F-SECURE PROTECTION SERVICE FOR BUSINESS

Solution Overview

F-Secure

CONTENTS

Executive summary 3
1. Solution overview 4
1.1 Solution packages 4
1.2 Solution components 6
1.3 Solution deployment 6
2. Management portal 7
3. Computer protection 9
3.1 Combining all required endpoint protection stack into one 9
3.2 Heuristic and behavioral threat analysis 9
3.3 Real-time threat intelligence 10
3.4 Industry-leading Mac security 11
3.5 Protection for Linux endpoints 11
3.6 Integrated patch management 11
3.7 Multi-engine anti-malware 11
3.8 Extensive and proactive web protection 12
4. Mobile protection 13
4.1 Mobile VPN 13
4.2 Security Cloud 13
4.3 Application protection 14
4.4 Browsing protection 14
4.5 Faster browsing and less data use 14
4.6 Third-party MDM deployment 14
5. Server protection 15
5.1 Heuristic and behavioral threat analysis 15
5.2 Real-time threat intelligence 15
5.3 Integrated patch management 16
5.4 Multi-engine anti-malware 16
5.5 Proactive web protection 17
5.6 Citrix 17
5.7 Linux 17
5.8 Multi-engine anti-malware 17
5.9 Integrity checking 17
5.10 Managed firewall service 17
6. Integration with SIEM/RMM 18
7. Professional serviceS 18
8. Data security 19

May 2020

DISCLAIMER: This document gives a high-level overview of the key security components in F-Secure Protection Service for Business. Details are omitted in order to prevent targeted attacks against our solutions. F-Secure is constantly improving its services. F-Secure reserves the right to modify features or functionality of the Software in accordance to its product life cycle practices.

EXECUTIVE SUMMARY

F-Secure Protection Service for Business helps companies stop threats like ransomware and proactively avoid data breaches on their workstations, laptops, mobiles and servers. The solution has everything businesses need for endpoint protection, including fully integrated patch management capabilities to effectively prevent attacks that leverage vulnerabilities in installed software. Protection Service for Business outperforms competing products, consistently earning top marks for providing the best protection in the industry.

F-Secure Protection Service for Business is favored by businesses that want:

- Broader endpoint and service coverage than what common solutions on the market can provide, at a much more attractive total cost of ownership (TCO)
- Achieve excellent protection level with minimum resource requirements with an option to completely outsource the management of the solution to a certified service provider
- A straightforward and scalable way to provide visibility and protection for multiple geographically dispersed sites from one location
- To avoid investing time and resources into maintaining local server environments

By merging the protection of various endpoints and value-added security tools into one unified solution, Protection Service for Business offers:

- Broader security coverage and capabilities than most endpoint security solutions
- Unified and streamlined cloud-based management that saves time and resources from security management and maintenance, further reducing TCO.

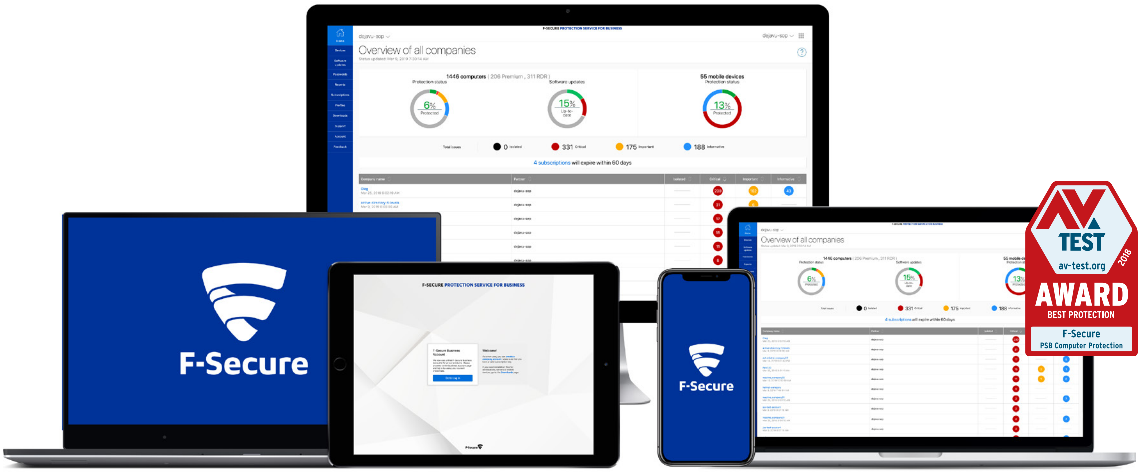
The solution is designed to be delivered as a cloud-based service; either as a self-managed service, managed service by a certified service provider, with an option to integrate it with 3rd party systems.

Our ability to provide better, more consistent protection than our competitors is proven year-by-year by testing done by independent industry experts and analysts.

F-Secure has earned 'Best Protection' awards from AV-Test in 6 years in the award's 8 year history. AV-Test is making comparison tests continuously throughout the year so in order to reach this precious award one needs to consistency show good results in protection tests.

To meet these demanding standards, the solution utilizes a multi-layered approach to security and leverages various modern technologies, such as heuristic and behavioral threat analysis, and real-time threat intelligence provided via the F-Secure Security Cloud.

This ensures that you're at the forefront of security.



1. SOLUTION OVERVIEW

Companies are facing challenges in minimizing the business risk brought on by cyber threats like ransomware. F-Secure Protection Service for Business is designed from the ground up to solve challenging business security needs with minimum maintenance and management overhead. It offers award-winning best protection for Windows and Mac computers, iOS and Android devices and a variety of server platforms. With integrated patch management, layered protection, and advanced behavior and heuristic analysis, Protection Service for Business stops tomorrow's cyber threats – today.

F-Secure Protection Service for Business delivers:

- **Best protection** in the industry improves business continuity and saves time in incident recovery
- **Proactively minimizes business risk** of cyber breaches with fully integrated patch management
- **Cloud-native solution** saves time in deploying, managing and monitoring security

F-Secure Protection Service for Business solution is also available as a managed service. F-Secure certified service providers can use Partner Managed version of the solution to leverage many unique service provider features, like multi-company dashboard, reporting and subscription management.

1.1 Solution packages

Protection Service for Business solution's Computer and Server Protection for Windows and Mac are available as standard, premium or advanced packages. Standard features include advanced anti-malware, patch management and many other endpoint security capabilities. Premium features add better protection against ransomware and application control.

✓ Advanced threat protection with detection and response *

✓ Anti-ransomware with dataguard and application control

✓ Advanced anti-malware and patch management

STANDARD
Computer / server protection standard

PREMIUM
Computer / server protection premium

ADVANCED
Computer / server protection premium + rapid detection & response

*Note: available features vary by operating platform

Also a fully integrated advanced protection package is available with F-Secure Rapid Detection & Response solution that delivers endpoint detection and response (EDR) features. It works with F-Secure Protection Service for Business as a single-client and management infrastructure for both workstations and servers. The EDR features are designed to detect and respond to targeted and other advanced cyber threats designer to get around even the most advanced preventive controls.

The different protection feature packages can be activated with a license key code change without having to re-install client software. More information on F-Secure Rapid Detection & Response from here.

Software Updater

Automated patch management to update Microsoft and 2500+ 3rd party software apps.

DeepGuard

An intelligent, heuristic anti-malware engine offering 0-day detection capability. Read F-Secure DeepGuard white paper.

Web content control

Improve security and productivity with controlled access to websites. Prevent access to websites based on categories and enforce your corporate policy.

Connection control

Activate additional security for sensitive transactions such as online banking.

Real-time protection

F-Secure Security Cloud protects against new malware as it utilizes threat details seen by other protected machines, making responses far more efficient.

Multi-engine anti-malware

Provide unmatched protection with highly advanced, multi-engine anti-malware.

Firewall

Additional rules and management functionality integrated with Windows Firewall.

Browsing protection

Proactively prevents employees from accessing harmful sites that contain malicious links or content.

Device control

Device Control prevents threats from entering your system via hardware devices such as USB sticks, CD-ROM drives, and web cameras. This also prevents data leakage, by allowing read-only access, for example.

DataGuard

Provides additional protection against ransomware, and prevents the destruction and tampering of data.

Application Control

Blocks execution of applications and scripts according to rules created by our penetration testers, or as defined by the administrator. In addition, Application Control can be used to block loading of DLL's or other files for additional security.

XFENCE

Unique security capability for protecting Macs against malware, trojans, back doors, misbehaving applications, and other threats by preventing applications from accessing files and system resources without explicit permissions.

1.2 Solution components

The solution is composed of four main components, each described in this document:

1. **Management Portal** as a cloud-based management portal
2. **Computer Protection** as dedicated security clients for workstations (Windows, Mac)
3. **Mobile Protection** for mobile devices with F-Secure Freedome for Business (iOS, Android)
4. **Server Protection** a variety of server platforms (Windows, SharePoint, Exchange, Citrix, Linux)

1.3 Solution deployment

Endpoint security clients can be deployed by email, local installation, batch script, enterprise management systems (SolarWinds, Kaseya, Datto) or with an MSI package via domain-based remote installation tools. Similarly, Mac clients are deployed by using MPKG, Mobile Device Management tools or with preconfigured self-made signed package.

For normal deployments, all endpoint security client deployments can be initiated from the portal via an email flow. The subscription key is automatically included in the link or installer so that the end-user need only click the link for the installation process to start automatically.

For larger environments, you can create an MSI package that can be deployed either with your own remote installation tools or with ours. The Windows client also contains built-in program flags, which can be used to automate client deployment via batch scripting.

Whenever the Windows client is deployed on systems with a conflicting security solution, our sidegrade feature detects it and automatically uninstalls it before continuing with the installation of F-Secure software. This ensures a much smoother and faster transition from one vendor to another.

When a new computer is added to Protection Service for Business a default configuration (profile) can be assigned automatically based on its location in an Active Directory hierarchy. This streamlines the deployment process and reduce risks for misconfiguration.

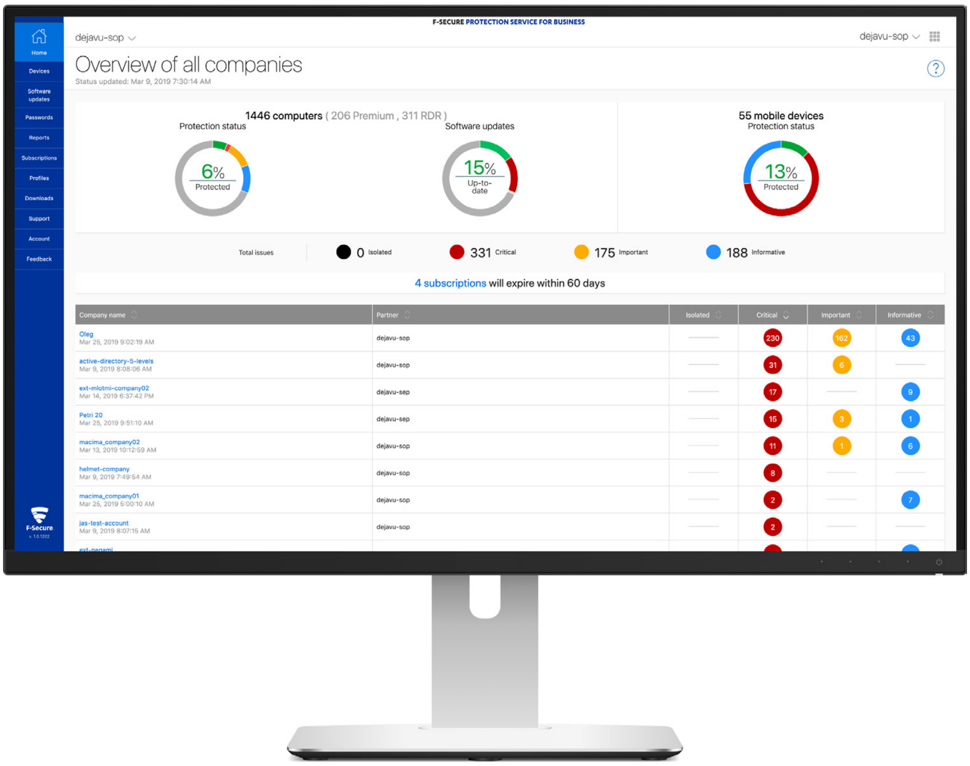
Mobile Protection features are commonly deployed by using a third-party mobile device management (MDM) available with a subscription that support the use of external MDM solutions.

The patch management capabilities are fully integrated into Windows server and workstation clients and can be controlled via the management portal. As a hosted solution, there is no need to install separate agents or management servers or consoles, unlike with traditional patch management solutions.

F-Secure Endpoint Proxy, also referred to as Policy Manager Proxy, is provided by F-Secure in order to minimize the bandwidth usage while downloading updates to Computer Protection clients. This proxy caches malware signature database updates as well as software updates of the Computer Protection client itself and patch management software updates.

Endpoint protection client software update malware signature databases and the client software itself automatically without administrator having to worry about the updates or upgrades manually.

F-Secure partners can customize both the endpoint protection client software and the Management Portal with their logo and support link.



Overview of all companies

Status updated: Mar 9, 2019 7:30:14 AM

1446 computers (206 Premium , 311 RDR)

Protection status: 6% Protected

Software updates: 15% Up-to-date

55 mobile devices

Protection status: 13% Protected

Total issues ● 0 Isolated ● 331 Critical ● 175 Important ● 188 Informative

4 subscriptions will expire within 60 days

Company name	Partner	Isolated	Critical	Important	Informative
Oleg Mar 25, 2019 9:02:19 AM	dejavu-sop	—	230	162	43
active-directory-5-levels Mar 9, 2019 8:08:06 AM	dejavu-sop	—	31	6	—
ext-mlotmi-company02 Mar 14, 2019 6:37:42 PM	dejavu-sep	—	17	—	9
Petri 20 Mar 25, 2019 9:51:10 AM	dejavu-sep	—	15	3	1
macima_company02 Mar 13, 2019 10:12:59 AM	dejavu-sop	—	11	1	6
helmet-company Mar 9, 2019 7:49:54 AM	dejavu-sop	—	8	—	—
macima_company01 Mar 25, 2019 5:00:10 AM	dejavu-sop	—	2	—	7
jas-test-account Mar 9, 2019 8:07:15 AM	dejavu-sop	—	2	—	—
ext-negami					

2. MANAGEMENT PORTAL

F-Secure Protection Service for Business makes it easy to deploy, manage, and monitor the security of your endpoints from a single, intuitive console. It gives you excellent visibility into all of your devices.

The management portal was designed from the ground up to simplify and accelerate security management in demanding, multi-device and multi-site environments. Below are some examples of how the solution considerably reduces the amount of time and resources needed for security maintenance and management:

- Endpoint clients automatically receive client, security, and database updates, minimizing the time needed for updates and maintenance
- By consolidating the security management of various endpoints and tools into one portal, the overall management is streamlined considerably, saving time
- Patch Management can be set to deploy missing security patches automatically as soon as they are available, saving time from manual software updates
- As a hosted service, there is no server hardware or software to install or maintain – all you need is a browser
- The portal has been designed by a dedicated User Experience team to utilize the most optimal user journeys, greatly increasing user efficiency

The console-endpoint communication works in real time. This allows IT admins to manage and monitor the security of the environment without disruptions or delays caused by polling intervals.

In essence, it allows IT admins to configure, deploy, and validate changes in one go.

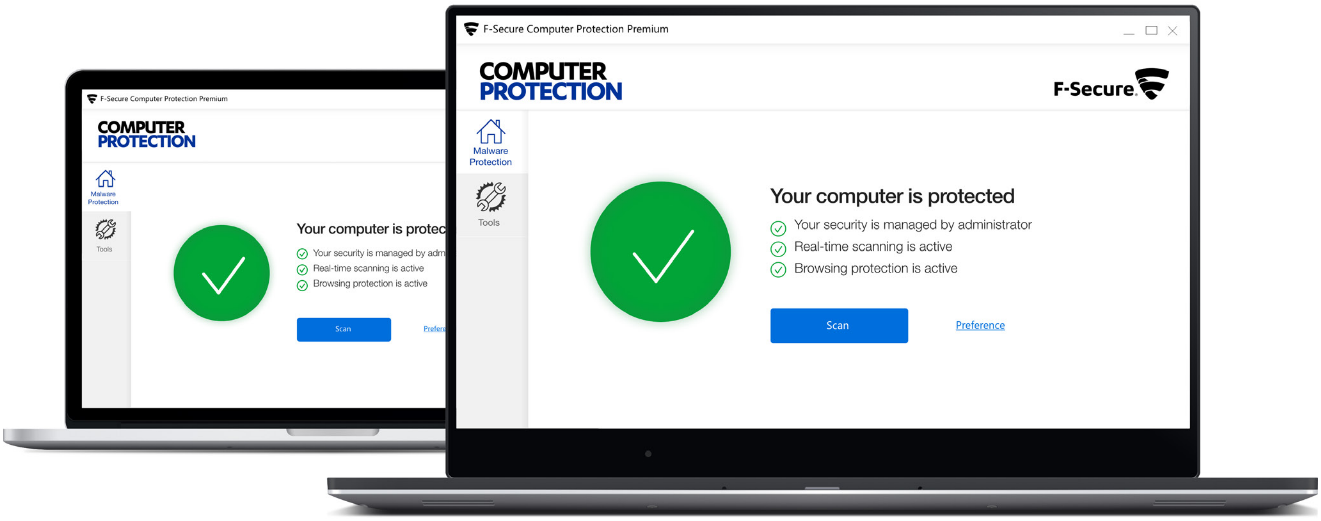
And if there is a security incident that needs to be solved ‘right now’, you can remediate and deploy a fix immediately.

You can create and customize individual security policies (profiles) and assign them either individually or in groups to computers, and servers by using labels. All settings and policies can be enforced down to the individual level if needed so that end-users cannot change them. Policies can be created e.g. per Active Directory group and assign the policies automatically to devices attached to the group.

The management portal gives you a complete overview of the security status of your entire environment. This includes potential software vulnerabilities, missing security updates, and the status of security features like real-time scanning and firewall.

For example, you can track the number of blocked infections and pay closer attention to the devices that are attacked the most. You can set automatic email alerts so that specific infection parameters get your attention first. If you need more information on any particular infection, you can obtain it directly from our security database.

The management portal delivers a wide range of graphical reports in an intuitive format, making data easier and faster to digest and understand—and more appealing for stakeholders to read. Device security details can also be exported as CSV files if required.



Your computer is protected

Your security is managed by administrator

Real-time scanning is active

Browsing protection is active

3. COMPUTER PROTECTION

Endpoint protection for computers forms the cornerstone of any secure environment. And in today's security landscape, it is vital to ensure that protection goes well beyond traditional anti-malware. With F-Secure Protection Service for Business, it is simple to deliver powerful, resource-friendly security for Windows, Mac, and Linux computers.

3.1 Combining all required endpoint protection stack into one

Modern endpoint protection suites employ a multi-layered approach to providing security. Technologies such as network filtering and scanning, behavioral analysis, and URL filtering augment traditional file scanning components. These different protection features are built into F-Secure Ultralight in a multi-layered design, so that if a threat escapes one layer, there is still another layer that can catch it. And as the threat landscape changes, some layers may be removed, or new ones may be added both in the endpoints and in the cloud.

Ultralight combines all of the technologies present in F-Secure’s full endpoint protection stack into a single package. It consists of a number of drivers, engines, and system services that provide mechanisms to protect both a device and its users. Ultralight provides traditional anti-virus functionality, such as real-time file scanning and network scanning. In addition, it includes modern, proactive protection technologies that aim to stop zero-day exploits and stay ahead of new attacks. F-Secure’s Security Cloud provides Ultralight components with real-time information as the threat landscape changes.

For more information on the integrated protection technologies done by Ultralight, see the technical whitepaper.

3.2 Heuristic and behavioral threat analysis

Heuristic and behavioral threat analysis, done by DeepGuard, is critical in identifying and blocking the most sophisticated malware prevalent today. DeepGuard provides immediate, proactive, on-host protection against new and emerging threats by focusing on malicious application behavior rather than through static identification of specific, known threats.

This shift in focus allows it to identify and block previously unseen malware based on their behavior alone, neatly providing protection until security researchers are able to analyze and issue a detection for that specific threat.

By communicating with F-Secure's Security Cloud, DeepGuard is also able to use the latest reputation and prevalence information available for any previously encountered object to fine-tune its security evaluations, reducing the risk of false positives or redundant analyses that can interfere with the user experience.

The on-host behavioral analysis also extends to intercepting attacks that attempt to exploit vulnerabilities in popular programs in order to install malware onto the machine. DeepGuard is able to identify and block routines that are characteristic of an exploit attempt, preventing exploitation – and in turn, infection. Exploit interception safeguards users from harm even when vulnerable programs are present on their machine.

For more information about the heuristic and behavioral threat analysis done by DeepGuard, see the technical whitepaper.

3.3 Real-time threat intelligence

The security client uses real-time threat intelligence provided by F-Secure's Security Cloud, ensuring that all new or emerging threats are identified, analyzed, and prevented within minutes.

A cloud-based threat analysis service affords many benefits over traditional approaches. F-Secure gathers threat intelligence from tens of millions of client nodes, building a real-time picture of the global threat situation.

For example, if heuristic and behavioral threat analysis identifies a zero-day attack on another endpoint on the other side of the world, the information is shared with all protected devices via Security Cloud—rendering the advanced attack harmless mere minutes after initial detection.

For more information on the functions and benefits of F-Secure's Security Cloud, see our technical whitepaper.

3.4 Industry-leading Mac security

F-Secure Computer Protection for macOS includes XFENCE, a unique security capability for Macs. It protects Macs against malware, trojans, back doors, misbehaving applications, and other threats by preventing applications from accessing your files and system resources without explicit permission.

The tool leverages advanced rule-based analysis to monitor apps that attempt to access confidential files and system resources, enhanced by the threat intelligence provided by Security Cloud to minimize false positives and user interaction through allow/disallow prompts.

In addition, XFENCE provides application layer firewall that can configure and control network access on application level. It can be used to isolate hosts, to allow network access only to trusted singed applications, and to blacklist/whitelist applications by bundle id.

3.5 Protection for Linux endpoints

F-Secure Protection Service for Business includes protection for Linux in F-Secure Server Protection. The product can be used to protect endpoint devices as well.

3.6 Integrated patch management

Windows endpoints include an automated patch management feature that is fully integrated with the clients. There is no need to install separate agents, management servers, or consoles.

It works by scanning for missing updates, creating a vulnerability report based on missing patches, and then downloading and deploying them automatically. You can also choose to install updates manually if needed.

Security patches include Microsoft updates and 2500+ third-party applications such as Flash, Java, OpenOffice, and others that commonly serve as attack vectors due to their popularity and larger number of vulnerabilities.

Administrators can define detailed exclusions for the automatic mode based on software names or bulletin IDs. Some updates are excluded by definition, such as Service Packs. Administrators can also flexibly define the day and time when installations should be performed, as well as how restarts are forced and the grace time before forcing a restart after installation.

Patch management is a critical security component. It's the first layer of protection when malicious content reaches endpoints and can prevent up to 80% of attacks simply by installing software security updates as soon as they become available.

3.7 Multi-engine anti-malware

Our computer component utilizes a proprietary, multi-engine security platform to detect and prevent malware. It offers superior protection compared to traditional signature-based technologies:

- Detects a broader range of malicious features, patterns, and trends, enabling more reliable and accurate detections, even for previously unseen malware variants
- By using real-time look-ups from F-Secure's Security Cloud, it can react faster to new and emerging threats in addition to ensuring a small footprint
- Emulation enables detection of malware that utilize obfuscation techniques, and offers another layer of security before a file is run

3.8 Extensive and proactive web protection

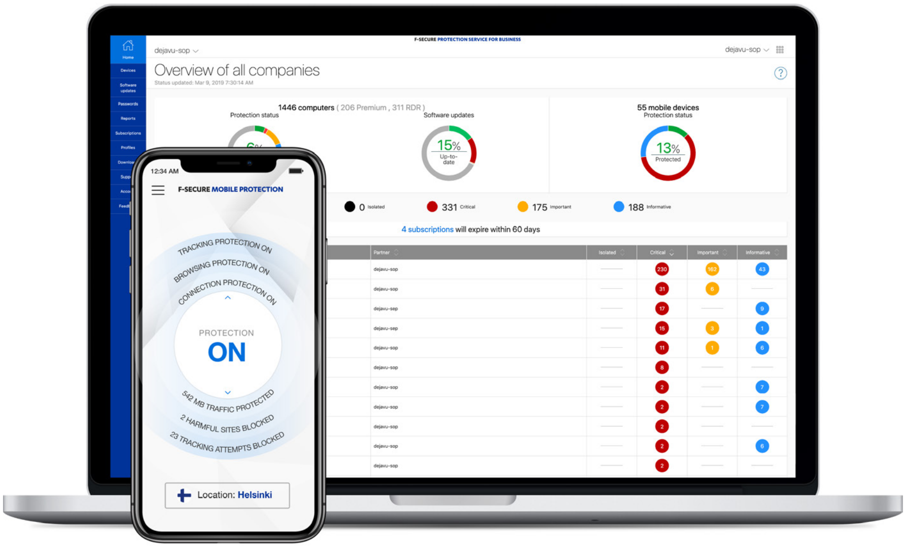
Furthermore, the solution offers extensive and proactive web protection, ensuring the most exploited attack vector is well defended.

- Proactively prevents access to malicious and phishing sites even before they are accessed (e.g. on Google search and when clicking on a web link). This is particularly effective, as early intervention greatly reduces overall exposure to malicious content and therefore to attacks.
- It prevents the exploitation of active content such as Java and Flash, which are utilized in the vast majority of online attacks. These components are automatically blocked on unknown and suspicious sites based on their reputation data, with the option of setting exclusions.
- The solution can also be used to restrict inappropriate web usage, granularly denying or allowing access to non-work-related destinations, such as social media sites and adult sites, to maximize efficiency and avoid malicious sites.
- After the initial layers of web protection, the content in HTTP web traffic is also subjected to analysis in order to provide additional protection against malware, before it gets into contact with the endpoint itself.
- IT admins can also designate business-critical web activities that utilize HTTPS (like intranets or sensitive cloud services, for example CRMs) to use an additional security layer. When active, it closes all untrusted network connections, preventing attacks and exfiltration of data from the services during the session.

The security features vary depending on the chosen operating system. Below is an overview of the feature comparison between Windows, macOS, and Linux.

	WINDOWS	macOS	LINUX
SECURITY			
Anti-malware	YES	YES	YES
DeepGuard	YES	NO	NO
DataGuard	YES	YES*	NO
Security cloud	YES	YES	NO
Patch management	YES	NO	NO
Application control	YES	NO	NO
Browsing protection	YES	YES	NO
Web traffic scanning	YES	NO	NO
Web content control	YES	YES	NO
Content type filtering	YES	NO	NO
Connection control	YES	YES	NO
Firewall	YES	YES	NO
Integrity checking	NO	NO	YES

* Part of the functionality provided by XFENCE



4. MOBILE PROTECTION

Maintaining control over mobile devices is a fundamental aspect of modern cyber security. With Protection Service for Business, IT admins have an easy way to secure and control mobile devices, both Android and iOS.

The component delivered by F-Secure Freedome for Business includes everything that is needed for exceptional mobile protection in one package: personal VPN, Wi-Fi security, and proactive App (Android) and web protection.

The mobile client is also designed to complement and be deployed via third-party MDM solutions.

4.1 Mobile VPN

The mobile VPN automatically encrypts traffic between your mobile device and a selected

F-Secure service node, allowing your employees to safely use public Wi-Fi and mobile networks.

It prevents the interception of emails, browser sessions, and use of online services, in addition to providing an extra security layer over HTTPS connections. It also enables you to change your virtual location, hide your IP address, and access local services when abroad.

4.2 Security Cloud

The security client uses real-time threat intelligence provided by F-Secure's Security Cloud, ensuring that all new or emerging threats are identified, analyzed, and prevented within minutes.

A cloud-based threat analysis service affords many benefits over traditional approaches. We gather threat intelligence from tens of millions client nodes, building a real-time picture of the global threat situation. For example, when an APK or file is downloaded, it is scanned and additionally its reputation is checked in the Security Cloud. Malicious files are prevented from running and unknown files or apps are uploaded for deeper analysis. Scan results benefit all users, for example by minimizing false positives and rendering new attacks harmless in a matter of minutes.

For more information about the functions and benefits of F-Secure's Security Cloud, see our technical whitepaper.

4.3 Application protection

When the VPN connection is active, mobile devices are automatically protected against malware and malicious content. F-Secure service nodes scan the traffic at the network level, utilizing the full extent of available security analytics. This allows us to provide better security than traditional mobile security solutions:

- Security is not hampered by limited mobile device resources
- Resource-intensive processes do not impact device performance and battery life
- Network-level scanning prevents contact with malicious content in the first place

For Android devices, security is further enhanced with local scanning—including real-time reputation checks from the F-Secure Security Cloud—even when the VPN is not connected.

4.4 Browsing protection

Browsing protection is a key security layer that proactively prevents end-users from visiting malicious sites. This is particularly effective, as early intervention greatly reduces overall exposure to malicious content - and therefore to attacks.

For example, Browsing protection prevents end-users from being tricked into accessing seemingly legitimate phishing sites, accessing malicious sites through an email link, or getting infected through malicious third-party advertisements on otherwise legitimate sites.

4.5 Faster browsing and less data use

The component is designed to have a minimal impact on mobile performance and battery life. In fact, by using traffic compression over VPN and preventing online tracking and advertising with Anti-Tracking, it increases browsing speed.

4.6 Third-party MDM deployment

The mobile client is also designed to complement and be deployed via third-party Mobile Device Management (MDM) solutions, such as AirWatch, MobileIron, Intune, and MaaS360.

By using a dedicated security component on top of the basic capabilities provided by the MDM solution, IT admins can significantly increase the security against malware, data theft, and phishing attempts that target mobile devices.

5. SERVER PROTECTION

Servers are critical to a company's communication, collaboration, and data storage. Protection Service for Business provides security for servers while enabling them to run at peak performance. The solution provides security for Windows, Citrix, and Linux servers.

Below is an overview of the core capabilities for different server platforms:

	WINDOWS	CITRIX	LINUX
CORE SECURITY			
Anti-malware	**YES**	**YES**	**YES**
Deepguard	**YES**	**YES**	NO
Security cloud	**YES**	**YES**	NO
Patch management	**YES**	**YES***	NO
Browsing protection	**YES**	**YES**	NO
Web traffic scanning	**YES**	**YES**	NO
Firewall	**YES**	NO	NO
Integrity checking	NO	NO	**YES**
REMOTE MANAGEMENT VIA PORTAL			
Security management	**YES**	**YES**	YES**
Security monitoring	**YES**	**YES**	YES**

* Also includes published applications; ** Available in 3Q/2020

5.1 Heuristic and behavioral threat analysis

Heuristic and behavioral threat analysis, done by DeepGuard, is critical in identifying and blocking the most sophisticated malware prevalent today. DeepGuard provides immediate, proactive, on-host protection against new and emerging threats by focusing on malicious application behavior rather than through static identification of specific, known threats. This shift in focus allows it to identify and block previously unseen malware based on behavior alone, neatly providing protection until security researchers are able to analyze and issue a detection for that specific threat.

By communicating with F-Secure's Security Cloud, DeepGuard is also able to use the latest reputation and prevalence information available for any previously encountered object to fine-tune its security evaluations, reducing the risk of false positives or redundant analyses that can interfere with the user experience. The on-host behavioral analysis also extends to intercepting attacks that attempt to exploit vulnerabilities in popular programs in order to install malware onto the machine. DeepGuard is able to identify and block routines that are characteristic of an exploit attempt, preventing exploitation – and in turn, infection. Exploit interception safeguards users from harm even when vulnerable programs are present on their machine.

For more information on the heuristic and behavioral threat analysis done by DeepGuard, see the technical whitepaper.

5.2 Real-time threat intelligence

The security client uses real-time threat intelligence provided by F-Secure's Security Cloud, ensuring that all new or emerging threats are identified, analyzed, and prevented within minutes.

A cloud-based threat analysis service affords many benefits over traditional approaches. F-Secure gathers threat intelligence from tens of millions of client nodes, building a real-time picture of the global threat situation. For example, if the heuristic and behavioral threat analysis identifies a zero-day attack on another endpoint on the other side of the world, the information is shared with all protected devices via Security Cloud—rendering the advanced attack harmless mere minutes after initial detection.

For more information on the functions and benefits of F-Secure's Security Cloud, see our technical whitepaper.

5.3 Integrated patch management

The component includes an automated patch management feature that is fully integrated with Windows server clients. There's no need to install separate agents, management servers, or consoles.

It works by scanning for missing updates, creating a vulnerability report based on missing patches, and then downloading and deploying them automatically. You can also choose to install updates manually if needed. Security patches include Microsoft updates and 2500+ third-party applications such as Flash, Java, OpenOffice, and others that commonly serve as attack vectors due to their popularity and large number of vulnerabilities.

5.4 Multi-engine anti-malware

Our computer component utilizes a proprietary, multi-engine security platform to detect and prevent malware. It offers superior protection to traditional signature-based technologies:

- Detects a broader range of malicious features, patterns, and trends, enabling more reliable and accurate detections, even for previously unseen malware variants
- By using real-time look-ups from the F-Secure Security Cloud, it can react faster to new and emerging threats in addition to ensuring a small footprint
- Emulation enables detection of malware that utilizes obfuscation techniques, and offers another layer of security before a file is run

5.5 Proactive web protection

Furthermore, the solution offers extensive and proactive web protection for terminals, ensuring the most exploited attack vector is well defended.

- Proactively prevents access to malicious and phishing sites even before they are accessed. This is particularly effective, as early intervention greatly reduces overall exposure to malicious content, and therefore to attacks.
- After the initial layer of web protection, the content in web traffic (HTTP) is also subjected to analysis, in order to provide additional protection against malware, before it gets into contact with the endpoint itself.

5.6 Citrix

On top of the same core security capabilities as for Windows servers, the Citrix component provides additional protection for Citrix environments by extending the integrated patch management capabilities for published applications. The client is Citrix Ready-certified, ensuring that it works flawlessly in Citrix environments.

5.7 Linux

Linux Security provides core security capabilities for Linux clients: multi-engine anti-malware and built-in firewall management, in addition to vital Integrity Checking. It is designed to detect and prevent both Windows and Linux-based attacks, making it particularly useful in mixed environments, where an unprotected Linux machine can be used as an easy attack vector.

5.8 Multi-engine anti-malware

The clients utilize a proprietary, multi-engine security platform to detect and prevent malware. It offers superior protection to traditional signature-based technologies, with the added benefit of not being reliant on one technology alone. The platform detects a broader range of malicious features, patterns, and trends, enabling more reliable and accurate detections, even for previously unseen malware variants.

5.9 Integrity checking

The component comes with a built-in integrity checker, which detects and prevents attackers from tampering with kernels, system files, or configurations. It is a vital security feature, as it protects the system against unauthorized modifications, which could otherwise go unnoticed.

Integrity checking can be configured to send alerts to the administrator of any attempts to modify the monitored files. This makes unauthorized changes easy to detect, ensuring that any incident response actions can be taken without delay. If changes are needed on the baseline, for example due to OS, security, and software updates, admins can use a protected installation tool to make the necessary updates without any hassle.

5.10 Managed firewall service

Linux clients come with a built-in firewall service based on Netfilter and Iptables, which can be managed via the server's local WebUi. It can be easily managed via predefined security profiles that are tailored for common use cases. IT admins can create their own rules that apply specifically to their networking requirements. All network traffic that does not match any firewall rules can be logged using syslog.

6. INTEGRATION WITH SIEM/RMM

F-Secure Protection Service for Business can be fully integrated with an SIEM, RMM, or any other third-party auditing, management, or reporting tool. These include tools offered by Kaseya, Tableau, N-Able, Splunk, among many others.

The integration helps to leverage an organization’s existing investments and benefits from centralized tools, for example by streamlining the administrator’s security and incident response-related work.

By using the capabilities of the SIEM/RMM systems, the integration enables – for example – the creation of additional automation, customized workflows, and reports, further reducing the workload and optimizing the solution towards your organization’s specific needs. The scope of the integration can be as large or as small as needed, as any operation can be accessed individually via the API calls. For example, IT admins can opt to only get relevant data to a reporting, logging, or auditing system, rather than integrating the management capabilities as well.

The integration is done via a REST API, called F-Secure Management API. It provides access to all the operations and data available in the Management Portal.

For more information about the Management API and SIEM/RMM integration, see PSB Management API from help.f-secure.com.

7. PROFESSIONAL SERVICES

F-Secure’s additional support packages offer a collection of services for more flexible and comprehensive support experience. Our support is available to you during business hours or even in 24/7 service. We offer Advanced – or Premium Support with different level of service to suit your need.

ADVANCED	PREMIUM
Local business hours (English, Finnish, French, German, Japanese and Swedish)	**24/7** (English)
Priority access to technical support	Respond to critical incidents within an hour
Online tools for ticketing and follow-up	Management level escalation
Phone and call-back	Upgrade consultation
Chat and remote	Advice on malware removal

8. DATA SECURITY

F-Secure Protection Service for Business platform uses Amazon Web Services (AWS). This allows us to ensure high availability and fault tolerance, in additional to better response times and ability to scale as needed. Currently available geographic regions are Europe, North America, and APAC.

AWS states that each of their data centers are in alignment with Tier 3+ guidelines. For further information about the AWS datacenters, please see: https://aws.amazon.com/compliance/

Based in Finland, F-Secure follows the strict privacy and security legislation of both Finland and the European Union. We are compatible with the European Union privacy framework and we understand the privacy needs of our customers. F-Secure operates under the Finnish implementation of the EU Data Protection directive.

We take the security of the data centers very seriously, and keep them secure by using dozens of security measures, such as:

- **Security by design:** Our systems are designed from the ground up to be secure. We embed privacy and security in the development of our technologies and systems from the early stages of conceptualization and design to implementation and operation.
- **Rigorous access controls:** Only a small vetted group of F-Secure employees have access to the customer data. Access rights and levels are based on their job function and role, using the concept of least-privilege matching to defined responsibilities.
- **Strong operational security:** Operational security is an everyday part of our work, including vulnerability management, malware prevention and robust incident management processes for security events that may affect the confidentiality, integrity, or availability of systems or data.

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure.