verizon

MANAGED SECURITY SERVICES – CLOUD PREMIUM +

1. **RATES AND CHARGES.** For Managed Security Services - Cloud Premium (MSS-Cloud) Customer orders, Customer will pay the monthly recurring charges (MRC) per MSS-Cloud service or Secure Cloud Interconnect ("SCI") service (or per other specified item) set forth in the applicable Contract, and at the following URL: www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm. Each instance of MSS-Cloud is a "Service Element" as further defined in Part V, Definitions. Confirmation Date and the initial MRCs will be invoiced upon Service Activation Date (as those terms are defined herein), and monthly thereafter.

1.1 **Minimum Order Quantity.** Customer acknowledges and accepts that, for some services, such as Service Tickets, a minimum order quantity may apply. Verizon will advise Customer if a minimum order quantity applies in advance of Customer's order. Any unused portion of such minimum quantity will be forfeited upon termination or expiration of the related MSS-Cloud service without refund, credit or other form of reimbursement of fees paid.

1.2 **Discounts.** Discounts, if any, will be automatically applied to each Contract, depending on the term of the Agreement indicated in the Contract.

1.3 **Service Reinstatement Charge.** If Customer has terminated a Service Element and requests Verizon to renew that Service Element after the related MSS-Cloud term has ended, Verizon may require payment of a service initiation fees to re-establish service.

2. **SERVICE DESCRIPTION AND REQUIREMENTS.** MSS-Cloud provides perimeter security to Customer's Internet traffic exclusively on Verizon IP Services on a Designated Circuit that have been routed to MSS-Cloud. Customer also may order MSS-Cloud to provide a security gateway between an eligible Verizon SCI Cloud Service Partner and Customer's Verizon MPLS network. Customers must already be subscribed to the Verizon IP Service before MSS-Cloud can be ordered. Verizon will evaluate the Verizon IP or SCI service for bandwidth, IPv6 and gateway router constraints before MSS-Cloud will be applied to the Designated Circuit. Verizon operates, manages and maintains the MSS-Cloud infrastructure. MSS-Cloud utilizes the Verizon Security Dashboard/Security and Compliance Dashboard for service administration/reporting and analytics functions and allows Customer to review the deployment

of its MSS-Cloud service. The Service Context section of the Security Dashboard/Security and Compliance Dashboard displays each virtual instance of MSS-Cloud related to a Verizon circuit ID as a Serviced Device. Capitalized terms used in the description that are not described therein shall have the meaning ascribed to them in Part V (Definitions) of this Service Attachment. Due to the inherent evolutionary nature of technology, Verizon reserves the right to change, modify, update or enhance MSS-Cloud Service Description from time to time. The Service Description provides additional details and information regarding service settings and service delivery. Verizon will notify Customer upon publishing a new release of the Service Description by (a) posting the updated Service Description to the Security Dashboard/Security and Compliance Dashboard or (b) communication via the Client Service Manager (CSM). New releases of the Service Description are effective upon such release.

2.1 **Initial Rule Set Creation (Security Policy).** Customer is responsible to provide an initial Rule Set prior to installation of MSS-Cloud either by utilizing an existing Rule Set, creating a limited Rule Set with Verizon's assistance as provided below, or obtaining a more complex Rule Set through a separate Verizon Professional Security Services (PSS) engagement prior to installation, at Customer's cost and expense. If Customer does not have an initial Rule Set, Verizon will provide assistance to Customer to create a limited initial Rule Set. Verizon will work remotely, via telephone and/or email, with Customer to develop and agree to such initial Rule Set. The initial Rule Set configuration will be limited to no more than 40 Objects and 20 Rules. More complex initial Rule Sets will be provided when mutually agreed between Verizon and Customer and may incur additional Service Ticket cost. This limitation does not apply to configurations developed by Verizon PSS on behalf of the Customer, at Customer's cost and expense. Rule Set creation by Verizon PSS will not be performed on active/live MSS-Cloud services. Rule Sets created by Verizon PSS will be provided to MSS-Cloud operations to implement.

2.1.1 MSS-Cloud does not include onsite Installation, configuration and Rule Set reviews, except as outlined above, or architectural or Rule Set design. These additional services can be carried out by Verizon if so agreed under a separate PSS statement of work at Customer's cost and expense.

2.1.2 **Service Delivery.** Verizon will initialize MSS-Cloud and associate it in the Security Dashboard in readiness for Service Configuration. Upon Initialization, Verizon will confirm to Customer that MSS Cloud is ready for Service Configuration and available to Customer via the appropriate portal and service level. This point is the Service Activation Date.

2.2 **Threat Analysis.**

2.2.1 **Overview.** A Security Incident is generated after logs and events have been processed through threat detection policies and use cases. Verizon defines Logs, Event, and Security Incidents as follows:

- **Logs:** A collection of various IT, network, application, and security related information created by Subordinate Devices.
- **Security Event:** A data record produced by the SEAM (State and Event Analysis Machine) correlation engine based on Verizon's proprietary threat detection policies.
- **Security Incident (Incident):** A single event or a series of events that have been aggregated and correlated based on Verizon's proprietary's threat detection policies. A security incident may represent an attack.
- **Incident Record Communication:** A record in the system which tracks and drives the workflow of incidents, change and service requests during their lifecycle to closure.
- Verizon's threat detection policies are, amongst others, based on a behavior based, multi-factor correlation capability processed through the SEAM that evaluates and correlates reputational and behavioral patterns and characteristics in addition to signature-based detection methods. Verizon correlates and aggregates related events into Security Incidents automatically through its threat detection policies. Verizon has a wide variety of methods to detect Security Incidents.
- Events may appear harmless when they are detected in isolation; however, when they are combined with information from other events or from information in the Service Context, a more harmful pattern may appear. Events will be compared with Customer's Service Context and output obtained from network vulnerability scans. The Security and Compliance Dashboard provides a range of reporting functions.
- For services providing Internet security (not SCI), Verizon will perform scans on Customer's Internet facing IP subnets and hosts on a quarterly basis for the locations under contract. The

scan data will be used to classify and assign risk scores to Security Incidents and related events, as well as tune the configuration of MSS-Cloud services, if applicable. The quality of Verizon's classification and the number of Incidents escalated as an Insufficient Info Incident depends on the quality and completeness of the information that Verizon receives on the network environment of the MSS-Cloud service, including up-to-date scanning and asset data. Customer acknowledges that, without up-to-date network scanning and asset criticality data, Verizon will not be able to maintain optimum configurations of the MSS-Cloud services, i.e., there will be an increased risk of false-positives being generated, and Verizon will not be able to assess accurately the impact of Incidents on Customer's environment. Scans for Internet-reachable IPs associated with Cloud Service Partners must not be instigated without permission from the Cloud Service Partner.

2.2.2 Security Incident Classification

Verizon Classifies Security Incidents into 4 Categories:

Incident Classification	Risk Levels	Conditions
Insufficient Info	L0	The Incident has been classified as Insufficient Info based on the associated events.
Harmful Attack	L1	The Incident is identified as an attack or an attempted attack that may result in damage or unauthorized access to a device or application. The cause of the Incident renders Customer's infrastructure vulnerable or compromised.
Harmless Attack	L2	The Incident is identified as a known attack, attempted known attack or reconnaissance effort. Customer's infrastructure is not considered vulnerable or compromised based on the Service Context.
False Positive	L4	The Incident may be falsely triggered, is informational or benign in nature.

Offline Analysis Category is used during first phase of deployment

Classification	Level	Conditions
Offline analysis	L 9	Level is used during the first phase of deployment or after major changes in the network (such as adding or removing a server or MSS-Cloud service, moving a MSS-Cloud service, changing security policies and rule sets, installing major signature updates or major software upgrades, implementing an Urgent Change Request or replacing a MSS-Cloud service). These Events will only be logged and will not involve real-time analysis.

2.3 **Security Incident Handling.** Verizon generates Security Incidents in both real- and non-real time, depending on the detection method. The status of the Incident will be changed throughout its lifecycle. Status changes are communicated by E-mail and are displayed on the Security and Compliance Dashboard. An SMC Time Stamp ("UTC") is added after each status change. A Security Incident can have the following status:

Security Incident Status

Incident status	Conditions
Open (Security Incident Detection)	The Incident has been generated based on Verizon's threat detection policies.
Escalated (Security Incident handling)	An Incident Record Communication is created with the Security Incident information to allow the mitigation, containment or resolution of the risk. A Security Incident is escalated when it is: o A Harmful Attack Incident and concerns a real threat

	○ An Insufficient Info Incident: the security analyst needs extra information to classify the Security Incident
Closed	The Incident has been auto-closed or closed by the security analyst.

An Incident classification and status may change based on additional analysis, intelligence information or after Customer feedback has been received.

2.3.1 **Real-Time Security Incidents.** Verizon uses threat detection policies based on one or more use cases to create Security Incidents in real time. All use cases and proprietary signatures are categorized to help (a) increase insight into Security Incidents and (b) reduce the number of false-positive Incidents. The Incident descriptions provide recommendations on possible actions Customer can take.

2.3.2 **Non-Real Time Security Incidents.** Verizon uses threat detection policies based on one or more use cases in order to find patterns over a longer period of time and to allow low confidence indicators to be analyzed more effectively. Security analysts will review these Incidents periodically as a block of security information. If an Incident or a combination of Incidents is considered to be important, the SOC will escalate it. This method optimizes Security Incident handling and focuses on escalating potentially harmful Incidents and reducing Insufficient Info Incidents and False Positives. The Security Incident Escalation SLA does not apply for non-real time security incident handling.

2.3.3 **Non-Real Time Security Incidents for Customer Digests.** Verizon uses Threat detection policies based on one or more use cases to present Security Incidents periodically without SOC review or analysis. These Security Incidents will be closed automatically, but can be reviewed by Customer on the Security and Compliance Dashboard in the Security Digest section. Customer digests are focused on specific topics. This Incident handling is optimized for certain types of Incidents that do not require real-time Incident handling and SOC review. They provide additional information to the customer and can support compliance initiatives. The Security Incident Escalation SLA does not apply for customer digests.

2.3.4 **Security Incident Escalation.** Verizon will only escalate Security Incidents that are classified as Insufficient Info and Harmful Attack. Verizon will examine the characteristics and context of the events and Incidents, and evaluate the possible impact of a threat/attack on Customer's MSS-Cloud services before escalating an Incident Record Communication. Verizon will provide additional information to support the investigation of a Security Incident and may propose possible recommendations for next actions. Verizon will not provide remediation services under this service.

Customer:

- Is responsible for providing missing Incident information for Incidents classified as Insufficient Info within the required timeframe; if Customer fails to provide such information, Verizon may send a reminder or change the status of the Incident to Closed.
- Will authorize a Change Request when mitigating actions are expected to be taken by Verizon on any of the managed devices.
- Is responsible for repairing the integrity of the affected applications and infrastructure for devices and any customer configured cloud environments under management by Verizon.
- Must inform Verizon of any actions taken by Customer in order to enable Verizon to update its inventory of Customer's infrastructure and set the Incident status to Closed.

Verizon will escalate an Incident Record Communication with the Following Incident Information:

- UTC timestamp of the Incident creation
- The identity of the affected MSS-Cloud service(s) and its Designated Circuit/SCI Service
- Source information and destination information
- Threat signature and use case information, if applicable: threat use case ID, name, and description
- Packet dumps, if obtainable from the MSS-Cloud service and Subordinate Devices using the existing infrastructure.

Targets for Security Incident Escalation

	Communication	Communication	Reporting
Channel	Email	Phone and Email	Security and Compliance Dashboard
Information Type	Incident Record Communication - Insufficient Info (L0)	Incident Record Communication - Harmful Attack (L1)	Security and Compliance Dashboard
Reference Time	SMC Time Stamp (UTC) Incident Creation	SMC Time Stamp (UTC) Incident Creation	
Response Time	≤ 30 minutes after Incident Creation	≤ 15 minutes after Incident Creation	Refreshed every 15 minutes
Contact Person	Authorized Contacts	Authorized Contacts	Authorized Contacts

There are no service level targets for Incidents created in non-real time or in Customer digests.

2.3.5 **Service Management and Reporting**

2.3.5.1 **Security Dashboard/Security and Compliance Dashboard.** Authorized Users have 24x7 access to the Security Dashboard/Security and Compliance Dashboard. Each Authorized User must have one SSL Certificate to access the Security Dashboard/Security and Compliance Dashboard. MSS-Cloud includes up to five SSL Certificates. The set-up of an additional Authorized User, and associated SSL Certificate, uses two Service Tickets.

2.3.5.2 **Other Incident Tickets.** Other Incident Tickets are tickets that are created by Verizon or Customer for service related Incidents. They can be logged on a 24x7 basis by the Authorized Users through the Security Dashboard/Security and Compliance Dashboard, via e-mail or telephone. Verizon will not manage Serviced Devices under Monitoring (only) services through an Other Incident Ticket. Verizon assigns a unique Call ID and a Severity Level (as shown below) to every support request that it accepts. The Severity Level is based on the information received from Customer and on the impact of the problem on the Customer's network environment.

- **Customer Responsibilities:** Customer must provide its representative's name, company name, telephone number, e-mail address, error codes/messages received, description of the impact to Customer's network or business environment, and a detailed description of the problem and how it may replicated, including the steps to replicate the problem.

Problem Severity	Level	Conditions
Severity 1	S1	An error causes the MSS-Cloud service to fail. Normal day-to-day business is not possible (e.g. system failure, an inaccessible or inoperable production system).
Severity 2	S2	An error significantly affects the functions of the MSS-Cloud service and prevents normal day-to-day business; or an error occurs in a high-risk environment (e.g., an error in one line of a high-availability setup).
Severity 3	S3	An isolated error impacts the functions of the MSS-Cloud service; there is no important impact on the day-to-day business. Or an error occurs that significantly affects the MSS-Cloud service, but a Work-around exists.
Severity 4	S4	A benign error occurs, or an improvement is asked. There are no problems with the MSS-Cloud service, and there is no immediate impact on the production environment.

For Severity 1 and 2 problems, Customer and Verizon will both assign a dedicated contact person. Severity 3 or 4 software problems may be resolved in the next revision or upgrade of software. Verizon reports on the status of a problem with status reports. Verizon reserves the right to refuse unreasonable or unsupportable requests including requests: (i) by unauthorized parties, (ii) that cover the installation of new devices or software, (iii) that amounts to training or consultancy, or (iv) that involves the redesign of Customer's infrastructure. Verizon will inform Customer of the resolution of 'Other Incident Ticket' when resolved. If Customer does not provide

the necessary information or undertake a specific task requested by Verizon, Verizon may change the severity level or close the Other Incident Ticket as set out below:

- After one Business Day, a Severity 1 or 2 problem will be lowered one level
- After five Business Days, Verizon may close the Other Incident Ticket.

Verizon notifies Customer when the Severity Level is lowered to a level that does not require further action. Verizon conducts root cause analysis of the problem and communicates the results to Customer. If the source of the problem lies within Customer's responsibility (for example, Customer networking issues or Subordinate Devices not under Verizon's management) the ticket will be an Other Incident Ticket and will consume four Service Tickets.

2.3.6 **Management Report.** Verizon will generate a monthly Management Report on the Security Dashboard that covers all MSS services. The Management Report shows: the status of the open Change Requests and Security Upgrades; summary of all Incidents of the past period; a closure report of all Harmful Attack and Insufficient Info Incidents, and management-level interpretation of the Incidents; most frequent sources, destinations, and ports of blocked packets; an overview of all planned and implemented Change Requests, Rule Set updates, and Security Upgrades of the past period; and requests for information from Verizon concerning Customer's network or to clarify irregularities in the Threat analysis of the past period.

2.3.7 **Requests for Information.** Customer can submit a Request for Information (RFI) on the MSS-Cloud service 24x7. RFIs can be raised through the Security Dashboard and will receive a unique call ID that must be used in all further communications on this RFI. Each question uses one Service Ticket. No Service Tickets will be charged if the RFI is related to an existing escalation of an Incident, Health or Other Incident. Service Tickets are charged once a Serviced Device has been declared Ready for Operations (RFO). Inquiries not directly available through the Security Dashboard or which require a more detailed analysis compared to what is available on the Incident Reports will not be considered as a regular RFI. Examples of such requests are requests to retrieve raw data for forensics and additional one-time reports. Verizon may accept such request pursuant to a separate agreement.

2.3.8 **Data Availability and Retention.** Log Management collects, stores and searches raw logs, and is enabled for all MSS-Cloud Services. Log Management supports field-based filtering and raw log searches for up to 90 days or 0.2 TB per MSS-Cloud Service, whichever occurs first. Log Analytics provides interactive search and analysis capabilities to search log data and works on the same data as the log management capability with the same data storage limitations.

Information on Security Incidents and raw Events associated with Incidents are stored in the SMC and are kept for one year. Archived Incidents can be made available to Customer via a Service Request - RFI through the Security Dashboard. The number of Service Tickets charged and the response time is dependent on the amount of data to be retrieved and the complexity of the request. The data on raw Events can be made available upon request up to one month after service has ended on that MSS-Cloud Service. At the end of such retention period, Logs and Customer sensitive data will be disposed of in accordance with the relevant Verizon policies.

The amount of data Verizon receives for a MSS-Cloud Service in any month may not exceed 10 GB. Verizon will charge Customer Service Tickets for any amount of data received for a MSS-Cloud Service during a month in excess of 10 GB as set forth in the following table:

Additional Data Received (each MSS-Cloud Service)	Service Tickets Charged
10 Gigabyte	6 Service Tickets

2.3.9 **Service Security Management.** Verizon will maintain a maximum of five user name and password combinations for authenticating on a Service Element. The Customer will provide, monitor, and manage an external authentication server if the number of user names and passwords exceeds five. The type of use of external authentication server with MSS-Cloud depends on the Customer determined capabilities of such Customer-provided server and the Customer's network environment.

2.3.9.1 **Configuration Management.** Verizon will pro-actively provide suggestions to the Customer for maintaining the configuration of a Service Element in line with new Threats and changes in the environment. The frequency is dependent on the sources of security intelligence and other factors Verizon uses in delivering the MSS-Cloud service to the Customer.

- **Customer Responsibilities.** Customer requested configuration changes to Service Elements are made using the Change Request procedures detailed in Change Management Process section. Customer is responsible for the configuration management of Subordinate Devices.

2.3.9.2 **Rule Set Management.** Verizon will implement the initial Rule Set that the Customer has developed, and Verizon has reviewed, during MSS-Cloud activation. Customer may request changes to a Rule Set at any time and Verizon may implement the change following Verizon's evaluation of the proposed change. Customer can obtain a copy of a Rule Set at any time via the Security Dashboard.

2.3.9.3 **Customer Initiated Change Requests.** Customer Initiated Change Request (Change Requests) can only be submitted by Authorized Users through the Security Dashboard. Verizon may reject Change Requests which are not properly submitted (e.g., a Change Request not submitted on the Security Dashboard or an ambiguous or unclear Change Request). Verizon will email the Authorized User if a Change Request is rejected. Verizon assigns a unique number to each Change Request submitted. Customer must use this number in all communications about the Change Request. The number of Service Tickets consumed by an implemented Change Request is determined by the type of change request and SLA to accept and implement. Verizon may ask Customer for additional confirmation and authorization before implementing a Change Request. Verizon will send a confirmation request to the Authorized Users. A Change Request has a status in each phase of its lifecycle as shown below. When the status changes, an SMC Time Stamp is attached and the Customer is emailed. The Service Description provides additional details and conditions relating to the different types of Customer-initiated Change Requests, as described below:

Status Levels in the Acceptance Phase	**Change Request Conditions**
New	The Change Request has been received by Verizon.
Assigned	The Change Request has been assigned to a security analyst.
Reopened	The Change Request has been reopened for further action or feedback. This may be due to an internal Customer or failed change.
Work in Progress	The Change Request is being managed by a Security Engineer.
Hold	The Change Request is under review and the SLA is paused
Status Levels in the Implementation Phase	**Change Request Conditions**
Hold - Accepted	The Change Request has been reviewed and accepted for implementation. The implementation SLA is in effect.
Hold - Internal	The Change Request has been put on hold by Verizon and the implementation SLA is in effect.
Hold – Under Review or Pending Peer Review	The Change Request is pending an action from Verizon. The implementation SLA is in effect.
Hold – Customer Request or Awaiting Customer Feedback	The Change Request is on hold by request Customer or it is on hold pending an action by Customer which is preventing the implementation of the Change Request. The implementation SLA is not in effect.
Hold – Internal Vendor	The Change Request is pending an action by a Verizon vendor and implementation of the Change Request is pending. The implementation SLA is in effect.
Hold – Scheduled Work	The Change Request has been scheduled for a specific date and time to activate the Change Request. The implementation SLA is in effect.

Status Levels in the Verification Phase	Change Request Conditions
Resolved - Discarded	The Change Request has been discarded. The implementation SLA is stopped.
Resolved - Implemented	The Change Request has been implemented. The implementation SLA is stopped.
Closed	The Change Request has been Implemented and Customer has verified the implementation. No further action is required.

- **Regular Change Request.** A Regular Change Request (RCR) is a planned change to the topology of Customer's infrastructure or security Rule Set that:
  - involves changes to existing rules, or the creation of new rules or objects, in the Service Rule Set,
  - involves creation of new hosts in the policy, and the host is part of a subnet that is already accessible and configured on the Serviced Device,
  - involves allowing or disallowing traffic between existing hosts,
  - involves a change to the application software, or
  - involves changes to operating system settings, except for changes to IP addresses.

  Verizon reviews and accepts an RCR within 24 hours after submission. Verizon implements an accepted RCR in the next Maintenance Window, provided that the minimum time between submitting an RCR and its implementation is at least 48 hours. RCRs consume two Service Tickets.

- **Major Change Request.** A Major Change Request may be needed in addition to an RCR. Such a change can be implemented subject to a separate agreement or at a mutually agreed number of Service Tickets under this Service Attachment. There are no SLA's for the implementation of a Major Change Request. A Change Request is Major when it involves any of the following:
  - More than ten simultaneous changes to a Rule Set,
  - Changes to the IP addresses of a designated Service Element,
  - A redesign of Customer's environment or infrastructure,
  - Introduction of a new device or application in the infrastructure, changes estimated to require more time than available in a Maintenance Window, or configuring of a new site-to-site VPN tunnel on the Serviced Device (Only available for Internet firewall services). Verizon provides management of up to 10 tunnels as part of the Firewall service. Major Change Requests do not include Availability or Health Monitoring for these tunnels. The first 10 tunnel configurations are included, but additional charges apply for > 10 VPN tunnels. There are no SLAs for the implementation of a Major Change Request.

- **Fast-Track Change Request.** A Fast Track Change Request is a planned or unplanned change that:
  - Impacts existing rules or the creation of new rules or objects in the Rule Set of the Serviced Device, as long as a maximum of three MSS Serviced Devices are involved.
  - Creates new hosts in the policy of the Serviced Element as long as the host is part of a subnet that is already accessible and configured on the Serviced Device.
  - Allows or disallows network traffic between existing hosts.

  A Fast Track Change Request consumes six Service Tickets.

- **Urgent Change Request.** An Urgent Change Request (UCR) is an unplanned change which:
  - Modifies existing rules or the creation of new rules and/or objects in the Rule Set of one MSS-Cloud service; or
  - Involves changes that specify the required configuration setting and its new value.

  Customer will provide the following when submitting a UCR:
  - Detailed information sufficient to allow Verizon to evaluate the request within the SLA target of ≤ two hours.
  - Availability of an Authorized Contact by telephone to further clarify the UCR.

- Confirmation of Customer decisions made during phone calls with Verizon sent via Email to the Verizon SOC.
- UCRs consume eight Service Tickets.

Customer acknowledges that a UCR gives Verizon less time to review and mitigate potential availability or security risks associated with the change request and, therefore, implementation of the UCR carries a higher degree of risk. Customer accepts all risks associated with a UCR when submitting such a request.

- **Verizon Initiated Emergency Change Request.** Verizon may implement Emergency Change Requests such as changing the Rule Set of the Service. Verizon may also disable Threat Signatures under the following circumstances:
  - Verizon witnesses or is notified of a massive attack or of a virus/worm outbreak with the risk of flooding Customer's infrastructure; or
  - Verizon notes flooding that may be caused by changes in the topology of Customer's infrastructure (e.g., rewiring, adding new subnets, new applications with new protocols, mis-configured Subordinate Devices); or
  - If Verizon believes that changes to the Service Context submitted by Customer to Verizon are believed to influence a Rule Set. These changes may include adding, removing, or moving servers, adding new applications or web servers, and changes to Rule Sets in adjacent Customer managed devices.

  Verizon is authorized to make changes to the Service Element Rule Set and to disable Threat Signatures in emergencies and according to the procedures for Urgent Change Requests.

2.3.9.4 **Security Services Advisor.** Customer is assigned a SSA who will host a quarterly service review meetings. The SSA is assigned to multiple MSS customer accounts and is not dedicated to Customer. The SSA assists with the following items:

- Training on Security Dashboard/Security and Compliance Dashboard.
- Manages Customer Communication and Security Advisories.
- Provides assistance in scheduling a quarterly external network scan.
- Manages service issues and Service Credit requests.
- The SSA may perform additional functions as described in the Service Description.

The SSA is the Customer escalation point for issues regarding the amount of Service Tickets allocated to a service request and with credits, inquiries about the scope of the services, and quality of the MSS – Premises Premium service and SLA. In addition, the SSA makes recommendations to improve Customer's security and risk posture, analyzes the Serviced Device capacity lifecycle, provides Customer-specific and industry-specific risk advisories, assists Customer with critical asset identification and internal/external vulnerability scanning and scan data uploads to improve Threat Analysis and Security Incident Handling, and provides training to Customer on the use and features of the Security and Compliance Dashboard. (Note: Unified Security Services do not include Security Services Advisor support.)

3. SERVICE TERMS AND CONDITIONS.

3.1 **Excluded Services.** The parties acknowledge that Verizon has no obligation to provide MSS-Cloud services for any Verizon IP Services that: (i) utilizes native IPv6 addressing, IPv6 parallel with IPv4 (aka "Dual Stack") or does not encapsulate IPv6 addresses within IPv4 addresses; (ii) employs Voice over IP ("VoIP") on their Verizon IP Service. Introduction or election of IPv6 or VoIP by Customer may render the MSS-Cloud services inoperable and subject Customer to loss of service.

3.2 **Service Period and Termination.**

3.2.1 This Service Attachment will continue in force and effect until the termination or expiration of all Service Elements that it covers. The Initial Service Period for each Service Element is effective upon the Service Activation Date and shall continue in force for no less than 12 months, at which time the terms are automatically extended until either party terminates it upon 30 days prior written notice. Customer accepts and agrees that, in the event (a) Customer terminates any Service Element for convenience or (b) Verizon terminates any Service Element for Cause prior to the end of the Service

Element term, then Customer will pay Verizon all unpaid fees payable under this Service Attachment with respect to such Service Element for the remainder of such Service Element term. Customer will promptly pay Verizon's invoice in accordance with the terms of the Agreement.

3.2.2 **Order Confirmation.** Verizon will confirm Customer's order via email and the date of this email is the Order Confirmation Date. The Order Confirmation will confirm the Service Elements requested.

3.2.3 **Ready For Service.** The Service Activation Date is the date on which Verizon begins providing a Service Element. Customer will receive a Service Activation Date notification as each Service Element becomes active.

3.3 **Customer Responsibilities.**

3.3.1 **MSS-Cloud Service Requirements.** MSS-Cloud is offered subject to (i) the Customer's continued subscription to eligible Verizon IP or Secure Cloud Interconnect services. It is the Customers responsibility to ensure subscriptions are maintained to enable Verizon to properly perform, provision, support and maintain MSS-Cloud; (ii) compliance with MSS-Cloud prerequisites and operational procedures as set forth herein; and (iii) prompt notification to Verizon of any changes to the nomination and/or authorization level of the individuals Customer has authorized to oversee, monitor or evaluate the provision of MSS-Cloud.

3.3.2 **Consents and Permissions.** Customer has obtained, or will obtain, all legally required consents and permissions from users communicating over the Internet or to a Cloud Service Partner via MSS-Cloud for Verizon's performance of MSS-Cloud, including without limitation the collection, use, processing, analyses and disclosure to Customer of Customer's Internet traffic data.

3.3.3 **Modifications.** The Customer acknowledges that modifications or changes to the Customer Environment may cause interoperability problems or malfunctions in a designated MSS-Cloud service and/or the Customer Environment. The Customer acknowledges that it is Customer's responsibility to maintain, at its sole cost and expense, the Customer Environment to ensure that the Customer Environment is interoperable with each MSS-Cloud service.

3.3.4 **User Interface.** In connection with the provision of MSS-Cloud, Customer may be provided with one or more user IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or such other means of authentication (Login) to access a web-based portal, dashboard, or other form of user interface (User Interface). The User Interface and Login may be used for accessing on-line services, authorizing instructions and requests using MSS and/or ordering additional services or Service Tickets (if applicable). Customer shall at all times keep its Login strictly confidential and shall take all reasonable precautions to prevent unauthorized use, misuse or compromise of its Login. Customer agrees to notify Verizon promptly upon learning of any actual or threatened unauthorized use, misuse, or compromise of its Login. Verizon is entitled to rely on Customer's Login as conclusive evidence of identity and authority. Customer shall be responsible for all activities and charges incurred through the use and/or compromise of Customer's Login, , unless the unauthorized use, misuse or compromise of Customer's Login is solely attributable to a Verizon's gross negligence or willful misconduct.

3.3.5 Customer acknowledges and agrees that MSS-Cloud is offered and provided by Verizon to multiple customers doing business in various industries. Absent terms to the contrary in the Agreement, MSS-Cloud is implemented without specific controls that may generally be required or customary for customers in any particular industry and is not designed to satisfy any specific legal obligations. Customer shall be solely responsible for determining that MSS-Cloud satisfies Customer's obligations under law or contract. Customer agrees to use MSS-Cloud in accordance with all applicable laws and not to use MSS-Cloud in any manner that imposes obligations on Verizon under any laws other than those laws with which Verizon agrees to comply as specifically set forth in the Agreement. Without limiting the generality of the foregoing, Customer agrees not to cause, or otherwise request that Verizon create, receive, maintain or transmit protected health information (as defined at 45 C.F.R. § 160.103) for or on behalf of Customer in connection with MSS-Cloud or in any manner that would

make Verizon a business associate (as defined at 45 C.F.R. § 160.103) to Customer. In the event Customer acts or uses MSS-Cloud in a manner not permitted under this Section 3.5, Customer shall (a) be in material breach of the Agreement, including this Service Attachment; (b) take, at Customer's expense, prompt action to correct and/or mitigate the effects of Customer's breach of this Section 3.5; and (c) provide Verizon with reasonable cooperation and support in connection with Verizon's response to Customer's breach of this Section 3.5, Customer shall assume and be solely responsible for any reporting requirements under law or contract arising from Customer's breach of this Section 3.5.

3.4 **Warranties.**

3.4.1 **Verizon Warranties.** Verizon warrants to Customer that it will perform its obligations in a good and workmanlike manner. The remedies set forth in the appropriate service level agreement (SLA) portion of this Service Attachment are Customer's sole and exclusive remedies in connection with the portions of MSS-Cloud related to the failure to meet any standard set forth in the SLA. Verizon does not warrant that MSS-Cloud will detect and prevent all possible threats and vulnerabilities or that such services will render Customer's network and systems invulnerable to all security breaches and vulnerabilities.

3.4.2 **Third Party Warranties.** For any third party products and/or services incorporated as part of MSS-Cloud, Customer shall receive only the warranties offered by such third party to the extent Verizon may pass through such warranties to Customer.

3.4.3 **Customer Warranties.** Customer represents and warrants that (a) it has and will continue to have all rights, permissions, authority and network user consents necessary to have Verizon perform MSS (including, without limitation, all rights, permissions and authority necessary in respect of any IP address assigned to a MSS-Cloud service) and consent from its network users to Verizon's logging and monitoring activities hereunder), (b) will not provide any PHI to Verizon for purposes of Verizon's performance of services hereunder; and (c) it will use MSS for lawful purposes only. Customer hereby assumes the sole responsibility for the accuracy of the IP addresses and domains provided to Verizon.

3.5 **Assumption of Risk.**

3.5.1 **Scanning Risks.** MSS-Cloud involves the use of Internet based network scanning technology that has inherent risks, including, but not limited to, the loss, disruption, or performance degradation of Customer's or a third party's business processes, telecommunications, computer products, utilities, or data (the Scanning Risks). When Customer requests network scanning, or any MSS-Cloud component utilizing network scanning, Customer authorizes Verizon to perform the network scanning and assumes all risk for adverse consequences resulting from or associated with such component of MSS-Cloud. Customer represents and warrants that it has obtained all consents and authorizations necessary to perform network scanning on any Cloud Service Partner IP addresses. Verizon shall take reasonable steps to mitigate these Scanning Risks; however, Customer understands that these Scanning Risks are inherent in the provision of certain computer security services and the use of certain computer security products and cannot be eliminated. Customer shall indemnify and defend Verizon for all costs and expenses related to a third party's claim of loss, damages and liabilities (including legal expenses and the expenses of other professionals) incurred by Verizon, resulting directly or indirectly from any claim attributable to or arising out of Verizon's use of network scanning technology (each, a Scanning Claim), including, without limitation, the use by Verizon of network scanning technology to analyze assets that are not controlled directly by Customer, including, without limitation, servers hosted by third parties. This obligation of Customer in connection with a Scanning Claim shall not apply if Verizon's gross negligence or willful misconduct gave rise to such Scanning Claim.

3.5.2 **Change Requests.** Customer assumes all risks associated with Change Requests initiated by Customer. Verizon will deliver Change Requests strictly in accordance with the instructions provided by Customer. Verizon has no responsibility to provide technical advice to Customer in relation to the Change Requests, and the risks associated with such Change Requests.

3.6 **Third Party Products or Services.** The parties agree that Verizon shall not be liable for any damages caused by hardware, software, or other products or services furnished by parties other than Verizon, its agents, subcontractors, or any damages caused by the products and/or services delivered by or on behalf of Verizon which have been modified, serviced, or otherwise attended to by parties other than Verizon or without Verizon's prior written and express consent. Customer acknowledges that Verizon shall not be liable for any damages resulting, directly or indirectly, from any act or failure to act by Customer or any third party (including, without limitation, the non-performance, defaults, omissions or negligence of any third party that provides telecommunications services in the country or countries in which Customer's premises or systems are situated and other countries from, across, to or in respect which MSS-Cloud is provided by or on behalf of Verizon).

3.7 **Industry Alerts and Third Party Updates and Patches.** WITH REGARD TO SERVICES WHICH PROVIDE INFORMATION SHARING AND/OR INDUSTRY ALERTS, VERIZON DISCLAIMS ANY LIABILITY TO CUSTOMER, AND CUSTOMER ASSUMES THE ENTIRE RISK FOR (A) INFORMATION FROM THIRD PARTIES PROVIDED TO CUSTOMER WHICH TO THE BEST OF VERIZON'S INFORMATION, KNOWLEDGE AND BELIEF DID NOT CONTAIN FALSE, MISLEADING, INACCURATE OR INFRINGING INFORMATION; (B) CUSTOMER'S ACTIONS OR FAILURE TO ACT IN RELIANCE ON ANY INFORMATION FURNISHED AS PART OF MSS-CLOUD; AND/ OR (C) THE USE OF ANY THIRD PARTY LINKS, PATCHES, UPDATES, UPGRADES, ENHANCEMENTS, NEW RELEASES, NEW VERSIONS OR ANY OTHER REMEDY SUGGESTED BY ANY THIRD PARTY AS PART OF MSS-CLOUD.

3.8 **Intellectual Property Rights.** Neither party acquires right, title or interest in or to the other party's information, data base rights, data, tools, processes or methods, or any copyrights, trademarks, service marks, trade secrets, patents or any other intellectual or intangible property or property rights of the other party by virtue of the provision of MSS-Cloud or materials delivered pursuant MSS-Cloud service. Customer retains all right title and interest in and to the underlying factual data gathered through the provision of MSS-Cloud. Verizon owns all right title and interest in and to Verizon's trade secrets, confidential information or other proprietary rights in any creative or proprietary ideas, information or other material used by Verizon or presented to Customer (each, a Technical Element), including, but not limited to: data, software, modules, components, designs, utilities, databases, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices, report formats, manner of data expression and specifications. Verizon grants Customer a nonexclusive, royalty-free license to use each Technical Element integrated into any deliverable solely for Customer's internal business purposes. Customer may disclose a Technical Element integrated into a deliverable to a third party as long as such third party is subject to a written nondisclosure agreement, requiring such third party to maintain the confidentiality of such Technical Element and to use such Technical Element only for the benefit of Customer. Notwithstanding anything contained herein to the contrary, Customer is prohibited from creating derivative works of all or any portion of a Technical Element.

3.9 **Confidential information.** Customer acknowledges that the following information constitutes Confidential Information hereunder: (a) the methods, systems, data and materials used or provided by Verizon in connection with the provision of MSS-Cloud; and (b) the results of Verizon's assessment of Customer and all reports issued by Verizon in connection with such results including, without limitation, security analyses and insight (Net Intel Information). Customer will disclose Net Intel Information only to Customer employees with a need to know for the purposes set forth in this Service Attachment and who are bound to confidentiality obligations at least as restrictive as those set forth in the Agreement and this Service Attachment. In no event may Customer use lesser efforts to protect Net Intel Information from use or disclosure not permitted under the Agreement than it uses to protect its own highly-sensitive confidential information, or less than reasonable efforts. The term Confidential Information shall not include information that is comprised of statistical information, or other aggregated information regarding security vulnerabilities, security configurations and the like insofar as such information does not identify Customer or Customer's computer network or computer systems.

3.10 **Encryption Approvals in India.** Encryption functionalities associated with the management service of MSS-Cloud may only be provided to Customers that have obtained permission from the Indian Department of Telecommunications or other Indian governmental authority or officer specially designated for the purpose. Customer is solely responsible for obtaining such approvals.

4. **Service Level Agreement.**

4.1 The service level agreement (SLA) for MSS-Cloud may be found at the following URLs:

Managed Security Services – Cloud Premium + Service Level Agreement (at www.verizonenterprise.com/external/service_guide/reg/cp_msscloud_plus_sla.pdf) for U.S. Services
Managed Security Services – Cloud Premium + Service Level Agreement (at www.verizonenterprise.com/external/service_guide/reg/cp_msscloud_plus_sla_2013JUL19.pdf) for non-U.S. Services

5. **Definitions.** Capitalized terms not defined herein have the meaning described in the Agreement. The following definitions apply to MSS-Cloud, in addition to those identified in the Master Terms and the administrative charge definitions at the following URL: www.verizonenterprise.com/external/service_guide/reg/definitions_toc_2017DEC01.htm

Defined Term / Acronym	Definition
24x7	Nonstop service, 24 hours a day, seven days a week, 365 (366) days a year, independent of time zones and local or international public holidays.
Business Days	Monday through Friday, excluding Christmas and New Year's Day, from 00:00 UTC to 24:00 UTC.
Change Request	A request from the Customer, or from Verizon, for a change to MSS Cloud.
Correlation	Comparing data from multiple sources to find patterns and relationships that may point to attacks and abuse.
Cloud Service Partner	A third party or Verizon entity providing Cloud Infrastructure and other services to the customer that is eligible for Secure Cloud Interconnect services.
Designated Circuit	A Verizon IP Service circuit specifically applied to MSS-Cloud for a Service Element.
Event	A data record produced by a Service Element when it detects a Threat. Such a record may be an SNMP trap, a Service Element-generated event, an entry in a log, or an xml event. An Event may also be called "alert".
Exploit	A method to use a Vulnerability to gain unauthorized access to functions, data, or privileges, generally with malicious intent. An exploit can include a script, virus, Trojan, or a worm. The exploit is mainly defined by the way it replicates and spreads. • An attack is the use of an Exploit. • A script refers to a document with steps to manually find and exploit vulnerabilities. A script is replicated by publishing it. • A virus refers to malicious software attached to a medium (e.g. files, removable media, or documents). A virus replicates using this medium. • A Trojan refers to malicious software embedded in applications. The Trojan will not replicate itself; it spreads with the application. • A worm refers to a self-contained program (or set of programs) that spreads copies of itself to other computers. A worm can spread through network connections and e-mails in a matter of hours.
Incident	A single Event, or a series of Events, that may represent an intrusion attempt, a reconnaissance attempt or that otherwise require the attention of a security analyst. An Incident may also reflect an "attack".
Incident Record Communication	A record in the system that tracks and drives the workflow of Incidents during their lifecycle to closure.
Logs	A collection of various IT, compliance, network, application, and security related Events.
Maintenance Window	A time window for Verizon to perform certain maintenance or management procedures on internal Verizon MSS infrastructure (not necessarily MSS-Cloud infrastructure) set in the Service Context. During a Maintenance Window, MSS may be temporarily disrupted or unavailable. Maintenance windows are limited to a maximum of 6 hrs.

MANAGED SECURITY SERVICES – CLOUD PREMIUM +

Defined Term / Acronym	Definition
Other Incident Ticket	A ticket for service related incidents logged with Verizon and created by the Customer or Verizon. Other Incident Tickets will consume Service Tickets, as outlined in this Service Attachment.
RFO	Ready For Operations - The date (following the Service Activation Date) that Verizon sends RFO notice to Customer documenting agreement by Customer and Verizon that the MSS-Cloud service and SEAM policy have been fine-tuned and the escalation parameters, Service Context and procedures have been set as mutually agreed. From this date, the SLA becomes effective. RFO is given per Service Element.
Refresh Rate	The rate at which information on the Security Dashboard/Security and Compliance Dashboard is refreshed. The Refresh Rate varies dependent on the type of information and the MSS-Cloud service to which the information relates as shown in this Service Attachment.
Rule Set	The security policy or rules used by a Service Element or by SEAM. The Rule Set may also be called "policy" when there is no confusion with corporate or other policies.
SEAM	State and Event Analysis Machine – Proprietary Software used by Verizon to process logs, alerts, and scan reports from MSS-Cloud services. Its functions include: • Normalization – converting entries in logs and individual alerts into generalized Events. • Classification – giving Events a first classification, using Verizon proprietary Event Classification Policy Language, filtering out false positives or Events related to vulnerabilities absent in the targeted environment. • Correlation – reclassifying or combining Events into meaningful Incidents that will be handled by Verizon security analysts. • Pattern matching – recognizing patterns pointing to reconnaissance scans, infections, or attacks. • Statistics – calculating averages to discover trends and anomalies, and to allow comparisons. • Workflow management – recording the activities for an Incident. • Information management – managing the information needed to examine, evaluate, and classify Incidents. • User management – defining the views and authorization levels of users
Secure Cloud Interconnect or SCI	A Verizon service that allows direct, secure access between selected Cloud Service Partners and private networks that Verizon provides for Customer. These connections do not traverse the public Internet.
Security and Compliance Dashboard / Security Dashboard	A secured web portal for Customer authorized staff to access in connection with Premium MSS-Cloud service. It is the main point of communication between the Customer and Verizon for Premium MSS-Cloud service.
Security Upgrade	Changes to a software program to fix a security hole; generally released by the software manufacturer or editor. A Security Upgrade concerns small improvements to the software; security Upgrades generally do not contain substantial new features or functions. A Security Upgrade may also refer to a "patch", "bug fix", "service pack" or "update".
Service Context	A set of documents, with version control, posted on the Security Dashboard, containing information about the Customer that Verizon uses for the provisioning of MSS-Cloud to the Customer. The Service Context is setup during the service initiation phase and is maintained via the change management process. Customer can also add or update host information in the Service Context. The Service Context may include one or more of the following: • Specification of Maintenance Windows • Procedures, templates for escalation, notification, reporting, change control processes and authorization procedure • Contact details and authorization for escalation, notification, and reporting • Secure E-mail Certificates • Roles and Responsibilities in the form of a RACI Matrix between Customer and Verizon for the different service components • Details on maintenance and support contracts • Network topologies and asset inventories of systems that can be reached through the security infrastructure
Service Element	A specific Rule Set applied on the MSS-Cloud infrastructure to perform MSS-Cloud service on Customer's Internet traffic on a Designated Circuit Service Elements are shown in the Service Context section of the Security Dashboard and called as "Service Devices" on the Security Dashboard.

MANAGED SECURITY SERVICES – CLOUD PREMIUM +

Defined Term / Acronym	Definition
Service Ticket	A unit for charging certain usage-based services under MSS. A number of Service Tickets are included in each MSS-Cloud service by default per 12-month period following the Service Activation Date.
SMC	Security Management Center. A data center that hosts the systems for monitoring, managing, or supporting the MSS-Cloud services. The SMC includes: equipment to collect events, management stations, the SEAM engines, signing engines, Security Dashboard, and back-end systems such as back-up devices, file servers, and terminal servers. The SMC may include equipment owned by the Customer.
SMC Time Stamp	A time stamp, recorded by Verizon at the SMC, reported on the Security Dashboard and taken as reference for measuring the service levels. The SMC Time Stamp is recorded in UTC and synchronized worldwide using the Network Time Protocol ("NTP").
Threat	A (suspected) use of an Exploit, or the (suspected) presence of a Vulnerability in the configuration, platform, or application code. A Threat can be an infection by a worm or virus, or it can be a targeted attack. Exploits can also be combined into blended Threats, exploiting multiple security holes.
Threat Signature	Code used to recognize a Threat by its pattern. A Threat Signature may contain algorithms to detect dynamically changed malicious behavior, combat obfuscation, or impersonation.
UTC	Coordinated Universal Time. Universal Time indication, standardized by the Bureau International des Poids et Mesures (BIPM) and defined in CCIR Recommendation 460-4. The UTC is the time indicated on atomic clocks. Verizon consults and uses it for its SMCs via the Internet protocol NTP. The UTC code uses the 24-hour clock. 4 pm (afternoon) is equal to 16:00 UTC. Depending on the daylight savings period, the UTC is 4 or 5 hours ahead of Eastern Standard Time ("EST"), and 1 or 2 hours behind Central European Time ("CET").
Verizon IP Services	The Verizon IP services that are eligible for MSS Cloud, namely; Verizon Secure Gateway Universal Port, Verizon Internet Dedicated Access and Verizon Internet Dedicated Ethernet services, including tiered and burstable bandwidth, as well as resilient or failover services.
Vulnerability	A security hole; a defect that can be exploited to gain access to data, functions, or privileges violating the intended authorization. Vulnerabilities can range from defects in application or system software (e.g. bugs), in the user administration (e.g. non-protected user accounts), in the configuration (e.g. unintended network or file access), in the policy and Rule Set definition (e.g. unrestricted open ports or exposed IP-addresses), etc. The combination of all vulnerabilities of a given system or infrastructure is the exposure.
Work-around	An alternative function or method, often using a temporary patch or reconfiguration, to achieve a result equivalent to the original function or method.