Secureworks®

SERVICE DESCRIPTION

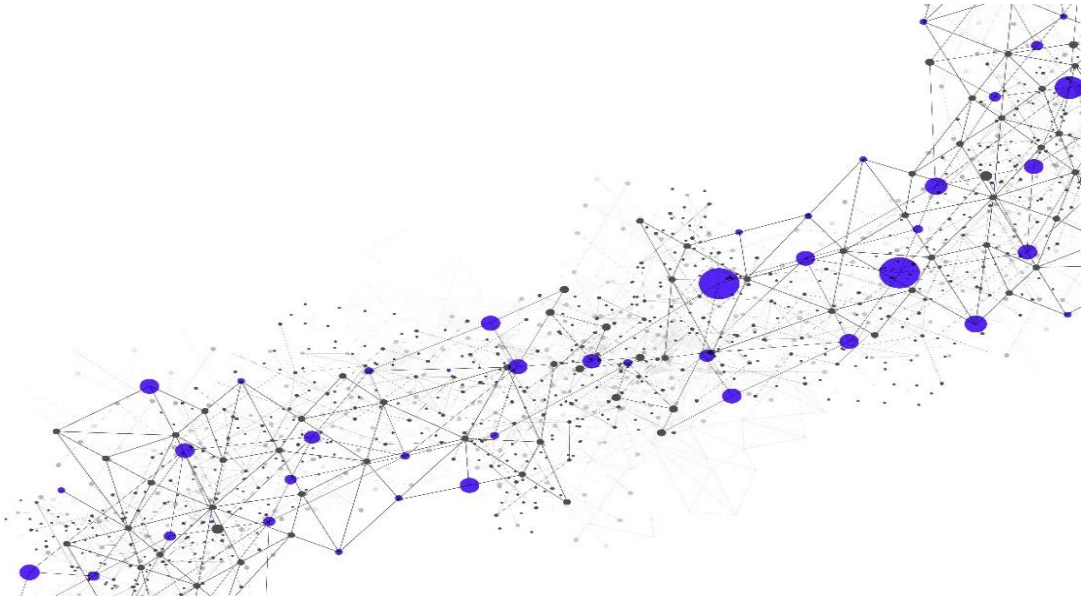
Vulnerability Management Service with Qualys

Release Date

February 06, 2024

Version

6.3



www.secureworks.com
A Dell Technologies Company

Global Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
Phone: +1 877 838 7947
Email: info@secureworks.com
Additional office locations: https://www.secureworks.com/about/offices

Table of Contents

1 Service Introduction

This Service Description ("**SD**") describes the Vulnerability Management Service with Qualys ("**Service**"). All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement.

1.1 Overview

Secureworks® will provide Customer with vulnerability scanning capabilities using a Qualys subscription. The Qualys subscription can be used within an on-premises or hosted environment, or both. The capabilities include both on-demand and scheduled vulnerability scanning, and remediation advice that tracks workflow, reporting, and trending of Customer's environment.

Secureworks will provide Customer with vulnerability scanning for a defined number of Internet Protocol ("**IP**") addresses that are associated with Hosts, devices, and/or web applications. The Service scales with the number of IP addresses for which scanning is needed, allowing scanning for up to 100,000 IP addresses and up to 200 web applications. To provide scanning for more than 100,000 IP addresses and up to 200 web applications, a Statement of Work would be needed.

The usage ***license*** entitles Customer access to a module within the Qualys subscription—per IP address Asset—that Customer purchases for the duration of the Services Term (i.e., one license is for one IP address Asset that is within one module, such as the Vulnerability Management Module, in a Qualys subscription). Upon conclusion of the Services Term, access to the module through the Qualys subscription is terminated. The ***subscription*** is software as a service for an online vulnerability management tool, such as Qualys. Customer must have a subscription with applicable licenses for this Service to be used. The license(s) and subscription can be purchased from Secureworks or transferred to Secureworks if Customer already has license(s) and a subscription.

Customer obtains the Qualys subscription from Qualys and can independently use the subscription without interacting with Secureworks. Customer can enter all required information into the subscription, or Customer can complete and return the Secureworks-provided forms and Secureworks will enter the information into Customer's subscription. After Customer's subscription is populated, Customer can complete tasks such as conducting on-demand scans and managing exclusions at Customer's risk – e.g., Customer would need to determine the best time to conduct an on-demand scan, the scope of the scan, and whether the scan needs to be conducted during a scheduled change interval. At Customer's request and subject to the limitations of this Service, Secureworks can also conduct the above-listed activities for Customer. Secureworks will work with Customer to ensure automated recurring vulnerability scans, and to provide remediation expertise and other support as described herein.

Customer will deploy all scanning appliances (virtual, physical, and cloud, as applicable) to Customer's scanning environment. After the scanning appliances are deployed, Customer can populate its scanning subscription in the Qualys Scanning Portal ("**Scanning Portal**"), or Customer can complete and submit Secureworks-provided forms and Secureworks can populate Customer's scanning subscription.

The Service includes the following components:

- Scanner Appliances and the performance of automated and recurring vulnerability scanning
- Configuration Support (includes initial implementation support: Healthy Start Program)
- Vulnerability Reporting
- Quarterly Review
- Periodic Webcasts

See Section 2, Service Details, for more information about the Service, including further explanation of the components listed above. Also, see the **Secureworks MSS Services – Service Description Addendum** for information about the following, as applicable to the Service: Device responsibilities, Maintenance Program, and Subscription Program.

Vulnerability Scanning Acknowledgement: Customer acknowledges that Secureworks services cannot identify weaknesses in network architecture (other than those identified during Service activation based on the documentation made available by Customer) or weaknesses in general application architecture. Secureworks does not guarantee that all vulnerabilities on every tested system or application will be discovered. Secureworks does not guarantee that there will be no false positives. The nature of vulnerability scanning is such that some vulnerabilities and misconfigurations of Customer's devices (e.g., un-patched Hosts or the use of older, unsupported versions of software) can pose risks when scanned. Secureworks cannot guarantee that Vulnerability Management Service ("**VMS**") vulnerability scans will not adversely affect the performance or availability of the target systems. Service Level Agreements ("**SLAs**") are defined further below.

Note: Secureworks will not install third-party software on any appliance or system, unless explicitly indicated in Section 2 as being part of the Service.

1.1.1 Qualys Vulnerability Management Module Subscription Types

Secureworks will provide Customer with the appropriate Qualys Vulnerability Management Module subscription type based on the following information that Customer will provide:

- IP address type (internal, external, or both)
- Total number of IP addresses that need to be scanned

Depending on the IP address type and total number of IP addresses to be scanned, the add-on for external IP addresses may be required.

Additional Information

- There is no limit to the number of user accounts that can be created for a subscription.
- Customer will determine access levels for each user account.
- Customer can divide the scanning environment into business units with which user accounts can be associated.

  For example, a group of user accounts can be given the Manager access level and users in this group will be able to execute scans, read reports from scans, and conduct other vulnerability scanning activities. Another group of user accounts can be provided with the Scanning – HR access level and users in this group will only be able to execute scans in the HR-specific area within the defined scanning environment.

The table below contains information about the subscription types and related information.

Subscription Type and Licenses for Vulnerability Management Module ("VMM")			
Subscription Types Based on Total Quantity of Internal and/or External IP Addresses	0-256 Internal IP addresses ***Add-on:*** External (Internet facing) IP addresses (additional charge and includes PCI)	257-5,120 Internal IP addresses ***Add-on:*** External (Internet facing) IP addresses (additional charge and includes PCI)	More than 5,120 Internal and/or External (Internet facing) IP addresses ***Add-on:*** PCI (additional charge)
Available Licenses *(see Section 1.1.1.1 for*	Vulnerability Management Module	• Vulnerability Management Module • Vulnerability Management Module with Cloud	

Subscription Type and Licenses for Vulnerability Management Module ("VMM")			
explanation)	with Cloud Agent	Agent	
Scanning Environment	• Internal (scanning in a private environment) • External (Internet facing; also referred to as "remote") • Hosted (e.g., AWS, Azure) (***Note:*** For remote vulnerability detection in an internal environment, a scanner appliance must be used.)		
Scanning Appliance Quantities	5 or less		Unlimited
Scanning Appliances *(Compatibility and Limitations)*	Compatible with physical, virtual, or cloud scanners Scanners can be provided for an additional charge Remote vulnerability detection requiring a physical or virtual scanner (for Internal IP addresses) can be provided for an additional charge	Compatible with physical, virtual, or cloud scanners One (1) virtual scanner ("**vScanner**") is included; additional virtual, physical, or cloud scanners can be provided for an additional charge Remote vulnerability detection requiring a physical or virtual scanner (for Internal IP addresses) can be provided for an additional charge	Compatible with physical, virtual, or cloud scanners Scanners can be provided for an additional charge
Available Add-on Modules for VMM *(Each add-on module can be purchased for an additional charge; see Section 1.1.1.2 for explanation.)* *Scanning add-on modules that are used for scanning internal IP addresses requires use of a scanner appliance or Cloud Agent.*	**Secureworks-supported Add-on Modules** **VMM Required:** • Threat Protection • Continuous Monitoring • Security Configuration Assessment • Asset View **VMM Not Required (can be purchased standalone):** • Web Application Scanning • Policy Compliance PCI Scanning ***Note:*** Customer can directly purchase from Qualys any modules not listed above.		

1.1.1.1 Explanation of Available Licenses

Below are explanations of the two options for the "Available Licenses" row in the table above. For each option, Customer purchases a license for each IP address Asset.

- **Vulnerability Management Module ("VMM"):** This option is the primary module that is needed for the Service. Both Customer and Secureworks will use this module to conduct activities for the Service. This module provides mapping, scanning, and reporting functionality. For issues that arise during use of this module, the VMS Support team will provide support—from reporting issues to issue resolution.
- **Vulnerability Management Module ("VMM") with Cloud Agent:** In addition to the above, this option includes Cloud Agents that Customer will install on compatible systems/endpoints (e.g., Linux, Windows) for Host-based vulnerability scanning. See the Appendix for more information.

1.1.1.2 Explanation of Available Add-on Modules for VMM

In the table above, ***Secureworks-supported Add-on Modules*** are Qualys modules for which the VMS Support team will provide support / issue resolution—from reporting issues to resolving issues. To obtain support, Customer will submit a Service Request ticket through the Secureworks Client Portal or other method for contacting the Secureworks SOC. Then, Secureworks will contact and work with Customer for issue resolution.

For the modules listed under ***VMM Required***, Customer must purchase the VMM for these add-on modules. For the modules listed under ***VMM Not Required***, Customer can purchase these add-on modules separately (each as a standalone module) ***without*** purchasing the VMM.

See the **Secureworks VMS Addendum – Qualys Add-on Modules** document for information about the add-on modules.

1.2 Customer Obligations

Customer will perform the obligations listed below, and acknowledges and agrees that the ability of Secureworks to perform its obligations hereunder, including meeting the Service Level Agreements ("**SLAs**") listed further below, are dependent on Customer's compliance with these obligations. Noncompliance with Customer obligations relative to this Service may result in suspension of managed components of the Service and/or SLAs, or a transition to monitor-only components of the Service.

1.2.1 Assets in Scope

Customer will provide and maintain accuracy of the Assets within the Scanning Portal that are required to execute scanning activities described in Section 2.2, Service Components, of this SD. This includes providing the minimum information required by the scanning tool. Secureworks will only update Assets per Customer request; Customer must submit a Service Request in the Secureworks Client Portal.

1.2.2 Data Backups

Customer acknowledges and agrees that the scanning of IP addresses and/or domain names may expose vulnerabilities and, in some circumstances, could result in the disruption of Service or corruption or loss of Customer Data. Therefore, Customer will perform regular backups of all Customer Data contained in or available through the devices connected to Customer's IP address(es) and/or domain names should backups need to be used to restore data.

1.2.3 Cloud-Based IP Address Acknowledgement

Customer acknowledges that the IP address of any cloud-based Asset is subject to change. Customer will identify the specific IP addresses of cloud-based Assets that are to be scanned and will update this information within the Scanning Portal or notify Secureworks through submitting a Service Request when any IP address for a cloud-based Asset changes, and Secureworks will update the information within the Scanning Portal.

1.2.4 Ownership and Authority for IP Addresses

Customer may use the Service to only scan the IP addresses owned by and registered to Customer, or for which Customer has the full right, power, and authority to consent to have the Services scan and/or map. Customer may not rent, lease, or loan the Service, or any part thereof, or permit third parties to benefit from the use or functionality of the Service through timesharing, service bureau arrangements or otherwise. If one or more of the IP addresses identified by Customer are associated with computer systems that are owned, managed, and/or hosted by a third-party service provider ("**Host**"), Customer represents that it has the consent and authorization from such Host(s) necessary for Secureworks to perform the Service. Customer

agrees to facilitate any necessary communications and exchanges of information between Secureworks and Host.

1.2.5 Connectivity

Customer will provide and maintain remote network connectivity to Customer's environment, including ensuring sufficient network bandwidth, and the in-scope Device(s) that are necessary for Secureworks to perform the Service. Customer will also allow connectivity from Qualys IP range to Customer location(s) as applicable to the Service. SLAs will not apply to the Device(s) that is experiencing connectivity issues that are beyond the control of Secureworks.

1.2.6 Application Program Interface ("API") Integration

Some vendors provide APIs to interact with their systems. Any script or code creation for, usage of, maintenance of, or integration with other third-party tools are not included in this Service; Customer will be responsible for all API integration, and related activities and licenses. Secureworks will not install any third-party software applications that use the API directly on the appliance.

1.2.7 Communications

Customer will communicate with the Secureworks Security Operations Center ("**SOC**") through telephone (Customer-authorized representative will be authenticated) or the Secureworks Client Portal using either the ticketing interface or Chat. Customer should submit all Service-related issues or requests as tickets in the Portal or as requests through the Chat in the Portal. It is Customer's responsibility to ensure that its list of authorized representatives is up to date with the Secureworks SOC. Customer is responsible for timely responses to tickets that Secureworks escalates to Customer through the Secureworks Client Portal.

1.2.8 Maintenance

Customer will notify the Secureworks SOC by submitting a ticket in the Portal or through the Chat in the Portal at least 24 hours in advance of planned Customer-side network maintenance to enable Secureworks to avoid disruptions with regard to scheduled scans.

1.2.9 Usage Overage

If, for any services identified in Customer's Transaction Document(s), Customer's actual usage exceeds the subscription limit of such services ("**Overage**"), then Secureworks may invoice Customer for Overage, and Customer will pay for the Overage as applicable to Customer's actual usage, from the date Secureworks identified the Overage until the end of the Services Term.

1.2.10 Provisioning in a Public Cloud or Private Virtual Environment

When provisioning in a Public Cloud or Private Virtual Environment, Customer will provide to Secureworks information about the environment, and may be required to make configuration changes as applicable to the Service. Customer will provide access and appropriate privileges within the environment to enable Secureworks to deploy and configure the Service.

1.2.11 Hardware Procurement

If Customer will be using physical hardware for this Service, then Customer will purchase the hardware necessary for Secureworks to deliver the Service. Secureworks will provide Customer with hardware that is current at the time of shipping, and it is Customer's responsibility to install the hardware in a timely manner. Customer will ensure that its hardware is at versions that are supported by Secureworks prior to provisioning of the Service, and remains at versions that are Secureworks supported during the Subscription Term. Secureworks SLAs will not apply to hardware or versions that are End-of-Life ("**EOL**"), end of support, or are otherwise not receiving updates by the vendor or supported by Secureworks.

1.2.12 General

- Customer will ensure that Customer personnel are scheduled and available to assist as required for the Service(s).
- Customer will have obtained consent and authorization from the applicable third-party, in form and substance satisfactory to Secureworks, to permit Secureworks to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications.
- Customer will provide to Secureworks all required information (primary personnel contact information, credentials, and related information) prior to work being started.
- Customer will promptly reply to all requests from Secureworks.
- Customer-scheduled interruptions and maintenance intervals will allow adequate time for Secureworks to perform the Service.
- Customer will promptly inform Customer personnel and third parties of Secureworks testing activities as needed, to prevent any disruption to Secureworks business and performance of the Service (e.g., takedown requests, ISP deny list)
- Customer will uninstall all licensed tools, return all leased hardware, and disable any accounts provided for Secureworks to perform the Service upon termination of the Service.
- Customer will do the following:
  - Implement all security patches (Customer personnel will need to implement these patches as applicable)
  - Provide a list of contacts for the locations where the in-scope scanner appliance(s) are installed
  - Complete configuration of scanners (if applicable)
  - Identify the in-scope IPs and excluded IPs for scanning
  - Identify sensitive areas (e.g., manufacturing domains and compliance-specific domains such as for PCI) and work with Secureworks to establish the limitations (e.g., rules for scanning sensitive areas) for both scanning and remediation
  - Provide Secureworks with credentials for authenticated scanning and website scanning *(**Note:** Customer can also directly enter this information into the Scanning Portal instead of providing the information to Secureworks.)*
    - If credentialed scans are used, then Customer must ensure that provided credentials are accurate and correct for each of the systems that must be scanned, and address any issues associated with scan credentials.
  - Enable Secureworks to access Customer's Asset database and/or similar organization tool (required for appropriate tracking of remediation)
  - Provide the scanner appliance(s) and valid subscription(s) or license key(s) for Qualys to be used for this Service
- Ensure proper installation and configuration of the scanners, and connectivity to the scanner vendor's platform

1.3 Initial Implementation Scheduling and Points of Contact

Secureworks will contact Customer within seven (7) Business Days after execution of the Transaction Document to schedule the first meeting during which Service Implementation will be discussed.

Customer and Secureworks will designate respective points of contact ("**POC**") to facilitate communication and support ongoing activities related to implementation of the Service.

2 Service Details

The subsections below contain details about the Service and how it will be implemented.

2.1 Service Implementation

The standard service implementation period begins after Secureworks reviews and approves Customer's signed Transaction Document, and ends when Customer is transitioned to ongoing operations (i.e., Customer is transferred to the Secureworks SOC and/or the Healthy Start Program as explained further below). Secureworks will activate Customer's Qualys subscription within 48 hours after the initial meeting, at which time Customer can begin to use the subscription. The subsections below explain the Secureworks implementation methodology for Managed Security Services (known as MSS Services) that is used to provision, install (if applicable), and activate the Service.

Note: *Secureworks does not provide SLAs for completing implementation within a specified period of time; the duration of the implementation is dependent on several factors, such as the number of scanners, the number of physical locations where scanners will be activated for the Service (if applicable to the Service), complexity of Customer requirements, and the ability of Customer to provide Secureworks with requested information within a mutually agreed-upon time period.*

2.1.1 Implementation Methodology

Secureworks will follow the Secureworks standard implementation methodology to implement the Service. The implementation methodology can be reasonably adjusted to meet Customer needs at the sole discretion of Secureworks. As part of implementation, Secureworks will help ensure Customer understands how to use the Service through collaborative meetings and training. Below is a high-level overview of the MSS implementation methodology.

- **Organize:** Start the project, document success criteria, baseline the project schedule, enable Secureworks Client Portal access, and create VMS subscription
    - Secureworks will work jointly with Customer to validate accuracy of the information used to create the original Transaction Document against the actual Customer environment where Services will be performed ("**Due Diligence**"). As a result of Due Diligence, changes in the types of services (e.g., VMS modules), the number of locations, or the quantities of equipment to be provisioned may be identified ("**Identified Changes**"). Customer acknowledges that (i) in order for Secureworks to provide intended Service coverage across such Identified Changes, an amended or additional Transaction Document may be required, which may include changes to scope and fees, and (ii) without such an amended or additional Transaction Document, Secureworks may only be able to provide Services as scoped, defined, and charged per the original Transaction Document. In some cases, an amended or additional Transaction Document may be required to provide the Services in the original Transaction Document. For example, an additional scanner may be required at a location that was not originally determined to be in scope.
- **Prepare:** Identify required training for the Secureworks Client Portal, and provide physical scanners to Customer for installation (if applicable); configure Customer's single sign-on access to Scanning Portal; and provide Customer with documentation necessary to populate VMS subscription (accessible to Customer through the welcome kit in the Secureworks Client Portal)
- **Execute:** Customer completes configuration of scanners (if applicable) and Customer provides details of Hosts that comprise the VMS subscription; Secureworks will populate the VMS subscription based on this information and confirm scanner connectivity

  Note: Secureworks provides telephone support to Customer for installing scanners.
- **Rationalize:** Confirm Customer's ability to access and participate in management of the Service within the portals; initiate Customer's Healthy Start Program (if applicable)

- **Accept:** Validate successful deployment of the Service and transition of Customer to steady-state operations

2.1.2 Service Provisioning, Installation, and Activation

Service provisioning consists of providing Customer with access to the Secureworks Client Portal and the Qualys subscription (through single sign-on), other initial actions that are completed in advance of implementing the Service for Customer, such as shipping scanners to Customer (if applicable) and configuring VMS Subscription. **Service installation** consists of validating Customer's access to the Secureworks Client Portal and the Qualys subscription (through single sign-on), Customer physically putting in place a scanner, connecting it to Customer's environment, and testing the connectivity of the scanner. **Service activation** consists of Customer and Secureworks validating all scanners and components of the Service are available to Customer for Customer's use, and the Secureworks implementation team transferring Customer to the Secureworks SOC.

Note: Not all add-on modules will require the activities listed above and below to be completed.

Secureworks performs the following provisioning, installation, and activation activities:

- Create implementation ticket in Secureworks Client Portal (for ongoing tracked communication between Customer and Secureworks during implementation)
- Schedule initial meeting (remote) with Customer and review Transaction Document (or on-site meeting for Customers in Japan, if needed) *(**Note:** Receipt of a Customer-executed Transaction Document is required prior to scheduling initial meeting.)*
- Complete provisioning and installation activities – e.g., shipping hardware to Customer, configuring VMS Subscription within Secureworks Counter Threat Platform ("**CTP**"), and performing connectivity testing if applicable
    - ***Activity for physical scanners only:*** Send physical scanner(s) to Customer through ground shipping method, if applicable *(**Note:** Installation and completion of minimal configuration by Customer for scanner is required.)* Customer is responsible for physical installation and completion of minimal configuration of the CTA(s).
- Provide Customer with access to the Scanning Portal (Customer's VMS Subscription) and the Secureworks Client Portal
- Collect Customer information to populate the VMS Subscription (optional: Customer can populate the VMS Subscription within the Scanning Portal instead of Secureworks)
- Notify Customer (e.g., through email, telephone, or scheduled meeting) of Service activation, which means Customer can begin to use its VMS Subscription *(**Note:** Customer and Secureworks will work together to ensure that Service is activated for in-scope Devices.)*
    - Secureworks can schedule Service activation in accordance with change management procedures communicated by Customer. Standard activations are performed during Business Hours on Business Days in the following regions: US, EMEA, APJ, and ANZ; however, activation can be performed at other times when scheduled in advance with Secureworks.
- Notify Customer (e.g., through email, telephone, or scheduled meeting) that the Service activation is complete, and Customer is transitioned to Secureworks SOC
- Provide Customer with opportunity to participate in Healthy Start Program (see Section 2.2.2.1)

2.1.2.1 Provisioning a Virtual Scanner ("vScanner") into a Virtual Environment

Virtualization includes various methods by which hardware resources are abstracted to allow multiple virtual machines to share a common hardware platform. This subsection explains provisioning a vScanner into a virtual environment (i.e., a Public Cloud or Private Virtual

Environment). See the Glossary for definitions of terms related to virtualization that are used in this SD.

If Customer has a Private Virtual Environment, then Secureworks will provide Customer with an image to install on the Hypervisor in Customer's Private Virtual Environment, which is used to create the vScanner on a Guest virtual machine. If Customer has a Public Cloud Environment, then Customer will access the Secureworks Client Portal and complete steps to obtain the vScanner for use in the Public Cloud Environment. Depending on Customer's environment, the specific steps for installing and provisioning the vScanner may vary, and Secureworks will provide applicable information to Customer.

When provisioning the vScanner into a virtual environment, Customer is responsible for creating and supporting the underlying Guest virtual machine. This includes all management and maintenance of the Guest virtual machine (i.e., the Host), Hypervisor, and related hardware. See Section 2.4, Support for Private Virtual Environments, for more information about virtual environments including additional Customer responsibilities.

Provisioning Requirements: Customer must perform the provisioning activities when provisioning the vScanner into Customer's Virtual Environment (including a private or public cloud). Customer must also provide all required virtual hardware needed, in accordance with vendor recommendations, to operate the vScanner on the Guest virtual machine. This includes vCPU(s), RAM, vHDD capacity, network interface card/adapter, and storage IOPS. Customer must also provide a Virtual Environment that supports the required network connectivity, which will enable the vScanner to integrate with Customer's VMS Subscription.

2.2 Service Components

The subsections below contain information about the components of the Service.

2.2.1 Scanner Appliances and Scanning

Customer can download virtual scanner images from within the Appliance area of the Qualys Subscription. Secureworks will ship physical scanner appliance(s) to Customer's location along with configuration instructions. Customer must apply the network configuration to the appliance and make any necessary Customer-side changes for the scanner appliance to properly communicate with the Qualys Cloud.

Secureworks will conduct scans per Customer's request, or Customer can conduct scans. Scans on Customer's internal IP addresses will be conducted from a scanner appliance(s) from within Customer's internal network. Scans on Customer's external IP addresses will be conducted from the Qualys Cloud, and ***do not*** require a scanner appliance. Secureworks will provide the range of IPs from which external scanning will be sourced.

2.2.2 Configuration Support

Secureworks will provide configuration support as explained in the subsections below.

2.2.2.1 Healthy Start Program

Within one (1) week after Service Implementation is completed, the Secureworks implementation team will transition Customer to the Healthy Start Program. Secureworks will contact Customer to schedule the initial meeting for this optional program, which provides guidance and direction during the initial phase of ongoing operations. The goals of this program are to help ensure Customer understands the Service, answer questions, and provide support to ensure scans are scheduled and Assets have been created in the Scanning Portal.

Activities include the following:

- A smooth transition from implementation to support during ongoing operations, providing an overview of the Service and the Qualys vulnerability scanning tool

- Validating that scanner appliance(s) is properly connected to Qualys Cloud and applicable hosts/endpoints
- Training support for the tabs and areas within the Qualys subscription user interface
- Guidance and direction to ensure establishment of the following:
  - Asset Groups / Asset Tags
  - Schedules for scanning and reporting
- Assistance and how-to support for on-demand scans, reading vulnerabilities and scan data, option profiles, scan templates, dashboard configuration and manipulation, and scanner appliance health checks
- First follow-up contact will be offered within 90 days to assess overall Service experience and address customer concerns; unless Customer declines, additional Service meetings will occur quarterly during first 12 months of Customer's subscription term

2.2.2.2 Creating Scan Schedules

Secureworks will assist Customer with creating scan schedules, which can be recurring or on demand. These schedules contain search lists, Asset groups, and option profiles for the scans. When creating a scan, IP addresses (i.e., the defined IP addresses) or the name of an Asset group (which can contain IP addresses) can be used. Creating scan schedules includes specifying the scanner to which each schedule will be associated.

Customer can create scan schedules or option profiles in the Scanning Portal, or complete and return to Secureworks the necessary forms for Secureworks to create the scan profile(s) or option profiles. Customer will submit one Service Request per scan profile (for one or more Asset Groups and/or defined IP addresses) to Secureworks through the Secureworks Client Portal and include the completed forms. Secureworks will validate the provided information within three (3) Business Days, then immediately activate the scan profile for Customer or activate the scan profile on the date Customer specifies on the designated form. Only the capabilities provided within Qualys can be used for profile creation.

2.2.2.2.1 Default Option Profiles

Selecting an Option Profile is a configuration option within the scan schedule, and it contains the parameters for executing a scan. Option profiles are stored within the Scanning Portal, and can be reused across multiple scans. Customer can create option profiles, and the following option profiles are available within the Scanning Portal:

- Qualys Top 20 Options
- SANS20 Options
- Payment Card Industry ("**PCI**") Options
- Initial Options

2.2.2.2.2 Asset Groups, Valuation, and Data Entry

Secureworks will import Customer-created Asset Groups, Asset values, and Asset owner data into the Scanning Portal. Customer must provide the relevant information to Secureworks using the supplied pro forma documentation. A minimum of three (3) Business Days after validation that the pro-forma documentation was completed is required prior to the desired date of import. Secureworks does not define Asset Groups, values, and owners.

2.2.2.2.3 Scheduling a Scan

Secureworks will work with Customer to gather targeted IP address and/or URL information and then schedule the scans within the Scanning Portal. Customer must contact Secureworks with relevant scan information using the supplied pro forma documentation. A minimum of three (3) Business Days after validation that the pro-forma documentation was completed is required prior to the date they wish to scan.

2.2.3 Vulnerability Reporting

Secureworks will provide Customer with access to the Scanning Portal to execute on-demand reports or to schedule reports (including delivery of reports to specified email addresses). In addition, other reporting capabilities will be available to Customer, such as creating remediation, scan, and patching reports. Limited report customization is provided within the Scanning Portal. Secureworks will work with Customer to set up standard and custom reports within the Scanning Portal. Customer will define, retrieve, and review reports.

2.2.4 Quarterly Review

Customer will submit a Service Request in the Secureworks Client Portal or otherwise contact the SOC to request a quarterly one-hour teleconference for reviewing items such as the following:

- Detected vulnerabilities, including remediation advice as applicable
- License and usage
- Scanner appliance status
- Corrective action planning
- Review of Asset Group and scan schedule configurations
- Engaging and interacting with the Secureworks support team

Customer and Secureworks will work together to determine an agreed-upon date and time for the teleconference.

Note: For customers in Japan, on-site quarterly reviews can be requested.

2.2.5 Periodic Webcasts

Customer can access pre-recorded webcasts, or attend scheduled webcasts, during which the VMS Support Team will discuss VMS best practices and industry updates. Scheduled webcasts include a question-and-answer period. Customer will be notified of scheduled webcasts through the Learning Center within the Secureworks Client Portal, and Customer can access the Webcasts within the same location.

2.3 Service Delivery

The subsections below contain information about how Service and support are delivered to Customer.

2.3.1 Security Operations Centers (“SOCs”)

Secureworks maintains SOCs in the United States and internationally. To provide Service to Customers around the world, Secureworks administers security services and support from these SOCs, such as monitoring Security Events, aggregating and correlating data, conducting analysis, escalating Security Events, and performing other security-related activities. Contact information for SOCs will be provided to Customer.

The Secureworks SOCs are available 24 hours a day, 7 days a week, for questions and support. During non-Business Days and Hours, some SOC inquires may be sent to other support groups to address during Business Days and Hours. The table below contains information about Service items for which the SOC can help Customer.

Support Available 24x7	
Asset Groups	• Creation and organization • Add, modify, and remove IPs
Asset Tagging	• Creation and modification • Static and dynamic

Support Available 24x7	
Scanning	• On-demand scans • Scheduled scans • Stopping scans • Maps
Results	Reviewing raw scan results
Search Lists	Static and dynamic
Report Creation	Built-in or customized templates
Additional Topics	• Scheduling Reports • Asset Search • Remediation Policy

If Customer requires support beyond the scope above, then the SOC will create a Service Request ticket in the Secureworks Client Portal for the VMS Support Team, and Customer will be contacted through telephone for follow-up during Business Hours, Monday – Friday, 9 a.m. – 5 p.m. US Eastern Time, excluding US holidays.

For Customers in Japan, support will be available Monday – Friday, 9 a.m. – 5 p.m. JST, excluding holidays in Japan. For emergencies not within these Business Hours, Customers in Japan can obtain support using the contact methods that will be provided to Customer.

2.3.2 Business Days and Business Hours

Business Days for Secureworks global headquarters are Monday – Friday and Business Hours are 8 a.m. – 5 p.m. US Eastern Time, excluding US holidays. Business Days and Business Hours for all other Secureworks locations vary according to local time zone and country.

2.3.3 Service Location(s) and Languages

The Service will be delivered remotely from a Secureworks location(s). Voice and email support are provided in English only. Other components of the Service that are visible to Customer (such as reports, documentation, and the Secureworks Client Portal) are provided in English only. Additionally, Secureworks requires that inputs and interfaces to the Service, including but not limited to logs, Application Programming Interfaces ("**APIs**"), and Command Line Interfaces ("**CLIs**"), be provided in English. Service options and availability may vary by country; contact Secureworks sales representative for details.

2.3.4 Service-Enabling Technology

Customer will be provided with access to the Secureworks Client Portal and the Secureworks Mobile Application ("**Mobile Application**"). Customer's use of the Mobile Application shall be subject to the terms and conditions set forth in the Mobile Application. In addition, one or more CTAs will be provisioned. Below are explanations of these items.

2.3.4.1 Secureworks Client Portal

The Secureworks Client Portal is the online site for all Managed Security Services Customers, and provides the following:

- Visibility to Customer's Secureworks Services
- Ability to submit tickets to Secureworks with concerns or issues relating to Managed Security Services
- Monitor events and escalations generated

- Access the Secureworks Learning Center (training and self-education – webinars, documentation, SDs, Secureworks Client Portal-specific features, and related content)

Access to the Secureworks Client Portal is enabled for Customer-specified authorized users during the Organize phase of service implementation (see Section 2.1.1 for more information), and training regarding Secureworks Client Portal use is conducted during the Execute phase of service implementation. It is Customer's responsibility to ensure that access for authorized users of the Secureworks Client Portal remains current.

All information received by Customer through the Secureworks Client Portal is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted externally from Customer's organization.

2.3.4.2 Secureworks Mobile Application

The Service is integrated into the Mobile Application. As part of Consultation, Customer and Secureworks will review Customer roles and access to Service features in the Mobile Application. All information received by Customer through the Mobile Application is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted externally from Customer's organization.

2.3.5 Customer and Secureworks Responsibilities

The responsibility assignment matrix below describes the participation required by both Customer and Secureworks in completing tasks or deliverables for a project or business process to facilitate successful service delivery. Secureworks uses standard RACI role criteria for managing Customer projects and deliverables. These roles are defined as follows:

- R – Responsible: Role(s) assigned to do the work. For any individual task, there could be multiple roles responsible.
- A – Accountable: Role(s) that make the final decision and has ultimate ownership.
- C – Consulted: Role(s) consulted as the subject matter expert ("**SME**") before a decision or action is taken.
- I – Informed: Role(s) updated with status of work being done, status of ongoing work, and results of work completed.

Notes:

- The SOC provides Quick Start guides to Customer, which contains more detail about SOC-specific roles and responsibilities.
- All tasks marked with one asterisk (" * ") in the table below are ***optional***. Customer can complete Secureworks-provided forms and Secureworks will perform these tasks for Customer or make changes for Customer.
- All tasks marked with two asterisks (" ** ") in the table below are ***co-management tasks that are required***; Customer can complete Secureworks-provided forms and Secureworks will perform these tasks for Customer or make changes for Customer; alternatively, Customer can perform these tasks within the Scanning Portal, depending on user access levels.
- All tasks marked with three asterisks (" *** ") in the table below are ***co-management tasks that are optional***; Customer can complete Secureworks-provided forms and Secureworks will perform these tasks for Customer or make changes for Customer; alternatively, Customer can perform these tasks within the Scanning Portal, depending on user access levels.

Vulnerability Management Service with Qualys			
Activity	**Task**	**Customer**	**Secureworks**

Vulnerability Management Service with Qualys			
Activity	**Task**	**Customer**	**Secureworks**
Service Preparation	Provide contact information for authorized contacts regarding Service-related activities	R, A	I
	Provide information for authorized users who need access to the Secureworks Client Portal and Scanning Portal (Customer will modify as needed at any time through the Portal, and add / remove users as needed)	R, A	I
	Provide shipping information for Secureworks to send physical Devices required to implement Service	R, A	I
	Provide information on support requirements, sizing recommendations and sample deployment scripts (applicable to Public Cloud Environments only)	I	R, A
	Provide to Customer the implementation guidelines for service implementation	I	R, A
	Ensure Device(s) meets Secureworks-provided hardware and software specifications prior to the start of implementation	R, A	C, I
	Ensure Device(s) meets minimum third-party vendor hardware and software specifications prior to the start of implementation (if applicable)	R, A	C, I
	Prepare the environment as required to implement Service, which may include rack space, power, cooling, network connectivity, public cloud access, or other modifications	R, A	I
	Identify in-scope Assets (e.g., IPs, web applications) applicable to the Service	R, A	C, I
	Identify placement for scanner appliances	R, A	C, I
Service Implementation	Provide Customer with Service forms	A, C, I	R
	Create Customer's scanning subscription in Scanning Portal; enable Customer access to this portal, and update access as needed per Customer request	C, I	R, A

Vulnerability Management Service with Qualys			
Activity	**Task**	**Customer**	**Secureworks**
	Configure and install physical vulnerability scanning device(s), and use connectors to appropriately connect device to network; for virtual vulnerability scanning logical device installation, Customer will download from location indicated in Scanning Portal ***Customers in Japan:*** Refer to Secureworks Customer-specific Transaction Document for installation of physical vulnerability scanning device	R, A	C, I
	Provide Customer-side post-install validation steps to Customer	I	R, A
	Complete Customer-side post-install validation steps	R, A	I
	Complete Secureworks-side post-install validation steps	I	R, A
Vulnerability Scanning *See the notes above the table for explanations of items with asterisks (" * ")*	Complete information-gathering SAP form to identify Assets (both internal and external) in scope for the Service*	R, A	I
	Complete ***internal*** Asset Group SAP form to confirm logical groupings for internal Assets*	R, A	I
	Complete ***external*** Asset Group SAP form to confirm logical groupings for external Assets*	R, A	I
	Complete Scan Request SAP form to define times and frequencies for a specific scan*	R, A	I
	Maintain list of IP addresses within the Scanning Portal**	R, A	I
	Create scan schedules (both on-demand and recurring) for executing scans; schedules include frequency and approved times**	R, A	I
	Configure logical asset groupings and scan schedules***	R, A	I
	Create and manage authentication records for authenticated scanning***	R, A	I

Vulnerability Management Service with Qualys			
Activity	**Task**	**Customer**	**Secureworks**
	Create and manage custom scanning configuration/option profiles***	R, A	I
	Monitor scans to confirm completion or if an error occurred; restart scans if needed	R, A	C, I
	Access Scanning Portal to obtain scan results	R, A	C, I
	Identify any anomalies, errors, or network impacts regarding scan results and adjust scan (e.g., adjust option profile) as necessary or submit ticket through Secureworks Client Portal (or otherwise contact SOC) for assistance	R, A	C, I
	Review each scan result (all vulnerability data) and report output (net vulnerability data) and determine next steps	R, A	C, I
	Adhere to any and all scanning license restrictions	R, A	C, I
	Develop and monitor KPIs to measure success of the Service (optional)	R, A	C, I
	Develop and maintain a remediation program or strategy	R, A	C, I
	Remediate vulnerabilities	R, A	C, I
	Identify and apply all patches as required to maintain scanning tool	R, A	C, I
	Review vulnerabilities within scanning tool; accept risk and ignore vulnerability as appropriate for each vulnerability	R, A	C, I
	Manage workflow for accepting risk and ignoring vulnerabilities	R, A	I
	Work with vulnerability scanning vendor for feature enhancements and bug identification	C, I	R
	Provide Customer with general remediation advice per Customer request	C, I	R
Remediation	Create API account to enable Customer to	R, A	C, I

Vulnerability Management Service with Qualys			
Activity	**Task**	**Customer**	**Secureworks**
and Reporting	obtain scan information		
	Design and implement scripts for use with vendor-supplied APIs	R, A,	C, I
	Integrate API data with custom (homegrown) and/or third-party tools	R, A	I
	Define report requirements (each request to set up a scan report in Qualys) and report criteria (the deliverable report within the Scanning Portal)	R, A	I
	Create report templates***	R, A	I
	Create custom reports (not part of vendor-supplied reporting capabilities)	R, A	I
	Access Scanning Portal to obtain scan reports	R, A	I
	Analyze report output	C, I	R, A
Support	Ensure Secureworks has current contact information for authorized contacts regarding Customer's account	R, A	I
	Provide support to Customer for issues relating to the Secureworks Client Portal (including mobile access)	I	R, A
General	Submit through Secureworks Client Portal (or otherwise contact SOC to submit) any tickets for in-scope work	R, A	I
	Perform all Customer-side network changes when needed	R, A	I
	Provide Secureworks with Customer network design and specification for integration with Secureworks services (includes auditing and providing updated designs and specifications when changes are made)	R, A	I

2.3.6 Secureworks Platform Maintenance

To ensure Customer receives the highest level of Service possible, Secureworks will conduct platform maintenance (updates, upgrades, patching, and other platform-specific work) on a periodic basis, as maintenance changes are validated and approved for release into the

Secureworks platform. Secureworks follows internal change control processes to ensure platform stability. Generally, maintenance does not require a network outage. Secureworks will conduct platform maintenance without Customer approval or a maintenance interval when a network outage is not required. Customer acknowledges and agrees that approval or a maintenance interval is only mandatory when a network outage is required.

2.4 Support for Private Virtual Environments

Secureworks will provide support as described herein, for a single-tenant Private Virtual Environment that is located on Customer's premises as part of a service that Customer purchases from Secureworks. The information in this section is part of Customer agreement with Secureworks, and takes precedence over any conflicting information elsewhere in this SD. The subsections below contain information about Customer responsibilities, Secureworks responsibilities, and out-of-scope services with regard to a Customer's Private Virtual Environment in which virtual scanners and/or VSAs are installed. See the Glossary for definitions of terms related to virtualization that are used in this SD.

Note: The Secureworks managed security services and SLAs are the same for both non-virtualized (physical) environments and virtual environments.

2.4.1 Customer Responsibilities

Customer agrees to the responsibilities explained in the subsections below and acknowledges and agrees that Secureworks' ability to perform its obligations and responsibilities, and its liability under the SLAs, are dependent upon Customer's compliance with these responsibilities.

2.4.1.1 Provisioning and Maintenance

Customer is responsible for all aspects of provisioning (installation, configuration, and setup) of supported Hypervisor technology, such as VMware, including but not limited to the following:

- Virtual switches
- Virtual network interfaces
- Virtual networks
- Virtual machines

Customer must perform all maintenance for the Guest virtual machine, which includes the items listed below.

- Guest virtual machine snapshot backup
- Restoration of the image on the Guest virtual machine
- Underlying Hypervisor that provides in-band management access (e.g., access to Customer's network through Simple Network Management Protocol/SNMP) for Secureworks (*Customer must resolve in-band access issues in case of loss of network connectivity for Secureworks to manage the Virtual Security Appliance, if applicable*)
- Troubleshooting (Hypervisor, hardware, and Host/Guest virtual machine)

2.4.1.2 Virtual Machines

Customer is responsible for providing the Guest virtual machine(s) on which the Virtual Security Appliance ("**VSA**") will be installed (if applicable). Customer must provision the virtual machine with the required central processing unit ("**CPU**"), memory, storage capacity, and network resources needed for proper functionality and delivery of the Service. Customer shall provide Secureworks with a privileged account with access to the Guest virtual machine(s). This account may also be used for automation purposes. The OS on the Guest virtual machine must have a valid license for support. Secureworks will not provide any assistance without in-band access to the Guest virtual machine and without a valid license.

2.4.2 Secureworks Responsibilities

If Customer purchases Qualys licenses from Secureworks, then Secureworks is responsible for providing the VSA, providing support to Customer during provisioning of the VSA, and managing and monitoring the VSA that are operating on the Guest virtual machine(s). Customer must maintain a suitable environment in which to operate the Guest virtual machine(s) that is being used for the VSA. This includes using a Secureworks-supported Hypervisor version.

2.4.3 Shared Responsibilities

2.4.3.1 VSA Upgrades

Secureworks will implement upgrades only for the VSA on the Guest virtual machine, as applicable to the Service; Customer is responsible for any other upgrades (e.g., Host/Guest virtual machine, Hypervisor).

2.4.3.2 VSA Backups

It is Customer's responsibility to back up (and otherwise maintain) the image or virtual hard disk for the Guest virtual machine. If a Guest virtual machine requires a rebuild, then Secureworks will restore the prior VSA configuration after Customer restores the Guest virtual machine and its connectivity. Secureworks recommends that any virtual infrastructure be deployed on redundant systems.

2.4.4 Out-of-Scope Services in a Virtual Environment

The following are considered out-of-scope for this Service:

- Restoring the virtual machine image backups
- Troubleshooting issues at the Hypervisor level
- Troubleshooting performance issues not directly related to the scanning tool such as hardware (e.g., a server that is hosting VMware with a scanning engine), Hypervisor, or Host-level issues
- Anything not specifically described herein as part of the standard offering for the Service

2.5 Out-of-Scope

The information in Section 2 comprises the Secureworks standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Items described below are examples of services and activities that are out of scope. Upon request, Secureworks can provide out-of-scope technical support on a time and materials basis pursuant to a separate Transaction Document.

- Custom or Customer-specific vulnerability checks
- Custom or Customer-specific workflows
- Any monitoring (including automated or manual) of scanner appliances
- Application Program Interface ("**API**") support with third-party or custom tools
- Creating API scripts or middleware for third-party tools to interact with scanning data or the Scanning Portal APIs
- Scan status monitoring
- Report customization beyond the native reporting capabilities of Qualys
- Recommendations on capacity planning
- Joining recurring meetings such as change boards or status meetings
- Accessing the Scanning Portal directly (bypassing single sign-on from the Secureworks Client Portal)

- Validating findings to confirm or deny vulnerabilities and remove any false positives
  Note: Only the VMS Support Team for Customers in Japan will provide best effort for false positive removal on a quarterly basis. If additional false positive analysis is needed and/or more frequently, then Secureworks can provide a separate Security Consulting service for an additional charge.
- Performing recurring tasks that are not defined within the service offering (example: purging host scans without schedules)
- Requesting support from specific/named engineers; professional services are available through a separate Transaction Document
- Supporting unsupported features, functionality, or modules
- Asset classification and/or compliance policy creation
- Monitoring Security Events and Qualys-specific Security Events, and alerting Customer about these events

2.5.1 Qualys Modules Not Supported by Secureworks

Customer can directly purchase from Qualys any Qualys modules that are not part of this Service, or are not supported by Secureworks. Contact Secureworks sales representative to be referred to a Qualys Technical Account Manager.

3 Service Fees and Related Information

Service Fees are based on Customer-defined number of IP addresses and/or web applications as indicated in Customer's Transaction Document, up to a maximum of 100,000 IP addresses and 200 web applications (combinations of IP addresses and web applications are subject to the same maximums). See Customer's MSA or CRA (as applicable) and Transaction Document for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Services Term

Note: For any Customer new to Secureworks VMS, following the initial onboarding, the Qualys subscription will be set up and access will be provided to Customer. Billing will commence upon the earlier of: (i) 30 days after access activation or (ii) Customer providing Secureworks with host IP information for its Qualys subscription. For an existing Secureworks VMS Customer adding services to a subscription, billing will commence immediately once access to these services is activated.

3.1 Invoice Commencement and Related Information

See the Service-specific Addendum or Transaction Document for information about invoice commencement.

4 Service Level Agreements ("SLAs")

The table below contains the SLAs that are applicable to the Service. The Secureworks VMS Support Team adheres to these SLAs for implementation and ongoing operations.

SLA	Definition	Credit
P1 Issue	P1 – Critical Priority Issue: In the event of a P1 Issue (defined as an issue that prevents	1/30th of monthly fee for

SLA	Definition	Credit
	Customer from accessing the Service, such as a Scanning Portal outage), Secureworks will respond as follows: – Initial Response*: < 8 hours – Initial Status Update: < 24 hours	scan Service
P2 Issue	P2 – High Priority Issue: In the event of a P2 Issue (defined as an issue in which Customer can access the Service, however, one or more significant functions are unavailable, such as the ability to launch a scan or map) Secureworks will respond as follows: – Initial Response*: < 24 hours – Initial Status Update: 2 Business Days	1/30th of monthly fee for scan Service
Implementation Timing	Secureworks will implement Asset Group configuration, schedule scans, create report templates, create Option Profiles, exclude Hosts, and implement any other configuration item within the Qualys Scanning Portal within three (3) Business Days from the time Customer provides all of the relevant and accurate information to the VMS Support Team through completing all required Secureworks-provided forms.	1/30th of monthly fee for scan Service

* See Glossary for definition.

Warranty Exclusion: While the Service is intended to reduce risk, it is impossible to completely eliminate risk, and therefore Secureworks makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on Customer's network.

The SLAs set forth above are subject to the following limitations:

- Secureworks schedules maintenance outages for Secureworks-owned equipment that is being used to provide the Service and will provide Customer-designated contact(s) with 24 hours of notice of an outage. The SLAs shall not apply during scheduled maintenance outages, and no SLA credit shall apply during a maintenance outage.
- Secureworks shall not be responsible for any Service impact related to any product configuration on a managed Device that is not supported by Secureworks.
- The SLAs shall not apply if any act or omission by Customer prohibits or otherwise limits Secureworks from providing the Service or meeting the SLAs, including but not limited to misconduct, negligence, provision of inaccurate or incomplete information, modifications to the Service, or any unauthorized modifications made to any managed hardware or software Devices, by Customer or its employees, or third parties acting on behalf of Customer.
- The SLAs shall not apply to the extent Customer does not fulfill and comply with the obligations and responsibilities set forth within this SD. The obligations of Secureworks to comply with the SLAs with respect to any false-positive validation would be dependent on Secureworks' ability to connect directly to Customer-Side Technology that is being validated.
- The SLAs shall not apply if Customer-Side Technology is unreachable for reasons that are not within the direct control of Secureworks, such as network connectivity issues, authentication issues, configuration issues, or public cloud unavailability.

For Customer to receive an SLA credit, subject to the limitations above, the notification of the SLA failure must be submitted to Secureworks within thirty (30) days of the date of such SLA failure. Secureworks will

research the notification and respond to Customer within thirty (30) days from the date such notification is received. The total amount credited to Customer in connection with any of the above SLAs in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. The foregoing SLA credit(s) shall be Customer's sole and exclusive remedy for failure to meet or exceed the foregoing SLAs.

5 Additional Considerations and Information

5.1 Vulnerability Management Services Additional Terms

Customer will return renewal paperwork for Qualys services to Secureworks in an agreed-upon time period.

5.1.1 Qualys Subscriber Terms and Conditions

Customer agrees to and accepts the terms and conditions located here:

https://www.qualys.com/docs/qualys-master-cloud-services-agreement.pdf

6 Glossary

Term	Description
Approved Scanning Vendor ("**ASV**") Company	Per the PCI Security Standards Council ("SSC"), an ASV Company is a data security company that has been qualified, and continues to be qualified, by PCI SSC to use an ASV scan solution of such company appearing on the ASV List to determine compliance of its Scan Customers with the external vulnerability scanning requirement of PCI DSS Requirement 11.2.2 for ASV Program purposes.
Asset	A Host object that is identified by its IP address or fully qualified domain name ("**FQDN**") depending on the Host tracking type selected for the Qualys subscription.
Asset Group	A user-defined logical grouping of Host Assets.
Counter Threat Appliance ("**CTA**")	Equipment that specifically allows Secureworks to collect data while performing a Secureworks-defined service for Customer, such as monitoring Customer's network and environment for security threats.
Counter Threat Platform ("**CTP**")	A Secureworks proprietary MSS Services platform that ingests log data to produce events within the CTP system, which are then correlated and analyzed to protect Customer's organization from emerging and existing threats.
Due Diligence	Validating the accuracy of information used to create Customer's original Transaction Document against the actual environment in which services will be performed.
Host Asset	An IP address or FQDN in Customer's Qualys subscription.
Identified Changes	Differences (e.g., Device quantity, make, model, software package, or software version) that are discovered while conducting due diligence for the Service.

Term	Description
In-Band	Activity within a defined telecommunications frequency band.
Initial Response	The first contact from Secureworks to Customer after creation of a P1 or P2-specific ticket by Customer or Secureworks.
Private Virtual Environment	Customer's on-premises virtual infrastructure.
Public Cloud Environment	Third-party virtual infrastructure that hosts the Customer's network and security devices.
Qualys Scanning Portal ("**Scanning Portal**")	The portal in the Qualys solution that provides Customer with access to reporting and other capabilities.
Definitions for Virtual Environments	
Guest	Separate and independent instance of operating system and application software that operates on a Host.
Host	Virtual Machine host server that provides the physical computing resources, such as processing power, memory, disk, and network I/O.
Hypervisor	Virtual Machine monitor that isolates each Guest, enabling multiple Guests to reside and operate on the Host simultaneously.
Virtual Contexts	A form of virtualization where one physical firewall is divided into two (2) or more virtual firewalls.
Virtual Machine	A logical instance of the physical Host that houses the operating system of the Guest.
Virtual Security Appliance ("**VSA**")	Software implementation of a security device—e.g., a log retention appliance, scanner appliance (VMS), intrusion detection system—that executes programs in the same manner as a physical machine.