WithSecure Co-Monitoring Service

Service Description

WITH secure

CLIENT RESTRICTED

Table of Contents

1 CONFIDENTIALITY & DOCUMENT CONTROL

1.1 Confidentiality Statement

All information in this document is provided in confidence. It may not be modified or disclosed to a third party (either in whole or in part) without the prior written approval of WithSecure Limited ("WithSecure™"). WithSecure™ will not disclose to any third-party information contained in this document without the prior written approval of the Client.

1.2 Document Control

Date	Change	Change by	Issue
31-03-2023	Document created	WithSecure	1.0
03-04-2023	Minor changes from legal team	WithSecure	1.1
23-05-2023	Added Section 8 – Responsibilities matrix	WithSecure	2.0
17-07-2023	• Updated information on Incident Response retainer benefits and SLAs • Updated Elevate to WithSecure token quantities • Added clarifications that service should cover the whole customer estate • Added clarifications that service must be activated with the Elements Security Center by Partners and Customers, and remain activated • Added 2-hour target response time to Threat Investigation section • Updated licensing section to remove reference to flat fee in pricing	WithSecure	2.1
30-09-2023	Updated for General Availability release: • Addition of out-of-office option as an alternative to 24/7 • Updated process for submission of escalation contact details using the Elements Security Center	WithSecure	3.0
06-10-2023	Updated to clarify email notification behaviour for severe BCDs	WithSecure	3.1

2 OVERVIEW

This document describes the 'WithSecure Co-Monitoring Service'.

The 'WithSecure Co-Monitoring Service' is a continuous 24/7 or out-of-office monitoring service in which WithSecure cyber security experts investigate and provide remediation advice relating to 'Broad Context Detections', later referred to as 'Detections', generated by 'WithSecure Elements EDR'.

3 WITHSECURE CO-MONITORING SERVICE

Detecting network intrusions by sophisticated threat actors and responding appropriately is very difficult, costly and resource intensive, especially when they happen outside of office hours.

Successful detection and response requires extensive monitoring capabilities, combined with advanced threat analysis and guidance provided by cyber security experts, as well as personnel on stand-by with the authority and ability to respond to security incidents 24/7.

For the vast majority of companies, acquiring these security capabilities is prohibitively expensive. The 'WithSecure Co-Monitoring Service' solves this issue by providing a cost-efficient, continuous monitoring service.

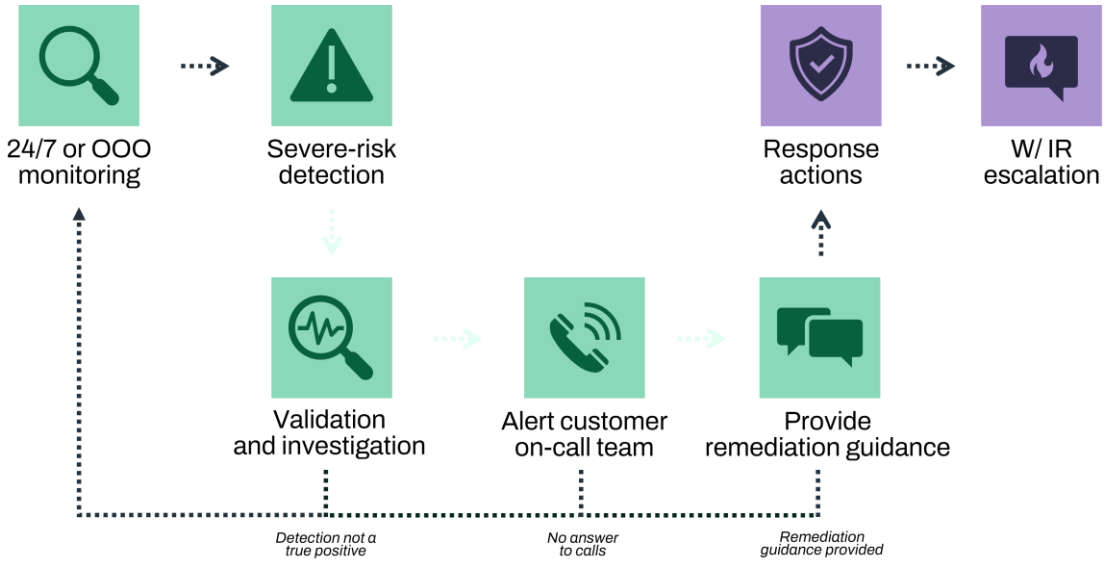
The service is provided 24/7 or as an out-of-office option, as selected by the customer at the time of purchase, and concentrates on investigating and providing remediation advice relating to detections provided by 'WithSecure Elements EDR'.

The four primary service elements are as follows:

- Maintaining constant watch over severe risk detections in customers' IT environments
- Validating and investigating detections to establish if they are true positive incidents that require action to remediate, or false positives which can be closed
- Ensuring that true positive incidents are escalated in a timely fashion to the correct contact customer representative(s) with the authority and ability to respond to the security incident in question
- Providing advice to the customer representative(s) for containment and remediation of the incident, for example recommending network isolation of the affected systems or termination of malicious processes

WithSecure recommends that companies facing a substantial risk of serious cyber security incidents complement the 'WithSecure Co-Monitoring Service' service with 'Incident Response' and 'Incident Readiness' services. WithSecure will also recommend Incident Response if thresholds for certain parameters are exceeded while reviewing a severe security incident, as the support required to remediate the incident is beyond the scope of the 'WithSecure Co-Monitoring Service'. These complementary services and thresholds are summarized at the end of this document. Complementary services must be acquired separately.

The following diagram shows how the 'WithSecure Co-Monitoring Service' works in summary:



3.1 Automated Monitoring

Upon acquiring the right to use the 'WithSecure Co-Monitoring Service', the customer's 'WithSecure Elements EDR' solution enables a built-in 'Auto-Elevation' mode. In this mode, 'WithSecure Elements EDR' will automatically elevate detections to a manual Threat Investigation process by a specialized WithSecure cyber security expert.

The automatic elevation process works by elevating detections coming from hosts that are enrolled in the scope of the service. See Section 3: Service Availability for more information.

During the 'Auto-Elevation' mode, detections which reach a 'Severe' risk level are automatically elevated for a manual Threat Investigation process by a specialized cyber security expert. Risk levels such as 'Severe' are assigned by 'WithSecure Elements EDR' using standard risk measures of likelihood and impact. The likelihood and impact are in turn calculated from various contextual identifiers, anomalies, telemetry patterns and abnormal activities, which allow 'WithSecure Elements EDR' to identify malicious techniques, tools and processes (TTP) used by threat actors. Note that detection risk scores are dynamic, meaning that a detection's risk score can increase as more malicious activity becomes apparent – what starts as low risk may later become severe and therefore trigger the 'Auto-Elevation' process.

3.2 Threat Investigation

Once a 'Severe' detection has been escalated for further investigation, a specialized cyber security analyst will manually conduct a deeper analysis of the detection. WithSecure's on-shift threat analysts will begin investigating the escalated detection within a 2-hour target response time.

Threat Investigation provides a highly detailed investigation into a specific Broad Context Detection, leveraging all recent and historical data. This also includes actionable incident response guidance from WithSecure cyber security experts, along with a detailed account of the detected attack type.

Each detection investigated is categorized in the following four general categories:

- a genuine threat or security incident that requires immediate escalation to the customer's contact person(s)
- suspicious activity that should be reacted on, but does not require immediate escalation
- suspicious activity that can be accepted as a risky behavior in the target environment, and does not require escalation
- a false positive

If the detection is confirmed as a genuine threat or security incident, the WithSecure analyst will initiate an escalation to the contact person(s) designated by the Partner/Customer. The contact person(s) will either be from the customer's internal IT team, or a partner to whom the customer has outsourced the management of their environment.

A false positive is a detection resulting from a detection rule incorrectly categorizing standard and benign activity as malicious. False positives are never escalated.

A detection which arises from suspicious activity conducted by a legitimate internal user of the customer is not considered a false positive. Suspicious activity warrants investigation and validation, regardless of whether it is performed by external or internal actors.

3.3 Incident Escalation

If the detection is confirmed to be a genuine threat or security incident, the WithSecure analyst will initiate an escalation to the contact person(s) designated by the customer.

The escalation process works as follows:

- An automated email notification is sent to the email address(es) specified in the Elements EDR service settings
- The detection is highlighted in the 'WithSecure Elements Security Center'
- The WithSecure analyst will contact each of the designated phone number(s) in priority order until a designated contact person is reached and alerted to the incident
- Once initial notification has been completed, further engagement between the analyst and the customer will happen via the 'WithSecure Elements Security Center'

Recommendations to contain the threat will be provided. These will be accessible to the customer in the 'WithSecure Elements Security Center'.

In some circumstances the customer may require assistance from WithSecure that goes beyond the scope of the 'WithSecure Co-Monitoring Service', for example in assessing the broader business impact of a detection or performing analysis of data from sources other than 'WithSecure Elements EDR', such as firewall logs. In these cases, the incident is considered to reach the threshold for Incident Response, which must be procured from WithSecure as a separate service – refer to Section 7 for more details.

3.4 Recommendations

After the security incident has been escalated to the designated contact person(s), with the authority and ability to conduct response actions, the analyst will suggest steps to mitigate the security incident. However, the analyst will not conduct response actions on behalf of the customer in question.

In the case of a genuine, ongoing attack, the analyst will suggest response steps, and further steps necessary to investigate. The primary focus is on helping to assess the extent of the compromise followed by recommended containment measures.

If the severity of the case meets the Incident Response threshold, or the contact persons designated by the customer feel that they are unable to remediate the incident independently, WithSecure analysts will recommend escalation to a separate, dedicated 'Incident Response' process to further contain and remediate threats in the target environment.

The 'Incident Response' process is not covered by the 'WithSecure Co-Monitoring Service' and must be acquired separately. See Section 7, 'Complementary Services', for further information and for the conditions for reaching the 'Major Incident Threshold'.

3.5 Manual Elevation to WithSecure

If a detection appears suspicious but does not qualify for an automatic escalation to WithSecure, as it does not reach the 'Severe' risk level, the customer can submit an optional 'Threat Investigation' request using the 'Elevate to WithSecure' tokens that are provided alongside the 'WithSecure Co-Monitoring Service'.

The Monthly Service Fee includes 3 'Elevate to WithSecure' Validation tokens per month and 1 'Elevate to WithSecure' Investigation token per month. Note that any unused 'Elevate to WithSecure' tokens will expire at the end of each month. They cannot be carried over to subsequent months.

Threat Validation provides additional information about a Broad Context Detection™ discovered during the last 7 days. This includes an expert-written summary and description of the detection, along with any other relevant data to help you determine whether it requires response actions.

Threat Investigation provides a highly detailed investigation into a specific Broad Context Detection™, leveraging all recent and historical data. This option also includes actionable incident response guidance from our cyber security experts, along with a comprehensive report of the detected attack type.

4 SERVICE AVAILABILITY

4.1 Prerequisites

To make use of the service, the following prerequisites must be met:

4.1.1 Commercial

- Valid WithSecure Elements EDR Subscription
- Valid WithSecure Elements EDR Co-Monitoring Subscription

4.1.2 Technical

- Deployed WithSecure Elements Agent to all endpoints on the customer's estate
- Access to WithSecure Elements Management Console

If the WithSecure Elements Agent cannot be deployed to the entire estate, this can affect the quality of the WithSecure Co-Monitoring Service. Monitoring only a segment of the environment affects service quality due to the myriad of methods used by attackers, for example lateral movement. It is an essential requirement to deploy the WithSecure Elements Agent to all endpoints on the customer's estate to detect an incident as quickly as possible.

4.1.3 Process

It is mandatory for the Partner or Customer to designate primary and secondary contact persons/groups (name and phone number), who are available on-call during the subscription period of the service.

This information will be recorded within the Elements Security Center during the onboarding phase by the Customer's internal IT team, or by a partner to whom the customer has outsourced the management of their environment. The relevant information will be made available to all WithSecure delivery teams.

If any mandatory information is missing, the service cannot be delivered, and will remain 'inactive' until the mandatory information is provided.

Once all steps in the onboarding process have been completed, the Partner or Customer must activate the WithSecure Co-Monitoring service within the WithSecure Elements Security Center. Instructions will be provided for this by WithSecure during the onboarding process.

The WithSecure Co-Monitoring Service must remain activated within the Elements Security Center for the WithSecure Co-Monitoring Service to be delivered according to the Partner or Customer's Co-Monitoring subscription.

Partners/Customers will also receive email notifications for any Severe BCDs, using the email address specified for their Elements EDR service settings.

4.2 Service Hours

The ‘WithSecure Co-Monitoring Service’ is available as a 24/7/365 option, or as an out-of-office option. The Customer must choose one of these options in writing when agreeing to buy the ‘WithSecure Co-Monitoring Service’. The pricing differs for these options.

4.2.1 24/7/365 Option

For the 24/7/365 option:

- Coverage applies 24 hours a day, 7 days a week, 365 days a year
- Due to the nature of this option, the customer’s local timezone has no bearing on the delivery of the service
- Due to the nature of this option, the customer would continue to receive a service on Public Holidays

4.2.2 Out-of-Office Option

For the out-of-office option:

- ‘Office hours’ are defined as 09:00 to 17:00 Monday to Friday in the customer’s local timezone
- ‘Out-of-office’ is defined as 17:00 to 09:00 (the following day) Monday to Friday, and 24/7 on Saturdays and Sundays, in the customer’s local timezone
- Partners/Customers must select the correct timezone in the ‘WithSecure Elements Security Center’ for their out-of-office subscription to follow the correct times
- Public holidays that occur Monday to Friday are not currently classified as out-of-office

For the out-of-office option, BCDs classified at Severe risk level will be automatically elevated to WithSecure outside of office hours as specified above.

During office hours, Partners and Customers are responsible for managing Severe BCDs. These will only be investigated by WithSecure, if manually elevated to WithSecure by the Partner/Customer.

4.3 Service Language

The ‘WithSecure Co-Monitoring Service’ is available in English only.

4.4 Service Delivery Locations

The WithSecure cyber security analysts who deliver the ‘WithSecure Co-Monitoring Service’ are located in Poznan, Poland; London, United Kingdom, and Singapore.

5 DATA COLLECTION & RETENTION

In order for a detection to happen, and to be escalated to a WithSecure analyst, the WithSecure Elements EDR Agent has to be installed on at least one device. These agents are installed on the customer network by the Partner/Customer, on devices designated by the Customer, in order to detect and preserve evidence about security anomalies in the network. The data is sent from the agent to WithSecure for analysis.

The WithSecure Elements EDR Agent collects the following kinds of event-based data from the device it is installed on, referred to later as 'Event Data':

- Technical user identifiers
- Domain names and network connections
- Metadata of process creation, behavior, and access to various systems/subsystems

Additionally, the agent collects information on applications present on the devices where the sensor is installed, as well as system/network information and other metrics.

Data is stored in identifiable form as long as it remains useful for the purposes of processing and for the duration of the customer's engagement of 'WithSecure Elements EDR'. At the time of writing this Service Description, the data is stored for two (2) years on a rolling basis during the customer engagement and is deleted within two (2) months after termination of the engagement.

For full details please refer to the WithSecure EDR Privacy Policy, which is available on the Partner Portal or can be provided upon request.

6 LICENSING

The 'WithSecure Elements Co-Monitoring Service' is based on a 'Monthly Unit Fee' per monitored device. The minimum subscription size for Co-Monitoring is 25 devices.

The Monthly Service Fee includes:

- 'WithSecure Premium Support'
- 3 'Elevate to WithSecure' Validation tokens per month
- 1 'Elevate to WithSecure' Investigation token per month

Note that any unused 'Elevate to WithSecure' tokens will expire at the end of each month. They cannot be carried over to subsequent months.

For more information about the licensing of the 'WithSecure Elements Co-Monitoring Service', or the separately acquirable Incident Response and Incident Readiness services, please refer to your local WithSecure representative.

7 COMPLEMENTARY SERVICES

WithSecure recommends that companies facing a substantial risk of serious cyber security incidents complement the 'WithSecure Co-Monitoring Service' service with 'Incident Response' and 'Incident Readiness' services. These services are briefly described below and must be acquired separately.

7.1 Incident Response

If the severity of a security incident meets the Incident Response threshold, WithSecure analysts will recommend escalation to a separate, dedicated 'Incident Response' process, to contain and remediate threats in the target environment. The Incident Response process is not covered by the 'WithSecure Elements Co-Monitoring Service'. The 'Incident Response Threshold' is considered reached when any one of the following conditions is met:

- The 'WithSecure Co-Monitoring Service' total hours spent reviewing a severe BCD exceeds 2 hours, without expected resolution within the next hour
- More than five devices have been infected in the target environment
- A business-critical asset has been compromised
  - 'Business critical' is defined as anything that could be taken offline that would wholly impede the customer's business operations
- A compromised device has been identified that does not have WithSecure Elements EDR coverage

Incident Response services are provided by the WithSecure Global Incident Response team that operate 24/7, specialize in major cyber crises and have dealt with live incidents for some of the world's largest organizations (including constituents of the Dow Jones, NASDAQ, and FTSE 100, and government agencies and departments).

Incident Response services follow their own service descriptions and must be procured separately. In some instances, due to the classification of the data impacted, government vetting maybe also be required, as well as continued reporting to the regulators or customers.

7.2 Tabletop Exercises

Organizations that lack preparation to effectively respond to an incident are more likely to experience significant losses when an incident occurs. Improved Incident Readiness enables organizations to proactively streamline incident response costs, quantify spend, and improve cross-departmental collaboration. To improve the client's Incident Readiness, WithSecure offers the client Tabletop Exercises to train response teams for improved performance when handling real incidents.

WithSecure offers the following tabletop exercises:

1. Incident response - exercises on how to triage, investigate, and contain a relevant incident prior to it becoming a crisis;
2. Incident management - exercises on how to manage a complex cross- organizational response through sound containment and recovery formulation;
3. Crisis management - exercises on how to strategically steer a company-wide response to an existential cyber crisis.

8 WITHSECURE AND PARTNER/CUSTOMER RESPONSIBILITIES

The table below outlines the responsibilities of WithSecure and the Partner/Customer for each different area of the 'WithSecure Co-Monitoring Service'.

Service category	Service feature	WithSecure Responsibilities	Partner/Customer Responsibilities
1. Onboarding	GTM	WithSecure will sell EDR Co-Monitoring through selected Partners and directly to customers. WithSecure will produce a Service Description, along with sales and marketing material. The following criteria will be used to guide Partner selection: 1) They offer services to their customers-base, preferably managing the customers' environments 2) They have a 24/7 technical on-call, preferably an active one rather than "woken up" 3) They have the potential to sell EDR in meaningful numbers, or preferably already do so	Selected Partners are able to sell Co-Monitoring subscriptions to customers within the appropriate target market.
1. Onboarding	Agent required	The Elements EDR agent is required for a Co-Monitoring subscription.	
1. Onboarding	Deployment management	WithSecure will make stable installers available for the Elements EDR agent for supported operating systems.	Partners or Customers are responsible for installing the Elements EDR agent and monitoring that agents are online and working at all times, in order for a Co-Monitoring service to be delivered. Once all steps in the onboarding process have been completed, the Partner or Customer must activate the WithSecure Co-Monitoring service within the WithSecure Elements Security Center.

			The WithSecure Co-Monitoring service must remain activated within the Elements Security Center for the WithSecure Co-Monitoring service to be delivered according to the Partner or Customer's Co-Monitoring subscription.
1. Onboarding	Automatic/ managed updates	WithSecure will issue automatic updates for the Elements EDR agent, which will be made available across the installed base for EDR Co-Monitoring customers. Managed updates are not available for Elements EDR customers, and by extension not for Co-Monitoring customers either.	Partners or Customers are responsible for monitoring that Elements EDR agents are online and working, including the successful installation of automatic updates.
1. Onboarding	Escalation contact information collection	WithSecure will provide guidelines on the escalation contact information required to deliver a Co-Monitoring subscription and make it possible to submit and manage contact information within the 'WithSecure Elements Security Center'.	Partners and Customers are responsible for providing and maintaining the escalation contact information required for the delivery of the Co-Monitoring service according to the guidelines provided by WithSecure. Partners/Customers are responsible for submitting and maintaining escalation contact information through the 'WithSecure Elements Security Center'.
1. Onboarding	Training	WithSecure will provide training materials for Elements EDR and Co-Monitoring to train Partners/Customers to deploy and operate the EDR Co-Monitoring service successfully.	Partners/Customers are required to complete the training materials provided by WithSecure to deploy and operate the EDR Co-Monitoring service successfully.
2. Detection	Detection and Incident Severity	The WithSecure Elements EDR agent will detect suspicious or unusual activity on any hosts where the Elements EDR agent is installed. When a BCD is classified at the Severe risk level, it will be managed according to the customer's Co-Monitoring subscription type. For a 24/7 Co-Monitoring subscription, all BCDs classified at the Severe risk level will be automatically elevated to WithSecure, at	Partners and Customers are responsible for the management of all BCDs at all times, other than those classified at the Severe risk level. When a BCD is classified at the Severe risk level, it will be managed according to the customer's Co-Monitoring subscription type. For a 24/7 Co-Monitoring subscription, all BCDs classified at the Severe risk level will be automatically elevated to WithSecure, at

		all times. There is no limit on the number of severe BCDs that might be auto-elevated. For an Out-of-Office Co-Monitoring subscription, BCDs classified at Severe risk level will be automatically elevated to WithSecure outside of office hours as specified in section 4 of the Service Description. There is no limit on the number of severe BCDs that might be auto-elevated during the specified hours.	all times. For an Out-of-Office Co-Monitoring subscription, BCDs classified at Severe risk level will be automatically elevated to WithSecure outside of office hours as specified in section 4 of the Service Description. During the office hours specified in section 4, Partners and Customers are responsible for managing Severe BCDs. These will only be investigated by WithSecure if manually elevated to WithSecure by the Partner/Customer.
2. Detection	Proactive threat hunting	None	As per Partner offer/agreement with customers.
3. Investigation	Investigation of BCDs	WithSecure will investigate all BCDs classified as Severe risk that are automatically elevated according to the customer's Co-Monitoring subscription type, as described in Section 3 of the Service Description. During the investigation, WithSecure will determine whether the BCD is a False Positive or True Positive. The WithSecure Analyst will add updates and comments to BCDs to keep the customer updated. These will be visible to the Partner/Customer in the 'WithSecure Elements Security Center'. In the case of a False Positive, the Elevation will be closed by the WithSecure analyst without contacting the Partner/Customer. The Partner/Customer will then be responsible for closing the BCD. In the case of a True Positive, the WithSecure Analyst will initiate the escalation process as described in Section 3 of the Service Description: - An automated email notification is sent to the email address(es) specified in the Elements EDR service settings - The detection is highlighted in the 'WithSecure Elements	Partners and Customers are responsible for the management of all BCDs at all times, other than those classified at the Severe risk level. This includes any investigations that are necessary. In the case of an Out-of-Office Co-Monitoring subscription, the Partner/Customer will investigate all BCDs classified as Severe Risk during office hours. These would not be automatically elevated to WithSecure. In all cases, the Partner/Customer is responsible for closing the BCD. Partners/Customers are responsible for responding to escalations and receiving contact made through the agreed escalation contact details.

		Security Center' - The WithSecure analyst will contact each of the designated phone number(s) in priority order until a designated contact person is reached and alerted to the incident. - Once initial notification has been made, further engagement between the analyst and the customer will happen via the 'WithSecure Elements Security Center'. The Elevation will be closed by a WithSecure analyst. The Partner/Customer will then be responsible for closing the BCD. - If contact is unsuccessful, the WithSecure analyst will continue to update 'WithSecure Elements Security Center' requesting a response and action from the Partner/Customer. Recommendations to contain the threat will be provided. These will be accessible to the customer in the 'WithSecure Elements Security Center'.	
3. Investigation	Elevate tokens	The Monthly Service Fee includes: 3 'Elevate to WithSecure' Validation tokens per month 1 'Elevate to WithSecure' Investigation token per month Note that any unused 'Elevate to WithSecure' tokens will expire at the end of each month. They cannot be carried over to subsequent months. There is no restriction on which BCDs can be elevated. These Elevations will be handled by WithSecure according to the current 'Elevate to WithSecure' scope. Please refer to current 'Elevate to WithSecure' documentation for further details.	
4. Response	First response	None - Response and remediation advice will be provided before an investigation is closed – see 'Investigation of BCDs' above.	As per Partner offer/agreement with customers.

		An Incident Response retainer can be purchased if the Partner/Customer requires response support from WithSecure.	
4. Response	Incident Response Included	Optional +	
4. Response	Post-incident support	Optional +	
5. Customer communication	In portal reporting	Results of investigations, comments, updates and outcomes for in-scope Severe BCDs will be visible to the customer and partner in the 'WithSecure Elements Security Centre'.	
5. Customer communication	Customer care	The Monthly Service Fee includes 'WithSecure Premium Support'.	
6. Service parameters	Support hours	Pilot: 24/7 GA: 24/7 or Out-of-Office as per customer subscription	
6. Service parameters	Europe only/Global	Global service provision only	
6. Service parameters	Language	English-only	
6. Service parameters	Data protection	WithSecure is responsible for the data that is collected and stored by WithSecure Elements EDR and also additional information stored on WithSecure systems to deliver the service successfully, including contact details for escalation purposes. This data is collected and stored according to WithSecure's privacy policies, which are available on request.	Partners/Customers are responsible for any data collected and stored in addition to the data collected by WithSecure. Partners/Customers should collect and store this data according to their own published privacy policies.
7. Readiness	Tabletop exercises	Optional +	