Vulnerability Management
Service Description and Service Level Agreements

This Service Description and Service Level Agreement is provided for the customer ("you" or "Customer") and the Dell entity identified in Customer's Service Order for the purchase of this Service (defined below). This Service is provided in connection with Customer's separate signed master services agreement or security services schedule that explicitly authorizes the sale of managed security services. In the absence of either a master services agreement or security services schedule, this service is provided in connection with the Dell SecureWorks Master Services Agreement, available at http://Dell.com/SecurityTerms and incorporated by reference in its entirety herein.

Service Overview

The Dell SecureWorks Vulnerability Management Services (referred herein as "VMS" or the "service") delivers vulnerability assessments of Customer's environment. VMS consists of automated and recurring vulnerability and compliance scanning.

Vulnerability Management Service Tiers

VMS includes the following IP Level Scanning tiers:

- VMS Express Lite Scans
- VMS Express Lite Perimeter Scan
- VMS Express PCI Scans

VMS includes the following Service Level tiers

- Gold

The VMS service tiers are described in more detail below.

VMS IP Level Scanning Tiers

VMS delivers vulnerability scanning, remediation tracking workflow, reporting, and trending of a Customer's environment. IP level is based on Customer's technical scanning requirements.

- **Express Lite**– The Express Lite option provides unlimited scanning recurrence of Customer's internal, external, and cloud-based live IP addresses. Scans of external IPs are conducted remotely. Scans of internal and cloud-based IPs are conducted from one or more Scan Appliances placed on Customer's network or in Customer's leased virtual datacenter. Scan Appliance quantities are restricted to two (2) per Customer. User accounts are limited to three (3) per Customer. Additional appliances and user accounts are not available at the IP level or service level.

  Express Lite Perimeter – The Express Perimeter option provides unlimited scanning recurrence of Customer's external live IP addresses. Scans are conducted remotely. Scan appliances are not available for this service. User accounts are limited to three (3) per Customer. Additional user accounts are not available at the IP or service level. Customers conduct scans in a self-service mode, which means

The Customer must choose one of the three (3) previously defined levels based on the consideration of the following:

- Live IP address quantity

- Application quantity
- Internal and/or external scanning
- Scanning appliance quantity
- User account quantity
- Scanning recurrence

Service Level Tiers

This section describes the features of the Gold Service Level tier. Some features are optional. Stand-alone options may be purchased at an additional cost, either at the time of execution of the initial Services Order or later during the Term, provided that Dell SecureWorks, in its sole discretion, continues to make such options generally available for individual purchase.

- **Gold** – The Gold Service Level tier features technical scanning functionality described in the Bronze service level as well as scan management delivered by the Dell SecureWorks MSS Security Operations Center. Scan management functions include scheduling scans, setting up profiles, running on-demand scans with advance notice, quarterly scan reviews upon Customer request, and the importing of assets groups, values, system owners, and compliance policies (with the Policy Compliance add on).

Service Level Tiers Matrix

✓ Denotes the feature is included with no additional fee or monthly recurring revenue (MRR) required
O Denotes the feature is optional with an additional fee or MRR associated
– Denotes the feature is not available under the specified Service Level

Service Features	Gold	Description
Customer Management	O	Customer Manager (CM) assigned to account
Additional User Accounts (Tokens)	O	Option to purchase User Accounts (Tokens) above maximum quantity level
24x7 SOC Access	✓	SOC documents requests for Engineering support SOC will be available to assist with user-access issues, stop scans, or service unavailable issues. SOC will not assist with questions regarding the service, reporting, troubleshooting, etc. These types of requests will be handled by the VMS Engineering team Monday – Friday, 9am-5pm EST.
Initial Implementation Support	9am-5pm EST, M-F, excluding U.S. holidays	Implementation team available remotely for implementation support
Expedited Provisioning	O	Optional expedited provisioning of scanning appliance (3 days)
Extended Data Retention	✓	Data is stored remotely for contract term
Upfront GSC Asset Classification and Compliance Policy Creation	O	Optional Security Risk Consulting required

Service Features	Gold	Description
Vulnerability Reporting	✓	Self-service vulnerability and compliance reporting within the capabilities offered in the Qualys tool
Enterprise Security portal	✓	Vulnerability data available through the Enterprise Security portal
Scan Scheduling	✓	Dell SecureWorks will schedule and manage recurring scans.
Quarterly Scan Review	✓	Dell SecureWorks will review scan results with Customer each quarter, upon Customer request.
Profile Setup	✓	Dell SecureWorks will adjust scan profiles based on Customer criteria.
Group/Asset Value/Asset Owner Entry	✓	Dell SecureWorks will import Customer-created group, asset, and owner data.
Asset Compliance Policy Entry	✓	Dell SecureWorks will enter an asset configuration policy within the compliance technology.
On-Demand Scan Request	✓	Dell SecureWorks will schedule Customer scans on request with three (3) business days advance notice.
Asset Compliance	O	Dell SecureWorks will audit asset compliance with pre-defined policies and controls.

Service Level Tiers Feature Descriptions

24x7 SOC Access

VMS Customers can contact Dell SecureWorks 24X7X365 via email or telephone. The Customer can use help desk calls for:

- Asking questions about the results of the Service, troubleshooting, or reviewing scan results, which will result in a ticket to the VMS Engineering team to be handled Monday – Friday, 9am-5pm EST.
- Changing contact information or rescheduling test dates and times.
- Solving issues associated with accessing the VMS service.
- Stopping scans during a network impacting event.

NOTE: Help desk calls cannot be used for general consulting advice that does not directly pertain to the results of the Service.

Extended Data Retention

Customer scanning data is available via the Qualys portal for the life of the contract if configured.

Vulnerability Reporting

Dell SecureWorks provides Customer with full access to the Qualys portal to run a variety of reports. Executive Remediation Reports, High Severity Reports, Top 20 Reports, Patch Reports, and Scan Results are examples of vulnerability reports that are available via the Qualys portal. Report capabilities are restricted to the capabilities of the platform and are Customer's responsibility to generate.

Additional scan report result information is as follows:

- Vulnerability reporting with a description of each vulnerability, level of severity, business and technical impact, CVSS, remediation suggestions, and links to relevant sites

- Discovery reporting, detailing live hosts discovered on the network, including graphical maps
- Trending of vulnerability data
- Vulnerability remediation tracking and workflow

NOTE: Custom reports are not generated and delivered as part of this feature.

Qualys portal

Dell SecureWorks provides Customer with access to the Qualys portal through use of the SSO functionality. The Qualys portal may only be accessed by the named individuals specified by Customer during the Information Gathering phase (defined below) and identified on the Service Activation Profile ("SAP") or by the individuals who have been added to the list of named individuals after Service Activation. All information received by Customer through the Qualys portal is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization.

Within the Qualys portal, Customer is able to access a dashboard, a network discovery map, perform discovery scans, schedule vulnerability scans, run reports, track remediation status, and perform asset searches.

Scan Scheduling

Dell SecureWorks will work with Customer to gather targeted IP address and/or URL information and then schedule, run, and maintain scans. The Customer must contact Dell SecureWorks with relevant scan information within ten (10) days of the date they wish to scan.

Quarterly Scan Review

The Customer contacts Dell SecureWorks ten (10) days prior to the requested date to schedule a conference call to review scan findings, answer questions related to scan results, and discuss remediation strategies. The conference call is limited to one (1) hour each quarter.

Profile Setup

Dell SecureWorks will assist Customer in selecting individual scan engine profiles as requested by Customer.

Asset Compliance Policy Entry

Dell SecureWorks will enter a Customer asset compliance policy into compliance technology. Policy entries are limited to three (3) per contract term and must be pre-defined by Customer. Up to eight (8) policy, control, and value changes are allowed per month.

Dell SecureWorks will not define asset policies or custom controls. This is the responsibility of Customer. Customer user defined controls will be evaluated on a case by case basis. The Customer will be responsible for managing and entering exceptions.

On-Demand Scan Request

Dell SecureWorks will run on-demand scans at Customer request. On-demand scans are limited to five (5) per month. Customer-run on-demand scans are unlimited. Dell SecureWorks requires at least 3 business days of lead time to schedule and run the scan.

Asset Compliance

Asset Compliance assists organizations with increasing security by assessing compliance with policies in regards to system configurations and access controls.

Through credential-based authentication, Dell SecureWorks collects operating system configurations and application access controls from hosts and servers within the enterprise and then maps this

information to pre-defined policies in order to measure compliance with external regulations and internal security requirements.

Provisioning, Activation, and Service Commencement

Provisioning

Provisioning refers to the service setup activities. The Standard Provisioning period begins at receipt of the signed SO by MSS Deployment Team and ends with the commencement of the service. The provisioning and setup period is dependent on a number of factors, such as the number of devices (if applicable), the number of physical sites, the complexity of the network and Customer requirements, and the ability of Customer to provide Dell SecureWorks with requested information within a mutually agreed-upon timeframe. Dell SecureWorks does not provide SLAs for completing Device service setup within a specified period of time.

Provisioning into Customer On-Premise Networks

Standard Provisioning activities include:

- Scheduling Kick-off and Solution Design call (assumes receipt of SO by MSS Deployment Team)
- Information Gathering (Dell SecureWorks provides information requirements and forms for completion to Customer)
- (Optional/as needed) Dell SecureWorks design of a solution architecture diagram (assumes Dell SecureWorks receipt from Customer of complete and accurate information and diagrams)
- Configuring Customer Relation Management ("CRM") / Ticket system (assumes Customer approval of MSS solution design diagram(s))
- Configuring the appliance (if applicable)
- Shipping the appliance – ground shipping (if applicable)

Provisioning into Customer Cloud-Based Networks

Standard Provisioning activities include:

- Scheduling Kick-off and Solution Design call (assumes receipt of SO by MSS Deployment Team)
- Information Gathering (Dell SecureWorks provides information requirements and forms for completion to Customer)
- (Optional/as needed) Dell SecureWorks design of a solution architecture diagram (assumes Dell SecureWorks receipt from Customer of complete and accurate information and diagrams)
- Configuring Customer Relation Management ("CRM") / Ticket system (assumes Customer approval of MSS solution design diagram(s))
- Customer download and provisioning of virtual Scan Appliance into Customer's cloud
- Configuring the appliance

VMS Service Activation

Service Activation and commencement consists of the following phases:

- Information Gathering
- Site Planning and Preparation

- Customers that require an internal scanning appliance

Information Gathering

Once Dell SecureWorks receives the Service Order, Dell SecureWorks provides Customer with a Service Activation Profile ("SAP") to be completed. SAPs include information required to provision the Service such as contact information, IP addresses, URLs, telephone numbers, and scan appliance locations.

Site Planning and Preparation

If scanning options are selected that include internal scanning, and for which Customer requires use of a Scan Appliance, Customer is responsible for ensuring that the implementation site complies with Dell SecureWorks' physical/environmental requirements.

Using data gathered during the Information Gathering phase, Dell SecureWorks determines the number of Scan Appliances required for the Service(s) and the appropriate deployment location(s) of the Scan Appliance(s) within Customer's environment. If changes to Customer's existing network architecture are required for Service implementation, Dell SecureWorks communicates these changes to Customer.

Service Commencement

The Service Commencement will occur on the date listed on the Service Activation Profile provided the following conditions have been met (as applicable):

- Information Gathering is complete
- Site planning and preparation is complete (if applicable)
- Customer data is available on the portal (Vulnerability Scanning, Asset Compliance Scanning)

Change Control

Customers can reschedule the date and time of any Gold Service by contacting Dell SecureWorks, via email or telephone, at least five (5) business days prior to the next scheduled test or scan. A new date for the test or scan must be provided when Customer contacts Dell SecureWorks to reschedule.

All tests and scans must be completed within the applicable Service period. Unused tests and scans will not be refunded and cannot be used after the applicable Service period has expired.

The Customer Security Portal

Dell SecureWorks provides Customer with access to Customer Security portal ("portal"). The portal may only be accessed by the named individuals specified by Customer during the Information Gathering phase and identified on the SAP. All information received by Customer through the portal is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization.

Customer Requirements

Dell SecureWorks requires Customer to agree to certain conditions of service delivery.

VMS Delivery

The following procedures apply to the delivery of Vulnerability Management Services:

- Total IP quantities selected are limited to unique live IP instances and may not be rotated throughout the term of the contract for Enterprise, Express, and Express Perimeter accounts.

- Scan results and suggested remediation guidance are made available on the Qualys portal in real time as the scan is completed.

Data Backups

The 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 Services or corruption or loss of data. The Customer agrees that it is Customer's responsibility to perform regular backups of all data contained in or available through the devices connected to Customer's IP address and/or domain names.

Cloud-Based IP Address Acknowledgement

The Customer acknowledges that the IP address of cloud-based assets is subject to change. The Customer agrees that it is Customer's responsibility to identify the specific IP addresses of cloud-based assets that are to be scanned.

Third Party IP Addresses: Authority and Indemnification

Except as set forth herein, Customer may use the Services only to scan the IP Addresses owned by and registered to Customer, or for which Customer otherwise 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 Services, or any part thereof, or permit third parties to benefit from the use or functionality of the Service via timesharing, service bureau arrangements or otherwise. In the event one (1) 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 warrants that it has the consent and authorization from such Host(s) necessary for Dell SecureWorks to perform the Services. Customer agrees to facilitate any necessary communications and exchanges of information between Dell SecureWorks and Host.

Indemnification

Customer agrees to indemnify, defend, and hold Dell SecureWorks harmless from and against any and all claims, losses, liabilities and damages, including reasonable attorney's fees, arising from (i) any and all third party claims brought against Dell SecureWorks that arise out of the scanning, testing and/or evaluation of incorrect or unauthorized IP Addresses that are provided by Customer, or (ii) any breach of a Customer representation or warranty.

Export

Customer acknowledges that the Products, Software and Services provided under this agreement, which may include technology and encryption, are subject to the customs and export control laws and regulations of the United States, and may be rendered or performed either in the U.S., in countries outside the U.S., or outside of the borders of the country in which you or your system is located, and may also be subject to the customs and export laws and regulations of the country in which the Products, Software or Services are rendered or received. Customer agrees to abide by those laws and regulations.

Service Level Agreements (SLAs)

Dell SecureWorks' VMS Services cannot identify weaknesses in network architecture (other than any identified during the upfront service activation based on the documentation made available by Customer) or weaknesses in general application architecture.

Dell SecureWorks does not guarantee that every vulnerability on every tested system or application will be discovered. Dell SecureWorks does not guarantee that there will be no false positives.

The nature of vulnerability scanning is such that certain vulnerabilities and mis-configurations of Customer devices (*e.g.* un-patched hosts or the use of older, unsupported versions of software) can pose risks when scanned. Dell SecureWorks cannot guarantee that VMS vulnerability assessments will not adversely affect the performance or availability of the target systems.

The SLAs and SLA Credits for VMS are shown in the below table.

Service	SLA	SLA Credit
VMS Scanning Services	P1 – Critical Priority Issue: In the event of a P1 Issue (defined as an issue that prevents Customer from accessing the Service), Dell SecureWorks' will respond as follows: • Initial Response: < 8 hours • Status Update: 24 hours	1/30th of monthly fee for scan service
VMS Scanning Services	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), Dell SecureWorks will respond as follows: • Initial Response: < 24 hours • Status Update: 2 business days	1/30th of monthly fee for scan service

"Initial Response" is defined as the initial contact from Dell SecureWorks following the creation and submission of a P1 or P2 related ticket by Customer or Dell SecureWorks.

A status update will be communicated to Customer if the incident cannot be resolved immediately. A final follow-up with Customer occurs on the resolution date. The issue will remain open until the issue is resolved, in Dell SecureWorks' reasonable opinion.

DISCLAIMER. The Vulnerability Management Services will be provided in accordance with this Service Description and the Service Level Agreements contained herein. Dell SecureWorks expressly disclaims all other warranties of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and non-infringement. Dell SecureWorks makes no warranty that the Services will meet Customer's requirements, or that the Services will be uninterrupted, timely, secure, or error-free. Dell SecureWorks makes no warranty as to the results that may be obtained from the use of the Services or as to the accuracy or reliability of any information obtained through the Services. Dell SecureWorks makes no warranty that Customer's vulnerability data will be protected or secure at all times. No advice or information, whether oral or written, obtained by Customer from Dell SecureWorks or through the Services shall create any warranty.

QUALYS SUBSCRIBER TERMS AND CONDITIONS

1. Ownership. As between the parties, all Intellectual Property Rights ("IP Rights") relating to the Qualys Hardware, Qualys Service and the Qualys Reports, all software, data and information contained therein or related thereto (excluding individual factual data gathered from Customer's network Internet Protocol addresses), are exclusively owned by Dell SecureWorks or its service provider Qualys, and Customer acknowledges and agrees that it will not obtain any rights or interests thereto, except as expressly granted in this Qualys Subscriber Terms and Conditions. Customer agrees not to use or access the any data or information contained in the Qualys Service or provided through the Qualys Service, except for the limited purpose of receiving and internally reviewing reports generated from scans of Customer's Internet Protocol addresses.

2. Restrictions on use. Customer agrees not to: (a) distribute, sublicense, lease, rent, loan, or otherwise transfer the Qualys Service to any third party or permit any third party to benefit from the use or functionality of the Qualys Service via timesharing, service bureau arrangements or otherwise; (b) use the Qualys Hardware, Qualys Service, Qualys Reports, API or any data or information contained in any of the foregoing, except for the limited purpose of vulnerability management with regard to the Internet Protocol addresses for which Customert has or may purchase subscriptions to the Qualys Services; (c) open, disassemble, or tamper with the Qualys Hardware in any fashion; (d) transfer possession of the Qualys Hardware to any third party; (e) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of the Qualys Software that is embedded in the Qualys Hardware or that provides the Qualys Service;. Customer will not remove, alter, or obscure in any way all IP Right notices (including copyright notices) of SecureWorks or its service provider, Qualys, on or within the copies of the Qualys Service.

3. Disclaimer. Customer acknowledges and agrees that the scanning of Internet Protocol addresses and/or domain names may expose vulnerabilities and in some circumstances could result in the disruption of the Qualys Services at such site(s). Certain optional features of the Qualys Service, including exploitive scans, involve substantial risk of Denial of Service (DOS) attacks, loss of service, hardware failure and loss or corruption of data. Consequently, Customer agrees that it is Customer's responsibility to perform backups of all Customer Data contained in or available through the devices connected to Customer's Internet Protocol addresses and/or domain names prior to invoking the use of the Qualys Service.