Virsec Platform and Services SLA

1. Overview of the Support Service

This page describes the support for Virsec Platform (the "Support Services").

These support services have two major components: Service Delivery and Service Assurance, as described in further detail below. Virsec may provide supplemental services as described in an addendum to this Annex as purchased by Customer pursuant to any mutually agreed upon ordering documents. For the avoidance of doubt, the Virsec Platform covered by this Annex comprises the following components: CMS, Probe.

The Support Services described cover one instance of the Virsec Platform.

The table below provides a short glossary of any terms crucial to the understanding of this document, and lists the acronyms and abbreviations used in the document. Any other capitalized terms not defined herein shall have the meaning provided to them in the End User Service Agreement and any other contractual reference to MPA (Master Purchase Agreement).

Term	Definition
CMS	Cloud-based central management system that probes connect to for policy distribution, incident collection, and centralized security control.
Probe	Virsec software agent installed on customer workloads that provides enforcement (security monitoring/protection).
CPM	Central Probe Management software installed on customer workloads that provides out-of-band management for remote operations.
Customer Infrastructure	workloads a probe is deployed to in order to deliver Detect and Protect functionality
Error	means a situation where the Virsec Platform does not behave as the end user expected.
Incident	means an unplanned interruption to the Virsec Platform or a reduction in the quality of the Virsec Platform services

Request For Enhancement	means a request to modify or enhance the Virsec Platform.
Service Request	means a request from for information, advice or help with the Virsec Platform
Update	Changes to the software used in the Virsec Platform, including but not limited to error corrections, bug fixes and other enhancements. Unless specifically agreed, Updates shall not include any release, option or future product which Virsec licenses separately or which is not included under the applicable level of support.
Upgrade	Changes to the software used in the Virsec Platform that includes new features and functionality. New features may require additional licensing. Upgrades may also include Updates.

2. Customer Operations

Customer operations covers both the pre-deployment phase of the implementation of the Virsec Platform, prior to commercial launch by Customer and various ongoing engagement management services post-launch.

2.1 Customer Responsibilities

Customer is responsible for the following aspects of probe management and day-to-day platform operations:

Infrastructure and Installation:

- CPM installation and uninstallation on customer workloads
- Underlying workload health and performance monitoring
- Network connectivity and access permissions for CPM operations
- Infrastructure management and performance issues not caused by probe software

Platform Operations:

- Asset management and inventory tracking
- Security metrics monitoring and analysis
- Incident triage and response coordination
- Daily CMS operations and configuration management
- User access management and administration

Optional Self-Service Tasks *(Customer may perform these tasks themselves or request Virsec assistance)*:

- Host profile creation and management
- Policy application and ACP rule configuration
- Registration window management for new probe deployments
- Probe installation and association with host profiles
- Security policy configuration and enforcement
- Incident triage and response coordination
- Daily CMS operations and configuration management
- User access management and administration

2.2 Virsec Responsibilities

Virsec is responsible for the following platform services and infrastructure:

Core Platform Services:

- CMS infrastructure management and availability
- Platform services and core functionality
- Software updates and platform upgrades
- 24x7 CMS monitoring and support
- Probe software functionality and performance impact resolution (excluding issues caused by overly restrictive customer-configured policies)

Optional Customer Support Services *(Available upon customer request)*:

- Host profile creation and template development
- Registration window management and scheduling
- Probe installation and deployment operations
- Policy updates and ACP rule management
- Third-party system integration guidance
- Incident triage and response coordination
- Daily CMS operations and configuration management
- User access management and administration

Technical Support:

- Remote operations capability via CPM
- Audit log retention and system availability
- Platform-level incident response and escalation
- Default policy and template development
- Configuration interface functionality

2.3 Service Management

2.3.1 Engagement Management

A Customer Success Manager (CSM) will be the point of contact for the Customer throughout the Customer lifecycle. The Customer Success Manager will coordinate business and roadmap reviews which will be scheduled at regular intervals as agreed by Virsec and the Customer. Status reporting will be provided if required. At roadmap reviews Virsec will provide updates on roadmap features and their release. Notwithstanding the foregoing, Virsec shall in no way be obligated to provide any new features discussed in such Product roadmap review meetings.

Integration services that are required post deployment to implement new features or devices are not covered in the software license or in the Support Services described in this Annex.

Feature and Integration requests will be reviewed by Virsec. At Virsec's discretion, these requests may be added to the product roadmap. Alternatively, these changes can be implemented by the Customer, or Customer appointed 3rd party, using documented software interfaces. Where additional hardware is required, Customer is responsible to purchase, install, support and operate the hardware.

2.3.2 Service Reviews

The Virsec CSM and the Customer shall conduct service review meetings at agreed upon intervals, as well as on demand (by conference call) in case of the need for escalation following a particular Incident, in order to find ways of improving collaboration and quality of the Support Service. The Service Review participants should include both technical and managerial representatives from Virsec and Customer.

3. Service Delivery

Virsec will handle platform definition, setup of appropriate architecture and tools, and application deployment in the cloud and on premises, as necessary. Virsec will also provide maintenance, Updates, bug fixes, and new features to the solution, following a continuous delivery methodology. The deployment/enablement of new features not included as an Update may be subject to any applicable purchase conditions. Ongoing improvements are not limited to the core portions of the system, but also include tools for monitoring and alarming.

3.1 Instance Hours of Operation

Virsec will operate the CMS Platform during the agreed Hours of Operation. Probe availability depends on customer-managed infrastructure and network connectivity. CMS availability targets apply to the central management services only. Outside of these hours, Virsec may reduce or entirely cease providing the CMS Platform. Service reduction may range from a decrease in scaling, to loss of major functionality, to complete Service Suspension.

Production Instance Hours of Operation will be 24x7x365 unless a Service Suspension is in place as defined herein.

3.2 Change and Release Management - Software Installation & Upgrades

The Support Service includes a continuous delivery process that will give the Customer access to the most recent releases of software being developed using agile software development practices. Virsec will perform quality assurance testing on all major and minor product releases internally before providing them to the Customer and will ensure that such releases do not remove critical functionality from the Service or degrade the performance of the Service. These regular software Updates may include new product roadmap items as well as bug fixes. As part of the pipeline release process the version of software used by Customer must not be more than two releases behind the current release version.

Virsec will be responsible for the installation of all software related to the CMS Platform in the cloud. The Customer is responsible for all probe software deployed on-premises at the Customer location that is part of the Virsec Platform. Virsec will provide Customer with at least 5 business days advance written notice of any proposed release.

In conjunction with the Support Services, the Customer will be provided with access to a web-based service desk as outlined in Section 4.1 herein.

Customer acknowledges that Virsec may need to perform emergency maintenance without providing advance notice. Emergency maintenance will only be performed when the anticipated impact to the CMS Platform of not carrying out the maintenance is considered to outweigh the impact of the maintenance actions. Emergency maintenance will be carried out such as to comply with the service level agreements in this Annex. Virsec will send automated email notifications to inform the Customer of any change.

4. Service Assurance

The Virsec Platform includes a dedicated service assurance function provided on a 24×7×365 basis. The service assurance function monitors and detects issues with the CMS Services and takes corrective action on an as needed basis. In the event of a

Customer raised Incident, Service Assurance can be reached via the methods outlined in Table 1 and in greater detail during the on-boarding process. Service Assurance acts as the single point of contact for case management and resolution. The priority of Service Assurance is to maximize the CMS Platform uptime. During an Incident, focus is initially on restoration of the CMS Platform. Once the CMS Platform is restored, root-cause analysis will take place when necessary and any longer-term corrective actions up to and including bug fixes will follow.

Virsec's service assurance team will interact with Customer's internal operations team and Virsec Platform users. Issues related to the installation of Probe components should be assessed by the Customer prior to escalation to Virsec.

Table 1 shows the coverage of Virsec's Service Assurance for production environments.

Table 1 Service Assurance Coverage

Virsec Service Region	Priority 1 & 2	Priority 3 & 4	Excluded Holidays
Asia Pacific	24x7x365	6AM-6PM AEDT Mon-Fri	Recognized APAC Holidays
EMEA	24x7x365	6AM-6PM CET Mon-Fri	Recognized EMEA Bank Holidays
North America	24x7x365	6AM-6PM PT Mon-Fri	Recognized U.S. Federal Holidays

There are several main activities of the Service Assurance function. They are described in the sections below.

4.1 Service Desk

The customer may contact Virsec regarding technical operations of the system via the Service Desk. The Service Desk can be reached via a web-based service portal for the following purposes including but not limited to:

- To report an Incident related to the Virsec Platform
- To ascertain the status of a previously logged Incident
- To research or query issues regarding the Services in a Virsec knowledge base
- To discuss an action plan or escalate an Incident with the Virsec support manager
- To make Service Requests related to the Virsec Platform
- Suggest improvements to the Virsec Platform

4.2 Incident Management

Service Assurance will be responsible for overseeing all activities related to Incidents opened by either Virsec or the Customer. This includes Incident detection and recording, triaging Incidents to the appropriate Services components, engaging the appropriate engineering teams, communication of Incident status, and resolving the Incident.

4.2.1 Incident Priority

Priority defines the level of effort that will be expended by Virsec and the Customer to resolve the Incident. Virsec Incident Management priorities are defined as follows:

Table 2 Incident Priority Level

Business Priority	Incident Priority Definition	Examples
Priority 1	An Error that (a) renders the CMS Platform completely inoperative or (b) makes Customer's use of material features of the Service impossible, with no alternative available, or (c) causes performance or production impact on customer workloads due to probe software malfunction.	All users unable to successfully login to CMS. All CMS application pages do not load following successful login. UI is severely degraded/unresponsive, for a significant period of time. Mass probe disconnection affecting >20% of deployed probes. CMS unable to receive probe data or incident reports. Registration window management functions unavailable. Any performance degradation or production impact on customer workloads caused by probe software (even affecting a single server).
Priority 2	An Error that (a) has a high impact to key portions of the Service or (b) seriously impairs Customer's use of material function(s) of the Service and Customer cannot reasonably circumvent or avoid the Error on a temporary basis without the expenditure of significant time or effort.	Login page presents errors for multiple users. Specific individual pages in the CMS application do not render for all users or are severely degraded. CMS API based integration is not syncing for all assets. Probe installation/uninstallation operations failing systematically. Host profile deployment or policy updates not applying. CPM remote operations unavailable for subset of probes. Individual probe disconnections affecting <20% of deployed probes.

Priority 3	An Error that has a medium-to-low impact on the Service, but Customer can still access and use some functionality of the Service.	Login page presents errors for under 10% of users. Specific control within a page does not render. CMS API based integration is partially syncing. Individual probe reporting inconsistencies without communication loss. Audit log retrieval delays or incomplete data. Policy deployment delays affecting individual profiles. UI returns an error when configuring CMS Platform.
Priority 4	An Error that has low-to-no impact on Customer's access to and use of the Service.	

Note on Probe Communication vs. Performance Issues:

- Probe communication loss affects visibility and management but does not impact enforcement capabilities
- Performance or production impact on workloads caused by probe software constitutes a Priority 1 incident regardless of the number of affected systems
- Issues caused by overly restrictive customer-configured policies are not covered under Virsec support unless the policy configuration interface itself is malfunctioning

The initial priority of an Incident will be determined by the Incident initiator based on the definitions and examples in Table 2. Incidents priority may subsequently be amended by agreement between Virsec and the Customer. If Virsec's Priority level designation is different from that assigned by Customer, Virsec will promptly notify Customer in advance of such designation. If Customer notifies Virsec of a reasonable basis for disagreeing with Virsec's designated Priority level, the parties will discuss in an effort to come to mutual agreement. If disagreement remains after discussion, each party will escalate within its organization and use good faith efforts to mutually agree on the appropriate Priority level.

4.2.2 Response Time

Based on the assigned priority, the Service Assurance team will provide the target response times specified in Table 3. If Incidents are raised within the service desk there will be an automated response to the Customer confirming the creation of the Incident that should be received within 5 minutes. Updates to Incidents will be recorded within the web-based service desk.

Table 3 Target Response Times

Incident Priority	Hours	Initial Update Response	Update Response
Priority 1	24 x 7	1 hour	4 hours, then every 4 hours
Priority 2	24 x 7	4 hours	4 hours, then every 4 hours
Priority 3	8 x 5	8 Business Hours	5 Business Days, then every month
Priority 4	8 x 5	8 Business Hours	Not applicable

"Initial Update Response" means the time elapsed from the occurrence of an actionable Incident as indicated in Virsec's ticketing system until the time the service desk is updated post acknowledgement.

4.2.3 Recovery Point Objective (RPO) and Recovery Time Objectives

RPO targets for enterprise applications are broadly categorized in the table below, in conjunction with Recovery Time Objectives (RTO), which define the maximum acceptable downtime.

Table 4 RPO and RTO Targets

Applications	RPO	RTO
Critical	>1 hour	>1 hour
Important	>4 hours	>4 hours
Supporting	>8 hours	>8 hours

4.3 Remote Support and VPN Requirements

The Virsec Platform includes probe components deployed on customer-managed infrastructure. Virsec will provide remote support for probe software through:

- **CPM-based remote operations:** Direct probe management via the CPM component for upgrades, configuration changes, and troubleshooting
- **Customer-provided access:** Desktop sharing, remote meetings, or VPN access as arranged by the customer
- **Audit logging:** All remote operations are logged in OpsBeacon for compliance and troubleshooting purposes

Customer is responsible for providing CPM connectivity and any additional remote access interfaces required for advanced troubleshooting.

4.4 Service Requests

Virsec will provide the facility for Customers to submit Service Requests via Virsec's Web Based Service Desk

Virsec will target to respond to all Service Requests within 8 Business Hours of the Service Request Creation

Service Request Examples:

- Probe deployment planning and registration window scheduling
- Host profile template creation or modification requests
- ACP policy customization guidance
- Audit log analysis and compliance reporting assistance
- Performance optimization recommendations for probe deployment

4.5 Requests For Enhancement

Virsec will provide the facility for Customers to submit Requests for Enhancement via Virsec's Web Based Service Desk

Virsec will target to acknowledge receipt of all Requests for Enhancement within 8 Business Hours of the Requests For Enhancement Creation.

Any Requests for Enhancement will be assessed by the Virsec Product management team, and if accepted, will be scheduled as part of the Product roadmap.

4.6 Monitoring and Logging

Virsec's Service Assurance involves a 24 x 7 x 365 monitoring capability for the CMS infrastructure and platform services. Customer is responsible for monitoring probe health, performance, and connectivity status through the CMS interface and their own monitoring systems. There is a continuous stream of monitoring information that is monitored and analyzed by the Service Assurance team with a goal of reacting to events and resolving Incidents before CMS Platform users are impacted. This monitoring capability includes availability and capacity management. Virsec continuously looks at system performance and will adjust the system as necessary and/or provide insight as to necessary system expansion requirements.

Virsec reserves the right to collect usage information for performance and service management in order to meet agreed CMS Platform availability targets.

4.7 Reporting Capabilities

Virsec will provide KPI/metrics reports to the Customer. These typically cover performance and usage metrics. These reports will be delivered on a monthly schedule or can be provided on-demand to a distribution list specified by the Customer. A sample list of KPI's and metrics is provided in Table 4 below. Some KPIs will be used to calculate the Availability of the Services, as further discussed in Section 5.

Note that these KPIs are examples. The actual KPIs that will be provided are dependent upon the Virsec Platform selected and not all of the following KPIs are applicable to all installations.

Table 4 Reported Key Performance Indicators (KPIs)

KPI Name	Description
Service Availability	The availability of the service to the end user as reported on a monthly basis
Incident SLA Compliance	The number of Incidents raised and their compliance to the target response and restoration times.
Service Requests	The number of Service Requests raised and their compliance to the target response and restoration times.

1. All KPI's are reported on a monthly basis, unless otherwise agreed with Customer.
    1. Data is generally collected continuously.

4.8 Escalation

The following escalation contacts are available:

Escalation Level	Contact	
L1	Rinish Balan, Director- Customer Success, rbalan@virsec.com, +91 988 653 9934	P1 Incidents - 24x7 - T0+12 P2 Incidents - 24x7 - T0+24 All Others - 8x5 09:00 - 17:00 UTC
	Head of Customer Success mclancy@virsec.com +1 636 699 0747	P1 Incidents - 24x7 - T0+12 P2 Incidents - 24x7 - T0+24 All Others - 8x5 14:00 - 22:00 UTC
L2	Simone Sassoli - CEO ssassoli@virsec.com +1 267 216 7860	P1 Incidents - 24x7 - T0+24 P2 Incidents - 24x7 - T0+48 All Others - 8x5 14:00 - 22:00 UTC

5. Target Service Availability

Virsec provides a Target Service Availability of 99.9% uptime for the CMS Platform. Availability is based on the ability of the Customer to:

- Successfully log into the CMS portal using valid credentials

- View incidents, threats, and security events
- Access probe management functions
- Retrieve audit logs and reporting data
- Perform policy and profile management operations

Probe availability is dependent on customer infrastructure, network connectivity, and proper probe configuration. Individual probe outages do not impact CMS availability calculations.

Availability will be calculated and reported on a monthly basis based on a 1 minute polling interval. The availability will be calculated as follows:

(Service Time In Minutes - Service Downtime In Minutes)

x 100%

Service Time In Minutes

Exceptions to Target Service Availability: Customer acknowledges that Target Service Availability shall not be measured when and to the extent access to and use of the CMS Platform has been to be suspended partially or totally due to the occurrence of any of the events listed below, individually or collectively referred to as 'Service Suspension(s)':

1. General Internet problems, force majeure events, or other factors outside of Virsec's reasonable control; or
2. for scheduled downtime to permit Virsec to conduct maintenance/emergency maintenance or make modifications to the CMS Platform as described herein in this Annex; or
3. in the event that Virsec receives a non-appealable order of any court of competent jurisdiction that any CMS Platform is prohibited by any applicable law or regulatory requirement; or
4. in the event of a significant denial of service attack or other security attack (i) that is commonly known as being SYN floods, ACK floods, UDP floods, Reflection attacks or HTTP slow reads and (ii) that Virsec determines may create a risk to the applicable CMS Platform, to the Customer or to any of Virsec's other customers if the CMS Platform were not suspended and (iii) to the extent of 2 days of service suspension maximum. (For the avoidance of doubt, Virsec shall not be held responsible for any attack on Customer's managed infrastructure that affects the Virsec Platform or its availability).
5. Issues arising due to Customer's equipment, software, network connections, or other infrastructure
6. Issues arising due to third-party software, not licensed through Virsec, or systems not approved by Virsec.

Virsec will use all commercially reasonable efforts to restore the CMS Platform to Customer as soon as is reasonably practicable following any Service Suspensions.

6. Operational Responsibilities Matrix

Component	Virsec Responsibility	Customer Responsibility
CMS Infrastructure	24x7 monitoring, maintenance, updates	Access management, user administration
CMS Platform Services	Service availability, performance, security	Daily operations, configuration management
Probe Software	Updates, patches, software functionality, performance impact resolution	Installation (via customer request or self-service), association, policy configuration
CPM Component	Remote operations capability, software updates	Installation, network connectivity, access permissions
Underlying Workloads	Performance impact resolution when caused by probe software malfunction	Health monitoring, infrastructure management, performance issues not caused by probe software
Host Profiles	Template development, best practices, creation (upon customer request)	Creation (self-service option), assignment, policy configuration
ACP Policies	Default policies, policy templates, configuration interface functionality, policy updates (upon customer request)	Customization, deployment, rule management, policy appropriateness
Registration Windows	Management and scheduling (upon customer request)	Self-service management (optional)
Incident Response	Platform-level incidents, escalation, probe software performance issues	Security incident triage, investigation, policy-related blocking issues
Audit Logging	Log retention, system availability	Log review, compliance reporting

7. Exceptions

The Support Services and the Service Levels shall not include the correction of any Incident due to:

1. Customer's neglect or misuse of the CMS Platform or its failure to operate the CMS Platform for the purposes for which the platform was designed;
2. Any accident, disaster, or other force majeure cause affecting the CMS Platform including without limitation fire, flood, water, wind, lightning, transportation, vandalism or burglary;
3. Malicious activity outside of the CMS Platform which results in the CMS Platform being made unavailable and which Virsec could not reasonably have been expected to prevent;
4. Customer's failure, inability or refusal to afford Virsec's personnel access to the Services;
5. Any fault or unavailability of any third party equipment, software or services owned, managed or controlled by Customer and working in conjunction with the CMS Platform (whether or not supplied by Virsec or forming part of the Services);
6. **Performance or operational issues caused by overly restrictive customer-configured security policies that block critical business functions, unless the policy configuration interface itself is malfunctioning.**

Any out of scope Support Services requested by the Customer may be provided to the Customer, after discussion between Virsec and Customer, at an agreed rate. Such services will be exempt from the agreed service levels outlined in this agreement.

8. Additional Obligations of Customer

In addition to any obligations noted previously, Customer shall also:

1. Maintain the location/s where any probe component/s of the Virsec Platform are installed in a manner consistent with the specific site requirements identified during delivery of the Services and generally provide a suitable environment for the operation and maintenance of the Services, cables and fittings associated therewith and the electricity supply at the location(s). To this end, Customer shall observe such reasonable directions with respect to the operating environment of the Services as Virsec may specify from time to time provided any such new directions given by Virsec after the date of this Agreement do not create any material financial or operational burden on Customer
2. Provide Virsec with all reasonable co-operation to facilitate Virsec's efficient discharge of its obligations under these Support Services. In particular, but without limitation, provide accurate information on Customer's hardware and

software environment, networking information and similar information required to provide the Virsec Platform, notify Virsec of any change to such system environment likely to have an impact on the Virsec Platform before the implementation of such changes, make available Customer owned spares, and any other matters arising that Virsec reasonably considers pertinent to its provision of the Support Services from time to time.

3. Take all reasonable precautions to guard the health and safety of Virsec staff and sub-contractors while working with the Services or any other equipment, which belongs to Customer or is located at any of the Customer location(s). These precautions will be in line with Customer's obligations to its own employees.
4. Keep and operate the Services in a proper and prudent manner in accordance with Virsec's operating instructions and ensure that only competent trained employees are allowed to operate the Services. Such operations include the day to day exercising of the system APIs, either via automated interfaces or supplied user interfaces, in order to modify the system data to effect changes based on business requirements. Examples of this would include adding new content, defining new policies, updating configurations etc.
5. Implement and maintain appropriate security measures and policies for the Customer's network and its interface with the CMS Platform components, including data-security for the network. Customer shall maintain and implement strong passwords and MFA for accessing Virsec infrastructure and the associated support portal and shall protect against unauthorised third party access any user IDs and passwords assigned for the use of the CMS Platform. Customer shall immediately modify the same if a unauthorised third party may have become aware thereof. Customer shall ensure the access authorization may be used only by that to whom it was assigned. Virsec shall not be liable if a third party uses or abuses the CMS Platform with a user ID assigned to the Customer.
6. Ensure any necessary support agreements are in place for third party infrastructure and services (not included as part of the Services).
7. Be responsible for renewal of third party support contracts on-going for infrastructure, software or services owned or controlled by Customer and working in conjunction with the CMS Platform.
8. Provide remote access (VPN) to the Services for Virsec personnel where agreed.
9. Reasonably ensure that only Virsec-trained personnel, or persons working under their direct supervision, shall be responsible for diagnosing Incidents.