F-SECURE CLOUD PROTECTION FOR MICROSOFT OFFICE 365

Solution Overview

F-Secure

CONTENTS

DISCLAIMER: This document gives a high-level overview of the key security components in F-Secure Cloud Protection for Microsoft Office 365. 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.

May 2020

EXECUTIVE SUMMARY

F-Secure Cloud Protection for Microsoft Office 365 helps organizations to mitigate their business email risks by providing effective threat protection for Microsoft Office 365 against increasingly sophisticated phishing attacks and malicious content. Seamless cloud-to-cloud integration eliminates the need for middleware or expensive IT work, making F-Secure Cloud Protection a cost-effective solution that is easy to manage.

F-Secure Cloud Protection for Microsoft Office 365 is favored by businesses that want:

- To minimize business disruption by mitigating email risks from harmful content undetected by standard Microsoft Office 365 email protection
- A cost-effective solution to protect Microsoft Office 365 email against phishing attacks, internal email risks, and malicious content and links
- Cloud-to-cloud integration with easy deployment and seamless administration to ensure uninterrupted and efficient email threat protection

F-Secure Cloud Protection for Microsoft Office 365 provides security features that mitigate the risks posed by files and URLs shared using Microsoft Office 365. Whenever an end-user receives or creates a Microsoft Outlook item, such as email, appointment, task, contact, or note in their mailbox, the solution analyzes all included attachments and links for harmful content, such as malware, Trojans, ransomware, or phishing. The solution also provides rich reporting, advanced security analytics, and system events to ensure faster response to the identified potential threats. F-Secure Cloud Protection for Microsoft Office 365 comprises a management portal for daily administration and a service backend that utilizes F-Secure's Security Cloud for analyzing the Microsoft Office 365 items for malicious files and URLs. You do not need to install any additional software or make any changes to your network configuration to start using the solution.

F-Secure has earned 'Best Protection' awards from AV-Test in 6 years* during the award's 8-year history. AV-Test makes comparison tests continuously throughout the year, so reaching this precious award requires consistent 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 F-Secure's Security Cloud.

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

1. SHARED RESPONSIBILITY MODEL

Some companies believe that when they purchase a cloud service, the cloud provider is responsible for the security as well. They are partly right, but with cloud services there is a model called the shared responsibility model, which states that cloud providers are responsible for the security OF the cloud, and customers using the cloud are responsible for security IN the cloud. In practice, this means that the cloud provider takes care of the physical security of data centers so that no-one can physically break into their facilities and undermine the security of the underlying platform. Cloud providers also take care of the authentication, identification, and user and admin controls. In GDPR terms, cloud providers are Data Processors.

Customers using the cloud services are responsible for the security of data stored in the cloud. This includes taking care that there is no malicious content or targeted attacks, internal data security risks, deception, or social engineering by offering security behavior training to their employees. This means that customers using the cloud services are responsible for the security of their email. They are the owners of the data.

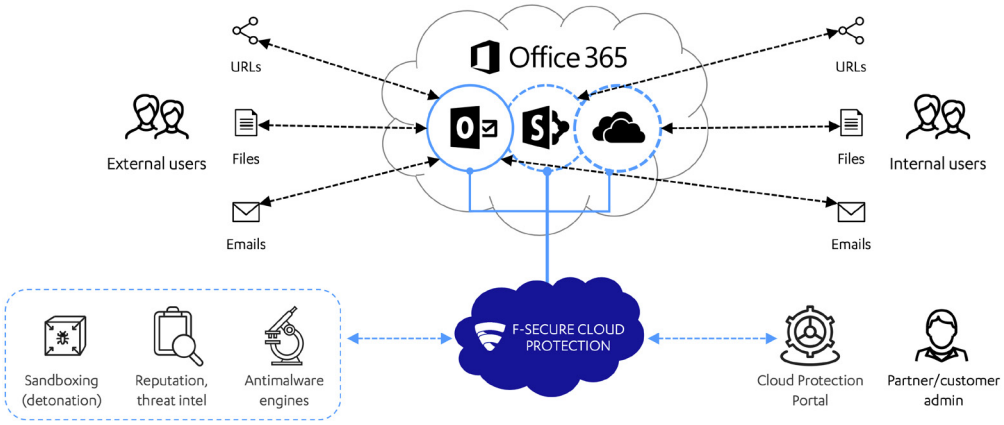
F-Secure Cloud Protection for Microsoft Office 365 delivers:

- A **cost-effective** solution to protect Microsoft Office 365 email against phishing attacks, internal email risks, and malicious content and URLs
- Combined with F-Secure's award-winning endpoint protection, as well as detection and response capabilities, the solution provides more **comprehensive protection** for your business than any email security solution alone
- **Cloud-to-cloud integration** with easy deployment and seamless administration to ensure uninterrupted and efficient email threat protection

2. SOLUTION OVERVIEW

F-Secure Cloud Protection for Microsoft Office 365 is a cloud-based security service that is designed to mitigate business email risks in organizations by providing effective threat protection for Microsoft Office 365 email messages against internal email threats, phishing attacks, and malicious content and URLs in inbound and outbound traffic. In addition to email messages, other Exchange items such as tasks, calendar appointments, contacts, and sticky notes are inspected for malicious content and URLs.

The diagram below gives you a high-level overview of the how the solution provides security for Microsoft Office 365.



Files, URLs, or emails

F-Secure Cloud Protection for Microsoft Office 365 processes the MS O365 user mailboxes to analyze file attachments and web links included in the body and headers of Exchange items such as email, calendar appointments, tasks, contacts, and sticky notes in inbound, outbound, and internal traffic.

F-Secure Security Cloud (sandboxing, reputation threat intelligence, antimalware engines)

F-Secure Security Cloud employs multi-stage content analysis in a stepped process triggered by the risk profile of the content. Additionally, high-risk files are subjected to a deeper analysis with our cloud sandboxing technology, which is designed to prevent zero-day malware attacks and other advanced threats.

F-Secure Cloud Protection for Microsoft Office 365 management portal

The F-Secure Cloud Protection portal is the management portal for administrators to manage the service in protecting MS O365 content. The management portal consists of advanced analytics and system events functionality to help administrators prioritize the threats based on the provided information in the portal and mitigate the related security risks in time. The portal also provides dashboard and reporting capabilities to check and report on the status of the system at all times. The reports can be downloaded for easy sharing among stakeholders.

Partner/customer administrator

The F-Secure Cloud Protection for Microsoft Office 365 service relies on partner/customer administrators to work on the security alerts and email notifications as a result of the malicious content found by analyzing the MS O365 user mailboxes and to take action based on the severity of the alert and threat category of the content.

Management roles

The F-Secure Cloud Protection for Microsoft Office 365 administrator can be assigned a role based on the management needs in the portal. The service allows Admin, Quarantine Manager and Read-only roles. Each role defines permissions that makes the portal management functionality accessible to the user. A user with the Admin role can add or remove users of different user roles using the web-based F-Secure Business portal for user management. The same user account can be used to access other F-Secure products and management portals by adding access to the respective solution using the F-Secure Business portal.

Users

Internal and/or external users are the entities that use the F-Secure Cloud Protection for Microsoft Office 365 service while exchanging the items such as emails, calendar appointments, tasks, contacts, sticky notes, etc. in their mailboxes. The internal user's mailbox is scanned for harmful contents in Exchange items in inbound, outbound, and internal traffic.

2.1. File protection

F-Secure Cloud Protection for Microsoft Office 365 scans harmful contents in file attachments found in Exchange items to protect against viruses, trojans, ransomware, and other advanced malware. It offers far superior protection compared to traditional technologies by leveraging real-time threat intelligence gathered from tens of millions of security clients, providing faster and better protection against new and emerging threats.

2.1.1. Initial analysis

A call is made to the F-Secure Cloud Protection backend with the checksum (SHA1) of the file attachments found in the MS O365 Exchange items (email, calendar, appointments, sticky notes, etc.). The checksum is compared to those saved in the existing threat detection cache in the backend to see if the file has been analyzed before. If analysis results are available from the cache, they are automatically used, and no further analysis is done. Existing threat detection results are periodically updated, and expired results cleared automatically in order to ensure up-to-date protection.

2.1.2. Threat intelligence check

If no results are found in the cache, a threat intelligence check is made via F-Secure's Security Cloud using the SHA-256 checksum. The service returns the file's safety reputation, prevalence, and possible threats detected. Depending on the policy settings, the system either removes the file attachment from the Exchange item, quarantines the whole item, deletes the whole item, and/or sends a notification to the user and administrator.

2.1.3. Multi-engine antimalware

If the file reputation is unknown, the contents of the file are uploaded to F-Secure's Security Cloud for further threat analysis. The file is subjected to deeper analysis by multiple complementary antimalware engines in order to find malware, zero-day exploits, and patterns of advanced threats. At this stage, the analysis process utilizes the full extent of the threat intelligence data and capabilities collected by F-Secure Labs.

2.1.4. Advanced threat analysis (sandbox)

Based on the threat analysis results, the system uses finetuned machine-learning techniques to decide whether to send the file to the cloud sandbox for deeper analysis. If it has suspicious risk indicators, a file is sent to the sandbox, where it is run in several virtual environments to analyze behavior. By focusing analysis on malicious behavior rather than static identifiers, the cloud sandbox can identify and block even the most sophisticated zero-day malware and exploits.

2.1.5. Analysis results

Based on the final verdict, the file attachment is categorized as either harmful or clean. Depending on

the specified settings, the file is removed from the Exchange item if it is harmful or suspicious and/or the user and administrators are notified about the incident. If no security threats are found, the file is accessible in its original Exchange item. The final verdict, file reputation, and other threat analysis details are stored in the threat detection cache for future use in the service backend.

2.2. URL protection

URL protection is a key security function that proactively prevents MS O365 users from accessing malicious or unwanted content through web links added to Exchange items such as emails, calendar appointments, tasks, contacts, and sticky notes. This makes it a particularly effective security service, as early intervention greatly reduces overall exposure to malicious content, and thus attacks. For example, it will prevent users from being tricked into accessing seemingly legitimate phishing sites and malicious sites.

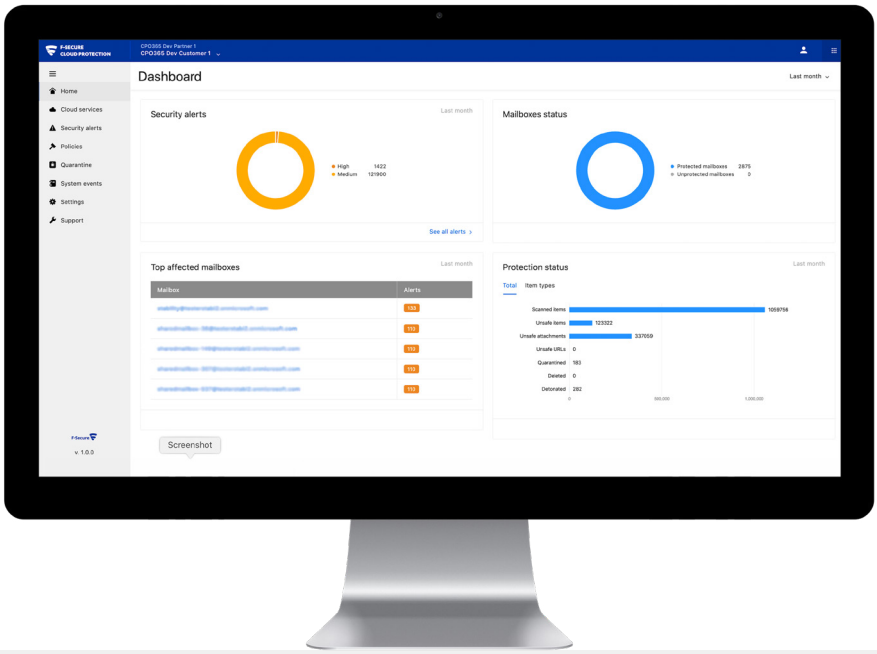
URL protection was created to deal efficiently with the billions of sites available on the internet and their constantly fluctuating security status. It is based on real-time lookup queries to F-Secure's Security Cloud. All queries go through several layers of anonymization to ensure the utmost business confidentiality.

The query fetches the latest reputation of the websites and their files, based on various data points, including IP addresses, URL keywords, site patterns, extracted website metadata like iframes and file types, and website behavior like exploit attempts, malicious redirects, or scripts.

2.2.1. URL security check

The solution scans the body of the Exchange items and queries the reputation of included URLs from

F-Secure's Security Cloud. If the link is deemed malicious based on the information received from the query, the access to the URL is either blocked or allowed, depending on the policy settings. The administrator can configure the policy to allow access to the URL by alerting the user in the subject of the Exchange item about the reputation of the URL. The administrator can also configure the policy to block access by quarantining the item or deleting the item if the URL is found to be malicious or suspicious.



2.3. Management portal

The F-Secure Cloud Protection for Microsoft Office 365 service provides a management portal for administrators to manage the MS O365 Exchange environments.

Thanks to rich reporting, flexible alerting, advanced security analytics, and system events, responding to threats is easy for system administrators, and full, 360-degree visibility makes sure that you know your MS O365 usage patterns. This is helpful when responding to an attack taking place through MS O365, investigating an attack coming from an unknown source, or in verifying whether MS O365 was part of an incident.

2.3.1. Deployment

F-Secure Cloud Protection for Microsoft Office 365 supports cloud-to-cloud integration without needing to install additional software or making changes on the server or clients. The protection is totally platform-agnostic and capable of detecting threats regardless of which device or application is used to access the Exchange mailbox items. Administrators can configure the service for scanning the MS O365 Exchange user mailboxes and provide comprehensive protection in just few minutes.

2.3.2. Dashboard

F-Secure Cloud Protection for Microsoft Office 365 management portal provides an easy-to-use dashboard for quick access to the most recent security alerts of malicious content found in the managed environments, the top affected mailboxes with the highest number of security alerts, and constantly up-to-date data about the Exchange items scanned and the type of action taken to protect against malicious content.

The dashboard also shows the coverage of the environment in terms of the number of mailboxes protected and ones that are not protected by the security service. This lets you know at all times if there are any security gaps in the environment due to unprotected mailboxes.

2.3.3. Security alerts

The security alerts widget provides quick and easy access to the most recent security alerts for an organization, sorted by the severity of the alert. The sorted list helps administrator to prioritize high-risk alerts immediately with detailed information about the found malicious content in the user mailboxes.

2.3.4. Mailbox status

The mailbox status widget on the dashboard provides a count of protected vs unprotected mailboxes in MS O365 tenants for the organization. This helps the administrator to understand at all times if there are any security gaps present due to those unprotected mailboxes.

2.3.5. Top targeted mailboxes

The top targeted mailboxes widget in the dashboard lists the top 5 user mailboxes with the most security alerts in an organization. The widget helps the administrator in checking if there is a sudden rise in the number of security alerts for certain mailboxes, which could be related to a possible security incident in the organization.

2.3.6. Protection status

The protection status widget shows the total amount of scanned and unsafe items. The widget also shows the type of actions taken to protect against the malicious content, such as quarantine or delete.

The item types tab in the widget provides more detailed information about the malicious content found per item type (emails, calendar appointments, tasks, sticky notes, contacts, groups, and others) in the user mailbox.

2.3.7. Protection trend

The protection trend widget shows the percentage of unsafe content during the current time period compared to the organization's average and previous period. The trend information helps administrators in knowing at all times if the organization security status is at the same level or if there is a sudden increase in unsafe content, which might be related to a possible security incident in the organization.

2.3.8. Analytics

F-Secure Cloud Protection for Microsoft Office 365 gives full, 360-degree visibility into MS O365 Exchange usage. All security alerts for malicious or suspicious content found in the user mailboxes are accessible in the portal in a convenient table view. The table is easily searchable and sortable based on different columns and criteria.

Many IT departments do not know what kind of content their users are sending or receiving via MS O365 Exchange items. That knowledge is often helpful, as IT administrators may, for example, find malicious files or URLs that should not be shared via MS O365.

Furthermore, a better understanding of internal customer needs and use cases helps administrators to serve their organization more effectively. With powerful search functionality, solution administrators and IT security departments can investigate content-based attacks very quickly.

2.3.9. Policy administration

F-Secure Cloud Protection for Microsoft Office 365 provides policies to define the security settings for the analyzed contents in MS O365 Exchange items. A policy is the set of settings and rules defining how the service protects user mailboxes and which actions are taken when a security threat is detected.

Administrators can use the F-Secure default policy to provide maximum protection from the get-go when configuring the tenants, or they can copy the default policy to modify the security settings according to the organization security requirements and make that the default policy, which is then assigned by default whenever a tenant is configured for protection.

2.3.10. Quarantine management

F-Secure Cloud Protection for Microsoft Office 365 allows administrators to quarantine an Exchange item based on the harmfulness of the files and URLs found in the item. The quarantine view in the management portal allows administrators to view, release, or delete quarantined items as needed. The administrator can also use various sorting and searching criteria to fine-tune the view while handling the list of quarantined items for the managed environments.

2.3.11. Reporting

F-Secure Cloud Protection for Microsoft Office 365 provides rich reporting capabilities for administrators to report on the security status of the protected environment at any time in an easily sharable format. The administrator can define the content and schedule (daily, weekly, monthly) reports to be automatically generated, and have the reports readily available in the portal for downloading. In addition, administrators can add a summary of the security status of the environment as a message that is added to the beginning of the generated report.

3. F-SECURE SECURITY CLOUD

F-Secure's Security Cloud is a cloud-based digital threat analysis system operated by F-Secure. It consists of a constantly growing and evolving knowledge base of digital threats fed by client system data and automated threat analysis services. The infrastructure for Security Cloud is hosted on servers in multiple Amazon Web Services data centers around the world. Security Cloud is a high-volume system that receives over 8 billion queries every day.

We collect only the minimum amount of client data necessary to provide our services. Every transferred bit must be justifiable from a threat prevention perspective, and data is never collected for presumed future needs. With the default settings, Security Cloud does not collect IP addresses, files, or other private information. Customers can give F-Secure permission to store suspicious executable files and/or suspicious non-executables files.

By evaluating the combined metadata with information drawn from in-house databases and various other sources, the automated analysis systems provide a fully-informed, up-to-date risk assessment for the threat, immediately blocking those that have been seen previously by any other service or device connected to Security Cloud.

Security Cloud also allows F-Secure Labs analysts to provide critical human intelligence and judgment to complement automated systems and on-host scanning technology. In addition to creating and maintaining the rules that underpin the databases and automated analysis systems, analysts actively monitor the latest threats and study malware characteristics and behavior patterns to find the most effective ways to identify malicious programs.

The following table documents our privacy principles in full detail:

Minimize upstream of technical data	F-Secure's Security Cloud employs multi-stage content analysis. File data is not sent to Security Cloud unless it is essential for providing protection and the customer has allowed it.
Do not send personal data upstream	No information on who posts or accesses the analyzed files or URLs, or from where, is sent to F-Secure's Security Cloud.
Do not trust the network	All metadata, files, and other content are transferred to Security Cloud securely either over HTTPS or separately encrypted and signed over HTTP.

Security Cloud principles:

Secure by design	A system is never secure unless it has been designed to be secure. Security cannot be added as a project afterthought. This is something that was put into practice when developing Security Cloud and its related systems.
Encrypted network traffic	Data is never transferred in plain text over the internet. In addition, encryption is used to ensure the integrity of various objects. F-Secure utilizes a mixture of generally available cryptographic libraries and protocols and customized cryptographic code.
Separated malware environments	We have over 20 years of experience in meeting the challenges of storing and testing malicious software. All malware handling is performed in networks isolated from the internet and other F-Secure networks. Storage and testing networks are isolated from each other, and files are transferred using strictly controlled methods.
Professional monitoring	All critical Security Cloud systems are monitored by F-Secure personnel. All systems storing or testing malware are hosted by F-Secure Corporation.
Controlled access	Only a limited number of F-Secure employees have access to Security Cloud's critical systems. Such access is granted, revoked, and documented according to a documented and controlled process.
Open attitude	The most fundamental principle in all security work is having an open and humble attitude. We have put a lot of effort into securing Security Cloud, but the work is never finished. A secure system can only be maintained by promoting an open attitude, in which system problems are reported, analyzed, and fixed promptly. This attitude includes public openness, should we encounter incidents that put customer security in jeopardy.

Find out more about F-Secure's Security Cloud in our Security Cloud Whitepaper and Security Cloud Privacy Policy.

3.1. Threat intelligence service

By leveraging real-time threat intelligence gathered from tens of millions of sensors, we can identify new and emerging threats within minutes of inception, ensuring exceptional security against the constantly evolving threat landscape. Our threat intelligence service enables F-Secure Cloud Protection to query the reputation of objects such as files and URLs. Files are verified by calculating the object's cryptographic hash SHA-1 and sending it to the reputation service.

3.2. Multi-engine antivirus

Multi-engine antivirus uses multiple security layers to detect exploits and unknown malware used in targeted attacks. The system combines behavioral analysis and heuristic and machine learning detection capabilities, which allow it to identify specific malware, families of malware with similar features, and broad ranges of malicious physical features and patterns. The results of this analysis may cause the file to be flagged as suspicious and sent on to the cloud sandbox for further processing.

3.3. Cloud sandbox

The cloud sandbox runs detected files in several virtual environments and analyzes the file behavior. If the file behavior is determined to be suspicious, information is sent to the multi-engine antivirus and threat intelligence service, where the next threat detection query will block the threat.

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