Solution overview

Part of WithSecure™ Elements
Extended Detection and Response (XDR)

WithSecure™ Elements **Collaboration Protection**

Advanced security for your Microsoft 365 environment

WITH secure

Contents

Last updated: September 2025
Information security classification: Public

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

Introduction

As more and more organizations rely on standard Microsoft 365 security, hackers and other malicious actors are incentivized to design attacks that bypass standard protection. WithSecure™ Elements Collaboration Protection detects and stops advanced threats in your Microsoft 365 (M365) environment. It fortifies Microsoft's native security capabilities against cyber attacks and malicious content across Microsoft 365, covering Exchange Online (email), SharePoint sites, OneDrive, and Teams.

The solution's advanced capabilities include detections for email forwarding rule anomalies and user credential compromise. The cloud-native product is a seamless extension of your Elements XDR security solutions. Elements Collaboration Protection is available as a standalone solution or as an integral capability in the modular WithSecure™ Elements Cloud cyber security platform.

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 also that customers using the cloud services are responsible for the security of their email. They are the owners of the data.

WithSecure™ Elements Collaboration Protection solution is also available as a fully managed service. WithSecure™ certified service providers can use Partner Managed or SaaS version of the solution to leverage many unique service provider features, like multi-company dashboard, reporting and subscription management. The SaaS version of the solution allows service providers to utilize flexible business models, e.g. Usage Based Invoicing for all the WithSecure™ Elements products.

Designed to protect your hybrid work environment

WithSecure™ Elements Collaboration Protection is favored by businesses that want:

- To minimize business disruption by mitigating email and collaboration risks from harmful content undetected by standard Microsoft 365 protection
- Cloud-to-cloud integration with easy deployment and seamless administration to ensure uninterrupted and efficient email threat protection.

Feature Highlights

WithSecure™ Elements Collaboration Protection provides security features that mitigate the risks posed by files and URLs shared using Microsoft 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. Similarly, whenever an end user stores or otherwise modifies a file stored on a SharePoint site*, the data is analyzed for harmful content.

The solution also provides rich reporting, advanced security analytics, and system events to ensure faster response to the identified potential threats. WithSecure™ Elements Collaboration Protection comprises a management portal for daily administration and a service backend that utilizes WithSecure's Security Cloud for analyzing the Microsoft 365 items for malicious files and URLs. In addition, the solution alerts if it detects that company email accounts have been compromised, giving IT admins precious time to react before the stolen credentials become available for broader criminal audiences.

WithSecure™ Elements Collaboration Protection delivers:

- **A cost-effective** solution to protect Microsoft 365 against phishing, ransomware, malicious files, internal email risks, malicious attachments and URLs
- **Cloud-to-cloud integration** with easy deployment and seamless administration to ensure uninterrupted and efficient email threat protection
- Combined with WithSecure'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 can.

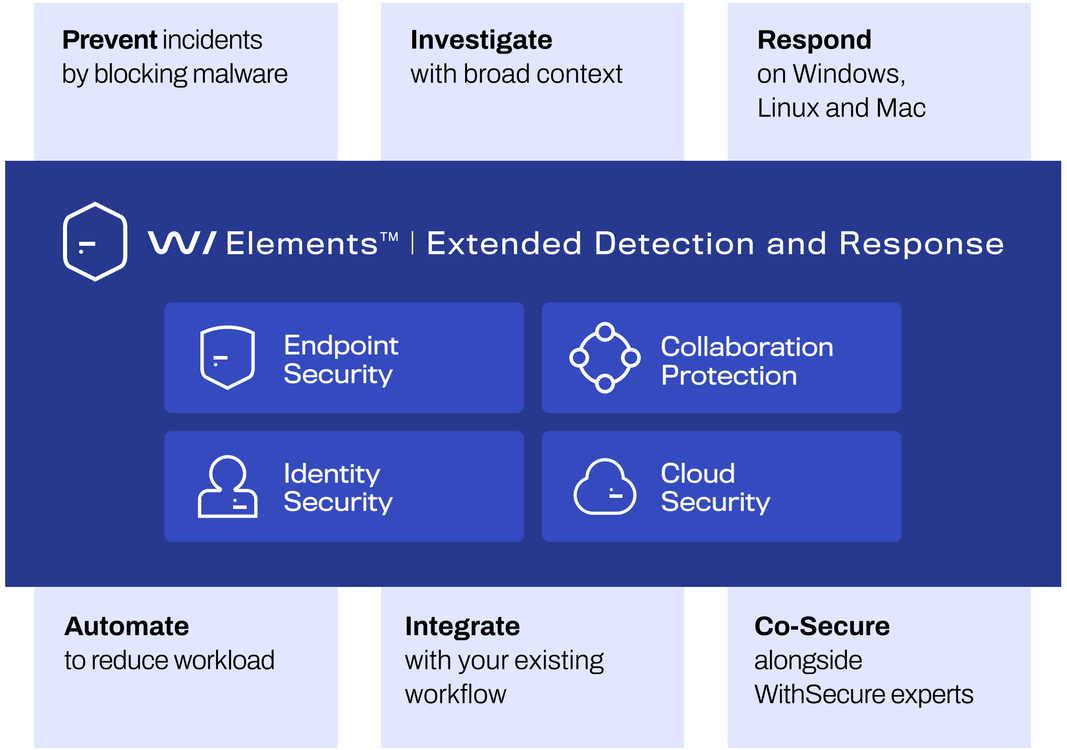
* SharePoint Embedded is currently not supported.

1. Part of WithSecure™ Elements XDR

WithSecure™ Elements Collaboration Protection is a module of WithSecure™ Elements Extended Detection and Response (XDR) that has been designed for modern IT estates. Not only does Elements XDR enable organizations to understand and respond to advanced threats across endpoints, identities, emails and collaboration tools, but its automated advanced preventative controls keep incident volumes and lower-level attacks at bay. Elements XDR enables you to recognize the entire attack chain that poses a threat to your business, extending beyond endpoints. Recognizing attacks early not only gives you a head start in reacting but can also save money by reducing the repercussions that follow from a compromised security posture.

Tap into the Power of WithSecure™ Elements Cloud

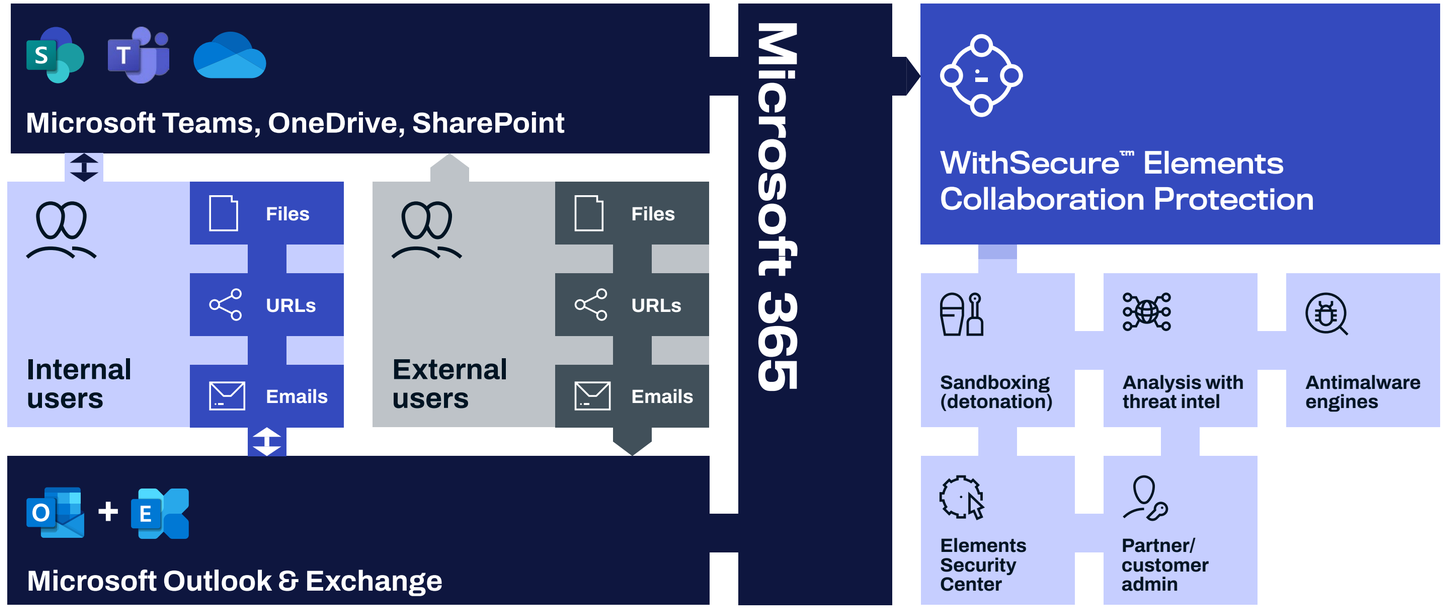
Elements XDR is part of our complete Elements Cloud platform that includes a wide range of tools and capabilities that are delivered from the cloud. Elements Cloud platform provides exposure management, automated patch management, dynamic threat intelligence and continuous behavioral analytics. Moreover, Elements Cloud allows you to manage all your security capabilities from a single, unified management portal – the Elements Security Center. Users of Elements Cloud can easily gain access to WithSecure's experts with our flexible Co-Security Services, so that you don't need to face cyber security challenges alone.



2. Solution overview

WithSecure™ Elements Collaboration Protection is a cloud-based security solution that is designed to mitigate business email and collaboration risks in organizations by providing effective threat protection. It secures your Exchange Online, Teams, OneDrive and SharePoint sites against ransomware, malicious files, internal email risks, malicious attachments and URLs. 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 gives you a high-level overview of the how the solution provides security for Microsoft 365.



Files, URLs, or emails
Elements Collaboration Protection processes data from Microsoft 365 user mailboxes, Teams, OneDrive and SharePoint sites to inspect and block malicious content. The analyses cover 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. In SharePoint, Microsoft Teams and OneDrive environments, the analysis covers data stored in selected OneDrive spaces and SharePoint and Teams sites.

WithSecure™ Security Cloud
WithSecure™ Security Cloud provides you with sandboxing, reputation threat intelligence, and antimalware engines. It 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.

WithSecure™ Elements Security Center
WithSecure™ Elements Security Center is the management portal for administrators to manage the solution in protecting Microsoft 365 content. The management portal consists of advanced analytics and system events functionality to help them prioritize the threats and mitigate the related security risks in time. Elements Security Center also provides dashboard and reporting capabilities to track and report on the status of the system at all times. The reports can be downloaded for easy sharing among stakeholders.

Partner/customer administrator
Elements Collaboration Protection relies on partner/customer administrators to work on the security detections and email notifications that result from the malicious content. The harmful content is found by analyzing the Microsoft 365 user mailboxes and files stored on SharePoint sites, OneDrive and Teams. The detections and notifications enable administrators to take action based on the severity of the alert and threat category of the content.

Management roles
The administrator of WithSecure™ Elements Collaboration Protection can be assigned a role based on their management needs within the portal. The service allows Admin, Quarantine Manager, and Read-only roles. Each role defines permissions that make certain portal management functionality accessible to the user. A user with the Admin role can add or remove users with different user roles by using Elements Security Center for user management.

Users
Internal and/or external users are the entities that use the WithSecure™ Elements Collaboration Protection solution while exchanging 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 among inbound, outbound, and internal traffic.

3.1. File protection

WithSecure™ Elements Collaboration Protection scans harmful contents within file attachments found in Exchange items, Teams, OneDrive, and SharePoint files. This enables the solution to protect you against viruses, trojans, ransomware, and other advanced malware. Elements Collaboration Protection offers superior protection compared to traditional technologies thanks to leveraging real-time threat intelligence gathered from tens of millions of security clients, thus providing faster and better protection against new and emerging threats.

3.1.1. Initial analysis

A call is made to the WithSecure™ backend with the checksum (SHA1) of the file attachments found in the Microsoft 365 Exchange items (email, calendar, appointments, sticky notes, etc.), Teams, OneDrive and SharePoint files. 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.

3.1.2. Threat intelligence check

If no results are found in the cache, a threat intelligence check is made via WithSecure'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. In SharePoint sites, Teams, and OneDrive, the files are placed to quarantine based on the Security Cloud's verdict.

3.1.3. Multi-engine antimalware

If the file reputation is unknown, the contents of the file are sent to WithSecure'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 WithSecure™ researchers.

3.1.4. 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.

3.1.5. 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, Teams chat, OneDrive, or SharePoint sites if it is deemed 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 location. The final verdict, file reputation, and other threat analysis details are stored in the threat detection cache for future use in the solution backend.

3.2. URL protection

URL protection is a key security function that proactively prevents Microsoft 365 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 WithSecure'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.

3.2.1. URL security check

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

3.3. Compromised account detection

Breach of user credentials is one of the biggest threat vectors for companies of all sizes. Access to user accounts often grants access to a wide range of company services and gives attackers an opportunity to steal company and customer data. Someone could log into any service you have access to—or even your computer if they can get access to it. In other words, a breached account is an easy way for the attacker to get into an organization. It is essentially like handing the attacker the keys to your house — so that they don't even have to see the effort to break in.

Moreover, if a user's email username and password are leaked, this could spread harm inside your organization like a wildfire, beyond just the one breached email account. For example, there could be further attacks done using a breached account, such as phishing campaigns or impersonation. These attacks are hard to detect because they use a legitimate company user account.

The compromised account detection feature detects compromised accounts as soon as information about the breach is available. It informs users and administrators of the account compromise, enabling them to take action to remediate the accounts by changing the password or by taking other security measures, such as turning on the multi-factor authentication to avoid further exploitation o the breached data.

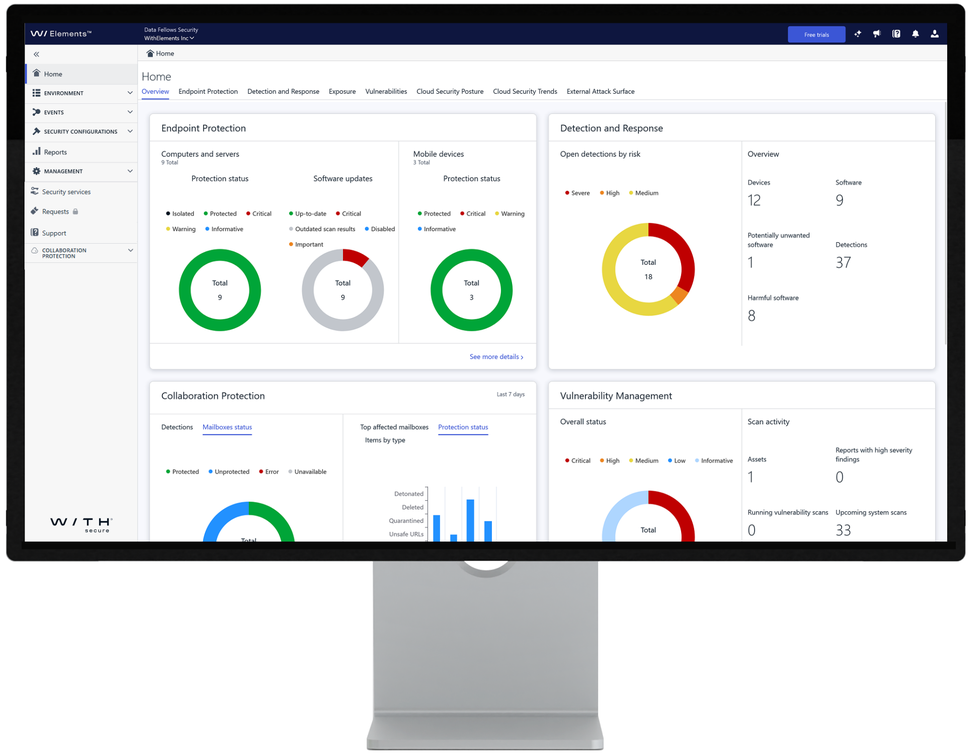
3.4. Inbox rule scanning

Inbox rules in Outlook work as a trigger to perform specific actions on incoming emails automatically. After gaining access to a mailbox, an attacker creates inbox rules to carry out different types of attacks, such as auto-forwarding and auto-deleting of emails. The scanning feature analyzes all the inbox rules in a mailbox. This analysis enables you to detect any suspicious rules that may indicate a compromise of the account. It also notifies the owner of the mailbox and the administrators to take action.

3.5. Management portal

WithSecure™ Elements Collaboration Protection provides a management portal for administrators to manage the Microsoft 365 Exchange, OneDrive, Teams and SharePoint environments.

Thanks to rich reporting, flexible alerting, advanced security analytics, and system events, responding to threats is easy for system administrators. Full, 360-degree visibility makes sure that you know your Microsoft 365 usage patterns. This is helpful when responding to an attack taking place through M365, investigating an attack coming from an unknown source, or in verifying whether M365 was part of an incident.



3.5.1. Deployment

Elements Collaboration Protection supports cloud-to-cloud integration without needing to install additional software or make 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, OneDrive, Teams, and SharePoint items. Administrators can configure the service for scanning the Microsoft 365 environment and provide comprehensive protection in just a few minutes.

3.5.2. Dashboard

The solution's management portal provides an easy-to-use dashboard for quick access to the most recent security detections of malicious content found in the managed environments. This includes the top affected mailboxes with the highest number of security detections, constantly up-to-date data about the 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 number of mailboxes, Teams channels, OneDrive users and SharePoint sites protected, or 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 Microsoft 365 services.

3.5.3. Security detections

The security detections widget provides quick and easy access to the most recent security detections 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.

3.5.4. Mailbox status

The mailbox status widget on the dashboard provides a count of protected vs unprotected mailboxes in Microsoft 365 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.

3.5.5. Top targeted mailboxes

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

3.5.6. Protection status

The protection status widget shows the total number 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.

3.5.7. 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. If there is a sudden increase in unsafe content, this might be related to a possible security incident in the organization.

3.5.8. Analytics

WithSecure™ Elements Collaboration Protection gives full, 360-degree visibility into your Microsoft 365 usage. All security detections 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 Microsoft 365 Exchange items. That knowledge is often helpful, as IT administrators may, for example, find malicious files or URLs that should not be shared via Microsoft 365.

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.

3.5.9. Policy administration

WithSecure™ Elements Collaboration Protection provides policies to define the security settings for the analyzed contents in Microsoft 365 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 WithSecure™ default policy to provide maximum protection from the get-go when configuring the tenants. Alternatively, they can copy the default policy and modify the security settings according to their organization's security requirements and make that the default policy, which is then assigned by default whenever a tenant is configured for protection.

3.5.10. Quarantine management

WithSecure™ Elements Collaboration Protection allows administrators to quarantine Exchange, OneDrive and SharePoint items based on the harmfulness of the file(s) or URL(s) 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.

3.5.11. Detections Management

Any alert generating system is usable only if it provides a good workflow for the administrators managing the alerts. With Elements Collaboration Protection, the administrators can manage the detections by filtering, changing alert lifecycle status, and by adding comments. Detections management is especially useful when working in multi-admin organizations where the work needs to be distributed and tracked.

3.5.12. Reporting

WithSecure™ Elements Collaboration Protection provides rich reporting capabilities, enabling administrators to report on the security status of the protected environment at any time in an easy-to-share 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.

4. WithSecure™ Security Cloud

WithSecure's 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. We collect only the minimum amount of client data necessary to provide our services.

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 the Security Cloud.

Security Cloud also allows WithSecure™ 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.

More information about WithSecure's Security Cloud:
WithSecure™ Security Cloud Whitepaper

More information about WithSecure's privacy policies:
WithSecure's Privacy Policy

4.1. 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 WithSecure™ Elements Collaboration 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.

4.2. 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, heuristics and machine learning detection capabilities, which allows 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.

4.3. 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.

5. Overview of WithSecure™ Elements Cloud Platform

Reduce cyber risk, complexity and inefficiency with our Elements Cloud platform. WithSecure™ Elements Collaboration Protection is available as an integral capability in the modular WithSecure™ Elements cyber security platform.

WithSecure Elements provides customers with complete protection in one unified platform and easy-to-use security center. The centralized platform combines powerful predictive, preventive, and responsive security capabilities into intelligent protection against threats from ransomware to targeted attacks. Our unparalleled simplicity lets customers focus on what is the most valuable to them.

Modular product packages and flexible pricing models give customers the freedom to evolve. WithSecure™ Elements can be part of the customer's eco-system. It can easily be connected with their SIEM, SOAR, security management, monitoring or reporting systems.

Try Elements today

Contact our sales for advanced protection beyond standard Microsoft 365 security.

Contact sales

Who We Are

WithSecure™, formerly F-Secure Business, is Europe's cyber security partner of choice. Trusted by IT service providers, MSSPs, and businesses worldwide, we deliver outcome-based cyber security solutions that protect mid-market companies.

Committed to the European Way of data protection, WithSecure™ prioritizes privacy, data sovereignty, and regulatory compliance.

Boasting more than 35 years of industry experience, WithSecure™ has designed its portfolio to navigate the paradigm shift from reactive to proactive cyber security. In alignment with its commitment to collaborative growth, WithSecure™ offers partners flexible commercial models, ensuring mutual success across the dynamic cyber security landscape.

Central to WithSecure's cutting-edge offering is Elements Cloud, which seamlessly integrates AI-powered technologies, human expertise, and co-security services. Further, it empowers mid-market customers with modular capabilities spanning endpoint and cloud protection, threat detection and response, and exposure management.

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

WITH secure™