WithSecure™ Elements Privacy Policy

October 2024

PUBLIC

Contents

1 In Brief

WithSecure™ Elements is a single modular cyber security solution. It is made up of a full range of cyber security applications, including vulnerability management, patch management, endpoint protection, and endpoint detection and response technologies.

WithSecure™ Elements consist of modular cyber security solutions (collectively the “WithSecure Elements Product Family”), namely:

- Elements Collaboration Protection.
- Elements Endpoint Detection and Response.
- Elements Endpoint Protection.
- Elements Exposure Management.
- Elements Identity Security.
- Elements Mobile Protection.
- Elements Vulnerability Management.

The above listed solutions may be provided separately or jointly, and this privacy policy describes the data collected by the WithSecure Elements Product Family and is to be read in conjunction with the WithSecure General Privacy Policy available here: Corporate privacy | WithSecure™ .

This privacy policy focuses on the items we believe are the most relevant for you. Such items are in particular:

- the type of personal and private data that the service collects,
- what we use it for,
- our justification,
- typical disclosures, and
- for how long we store it.

More information on such topics as well as on other aspects (data subject rights, contact information, etc.) of the processing of your personal data is also available via the embedded links on this page.

This privacy policy is given by WithSecure Corporation, a Finnish publicly listed corporation with Business ID 0705579-2 ("WithSecure", "we", "our"). All our relevant subsidiaries also apply this policy.

2 Elements Collaboration Protection

WithSecure Elements Collaboration Protection is a cloud-based security solution that is designed to mitigate business email risks in organizations by providing effective threat protection for email messages and file exchange of selected cloud services (such as Microsoft 365). The solution provides effective threat protection against internal email threats, advanced phishing attacks, and malicious content and URLs. In addition to email messages, the solution protects different types of content,

including cloud service specific content, such as tasks, calendar appointments, contacts, and sticky notes, against malicious content and URLs.

- The focus of data collection is on finding malicious content in users' mailboxes and not on any personal information about individuals.
- Much of the processed and collected data remains in the customer company's selected tenant.

2.1 What kind of data is collected

2.1.1 Security data

Elements Collaboration Protection processes content such as email messages, calendar appointments, tasks, contacts, and groups in selected mailboxes of customer employees, which are defined in the security policy and have a valid license assigned.

While processing this data, the solution analyzes files, web links (URLs) included in message bodies, and some parts of message headers. To identify security threats, files and URLs are sent to WithSecure's Security Cloud for reputation checks and advanced threat analysis.

Please see section 11 (“Security Cloud”) below for more information about the Security Cloud.

If harmful content is detected (such as a malicious attachment or URL), the solution moves or copies the entire object or affected parts to the hidden quarantine folder located in the customer's selected tenant. The relevant properties of quarantined items such as user mailbox, sender and recipient addresses, item subject, folder name, and harmful attachment name and URL are saved in the quarantine database.

For data the service collects on administrator users, which is available through the management portal, please see section 8 (“Data on Portal Users”) below.

Of the data collected by the scanning activity, the results are made available to the users administering the solution via the WithSecure Elements Collaboration Protection portal. The results may include:

- name of the user mailbox where the message or item with harmful content was found
- email address of the sender (messaging metadata)
- email addresses of recipients (messaging metadata)
- subject of message or item (messaging metadata)
- email message headers (messaging metadata)
- name of the folder where harmful content was found (messaging metadata)
- names of the files where harmful content was found
- web links (URLs) found to be harmful

WithSecure processes the data to protect the target networks, the devices and data therein. In particular:

- to block real or potentially harmful content in inbound, outbound, and internal email traffic
- to detect malicious and suspicious activity in users' mailboxes
- to detect other threats and security attacks against or via selected cloud services (such as Microsoft 365)

- to analyze the service and security data collected for the purposes of improving the detection capability of WithSecure services, with emphasis on improving the functionality, usability, and detection capability of this service

The WithSecure Elements Collaboration Protection portal collects non-identifiable telemetry data on the use of its features for service improvement purposes, which the administrator can choose to opt out from sending in the policy settings.

WithSecure checks your email address on a regular basis for data breaches. WithSecure engages a third-party provider for detecting and collecting information on data breaches that relate to the email address that WithSecure checks for you.

The data processing undertaken by the Service is necessary for the efficient protection of customer company data in its cloud service organization (such as Microsoft 365). While the individual service's settings may enable an IT administrator to limit the processing of security data by WithSecure, such adjustments are not recommended, as they endanger achieving the intended purposes of the Services.

3 Elements EDR and EPP

WithSecure Elements Endpoint Detection and Response (EDR) and WithSecure Elements Endpoint Protection (EPP) services are often used in conjunction with each other. We have combined the EDR and EPP specific wording into one section in this privacy policy for convenience.

You can still subscribe to either service separately, however if you extend the EPP service with the EDR module the wording in this privacy policy pertaining to the EDR service will prevail if it is in conflict or inconsistent with the wording pertaining to the EPP service.

3.1 General privacy considerations

Both EDR and EPP form a part of security measures that protect valuable data (such as employee information, trade secrets, business plans) residing in the customer devices and network. WithSecure's processing of data collected by EDR and EPP is bound to the purpose of providing information security services of constantly evolving capabilities to its customers.

3.1.1 WithSecure Elements Endpoint Protection

Our EPP combines device management, software update management as well as workstation and server security, which are all controlled via the management portal.

The core privacy aspects of the EPP service are:

- the focus of data collection is on your device and our service, not you as an individual;

- all of the collected data is available for your employer's IT administrator, so they can better manage company devices and applications and react to threats efficiently;
- we collect anonymous security data to protect your device.

The EPP service does not enable WithSecure or your company's IT administrator to follow your movements, view your photos, or see who you call or communicate with, nor are we able to track the sites that you visit through the service. The company's IT administrator can enable features in the EPP service that when turned on prevent the user from accessing websites deemed as harmful or blocked for compliance reasons. In such cases the alert in the portal visible to the company's IT administrator will include information on the domain that was blocked.

3.1.2 WithSecure Elements Endpoint Detection and Response

The EDR is a security solution specifically designed to detect technical information security anomalies and advanced attacks using methods beyond the reach of more traditional antivirus solutions.

EDR consists of a number of sensors placed within customers' networks, a backend run by WithSecure, and a service portal that operates as the communication venue between WithSecure, our corporate end user ("customers"), and the reseller partner.

These EDR sensors are only installed on the customer network on devices designated by the customer or IT admin managing the company's assets to detect and preserve evidence about security anomalies in the customer's network. These sensors gather event logs and record relevant aspects of device usage. The data is sent from the EDR sensor to WithSecure for analysis.

Through EDR, the customer gains additional visibility to their own network. Such visibility enables spotting and investigating signs of ongoing and past attacks and attempts to breach security controls.

The core aspects of the EDR service are:

- the focus of the data collection is not on an individual employee, business document or email contents;
- the focus of the data processing is on detecting technical security anomalies in customer devices and networks;
- the solution is not intended for monitoring non-security-related activities such as profiling employees' activities, interests or interactions.

All data collection and handling in the context of EDR is aimed at supporting the detection and subsequent investigation of security breaches and attempts to circumvent the technical security controls of the customer's technical infrastructure and other assets.

3.2 What kind of data is collected

For data the service collects on administrator users, which is available through the management portal, please see section 8 ("Data on Portal Users") below.

3.2.1 Data on other users in the management portal

3.2.1.1 EPP data in management portal

Depending on the software that you have a subscription for and its configuration, the EPP service may collect the following data about you, your device, and use of the service, and makes it available through the management portal:

- User's name, user's email address, device name, and device identifiers (e.g. UUID, UPN, WINS name, IP address) that act as identifiers for the user data in the system.
- The service version number, subscription key, installation and update date and time, blocked malware (may include the file name and path), blocked applications, blocked USB devices, device operating system and version, feature status.
- Installed applications as part of the service offering.
- Connected USB devices as part of the device control feature.
- Various data on operating system, user and application configuration (e.g. encryption state, user privileges, password policies, etc.) describing the security posture and usage of the company devices for better manageability.
- Mobile device model and configuration when related to security or compliancy, as well as the potential jailbreak or root status, service statistics per device such as the harmful sites, the number of blocked tracking attempts and blocked website counters.
- Customer credentials (e.g. Bitlocker recovery key, if configured to do so).
- Other substantially similar data.

The collected data varies according to what devices and services you use.

This data is visible to your company's IT administrator for similar purposes. The data is also available to WithSecure and through the portal. If the company's IT administration has been outsourced, the data is also available to the outsourcing partner (WithSecure's 'distributor partner'), so that they can provide your company with support and corresponding IT services.

3.2.1.2 Use of collected data in EPP

The collected data is used to carry out the following functions:

- to operate the services,
- to manage the services (including identifying authorized users, managing licenses, and sending push notifications),
- to measure performance, and
- to further develop, enhance, and improve the service.

The data can be used to provide support and problem resolution services.

3.2.1.3 Other data collected by EPP

In addition to data that is made available in the portal WithSecure also collects the following data directly via the EPP service. This data is not shared with the customer company or distribution partner.

- Your device's language, so the Service language is consistent with the device language; and

- ***For mobile clients***, internal memory and SD card memory sizes, and a list of installed applications.

This data is used for operating the service, troubleshooting, performance measurement, statistics, and service development.

WithSecure and the reseller partner may also each initiate a collection of additional diagnostic data from the protected device, where it is necessary to resolve a support case. By default, you will be prompted prior to sending the diagnostic data to WithSecure, however your IT administrator can switch this prompt feature off. More information on related data collection is available in the WithSecure Support Tool privacy policy.

3.2.1.4 Data collection for mobile devices in EPP

Our guiding principle is that we do not seek to spy on the exact content of your private communications. We validate URLs before they are loaded to provide you the service and to keep your data transfers clean. To be more exact we analyze the traffic for suspicious or malicious files and destinations (i.e. URLs).

3.2.1.5 Automated data collection in EDR

The EDR sensors collect the following kinds of event-based data ("Event Data"):

- technical user identifiers;
- domain names and network connections;
- metadata of process creation, behavior, and access to various systems / subsystems;
- system log entries relevant to detecting security breaches;
- data that matches known attack patterns that trigger detection rules and other known indicators of compromise;
- unwanted behavior which could be a security risk to the company (e.g. authenticating to a server with weak authentication protocol); and
- other substantially similar device and service data.

Events are timestamped, and annotated in a fashion to enable automation to identify the user and device under which the events took place.

Data sent to the service backend on an ongoing basis is filtered both to minimize the amount of data traffic and to protect the privacy of the customer's employees.

Application metadata. The EDR solution also collects information on applications present on endpoints where the sensor is installed, as well as system/network information and other metrics from such EDR sensors (“Application Metadata”). Application Metadata does not include Event Data.

Portal data. In the EDR service the portal collects non-identifiable telemetry data on the use of its features for service improvement purposes.

3.2.1.6 Use of automatically collected data in EDR

The collected data is used to carry out the following functions:

- To provide effective security anomaly detection;
- To service performance monitoring and direct troubleshooting efforts;
- To further develop and enhance the service functionality and WithSecure's overall detection capability to respond to threats;
- To network health status measurement; and
- To provide customers with visibility about the applications and activity in their network.

3.2.1.7 Manual data collection in EDR

Through EDR, customers gain the capability to retrieve additional data to fully investigate or confirm a suspected security incident which was identified from automatically collected data. EDR sensors provide several data collection features which can be manually invoked by the customer:

- Map File System – retrieving the names and properties, for example, the size of all files and foldersin a particular disk location;
- File/Folder Retrieval – retrieving the full contents of a particular file or folder;
- Map Registry – retrieving the keys and values from a particular location in the Windows Registry;
- Registry Hive Retrieval – retrieving an entire Hive from the Windows Registry;
- Process Memory Image Retrieval – retrieving a full copy of the memory from a particular process;
- Full SystemMemory Image Retrieval–retrieving a full copy of the entire system memory space for a particular device;
- Process Enumeration – retrieving a list of all running processes;
- Service Enumeration – retrieving a list of all Operating System services;
- Scheduled Task Enumeration – retrieving a list of all Operating System scheduled tasks;
- Windows Event Log Retrieval – retrieving some or all contents of a Windows device’s event logs;
- Master File Table (MFT) Retrieval – retrieving the MFT from Windows devices;
- Master Boot Record (MBR) Retrieval – retrieving the MBR from Windows devices;
- Network Connection Enumeration – retrieving an enumeration of all open network connections.

3.2.1.8 Use of manually collected data in EDR

These data collection capabilities are to be used only when required in the following situations:

- To investigate a security incident;
- To identify security risks that cannot be identified from automatically collected data.

The data is sent from the EDR sensor to a backend run by WithSecure to be made available for our customers.

4 Elements Exposure Management

WithSecure Elements Exposure Management (XM) is a continuous and proactive solution designed to predict and prevent breaches against your company's assets and business operations. XM provides visibility into your company's attack surface and enables the efficient remediation of its highest-impact exposures through a unified view.

In addition to the general sections applicable to the WithSecure Elements Product Family, the data collected in XM is described in more detail in the following sections.

Elements XM also collects the following data on the users:

- Users' name and email address;
- Information on credentials;
- Status of the MFA;
- Date of last password change.

Elements Vulnerability Management. XM for User contains the data processing of Elements Vulnerability Management. See more details in section 7 below.

Exposure Management for Cloud (formerly known as Cloud Security Posture Management). See more details on data processing in section 4.1 below.

Attack Surface Management. The XM solution may process contact email, name, phone number and address information, if any.

4.1 Exposure Management for Cloud

XM for Cloud is a vulnerability and misconfiguration scanning and management capability that allows you to identify and manage threats, report risks, and get an outlook on the security posture of your cloud infrastructure accounts. The core privacy aspects of this service are:

- the focus of data collection is on detecting vulnerabilities and misconfigurations in your employer's cloud account, not on any individual's activities therein;
- the only directly identifying data that we need is your name, email, and optionally phone number;
- we monitor service use to maintain its performance and prevent misuse.

The service is built to find vulnerabilities and misconfigurations in your employer's cloud infrastructure account, enabling you to find and fix them and thus prevent breaches performed by malicious parties.

It can be subscribed either alone or with XM for User. Having both will enable attack path simulation taking into account threats between the cloud and other asset types.

4.1.1 What kind of data is collected by XM for Cloud

4.1.2 Data in the management portal

For data the service collects on administrator users, which is available through the management portal, please see section 8 (“Data on Portal Users”) below.

The service automatically collects the following data on its operational environment, and on the use of the service, and makes it available through the management portal:

- **Data on service use.** Subscriber access tokens, scan node, device identifiers (including IP address), EntraID (users, user groups, user devices, roles), service version number, subscription key, installation and update date and time, feature status, and basic operating system status (such as memory and disk usage).
- **Data on vulnerability and misconfiguration scan results.** Information about the occurrence of known security issues and risks identified during the scan as presented to you via the service.

The portal provides limited visibility among those who share the same subscription.

4.1.3 Data in WithSecure systems

In addition to vulnerability scan result data that is made available to you via the service, WithSecure also collects the following organization-level data directly via the service. This data is not shared with the customer company or distribution partner.

- The customer ID and name;
- the customer’s cloud account ID (and possible nick name);
- metadata related to scanned assets;
- the amount and the value of unique cloud assets scanned for misconfigurations and vulnerabilities within a cloud account / organization; and

This data is used for operating the service, troubleshooting, performance measurement, statistics, logging and resolving malicious usage, and service development.

4.2 Exposure Management for User

XM for user subscription includes a vulnerability and misconfiguration scanning and management capability that allows you to identify and manage threats, report risks, and get an outlook on the security posture of your devices (VM), Identity (EntraID) and External Attack Surface.

The service is built to find vulnerabilities and misconfigurations in your employer's environment, enabling you to find and fix them and thus prevent breaches performed by malicious parties.

It can be subscribed either alone or with XM for Cloud. Having both will enable attack path simulation taking into account threats between the cloud and other asset types.

4.2.1 What kind of data is collected by XM for User

4.2.2 Data in the management portal

For data the service collects on administrator users, which is available through the management portal, please see section 8 (“Data on Portal Users”) below.

The service automatically collects the following data on its operational environment, and on the use of the service, and makes it available through the management portal:

- **Data on service use.** Subscriber access tokens, scan node, device identifiers (including IP address), EntraID (users, user groups, user devices, roles), service version number, subscription key, installation and update date and time, feature status, and basic operating system status (such as memory and disk usage).
- **Data on vulnerability and misconfiguration scan results.** Information about the occurrence of known security issues and risks identified during the scan as presented to you via the service.

The portal provides limited visibility among those who share the same subscription.

4.2.3 Data in WithSecure systems

In addition to vulnerability scan result data that is made available to you via the service, WithSecure also collects the following organization-level data directly via the service. This data is not shared with the customer company or distribution partner.

- The customer ID and name;
- the customer’s cloud account ID (and possible nick name);
- metadata related to scanned assets;
- the amount and the value of unique cloud assets scanned for misconfigurations and vulnerabilities within a cloud account / organization; and

This data is used for operating the service, troubleshooting, performance measurement, statistics, logging and resolving malicious usage, and service development.

5 Elements Identity Security

WithSecure Elements Identity Security is a module within Elements XDR designed to detect and respond to identity-based threats. It accomplishes this by alerting you to potentially compromised users and providing insights into malicious activity and appropriate responses. The integration with Entra ID allows collection of the following data:

- Sign-in logs: These logs identify risky sign-ins when users log into the Microsoft 365 environment or third-party applications using Entra ID for single sign-on.
- Audit logs: Captured to detect actions after the initial access step in the attack lifecycle.
- Non-interactive sign-in logs: These relate to system activities where there is no human interaction. This is crucial because Entra ID service accounts can be targeted by attackers.

The purpose of this service is to swiftly detect suspicious activity, preventing the impact of cyber attacks such as data breaches or financial losses. Importantly, it is not intended for employee monitoring. WithSecure does not allow your company's IT administrator to track your movements, view your photos, or monitor your communication.

5.1 What kind of data is collected

Our guiding principle is that we do not aim to spy on the specific content of your private communications. Instead, we analyze metadata from logins, allowing us to observe Entra ID tenant management actions. For instance, we can track activities such as signing in from new countries, adding new users, granting permissions, or creating application principals.

We do collect events from the Entra ID Tenant. These events typically include access time, associated usernames, device types, applications used, whether multi-factor authentication was employed, and the IP address along with its associated location information.

6 Elements Mobile Protection

WithSecure Elements Mobile Protection combines our Network Gateway solution (detects and blocks malicious network requests) and malware protection with mobile device management, which are both controlled via the management portal. To achieve this:

- the focus of data collection is on your device and our service, not you as an individual;
- results of the query will be available for your employer's IT administrator, so they can better manage company devices and applications.

The purpose of the service is to secure and manage your device and its connections. The service is not built to monitor employees. The service does not enable WithSecure or your company's IT administrator to follow your movements, view your photos, or see who you call or communicate with.

The URL requests, for example, are evaluated based on their reputation and harmful websites are blocked based on the settings controlled by your employer's IT administrator. If you would like more information on allowed-listed or blocked websites, please contact your employer's IT administrator.

6.1 What kind of data is collected

Our guiding principle is that we do not seek to spy on the exact content of your private communications. We only analyze the URL request to provide you the Service and to keep your data transfers clean. To be more exact, this means that:

- the solution automatically analyzes suspicious or malicious requests; and
- the solution automatically inhibits usage that is against your company's acceptable use policy.

Securing your device with Security Cloud. The service sends queries on potential malicious activity, malicious software, or unwanted applications on protected devices, URL requests to WithSecure Security Cloud. WithSecure Security Cloud is a cloud-based system for cyber threat analysis that is

operated by WithSecure. With the Security Cloud, WithSecure can maintain an up-to-date overview of the global threat landscape and protect our customers against new threats the moment they are first found. These queries — such as URLs, file identifiers, and application metadata — cannot be connected to an identifiable user by WithSecure.

To protect your privacy, WithSecure separates the above security data from other data collected on your use of the service, anonymizes it, and destroys it when it is no longer needed for the purpose.

6.1.1 User data

6.1.1.1 User data in the management portal

For data the service collects on administrator users, which is available through the management portal, please see section 8 (“Data on Portal Users”) below.

The Service collects the following data about you, your device, and use of the Service, and makes it available through the management portal:

- User’s email, first name, family name, and alias. This data is linked to your "device UUID" that acts as an identifier of the user data in the system.
- The service version number, device identifiers (e.g. UUID, model, etc.), subscription key, installation and update date and time, operating system and version, feature status.
- In addition to the above, the service may collect other information from the devices related to security and compliancy, such as: your mobile device model, as well as the potential jailbreak or root status, service statistics per device such as the amount of traffic scanned, the harmful sites, the number of blocked tracking attempts and blocked website counters.

The collected data varies according to what devices and services you use.

By default, the blocked URLs are not sent to the management portal, but this setting can be enabled by your employer’s IT administrator.

We use this data to operate the services, to manage them (including identifying authorized users and managing licenses), to measure performance, and to further develop, enhance, and improve the service. The data can be used to provide support and problem resolution services.

This data is visible to your company's IT administrator and is also available to WithSecure and through the portal. If the company's IT administration has been outsourced, the data is also available to the outsourcing partner (WithSecure's 'distributor partner'), so that they can provide your company with support and IT services.

6.1.1.2 User data in WithSecure systems

In addition to data that is made available in the portal, WithSecure also collects the following data via the Service:

- your device ID, so we can send push notifications to the devices and to combine different types of user data;

- your device's language, so the service language is consistent with the device language; and
- we may also collect the battery level, internal memory and SD card memory sizes, and a list of installed applications (to check that the service is installed correctly) for management feature development purposes.

6.1.1.3 Analytics data

We also reuse the above service data and security data for data analytics purposes, based on the legal grounds established above. Data analytics are an integral part of our service delivery, as nearly all WithSecure services are dependent on our infrastructure to properly operate. Our data analytics enables us to direct that infrastructure to support your use of the services.

7 Elements Vulnerability Management

WithSecure Elements Vulnerability Management is a vulnerability scanning and management platform that allows you to identify and manage threats, report risks, and get an outlook on the security posture of your IT systems. The core privacy aspects of this service are:

- the focus of data collection is on detecting vulnerabilities in your employer's corporate network, not on any individual's activities therein;
- the only directly identifying data that we need is your name, email, and optionally phone number;
- we monitor service use to maintain its performance and prevent misuse.

The service is built to find vulnerabilities in the hardware and software of your employer's corporate network, enabling you to find and fix them and thus prevent breaches performed by malicious parties.

7.1 What kind of data is collected

7.1.1 Data in the management portal

For data the service collects on administrator users, which is available through the management portal, please see section 8 (“Data on Portal Users”) below.

The service automatically collects the following data on its operational environment, and on the use of the service, and makes it available through the management portal:

- **Data on service use.** Subscriber access tokens, scan node, device identifiers (including IP address), service version number, subscription key, installation and update date and time, feature status, and basic operating system status (such as memory and disk usage).
- **Data on vulnerability scan results.** Information about the occurrence of known vulnerabilities and risks identified during the scan as presented to you via the service.
- for authenticated Elements Vulnerability Management system scans:
    - The certificate or credentials that act as access tokens to perform an in-depth scan;
    - The software and its version installed on target systems

The portal provides limited visibility among those who share the same subscription.

7.1.2 Data in WithSecure systems

In addition to vulnerability scan result data that is made available to you via the service, WithSecure also collects the following organization-level data directly via the service. This data is not shared with the customer company or distribution partner.

- The amount and the value of unique IP addresses scanned for vulnerabilities within organization; and
- in the case of on-premise scan node deployments, the scan node's configuration details, such as installation directory and hardware fingerprint of the device on which the scan node agent is installed.

This data is used for operating the service, troubleshooting, performance measurement, statistics, logging and resolving malicious usage, and service development.

8 Data on Portal Users

8.1 What kind of data is collected

The service collects the following data, which is available through the management portal, on administrator users:

- Username of the user logged onto the managed device
- The user's email address
- The user's phone number (optional)
- Logs of the user's actions visible in the portal in the audit log

8.2 Use of collected data

Data on access and actions performed by administrators in the management portal is collected for audit purposes. Generally, this is limited to changes performed or access to sensitive data (for example downloading endpoint diagnostic files). This data is visible to administrators in the portals audit log.

9 Analytics

In addition to the data visualized in the portal, the service also uses a subset of collected data for service analytics. We do this so that we can create services that are of value to you and our other customers. WithSecure also collects analytics data on the service portal to learn how the administrator users use the service portal so we can improve the portal user experience.

This section outlines our general practices for the collection and processing of data for analytics purposes.

When speaking about WithSecure data analytics, it comprises both reused service data, reused security data, and the data that is collected for analytics purposes to begin with.

We want to give you a more personal customer experience and provide you with even better services in the future. For that we need to track usage patterns and create customer segments. For example, what features are used most, where the service fails, what needs fixing, and how you found out about our services.

What we collect. The data that we process for the purposes of data analytics include things like asset identifier and relations between devices / users / user groups, operation environment, service operation time, license type (trial or paid version), device metrics (such as phone model and operating system, language), partial IP address, service errors, problematic files and URLs, service performance data, how you interact with our services (such as which features are used and how often), the domain name from which you connect to the service, elements clicked, timestamps, regional location, effectiveness of our in-service messaging, service activation (such as tracking that you have received the related messages and that installation was successful), installation and activation paths, service performance, connections, data routing, quota, and other similar data.

On a practical level, when we ask for your consent in our services' user interface, it controls whether the following data is sent: i) additional data, like which features are used and how often, and service metrics, and ii) the number of attributes sent in a given data set.
The above relates to your use of our cyber security services. Data analytics running on our websites are described in our website privacy policy.

Opting out. We really appreciate your help in improving our services. However, if you want to minimize all data traffic towards WithSecure, we respect that. Those of our services that employ additional analytics give you the choice on whether to contribute. You can opt out at any time from the subsequent collection of analytical data that is non-essential to our service provisioning.

If you have opted out from all analytics data collection, our messaging directed to you will be based only on the service data collection (the data that we collect in any case to provide you with the services) and some of our messaging is likely to be less relevant.

If you oppose all collection of data from your online life (including our websites), the more wholesale method for preventing online advertisers from profiling your mobile device usage is to reset the advertising identifier from time to time and to turn on the do-not-track setting in your device settings, or to use our privacy product.

Analytics data retention. In our data analytics activities, we combine analytics data with the service data. The resulting combined data set then continues to be processed based on a "legitimate interest". The previously collected analytical data is retained as part of the service statistics, as its retroactive removal would break the statistics. When you cease subscribing to our services (i.e. your account is deleted), the analytical data related to your service use will be reverted to anonymous data, and we are no longer able to associate it with you.

Data exchange. Because of the technical environment (that is, the internet, the app store ecosystem, and social media), we are not able to do all of the collection and activities related to data analytics ourselves. We have to exchange some data (such as “Android marketing identifier” and other like identifiers) with our online analytics and marketing partners to enable our digital analytics and marketing activities. The vast majority of the data that we have on you is not shared with others.

Some of our subcontractors who provide us with analytical capabilities for our products may also create and publish aggregate reports on the data that they have collected. In such cases, the statistics and aggregate reports do not contain any data that could be linked to any individual person.

We do not sacrifice your privacy. Where we differ from most companies doing this is in that we understand how the ecosystem works and go through great pains to select our few partners with care, removing all data that is not absolutely necessary for the above purpose. You can naturally opt out from the collection of analytics data at any time via the service settings.

When we process the data for analytical or statistical purposes, we pseudonymize the data. In other words, our data analysts do not know the individual to which a specific data set refers to. The pseudonymization is only reversed in specified use cases. For example, when we communicate with you, we connect the results — not the full data — of our data analytics to your email address. Another example is that we may use the data to resolve issues you may have with our product, when providing you with technical support services.

We also limit such added analytics only to the surface of our services and keep them at arm’s length from the core privacy areas of our services. For example, we do not have any external analytics in our Security Cloud.

10 Luminen™ and use of GenAI

WithSecure Luminen™ is a layer of user experience of Elements that is utilizing Generative AI algorithms / Large Language Models in order to provide a natural language and localized assistance to our users. Naturally, the use of LLM raises questions about privacy and the use of the data.

We use LLMs as provided by Amazon AWS Bedrock service and our users’ data does not leave AWS. The introduction of Luminen does not change anything compared to the rest of Elements' functionality. All data is processed in AWS in Europe. Data of our users is not and will not be used to train future versions of foundational models. We never query models outside of AWS with our users’ data. Any possible training of non-foundational models by WithSecure will only use anonymized data.

To limit the risk of leakage and hallucination, we use a common LLM technique known as Retrieval-Augmented Generation – RAG and provide the model with a specific prompt along with specific context data – which is pre-computed for a specific need. The user cannot define or modify the prompt, and the model cannot freely query for data across Elements.

The data that is made available to the LLM, as part of the context consists of Security Events, XDR/BCD incidents and relevant threat intelligence data. This data can contain information like username, workstation name, email address (in case of ECP Security Event). However, Luminen™ does not have access to any additional data, which would not be already in Security Events or XDR/BCD incidents.

11 Security Cloud

11.1 General

The WithSecure Security Cloud is a cloud-based system for cyber threat analysis, designed, developed, and operated by WithSecure Corporation. With the Security Cloud, we can maintain an up-to-date overview of the global threat landscape and protect our customers against new threats the moment they are first found. For more information, please read our Security Cloud whitepaper.

11.2 Solution-specific use

11.2.1 Elements Endpoint Protection

The service sends queries on potential malicious activities or protected devices and networks to WithSecure Security Cloud. While we limit the processing of any information that could be considered sensitive by our users, we collect the minimum amount of user and organization information for the purpose of providing high quality protection to our users. The collected data may contain:

- Files that are blocked by WithSecure for a security reason, and related metadata. The metadata includes for example file hash, file name and file path. We need to analyze files and emails for malicious content and behaviors for your protection. Files are processed in a safe environment to catch harmful behaviors. Collection of this data helps WithSecure to keep a global threat situation map that allows reacting quickly to new threats.
- Web addresses that you have tried to visit but have been blocked by WithSecure for a security reason or which exhibit potentially malicious behavior, and related metadata. The metadata includes for example response headers. A site may get blocked based on selected protection preferences and parental control reasons. The collected information also allows protection against phishing and ransomware attacks.

The portal administrators will only see a summary of the result, for example if the file is infected or not. However, if the service detects malware, a summary of the detection is visible in the portal and can be connected to an individual device by those having access to portal.

11.2.2 Elements Collaboration Protection

Data sent to Security Cloud is always anonymized and cannot be connected to an individual user in any way.

11.2.3 Elements Mobile Protection

The service sends queries on potential malicious activity, malicious software, or unwanted applications on protected devices, and URL requests to WithSecure Security Cloud. These queries — such as URLs, file identifiers, and application metadata — cannot be connected to an identifiable user by WithSecure.

11.2.4 Elements Endpoint Detection and Response

The service sends queries on potential malicious activity, malicious software, or unwanted applications on protected devices, data traffic, and networks to WithSecure Security Cloud. These queries – such as URLs, file identifiers, and application metadata – cannot be connected to an identifiable user by WithSecure.

To protect your privacy, WithSecure separates the security data set out in section 7 above from other data collected on your use of the service, anonymizes it, and destroys it when it is no longer needed for the purpose.

12 Legal Grounds

As a data controller we are committed to maintaining high standards of data protection when we are processing personal data. We try to minimize our exposure to personal data as much as possible and when personal data is processed by WithSecure within our Elements Services we generally rely on legitimate interest as a basis for processing personal data.

12.1 Elements Collaboration Protection

Both WithSecure and each customer company operate as independent controllers over their respective areas of data processing that takes place in the context of the services.

To the extent that the data processed by WithSecure in the services is identifiable to an individual, the services process data to safeguard the following legitimate interests;

- providing WithSecure services to secure our customers' networks and devices as well as the confidentiality and availability of the data therein;
- enabling WithSecure to detect emerging threats and security-relevant trends among all of its customers, so that our services can keep on par with evolving threats;
- enabling WithSecure to provide a centralized security service framework across multiple continents to a large number of customers and partners.

The data processing undertaken by the service is mandatory for the efficient protection of customer company data in its cloud service organization (such as Microsoft 365). While the individual service's settings may enable an IT administrator to limit the processing of security data by WithSecure, such adjustments are not recommended, as they endanger achieving the above intended purposes of the services.

12.2 Elements Endpoint Protection

To the extent that the data processed by WithSecure in the EPP services is identifiable to an individual, the services process such data to safeguard the following legitimate interests:

- providing WithSecure services to secure our customers' networks and devices as well as the confidentiality and availability of the data therein;
- enabling WithSecure to detect emerging threats and security-relevant trends among all of its customers, so that our services can keep on par with evolving threats;
- enabling WithSecure to provide a centralized security service framework across multiple continents to a large number of customers and partners.

Additionally, Web Portal analytics are put in place to improve WithSecure products.

In the case of data that is not strictly necessary to provide you with the Services — but would help us in providing you with better services in the long run — we collect such data only with your consent.

Your employing company independently establishes its legal grounds for the processing of identifiers for the purposes set out above.

12.3 Elements Exposure Management

For both Elements Vulnerability Management and Elements Exposure Management WithSecure has a legitimate interest in identifying its portal users and monitoring such users' portal usage as set out above to make sure that only authorized users are able to utilize the service and that services are only used for their lawful purposes. To this effect, you are responsible for providing accurate and truthful access credentials to be able to use the service.

The data collected by the services in the form of "vulnerability scan results" is processed for the dual purposes of:

- improving WithSecure's customers' network and device security as well as the confidentiality and availability of the data therein, and
- allowing WithSecure to detect emerging threats and security-relevant trends among all of its customers, so that WithSecure services can keep on par with evolving threats. The vulnerability scan results do not, by default, contain personally identifiable data.

Any contact details processed in Attack Surface Management are processed on the basis of legitimate interest.

12.4 Elements Mobile Protection

The data processing by the services is mandatory for the efficient protection of the device and a prerequisite for WithSecure's capability to provide its contracted services. As such processing is inseparable from the services that we provide to you, this gives us a valid need to process your data and a justification to do so.

In some cases, processing may take place in the form of "legitimate interest".

12.5 Elements Endpoint Detection and Response

The results of these services are utilized for the benefit of WithSecure's customers. Both the customer and WithSecure – as a provider of security services – have a recognized legitimate interest in undertaking necessary and proportional activities to that effect.

The core "privacy interest" of the EDR solution is to safeguard the valuable data residing in the customer's devices and network. This also includes personal data of the employees of the customer whose devices the EDR sensors monitor. To achieve the above, the solution profiles the events taking place on the devices of the corporate network(s) to reveal potentially malicious activities taking place on specific devices within customer networks. Objecting to such data collection has a negative impact on the protection awarded by the WithSecure services for the above data in your organization.

The potential negative privacy impact of consequent employee device monitoring is mitigated by technical safeguards, limitations on collected data types, and correlating the collected data to identifiable individuals / devices only in pre-designed phases of processing. Providing the EDR solution is dependent on automated data collection from the protected devices / environment.

12.6 Secondary uses

In addition, we may also need to use and/or continue to store data i) to meet a "legal obligation" to process data for specified purposes, or ii) under the grounds of "legitimate interest". For an example list of situations where we may resort to such justifications, see the "Other uses and disclosures" section in our general privacy policy.

13 Transfers and Disclosures

The data presented in the service portal is visible to your company's IT administrator, whether internal or external. If the company's IT is managed by a third party, this data is also available to them (WithSecure's "distributor/reseller partner"), so that they can provide your company with support for our services and corresponding IT services.

WithSecure further employs its own affiliates and subcontractors so we can provide our services globally.

More information on transfers and disclosures is available in the WithSecure General Privacy Policy.

14 Retention

WithSecure Elements services gather and share data with other Elements services. This data is stored for a length of service provisioning to our customer company and is visible in the respective Elements portal for the same duration. After the last Elements subscription has expired, the data is retained in

WithSecure storage for a maximum of four (4) months before final deletion or anonymization unless otherwise agreed on a case-by-case basis with the customer. This enables renewal of the service after its expiration without the need to reinstall and without losing old data.

This maximum retention time after expiration of the last subscription applies also to the data for which Elements allows customers to set custom retention time during the use of the service, e.g. Elements Vulnerability Management allows retention time to be set for vulnerability findings and Elements Collaboration Protection for quarantined emails.

Logs, such as basic audit logs, which show which users accessed the portal or API, and detailed service logs, which show what actions were used, are kept for a maximum of two years on a rolling basis.

WithSecure's Security Cloud is a cloud-based threat analysis and reputation system that scans data for any malicious or harmful content. Data sent to Security Cloud is always anonymized and cannot be connected to an individual user in any way. Any files or URLs sent to Security Cloud, are automatically deleted near-instantaneously after analysis, if they are not found to be suspicious.

Anonymized security data and statistical data are stored on WithSecure servers without a set end date as long as the data continues to be useful for the purpose it was collected for.

More information, exceptions, and additions:

The customer company has a right to request their data to be removed earlier than the data would otherwise be stored based on the above mentioned retention times. The default rule under the law is that personal data should be deleted or anonymized once it is no longer needed for its purpose. However, there are exceptions when we need to deviate from the primary retention times including the following examples:

- backups (e.g. copy of your personal data may exist in backups until they are rotated);
- applicable laws require us to store the data (e.g. to keep track of the purchase and payment of our services);
- to pursue available remedies or to limit any damages that we may sustain (e.g. due to an ongoing dispute or investigation);
- to solve or contain a recurring problem or to have enough information to respond to future issues (e.g. your support ticket related to a problem that was not permanently corrected during your customership);
- to prevent fraudulent activity (e.g. to enforce a ban on our community);
- your personal data is incorporated to other data for a secondary purpose (e.g. retaining logs);
- other similar circumstances, where there continues to be a legitimate need for the ongoing storage of personal data.

The final removal of your user account, WithSecure Business Account, may be delayed to avoid disturbing the other interactions you have with us. This is the case when you i) have an WithSecure Community, Learning Management System or Partner Portal account, ii) you continue to subscribe to our marketing messages. You can opt out from our marketing messages at any time.

If we have received your information when providing you with technical support, the information is stored as long as the respective support case remains unsolved. Once solved, the information is gradually deleted or anonymized within two years from closing the case.

Analytics data collected with the user's consent is retained for statistical purposes and is not deleted on removal of personal data and the user account. After termination of the account, analytics data cannot be linked to any personally identifiable user.

15 Security

We apply strict security measures to protect the confidentiality, integrity, and availability of your personal data when transferring, storing, or processing it.

We use physical, administrative, and technical security measures to reduce the risk of loss, misuse, or unauthorized access, disclosure, or modification of your personal data.

All personal data is stored on secure servers operated by WithSecure or our partners with access limited to authorized personnel only.

16 Your Rights

Information on your statutory rights and how to contact us is available in the WithSecure General Privacy Policy here: Corporate privacy | WithSecure™

17 General

This privacy policy is effective as of Oct 15 2024. Please note that this privacy policy will regularly be updated to reflect any changes in the way we handle your personal data or any changes in applicable laws.

This version of the policy clarifies, updates, and replaces the previous version. To continue keeping this document up to date, we will make changes and additions to this from time to time also in the future.

More information on definitions and change management is available in the WithSecure General Privacy Policy here: Corporate privacy | WithSecure™

*****END OF DOCUMENT*****