Solution overview

WithSecure™ Cloud Protection for Salesforce

Contents

DISCLAIMER: This document is intended to give a high-level overview of the WithSecure™ solution and its security components. Details are omitted in order to prevent targeted attacks against our solutions. WithSecure™ is constantly improving its services and reserves the right to modify features or functionality of the software in accordance to its product life cycle practices.

1. Executive overview

WithSecure™ Cloud Protection for Salesforce is a cloud-based security solution designed to complement the native security capabilities of the Salesforce platforms.

Together with Salesforce, we make it easier for companies to handle their part of security under the Shared Responsibility model used in cloud ecosystems. WithSecure™ Cloud Protection is an excellent choice for complementing overall security capabilities, and for ensuring that the company security strategy also extends to cloud services.

WithSecure™ Cloud Protection for Salesforce provides dedicated security components that mitigate the risks posed by files, URLs and emails handled by Salesforce platform users, without hindering the use of Salesforce. The solution also provides rich reporting, advanced security analytics, and full audit trails, ensuring that incident response is fast and efficient.

Thanks to native cloud-to-cloud integration between Salesforce and WithSecure™, Cloud Protection is an optimal choice from both security and resourcing perspectives.

First, there is no need to expend resources on deploying or maintaining middleware, such as servers or proxies, or modifying network configurations.

Furthermore, Salesforce uses HTTPS encryption in all their communications, which means solutions using proxies, like traditional Cloud access security brokers (CASBs), would have to break the encryption midway, making the system less secure and much more prone to vulnerabilities.

Finally, tight integration enables streamlined deployment via Salesforce AppExchange. The deployment takes only a few minutes, eliminating the need for expensive, time intensive IT work.

To summarize, WithSecure™ Cloud Protection for Salesforce offers the following benefits:

Advanced Threat Protection

- High-fidelity detections of known and unknown malware
- Protection against phishing links
- Powered by multi-stage content analysis, real-time threat intelligence, AI, and sandboxing

Real-time protection and visibility

- Automated scanning on upload and download
- Flexible on-demand and scheduled scans
- Click-time URL protection against dormant and mutating cyber threats
- Real-time visibility with full forensics trail for threat hunting

Click-and-go security – made with Salesforce

- Natively integrated, purpose-built in close collaboration with Salesforce
- No single point of failure, no additional middleware, connectors, configuration hassle, or additional hosting costs
- Up and running in minutes giving you instant value

2. WithSecure™ corporation

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

Founded in 1988, WithSecure™ is listed on the NASDAQ OMX Helsinki Ltd.

3. Shared responsibility model

In cloud ecosystems, cloud service providers and their customers typically share responsibility when it comes to security.

Salesforce, for example, covers various aspects of system and application level security such as authentication, rules, user permissions and roles.

It is every organization’s responsibility to secure files and links uploaded to Salesforce platforms by their users. However, organizations cannot guarantee identity and access control measures, overall security level, nor the safety of content used and shared in Salesforce clouds by external users such as partners or customers.

Furthermore, as many organizations provide direct access for cloud applications through their firewalls and other network security functions, protection against malware, ransomware and malicious links is often left solely to endpoints.

Consequently, it is necessary to provide additional security measures to mitigate this risk.

For example, organizations need to:

- Prevent targeted attacks through their Service/Customer Care teams utilizing Salesforce's Service Cloud.
- Prevent sharing of unwanted or malicious content such as pornography or ransomware in the organization's Community Cloud, which will reflect negatively on the organization, as it was their platform that was used to distribute the content and malware in the eyes of community users.
- Prevent malware from propagation within the organization though malicious attachments shared, for example, in the Sales Cloud or Chatter.

WithSecure™ Cloud Protection for Salesforce has been specially designed to prevent such risks. It complements native Salesforce security capabilities with dedicated security components that allow organizations to handle their part of security, as dictated by the Shared Responsibility model used in cloud ecosystems.

4. Solution overview

WithSecure™ Cloud Protection for Salesforce is a cloudbased security solution designed to complement the native security capabilities of the Salesforce platforms. It provides dedicated security components that mitigate the risks posed by files and URLs uploaded by users.

The solution supports most of Salesforce Clouds, including but not limited; Sales Cloud, Community Cloud and Service Cloud. It supports the following Salesforce editions: Professional, Enterprise, Unlimited and Developer.

WithSecure™ Cloud Protection for Salesforce has been designed and developed in close cooperation with Salesforce in order to ensure maximum compatibility and reliability in their various clouds.

The solution utilizes cloud-to-cloud architecture, so there is no need to deploy or maintain middleware like proxies, or to implement additional network configurations. Together with the streamlined AppExchange deployment process.

4.1 Function Diagram

4.1.1 File, URL or Email

WithSecure™ Cloud Protection constantly monitors all files, links and emails used via Salesforce platforms.

4.1.2 Salesforce Cloud

Whenever an end-user makes use of, uploads or downloads content via Salesforce, the traffic is intercepted and subjected to a patented threat analysis and detection process in the WithSecure™ Security Cloud. The user experience is of the utmost importance for our customers, so the solution is designed to minimize user delays and complement the inherent usability of Salesforce.

4.1.3 WithSecure™ Security Cloud

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

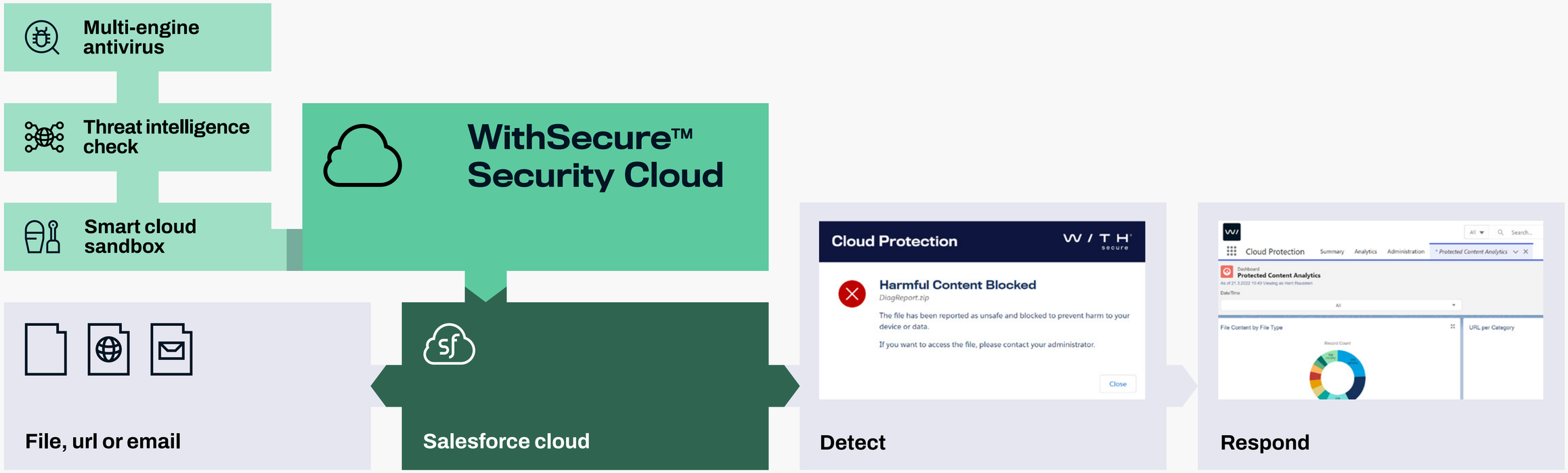
4.1.4 Detect

Content detected as harmful or disallowed, is automatically deleted or blocked, the end-user is notified that content was blocked, advised on what to do next, and further access is prevented. Security alert is sent to the solution administrator and the security team. Disallowed content is defined with a content filtering policy by file type or extension. As an example, administrator can choose to block all executables such as .com, .exe, .bin, and .bat files.

4.1.5 Respond

Thanks to rich reporting, advanced security analytics and full audit trails, responding to threats is easy for system administrators, whether responding to an attack taking place through Salesforce, or investigating an attack coming from an unknown source.

Below is a high-level overview of the process by which the solution provides complementary security for Salesforce clouds.



4.2 File Protection

WithSecure™ Cloud Protection utilizes a proprietary, multi-layered security platform to detect and prevent viruses, trojans, ransomware and other advanced malware. It offers far superior protection compared to traditional technologies:

- It detects a broader range of malicious features, patterns and trends, enabling more reliable and accurate detection, even for previously unseen malware variants
- By leveraging real-time threat intelligence gathered from tens of millions of security clients, it provides faster and better protection against new and emerging threats
- Emulation enables the detection of malware that utilizes obfuscation techniques

Our patented scanning logic ensures a transparent threat detection process when users upload and download files, thanks to seamless integration with Salesforce platforms.

4.2.1 Upload Protection

Whenever a user uploads a file to Chatter, Salesforce Files or Attachments, a multi-layered background analysis process begins:

Initial Analysis

A checksum (SHA1) of the file is calculated and stored in a threat detection cache within Salesforce Cloud, along with file content and its metadata. The checksum is compared to those saved in the existing threat detection cache to see if the file has been analyzed before. In this way, cloud calls can be limited and the user experience further improved. Existing threat detection results are periodically updated and expired results cleared automatically in order to ensure up-to-date protection. If analysis results are available from the cache, they are automatically used.

Threat Intelligence Check

If no results are found in the cache, a threat intelligence check is made via the WithSecure™ Security Cloud using the SHA-1 checksum. The service returns file safety reputation, prevalence and possible threats detected, automatically blocking any malicious files. Depending on the settings, the system either replaces the malicious files with a .txt file explaining why the original file has been removed, or simply blocks any further access to malicious files.

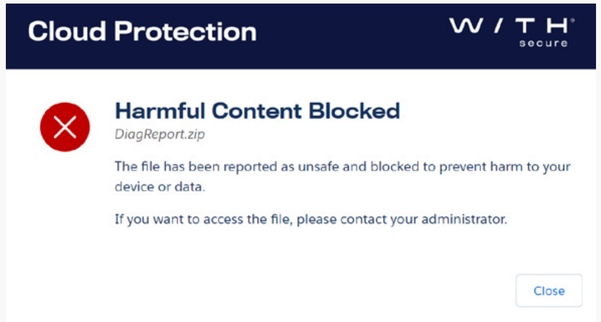
Multi-Engine Anti-Malware

If file reputation is unknown, the contents of the file are uploaded to the WithSecure™ Security Cloud for further threat analysis. The file is subjected to deeper analysis by multiple complementary anti-malware 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 WithSecure™ Labs.

Content Filtering

Before performing a threat analysis, the Cloud Protection app checks the file against the list of disallowed file types or extensions defined in the solution settings. If the file is found with one of extensions or file types from the disallowed list, the app takes action to block the file. Administrator receives an security alert according to the notification settings.

With the content filtering, the organization can prevent users from uploading inappropriate or dangerous content. For example, to minimize a risk of spreading malware, Cloud Protection can be configured to block any executables (such as EXE, COM) or scripts (such as VBS, PS1) uploaded to Salesforce Cloud.



Smart Cloud Sandbox

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

Analysis Results

Based on the final verdict, the uploaded file is categorized as either harmful or clean. Depending on settings specifications, the file is removed if it is harmful or suspicious and/or the file uploader and administrators are notified about the incident. If no security threats are found, the file is accessible in its original upload location and a file threat detection event is recorded to the scan log for further analysis and auditing, if needed. The final verdict, file reputation and other threat analysis details are stored in the threat detection cache for future use. Detection details of malicious files are sent to WithSecure's threat intelligence service so that the next threat detection query can identify and block the threat immediately.

4.2.2 Download Protection

Download Protection makes sure that users cannot download harmful or disallowed content from Chatter, Salesforce Files or Attachments. WithSecure™ Cloud Protection goes through the same process as described above. If the file verdict is already available in the threat detection cache, the file is allowed/ blocked accordingly, and if not, it will be subjected to the same process as above. If the file is safe, the user will download the file seamlessly, as per the regular Salesforce user experience. If the file is detected as harmful or disallowed, the application will block user access to the file and, depending on solution settings, send an alert to the administrator. Checks at both upload and download stages are critical to ensure that the latest security intelligence is always used. Malware that might have bypassed the process earlier is caught later when new threat intelligence becomes available.

4.2.3 Manual Scanning

Manual scanning can be used to scan Salesforce files and attachments which were either added to the Salesforce Cloud before installing WithSecure™ Cloud Protection or were excluded from scanning by Upload and Download Protection. Additionally, a scheduled scan can be set to scan the full system at regular intervals. The scans are executed in background without interference to the user experience or performance.

4.3 URL Protection

URL Protection is a key security function that proactively prevents Salesforce users from accessing malicious or unwanted content through web links added to Chatter posts and comments, Case descriptions and comments, as well as bodies of messages received via Email-To-Case.

This makes it a particularly effective security component, as the early intervention greatly reduces the overall exposure to malicious content, and thus attacks. For example, it will prevent users from being tricked into accessing seemingly legitimate phishing sites, malicious sites, or accessing content that is deemed inappropriate in a business context, such as adult or gambling 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 realtime lookup queries to WithSecure's scurity Cloud. All queries go through several layers of anonymization to ensure 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.

4.3.1 URL Security Check

The solution intercepts URLs that users post to Chatter or forms part of the email body (Email-to-Case) and replaces them with special redirect links, as shown on the screenshot below. The original link is included in brackets for recognition purposes, but the user cannot click it. Copying is prevented by obfuscating the URL.

In case the link is deemed malicious based on the information received from the query, entry to the website is blocked before any content in loaded, and the end-user receives a warning.

When the user clicks a redirect link, WithSecure™ Cloud Protection will send the original URL to the WithSecure™ Security Cloud for a threat intelligence check. Based on URL threat intelligence, access to the original URL iseither allowed or blocked.

4.3.2 URL Classification

URL Classification allows administrators to control and enforce the web pages that Salesforce users can access. They can, for example, deny access to non work- related destinations, such as social media sites, to avoid loss of working time. Sites in higher risk categories such as Adult or Gambling can be blocked to avoid potentially malicious sites and the viewing of inappropriate content in the business environment and on customer or partner portals.

When the user clicks a redirect link, WithSecure™ Cloud Protection sends the original URL to the WithSecure™ Security Cloud for a threat intelligence check. Based on the URL threat intelligence information, access to the original URL is either allowed or blocked.

Solution administrators can enforce usage rules in 28 different categories: Abortion, Ad services, Adult, Alcohol and tobacco, Anonymizers, Auctions, Banking, Blogs, Chat, Dating, Drugs, Entertainment, Gambling, Games, Hacking, Hate, Job search, Payment service, Scam, Shopping, Social networking, Software download.

4.4 Email Protection

Salesforce Email-to-Case automatically creates cases and auto-populates case fields when customers send messages to specified email addresses. WithSecure™ Cloud Protection intercepts inbound email and starts threat detection for all attachments and URLs. If the file verdict is already known and threat detection Time- To-Live (TTL) is still valid, malicious files are removed or administrators are notified about the incident. In addition, all URLs are rewritten.

If the file is new or the TTL is expired, WithSecure™ Cloud Protection will start the same threat detection process used in upload protection. See section 4.2 File Protection.

When a user clicks a URL, WithSecure™ Cloud Protection wills start the same threat detection process used in URL Security Check. See section 4.3 URL Protection.

4.5 Management

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

4.5.1 Analytics

WithSecure™ Cloud Protection gives 360-degree visibility into Salesforce content. All upload and download file actions and URL clicks are stored in an analytics log. Analytics includes File and URL event history view which is helpful when administrator wants to identify all users who have accessed Salesforce content.

Many IT departments don’t know what kind of content their organizations store in Salesforce. That knowledge is often helpful, as IT administrators may, for example, find executable files that should not be stored there.

Furthermore, better understanding 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 in seconds:

- Confirm or rule out Salesforce as an attack vector
- Find attacker details such as an IP address
- Identify users who accessed malicious content

Analytic log includes the following Information:

- Timestamp
- Action
- Verdict + File Prevalence
- Reason
- Direction
- (Upload/Download/Post/Click)
- Username
- Filename
- File type
- File version
- File Size
- URL
- URL Categories
- Location (Where the file/URL is stored)
- File SHA-1 checksum
- IP-Address

4.5.1 Alerts

All security alerts and audit events are written to the Security Alerts log. Salesforce administrators can enable solution administrators and IT security personnel to receive alerts in the following situations:

- Harmful content found
- Harmful content blocked on upload (alert to uploader if the user is internal)
- Harmful URL found
- Harmful URL found on upload (alert to uploader if the user is internal)
- Disallowed URL found (alert to uploader if the user is internal)
- If file or URL scanning results changed from safe to unsafe
- Disallowed file type found
- Disallowed file type found on upload (alert to uploader if the user is internal)

4.5.3 Reporting

WithSecure™ Cloud Protection gives you a rich view of Salesforce content:

Summary Protection Dashboard:

- Protected file uploads + trend
- Protected file downloads + trend
- Protected URL posts + trend
- Protected URL clicks + trend
- Threat intelligence events + trend
- Protected users + trend

Protected Content Analytics - Dashboard:

- Protected Users
- Active File Protection Users
- Active URL Protection Users
- File Uploads
- File Downloads
- File Events by Users
- File Content by Location
- File Content by File Type
- Threat Intelligence Events
- URL Posts
- URL Clicks
- URL Events by User
- URL by Location

URL per Category File Protection Details - Dashboard:

- File Protection Alerts by Severity
- File Threats Handled
- File Threats Handled by Location
- File Threats Handled by File Type
- File Threats Handled by User

Top File Threats (Infections) URL Protection Details - Dashboard:

- URL Protection Alerts by Severityv
- URL Threats Handled
- URL Threats Handled by Location
- URL Threats Handled by User
- Top URL Categories

WithSecure™ Cloud Protection also support custom reports via Salesforce Reports.

The following attributes are available in File Protection reports:

- **Created By:** Full Name, Created Date, Date/Time, File
- Extension, File Name, File Scan ID, File Size, File Type, IP Address
- **Last Modified By:** Full Name, Last Modified Date, Name, Owner: Full Name, Record ID, Scan Type, SHA1, Location
- **User:** Full Name, Verdict, Owner (First Name, Full Name, Last Name, Owner ID, Phone
- **Profile:** Name Rule: Name, Title, Username, Email, Alias, Active), Reason, File Prevalence, File Reputation Rating

The following attributes are available in URL Protection reports:

URL Scan: ID, **URL Scan:** Name, Action, Categories, Date/ Time, Direction, IP Address, Location, Reason, Reputation, Reputation Description, URL, User, Verdict, Owner Name, Owner Alias, Owner Role, Created By, Created Alias, Created Date, Last Modified By, Last Modified Alias, Last Modified Date

4.5.4 Administration

Solution administrator can enable or disable protection functionality and actions based on company security policies. For example, if strict compliance or secrecy requirements prevent uploading of files to the cloud for analysis, settings can be changed.

4.5.5 Deployment

WithSecure™ Cloud Protection is a combination of a native Salesforce application and the WithSecure™ Security Cloud, which provides reputation and security services used in other WithSecure™ and third party products. The solution is installed on the Salesforce platform and offers protection to all Salesforce clouds that your company uses like the Sales, Service or Community Cloud. No other software or network configuration changes are required.

Alternatively, you can deploy the solution as a connected app. A connected app is an application type that securely accesses and interacts with data and functionalities within the Salesforce platform by leveraging APIs. This solution type provides fortified scanning and threat analysis capabilities. We highly recommend creating a separate integration user to manage connected app integration.

4.5.6 Customization

WithSecure™ Cloud Protection allows Salesforc administrators to customize all end-user messages. It is possible to use a custom banner in scanning pages and customize the following messages:

- Harmful content found (Alert for administrators)
- Harmful content found on upload (Alert for internal users)
- Malicious file is replaced with a text file (File content)
- Harmful URL found (Alert for administrators)
- Harmful URL found on upload (Alert for internal users)
- Disallowed URL found (Alert for administrators)
- Disallowed URL found on upload (Alert for internal users)
- If file or URL scanning results changes from safe to unsafe (Alert for administrators)
- Disallowed content found (Alert for administrators)
- Disallowed content found on upload (Alert for internal users)

5. WithSecure™ Security Cloud

WithSecure™ Security Cloud is a cloud-based digital threat analysis system operated by WithSecure™. 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 default settings, Security Cloud does not collect IP addresses, files or other classified information. Customers can give WithSecure™ permission to store suspicious executables files and/or suspicious non-executables files.

By evaluating the combined metadata with information drawn from in-house databases and various other sources, the auto-mated 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 WithSecure™ Response 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 research 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	WithSecure™ Security Cloud employs multi-stage content analysis. File data is not sent to Security Cloud unless it is essential to providing protection and customer has allowed it.
Do not send personal data upstream	No information on who posts or accesses analyzed Files/URLs, or from where, is sent to WithSecure™ 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 can't 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 plaintext over the Internet. Encryption is, in addition, used to ensure the integrity of various objects. WithSecure™ 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 WithSecure™ 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 WithSecure™ personnel. All systems storing or testing malware are hosted by WithSecure™ corporate.
Controlled access	Only a limited number of WithSecure™ 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 WithSecure™ Security Cloud in our Security Cloud Whitepaper and Security Cloud Privacy Policy.

5.1 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. Threat Intelligence Service enables WithSecure™ Cloud Protection to query the reputation of objects like files and URLs. Files are verified by calculating the object's cryptographic hash SHA-1 and sending it to the reputation service.

5.2 Multi-Engine Anti-Virus

Multi-Engine Anti-Virus uses multiple security layers to detect exploits and unknown malware used in targeted attacks. The system combines behavior-al 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 Smart Cloud Sandbox for further processing.

5.3 Smart Cloud Sandbox

The Smart Cloud Sandbox runs suspect files in several virtual environments and analyzes file behavior. If the file behavior is determined to be suspicious, information is sent to the multi-engine anti-virus and threat intelligence service, where the next threat detection query will block the threat.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

W / T H™
secure