F-Secure Total - Internet Security module

Device Protection

Every layer of your security starts here. Device Protection is the core of F-Secure Total protection — the essential foundation that keeps the device safe, data secure, and online activities protected. Without it, nothing else stands on solid ground.

Device Protection guards where threats often strike first: the websites that try to steal personal information, the malware that targets the device, the privacy risks hiding in plain sight, and the basic vulnerabilities that leave exposed. Browsing and Phishing Protection, Virus Protection, Privacy Advisor, Device Lock Check, and Outdated OS Check work together as the first front of defense — so the rest of the protection has something strong to build on.

Virus Protection

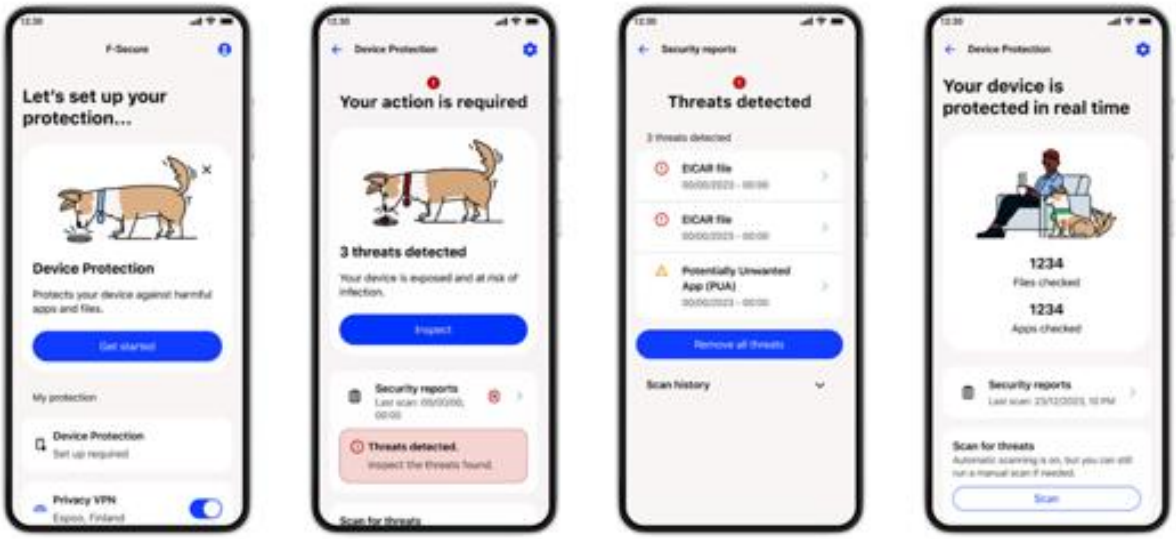
Overview

Virus Protection is one of the core security elements of F-Secure Total. F-Secure Total provides protection against malware on all open operating systems, Windows, macOS and Android, which are more vulnerable to the threat. It is not available for iOS due to Apple’s restrictions.

Virus Protection safeguards your customers against malware like viruses, trojans, spyware, ransomware, and infostealers which may collect and distribute personal information, spy on their online activities, or even lock all their personal data and demand a ransom to unlock it. Malware infections (infostealers) are one of the most common security incidents leading to identity theft and various forms of scams. F-Secure Total protects your customers by preventing security incidents from happening.

To prevent malware infections all files and applications are automatically scanned. In addition to the clearly bad files or applications, Total scans for potentially unwanted applications which may behave in an undesirable way on the device like aggressive marketing tools. Files are scanned in real-time, on-demand (manual scanning) or triggered upon certain events like installation of an application. Once a malware or a potentially unwanted application (PUA) is discovered, user will be immediately instructed to remove it. The scanning logic depends on the underlying operating system.

Note! Virus Protection is now under **Device Protection** feature card. See Total Android images below.



Security cloud and AI

In addition to the traditional on-device scanning, F-Secure uses advanced AI-based cloud scanning technologies. File reputations are checked from the cloud just like the traditional fingerprint-based scanning engine checks from the local database. As the reputations are maintained in the cloud, the changes in the file reputations are dynamic and immediate. Any changes in the file reputations are immediately deployed to entire user base making sure every user has always the latest database in use. Cloud based detection technologies are available on all supported platforms.

Intelligent cloud-based logic decides which applications need to be scanned making sure the device resources are optimally available for the user. Unknown application binaries are uploaded and analysed in the cloud with multiple technologies including AI & Machine Learning. Scanning results are automatically passed on to other systems making the infected file immediately known and removing the need to get the same sample from other users. Scanning engines and databases are maintained in the cloud making all changes immediately effective to all users.

Behaviour Detection

Behaviour Detection observes an application's behaviour and prevents any potentially harmful action from successfully completing. Behaviour-based detections cover that crucial gap between the first appearance of new malware and a detection being issued for the threat. By moving the focus from structural to functional characteristics of a sample, Behaviour Detection can identify and block programs performing harmful actions, even before an actual sample has been acquired and examined.

Behaviour Detection is also available for Mac. For most Mac users, the functionality is practically invisible if they use only well-known and trusted software. Every time an application tries to modify a document, Behaviour Detection will automatically check whether the application comes from a trusted publisher. If an application unknown, attempts to modify a file will result into a user confirmation before allowing the application to proceed.

Ransomware protection

F-Secure Total PC provides robust protection against ransomware as part of its core Virus Protection feature. The integrated ransomware protection is now fully managed by the backend security systems for improved effectiveness. This protection uses advanced detection technology to identify and block ransomware-like behaviour before it can encrypt your files. When suspicious activity is detected, Total automatically blocks the malicious process and alerts the user.

Gaming Mode

F-Secure Total supports Gaming mode which improves the PC gaming experience. Gaming Mode adjusts many security and Windows operating system settings and functionalities for optimized and uninterrupted gaming. In Gaming Mode Total updates are paused to save bandwidth and CPU load, prompts, notifications, and PUSH messages (Windows Toasts) are not shown, and automatic or scheduled antivirus scans are not started. F-Secure Total PC has been optimized for the best gaming performance. It improves your computer's performance compared to many other security products like Microsoft Defender.

F-Secure Total Mac has "light" gaming mode. User can suspend antivirus scanning for a selected period of time to save resources during gaming or other resource consuming operations.

Virus Protection	Windows	Mac	Android	iOS
Virus Protection	Yes	Yes	Yes	-*
Manual scanning *User can execute on-demand scan*	Yes	Yes	Yes	-
Scheduled scanning *Automatic scanning with timed interval*	Yes	-	Yes	-
Real-time scanning *Scans files constantly in the background*	Yes	Yes	-	-
On install scanning *Scans apps as they are installed to device*	Yes Real-time scanning	Yes Real-time scanning	Yes	-
In-cloud scanning *Checks file reputations from the cloud*	Yes	Yes	Yes	-
Behaviour based protection *Warns about risky app behaviour*	Yes In-app + Cloud	Yes In-app + Cloud	Yes Cloud	-
Ransomware protection *Monitors/blocks ransomware like behaviour*	Yes	Yes	-	-
Antibot protection *Botnet detection and removal*	Yes	-	-	-
Gaming mode/ suspend scanning *Suspend interruptions during gaming*	Yes	Yes User timed	-	-
Sample submission	Yes	Yes	Yes	-

*Note! It is not possible to offer Virus Protection for iOS platform due to Apple's review guidelines. According to Apple, there are no malware on iOS thus any feature claiming to protect user against malware makes false promises to user and are not allowed on the AppStore.

Browsing and Phishing Protection

Overview

Increasing portion of everyday activities happen online – banking, shopping, information searching, bookings, appointments, hobbies, communication, entertainment etc. Browsing Protection has been designed to keep your customers on the safe side of the Internet. It protects their security, privacy and helps them avoid scams by keeping them away from web pages which target at collecting personal information or spreading malicious content like malware and exploits.

By intercepting the web page requests and by checking their reputation from F-Secure's web reputation service, Browsing Protection makes sure that your customers can explore the Internet safely.

F-Secure's reputation services

Browsing Protection is a reputation service, which treats the internet pages as either safe or unsafe. Unsafe sites are typically phishing or malware sites. The page reputations are checked silently in the background while browsing the Internet. The reputation queries are optimized for the best browsing experience. Access to safe sites happens normally without any interruptions. Access to unsafe sites is simply blocked with a dialog. Browsing protection also protects your customers from email or SMS scams pointing to, for example, fake banking sites as long as they use browsers secured by Browsing Protection.

Banking protection

Banking Protection adds another layer of security to Browsing protection and Virus protection. Where Browsing protection prevents access to unsafe web sites like known fake banking or phishing sites, Banking protection improves the visibility and security when entering a safe banking site. Browsing protection provides the security silently in the background causing no interference with the normal browsing experience. Banking protection has been designed to make the security more visible and tangible.

Banking Protection is the most liked features among the consumers due to the sense of security it provides when handling online shopping and banking. The feature also responds to the biggest consumer concern related the Internet – loss of money while shopping and banking online. Due to high consumer value the feature area is continuously developed e.g. by improving the usability and the sense of security.

Banking Protection shows user an indicator (banner, frame or toast) in the browser context when entering a safe banking site and the connection to the site is secured (https). Browsing Protection part automatically prevents access to phishing or fake banking sites.

F-Secure Total for Windows Banking Protection also prevents other connections from happening while on a safe banking site. Only trusted applications are allowed to open new connections. In

practice this happens so that when Banking Protection session is started all internet connections of untrusted processes are cut off. Also, all connections of the trusted processes are checked. If trusted processes connect to untrusted or unknown IP-addresses, the connections are automatically blocked. Banking Protection allows new trusted processes to communicate to the internet.

The ability to block untrusted connections prevents hijacking of banking sessions – the user's money is safe. Total for Windows closes Banking Protection automatically after user have completed the banking session. Banking Protection will start again when entering another banking site.

Remote Access Tool (RAT) Protection prevents using RAT tools while in banking session (Banking Protection started). This prevents scammers from leveraging remote access software to perform thefts e.g. on user's online bank account.

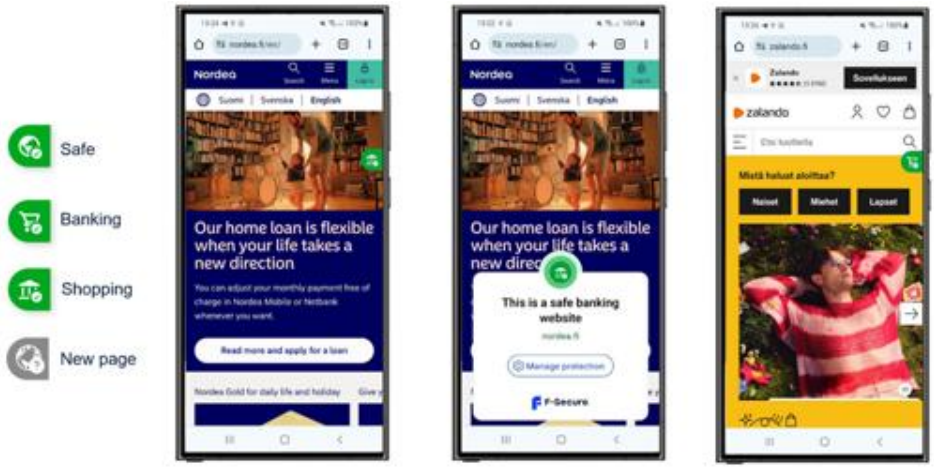
Safari and Chrome Protection

Safari Protection brings Browsing Protection features in the iPhones or iPad's native Safari Browser. Similarly, Chrome Protection adds Browsing Protection to Android phones or tablet's native browser. The supported features include Browsing Protection, Banking Protection and Shopping Protection (Part of Scam Protection module).

Both Safari and Chrome Protection require some configuration from the user. Setup is promoted using a SmartTask inside the app. User is guided through the setup. Once enabled browsing the internet with the native browser is protected against dangerous web sites like known malware and phishing sites.

There are different kind of indicators depending on a type of page user is vising. Safe pages are marked with green. Also, safe shopping and banking sites are highlighted separately.

Safari Protection (images below) shows an indicator of the page reputation already in the search results making it easy to avoid unsafe pages. By clicking the indicator, the user can see further details. Access to unsafe pages is blocked – if user accidentally clicks a wrong link.



Both Safari and Chrome Protection (images above) show an indicator of the page reputation as an overlay when browsing. User can move the indicator on the screen so that it is not disturbing the browsing experience. The indicator immediately shows the web page type whether safe, banking, shopping or new/not analysed. By clicking the indicator, the user can see further details. Access to unsafe pages is blocked.

Note! Shopping Protection is part of the Scam Protection feature set. See Scam Protection section of this document for further details.

Browsing and Phishing Protection	**Windows**	**Mac**	**Android**	**iOS**
Browsing Protection *Checks web site reputations*	Yes	Yes	Yes	Yes
Supported browsers *Browsers on which the feature works*	Edge, Chrome, and Firefox	Safari, Edge, Chrome, and Firefox	Chrome,	Safari
Blocks access to bad sites *Blocks phishing and malware sites*	Yes	Yes	Yes	Yes
Safe banking site indicator *Shows when on safe banking site and connection is secure (https is in use)*	Yes	Yes	Yes	Yes
Banking Protection auto-on *Automatically enabled when entering a banking site*	Yes	Yes	Yes Entering only	Yes Entering only
Blocks unknown processes *Blocks connections of untrusted processes when banking protection enabled*	Yes	-	-	-
Blocks unknown connections *Blocks unknown connections of trusted processes when banking prot. enabled*	Yes	-	-	-
Blocks Remote Access Tools *Blocks Remote Access Tools when banking protection is enabled*	Yes	-	-	-

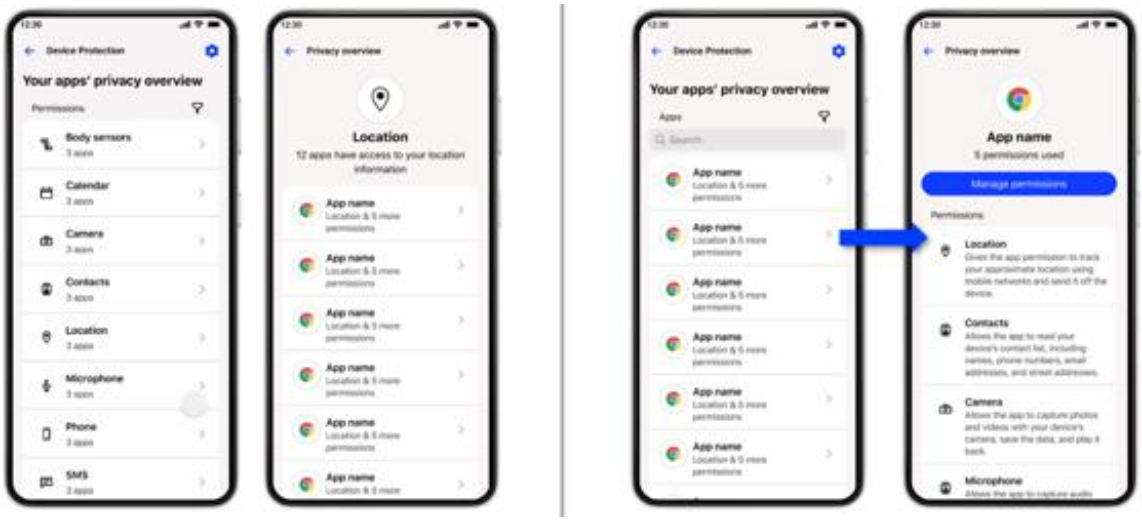
Search result rating *Shows page reputation rating with an indicator in search results*	Yes Google, Yahoo and Bing	Yes Google, Yahoo and Bing	-	Yes Safari
Support for https traffic *Checks URL reputations even in https traffic (happens in browser)*	Yes	Yes	Yes	Yes

Note! Safe Browser (mobile) has been deprecated end of 2025 as the protection has been enabled in mobile default browsers Safari and Chrome.

Privacy Advisor

Even safe and trustworthy applications may request very extensive permissions on the user's device. Privacy Advisor is a new F-Secure Total for Android feature that helps your customers to manage the permissions applications have on their devices. It highlights the use of critical permissions like location, contacts, photos etc. that may jeopardise user's security and privacy.

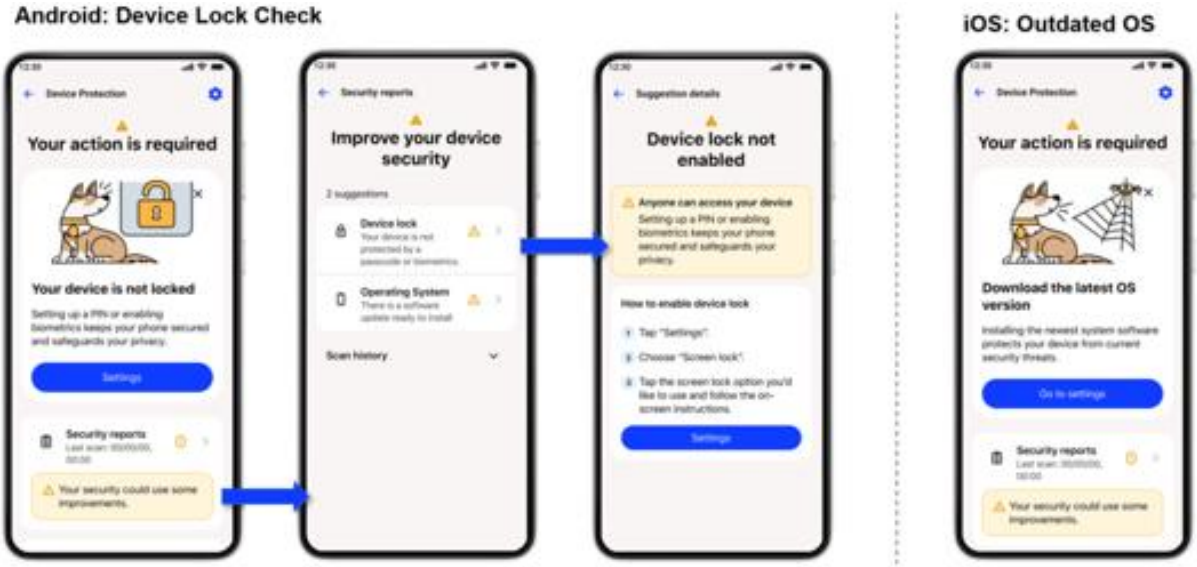
The ability to filter apps based on permissions helps the user to decide if the application is important enough to grant access to those resources.



Device Lock Check

Device's own screen lock is probably the most important security feature of a phone. Screen lock prevents unauthorized access to the device, user's data and all the apps and services on the device. This is particularly critical in case of mobile devices as they can be easily lost or stolen.

Device Lock Check simply verifies whether the user has enabled the screen lock. In case the user has not enabled the screen lock, the feature will highlight it as a security risk and guide user to setting it up through the device settings. Once setup, the user will not be bothered with the topic.



Outdated Operating System Check

Mobile devices often create a false feeling of security around them. Somehow many activities seem less serious when handled with a phone or a tablet - and the threats seem more unlikely and less severe. One of the symptoms of this is the laziness of updating apps and the underlying operating system.

Regardless of the platform, operating system updates are frequently published to introduce new features, to enhance usability and to fix bugs and security vulnerabilities. From security perspective outdated operating system is a major risk to the user's security and privacy. Cyber criminals are continuously seeking new ways to gain access to critical personal information like banking credentials. Unpatched operating system enables them to leverage even old tricks.

Outdated OS Check verifies the user's operating system version against the latest available version. User is guided to update the operating system in case a newer version is available.

Device Protection	Windows	Mac	Android	iOS
Privacy Advisor *Highlights the use of critical permissions*	-	-	Yes	-
Device Lock Check *Guides user to enable screen lock*	-	-	Yes	Yes
Outdated OS Check *Guides user to update OS*	-	-	-	Yes

Firewall functionality

Overview

Firewall is one of the core security components filtering out the unwanted network traffic (inbound and outbound) and preventing intrusion attempts targeting your devices. F-Secure aims to offer best possible firewall protection and interoperability for the consumers in all operating system environments.

For basic firewall capabilities like managing TCP/IP traffic and open ports, F-Secure Total PC and Mac leverage the firewall that comes with the operating system. This ensures the best interoperability for the consumer as virtually every application (game, utility, networking, media…) is tested against the operating system firewall.

Application-level controls

On top of the TCP/IP firewall layer, F-Secure Total Windows adds application-level firewall capabilities. In practice this means that F-Secure monitors in real-time application behaviour and can block apps that show malicious behaviour (whether existing app turning bad, or a completely new install). F-Secure's solution also contains real-time web traffic scanning capabilities to identify if malicious or potentially unwanted content is being downloaded. This combination of operating system level firewall and F-Secure's advanced application-level protection together provide the best level of protection for the consumer.