F-Secure Total - Internet Security module

Device Protection

Elke laag van uw beveiliging begint hier. Apparaatbescherming is de kern van F-Secure Total Protection — de essentiële basis die uw apparaat, gegevens en online activiteiten beschermt. Zonder deze bescherming staat niets op een solide fundament.

Apparaatbescherming beschermt waar bedreigingen vaak als eerste toeslaan: websites die persoonlijke informatie proberen te stelen, malware die zich op uw apparaat richt, privacyrisico's die voor het oog verborgen zijn en fundamentele kwetsbaarheden die uw apparaat onbeschermd achterlaten. Bescherming tegen browsen en phishing, virusbescherming, privacyadvies, controle op apparaatvergrendeling en controle op verouderde besturingssystemen werken samen als de eerste verdedigingslinie — zodat de rest van de bescherming een sterke basis heeft om op voort te bouwen.

Virus Protection

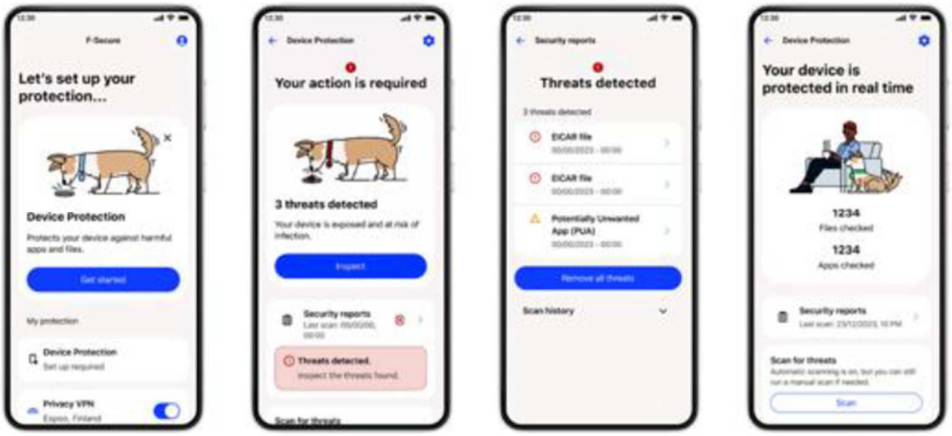
Overzicht

Virusbescherming is een van de kernbeveiligingselementen van F-Secure Total. F-Secure Total biedt bescherming tegen malware op alle open besturingssystemen, zoals Windows, macOS en Android, die extra kwetsbaar zijn voor deze dreiging. Vanwege beperkingen van Apple is het niet beschikbaar voor iOS.

Virusbescherming beschermt uw klanten tegen malware zoals virussen, trojans, spyware, ransomware en infostealers. Deze malware kan persoonlijke informatie verzamelen en verspreiden, online activiteiten bespioneren of zelfs al hun persoonlijke gegevens vergrendelen en losgeld eisen om ze te ontgrendelen. Malware-infecties (infostealers) behoren tot de meest voorkomende beveiligingsincidenten die leiden tot identiteitsdiefstal en diverse vormen van oplichting. F-Secure Total beschermt uw klanten door dergelijke incidenten te voorkomen.

Om malware-infecties te voorkomen, worden alle bestanden en applicaties automatisch gescand. Naast de duidelijk schadelijke bestanden of applicaties scant Total ook op potentieel ongewenste applicaties die zich op een ongewenste manier op het apparaat kunnen gedragen, zoals agressieve marketingtools. Bestanden worden in realtime, op aanvraag (handmatig scannen) of geactiveerd door bepaalde gebeurtenissen, zoals de installatie van een applicatie, gescand. Zodra malware of een potentieel ongewenste applicatie (PUA) wordt gedetecteerd, wordt de gebruiker direct gevraagd deze te verwijderen. De scanlogica is afhankelijk van het onderliggende besturingssysteem.

Let op! Virusbescherming bevindt zich nu onder de functie 'Apparaatbescherming'. Zie de Total Android-afbeeldingen hieronder.



Beveiliging Cloud en AI

Naast de traditionele scans op het apparaat zelf, maakt F-Secure gebruik van geavanceerde AI-gebaseerde cloudscantechnologieën. Bestandsreputaties worden vanuit de cloud gecontroleerd, net zoals de traditionele, op vingerafdrukken gebaseerde scanengine dat doet vanuit de lokale database. Omdat de reputaties in de cloud worden beheerd, zijn wijzigingen in de bestandsreputaties dynamisch en direct. Eventuele wijzigingen in de bestandsreputaties worden onmiddellijk doorgevoerd naar alle gebruikers, zodat elke gebruiker altijd over de meest recente database beschikt. Cloudgebaseerde detectietechnologieën zijn beschikbaar op alle ondersteunde platforms.

Intelligente, cloudgebaseerde logica bepaalt welke applicaties gescand moeten worden, zodat de apparaatbronnen optimaal beschikbaar zijn voor de gebruiker. Onbekende applicatiebestanden worden geüpload en geanalyseerd in de cloud met behulp van diverse technologieën, waaronder AI en machine learning. Scanresultaten worden automatisch doorgegeven aan andere systemen, waardoor het geïnfecteerde bestand direct bekend is en het niet nodig is om hetzelfde voorbeeld van andere gebruikers te verkrijgen. Scanengines en databases worden in de cloud beheerd, waardoor alle wijzigingen direct van kracht worden voor alle gebruikers.

Behaviour Detection

Gedragsdetectie observeert het gedrag van een applicatie en voorkomt dat potentieel schadelijke acties succesvol worden voltooid. Gedragsgebaseerde detecties overbruggen de cruciale kloof tussen het eerste verschijnen van nieuwe malware en het moment waarop een detectie voor de dreiging wordt uitgegeven. Door de focus te verleggen van structurele naar functionele kenmerken van een sample, kan gedragsdetectie programma's identificeren en blokkeren die schadelijke acties uitvoeren, zelfs voordat een daadwerkelijk sample is verkregen en onderzocht.

Gedragsdetectie is ook beschikbaar voor Mac. Voor de meeste Mac-gebruikers is de functionaliteit praktisch onzichtbaar als ze alleen bekende en vertrouwde software gebruiken.

Telkens wanneer een applicatie een document probeert te wijzigen, controleert gedragsdetectie automatisch of de applicatie afkomstig is van een vertrouwde uitgever. Als een onbekende applicatie een bestand probeert te wijzigen, wordt de gebruiker om bevestiging gevraagd voordat de applicatie verder mag gaan.

Ransomwarebescherming

F-Secure Total PC biedt robuuste bescherming tegen ransomware als onderdeel van de kernfunctie Virusbescherming. De geïntegreerde ransomwarebescherming wordt nu volledig beheerd door de backend-beveiligingssystemen voor een verbeterde effectiviteit. Deze bescherming maakt gebruik van geavanceerde detectietechnologie om ransomware-achtig gedrag te identificeren en te blokkeren voordat het uw bestanden kan versleutelen. Wanneer verdachte activiteit wordt gedetecteerd, blokkeert Total automatisch het schadelijke proces en waarschuwt de gebruiker.

Gamingmodus

F-Secure Total ondersteunt de gamingmodus, die de game-ervaring op de pc verbetert. De gamingmodus past veel beveiligings- en Windows-instellingen en -functionaliteiten aan voor geoptimaliseerd en ononderbroken gamen. In de gamingmodus worden Total-updates gepauzeerd om bandbreedte en CPU-belasting te besparen, worden prompts, meldingen en pushberichten (Windows Toasts) niet weergegeven en worden automatische of geplande antivirusscans niet gestart. F-Secure Total PC is geoptimaliseerd voor de beste gameprestaties. Het verbetert de prestaties van uw computer in vergelijking met veel andere beveiligingsproducten zoals Microsoft Defender.

F-Secure Total Mac heeft een 'lichte' gamingmodus. Gebruikers kunnen antivirusscans voor een bepaalde periode onderbreken om resources te besparen tijdens het gamen of andere resource-intensieve bewerkingen.

Virus Bescherming	**Windows**	**Mac**	**Android**	**iOS**
Virus Bescherming	Ja	Ja	Ja	-*
Handmatig scannen *De gebruiker kan een scan op aanvraag uitvoeren*	Ja	Ja	Ja	-
Gepland scannen *Automatisch scannen met een ingesteld tijdsinterval*	Ja	-	Ja	-
Real-time scanning *Scant bestanden continu op de achtergrond.*	Ja	Ja	-	-
Scant apps tijdens installatie *Scant apps zodra ze op het apparaat worden geïnstalleerd*	Ja Real-time scanning	Ja Real-time scanning	Ja	-
In-cloud scanning *Controleert de reputatie van bestanden vanuit de cloud.*	Ja	Ja	Ja	-
Bescherming op basis van gedrag *Waarschuwt voor risicovol app-gedrag*	Ja In-app + Cloud	Ja In-app + Cloud	Ja Cloud	-
Bescherming tegen ransomware *Bewaakt/blokkeert ransomware-achtig gedrag*	Ja	Ja	-	-
Antibot-bescherming *Opsporing en verwijdering van botnets*	Ja	-	-	-
Spelmodus/scan onderbreken *Suspendeer onderbrekingen tijdens het gamen.*	Ja	Ja Gebruiker getimed	-	-
Voorbeeldinzending	Ja	Ja	Ja	-

*Let op! Het is niet mogelijk om virusbescherming aan te bieden voor het iOS-platform vanwege de beoordelingsrichtlijnen van Apple. Volgens Apple is er geen malware op iOS, dus elke functie die beweert gebruikers tegen malware te beschermen, doet valse beloftes en is niet toegestaan in de App Store.

Bescherming tegen browsen en phishing

Overzicht

Een steeds groter deel van onze dagelijkse activiteiten vindt online plaats – bankieren, winkelen, informatie zoeken, boekingen, afspraken, hobby's, communicatie, entertainment, enzovoort. Browsing Protection is ontworpen om uw klanten veilig te houden op internet. Het beschermt hun veiligheid en privacy en helpt hen oplichting te voorkomen door hen weg te houden van webpagina's die gericht zijn op het verzamelen van persoonlijke informatie of het verspreiden van schadelijke inhoud zoals malware en exploits.

Door webpaginaverzoeken te onderscheppen en de reputatie van webpagina's te controleren via de webreputatieservice van F-Secure, zorgt Browsing Protection ervoor dat uw klanten veilig op internet kunnen surfen.

Reputatieservices van F-Secure

Browsing Protection is een reputatieservice die internetpagina's als veilig of onveilig beschouwt. Onveilige sites zijn doorgaans phishing- of malwaresites. De reputatie van pagina's wordt stilzwijgend op de achtergrond gecontroleerd tijdens het browsen. De reputatiecontroles zijn geoptimaliseerd voor een optimale browse-ervaring. Toegang tot veilige sites verloopt normaal en zonder onderbrekingen. Toegang tot onveilige sites wordt eenvoudigweg geblokkeerd met een dialoogvenster. Browserbeveiliging beschermt uw klanten ook tegen e-mail- of sms-fraude die bijvoorbeeld verwijst naar nepbankwebsites, zolang ze browsers gebruiken die beveiligd zijn met browserbeveiliging.

Bankbeveiliging

Bankbeveiliging voegt een extra beveiligingslaag toe aan de browsebeveiliging en virusbeveiliging. Waar de browsebeveiliging de toegang tot onveilige websites, zoals bekende nepbank- of phishingwebsites, blokkeert, verbetert de bankbeveiliging de zichtbaarheid en veiligheid bij het bezoeken van een veilige bankwebsite. De browsebeveiliging biedt de beveiliging stil op de achtergrond, zonder de normale browse-ervaring te verstoren. De bankbeveiliging is ontworpen om de beveiliging zichtbaarder en tastbaarder te maken.

Bankbeveiliging is een van de meest gewaardeerde functies onder consumenten vanwege het gevoel van veiligheid dat het biedt bij online winkelen en bankieren. De functie beantwoordt ook aan de grootste zorg van consumenten met betrekking tot internet: geldverlies tijdens online winkelen en bankieren. Vanwege de hoge waarde voor de consument wordt dit onderdeel continu verder ontwikkeld, bijvoorbeeld door de gebruiksvriendelijkheid en het gevoel van veiligheid te verbeteren.

Bankbeveiliging toont de gebruiker een indicator (banner, frame of toast) in de browsercontext wanneer een veilige bankwebsite wordt bezocht en de verbinding met de site beveiligd is (https). De browsebeveiliging blokkeert automatisch de toegang tot phishing- of nepbankwebsites.

F-Secure Total voor Windows Banking Protection voorkomt ook dat er andere verbindingen tot stand komen terwijl u zich op een veilige bankwebsite bevindt. Alleen vertrouwde applicaties mogen nieuwe verbindingen openen. In de praktijk gebeurt dit doordat, wanneer een Banking

Protection-sessie wordt gestart, alle internetverbindingen van onbetrouwbare processen worden verbroken. Ook worden alle verbindingen van de vertrouwde processen gecontroleerd. Als vertrouwde processen verbinding maken met onbetrouwbare of onbekende IP-adressen, worden de verbindingen automatisch geblokkeerd. Banking Protection staat nieuwe vertrouwde processen toe om met internet te communiceren.

De mogelijkheid om onbetrouwbare verbindingen te blokkeren voorkomt het kapen van banksessies – het geld van de gebruiker is veilig. Total voor Windows sluit Banking Protection automatisch af nadat de gebruiker de banksessie heeft voltooid. Banking Protection wordt opnieuw gestart wanneer een andere bankwebsite wordt bezocht.

Bescherming tegen Remote Access Tools (RAT) voorkomt het gebruik van RAT-tools tijdens een banksessie (wanneer Banking Protection is gestart). Dit voorkomt dat oplichters software voor toegang op afstand gebruiken om bijvoorbeeld diefstallen te plegen op de online bankrekening van de gebruiker.

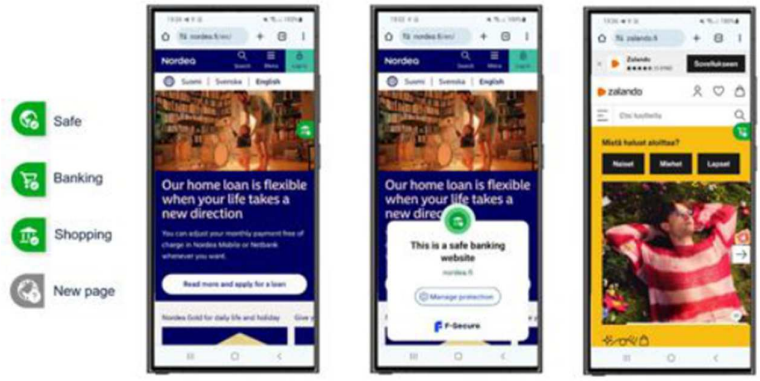
Safari- en Chrome-bescherming

Safari Protection voegt browsebeschermingsfuncties toe aan de native Safari-browser van iPhones en iPads. Chrome Protection voegt op vergelijkbare wijze browsebescherming toe aan de native browser van Android-telefoons en -tablets. De ondersteunde functies omvatten browsebescherming, bankbescherming en winkelbescherming (onderdeel van de module voor fraudebescherming).

Zowel Safari als Chrome Protection vereisen enige configuratie door de gebruiker. De installatie wordt ondersteund via een SmartTask in de app. De gebruiker wordt door het installatieproces geleid. Eenmaal ingeschakeld, is internetten met de native browser beschermd tegen gevaarlijke websites zoals bekende malware- en phishingwebsites.

Er zijn verschillende indicatoren, afhankelijk van het type pagina dat de gebruiker bezoekt. Veilige pagina's worden groen gemarkeerd. Veilige winkel- en bankwebsites worden apart gemarkeerd.

Safari Protection (zie onderstaande afbeeldingen) toont al in de zoekresultaten een indicator van de reputatie van de pagina, waardoor het gemakkelijk is om onveilige pagina's te vermijden. Door op de indicator te klikken, kan de gebruiker meer details bekijken. Toegang tot onveilige pagina's wordt geblokkeerd als de gebruiker per ongeluk op een verkeerde link klikt.



Zowel Safari als Chrome Protection (zie afbeeldingen hierboven) tonen een indicator van de reputatie van de pagina als een overlay tijdens het browsen. De gebruiker kan de indicator op het scherm verplaatsen, zodat deze de browse-ervaring niet verstoort. De indicator toont direct het type webpagina: veilig, bankieren, winkelen of nieuw/niet geanalyseerd. Door op de indicator te klikken, kan de gebruiker meer details bekijken. Toegang tot onveilige pagina's wordt geblokkeerd.

Let op! Winkelbeveiliging maakt deel uit van de functionaliteit 'Oplichtingsbeveiliging'. Zie het gedeelte 'Oplichtingsbeveiliging' in dit document voor meer informatie.

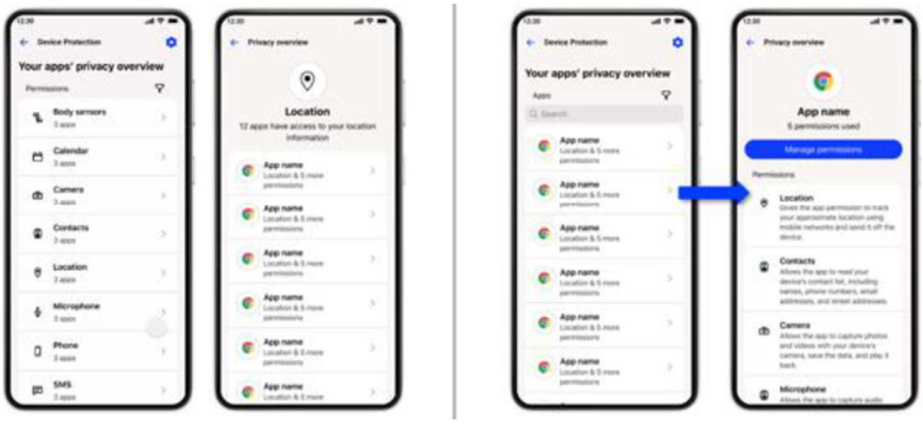
Bescherming tegen ongewenst browsen en phishing	**Windows**	**Mac**	**Android**	**iOS**
Browsingbeveiliging *Controleert de reputatie van websites*	Ja	Ja	Ja	Ja
Ondersteunde browsers *Browsers waarop de functie werkt*	Edge, Chrome, and Firefox	Safari, Edge, Chrome, and Firefox	Chrome,	Safari
Blokkeert de toegang tot schadelijke websites *Blokkeert phishing- en malwarewebsites*	Ja	Ja	Ja	Ja
Indicator voor veilige bankomgeving *Geeft aan wanneer u zich op een veilige bankomgeving bevindt en de verbinding beveiligd is (https wordt gebruikt)*	Ja	Ja	Ja	Ja
Bankbeveiliging automatisch ingeschakeld *Wordt automatisch ingeschakeld bij het*	Ja	Ja	Ja Enkel toegang	Ja Enkel toegang

bezoeken van een bankwebsite				
Blokkeert onbekende processen *Blokkeert verbindingen van onbetrouwbare processen wanneer bankbeveiliging is ingeschakeld*	Ja	-	-	-
Blokkeert onbekende verbindingen *Blokkeert onbekende verbindingen van vertrouwde processen wanneer bankbeveiliging is ingeschakeld*	Ja	-	-	-
Blokkeert tools voor toegang op afstand *Blokkeert tools voor toegang op afstand wanneer bankbeveiliging is ingeschakeld*	Ja	-	-	-

Let op! Safe Browser (mobiel) wordt eind 2025 uitgefaseerd, omdat de bescherming is ingeschakeld in de standaard mobiele browsers Safari en Chrome.

Privacy Advisor

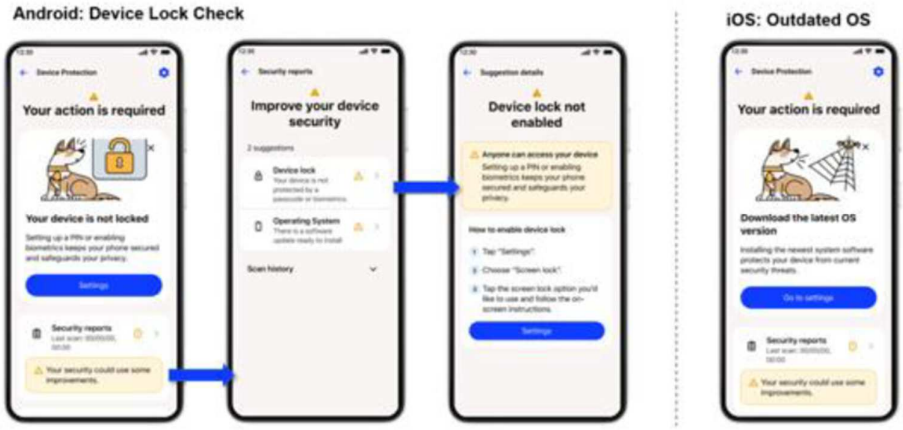
Zelfs veilige en betrouwbare apps kunnen zeer uitgebreide machtigingen op het apparaat van de gebruiker aanvragen. Privacy Advisor is een nieuwe functie van F-Secure Total voor Android waarmee uw klanten de machtigingen van apps op hun apparaten kunnen beheren. Het markeert het gebruik van kritieke machtigingen zoals locatie, contacten, foto's, enz., die de veiligheid en privacy van de gebruiker in gevaar kunnen brengen. De mogelijkheid om apps te filteren op basis van machtigingen helpt de gebruiker te bepalen of de app belangrijk genoeg is om toegang tot die bronnen te verlenen.



Apparaatvergrendeling controleren

De schermvergrendeling van een apparaat is waarschijnlijk de belangrijkste beveiligingsfunctie van een telefoon. Schermvergrendeling voorkomt ongeautoriseerde toegang tot het apparaat, de gegevens van de gebruiker en alle apps en services op het apparaat. Dit is vooral belangrijk bij mobiele apparaten, omdat deze gemakkelijk verloren of gestolen kunnen worden.

De functie Apparaatvergrendeling controleren of de gebruiker de schermvergrendeling heeft ingeschakeld. Als de gebruiker de schermvergrendeling niet heeft ingeschakeld, zal de functie dit als een beveiligingsrisico markeren en de gebruiker begeleiden bij het instellen ervan via de apparaatinstellingen. Na de instelling hoeft de gebruiker zich hier geen zorgen meer over te maken.



Controle op verouderd besturingssysteem

Mobiele apparaten geven vaak een vals gevoel van veiligheid. Veel activiteiten lijken minder ernstig wanneer ze met een telefoon of tablet worden uitgevoerd - en de bedreigingen lijken onwaarschijnlijker en minder ernstig. Een van de symptomen hiervan is het nalaten om apps en het onderliggende besturingssysteem bij te werken.

Ongeacht het platform worden er regelmatig updates voor het besturingssysteem uitgebracht om nieuwe functies te introduceren, de gebruiksvriendelijkheid te verbeteren en bugs en beveiligingslekken te verhelpen. Vanuit een beveiligingsperspectief vormt een verouderd besturingssysteem een groot risico voor de veiligheid en privacy van de gebruiker.

Cybercriminelen zoeken voortdurend naar nieuwe manieren om toegang te krijgen tot cruciale persoonlijke informatie, zoals bankgegevens. Een niet-gepatcht besturingssysteem stelt hen in staat om zelfs oude trucs te gebruiken.

De controle op verouderde besturingssystemen controleert de versie van het besturingssysteem van de gebruiker aan de hand van de nieuwste beschikbare versie. De gebruiker wordt geadviseerd het besturingssysteem bij te werken als er een nieuwere versie beschikbaar is.

Apparaatbeveiliging	**Windows**	**Mac**	**Android**	**iOS**
Privacyadviseur *Benadrukt het gebruik van essentiële machtigingen*	-	-	Ja	-
Device Lock Check *Begeleidt de gebruiker bij het inschakelen van de schermvergrendeling.*	-	-	Ja	Ja
Controle op verouderde besturingssystemen: *gebruikers worden geadviseerd het besturingssysteem bij te werken.*	-	-	-	Ja

Firewallfunctionaliteit

Overzicht

De firewall is een van de belangrijkste beveiligingscomponenten die ongewenst netwerkverkeer (inkomend en uitgaand) filtert en inbraakpogingen op uw apparaten voorkomt. F-Secure streeft ernaar de best mogelijke firewallbescherming en interoperabiliteit te bieden aan consumenten in alle besturingssystemen.

Voor basisfunctionaliteiten zoals het beheren van TCP/IP-verkeer en open poorten, maken F-Secure Total PC en Mac gebruik van de firewall die standaard in het besturingssysteem is ingebouwd. Dit garandeert de beste interoperabiliteit voor de consument, aangezien vrijwel elke applicatie (game, hulpprogramma, netwerk, media, enz.) wordt getest tegen de firewall van het besturingssysteem.

Beheer op applicatieniveau

Bovenop de TCP/IP-firewalllaag voegt F-Secure Total Windows firewallfunctionaliteit op applicatieniveau toe. In de praktijk betekent dit dat F-Secure het gedrag van applicaties in realtime monitort en apps kan blokkeren die zich schadelijk gedragen (of het nu gaat om een bestaande app die zich misdraagt of een volledig nieuwe installatie). De oplossing van F-Secure bevat ook mogelijkheden voor het scannen van webverkeer in realtime om te detecteren of

schadelijke of potentieel ongewenste inhoud wordt gedownload. Deze combinatie van een firewall op besturingssysteemniveau en de geavanceerde applicatiebeveiliging van F-Secure biedt de consument de beste bescherming.