verizon

MANAGED SECURITY SERVICES – PREMISES PREMIUM

1. GENERAL

1.1 **Service Definition.** Managed Security Services (MSS) - Premises Premium offers Monitoring or Monitoring and Management services for a selection of Serviced Devices, where available, as described below and in the service matrix table attached as Appendix I. MSS Premium Plus or Security Enterprise Service+ are available as additional optional services, as described in Section 1.6. Unified Security Services (USS) is only available for Monitoring and Management service, as described in Section 2.0.

1.1.1 **Platforms**. Except where explicitly stated otherwise, these terms apply to Optimized Service (denoted with a + and sometimes referred to as Rapid Delivery) and non-Optimized Service.

1.2 **Service Implementation.** Verizon will assign a Project Manager to Customer who will schedule a kick off meeting to introduce the Verizon service delivery team, identify the Authorized Contacts for Customer, discuss the scope of the MSS – Premises Premium service and its business impacts, and obtain any required information from Customer. Upon receipt from Customer of a completed Deployment Kit, Verizon

will create a proposed project plan with high-level milestones and timelines. Verizon will only provision MSS – Premises Premium after Customer has approved the project plan.

1.3 Premium Service: Monitoring

1.3.1 Device Availability, Device Health Monitoring and Other Incidents

- **Device Availability.** Verizon monitors the availability of the Serviced Device 24x7.
- **Device Health Monitoring.** Verizon monitors the health of the Serviced Device 24x7 by measuring disk space, CPU resource usage, memory and swap usage, network utilization, time synchronization, failover status, Log intake, and other device and service level statistics depending on the device type. Verizon establishes a health threshold for each of the health parameters reported by the Serviced Device and creates a Health Incident if one or more thresholds are exceeded.
- **Other Incidents** are tickets that Verizon or Customer can create for service related incidents on the Serviced Devices that are not related to an availability, health or Security Incident. They can be logged on a 24x7 basis.

1.3.1.1 **Severity Level.** The Severity Level is based on the information received from Customer and on the impact of the problem on Customer's network environment. For Severity 1 and 2 problems, Customer and Verizon will each assign a dedicated contact as defined in the Service Context. Verizon will only interact with the Authorized Contacts registered in the Service Context. Verizon assigns a Severity Level (as shown below) to every support request that it accepts.

Problem Severity	Level	Error Conditions
Severity 1	S1	A critical error causes the Serviced Device or the Services to fail. Normal day-to-day business is not possible, e.g. system failure, or an inaccessible or inoperable production system.
Severity 2	S2	An error significantly affects the functions of a serviced device in a high availability set-up and impacts normal day-to-day business. Non-critical performance degradation. A severity 1 incident where a Workaround exists.
Severity 3	S3	An isolated error impacts the functions of the Serviced Device and there is no important impact on the day-to-day business. A severity 2 incident where a Workaround exists.
Severity 4	S4	An error has been identified. There are no problems with the Serviced Device, and there is no immediate impact on the production environment. A severity 3 incident where a Workaround exists.

1.3.2 Threat Analysis, Threat Detection and Security Incident

1.3.2.1 **Threat Analysis.** A Security Incident is generated after Logs and Security Events have been processed through threat detection policies and use cases. Verizon defines Security Incidents and Security Incident Tickets as follows:

- **Security Incident.** A single Security Event or a series of Security Events that have been aggregated and correlated based on Verizon's proprietary's threat detection policies. A Security Incident may represent an attack.
- **Security Incident Ticket.** A record in the system which tracks and drives the workflow of escalated Security Incidents during their lifecycle to closure. A Security Incident Ticket may contain one or more Security Incidents.

1.3.2.2 **Threat Detection.** Verizon's threat detection policies are, amongst others, based on a behavior-based, multi-factor correlation capability processed through the Verizon Security Analytics Platform which evaluates and correlates reputational and behavioral patterns and characteristics in addition to signature-based detection methods. Verizon correlates and aggregates related Security Events into

Security Incidents automatically through its threat detection policies. Verizon has a wide variety of methods to detect Security Incidents.

Security Events may appear harmless when they are detected in isolation; however, when they are combined with information from other Security Events or from information in the Service Context, a more harmful pattern may appear. Security Events will be compared with Customer's Service Context and output obtained from network vulnerability scans. The Customer Portal provides a range of reporting functions.

1.3.2.3 **Security Incident Classification.** Verizon classifies Security Incidents in the 4 categories listed in the chart below. A Security Incident classification may change based on additional analysis, intelligence or after Customer provided feedback.

Security Incidents Classification

Security Incident Classification	Risk Levels	Conditions
Insufficient Info	L0	The Security Incident has been classified as Insufficient Info based on the associated Security Events.
Harmful Attack	L1	The Security 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 Security Incident renders Customer's infrastructure vulnerable or compromised.
Harmless Attack	L2	The Security 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 Security 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	L9	These levels are used during the first phase of a deployment, or after major changes in the network (such as adding, removing, moving or replacing a Serviced Device, changing security policies and Rule Sets, installing major signature updates or major software upgrades, or implementing an Urgent Change Request). These Security Incidents will only be logged without real time analysis.

1.3.2.4 **Security Incident Handling.** Verizon generates Security Incidents in both real and non-real time, depending on the detection method. The status of the Security Incident will be changed throughout its lifecycle. Status changes are communicated by email and are displayed on the Customer Portal.

1.3.2.5 **Security Incident Status.** A Security Incident status may change based on additional analysis, intelligence or after Customer provided feedback.

Security Incident Status

Security Incident Status	Conditions
Open	The Security Incident has been generated based on Verizon's threat detection policies. SMC Timestamp (UTC) when the Security Incident is created.
Active	The SOC starts the investigation.
Notify	The SOC identifies whether Security Incident is a Harmful Attack (L1) or if it requires further information, Insufficient Info (L0), to classify the Security Incident.
Escalated	A Security Incident Ticket is created with information to allow the mitigation, containment or resolution of the risk.
Closed	The Security Incident has been auto-closed or closed by the Security Analyst.

1.3.2.6 **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 increase insight into Security Incidents and reduce the number of false-positive Security Incidents. The Security Incident descriptions provide recommendations on possible actions Customer can take. The Security Notification SLA applies.

1.3.2.7 **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 Security Incidents periodically with broader security information. If a Security Incident or a combination of Security Incidents is considered to be important, the SOC will escalate it. This method optimizes Security Incident handling and focuses on escalating potentially harmful Security Incidents and reducing Insufficient Info Security Incidents and False Positives. The Security Incident Notification SLA applies.

1.3.2.8 **Non-Real Time Security Incidents for Security 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 (known as Security Digests) will be closed automatically, but can be reviewed by Customer on the Customer Portal. Security Digests are focused on specific topics. This Security Incident handling is optimized for certain types of Security Incidents that do not require real time Security Incident handling and SOC review. They provide additional information to Customer and can support compliance initiatives. The Security Incident Notification SLA does not apply for Security Digests. Customer-specific Security Digests can be developed at Applicable Rates.

1.3.2.9 **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 Security Events and Security Incidents, and evaluate the possible impact of a threat/attack on Customer's Serviced Devices before escalating a Security Incident Ticket. 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.

- Verizon will escalate a Security Incident Ticket with the following Security Incident information:
  - Security Incident Ticket number
  - UTC timestamp of the Security Incident creation with the identity of the affected Serviced Device(s) and their source and destination information, if available
  - Threat signature and use case information, if applicable: threat use case ID, name, and description
  - Packet dumps, if obtainable from the Serviced Device and Subordinate Devices using the existing infrastructure.

- Security Incidents classified as Insufficient Info require missing information from Customer within 14 days. If missing information is not provided, Verizon will send a reminder or change the status of the Security Incident to Closed.

- For up-to-date and accurate records of Customer's infrastructure inventory, to tune the detection policy, and to close and classify the Security Incidents appropriately for reporting purposes, any Customer remediation action shall be reported to Verizon.
- In the event that mitigating actions are to be taken by Verizon on any Serviced Device, Customer understands that they will be required to authorize a Change Request to enable such action by Verizon.

1.3.3 **Basic Monitoring.** Monitoring is also available as Basic Monitoring which does not include Device Availability and Health Monitoring or Device Management services.

1.4 **Premium Service: Monitoring and Management.** If Customer orders Monitoring and Management service, in addition to the Monitoring services described in Section 1.3, Verizon will manage the Customer's Serviced Devices as follows:

1.4.1 **Device Health Management.** Device Health Management includes the following:

1.4.1.1 **Device Troubleshooting.** Verizon investigates the cause of an availability, health or other incident problem of the Serviced Device through remote problem diagnosis and initiates device troubleshooting to remedy the problem remotely. Verizon may conduct root cause analysis of the problem and communicates the results to Customer, if applicable. Verizon will not conduct analysis if the source of the problem lies within the Customer responsibility (for example, Customer networking issues or Subordinate Devices not under Verizon's management). The Mean Time to Resolution (MTTR) SLA applies to Availability, Health and Other Incident Tickets for Severity 1 tickets.

1.4.1.2 **Hardware Management.** Customer has to purchase vendor maintenance and has to provide Verizon with all the associated maintenance and support credentials. Customer must have 24x7 maintenance support for the Serviced Device and authorize Verizon to act on Customer's behalf for such maintenance support. Customer must coordinate with Verizon for any upgrade or replacement of a Serviced Device. Customer may not return a Serviced Device (or any components thereof) to the manufacturer or vendor without Verizon's written consent.

Verizon escalates the problem to the vendor or the manufacturer of the Serviced Device if it detects a hardware failure. Verizon coordinates the on-site servicing of the hardware by the relevant third party maintenance service provider. Verizon does not provide any on-site maintenance for hardware unless mutually agreed under a separate written work agreement and charged at the Applicable Rates. An escalation to the manufacturer or vendor, followed by a hardware replacement or maintenance, follows the terms and conditions and the service level of the equipment manufacturer/vendor and its Return Material Authorization (RMA) policies. Hardware replacement and RMA is not supported for end-of-life devices. When Customer directly manages its maintenance and support contract with the vendor, Customer will authorize Verizon with the third party vendor to raise support cases on its behalf.

1.4.1.3 **Device Restoration.** Verizon will restore the configuration and Rule Sets of the Serviced Device, including the operating system configuration and the application software, from its own back-up copies. Following restoration, Verizon will work with Customer to test the operational availability of the Serviced Device and the connection to the SMC. Customer is responsible for installing the correct operating system version and patch level on the restored Serviced Device if it is deployed on a server platform. Replacement of a Serviced Device will also include physical installation of the replacement device and configuration of an external IP address on that device.

1.4.1.4 **Hardware Replacement and Software Upgrades.** Verizon will notify Customer on the end-of-life of a Serviced Device. The end-of-life date is the date communicated by the relevant manufacturer when the support ceases for the Serviced Device so that Customer can foresee a hardware replacement and/or a software version upgrade. Customer is responsible for replacing end-of-life or unsupported devices. Verizon will notify Customer of any critical vulnerability related to the current software version

running on Customer's Serviced Device that poses a risk to Customer's environment. Verizon may recommend an upgrade to a software version that remediates these issues. These software upgrades may require Customer to upgrade or replace its existing hardware. Customer may request software upgrades to benefit from new features and functionality released by the vendor or manufacturer, provided Verizon supports the requested software version. Hardware replacements and software upgrades/migrations may be planned and carried out by Verizon if mutually agreed under a separate written work agreement and charged at the Applicable Rates. If Customer wants to change the vendor of a Serviced Device, upgrade a model of a Serviced Device provided by the same vendor or change the location of a Serviced Device, Verizon will charge a device set-up fee NRC to perform the operational changes.

1.4.2 **Device Maintenance.** Device Maintenance includes the following:

1.4.2.1 **Software Maintenance.** Verizon monitors the manufacturer release of new security upgrades for Serviced Devices. The availability of security upgrades depends on the release schedule of the Serviced Device manufacturer. Verizon does not proactively upgrade features for each Serviced Device. Customer can request these types of upgrades through a Major Change Request for versions certified by Verizon. Additional charges may apply for major software upgrades. Verizon does not provide on-site software maintenance; Customer may purchase on-site software maintenance under a separate written work agreement at the Applicable Rates. Verizon monitors the release of security vulnerabilities and notifies Customer on critical security patches or upgrades for the Serviced Device after they have been validated by Verizon and if applicable for Customer. Verizon informs Customer of critical security patch or upgrade installations, which are installed during an agreed Maintenance Window, and confirms with the Authorized Contacts when the installation of a critical security patch or upgrade has been completed.

1.4.2.2 **Device Back-up.** Verizon uses an automated process to perform a back-up of the Serviced Devices after each configuration change or Rule Set change with a minimum of one day of interval. The back-up tools may vary depending on the device type and manufacturer, but Verizon keeps at least one back-up of the previous configuration version. These back-ups are securely stored in the SMC and may also be used to return to the previous version if updates do not have the expected result.

1.4.3 **Device Security Management.** Device Security Management includes:

1.4.3.1 **Configuration Management Changes.** Customer must use the Change Request procedure on the Customer Portal. Customer is responsible to define the configuration changes. Verizon implements configuration changes as requested by Customer through the change management process. A separate change request ticket needs to be raised per Serviced Device or per high availability cluster that requires a change.

1.4.3.2 **Rule Set Management.** Verizon implements the initial device Rule Set developed by Customer that is approved by Verizon during the service provisioning phase. The development, migration, and review of Rule Sets and/or Serviced Device policies will be subject to a separate written work agreement and charged at the Applicable Rates. Customer may request changes to the Rule Set of a Serviced Device. Verizon evaluates, prepares, and implements changes to the Rule Set of a Serviced Device as described in the change management process. Customer can obtain a copy of the Rule Set via the Customer portal.

1.4.3.3 **Customer Initiated Change Requests.** Change Requests are submitted and tracked through the Customer portal by Authorized Contacts registered in the Service Context. Verizon assigns a unique Change Request number to each Change Request submitted and Customer must use this number in all communications about the Change Request. Each Change Request Verizon implements will consume a number of Service Tickets, depending on the type of Change Request and the SLA agreement to accept and implement. Verizon will send a confirmation request to the Authorized

Contact who has submitted the Change Request, and to other Authorized Contacts registered in the Service Context if deemed necessary. The various status levels in the Acceptance, Implementation, and Verification Phase of the Change Request are 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 team.
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 of 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 – Customer's Vendor	The Change Request is pending an action by Customer's vendor, which is preventing implementation of the Change Request. The implementation SLA is not in effect, as Verizon is awaiting action from Customer's vendor.
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.

1.4.3.4 **Regular Change Request (RCR).** Verizon reviews and accepts a RCR within 24 hours after Customer submission. Verizon implements an accepted RCR in the next Maintenance Window as specified in the Service Context, provided that the minimum time between Verizon's acceptance of an RCR and the implementation is at least 48 hours. RCR is a planned change to the topology of the infrastructure or security policy that:

- is a planned change which involves changes to existing rules, or the creation of new rules and/or objects, in the Rule Set of the Serviced Device.
- 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 the distribution of traffic between existing hosts.
- involves a change to the application software.
- involves changes to operating system settings, except for changes to IP addresses.

1.4.3.5 **Major/ Complex Change Request.** A Change Request is Major or Complex when it involves any of the following:

- More than10 changes to the Rule Set of the Serviced Device.
- Changes to the IP address(es) of a Serviced Device.
- A simple architecture change (e.g., adding a DMZ or web server behind the firewall).
- To perform software upgrades.
- Changes estimated to require more time than available in a Maintenance Window.
- Configuring a new site-to-site VPN tunnel on the Serviced Device.

No SLAs apply for implementation of Complex or Major Change Requests.

1.4.3.6 **Fast Track Change Request (FCR).** Verizon reviews and accepts an FCR within four hours and implements an accepted FCR within 36 hours after acceptance. An FCR is a planned or unplanned change which:

- impacts changes to existing rules or the creation of new rules and/or objects in the Rule Set.
- creates new hosts in the policy of the Serviced Device and 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.

1.4.3.7 **Urgent Change Request (UCR).** Verizon will review and accept a UCR within two hours and will implement an accepted UCR within four hours after acceptance. A UCR is an unplanned change which:

- Modifies the existing rules or the creation of new rules and/or objects in the Rule Set of a serviced device or a cluster.
- Involves changes which specify the required configuration setting and its new value.

Customer will provide the following when submitting a UCR:

- Detailed data to allow Verizon to review the request within the SLA target of ≤ two hours.
- Availability of an Authorized Contact by telephone to further clarify the UCR.
- Written confirmation via Verizon email(s) of Customer decisions made during phone calls with Verizon.

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

1.5 **Premium Service: Service Management and Reporting.** Service Management and Reporting is available for both Monitoring and for Monitoring and Management services.

1.5.1 **Customer Portal.** Authorized Contacts have 24x7 access to a Customer Portal exclusive of Maintenance Windows.

1.5.2 **Request for Information.** Customer can submit a Request for Information (RFI) on Serviced Devices or on MSS - Premises Premium services. RFIs can be raised through the Customer Portal and will receive a unique reference number 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. Inquiries not directly available through the Customer Portal or which require a more detailed analysis compared to what is available on the Security Incident reports will not be considered as a regular RFI. Verizon may accept such request pursuant to a separate agreement and charged at the Applicable Rates.

1.5.3 **Data Availability and Retention**

1.5.3.1 **Data Storage.** Logs collected for Serviced Devices under MSS – Premises Premium Monitoring are stored and searchable via the Customer Portal for up to 90 days per Serviced Device. Security Incidents and raw Log data associated with Security Events are stored in a Verizon proprietary format in the SMC database for one year. Raw Log data associated with Security Events that occurred during the immediately preceding one year period will be made available upon Customer's request up to one month after service has ended.

1.5.3.2 **Archived Data and Data Retention.** Archived Security Incidents can be made available to Customer via RFI. Archived Security Incidents requested by Customer will be made available in a downloadable file or via an alternative storage medium, in a Comma Separated Value (CSV) format or another format mutually agreed upon by the Parties. At the end of the retention period, Logs and Customer data will be disposed of according to the relevant Verizon Asset Classification and Handling Policy.

1.5.4 **Security Services Advisor (SSA).** Customer is assigned an SSA who will host a quarterly service review meeting. The SSA is assigned to multiple MSS - Premises Premium customer accounts and is not dedicated to any one customer; The SSA:

- Provides training on the Customer Portal
- Manages Customer Communication and security advisories
- Provides assistance in scheduling quarterly scans on Customer's internet facing IP subnets and hosts for Customer Sites under contract
- Manages service issues and service credit requests
- Updates on release and service features, if applicable
- Provides recommendations for improving security posture

A dedicated SSA and Client Security Engineer can be contracted at an additional charge to perform additional services.

1.6 **Optional Services.** The below table outlines the additional Premium Plus and Security Enterprise Service+ options available under MSS - Premises Premium. Premium Plus and Security Enterprise Service+ Options cannot be purchased on a standalone basis.

Premium Plus and Security Enterprise Service+ Options	Monitoring	Monitoring and Management Service
Remote Office	√	√
Device Availability SLA		√
Executive Reporting	√	√
Security Policy Program	√	√
Security Policy Program Reporting and Review	√	√

1.6.1 **Optimized Service.** Security Enterprise Service+ is the optimized service.

1.6.2 **Non-Optimized Service.** Premium Plus is the non-optimized service.

1.6.3 **Remote Office.** Remote Office may be ordered if the Serviced Device is the only device and protects the network assets on the remote physical location, the Serviced Device is a Firewall, Router, or UTM Security Appliance, and the Serviced Device has no more than three distinct remote office Rule Sets across all remote locations. A Change Request to a distinct Remote Office Rule Set is implemented on all Serviced Devices with that Rule Set and is treated as a Major or Complex Change Request under the change management process.

1.6.3.1 **Remote Office Limitations.** Remote Office is limited to:

- **Monitoring:** Availability Monitoring, Threat Analysis, and Service and Security Incident Reporting.

- **Monitoring and Management:** Availability Monitoring, Threat Analysis and Service and Security Incident Reporting, Device Troubleshooting, Hardware Maintenance, Device Restoration, Device Maintenance, and Device Security Management (with the additional limitation that Change Request to a distinct Remote Office Rule Set is implemented on all Serviced Devices with that Rule Set and is treated as a Major or Complex Change Request under the change management process).
- The SLA's do not apply to Remote Office devices.

1.6.4 **Device Availability SLA.** The Device Availability SLA may be ordered if:

- The Serviced Device has to be located in line with the Customer network traffic and all traffic ceases flowing through the Serviced Device while the Serviced Device is unavailable (Serviced Device Service Outage).
- The Serviced Device is installed in a; i) High Availability Active/Passive mode where a secondary device will automatically takeover the critical device functions in case of failure of the primary device; or ii) High Availability Active/Active mode where either device may automatically take over the critical device functions and network load of the other device in case of a single device failure.
- The Serviced Device is covered by a manufacturer or vendor maintenance with a minimum hardware replacement service level of 8x5xNext Business Day maintenance contract. The Serviced Device is equipped with a Verizon accessible serial console interface allowing device-level access. Serviced Device in this section refers to both devices whether the configuration is High Availability Active/Passive or High Availability Active/Active.

Note: In an Active/Active configuration, each device is treated as a separate Serviced Device under MSS - Premises Premium, subject to a separate MRC. However, the rate for the optional Device Availability SLA covers both devices.

1.6.5 **Executive Reporting.** Executive Reporting provides daily and/or weekly reports with an overview of escalated Availability, Health, and Security Incidents over the last reporting period as well as an overview of the Change Requests over the last reporting period.

1.6.6 **Security Policy Program.** The Security Policy Program provides a monthly in-depth review of threat management and provides Customer with the following services:

- Device Policy reviews to review Customer's Rule Sets
- Policy assistance in managing vendor signatures and updates
- Monthly strategic review of Security Incidents to provide broader trends on Security Incidents
- Development of Customer Digests (non-real time threat monitoring)
- Interpretation and integration of scan data on quarterly internal network vulnerability scans conducted by Verizon and up to eight additional scans

The Security Policy Program applies to all devices under contract and is applied at a client level and not on a device level.

1.6.7 **Security Policy Program Reporting and Review.** In conjunction with the Security Policy Program, Customer can contract for a monthly reporting summary review. The report contains a detailed overview of Security Incident handling and provides a recommendation for continuous improvement on how to resolve specific security issues. It includes a monthly meeting to review the reporting summaries with a Client Security Engineer to review and improve the customer's overall threat management.

2. SUPPLEMENTAL TERMS

2.1 **MSS-Premises Premium Updates.** Verizon may change, modify, update or enhance MSS - Premises Premium Service Description from time to time. The latest release of the commercial service description is applicable.

2.2 **Excluded Services.** MSS - Premises Premium is not available for any Serviced Device that: (i) has been subjected to unusual physical or electrical stress, misuse, negligence or accident; (ii) has been modified, merged, relocated, repaired, serviced or otherwise attended to by a Party other than Verizon or without Verizon's prior written consent; (iii) runs a version of operating system and/or application software that is not supported by Verizon, or that is no longer supported or maintained by the relevant manufacturer or licensor; or (iv) has not been properly registered and/or for which required permits or approvals are no longer maintained.

2.3 **Service Equipment.** Verizon may use Service Equipment (e.g. Connection Kits) to collect Logs and Security Events from Serviced Devices and to forward such Logs and Security Events to the SMC. If Verizon determines that a Connection Kit is needed on Customer's Site, Customer must either: (i) provide such Connection Kits subject to Verizon specifications, or (ii) Verizon may provide Connection Kits to a limited number of countries at an additional cost. Verizon will configure and access such equipment remotely. Where Verizon supplies Connection Kits, Customer return such Connection Kits at Customer's sole cost to the address indicated by Verizon upon termination of MSS - Premises Premium. Connection Kits must be returned in the same condition as they were originally delivered, normal wear and tear excepted, and packaged in its original packaging or other equivalent packaging materials. If Customer fails to return the Connection Kit within 14 days following the termination of MSS - Premises Premium, Customer shall pay the greater of: (i) 50% of the relevant set-up per site NRC indicated in the Service Order; or (ii) the actual cost and expense to replace such Connection Kit.

2.4 **Service Tickets.** Verizon provides a standard number of Service Tickets per Serviced Device and per year which are available to Customer. Customer may order additional Service Tickets.

Service Tickets included per Serviced Device per year	
Monitoring and Management	96
Monitoring Only	24

2.5 **Management Stations.** If applicable, a management station may be required to capture and manage the Logs or Security Events from specific Serviced Devices. Verizon may provision Customer or Verizon-owned management stations hosted in Verizon's SMC for certain types and categories of Serviced Devices. In all other situations, Customer is responsible for the necessary management licenses and/or related software/hardware to enable Verizon to provide MSS - Premises Premium on the Serviced Device. The required management station design and architecture is determined solely by Verizon in consultation with the Customer prior to activation of MSS - Premises Premium service.

2.6 **Installation, Configuration, Design, and Review Services.** Verizon does not provide onsite installation, architectural and policy design services under MSS - Premises Premium service. MSS - Premises Premium service also does not include policy and configuration reviews, initial setup or maintenance of configuration on Subordinate Devices, or migrations from management stations located on Customer Sites to management stations hosted the SMC or from third party owned management stations to management stations either located on Customer Sites or hosted in the SMC. All of these excluded services, however, can be conducted by Verizon under a separate agreement.

2.7 **Unsupported Devices.** Unsupported devices are devices where either the Hardware has reached end-of-life, or when the software version is no longer supported by the vendor or Verizon. Verizon may manage Unsupported Devices and end-of-life devices if mutually agreed to by amendment to this service attachment for a maximum duration of six months after Customer has been notified that the hardware or software is no longer supported, and when there is a transition plan in place to replace or upgrade the device to a Verizon supported hardware or software version, or to phase out the device or managed service within that timeframe. When no corrective steps are taken within six months after the initial notification, Verizon reserves the right to terminate the management service for the affected device. The following restrictions apply for unsupported devices. The management of the unsupported device is provided on an

as is and best effort basis, and Customer understands and accepts full liability on the increased security risk and exposure. Customer will receive availability monitoring, troubleshooting, configuration and Rule Set management services and these will be provided to the extent mutually agreed upon by amendment to this service attachment. SLAs do not apply.

Hardware replacements and software upgrades/migrations for unsupported devices or end-of-life software may be planned and carried out by Verizon, if mutually agreed under a separate written work agreement. If Customer wants to change the vendor of a Serviced Device or upgrade a model of a Serviced Device provided by the same vendor, Verizon will charge a device set-up fee to perform the operational changes.

2.8 **CPE Purchase.** Customer may purchase CPE from Verizon pursuant to the terms found here:

- For U.S. Services: Customer Premises Equipment and Related Services + (at www.verizonenterprise.com/external/service_guide/reg/cp_cpe_plus_customer_premises_equipment_and_related_services.pdf)
- For non-U.S. Services: Customer Premises Equipment and Related Services + (at www.verizonenterprise.com/external/service_guide/reg/cp_cpe_plus_customer_premises_equipment_and_related_services_2019JAN01.pdf)

2.9 **Maximum Monthly Data Ingest Volume.** The amount of data Verizon receives for a Serviced Device in any month may not exceed 10 GB. Verizon will charge Customer Service Tickets for any amount of data received for a Serviced Device during a month in excess of 10 GB as set forth in the below table:

Additional Data Received (each Serviced Device)	Service Tickets Charged
Per 10 Gigabyte	Six Service Tickets

2.10 **Customer Responsibilities**

2.10.1 **Customer Deliverables for Implementation.** Customer will complete a Verizon Deployment Kit within 15 Business Days of the kick off meeting. Verizon may terminate Customer's Service Order for MSS – Premises Premium if Deployment Kit is not timely received. Customer will timely approve the project plan, or provide necessary information to implement the project plan. Verizon may terminate Customer's Service Order if delays in project plan approval or necessary information causes any activity on the critical path of the project plan to be delayed by more than 25 Business Days. Upon termination of any such Service Order(s), Verizon may charge Customer for any expenses incurred by Verizon (including labor fees) up through the date of termination based on such project plan delay.

2.10.2 **Subordinate Devices and Maintenance Contract.** Unless otherwise provided herein, Customer is responsible for any monitoring/management or activities for Subordinate Devices. Customer shall (i) at its own expense, procure and maintain with each vendor adequate maintenance contracts and all licenses necessary for the Serviced Devices to enable Verizon to properly perform MSS - Premises Premium; (ii) comply with MSS - Premises Premium prerequisites and operational procedures as set forth in the applicable terms; and (iii) promptly inform Verizon of any changes effectuated in the Customer Environment and any changes to the nomination and/or authorization level of the individuals Customer has authorized to oversee, monitor or evaluate the provision of MSS - Premises Premium. Verizon is not responsible for the actual propagation of the Rule Set updates to those Subordinate Devices but will only inform the Customer via email should the propagation of the Rule Set updates not reach Subordinate Devices.

2.10.3 **Interoperability.** Customer acknowledges that modifications or changes to the Serviced Devices (such as future releases to the Serviced Device's operating software) or to the Customer Environment may cause interoperability problems or malfunctions in a Serviced Device and/or the Customer Environment. Customer acknowledges that it is Customer's responsibility to ensure that the Customer Environment is interoperable with each Serviced Device.

2.10.4 **Installation Sites and Equipment**. Customer shall prepare any installation site and Customer Environment in accordance with Verizon's instructions to ensure that any equipment that interfaces with Customer's devices is properly configured as required and operates in accordance with the manufacturer's specifications. Customer is responsible for any costs associated with preparation of the installation site and Customer Environment. All Serviced Devices must have a routable network path to the Connection Kit and, if required, a Log Transport Agent must be loaded on each Serviced Device. Customer will procure, install, and maintain software Log Transport Agents required for the provision of MSS - Premises Premium to Serviced Devices (e.g. for syslog logging for operating system (OS) and active directory server), at its cost. If Customer fails to make any preparations required herein and this failure causes Verizon to incur costs during the implementation or provision of MSS - Premises Premium service, then Verizon will invoice Customer for such costs.

2.10.5 **User Interface.** In connection with the provision of MSS – Premises Premium, Verizon may provide Customer with one or more user Logins for use with MSS Premises Premium. 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.

2.10.6 **Protected Health Information (PHI).** MSS - Premises Premium 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 with regard to PHI. Customer agrees to use MSS - Premises Premium in accordance with all applicable laws and not to use MSS - Premises Premium 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 - Premises Premium 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 - Premises Premium in a manner not permitted under this Section 2.10.6, 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 2.10.6; and (c) provide Verizon with reasonable cooperation and support in connection with Verizon's response to Customer's breach of this Section 2.10.6. Customer shall assume and be solely responsible for any reporting requirements under law or contract arising from Customer's breach of this Section 2.10.6.

2.11 **Warranties**

2.11.1 **Verizon Warranties.** Verizon warrants to Customer that it will perform its obligations in a good and workmanlike manner. The remedies set forth in the service level agreement (SLA) portion of this Service Attachment are Customer's sole and exclusive remedies in connection with the portions of MSS - Premises Premium related to the failure to meet any standard set forth in the SLA. Verizon does not warrant that MSS - Premises Premium 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.

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

2.11.3 **Customer Warranties.** Customer represents and warrants that (a) it has and will continue to have all rights, power, permissions and authority necessary to have Verizon perform MSS - Premises Premium services in the Customer Site and Customer Environment (including, without limitation, all rights, power, permissions, authority and network user consents necessary in respect of any IP address assigned to a Serviced Device and consent from its network users to Verizon's logging and monitoring activities hereunder), and (b) will not provide any PHI to Verizon for purposes of Verizon's performance of services hereunder. Customer hereby assumes the sole responsibility for the accuracy of the IP addresses and domains provided to Verizon. Customer will be liable for all costs and expenses from any third party claims of loss, damage (including reasonable attorneys' fees) and liability of any kind that may be incurred as a result of Customer's breach of the foregoing warranty.

2.12 **Termination**

2.12.1 **Pre-RFS Termination.** Either Party may terminate a request for MSS - Premises Premium prior to RFS prior to the Service Activation Date with or without Cause, effective 30 days after written notice of cancellation. If Customer requests for a termination of an MSS - Premises Premium service prior to the RFS as set forth under this provision, or Verizon terminates an MSS - Premises Premium service as a result of Customer's failure to provide the necessary information or reasonable assistance required by Verizon to provision MSS - Premises Premium service and deem it as the Service Activation Date, Customer will pay any set-up fees and other provisioning charges if applicable.

2.12.2 **Post-RFS Termination.** Either Party may terminate MSS - Premises Premium, or an MSS - Premises Premium service on any Serviced Device, with or without cause, effective 60 days after written notice of termination is given to the other Party. Customer accepts and agrees that, in the event (i) Customer terminates any Service for convenience or (ii) Verizon terminates any Service for Cause prior to the end of the Service Commitment, then Customer will pay Verizon all unpaid fees payable under this Service Attachment and the applicable Service Order for the remainder of such Service Commitment. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

2.12.3 **Termination for Chronic SLA Failure**. In the event that Verizon breaches the SLAs described in Section 3 for six or more consecutive months, Customer shall have the right to terminate this Agreement in whole or in part, so long as such SLA failure is not remedied within 90 days after Verizon has received a registered written notice of the service problems.

2.13 **Scanning Risks.** Verizon may scan Customer's internet facing IP subnets and hosts. Additional scanning may be requested by Customer or be performed by Verizon. Customer acknowledges that network scanning technology may have inherent risks, including, but not limited to loss, disruption, or performance degradation of Customer's network and services.

2.14 **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 - Premises Premium is provided by or on behalf of Verizon).

2.15 **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 - Premises Premium; 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 - Premises Premium.

2.16 **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 - Premises Premium or materials delivered pursuant MSS - Premises Premium service. Customer retains all right title and interest in and to the underlying factual data gathered through the provision of MSS - Premises Premium. Verizon owns all right title and interest in and to Verizon's use cases, 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.

2.17 **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 - Premises Premium; 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. 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.

2.18 **Restriction on Encryption Functionality in India.** Prior to connecting any encryption equipment to Verizon facilities in India Customer must obtain prior evaluation and approval from the relevant telecom authority.

3. SERVICE LEVEL AGREEMENT (SLA). .

The SLA for Managed Security Services - Premises Premium can be found at the following URL:
www.verizonenterprise.com/external/service_guide/reg/cp_msspremises_sla.pdf

4. FINANCIAL TERMS

4.1 **Rates and Charges.** Rates and charges are the same for Optimized and Non-optimized platform. For all services under this service attachment, non-recurring charges (NRCs) are billable for new installs or physical location moves. Unless expressly indicated otherwise, all NRCs will be invoiced upon Order Confirmation Date and the initial monthly recurring charges (MRCs) will be invoiced upon Service Activation Date or RFS.

4.1.1 **MSS – Premises Premium.** The provision of MSS - Premises Premium to each Serviced Device listed in the applicable Contract is a separate MSS - Premises Premium service. Customer will pay the NRCs and MRCs per MSS - Premises Premium service as set forth in the applicable Contract, and at the following URL: www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm.

4.1.2 **Optional Services.** MSS –Premium Plus and Security Enterprise Service+ are subject to additional NRC and MRC charges as set forth in the applicable Contract.

5. **DEFINITIONS.** The following definitions apply to MSS - Premises Premium, 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

Term	Definition
8x5xNext Business Day	Nonstop service, eight hours a day during Business Days.
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.
Applicable Rates	The rates that apply for professional services work not covered under this Service Attachment. All such work is subject to the execution of a separate written agreement that describes the activities and the Applicable Rates for performing such work.
Authorized Contacts	Customer personnel authorized by Customer to access the Customer Portal and to interact with Verizon.
Change Request	A request from Customer or from Verizon for a change to the Rule Set, device configuration or Service Context.
COTS/GOTS	Common or Commercial Off-the-Shelf/Government Off-the-Shelf product. A product, typically hardware or software, developed, marketed, sold and maintained by a specialist business, e.g., Microsoft Windows OS is a COTS product. GOTS products are often developed by government agencies (either in-house or via a specialist contractor paid by that agency) and are preferred by the government for use as all elements of the product can be controlled and built for government purposes.
Connection Kit	Equipment installed on the Customer Sites used to set up secured monitoring and/or management connections between the Serviced Devices and one or more Security Management Centers.
Customer Environment	The Customer network and/or information technology infrastructure.
Customer Portal	Online portal where Customers can have a near real time view on the Security Events/Security Incidents being processed, and where they can view the security posture and effectiveness of the Security Devices and services at various levels.
Deployment Kit	A group of documents provided to Customer including various instructions as well as forms for the collection of additional data to enable onboarding.
End-of-Life	The end-of-life date is the date communicated by the relevant manufacturer when the support ceases for the Serviced Device so that Customer can foresee a hardware replacement and/or a software version upgrade.
Exploit	A method to use a Vulnerability to gain unauthorized access to functions, data, or privileges 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, and 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 to other computers. A worm can spread through network connections and e-mails in a matter of hours.
High Availability Active/Active mode	A configuration of two or more devices in a load balancing setup with all the devices passing network traffic. In case of failure of one device, the other device(s) either manually or automatically takes over the device functions of the failed device. This configuration is supported on a limited basis based on specific network architectures and Serviced Devices. Verizon will review and approve, if applicable, during the pre-sales design phase.
High Availability Active/Passive mode	A redundant configuration of two devices with duplicate software and data not necessarily co-located where the passive device is activated manually or automatically when the active device fails.
Login	IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or other means of authentication.
Logs	A collection of various IT, compliance, network, application, and security related information created by Subordinate Devices.
Log Transport Agent	A Log Transport Agent is a third party software component that runs on Serviced Devices to enable the transport of the Security Event Logs generated by the Serviced Device to the Connection Kit and to the SMC. Like any agent software, a Log Transport Agent may impact available resources to perform tasks and functions.
Maintenance Window	A time window used for Verizon's performance of maintenance or management services on the Serviced Devices. During a Maintenance Window, the Serviced Devices and/or MSS - Premises Premium services may be temporarily disrupted or unavailable. In the case of Verizon's performance of Customer requested change request(s), the scheduling of Maintenance Windows may be agreed between Customer and Verizon. Maintenance windows are limited to a maximum of six hours unless otherwise communicated in writing by Verizon.
Order Confirmation Date.	Verizon will confirm Customer's Service Order via email and the date of this email is the Order Confirmation Date. The Order Confirmation will confirm the MSS service(s) requested.
Project Manager	A Verizon-designated person who will act as the central point of contact throughout the MSS - Premises Premium implementation process and MSS - Premises Premium staging services, if applicable. The Project Manager will be responsible for managing the schedule and will also collaborate with Customer to develop a project plan that will specify resources, dates, times, and locations for the tasks described in the project plan. The Project Manager also is responsible for managing the change control process. The Project Manager is not dedicated to Customer.
RFI	Request for Information – A Customer inquiry regarding a Serviced Device or MSS Premises Premium Service. Service Tickets are charged once a Serviced Device or MSS Premises Premium service has been declared RFO. Customers are charged one Service Ticket per RFI, unless the inquiry is related to an existing escalated Security Incident, in which case no Service Tickets are charged.
RFO	Ready For Operations - The date (following RFS) that Verizon sends RFO notice to Customer and informs Customer that the Serviced Device has been fine-tuned and the escalation parameters, Service Context, and procedures have been set as mutually agreed. The SLA is effective as of this date. RFO is given per Serviced Device.

RFS	Ready For Service - The date on which Verizon starts providing the MSS - Premises Premium service on a Serviced Device. The RFS may vary for each MSS - Premises Premium service.
Rule Set	The security policy installed on the Serviced Device. The Rule Set may also be called policy when there is no confusion with corporate or other policies.
Security Analytics Platform	Verizon's security analytics platform that uses Verizon proprietary technology as well as COTS/GOTS hardware/software to process data and Security Events from Customer Serviced Devices. Platform functions include: • Data and Log Processing, • Security Event Processing • Security Incident Handling • Vulnerability and Asset Processing • Health Monitoring
Security Digest	Security Incidents that do not require real time Security Incident handling or SOC review and analysis.
Security Event	A data record produced by Verizon's Security Analytics Platform based on Verizon's proprietary threat detection policies.
Security Incident	A single Security Event or a series of Security Events that have been aggregated and correlated based on Verizon's proprietary threat detection policies. A Security Incident may represent an attack.
Security Upgrade	Changes to application software program to fix a security weakness or defect and which is generally released by the Serviced Device manufacturer as a Security Patch. A Security Upgrade may include signature or threat content updates.
Service Context	A set of documents with version control, posted on the Customer Portal, containing information about Customer that Verizon uses for the provisioning of MSS - Premises Premium to 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: • Authorized Contact details and authorization procedure for escalation, notification, and reporting • Service Description • Escalation, notification, reporting, and change control processes • Authorized Contacts • Information on maintenance and support contracts • Timeframe of Maintenance Windows • Roles and Responsibilities in the form of a RACI Matrix for complex and/or custom solutions Network topologies and asset inventories of systems
Serviced Device	A Serviced Device can be a device, (virtual) appliance, software application or a system located on a security device installed on the Customer Site which is monitored and/or managed by Verizon's Managed Security Services. Serviced Devices may include operating systems (OS) (e.g. Windows or Linux server) and active directory server. A Serviced Device can be deployed in the following configurations: • Primary: A device processing the day-to-day load. • High Availability Active/Passive mode. • High Availability Active/Active mode.

Service Ticket	A unit for charging certain usage-based services under MSS - Premises Premium. A number of Service Tickets are included in each MSS - Premises Premium service by default for each Serviced Device annually following RFS.
SLA (Service Level Agreement)	The agreement setting forth the specific service levels and the terms and conditions for receiving Service Credits if Verizon were to fail to meet these service levels.
SMC (Security Management Center)	A data center that hosts the Managed Security Services platform and the systems for monitoring, managing, or supporting the Serviced Devices. The SMC includes: equipment to connect to the Connection Kit, management stations, hosts the Verizon Local Event Collector and analytics engines, and back-end systems such as back-up devices, file servers, and terminal servers.
SMC Time Stamp	A time stamp recorded by Verizon at the SMC and reported on the Customer Portal. The time stamps are used as the reference for measuring the Service Level Agreement. The SMC Time Stamp is recorded in UTC and synchronized worldwide using the Network Time Protocol (NTP).
SOC (Security Operations Center)	A data center where the Verizon security analysts work.
Subordinate Device	A subordinate device can be a (virtual) appliance, system, software, Log data, application located on a Customer Site or on the Customer's Service Provider's premises and which integrates with the Serviced Devices but which is NOT monitored or managed by Verizon under MSS – Premises Premium.
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 weaknesses or defects.
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.
Unsupported Devices	A Serviced Device that is either (i) no longer supported or maintained by its manufacturer; or (ii) an appliance, system, network, or software that is not included in Verizon's portfolio of security products supported on the MSS – Premises Premium platform. Certain limitations and conditions with respect to the availability of MSS – Premises Premium apply for Unsupported Devices.
UTC (Coordinated Universal Time)	Universal Time indication standardized by the Bureau International des Poids et Measures (BIPM) and defined in CCIR Recommendation 460-4. The UTC is the time indicated on atomic clocks. Verizon consults and uses it for its SOC via the Internet protocol NTP. The UTC code uses the 24-hour clock. 4 pm (afternoon) is equal to 16:00 UTC.
Verizon Local Event Collector	The Verizon Local Event Collector or LEC is a Verizon proprietary system that acts as a monitoring system, a data collector and a jump host system for the SOC analyst towards the Serviced Devices.
Vulnerability	A weakness or 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.

Workaround	An alternative function or method, often using a temporary patch or reconfiguration, to achieve a result equivalent to the original function or method.

Appendix I
MSS Premises Premium Service Matrix

	Monitoring Services				Management Services			
	Device Availability and Health Monitoring	Threat Analysis	Security Incident Handling	Service Manage-ment and Reporting	Device Mainten-ance	Device Health Manage-ment	Device Security Manage-ment	Service Manage-ment and Reporting
Firewall	√	√	√	√	√	√	√	√
Network Switch	√		√	√	√	√	√	√
Router	√			√	√	√	√	√
Security Appliance	√	√	√	√	√	√	√	√
Network Intrusion Detection System (NIDS)	√	√	√	√	√	√	√	√
Network Intrusion Prevention System	√	√	√	√	√	√	√	√
External NIDS sensors	√	√		√	√	√	√	√
HIDS/HIPS on Servers – Full Escalation (1)		√	√	√	√		√	√
HIDS/HIPS on Servers – Threshold Escalation (2)		√		√	√		√	√
HIDS/HIPS on Clients		√		√	√		√	√
Application Level Firewall	√	√	√	√	√	√	√	√
Log Monitoring and Management	√	√	√	√	√	√	√	√
Load Balancer	√			√	√	√	√	√
SSL VPN	√	√	√	√	√	√	√	√
Email Security Gateway	√	√	√	√	√	√	√	√
Proxy Server	√	√	√	√	√	√	√	√
Content Screening	√	√	√	√	√	√	√	√
FIPCM Servers and Clients		√	√	√	√		√	√

	Monitoring Services				Management Services			
	Device Availability and Health Monitoring	Threat Analysis	Security Incident Handling	Service Manage-ment and Reporting	Device Mainten-ance	Device Health Manage-ment	Device Security Manage-ment	Service Manage-ment and Reporting
Endpoint Security on Servers and Clients		√	√	√	√		√	√
Premium Plus/Security Enterprise Service+ Remote Office	√ Availability only	√		√	√	√	√	√
OS Log Monitoring	#	√	√	√				
Active Directory Log Monitoring	#	√	√	√				

(1) HIDS/HIPS – Full Escalation: This service is available for HIDS/HIPS agents residing on servers only. When a Customer orders this service, Security Events and Security Incidents are created for each individual HIDS/HIPS agent. On-line and off-line reporting happens per HIDS/HIPS agent.

(2) HIDS/HIPS – Threshold Escalation: This service is available for HIDS/HIPS agents residing on servers or on clients (desktops/laptops). When a Customer orders this service, sensors with the same policy are grouped together. For each group, a number of Customer-specific thresholds are defined. When a threshold is exceeded, an automated escalation is sent to Customer. On-line and off-line reporting happens per group.

Availability limited to Verizon contacting Customer when Serviced Devices are no longer sending Logs to the SMC.