WithSecure Elements Infinite

Service Description

Table of Contents

1 CONFIDENTIALITY

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™").

2 OVERVIEW

This document describes the 'WithSecure Elements Infinite' service. It is a comprehensive managed service delivered by WithSecure, using fully in-house resources, meant for clients with demanding cybersecurity requirements.

The core service and its optional add-on modules for Identities (EntraID) and Cloud (AWS, Azure) are described in this document in its entirety. Refer to the appropriate Statement of Work (SOW) to understand which capabilities have been acquired.

WithSecure reserves the right to amend the service description, as capabilities are introduced or deprecated in the service or the underlying platform, to address the evolving threat landscape, changes in modern IT-infrastructure and expansion of AI-capabilities.

3 WITHSECURE INFINITE

WithSecure Infinite provides comprehensive suite of security tools and capabilities as a continuous managed service. It offers significant advantages in terms of cost, expertise, scalability, and security outcomes, allowing the IT department to refocus their resources from exposure management to their core business goals.

The service delivery and client collaboration with WithSecure's cybersecurity personnel is done through the WithSecure Elements platform, including responding 24/7 to cyber security incidents and improving customers security posture, to providing on-demand assistance where needed.

The primary service components are as follows, covering the environments external attack surface(s), identity management systems (Entra ID), physical endpoints, corporate networks and cloud environments (AWS, Azure).

- **Continuous Threat Exposure Management (CTEM):** WithSecure proactively identifies vulnerabilities, misconfigurations and other weaknesses in customer's IT environment, prioritizing and reporting them for remediation. Issues are prioritized based on business context and exposure score, and remediation progress is monitored and evaluated as mitigation activities are implemented.

- **Endpoint Protection, Detection and Response (EPP, EDR):** WithSecure provides build-in Endpoint Security capabilities, which have an exceptional track record in threat detection in real-world scenarios and preventing 100% (AV-Test) of tested ransomware, 0-day malware and other malware facing modern companies.

- **Managed Detection and Response (MDR):** WithSecure maintains constant 24/7 watch over customer's IT environment, investigating any detected suspicious activity, and taking decisive and appropriate containment and eradication actions on behalf of the customer, according to agreed SLAs and authorizations given.

- **Incident Response Retainer (IR):** WithSecure provides SLA-backed, on-demand access to skilled Incident Response resources during cybersecurity incident(s) to ensure the business continuity of the client and effective remediation of the incident.

- **Elements Platform Access:** WithSecure provides 24/7 on-demand access to the underlying security and management tooling, providing unified visibility, reporting and management capabilities across the customer estate, in addition to AI-powered security tooling.

- **Customer Success Management (CSM):** WithSecure provides a dedicated Customer Success Manager, who's primary aim is to ensure that the customer gets full value of the service, and to act as the main point of contact and coordinator towards WithSecure.

WithSecure Elements Infinite's development and operations, as well as the related managed security services, are in scope of WithSecure ISO 27001 Certification. WithSecure's Incident Response capabilities are accredited by government agencies: by the NCSC-UK (CIR L1 & L2) and by the NCSC-DE (APT- Responder Provider)

4 CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)

WithSecure Infinite includes a Continuous Threat Exposure Management (CTEM) service, which provides a continuous process that over time delivers significant improvements to the environment's security posture, reducing dramatically its exposure to threats and thus probability to cyber security incidents.

The primary service elements are as follows:

- **Continuous Exposure Monitoring**: Continuous 24/7 monitoring of an organization's exposure to cyber threats; identifying vulnerabilities, misconfigurations, outdated software and other gaps in security controls that could expose the organization to cyberattacks.

- **Exposure Risk Prioritization:** The findings are prioritized for remediation based on organization's operational requirements, business impact and contextual technical factors, such as asset criticality, exploitability, technical severity (e.g., CVSS scores) and attack path mapping.

- **Remediation Roadmap:** The creation of a remediation roadmap is done jointly with the customer to address identified risks in priority order, along with recommended remediation actions and compensating controls factoring the organization's infrastructure and operational requirements.

- **Remediation and Validation:** After remediation/mitigation actions are implemented, their effectiveness is validated and any residual exposure is identified, feeding into the next step in the remediation plan and its execution.

- **Exposure Reviews and Reporting**: A quarterly exposure deep-dive meeting is held together with customer's IT leadership and stakeholders, where organization's exposure risk is reviewed through clear KPIs, reports, and actionable insights that supports the client's strategic decision-making and operational requirements.

Throughout the CTEM process, WithSecure Exposure and Risk Management team can provide on-demand remediation and mitigation advice, such as interpretation of exposure finding or threat hunt, assisting with risk assessment or offering further mitigation strategies if patching or compensating controls are not an option.

The following sections describes the service elements in more detail.

4.1 Continuous Exposure Monitoring

The protected environment is continuously monitored 24/7 with ongoing evaluation for vulnerabilities, misconfigurations, outdated software and security gaps across its external attack surface(s), identity management systems (Entra ID), physical and virtual endpoints, corporate networks and cloud environments (AWS, Azure).

The scans are supplemented by real-time threat intelligence feeds, which provide insights into emerging vulnerabilities, exploit tactics, and active threat actors. Additionally, WithSecure will conduct targeted Exposure Hunts to identify new and emerging threats.

4.1.1 Asset Discovery

Asset Discovery provides automatic identification and cataloging of detected hardware, software, cloud instances, and digital assets within the customer's IT environment. Using a combination of network scanning, API integrations, and endpoint detection tools. It identifies both authorized and unauthorized assets, including devices, applications, and virtual machines. This process provides real-time visibility and mapping of the entire asset landscape, ensuring that any new, outdated, or rogue assets are accounted for.

4.1.2 Identity Management Systems

Identity Exposure monitors your EntraID accounts for identity related exposure, including weaknesses such as lack of multifactor authentication (MFA) and old and weak passwords. It also monitors whether the accounts have been part of a data breach and severity of the compromise, based on the type of information compromised and whether those accounts are still exploitable.

4.1.3 External Attack Surface Management (EASM)

External Attack Surface Management monitors and analyzes all potential entry points into an organization's digital environment. It actively monitors the external attack surface to identify vulnerabilities, misconfigurations, and unauthorized changes that could be leveraged by a threat actor to initiate an attack against the customer's environment.

4.1.4 Cloud Security Posture Management (CSPM)

Cloud Security Posture Management (CSPM) continuously monitors and evaluates Azure and AWS cloud environments for misconfigurations and compliance violations against security best practices and regulatory frameworks. It detects vulnerabilities like open storage buckets, excessive permissions, and unencrypted data, while offering real-time remediation guidance.

4.1.5 Vulnerability Management (VM)

Vulnerability Management periodically scans the customer's environment for known security vulnerabilities. Using various detection methods, it identifies unpatched software, misconfigurations, open ports, outdated protocols, and exploitable vulnerabilities in real time. The scanner compares the system's state against regularly updated vulnerability databases (e.g., CVE) and produces detailed reports on identified vulnerabilities, providing prioritized insights based on severity and potential impact.

4.1.6 Proactive Exposure Hunts

In addition to the continuous exposure monitoring done automatically by the technology layer, WithSecure will proactively conduct manual exposure hunts against our customer's environments. These are correlated with various global and regional Threat Intelligence feeds, enabling proactive identification of emerging risks before they materialize into active threats.

The Exposure Hunts focus on new or emerging threats, which have either:

- have gained traction in media, security and research community
- are considered high-risk by WithSecure Threat Intelligence department

These proactive exposure hunts do not require customer or partner involvement. At the end of each Threat Hunt, the results of the findings are shown in the Elements Security Center, including whether the customer is impacted, any related information and our recommendations for remediation.

If the customer needs support in interpreting the results of the Exposure Hunt(s), or assistance in risk assessment, it is available on-demand via Elevate to WithSecure. Additional and/or tailored Threat Hunts can be acquired separately.

4.2 Exposure Risk Prioritization

The exposure findings across the environment are prioritized using their remediation impact to the overall company risk score and thus exposure to cyber threats, based dynamically on multiple factors and datapoints highlighted below.

Prioritization is enriched by the manual weighting given by the WithSecure Exposure Management team, which emphasizes findings that align with the organization's strategic objectives, including compliance and operational requirements

4.2.1 Severity Ratings

The prioritization leverages established scoring frameworks, such as the Common Vulnerability Scoring System (CVSS), to assign a base severity score to each finding. This considers factors such as availability of public exploits, exploit maturity, compromise impact, and complexity of the attack.

4.2.2 Attack Surface

The product determines whether the finding is externally exposed, such as being accessible via the internet or across unsegmented networks. Publicly exposed vulnerabilities receive higher remediation priority, as they are likely to be used by the attacker to gain foothold in the environment.

4.2.3 Asset Criticality

The criticality of the affected asset is evaluated based on its role within the organization and its business operations. For example, findings in systems hosting sensitive data, critical applications, or production environments are given higher priority.

4.2.4 Attack Path Mapping

Attack Path Mapping simulates attack paths that an attacker could take to compromise a customer's estate, increasing the risk of vulnerabilities, misconfigurations and other security gaps on those attack paths.

With AI-powered adversarial attack path simulation, the attack paths are built on heuristic scoring through the lens of the attacker, prioritizing things like exploitability and possibility for lateral movement, privilege escalation, or chaining of vulnerabilities. This makes the attack paths significantly more credible, unlike simple an inaccurate 'shortest-route-to' models.

4.2.5 Threat Intelligence Correlation

Correlation of exposure findings to global threat intelligence feeds allows the prioritization of those findings that have been actively exploited in the wild in recent or ongoing attack campaigns.

4.2.6 Compliance Requirements

Findings linked to non-compliance with regulatory frameworks (e.g., PCI DSS, NIS2, GDPR) or organizational security policies are prioritized for immediate remediation to avoid penalties or operational risks.

4.2.7 Actionability and Feasibility

Vulnerabilities and misconfigurations with available and tested patches or simple configuration fixes are prioritized due to their ease of remediation. Findings that require coordinated changes across multiple systems or dependencies are evaluated for phased remediation, ensuring they are addressed in alignment with resourcing constraints, balancing high-impact fixes against organizational capabilities and timelines.

4.3 Remediation Roadmap

WithSecure Exposure Management team will facilitate the creation of a remediation roadmap and recommended actions, which allows the customer to address found issues according to their priority. The remediation roadmap can be referenced for audits, compliancy reporting and iterative improvements in the subsequent CTEM cycles.

These actions include deploying software patches, modifying configurations, applying access control policies, or implementing compensating controls such as network segmentation or monitoring rules, ensuring that the remediation efforts are both practical and effective.

The remediation roadmap emphasizes high-risk and/or easy to remediate findings to minimize immediate exposure. Where fixes are unavailable or infeasible, the team will also suggest alternative risk mitigation strategies, such as disabling vulnerable services, enhancing monitoring, or introducing temporary compensating controls. Clear ownership must be established on the client side for remediation task to provide accountability and efficiency to the CTEM process.

4.4 Remediation and Validation

Through the patch management capability of the Element platform, the client can orchestrate and deploy software patches to managed Windows endpoint devices, significantly streamlining the remediation process and reducing exploitable attack surface. This allows the customer's internal administrators to focus their time and resources on more complex remediation actions which require manual intervention.

Validation of remediation actions is an integral part of the CTEM process. Subsequent monitoring will validate that the actions were conducted successfully without introducing new exposure findings.

4.5 Exposure Review and Reporting

An Exposure Review session is held quarterly during the online Service Review meeting, together with key stakeholders from the customer's IT leadership, Security Operations and IT Administration. During the meeting, organization's exposure risk is reviewed through clear KPIs, reports and actionable insights that supports the client's strategic decision-making and operational requirements, focusing on:

- Review customer's current security posture and effectiveness of previous remediation actions, trends and associated scope of risks, including the possible non-compliance to regulatory standards.
- Review the priority and impact of recommended remediation actions, so that appropriate budget and resource allocation is given to the most effective and necessary remediation actions.
- Improving communication between decision-makers, security teams and IT teams so that operational teams and executives are on the same page concerning risk and remediation priority.

4.5.1 Exposure Management Projects

When the client requires support that is beyond the scope of the CTEM service, such as:

- delivering an in-depth strategic remediation plan that is tailor-made to the organization's infrastructure, operational requirements and business objectives (e.g. acquisitions, migrations),
- supporting complex remediation processes which require sequential remediation or coordination across multiple customer teams,

WithSecure will request the client to provide a signed Statement of Work (SoW) for the additional project, defined jointly together with the customer, before additional resources are assigned to the project.

5 ENDPOINT PROTECTION, DETECTION, RESPONSE (xDR)

WithSecure Infinite includes build-in Endpoint Protection, Detection and Response capabilities (EPP, EDR), which has an exceptional track record in threat detection in real-world scenarios and preventing 100% (AV-Test) of tested ransomware, 0-day malware and other malware facing modern companies.

These advanced security capabilities allow WithSecure Threat Analysts to focus on detecting and responding to threats, which aren't addressable with traditional endpoint and network security solutions, such as advanced and persistent threats (APT), attacks using zero-day exploits or legitimate software, and skilled threat actors using novel tactics, techniques and procedures (TTP).

The primary security capabilities are listed, but not limited to, below:

- **Signature-Based Detection**: Employs traditional antimalware techniques to identify known threats using multiple signature databases, supported by cloud reputation queries and runtime behavioral monitoring for enhanced accuracy.
- **Cloud-Based Reputation Services:** Real-time cloud reputation queries provide always up-to-date protection against emerging threats.
- **Behavioral and Heuristic Analysis:** Runtime monitoring of application, script and process behavior down to the kernel level allows identification of malicious activity and deviations from benign baseline activity, even in case of fileless attacks or use of legitimate software.
- **Machine Learning (ML) Models**: Utilizes advanced machine learning (ML) models trained on vast telemetry and threat datasets to detect malicious anomalies and novel, modified or polymorphic malware strains.
- **Threat Intelligence (TI):** Leverages global threat intelligence data and feeds for real-time threat correlation, identifying emerging indicators of compromise (IoCs) and tactics, techniques and procedures (TTPs), in addition to enriching detections and providing contextual insights on potential threats.
- **Ransomware Protection and Rollback:** Monitors specifically unusual file encryption activity and deletion patterns indicative of ransomware, blocking the process in real time, and reverting affected files to their pre-attack state from local cache.

For full list of security capabilities, please refer to WithSecure Elements product guide.

The use of the Endpoint Protection (EPP) capabilities is optional, and their daily use and management is the responsibility of the customer, or the partner managing their IT environment on their behalf. This enables the joint use of a 3rd party endpoint security products together with WithSecure Infinite, in case of multivendor policy for example.

WithSecure provides the Endpoint Detection and Response (EDR) capabilities as a Managed Detection and Response service (MDR) as part of the WithSecure Infinite.

WithSecure Elements EDR tested by AV-TEST (July 2024)
WithSecure Elements EPP tested by AV-TEST (September - October 2023)
Threat Protection (ATP) in October 2023)

6 MANAGED DETECTION AND RESPONSE (MDR)

WithSecure Infinite provides SLA-backed 24/7 managed detection and response (MDR) service, which leverages the broad context detections (BCDs) and response capabilities of 'WithSecure Elements EDR'.

The primary service elements are as follows:

- **Continuous Threat Monitoring:** Maintaining constant 24/7 watch over customers' IT environment for any suspicious or non-baseline activity, indicators of compromise (IoCs) and potential compromises.
- **Threat Investigation:** Indept investigation and analysis of such activity to identify potential security incidents and validating them to establish if they are true positive incidents that require action to remediate, and which can be closed without disturbing the client.
- **Incident Coordination:** Escalation of confirmed security incidents to the correct customer representative(s), and/or to the customer's IT partner managing their environment, in order take coordinated action in responding to the security incident.
- **Incident Response:** Taking decisive and appropriate investigation, containment and eradication actions on behalf of the customer, according to the SLAs and authorizations given, in order to contain and remediate the detected security incident.
- **Retainer Activation:** Evoking SLA-backed access to additional skilled incident response resources, in case a major cyber security breach occurs.

Throughout the service delivery, WithSecure Threat Analysts can provide on-demand assistance, such as interpretation of a detection or threat hunt, or investigating a host that is not included in a security incident.

The following sections describes the service elements in more detail.

6.1 Threat Detection

Broad Context Detections (BCDs) within the WithSecure Elements Platform are generated through systematic analysis and correlation of sensor telemetry, threat intelligence and cloud lookups, among others. This data is analysed to identify anomalies and patterns of activity that may pose a risk.

Suspicious or potentially harmful BCDs are escalated to a human-led Threat Investigation process, where experienced WithSecure Threat Analysts assess the context and determine whether further action is necessary.

Once a BCD is generated, its initial status is set to 'Monitored', indicating that no immediate action is required from the client or their authorized IT partner. However, all BCDs remain visible in the Elements Security Center (ESC) to allow for optional review and awareness.

If a specific BCD—or a combination of multiple BCDs—is deemed to require client or partner intervention, it is clearly highlighted in the management console. This console also provides visibility into which BCDs or BCD groups are actively under investigation, and which have already been closed following analysis.

6.1.1 Risk Level

'WithSecure Elements Platform' uses 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 identification of malicious techniques, tools and processes (TTP) used by threat actors.

These include, but are not limited to, things such as:

- anomalies, spikes, dips and/or patterns found in the telemetry of the asset(s) and their network connections,
- abnormal activity of standard programs, running unexpected scripts and unexpected running of system tools from standard processes
- cross-referencing the telemetry and detection data against the threat intelligence we are seeing globally in our detections and IR operations

Note that BCD risk scores are dynamic, meaning that the score can increase or decrease as investigation continues or more suspicious or malicious activity is detected;

- A low-risk BCD may become high risk and trigger threat investigation as more information becomes available.
- A high-risk BCD may be downgraded during investigation if deemed low risk.

6.1.2 Proactive Threat Hunts

In addition to the continuous threat detection done automatically by the sensors, WithSecure will proactively conduct manual Threat Hunts against our customer's environments. These proactive Threat Hunts do not require customer or partner involvement, and their outcomes are visible in the Elements Security Center.

Threat Hunting is the process of proactively looking for threats in customer environments that may have bypassed existing security controls. Given that attackers are constantly seeking ways to evade these controls, it is necessary that these gaps are quickly identified and plugged with new detection capabilities.

The basic premise of Threat Hunting is to assume that the organization has already been breached, to identify evidence that supports the theory and then develop a detection use case that will automatically detect that activity in future. The process is outlined below:

1. Combination of independent research, threat intelligence output and data from live incidents are used to develop hypotheses on how the behaviors, TTPs and IoC of an emerging attacker might look like, and how they could be detected.
2. A manual Threat Hunt is conducted to detect the activity and identifiers across the whole Infinite customer base, and how it could be further developed and automated.

3. If no malicious indicators or identifiers are found in customer environments, the Threat Hunt is concluded.
4. If malicious indicators are found in the customer environments, a security incident is created, which follows the standard incident response process and escalation procedures
5. Any possible improvements or additions are added to the detection logic at the conclusion of the Threat Hunt.

6.2 Threat Investigation

Once a Broad Context Detection (BCD) reaches a threshold to warrant an investigation, a Threat Investigation process is triggered, in which a Threat Analyst will manually conduct a deeper analysis into the target endpoint, identity or cloud service. Our built in GenAI Investigation Assistant, Luminen, may also be used autonomously by the client to obtain a clear language description of any BCD.

The Threat Investigation process analyses the BCD(s) of the target(s) using, among other things, the telemetry available from the target. This data is collected either passively by the Elements Agents or integration with Entra ID, or via investigation response action(s) triggered by the Threat Analyst to further aid investigation. See Section 6.4 for more information about Response Actions.

Each investigation is categorized to the following four categories:

- genuine threat or security incident, which requires urgent escalation to the client's contact person(s) and/or immediate incident response actions.
- suspicious activity, which doesn't require urgent escalation and immediate response actions, but should be monitored, and reacted to by the client when available.
- accepted behavior, where suspicious or risky activity is accepted by the client as legitimate behavior in the system.
- false positive, that does not require attention from the client.

If the BCD is confirmed as a genuine threat or security incident, WithSecure Threat Analyst will change the status to 'Awaiting Client', triggering automatically the escalation process described in Section 6.3.1 This is followed in parallel with immediate initiation of appropriate Containment and Remediation actions described in Section 6.4.

If the BCD is deemed suspicious, but which doesn't require urgent escalation or immediate incident response actions, WithSecure Threat Analyst will change the status to 'Awaiting Client' which triggers automatically the escalation process described in Section 6.3.2

If the BCD is deemed suspicious, but eventually accepted and confirmed by the client as acceptable behavior in the context of their environment (for ex. admin user has an acceptable reason for the suspicious looking activity), the BCD is closed with 'Accepted Behavior' resolution.

If the BCD is deemed false positive, it was investigated and subsequently deemed benign activity which doesn't pose risk to the environment. False positives are never escalated. They are closed by the Threat Analyst using 'False Positive' resolution. The client can see auto-closed BCDs by filtering using the 'Auto False Positive' resolution.

'Accepted Behavior' and 'False Positive' resolutions automatically create appropriate suppression rules, which automatically accept or clos BCDs with similar behavior from the same user or process.

Automatically suppressed BCDs can be found by filtering using ‘Auto False Positive’ and ‘Auto Accepted Behavior’ solutions.

This refinement process allows WithSecure to continually enhance the accuracy of the detection rules and algorithms, ensuring outmost fidelity in detection capabilities within the client environment.

6.3 Incident Escalation

If the Broad Context Detection (BCD) is confirmed to be a genuine threat or security incident, or activity requiring action from the client, WithSecure will escalate according to the processes described below. All clients are encouraged to enable notifications in the Elements Security Center to receive timely updates

6.3.1 Security Incident

Any genuine threat or security incident (also called true positive), and suspicious activity deemed risky enough to warrant escalation, is immediately escalated to the emergency contact person(s) or team(s) explicitly designated and authorized by the client.

The escalation process works as follows:

- An automatic email notification is sent to the designated email address(es), when a BCD is set to ‘Waiting for Client’ status.
- In parallel, the Threat Analyst will contact each of the designated phone number(s) in their defined priority order.
- Once a designated emergency contact is reached and alerted of the incident, the engagement with the initiating Threat Analyst and members of the WithSecure Detection and Response Team (DRT), is moved to the Elements Security Center
- From there on, any communication, coordination, collaboration and requesting authorizations needed in responding to the incident, are then managed in the comments section of the relevant BCD.
- In case the designated contacts are unresponsive, any pre-approved remediation steps may be taken.

6.3.2 Suspicious Activity

If the investigation deems the activity suspicious, but not requiring urgent escalation or immediate incident response actions, the client receives automatic notification of the activity requiring action. It is then managed when the client becomes available.

- An automatic email notification is sent to the designed email address(es), alerting them of a BCD requiring action.
- Any communication, coordination, collaboration and requesting authorizations are then managed in the comments section of the relevant BCD, when the client becomes available.

6.3.3 No Escalation

Investigations that result in False Positive' resolution, and any BCDs automatically closed by suppression rules, are recorded in the portal for clients to review if required. They are never escalated in order to ensure minimum client disturbance.

6.4 Incident Response

If the Broad Context Detection (BCD) is confirmed to be a genuine threat or security incident, the Threat Analyst will in parallel to the Incident Escalation process begin immediate and decisive first response measures, using appropriate response actions within the parameters of authorizations given. These include, but are not limited to, the following:

6.4.1 Manual Response Actions

WithSecure Threat Analysts may manually use any native response action provided by 'WithSecure Elements Platform' to conduct the necessary investigation, containment, and remediation actions.

6.4.1.1 Investigation Actions

These actions are used to investigate the environment, the attack, the TTPs that the attacker is using, and therefore are often done prior to the other response actions. These include retrieving a forensics package and related information, retrieving memory dumps and other useful artifacts and enumerating processes/services/WMI objects from the target(s).

6.4.1.2 Containment Actions

These actions are used to actively prevent attackers from continuing their objective and propagating in the environment, once an incident has been confirmed. These include killing processes and threats in the host, in addition to isolating it from the network.

6.4.1.3 Remediation Actions

These actions are used to remove persistence mechanisms from endpoints that have been installed by an attacker to ascertain a foothold on an IT estate. They include deleting files, folders, registry keys/values, and Windows Management Instrumentation (WMI) objects related to persistence from host(s).

Given the risks of potential business impact that Incident Response actions present, WithSecure may require authorization before using said actions. See Section 6.5 for more information.

Please note that availability and scope of response actions vary between endpoint operating systems, identity management systems and cloud computing platforms, due to their technical differences. Full list of available response actions per operating system can be found from the Elements User Guide.

6.4.2 Automated Response Actions

Where available, and prior authorized by the client, WithSecure may automate use of the above response actions using conditional triggers provided by the Elements Platform to enhance speed of response measures. For example, a target host could be automatically isolated when a highly suspicious BCD is created.

6.5 Authorizations

Client authorization is required for WithSecure to carry out certain response actions when responding to a live security incident, given their intrinsic risks and potential business impact that these disruptive actions present. For example, there is a small possibility that when using these mechanisms, a service, identity, task or registry key will be processed inappropriately, which can lead to problems ranging from system slowness to an eventual crash.

It should be explicitly noted, that while the risk of such an impact may be low, client explicitly understands and accepts these risks when using the service. Similarly, assessing the wider business impact is always responsibility of the client providing the authorization to conduct said response actions.

The authorizations should be provided by the client in advance in their broadest extent possible, as the lead-time in obtaining needed authorizations will delay critical containment and remediation actions, which in turn will significantly increase the risk of major business impact during a cyber security incident.

The Threat Analyst will always endeavor to minimize potential impact to client operations and can describe the immediate localized consequence(s) of a response task when requested. Whilst authorization is required for some actions, it does not imply that these actions will always be executed. The Threat Analyst will decide on execution of the said actions case-by-case, weighting the benefits against several factors, including but not limited to, scope of the service, risk of further disruption, risk of data loss etc.

The authorizations fall into the following categories:

6.5.1 Unrestricted Actions

Unrestricted response actions are by nature mostly non-disruptive to the environment and business processes of the client. Seeking approval for these administrative and informational actions would prohibitively impede service delivery and quality, due to the time sensitive nature of a potential security incident, without comparative benefits. All Investigation Actions belong to this category.

The use of Unrestricted Actions is not limited, does not require authorizations, and clients are not actively notified of their use.

6.5.2 Authorized Actions

Given the disruptive nature of majority of the Containment and Remediation actions, and inherent risks of potential business impact that these actions present, WithSecure requires authorization from the client before proceeding with the aforementioned measures.

Needed authorization can be provided in one of the following ways:

6.5.2.1 Pre-Authorization

By default, pre-authorization is provided for all workstations at organizational level. This means that for incidents involving workstations, Containment and Remediation tasks are pre-authorized by default.

By default, pre-authorization is not provided for servers, due to the greater potential impact on the client's IT estate or business operations.

If the client wishes to adjust the default pre-authorizations, they can choose between the following options on an organizational level:

- Workstations (All)
- Workstation and Servers (All)
- No Pre-Authorization

Hosts are classified as a workstation or server according to the operating system installed on the endpoint, as follows:

Operating System type	Classification
Windows Workstation	Workstation
Windows Server	Server
MacOS (All versions)	Workstation
Linux (All versions)	Server

6.5.2.2 Explicit Approval

Where prior pre-authorization does not apply, for example for servers, 'Explicit Approval' is required prior to the submission of any Containment or Remediation activities. 'Explicit Approval' can be provided over the phone by client's pre-designed contact person(s) or team(s), or by adding a comment to the BCD within the Elements Security Centre.

6.5.2.3 No Authorization

In a situation where the Threat Analyst does not receive an 'Explicit Approval', and prior pre-authorization does not apply, the Threat Analyst will not conduct response actions on behalf of the client.

6.6 Retainer Activation

In case the cyber security incident meets the 'Major Incident' described below, Threat Analyst will recommend an escalation to WithSecure Incident Response team, in order to access additional resources needed to contain the incident in a timely and effective manner.

As a result of seamless and well-practiced processes, in addition to familiar in-house teams, technologies and telemetry, the transition from initial containment and triage activities to full-blown incident management is significantly faster and efficient. This leads into considerable time and cost savings for the client, in addition to improved security outcomes.

6.6.1 Major Incident Definition

'Major Incident' is considered reached, when any one of the following conditions is met:

- A business-critical asset has been compromised, i.e. an asset that if taken offline would wholly impede the customer's business operations (critical production machine, domain controller, exchange server etc).
- The extent of a compromise is such, that the normal business operations of the client are jeopardized or impeded.
- A compromised device has been identified that does not have WithSecure Elements EDR coverage and/or the infection vector originates from a host that WithSecure Elements EDR has no visibility to
- Incident Management would require coordination from multiple Client's internal teams and/or collaboration with external parties such as law enforcement or hosting partner.
- Incident Management would require on-site assistance
- Incident Management would require work, which goes beyond immediate short-term triage and containment, such as full disk forensics or root cause analysis

7 INCIDENT RESPONSE RETAINER (IR)

WithSecure Infinite customers have SLA-backed (4h), on-demand access to skilled Incident Response resources, via the included WithSecure Incident Response Retainer service. These resources are used to cover incident response activities beyond the scope of the WithSecure MDR, such as assessing the broader business impact of a detection, performing analysis on devices not covered by the Elements Agent, or analyzing data from 3rd party sources such as firewalls.

Similarly, in case the cyber security incident meets the 'Major Incident' described above, Threat Analyst will recommend an escalation to WithSecure Incident Response team, in order to evoke the additional resources needed to contain the incident in a timely and effective manner.

WithSecure Incident Response Retainer includes one (1) WithSecure First Response Package and one (1) additional Incident Response Day per each contract year. Additional First Response Packages and Incident Response Days can be acquired separately.

7.1 First Response Package

WithSecure 'First-Response Package' is designed to provide immediate support by a team of IR specialists during the critical first three (3) days, to a total of 36h of incident response over those three days. In addition to providing immediate investigation and containment support to ensure the business continuity of the client, WithSecure also provides the client with an initial scope of the incident and an estimate of the effort required to remediate accordingly.

During the initial hours of the incident, WithSecure's IR team will engage with the client teams to review the available data sources to assist with containment and remediation actions to ensure ongoing business activities. Further tasks performed as part of the First Response Package include, but are not limited to, evidence preservation, incident management, stakeholder liaison, and threat identification where possible.

During the delivery of the 'First Response Package', WithSecure provides the client with the following:

- An immediate assessment of the available information to validate the compromise and gauge the scope and nature of the incident at hand;
- Initial advice for immediate containment and remediation actions to mitigate an ongoing incident and to ensure client's business continuity (As an example, this could changing firewall rules or using pre-deployed technologies to limit threat actor actions);
- Guidance for preserving evidence that is required for investigation;
- Initial analysis from the collected evidence (system data, log, or malware analysis);
- A summary of key actions and advice provided at the end of the FRP engagement;
- A follow-on Statement of Work for the possible remaining work relating to the investigation along additional work requested by the client.

The First Response Package is limited to 12 hours of Incident Response consultancy per calendar day for three calendar days, split between one or more consultants.

The client can continue the investigation following the use of the First Response Package by consuming Incident Response Days or initiating an Incident Response with an associated standard Statement of Work.

The client can top up their retainer with additional First Response packages in the following cases:

- When the initial retainer contract is made or renewed;
- In case of a multi-year retainer, at the start of each new contract year.

7.2 Incident Response Days

The client can use 'Incident Response Days' for *ad hoc* IR related tasks or to continue a response after a First-Response Package.

The client can top up its retainer package with Incident Response Days as necessary. The client can use Incident Response Days at any time during the contract, or as part of an Incident Response Project. Clients with Incident Response Retainers benefit from lower IR day-rate costs, as compared with WithSecure's non-contracted (walk-in) clients.

7.3 Incident Response Project

When the client requires IR support that is beyond the scope of its First Response Package and the Prepaid IR days are not enough to cover the support scope, WithSecure will request the client to provide a signed Statement of Work (SoW) before any further efforts are expended on the case.

WithSecure's Incident Response team defines with the client the scope of SoW, including the project's objectives, size and duration. WithSecure Incident Response teams support both SANS and NIST IR lifecycle standards, delivering the defined outcomes according to the industry best practices.

To benefit from faster turn-around and service quality, any Incident Response Project needs to be initiated through the dedicated, SLA-backed escalation paths meant for contracted clients. Non-standard contact methods or use of channels meant for non-contracted clients (walk-ins) are not guaranteed to reach the team in agreed speed or quality.

8 ELEMENTS PLATFORM ACCESS

As part of WithSecure Infinite service, IT administrators and security operations teams managing the protected environment are granted access to the underlying security and management platform, called WithSecure Elements.

It provides the teams with comprehensive management, reporting and GenAI tools that enable organizations to independently maintain robust security operations, streamline administrative tasks, make informed prioritizations and decisions based on real-time security insights.

The platform forms the foundation for effective collaboration with WithSecure's cybersecurity personnel, from responding 24/7 to cyber security incidents and improving the customers security posture, to providing on-demand assistance where needed.

8.1 Luminen (GenAI)

WithSecure Luminen is a Generative AI (GenAI) capability integrated into the WithSecure Elements platform. It utilizes advanced Large Language Models (LLM) to provide natural language explanations of security events and Broad Context Detections (BCD). Luminen summarizes security events and offers actionable recommendations, aiding IT and cybersecurity teams in managing complex tasks.

The Investigation Assistant within Luminen helps clients IT and security teams by providing detailed analysis of security incidents. It offers insights into the nature and scope of threats, helping teams understand the root causes and potential impacts.

The Awareness Assistant is designed to enhance the cybersecurity knowledge of IT teams. It provides educational content and updates on the latest threats and best practices. By keeping teams informed, the Awareness Assistant helps organizations maintain a proactive security posture, reducing the risk of successful attacks.

8.2 Exposure Management (XM)

The platform provides access to customers exposure data, providing extensive information to the customers vulnerabilities, misconfigurations and outdated software across their IT environment, covering its external attack surface(s) (EASM), identity management systems (EntraID), physical endpoints, corporate networks and cloud environments (AWS, Azure).

The findings are prioritized for remediation based on business impact, and relevant remediation and mitigation recommendations are available for all findings. On-demand assistance is provided via the Luminen GenAI and Elevate to WithSecure capabilities.

Through full access to customer's prioritized exposure data, remediation recommendations, and on-demand assistance, the client's security and IT teams can act independently outside of the Continuous Threat Exposure Management (CTEM) service delivered by WithSecure, if they so wish.

8.3 Asset Management

The platform provides continuous real-time discovery and cataloging of endpoints and other devices in the customers environment, and supports detection for both managed and unmanaged workstations, mobiles, servers and other devices such as switches, routers and OIT devices within the customer's network, and dynamically classifies the assets based on type, operating system and installed software.

The collected asset data is shown in the portal, encompassing hardware specifications, firmware versions, and installed applications, including any relevant security information such as vulnerabilities, misconfigurations and detections related to the device. The portal supports also custom tagging and grouping to organize assets for example by departments, geographies, or business units.

Available data varies depending on capabilities deployed to the environment, access rights given to data sources (such as AD), network access of service components and presence of the Elements Agent.

8.4 Incident Management

The platform provides access to customers prioritized threat telemetry data, detections and live security events, in addition to advanced search and query functionalities to filter and locate specific events, endpoints or detection in the environment, and attack visualization tool to show data, timelines and progressing of attack in an easily digestible format. On-demand threat investigation assistance is provided via the Luminen GenAI and Elevate to WithSecure capabilities.

Through access to customer's prioritized incident data in an easily digestible visual format, in addition to search and query tools, and on-demand investigation assistance, the client's security and IT teams can act independently to address security incidents and conduct threat hunts outside of the Managed Detection and Response (MDR) service delivered by WithSecure, if they so wish.

8.5 Central Management

The management console of the platform provides centralized views, reports and dashboards that unifies management, security operations and collaboration with WithSecure personnel into one single-pane-of-glass interface. The management console supports SSO login using Entra ID.

Multitenancy and three-tier hierarchy allows large organizations to manage multiple business units or offices within a single platform instance, for each of which access, visibility and management rights can be customized per user or user group using Role-Based Access Control (RBAC).

Customer's administrators can also create, customize, and deploy template-based policies for various organizational units, device groups, or users, while granular configuration settings allow precise adjustments to behavioral analysis thresholds, device control rules, and web protection settings, ensuring tailored and robust security management.

The platform maintains detailed logs of all platform activities, including policy changes, user logins, scanning and deploying missing patches, and actions taken on incidents, ensuring accountability.

8.6 Automation and Orchestration

Through the security platform, the customer's IT and security teams can centrally automate and orchestrate various workflows, such as setting up pre-configured responses for detected threats, initiating scans, deploying patches or sending reports to selected recipients at predefined intervals, all of which will significantly reduce the manual overhead of the teams managing the environment. The platform also supports customer-driven, API-based integration with third-party tools like SIEM (e.g., Splunk, QRadar) and SOAR solutions, enhancing orchestration capabilities.

8.7 Advanced Reporting

Through the platform, customer's IT and security teams have access to extensive and customizable reporting and alerting capabilities. This includes the ability to create multiple customizable dashboards based on the predefined templates, widgets and data sources, creation of manual .pdf reports based on those dashboards, in additional to the possibility to automate generation and delivery of customizable reports to designated recipients at predefined intervals.

9 CUSTOMER SUCCESS MANAGEMENT

WithSecure's Customer Success team is responsible for delivering the Infinite service against the defined customer journey, and ensuring it is aligned to the customer's expectations through continuous communication, regular meetings and feedback collection.

9.1 Customer Success Manager

Each WithSecure Infinite customer is provided a named Customer Success Manager (CSM), who is the single-point-of-contact for the customer in general queries, escalations and service issues.

9.2 Deployment Support

During deployment of WithSecure Infinite, each customer is supported by a Technical Project Manager, alongside their named Customer Success Manager, who will assist during the deployment and onboarding of the service. The support includes:

- Kick-off meeting (2h) with the customer's technical resource to discuss the deployment and onboarding steps, related best practices and deployment phasing.
- Two (2) follow-up meetings (1h) to monitor the deployment progress and to share best practices on how to configure the Elements portal to fit the Customer's needs.

WithSecure will also provide an in-depth Product Guide, which will outline all the prerequisites for the installation and steps how to install the agent across various Operating Systems. The Product Guide also includes most common troubleshooting advise and FAQ.

9.3 Quarterly Service Reviews

During the delivery of the service, Service Reviews are arranged together with the customer's internal stakeholders, such as Security Operations, IT and Management. Service Reviews are arranged quarterly (4) during each contract year. The Service Reviews contain:

- General discussion on customer satisfaction to service delivery, in addition to feedback collection and updates in customer's environment and any possible housekeeping updates.
- Deep dive into the customers security events and security posture
    - Volumes, trends and benchmarks of various detections, findings and recommendations, in addition to other insights drawn from the customer data.
    - Review of threat investigations conducted by WithSecure, confirmed security incidents and actions done to remediate them.
    - Review of security posture weaknesses discovered by WithSecure, their contextual priority and recommendations for remediation and/or mitigation, and follow-up on mitigation action.
    - Review of Threat and Exposure Hunts conducted by WithSecure, their outcomes and recommendations for remediation and/or mitigation.
- Sharing best practices on how to get the most out of the Elements platform, and how to maximize value from the tools and the service.

9.4 Monthly Meetings

Between the Service Reviews, if the customer wishes so, Customer Service Manager and customer can meet monthly to have more generic service catch-up call to go through any open topics.

9.5 Technical Support

Outside of the Quarterly Service Reviews and Monthly Meetings, the customer is entitled to priority access to higher tiers of technical support according to respective SLAs. Please refer to WithSecure Technical Support service description for details.

9.6 Elevate to WithSecure

WithSecure Elevate tokens that are provided with the service can be used to contact WithSecure subject matter experts in non-urgent questions to receive more in-depth information, support with interpretation of an incident or threat hunt, and assisting with risk assessment.

For example, the customer or their IT-partner managing the environment for them, can use the included Elevate tokens included to ask a question about:

- a BCD that has been closed as a false positive, or
- a BCD that has not been included in an investigation,
- confirming detection coverage or querying about a missed detection,
- remediation and/or mitigation assistance with a vulnerability,
- investigate a host that is not included in the original incident,
- general service query to the customer success team.

WithSecure Elevate tokens can be used for querying about detections and/or findings within 30 days of their creation. If the query is related to an item older that 30 days, the customer must consume an Incident Response Day to cover additional work needed to investigate historical events and logs.

The service includes a monthly quota of ‘Elevate to WithSecure’ tokens, which refill at the start of each 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. Elevate to WithSecure is an additional service that is not required for the functioning of the WithSecure Infinite.

9.7 Pentests and Purple Teaming

WithSecure welcomes any lawful customer-driven penetration and purple teaming exercises against the service and will fully collaborate with the customer and any third-party in such endeavors.

Clients should pre-notify WithSecure of any major penetration testing or purple teaming exercises, to ensure that operational priority is given to investigating and responding to real security incidents and/or ongoing attacks. As such, any testing activity is absolved from SLAs.

WithSecure will respond to queries related to the testing activity based on technical report(s) written in English, provided by the customer and/or third-party testing organization, during the next monthly meeting with the client organized by the Customer Success Manager.

10 SERVICE AVAILABILITY

10.1 Prerequisites

To make use of the service, the following prerequisites must be met. If the prerequisites are not met, the service cannot be delivered, and will remain 'inactive' until the prerequisites are met.

The named Customer Success Manager (CSM) will go through these pre-requisites with the customer in the onboarding phase of the service.

10.1.1 Commercial

- Valid WithSecure Infinite Subscription

10.1.2 Technical

- WithSecure Elements Agent is deployed to all endpoints in client's estate
- WithSecure Elements Agent has the required network connectivity to operate
- Access to WithSecure Elements Security Center
- (Optional): Elements Security Center is connected Microsoft Entra ID via an Event Hub configuration.
- (Optional): Elements Security Center has correct privilege roles in Entra ID to submit Entra ID response actions.

Microsoft's Entra ID and Event Hub, in addition to their access and privilege management, are paid for, managed and maintained by the client.

In case Elements Agent(s) or any other relevant sensor(s) are not deployed to the entire applicable estate, the coverage and quality of the service can degrade. By leaving parts of their estate uncovered and unmonitored, the client decreases their general security posture by reducing available telemetry, detection coverage and limiting the means of responding to incidents. This in turn allows for example the attacker to more easily create beachheads, achieve persistence, move laterally in the environment, and to finally, achieve their goals.

For full technical and network connectivity requirements, in addition information related to Event Hub configuration, please see the Elements User Guide.

10.1.3 Process

It is mandatory for the 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, and the information is 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.

The customer must ensure that 'Advanced Response' is enabled, so the WithSecure team are able to issue response jobs. If response is not enabled, WithSecure will assume that the partner/customer has the correct configuration, and only response guidance will be provided.

10.2 Service Hours

The 'WithSecure Infinite' service is available 24/7/365. Due to the nature of the service coverage, the customer's local time zone or Public Holidays has no bearing on the delivery of the service. Customer can raise issues towards WithSecure as follows:

- Security related issue to the DRT on a 24/7 basis via the phone or Elements Security Center.
- Non-security related issue to Customer Care on a 24/7 basis via the phone or eService Portal.

Customer Success Manager (CSM) is available to during working hours on United Kingdom (GMT+0) and Finland (GMT+2) time zones.

10.3 Service Language

The 'WithSecure Infinite' is available in English only for the purposes of managing security events and support requests. The named Customer Success Manager (CSM) will support the customer in following languages: English, Finnish, German, French.

10.4 Service Delivery Locations

The WithSecure personnel, who deliver the 'WithSecure Infinite' service, are located in Europe in Finland, Poland and United Kingdom.

10.5 Supported Platforms

Supported Windows, Mac and selected Linux distributions, both on workstations and servers, according to the standard WithSecure Life-Cycle Policies, are available at www.withsecure.com.

11 SERVICE LEVEL AGREEMENT (SLA)

The SLA refers to the Response Time (defined below) by WithSecure's Detection and Response Team (DRT) and is only applicable to the WithSecure Infinite service in environments where more than 90% of the applicable hosts are covered by the WithSecure Elements EDR sensor.

11.1 Response Time

"Response Time" means the elapsed time between the creation of an investigation task, and the time the DRT initiates: (i) contact to notify Client of such a detection either via email or phone, or (ii) Response Action for Clients that have pre-authorized response actions.

Response Time will be within sixty (60) minutes for ninety percent (90%) of the aforementioned cases measured monthly, beginning on: (i) the first day of the Service subscription renewal date for existing Clients; and (ii) the first day of the fourth month of provisioning the Service for new Clients.

11.2 Service Commitment

If WithSecure fails to meet the foregoing Response Time more than three times in any rolling twelve (12) month period, then WithSecure shall be deemed to have missed the SLA.

11.3 Service Credits

For each instance of missing the aforementioned SLA, the client will accrue one (1) day worth of service credits, which are redeemable at the end of the contract year as a monetary sum of equivalent value to the days of service accrued.

11.4 Service Exclusions

The above service commitment is given in good faith, in a spirit of partnership and WithSecure shall use reasonable endeavours to rectify an issue in a timely manner. In accordance with industry standard terms, the SLA does not apply:

- To any hardware, software or services not managed by or under the control of WithSecure
- To any hardware, software or services, which has exceeded its End-of-Life date
- During a planned or unplanned maintenance window
- During a planned or unplanned penetration test and/or purple teaming exercise
- A Force Majeure Event

When an incident (an unplanned interruption or a reduction in the quality of our service) resulting in late or absent notification has been caused as a result of the client:

- Using hardware, software or services in a way that is against local laws or security best practices
- Making unauthorized changes to the configuration or set up of WithSecure software or service
- Preventing WithSecure from performing necessary maintenance and update tasks
- 3rd party provider preventing WithSecure software to function as expected by WithSecure
- Breaching of its contract with WithSecure for any reason (e.g. late payment of fees.

12 DATA COLLECTION & RETENTION

In order to deliver the service, WithSecure Elements Agent has to be installed on at least one device. These agents are installed on the customer network by the customer, or their IT partner managing the environment, on devices designated by the Client, 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 Agent collects the following kinds of event-based data from the device it is installed on, referred to 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 with WithSecure. The data is stored for a minimum of three (3) months on rolling basis during the customer engagement and is deleted within three (3) months after termination of the engagement. Longer retention times are available separately.

For full details please refer to the WithSecure Privacy Policy, which is available online or provided upon request.

13 LICENCING

WithSecure Infinite is licensed based on the number of protected endpoint devices. License includes all the necessary technology and service components, including platform access and supporting functions like Customer Success Management, Technical Support, Elevate to WithSecure and Luminen GenAI.

Additional protection modules for Identities (Entra ID) and Cloud Environments (AWS, Azure) are priced and acquired separately. Similarly, additional Incident Response Days and Exposure Management Days are priced and acquired separately.

14 RESPONSIBILITY MATRIX

The table below outlines the responsibilities of WithSecure and the client organization and/or their contracted partner managing their environment:

Task	WithSecure	Partner/ Customer
Ensuring the onboarding documents and agent installers are available	Responsible	
Installing the Elements Agent on 90% of endpoints to activate SLA		Responsible
Installing optional scan nodes and provide access to cloud resources		Responsible
Managing deployment of Elements agent across the environment		Responsible
Ensuring the escalation contact information is provided and maintained		Responsible
Ensuring 'Advanced response' is enabled on all relevant endpoints		Responsible
Ensuring data collection mechanisms are deployed for any additional modules included		Responsible
Monitoring and maintaining Elements Agent to Elements Platform connectivity on the desired set of endpoints		Responsible
Issuing automatic upgrades to the Elements Agent to develop detection capability and improve performance	Responsible	
Ensuring Elements Agents are online and working, including the successful installation of automatic updates.		Responsible
Ensuring that the Elements Security Center is deployed, available and maintained	Responsible	
Providing 24/7 detection and response across a corporate IT estate using the elements agent	Responsible	
Performing investigations into suspicious activity, containing and reporting confirmed incidents according to SLA and process.	Responsible	
Ensuring Elements Security Centre Incident Email Notifications are configured		Responsible
Providing confirmation of pre-authorized response scope		Responsible
Providing continuous monitoring of customers exposure to cyber threats and prioritizing them for remediation actions.	Responsible	
Assigning internal ownership and executing necessary remediation actions		Responsible
Provide technical support when customer has service issues and/or technical escalations	Responsible	
Organizing and scheduling service reviews	Responsible	

WITH secure

CLIENT RESTRICTED