IMPORTANT

Please read this Support Service Agreement (this "**Agreement**") carefully. Customer's execution of an Order Form for a subscription to the Service or Customer's access to or use of the Service constitutes Customer's consent to this Agreement. This Agreement is between you and the company or organization that you represent ("**Customer**") and ThreatConnect, Inc. at 3865 Wilson Blvd, Suite 550, Arlington, VA 22203 ("**ThreatConnect**") concerning Support Services for RSA Netwitness Orchestrator 6.0+. Customer's agreement to these terms in accordance with the process set out in this Agreement will constitute a valid and binding signature, and upon ThreatConnect's request, Customer will also sign a non-electronic version of this Agreement. ThreatConnect and Customer are herein referred to each as a "Party" and collectively as the "Parties". Notwithstanding anything the contrary herein, Licensor shall promptly inform RSA of any Severity 1 or 2 Errors of which it becomes aware and shall promptly respond to RSA queries about the status of any open support tickets.

General. Enhanced or Standard Support will be provided to Customer and its users in accordance with the terms and conditions contained herein. ThreatConnect will use commercially reasonable efforts to promptly respond to each case, and will use commercially reasonable efforts to promptly resolve each case as more fully described herein.

Warranty Period. ThreatConnect warrants that the support provided in accordance with this Support Plan will be performed by individuals with the requisite knowledge and experience necessary to fulfill ThreatConnect obligations contained herein and at the support level and term indicated in the applicable purchase order or other applicable ordering document.

ThreatConnect Software Version Support. ThreatConnect versioning follows the pattern of Major/Minor/Patch (for example 5.8.2). Support will provide support for 2 minor versions of ThreatConnect products only.

Resolution Policy. Actual resolution time will depend on the nature of the case and the resolution. A resolution may consist of a fix, workaround, recommendation to update to the latest version, or other solution in ThreatConnect's reasonable determination. If a Customer or RSA has not responded to a question, inquiry or other communication from the ThreatConnect Support team after 3 business days then Support will identify the case as "Customer Has Not Responded" and cancel the case.

Designated Contacts. "Designated Contacts" are Users that the Customer identifies as primary liaison(s) between Customer and ThreatConnect for technical support. RSA shall also have up to four (4) Designated Contacts for technical support which Designated Contacts may be changed upon notice from RSA to Licensor. Customer shall identify a minimum of one (1) and a maximum of four (4) Designated Contacts. Customer may be charged an additional fee for Designated Contacts in excess of four (4) at any given time. Customer shall notify ThreatConnect whenever Designated Contact responsibilities are transferred to another individual, and upon departure of a Designated Contact.

Customers' Designated Contacts shall be responsible for:

1. Overseeing Customer's support case activity.
2. Developing and deploying troubleshooting processes within Customer's organization.
3. Resolving password reset, username and lockout issues for Customer.
4. Managing Customer's software update and patching processes.

Customer shall ensure that Designated Contacts:

1. Have completed, at a minimum, the basic Services administration course currently titled "Administrative Training," which is included as part of On-Premises and Dedicated Cloud training. For RSA Designated Contacts, this training shall be provided at no charge.
2. Are knowledgeable about the applicable Services in order to help resolve, and to assist ThreatConnect in analyzing and resolving technical issues.
3. Have a basic understanding of any problem that is the subject of a case, and the ability to reproduce the problem in order to assist ThreatConnect in diagnosing and triaging the issue.

Customers Obligations. Customer will follow the ThreatConnect provided documented technical and user guides. Customer will provide a response to Support requests or inquiries within 2 business days.

Required Information. In regard to the Branded Software and in an effort to expedite the resolution process, the customer will provide the following as necessary:

1. ThreatConnect Environment: Dedicated Cloud or On-Premise. If On-Premise then purchased version of ThreatConnect, underlying OS version, Python, Java, JCE, MySQL, PostGreSQL, etc.
2. ThreatConnect platform user account and organization.
3. Nature of the problem (integration, TAXII, email ingest, etc).
4. Any initial triage steps taken thus far.

5. Any error messages encountered.
6. Any data the user was trying to use or type of data such as the format of the data, version information, file extension, etc.
7. tc-log, server, and playbook log files as applicable.
8. If an On-Premise deployment, the session logs if applicable.

Optional: Screenshots or video clips or steps demonstrating the process/workflow that induced the error or issue.

For software that is not developed or maintained by ThreatConnect, that reside on another platform, that operate within ThreatConnect or another platform, the following will be required:

1. Platform Environment: Version, underlying OS, any changes at all that deviate from the documented default deployment.
2. Target and destination end-points for integrations.
3. Any log files from either the ThreatConnect platform, the platform that is hosting the software or integration or service.
4. Nature of the problem.
5. Triage steps taken thus far.
6. Any error messages encountered.
7. Any data the user was trying to use or type of data such as the format of the data, version information, file extension, etc.
8. Log files from both app and platform the hosting platform for the app.

Optional: Screenshots or video clips or steps demonstrating the process/workflow that induced the error or issue.

Support Contact Procedures. Contact via support email, web portal, or phone. No other means of communication will be bound to the Support agreement without prior authorization.

- By sending an email to Customer Support at the following email address: support@threatconnect.com. Customers will receive back an assigned support ticket number and will be contacted within a timeframe of such Customer's particular service level.
- By using the Support web portal, a Customer can submit a case and a ticket number will automatically be generated. The web portal URL is: https://jira-tc.atlassian.net/servicedesk/customer/portal/2
- Telephone support is available in English during the times applicable to the service level purchased. Calls will normally be answered by a triage agent, who will document the case and route it to the appropriate support team for response to Customer.
- Main toll-free Customer Support telephone number is as follows:
  - United States: + 1.800.965.2708
  - United Kingdom: + 44.20.7936.9101

Service Commitments and Service Credits For Dedicated Cloud Deployments. ThreatConnect will use commercially reasonable efforts to make the Branded Software available with a Monthly Uptime Percentage (defined below) of at least 99.8%, in each case during any monthly cycle (the "Service Commitment"). In the event ThreatConnect does not meet the Service Commitment, you will be eligible to receive a "Service Credit," as described below.

Definitions.

"**Monthly Uptime Percentage**" or "**System Availability**" is calculated by subtracting from 100% the percentage of minutes during a given month that ThreatConnect was "**Unavailable**." Monthly Uptime Percentage measurements exclude downtime to the extent caused by an "SLA Exclusion," as hereafter defined.

A ThreatConnect running instance is "**Unavailable**" when it cannot be accessed by an End User unless such inability to access is caused solely by the End User or one of its agents, subcontractors, or vendors (other than Licensor and other than actions of the End User or one of its agents, subcontractors, or vendors in accordance with the Branded Software Documentation) (e.g., power outage at End User facility). The Service Commitment excludes any scheduled maintenance periods, as coordinated and agreed upon mutually, in advance, with the customer.

A "**Service Credit**" is a dollar credit, calculated as set forth below, that, if owed, Licensor will automatically credit to RSA on behalf of the applicable End User(s).

Service Commitments and Service Credits. Service Credits are calculated as a percentage of the total charges paid by the End User for the Branded Software for the monthly billing cycle, in accordance with the schedule below.

If the System Availability percentage is:	Then the Service Credit shall equal this percentage of the monthly fee for the month in which the Unavailability occurred:
99.8% or greater	0%
Greater than 99% but less than 99.8%	3%
Greater than 98% but not more than 99%	5%

Greater than 97% but not more than 98%	10%
Greater than 96% but not more than 97%	15%
Greater than 95% but not more than 96%	20%
less than 95%	25%

Service Level Agreement Tiers, SLA Definition, Target Response Times, Incident Definition

Definitions

The following terms will have the following meanings when used in this Schedule:

Performance Credit means one percent (1%) of the average monthly subscription fee for the Branded Software.

Resolution Time means the elapsed clock time between (i) RSA's (or End User's, as applicable) Software Service Call to Licensor to report a problem and (ii) implementation of an Update in the Branded Software that corrects the problem and causes the Branded Software to be in compliance with the Branded Software Documentation and operate without malfunction.

Response Time means the elapsed clock time between (i) the Software Service Call to report a problem and (ii) a Licensor technical support analyst capable of understanding the problem speaking to RSA or End User's support contact about the problem.

Workaround means a solution that resolves a problem without decreasing the Branded Software features, functionality or performance or resulting in an added burden or expense to the End User.

SERVICE LEVELS.

Response and Resolution Times. Licensor will respond to and resolve problems so as to meet all of the Service Levels in Software Maintenance Service Levels Table below. Also, subject to Customer's approval on a case-by-case basis, Users may be asked to provide visibility (via screenshare / webex sessions only) to their ThreatConnect application and/or desktop system for troubleshooting purposes. If Licensor does not satisfy one or more of those Service Levels, RSA (on behalf of its End Users) will receive the Performance Credits specified below.

Notice of Delayed Resolution. If Licensor does not resolve a problem within the Resolution Times listed in Software Maintenance Service Levels Table below, Licensor will immediately notify RSA. This notice will include (i) a reasonable explanation for the delay and (ii) a good faith schedule and plan for correction. This notice will not constitute an excuse or waiver of performance. Licensor will keep RSA informed of the progress of its efforts to resolve Severity 1 or 2 problems at appropriate intervals or as otherwise requested by RSA.

On-Site Support.

For On-Premises End Users, or issues with maintained integration software for Dedicated Cloud Customers as relevant, if a Priority 1 problem is not resolved by Licensor within 60 hours after Licensor learns of the problem, or a Priority 2 problem is not resolved within six (6) days after Licensor learns of the problem, then Licensor will, within 48 hours after RSA's request, provide qualified Licensor Personnel at the End User's designated location to work exclusively and continuously on the problem until it is resolved. If Licensor subsequently demonstrates that the problem was not the result of a failure of the Branded Software or otherwise caused by Licensor, End User (or RSA, as applicable) will reimburse Licensor for those on-site services at the Professional Services rate included in the attached pricing schedule, as well as travel and expenses if the End User work location is outside the continental United States.

Initial troubleshooting will involve phone, email or other communication methods between Licensor and the End User. Licensor must be able to reproduce errors in order to resolve them, or alternatively, the End User agrees to reproduce errors and to provide visibility into problems with the Branded Software by sharing with Licensor via Webex or screen shares. After first attempting these initial remote resolution attempts, Licensor, in its sole discretion, may determine that an onsite visit is required to resolve the issue. Upon written/ email confirmation by an Customer's Designated Contact that the Customer will approve the onsite visit, Licensor may travel to the End User's facility to access the Branded Software (the level and extent of such access to be determined solely by the End User) as necessary in order to troubleshoot the problem. The End User agrees to cooperate and work closely with Licensor to conduct diagnostic or troubleshooting activities as reasonably requested by Licensor. End User (or RSA, as applicable) agrees to reimburse Licensor for all pre-approved reasonable travel, lodging, meal and related expenses in connection with such onsite. If the Customer or RSA denies Licensor's request for an onsite visit that Licensor reasonably deems necessary, the Resolution Times in this Schedule shall not apply to the error at issue.

Service Level Agreement (SLA) Tiers

Customer's Purchase Order will identify the level of Support purchased: Enhanced or Standard. Standard Support is included in the subscription. Enhanced Support is currently priced at 10% of the customer's annual subscription, billed annually with the subscription. By default both levels of customer support tiers have access to email, web portal, and phone support. Additional resources available to all Customers are the Knowledge Base, API and SDK documentation, mercurial code repositories, chat channels, and secure customer repositories for documentation.

Submitting a Case. Severity Level 1 and 2 cases must be submitted via telephone as described in the Support Contact Procedures section. Severity Level 1 and 2 target initial response times do not apply to cases submitted via web portal, e-mail, other messaging methods, or other means. Initial response times submitted via web-portal, e-mail, or other messaging methods will begin once Licensor Support receives the communication.

Target Response & Resolution Time by Case Severity				
SLA	Severity	Telephone Support	Target Initial Response Time	Target Resolution Times
Enhanced	S1	24x7	1 hour Remedy: One Performance Credit: • if Response Time exceeds 1 hour; and • for each 60 minute interval thereafter until a response is provided.	Workaround: 60 hours for when cause can be identified remotely by Licensor (e.g., if Licensor is able to either a) reproduce Error or b) Customer is able to reproduce error and share such reproduction with Licensor via Webex or screenshare). 96 hours for a Workaround when Licensor deems it necessary to go onsite to determine the cause of the problem. Fully tested Permanent Correction: Six Days (144 hours). Remedy: One Performance Credit: • if Resolution Time for a Workaround exceeds 60 hours when an onsite visit is not necessary, Ninety-six (96) hours when an onsite visit is necessary • for each eight (8) hour interval thereafter until a Workaround is provided.
Enhanced	S2	24x7	2 hours Remedy: One Performance Credit: • if Response Time exceeds 2 hours; and • for each 60 minute interval thereafter until a response is provided.	Workaround: Six Days (144 hours). Fully tested Permanent Correction: Eight Business Days. Remedy: One Performance Credit: • if Resolution Time for a Workaround exceeds 144 hours; and • for each eight (8) hour interval thereafter until a Workaround is provided.
Standard	S1	9-6 EST, M-F	2 business hours Remedy: One Performance Credit: • if Response Time exceeds 2 business hours; • and for each 60 minute interval during business hours thereafter until a response is provided.	Workaround: 80 hours for when cause can be identified remotely by Licensor (e.g., if Licensor is able to either a) reproduce error or b) Customer is able to reproduce error and share such reproduction with Licensor via Webex or screenshare). 120 hours for a Workaround when Licensor deems it necessary to go onsite to determine the cause of the problem. Fully tested Permanent Correction: Seven Days (168 hours) Remedy: One Performance Credit: • if Resolution Time for a Workaround exceeds 80 hours when an onsite visit is not necessary, One twenty (120) business hours when an onsite visit is necessary; and • for each eight (8) hour interval thereafter until a Workaround is provided.
Standard	S2	9-6 EST,	4 business hours	Workaround: Six Business Days (168 hours). Fully tested

		M-F	Remedy: One Performance Credit: • if Response Time exceeds 4 business hours; and • for each 60 minute interval during business hours thereafter until a response is provided.	Permanent Correction: Ten Business Days. Remedy: One Performance Credit: • if Resolution Time for a Workaround exceeds 6 business days • for each business day thereafter until a Workaround is provided.
Enhanced/Standard	S3	9-6 EST, M-F	4 business hours	Workaround: Eight (8) days. Fully tested Permanent Correction: Part of Licensor's next regularly scheduled release or update.
Enhanced/Standard	S4	9-6 EST, M-F	8 business hours	Licensor will provide a permanent correction as part of Licensor's next regularly scheduled release or update or as Otherwise mutually agreed by the parties.

Target Response Times. 24X7 Support that provides 1 hour response time for S1 and 2 hour response time for S2 is available for an extra fee that is equal to 10% of the subscription license pricing.

Incident Definition

Severity 1 (Urgent). An Issue that results in a critical business impact for a Production System; may be assigned to an Issue where customer experiences (i) a complete or substantial loss of service when using a Production System, or (ii) real or perceived data loss or data corruption making an essential part of the Production System unusable, or (iii) the inability to use a mission critical application within a Production System.

Severity 2 (High). An Issue that results in a high business impact for a Production System; may be assigned to an Issue where customer experiences (i) the functionality of the software is adversely affected, but can be circumvented, or (ii) certain functions within the software are disabled, but the Software remains operable, or (iii) a complete or substantial loss of service when using a Development System.

Severity 3 (Medium). An Issue that results in a medium business impact for a Production System; may be assigned to an Issue where customer experiences (i) partial non-critical functionality loss and the Issue has no significant effect on the usability of the software, or (ii) time-sensitive Issue important to long-term productivity that is not causing an immediate work stoppage.

Severity 4 (Low). An Issue that results in a minimal business impact for a Production System; may be assigned to an Issue with no impact to quality, performance, or functionality of the software, or cases of general information requests, such as usage and configuration.

ThreatConnect Support Plan SLA Exclusions. Below lists the conditions that are excluded from the ThreatConnect Support plan:

1. Support of ThreatConnect Software Products and Services without the assistance of ThreatConnect Support Engineers or ThreatConnect Deployment Engineers.
2. Assistance with ThreatConnect password resets. For password resets, Users should click the "Forgot your password?" link on the login page or contact their Organization administrator for Public Cloud products and their System Administrator/Organization Administrator for Dedicated Cloud or On-Premise products.
3. Assistance with ThreatConnect usernames. For assistance with usernames, Users should contact their Organization administrator for Public Cloud products and their System Administrator/Organization Administrator for Dedicated Cloud or On-Premise products.
4. Assistance with ThreatConnect lockouts due to incorrect login attempts. For assistance with ThreatConnect lockouts due to incorrect login attempts, Users should contact their Organization or System administrator to unlock the account, or wait for the lockout period to expire.
5. Installation, configuration, administration, maintenance, training, or troubleshooting of databases, database systems, search engines, analytic engines, or other software not maintained by the Licensor not listed.
6. Installation, configuration, administration, maintenance, training, or troubleshooting of other security products such as loggers, SIEMs, firewalls, API gateways, gateways, proxies, or others not listed.
7. Installation, configuration, administration, maintenance, training, or troubleshooting of authentication protocols or mechanisms such as kerberos, NTLM, or others not listed.
8. Installation, configuration, administration, maintenance, training, or troubleshooting of network or communications switches, routers, or others not listed.

9. Installation, configuration, administration, maintenance, training, or troubleshooting of third-party integrations/applications/code that resides on a ThreatConnect product or use the ThreatConnect API or SDK.
10. Installation, configuration, administration, maintenance, training, or troubleshooting of third-party integrations/applications/code that do not reside on a ThreatConnect product or use the ThreatConnect API or SDK.
11. Installation, configuration, administration, maintenance, training, or troubleshooting of Playbooks Apps or Templates that have been developed by a third-party.
12. Installation, configuration, administration, maintenance, training, or troubleshooting of Spaces Apps that have been developed by a third-party.
13. Installation, configuration, administration, maintenance, training, or troubleshooting with ThreatConnect after the customer has customized, changed, or installed third party software to interact with ThreatConnect in a non-approved configuration.
14. Installation, configuration, administration, maintenance, training, or troubleshooting with ThreatConnect after the customer has customized, altered, or configured ThreatConnect from the accepted configuration in any undocumented manner without prior approval from ThreatConnect.
15. Installation, configuration, administration, maintenance, training, or troubleshooting with additional environments, such as a DEV or UAT, without prior approval from ThreatConnect.
16. Installation, configuration, administration, maintenance, training, or troubleshooting of hardware, including computers, hard drives, networks or printers.
17. Installation, configuration, administration, maintenance, training, or troubleshooting of virtual machines, to include virtual environments, hypervisors, hosts, or others not listed.
18. Installation, configuration, administration, maintenance, training, or troubleshooting of underlying operating systems, related packages, services, dependencies, or others not listed.
19. Installation, configuration, administration, maintenance, training, or troubleshooting of any technologies not derived by ThreatConnect that utilize or reside on the Application Layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data-Link Layer, Physical Layer, Host-To-Host Transport Layer, Internet Layer, Network Interface Layer. To include encryption, protocols, services, or others not listed.
20. Creation or testing of custom code, SQL/API queries, queries on other platforms.
21. Data migration between products that are not derived by ThreatConnect.
22. Feature Requests, suggestions, general product knowledge questions. For these items utilize the Customer Success Engineers or Customer Success Managers.
23. Compliance with any standards or organizations.
24. Force Majeure.

ThreatConnect Support Plan Applicability By Deployment Method

Dedicated Cloud Deployment

The items within the previous section, "ThreatConnect Support Plan SLA Exclusions" apply to Dedicated Cloud installations.

On-premise Deployment

ThreatConnect will work with the Customer to ensure that proper configuration and installation of the Branded Software is completed according to the official and updated installation guides with the direction of the Deployment Engineer. ThreatConnect will ensure that the Customer is made aware of any requirements, both hardware and software, in prior meetings before a deployment is scheduled. A Deployment Engineer will be involved in the installation of ThreatConnect either in person or remotely at the discretion of ThreatConnect unless otherwise agreed by the Parties, with the Deployment Engineer able to view and assist as necessary during the installation process. The items within the previous section, "ThreatConnect Support Plan SLA Exclusions" apply to On-premise installations.