité de pare-feu applicatif. Concrètement, cela signifie que F-Secure surveille le comportement des applications en temps réel et peut bloquer celles qui agissent de manière malveillante (qu'il s'agisse d'une application défaillante existante ou d'une toute nouvelle installation). La solution F-Secure inclut également des fonctionnalités permettant d'analyser le trafic web en temps réel afin de détecter le téléchargement de contenus malveillants ou potentiellement indésirables. Cette combinaison d'un pare-feu au niveau du système d'exploitation et de la sécurité applicative avancée de F-Secure offre à l'utilisateur une protection optimale.