SECURITY SAAS – QUALYSGUARD +

Part I: Rates and Charges.
Part II: Service Description and Requirements.
Part III: Terms and Conditions.
Part IV: Service Level Agreement.
Part V: Definitions.

Part I: Rates and Charges.

1. Customer will pay the ARC and NRC shown in the Customer's Contract, and at the following URL: www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm based upon the Modules and features ordered. Customer will be invoiced the ARC upon the Service Activation Date.
2. **Usage and Upgrades.** Customer's usage of Security SaaS - QualysGuard + ("QualysGuard Services") is limited to the level initially ordered by Customer. In order to receive additional QualysGuard Services or change a QualysGuard Service tier within a Service Commitment, Customer must place an additional order and enter into a separate Contract or amendment to the Contract with amended rates and charges, as applicable.

Part II: Service Description and Requirements.

1. **QualysGuard Services.** QualysGuard Service allows Customer to automate the process of IT security and compliance management, including network discovery, mapping and business prioritization of IT assets; network and web application vulnerability assessments, policy compliance assessments; remediation task management; and reporting according to Customer-defined criteria. The QualysGuard Service is a third party product which is supplied to Customer by Verizon under license from Qualys, Inc. The QualysGuard Service is delivered to Customer using the QualysGuard Platform that supports single or multiple Modules that may be configured by Customer from time to time via the Web Portal. The QualysGuard Service does not provide service, maintenance or repair to or for any real or personal property.

1.1 Certain elements of the QualysGuard Service require a Network Scan. Network Scans for external IP addresses (i.e. Internet accessible IP addresses) are performed with Internet remote scanners from the SOC. Network Scans of Customer internal IP addresses (e.g. network devices, laptops, servers, printers, etc.) require an internal scanning subscription ("Internal Scanning Subscription") that includes the use of an Appliance. Network Scans will be executed on the Identified IP Addresses.

1.2 QualysGuard Platform. The QualysGuard Platform uses a software-as-a-service delivery model to make the Modules available. QualysGuard Platform consists of the following components: the Web Portal, SOC, and Vulnerability KnowledgeBase, each as further detailed below. The QualysGuard Platform components used for Customer depend on the Modules ordered on the Contract.

1.2.1 Web Portal. The Web Portal allows Customer to administer IP addresses by individual hosts, web applications, domain names, groups, or groups of groups (i.e. business units). Other tools within the Web Portal are used to administer user accounts, Internal Scanning Subscriptions, and activity logs. Further, Customer can configure Network Scans, option profiles of Network Scans, report templates, search lists, compliance policies, IT controls, and remediation workflow settings. Once Network Scans have been completed, the Web Portal has tools to visualize reports based on the Network Scan results. Report search features are available to show results pre-defined that Customer can select, such as date, vendor name and product name of the vulnerable product, and severity levels. Reporting information can be visualized in list or graphical format and can vary in degree of detail, i.e. more technical for system administrators and more high-level for executives. Trending information is available by visualization of results over a period of time.

Only users authorized by Customer with active login credentials can access the Web Portal. Customer must provide information for one point of contact for the initial login credentials to be issued. Customer's authorized user can then authorize additional users via the Web Portal. The Web Portal allows for the assignment of role-based privileges for users.

1.2.2 Secure Operations Center. The SOC is the technology and infrastructure facilities for the QualysGuard Platform. The SOC is used for storage and processing of Customer data as well as hosting of Vulnerability KnowledgeBase and Internet Remote Scanners. Internet Remote Scanners are multi-threaded processes hosted on systems in SOC for the sole purposes of executing external Network Scans.

1.2.3 Vulnerability KnowledgeBase. Vulnerability KnowledgeBase is the vulnerability intelligence used in Network Scans to identify IT assets, IP and web application vulnerabilities, TCP/IP services, and operating systems. The Vulnerability KnowledgeBase is updated from time to time with signatures for new vulnerabilities, validated patches, fixes for false positives, and other TCP/IP data.

2. **Module Descriptions.** The QualysGuard Platform supports the following Modules that are accessed via the Web Portal unless otherwise noted below:

- QUALYSGUARD VULNERABILITY MANAGEMENT.
- QUALYSGUARD ZERO DAY SERVICE
- QUALYSGUARD POLICY COMPLIANCE.
- QUALYSGUARD FEDERAL DESKTOP CORE CONFIGURATION.
- QUALYSGUARD PCI COMPLIANCE
- QUALYSGUARD WEB APPLICATION SCANNING.
- QUALYSGUARD MALWARE DETECTION SERVICE
- QUALYS SECURE SEAL

2.1 QualysGuard Vulnerability Management Module. QualysGuard Vulnerability Management Module ("VM Module") allows Customer to execute Network Scans for purposes of network discovery, mapping and business prioritization of IT assets and to identify network vulnerabilities. The VM Module has the following features:

- The VM Module is applicable for external and internal Network Scans.
- Network Scans are available for discovery, mapping and business prioritization of IT assets.
- Network Scans use the Vulnerability KnowledgeBase to identify network vulnerabilities.
- Network Scans can be scheduled to execute automatically on a recurring basis.
- Activity logs show user and system activity.
- Asset search feature to find IT assets based on Network Scan results.
- Authenticated Network Scan for VM Module is optional, but recommended.
- Reporting options available for mapping, scans, and remediation. Map and scan reports are fully customizable through Web Portal template settings, allowing Customer to specify the type of discovered information to be displayed in a report.
- Remediation reports show status of remediation workflow based on tickets associated to asset groups, users, and vulnerabilities.
- Trend and time differential reports can be generated to see results over time.
- Report templates can be used as-is for technical or executive reports or templates can be edited to create specialized reports according to Customer need.

2.1.1 QualysGuard Zero-Day Service Module. The QualysGuard Zero-Day Risk Analyzer Service Module ("Zero-Day Module"), in conjunction with the VM Module, provides vulnerability scanning and reporting capabilities on vulnerabilities in software products that have been discovered before the software product vendor has released a patch addressing the vulnerability. The Zero-Day Module provides Customer with a vulnerability report, scan, and applicable defensive measures based on Verisign's iDefense service. The Zero-Day Module provides:

Scan Signatures. The module delivers QualysGuard VM scan signatures for zero-day vulnerabilities from iDefense. Customers build a scan profile to scan and detect these zero-day vulnerabilities as part of their automated QualysGuard scans. Once such a profile is created, it can be updated automatically.

Alerting. Customer can sign-up new zero-day threat alerts based on the profile of assets gathered from the VM Module Network Scans.

Supplemental Vulnerability Intelligence. The Zero-Day Module provides supplemental intelligence gathered by iDefense including deep analysis, insight, and mitigation strategies.

2.2 QualysGuard Policy Compliance Module. QualysGuard Policy Compliance Module ("PC Module") allows Customer to execute Network Scans for purposes of discovery of operating system configuration information and application access control information. PC Module correlates this information to user-defined policies to report degree of compliance to IT security standards, regulations, and other business mandates. The PC Module has the following features:

- The PC Module is applicable for internal Network Scans only.
- Network Scans can be scheduled to execute automatically on a recurring basis.
- Activity logs show user and system activity.
- Asset search feature to find IT assets based on Network Scan results.
- Authenticated Network Scan for PC Module is required. Customer must configure authentication credentials so PC Module can assess important information, such as current patch level and current password settings, to identify potential policy violations.
- Customer can create user-defined policies using the QualysGuard Policy Editor and QualysGuard Policy and Controls Library on the Web Portal.
- QualysGuard Policy Editor is used to define a policy according to IT technology, IT controls defined by

implementation; IT assets defined by specific IP addresses; and style formatting including cover page, section titles, and outline numbering.

- QualysGuard Policy and Controls Library includes a set of technologies and controls, based on Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST) standards and maps to many frameworks and regulations (as shown in the Web Portal) such as Control Objectives for Information and related Technology (COBIT), International Organization for Standardization (ISO), Information Technology Infrastructure Library (ITIL), Federal Financial Institutions Examination Council (FFIEC), Health Insurance Portability and Accountability Act (HIPAA), North American Electric Reliability Corporation's (NERC).
- Report templates to identify policy violations according to defined policy, authentication pass/fail status, compliance status for a specific host, and individual control pass/fail status.
- Exception management workflow for policy violations allows users to submit requests for exceptions and administrators to evaluate and approve request. Workflow can be used to collaborate with internal and external auditors.

2.3 QualysGuard Federal Desktop Core Configuration Module. QualysGuard Federal Desktop Core Configuration Module ("FDCC Module") allows Customer to execute Network Scans for purposes of discovery of operating system configuration information and application access control information. FDCC Module uses this information to report degree of compliance to Federal Desktop Core Configuration (FDCC) requirements. FDCC Module has been validated by NIST (http://nvd.nist.gov/validation_qualys.cfm) as conforming to Security Content Automation Protocol (SCAP) and its component standards. The FDCC Module is included at no additional fee when PC Module is purchased. The FDCC Module has the following features:

- The FDCC Module is applicable for internal Network Scans only.
- Network Scans can be scheduled to execute automatically on a recurring basis.
- Activity logs show user and system activity.
- Asset search feature to find IT assets based on Network Scan results.
- Import FDCC checklists from QualysGuard Policy and Controls Library maintained according to NIST updates.
- Create custom FDCC checklists by uploading custom SCAP content files.
- Report templates to identify policy violations according to defined FDCC policy, compliance status for a specific host, and individual control pass/fail status.
- Authenticated Network Scan for FDCC Module is required. Customer must configure authentication credentials so FDCC Module can assess important information, such as current patch level and current password settings, to identify potential policy violations.

2.4 QualysGuard PCI Compliance Module. QualysGuard PCI Compliance Module ("PCI Module") allows Customer to execute Network Scans for purposes of discovery of operating system configuration information and application access control information. PCI Module uses this information to report degree of compliance to PCI DSS. PCI Module has been validated by PCI Security Standards Council to be designated as an Approved Scanning Vendor. PCI Module provides Customer with compliance tips and a step-by-step approach to work through the compliance process. The PCI Module is accessible via the PCI Portal and is subject to the terms and conditions found at the PCI Portal. PCI Portal is accessible from the Web Portal or can be accessed independently. PCI Module is included at no additional fee when VM Module is purchased. The PCI Module has the following features:

- PCI Module is applicable for external Network Scans. Internal network scans require an Internal Scanning Subscription for an additional fee.
- Network Scans can be scheduled to execute automatically on a recurring basis.
- Network Scans use the Vulnerability KnowledgeBase to identify network vulnerabilities.
- Activity logs show user and system activity.
- Asset search feature to find IT assets based on Network Scan results.
- PCI Module provides PCI Self-Assessment Questionnaire functionality for completion and submission to acquiring banks.
- The PCI Module allows Customer to auto-submit PCI compliance status directly to an acquiring bank.
- PCI Module can be combined with VM Module and or WAS Module to address other PCI DSS requirements.

2.5 QualysGuard Web Application Scanning Module. QualysGuard Web Application Scanning Module ("WAS Module") allows Customer to execute Network Scans for purposes of discovery of application layer information for web applications with a starting URL and/or TCP/IP port. WAS Module uses this information to help Customer assess, track and remediate web application vulnerabilities. WAS Module automates techniques used to identify web vulnerabilities and provides testing of web application vulnerabilities such as those described by Open Web Application Security Project ("OWASP") Top 10 and Web Application Security

Consortium ("WASC") Threat Classification, including but not limited to SQL injection, cross-site scripting, and web site misconfigurations. The WAS Module has the following features:

- WAS Module is applicable for external and internal Network Scans.
- Network Scans can be scheduled to execute automatically on a recurring basis.
- Network Scans use the Vulnerability KnowledgeBase to identify web application vulnerabilities.
- Activity logs show user and system activity.
- Asset search feature to find IT assets based on Network Scan results.
- Authenticated Network Scan for WAS Module is optional but recommended. Customer must configure authentication credentials so WAS Module can assess additional web pages.
- Automated web crawling and HTML link discovery using several techniques, including but not limited to pattern recognition and observed behaviors, to assess as much of the target web application functionality as possible.
- Block list or trusted list scanning limits Network Scan to selected parts of the web application. The block list instructs Network Scan to not assess links explicitly defined, while the trusted list instructs Network Scan to only assess links explicitly defined.
- The WAS Module includes sensitive content search that enables automated expression searches for content in HTML, such as social security numbers, credit cards as well as custom strings.
- Performance tuning and scheduling to define bandwidth usage levels for parallel scanning to control impact on web application performance.

2.5.1 QualysGuard Malware Detection Service Module. QualysGuard Malware Detection Service Module ("MDS Module") utilizes behavioral and static analysis to detect malware and enables Customer to scan, identify and remove malware from its websites. The MDS Module supports regularly scheduled scanning with email alerts to notify Customer when malware is discovered. Malware details are provided so that Customer can act to isolate and remove malware. The MDS Module is bundled with the WAS Module for no additional fee.

2.6 Qualys Secure Seal. Qualys Secure Seal allows Customer to execute Network Scans for purposes of discovery of security status based on assessments performed. Secure Seal will assess Customer web site for network and web application vulnerabilities, the presence of malware, and the strength and validity of SSL certificates. Customer can generate a Secure Seal icon for placement on its web site to display the results of Network Scans performed on the same web site. Secure Seal permits web site visitors to verify current Network Scan status via link to QualysGuard. Secure Seal is included at no additional fee when VM Module and WAS Module are purchased. When Secure Seal is purchased separately, it is accessible via the Secure Seal Portal and not via the Web Portal. The Secure Seal Portal is accessed using Secure Seal log in credentials. Secure Seal has the following features:

- Secure Seal is applicable for external Network Scans only.
- Network Scans use the Vulnerability KnowledgeBase to identify network and web application vulnerabilities.
- Network Scans are scheduled to execute automatically on a recurring basis.
- Activity logs show user and system activity.
- Asset search feature to find IT assets based on Network Scan results.
- Presence of malware will be assessed by evaluation of web site for malicious code or software that could adversely affect the browser or computer of web site visitors.
- Strength and validity of SSL certificates will be assessed to determine a number of security factors including but not limited to issuer and expiry of certificate, protocols supported, and cipher suites supported.

3. **Optional Features.** The following optional features can be added in conjunction with certain Modules:

- QUALYSGUARD APPLICATION PROGRAMMING INTERFACE.
- QUALYSGUARD SCANNER INTERNAL SCANNING SUBSCRIPTION.

3.1 QualysGuard Application Programming Interface. QualysGuard Application Program Interface ("API") provides an extensible XML interface that allows bi-directional flow of data and/or instructions allowing integration of the QualysGuard Service with custom or off-the-shelf applications purchased separately by Customer. API provides integration with the functionality listed below:

- Vulnerability Scan - to search and view scans in the scan history; cancel, pause, and resume network scans.
- Network Discovery– to produce an inventory of all scanned network devices characterizing devices with information such as: access points to the network, machine names, IP addresses, operating systems, and discovered services such as HTTP, SMTP, and Telnet.
- Account Preferences– to view information contained in account preferences such as scheduled network scans, scan options in the default option profile, asset groups, and Appliances.

- Asset Management - to list information about hosts scanned using the VM Module or PC Module
- Remediation Management - to retrieve host information and ticket information for the purpose of remediation tracking and reporting
- User Management– to manage users with access to the QualysGuard Web Portal.
- Report Share - to generate, store, and distribute reports of networks scans
- Compliance - to view compliance control list, policy list, and policy violations
- Scan Authentication - to manage authentication records used for authenticated scanning
- WAS Scan Results - to view, download, and delete web application scan results.

3.2 QualysGuard Internal Scanning Subscription. One or more Internal Scanning Subscriptions are required for each internal network or network segment that is to be scanned, depending on the size of such network. An Internal Scanning Subscription includes provision of an Appliance and Embedded Software which is hosted on Customer's internal network. The Appliance executes internal Network Scans and does not store any results but transmits results via an HTTPS connection to the QualysGuard Platform. An Appliance polls the QualysGuard Platform to receive software and operating system updates and to receive information about execution of Network Scans.

A Virtual Appliance may be provided. A Virtual Appliance is a packaged set of data files which Customer must deploy onto a Customer-provided virtualization platform (e.g., VMware) in order to function. Once deployed, the Virtual Appliance enables Customer to bring QualysGuard security and compliance assessment capabilities to its network without the need to deploy dedicated hardware. The Virtual Appliance is built upon open source Linux operating system software, combined with proprietary Embedded Software which provides the QualysGuard product functionality.

Part III: Terms and Conditions.

1. **Service Commitment and Termination.** The Service Commitment will be one year if no Service Commitment is specified elsewhere in the Customer's Contract. The Service Commitment for any order will commence upon the Service Activation Date. Customer may order additional services at any time and each order will have its own Service Commitment.

1.1 Service Activation Date. After Customer's order of QualysGuard Service, Customer will receive an email from support@qualys.com notifying Customer that the QualysGuard Service is ready for service. The email will contain a welcome letter with Customer's QualysGuard login and password. The date of this email is the Service Activation Date.

1.2 Termination. If: (a) Customer terminates a Contract for QualysGuard Service before the end of the relevant Service Commitment for reasons other than Cause (as defined in the Master Terms); or (b) Verizon terminates a Contract for QualysGuard Service for Cause pursuant to the Master Terms; then there will be no pro rata refund of any ARC paid and Customer will pay the ARC for the remaining Service Commitment, if any and any termination charges due under the Master Terms.

2. **User Name and Password.** Customer is responsible for keeping Customer's user name and password confidential and to create and protect its users' login credentials. Customer must immediately notify Qualys (support@qualys.com) upon learning of any unauthorized use of login credentials. In such case Qualys will deactivate the compromised login credentials and issue new login credentials. Customer is responsible for all activities and charges incurred through the use of the compromised login credentials until Qualys has been notified.

3. **License Terms and Restrictions.**

3.1 Customer is granted a non-transferable, non-exclusive license to use the Embedded Software and the Web Portal and/or the Secure Seal Portal solely in connection with Customer's use of the QualysGuard Service. Except as otherwise permitted herein, Customer understands and agrees that it is not permitted to distribute the Embedded Software in any form, or to use the Embedded Software except as it is embedded in the Appliance. Customer agrees that it shall not and shall not allow any third party to attempt to reverse engineer, de-compile, or disassemble the Embedded Software for any reason, except and only to the extent that it is expressly permitted by applicable law notwithstanding this limitation or permitted pursuant to the licensing terms (e.g., Open Source licensing terms).

3.2 Certain components of the Embedded Software are subject to the GNU General Public License Version 2 ("GPL") and such components are referred to herein as "Open Source Software." Customer is free to use, modify and distribute Open Source Software that is subject to the GPL, so long as Customer complies with the terms of the GPL (available at http://www.gnu.org/copyleft/gpl.html#SEC1).

3.3 The rights granted to Customer in the Contract are subject to the following restrictions, and Customer hereby agrees as follows: (a) Customer may use the QualysGuard Service and the Embedded Software (i) only to scan IP addresses and/or map domain names owned by and registered to Customer, or for which Customer otherwise has the full right, power, and authority to consent to have the QualysGuard Service scan and/or map, and (ii) only up to the number of IP addresses or the number of scans permitted by Customer's subscription; (b) Customer must notify Qualys, using the Web Portal if appropriate, of any changes in the IP addresses or domain names to be scanned and an increase may require the payment of additional fees. If Customer receives the PCI Module as part of the QualysGuard Service, Customer acknowledges that the QualysGuard Service is provided in connection with PCI DSS, including any customized reports and individualized assistance, solely as a tool to enable Customer to evaluate its compliance with the PCI DSS and that third party payment card organizations, and not Verizon or Qualys, establish the security criteria and other terms and conditions of the PCI DSS. Customer acknowledges that Qualys may disclose a report related to Customer's PCI DSS compliance scan(s) to the PCI Security Standards Council, LLC, or similar entities, successors, and assigns as required by such entity for approved scanning vendors.

4. **Identified IP Addresses.** Because of the sensitive nature of performing security checks on IP addresses, Customer represents and warrants that Customer has full right, power, and authority to allow the QualysGuard Service to test for vulnerabilities ("scan") the Identified IP Addresses and/or domain names identified for scanning, whether electronically or by any other means, whether at the time of initial registration or thereafter, and Customer hereby consents to such scanning and to the transfer of IP Addresses or domain names to a third country (including intra-group transfers and transfers to entities in countries that do not provide statutory protections for personal information) for use or processing under the terms of the Agreement. Customer also acknowledges and agrees that the scanning of Identified IP Addresses and/or domain names may expose vulnerabilities and in some circumstances could result in the disruption of services at such site(s). Certain functionality of the QualysGuard Service involves circumvention of Customer's firewall and/or other protective devices, substantial risk of Denial of Service (DOS) attacks, loss of service, hardware failure and loss or corruption of data. Customer acknowledges that it understands and accepts the risks associated with the QualysGuard Service that involves a scan, and by entering into a Contract for such service elements, it authorizes the performance of those QualysGuard Service elements. Customer agrees that it is Customer's responsibility to perform backups of all data contained in or available through the devices connected to Customer's IP addresses and/or domain names prior to invoking the use of the QualysGuard Service. Customer agrees to indemnify, defend and hold harmless Verizon and its affiliates, subcontractors, directors, officers, employees, agents, successors or assigns (each, a "Verizon Indemnified Party") from and against any and all loss, damages, liabilities, costs and expenses (including legal expenses and the expenses of other professionals) incurred by such Verizon Indemnified Party, resulting directly or indirectly from any claim attributable to or arising out of a scan (each, a "Scanning Claim"), including, without limitation, a scan to analyze assets that are not controlled directly by Customer (e.g., servers hosted by third parties). The obligation of Customer to indemnify, defend and hold a Verizon Indemnified Party harmless in connection with a Scanning Claim will not apply to the extent that the Scanning Claim is based on the Verizon Indemnified Party's gross negligence or willful misconduct.
5. **Appliance and Network Connection.** Customer will permit the connection between the Appliance and Customer Network for purposes of receiving the QualysGuard Service. Verizon has no liability or obligation for: (a) the installation, operation or maintenance of the Customer Network; (b) the availability, capacity and/or condition of the Customer Network; or (c) any adverse impact of the QualysGuard Service on the Customer Network. The Appliance will remain the property of Qualys, as Verizon's third party supplier and shall be deemed to be Service Equipment for the purposes of the Master Terms, and Customer will not have any right or interest in it. Customer may not move, alter, or attach anything to the Appliance without Verizon's prior consent. Customer assumes all risk of loss and shall pay for all cost of repair, replacement, or refurbishment caused by accident, misuse, abuse, neglect, or Customer's other failure to install, use and maintain the Appliance in accordance with the applicable documentation and specifications. Customer may retain and use the Appliance during the Service Commitment, provided that Customer pays the applicable charges for such renewal term. Upon termination or expiration (including non-renewal) of the Contract, Customer will return the Appliance provided under this Service Attachment within 15 days of such expiration or termination, in substantially the same condition in which it was delivered to Customer, reasonable wear and tear excepted. Customer will pay all return transportation and delivery costs.
6. **Confidentiality.** All data regarding Customer's IP addresses, domain names or network characteristics (including data that is obtained as a result of its provision of the QualysGuard Service hereunder) will be deemed Confidential Information of the Customer, and all data and information contained within the QualysGuard Service or the reports (excluding Customer's Confidential Information) and all information concerning or materially relating to the Appliances, will be deemed Confidential Information of Verizon or its licensors. . Notwithstanding the above, Customer agrees that certain information generated in connection with its vulnerability testing services may be used in an aggregated, anonymized form, as defined below, in connection with its reporting of vulnerabilities, vulnerability behavior and vulnerability trends generally. Data in "aggregated, anonymized form" shall mean generalized data that does not include, identify, or reveal information relating to any specific Verizon customer or of the Customer or any specific network addressing information, including, but not limited to, information relating to a Verizon customer or company name, vertical market, specific IP addresses, host names, subnets, MAC, circuit IDs, or any other customer- or user-specific network addressing identifiers or user or its data.
7. **Intellectual Property Ownership.**

7.1 As between the parties, all title, copyrights, trademarks, service marks, patents, patent applications and all other intellectual proprietary rights now known or hereafter recognized in any jurisdiction in and to the QualysGuard Service, or any aspect thereof including but not limited to the design and function of the Appliances--and all software embedded therein or related thereto, all data and information contained therein (excluding individual factual data gathered from the Customer's IP addresses) (the "Intellectual Property Rights") are owned by Verizon and/or its licensors. Customer acknowledges that no title to the Intellectual Property Rights is transferred to Customer, and that Customer does not obtain any rights, express or implied, in the QualysGuard Service or the reports, including any information contained within the reports, other than the rights expressly granted in this Service Attachment.

7.2 Copyright in Customer Information in Deliverables and License to Verizon. Notwithstanding the foregoing and to the extent it is within the authority of Verizon (as used here, "Verizon" excludes its suppliers and contractors) to grant it, Customer will own the copyright in that portion of the Deliverable that is unique to Customer, first created by Verizon during the Service Commitment in the performance of a Contract, and delivered to Customer under this Service Attachment ("Customer Information Copyright"). Other than any copyright assigned to Customer in the previous sentence, all intellectual property rights in the Deliverables, or based thereon, are and shall remain the sole and exclusive property of Verizon or its suppliers or contractors. Customer hereby grants Verizon, its affiliates and their contractors a worldwide, non-exclusive, royalty free, non-transferable license to use, disclose, copy, display, and create derivative works of the Customer Information Copyright during the Service Commitment in connection with the provision of services and products, including, without restriction, the QualysGuard Services and Deliverables, by Verizon to Customer.

7.3 The QualysGuard Services may provide that the Customer is issued a statement of compliance or certification or other form of attestation ("Attestation Letter") if pre-defined security standards or controls ("Standards") established by Verizon or a third party are, in Verizon's or Verizon's independent service provider's opinion, met for the information technology assets, infrastructure and/or products that are evaluated and assessed as part of the QualysGuard Services ("Subject Assets"). The QualysGuard Services may further provide that if Standards or other pre-defined criteria are met Customer is granted the right to use a particular Verizon seal, logo, mark or other indicium ("Seal"). Customer may use any Attestation Letter only for the purpose of conveying to appropriate third parties the fact that the Subject Assets have been assessed and evaluated against the Standards and only in the form as provided by Verizon or its independent service provider. Customer acknowledges that any Attestation Letter is Verizon's or Verizon's independent service provider's statement of opinion at the time of issuance based on the results obtained from the QualysGuard Services. Customer understands and accepts that any such Attestation Letter does not represent any other opinion at any other point in time. Customer must not use any Attestation Letter or Seal in any manner that is false, deceptive, fraudulent or misleading or implies that its products and services are endorsed by or affiliated with Verizon, its independent service provider, or both. Customer must cease all use of the Seal immediately upon (i) termination or expiration of the QualysGuard Services pursuant to which Customer was granted the right to use such Seal; (ii) the relevant Standards or criteria are no longer met. Customer's usage of any Seal must conform to, as applicable, Verizon's or Qualys's then current usage guidelines, which may be modified from time to time upon written notice to Customer. Customer's failure to comply with the foregoing provisions may result in, as applicable, Verizon or Qualys revoking the right to use the relevant Attestation Letter(s) and Seal(s).

8. **Disclaimer.** The parties agree that it is impossible to detect, disclose and/or resolve every vulnerability or security hazard and that impenetrable security cannot be attained. Nothing herein therefore shall be construed as a guaranty against breaches of security.

9. **Restriction on Using Encryption Services (India Customers Only).** The QualysGuard Service employs encryption technology to secure data. Accordingly, Customer must ensure that it has obtained any permits or approval of the Department of Telecommunications or other regulatory agencies in India that governs the use of encryption in India prior to Customer's use of the QualysGuard Service. Customer hereby indemnifies and hold harmless Verizon, from and against any claims, suits, judgments, settlements, losses, damages, expenses (including reasonable attorneys' fees and expenses), and costs (including allocable costs of in-house counsel) asserted against or incurred by Verizon arising out of a failure by Customer to comply with the restrictions described in this clause or as otherwise imposed by the licenses or statutory guidelines from time to time.

Part IV: Service Level Agreement.

Verizon does not offer an SLA as part of this service offering. Customer is eligible for the service level objectives relating to QualysGuard service directly from Qualys.
http://www.qualys.com/support/sla.

SECURITY SAAS + QUALYSGUARD

Part V: Definitions. The following definitions apply to QualysGuard Services, 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

“ARC” means annual recurring charge.

“Appliance” means an item of QualysGuard equipment, or, in the case of a Virtual Appliance, a piece of software, to be installed on each segregated Customer internal network.

“Authenticated Network Scans” means Network Scans utilizing Customer-supplied user credentials to authenticate to target hosts.

“Customer Network” means Customer’s internal network and equipment.

“Deliverables” means reports and other documents provided by Verizon to Customer in connection with the QualysGuard Service, which may contain Customer test results, descriptions of the work or process flows relating to Customer’s network tests and other similar information pertaining to Customer Network.

“Embedded Software” means the Qualys software within an Appliance.

“Identified IP Addresses” means IP Addresses or ranges of IP addresses specifically identified by Customer as part of the QualysGuard registration and service activation process or configured by Customer as part of a Module.

“Module” means the security and compliance modules which may be configured by Customer as part of the QualysGuard Service

“NRC” means non-recurring charges.

“Network Scan” means a probe of active Internet protocol (“IP”) addresses on a network to discover information such as active TCP/IP services, applications, operating systems, and their respective configuration settings.

“PCI DSS” means the Payment Card Industry Data Security Standard.

“QualysGuard Platform” means the collection of technologies and components used to deliver QualysGuard Service to Customer.

“Secure Operations Center” or “SOC” means a QualysGuard security operations center.

“Service Activation Date” means the date on which the Customer receives an email from support@qualys.com notifying Customer that the QualysGuard Service is ready for service. This shall be the same as the Service Activation Date under the Master Terms.

“Virtual Appliance” means a software-only distribution, based upon the same software architecture as an Appliance.

“Web Portal” means a web application accessible to Customer from Qualys via the public Internet.