1 VMS Addendum: Qualys Add-on Modules

This document is an Addendum to the **VMS with Qualys** and **VMS Platinum** service descriptions.

1.1 Secureworks-supported Add-on Modules

The Secureworks-supported add-on modules listed below are optional and are sold independent of a Vulnerability Management Service ("**VMS**" or the "**Service**") for an additional charge or bundled with VMS. In addition, output from the Service can be used in delivering these add-on modules. Customer will access purchased add-on modules and associated functions/outputs directly from within the Qualys Scanning Portal.

Note: Each explanation below indicates Customer's responsibilities as applicable to VMS with Qualys and VMS Platinum.

- **Cloud Agent:** The Cloud Agent facilitates transfer of information between the Qualys cloud and the system on which the Cloud Agent is installed—for purposes of conducting vulnerability scanning and conducting activities for other host-based Qualys services. Customer can deploy Cloud Agent through their preferred endpoint manager. Secureworks will assist Customer with the Cloud Agent as needed.

  A license must be purchased for each Cloud Agent that will be installed on each Host. Hosts on which the Cloud Agent will be installed require a VMM or Policy Compliance license; therefore, Customer must purchase VMM or Policy Compliance if Customer will be using Cloud Agent. Hosts on which Cloud Agents are installed must be connected to Customer's network with access to the Internet. Customer will install Cloud Agents on compatible systems/endpoints (e.g., Linux, Windows) for Host-based vulnerability scanning.

  For Customers purchasing VMS with Qualys, it is Customer's responsibility to do the following:

  - Ensure all Qualys Cloud Agent hosts underlying operating system version type(s) are in scope for the Service and are supported by the vendor
  - Manage and maintain both endpoints and Cloud Agents, including installation, upgrades, and ongoing maintenance
  - Ensure and monitor Qualys Cloud Agent availability and connectivity
  - Remediate issues with Qualys Cloud Agent availability and performance
  - Troubleshoot Qualys Cloud Agent software
  - Deployment of Cloud Agents and applying appropriate license keys

  For Customers purchasing VMS Platinum, see the RACI table ("Customer and Secureworks Responsibilities") in the **VMS Platinum SD**.

1.1.1 Additional Customer Obligations

1.1.1.1 Endpoint Software Requirements

Customer must ensure that the operating system versions for all Hosts on which Qualys Cloud Agents are installed are supported by both the vulnerability management tool vendor and Secureworks.

1.1.1.2 Endpoint Management

Customer is responsible for managing and troubleshooting the endpoints, including the following:

- Installations and upgrades of the Qualys Cloud Agent
- Ensuring Qualys Cloud Agent availability and connectivity
- Monitoring Qualys Cloud Agent performance
- Responding to and remediating issues with Qualys Cloud Agent availability and performance

- **Threat Protection:** Cloud-based solution that helps Customer automatically prioritize vulnerabilities that pose the greatest risk to its organization by correlating active threats against the vulnerabilities. A prioritized view of vulnerabilities enables Customer to identify which vulnerabilities to focus on first and which actions will have the most impact to Customer's organization. A live Threat Intelligence Feed is included; Qualys security engineers continuously validate and rate new threats from internal and external sources. The feed also shows how many of Customer's Assets are impacted by each threat, and enables Customer to drill down into each Asset for remediation. It is Customer's responsibility to create threat protection dashboards, and customize all dashboards and widgets within the Scanning Portal.
    - ***Dashboards and Trending:*** Customer can view threat posture with dashboards, see how systems are exposed to active threats (such as zero-day threats, denial-of-service attacks, actively attacked vulnerabilities, and other types of active threats); create multiple dashboard views and convert any search query into a dashboard widget; measure progress and remediation efforts with real-time trend analysis; and generate scan and patch reports for other stakeholders
    - ***Searches:*** Enables users to save any search; convert any search into a dashboard widget; export relevant data to files; share search results through Qualys APIs; and drill down and fine-tune results using sort, tags, filters, or specific vulnerabilities

- **Continuous Monitoring:** Provides Customer with a centralized interface for finding hosts and digital certificates, organizing Assets by business function or technology, and setting up automated, targeted alerts to report on changes; also, allows Customer to identify which hosts need to be monitored, what to monitor for, and who to alert when there is a change; alerts can be tailored to specific conditions such as the following:
    - ***Hosts and Devices:*** See when systems appear, disappear, or are running unexpected operating systems
    - ***Digital Certificates:*** Rack SSL certificates used on systems to know if they are weak or self-signed, and when they are due to expire
    - ***Ports and Services:*** Keep tabs on which network ports are open, which protocols are used, and whether they change over time
    - ***Vulnerabilities on Hosts or in Applications:*** Know when potential or confirmed vulnerabilities appear (or reappear), how severe they are, whether they can be exploited, and if patches are available
    - ***Applications Installed on Perimeter Systems:*** Find out when application software is installed or removed from these systems

  For Customers purchasing VMS with Qualys*,* it is Customer's responsibility to configure the rules in the Scanning Portal, and to define which hosts to monitor, what to monitor for, and who to alert when there is a change. ***For Customers purchasing VMS Platinum***, Secureworks will configure the rules in the Scanning Portal, and it is Customer's responsibility to define which hosts to monitor, what to monitor for, and who to alert when there is a change.

- **Security Configuration Assessment ("SCA"):** Qualys SCA helps Customer assess, report, monitor, and remediate security-related configuration issues based on the Center for Internet Security (CIS) Benchmarks. SCA supports the latest out-of-the-box CIS Benchmark releases of operating systems, databases, applications, and network devices.
    - ***Accountability for Controls:*** Qualys SCA controls are developed and validated by Qualys security experts and certified by CIS. The controls are optimized for performance, scalability, and accuracy. Qualys SCA can be used in IT environments of any size, from small to the largest organizations.
    - ***Ease of Use:*** SCA CIS assessments are provided through a web-based user interface and delivered from the Qualys Cloud Platform, enabling centralized management with minimal deployment overhead. CIS controls can be selected and customized according to an organization's security policies. This eliminates the cost, resource and deployment issues associated with traditional software point products for configuration management.

- ***Reports and Dashboards:*** SCA users can schedule assessments, automatically create downloadable reports of configuration issues, and view dashboards for improving their security posture. This brings full circle Qualys SCA's automation of security best practices behind leading benchmarks, and lets InfoSec teams take a proactive approach towards digital business security.

For Customers purchasing VMS with Qualys, it is Customer's responsibility to do the following:

- Complete Asset Identification SAP to identify Asset Groups
- Define scan schedules, scan frequency and approved scanning times
- Complete Scan Schedule SAP
- Monitor scans for errors and completion
- Retrieve SCA policy scan results from Customer's scanning subscription
- Identify any anomalies, errors, or network impacts regarding scan results and adjust scan (e.g., adjust option profile) as necessary
- Review scan result and report output for accuracy
- Customer must ensure staying within their license restrictions
- Develop and monitor KPIs to measure success of the compliance service
- Remediate failures
- Identifying and applying any patches to be applied
- Ignoring failures or granting exceptions
- Managing workflow for ignoring failures or granted exceptions
- Create and manage authentication records for authenticated scanning
- Address any issues with authentication failures within Customer environment
- Import any policies (where technology applicable) as necessary to measure compliance
- Validate success of policies and controls within the Customer's environment
- Customize control/plugin values to match Customer defined policy

For Customers purchasing VMS Platinum, see the RACI table ("Customer and Secureworks Responsibilities") in the **VMS Platinum SD**.

Secureworks will submit requests to vendor for feature enhancements and bug identification. If Customer wants Secureworks to configure Asset Groups and/or scan schedules within Customer's scanning subscription, then Customer will complete and return the necessary Secureworks-provided forms; otherwise, Customer will configure Asset Groups and/or scan schedules.

- **Web Application Scanning:** The Secureworks Web Application Scanning Service ("**WAS**") consists of automated, self-service vulnerability scanning of internal and external (Internet-facing) web-based applications using QualysGuard Web Application Scanning Service (QG WAS). This service supports Customers' compliance with PCI DSS version 3.2 Requirement 6.6, regarding the security of Internet-facing web applications.

Secureworks provides a self-service WAS solution on the Scanning Portal access to a user interface to conduct WAS for both internal and external applications (note: scanning internal, i.e., non-Internet-facing web applications, requires Customer subscription to and acquisition of a QualysGuard scanner appliance). Customer has the ability to conduct WAS scans with complete vulnerability detection, customizable password brute forcing, standard scanning for sensitive content and standard scanning using authentication. Scan scheduling, report generation, and scan results retrieval is available as part of the Scanning Portal.

For the purposes of this SD and delivery of the Service, an "application" is a unique URL or fully qualified domain name ("**FQDN**"), such as the following: www.acme.com, 201.12.50.100/production, and www.xx2.com/users.

To improve the value of the WAS results, upon Customer's request, the VMS Support Team will validate the findings that can be manually reproduced using one or more third-party scanning tools, with a response goal of three (3) Business Days for each validation request. This is limited to ten (10) validations per calendar quarter per one hundred subscribed web applications, with a validation being defined as a combination of URL and parameter. For example, validation of a single URL with five (5) parameters would be five (5) validations, as would validation of five (5) separate URLs with one parameter each.

For Customers purchasing VMS with Qualys, it is Customer's responsibility to do the following:

- Fill out Web Application SAP to identify FQDNs for web apps to be scanned
- Define scan schedules, scan frequency and approved scanning times
- Fill out Scan Schedule SAP
- Monitor scans for errors and completion
- Retrieve web application scan results from Customer scanning subscription
- Identify any anomalies, errors, or network impacts regarding scan results and adjust scan (e.g., adjust option profile) as necessary
- Review scan result and report output for accuracy
- Customer must ensure staying within their license restrictions
- Identifying and applying any patches to be applied
- Develop and monitor KPIs to measure success of the WAS service
- Develop and maintain a remediation program or strategy
- Remediate vulnerabilities
- Ignoring vulnerabilities or granting exceptions
- Managing workflow for ignoring vulnerabilities or granted exceptions
- Create, manage and troubleshoot authentication records for authenticated web application scans
- Identify any black/white lists for web application scan

For Customers purchasing VMS Platinum, see the RACI table ("Customer and Secureworks Responsibilities") in the **VMS Platinum SD**.

Secureworks will do the following:

- Provide generic remediation advice as applicable and as provided by the scan results
- Submit requests to vendor for feature enhancements and bug identification
- Perform manual validation of specific findings (the WAS results) request as explained above, upon Customer's request

If Customer wants Secureworks to configure web applications and/or scan schedules within Customer's scanning subscription, then Customer will complete and return the necessary Secureworks-provided forms; otherwise, Customer will configure Asset Groups and/or scan schedules.

- **PCI Scanning:** The Payment Card Industry ("**PCI**") Scanning Service consists of vulnerability scanning of in-scope PCI IP addresses, review of Customer-submitted false-positive exceptions, reports available through the PCI Portal, and attestation signing as specified by the PCI Security Standards Council. Qualys is a PCI Security Standards Council Approved Scanning Vendor (ASV) Company. Secureworks VMS customers will leverage Qualys as their ASV Company to deliver the attestation reports in accordance with the PCI ASV guidelines and handle false-positive attestations, while Secureworks will provide informational support in using the Qualys platform.

  Secureworks provides merchants and service providers with a self-service PCI solution that includes PCI compliance workflow. The Qualys PCI Portal, which is separate from the Scanning Portal, allows Customers to access a self-service scanning interface to schedule quarterly scanning and reporting with the electronic filing capabilities to simplify PCI administration.

  Note: For PCI customers in Japan, ASV attestations, false-positive exceptions, and other support from Qualys is only available in English.

Service Feature	Description
Executive Report	Self-Service vulnerability reporting within the capabilities offered in the Qualys tool.
Attestation Report	Vulnerability data available through the Enterprise Security Portal.

Service Feature	Description
PCI-level scans of in-scope websites	Meets PCI requirements for scanning in-scope websites. Customer provides IP addresses. NOTE: In-depth web scanning beyond PCI is available as a separate service

For Customers purchasing VMS with Qualys, it is Customer's responsibility to do the following:

- Identify PCI in-scope hosts
- Fill out scan schedule SAP
- Configure scan schedules within Customer's scanning subscription
- Identify any false positives
- Submit false positive requests via scanning tool
- Submit any required evidence for false positive submission
- Retrieve vulnerability scan results from Customer scanning subscription
- Identify any anomalies, errors, or network impacts regarding scan results and adjust scan (e.g., adjust option profile) as necessary
- Review scan result and report output for accuracy
- Customer must ensure staying within their license restrictions
- Develop and monitor KPIs to measure success of the PCI service
- Develop and maintain a remediation program or strategy
- Remediate vulnerabilities
- Identifying and applying any patches to be applied
- Submit report Attestation requests for signing
- Submit Attested reports to acquirers
- Fill out PCI SAQ
- Submit SAQ to necessary entities
- Working with a QSA as necessary

For Customers purchasing VMS Platinum, see the RACI table ("Customer and Secureworks Responsibilities") in the **VMS Platinum SD**.

Secureworks will provide generic remediation advice as applicable and as provided by the scan results, and submit requests to vendor for feature enhancements and bug identification.

- **PCI Scanning Reporting** – Various PCI specific reports are available depending on the selected scanning technology. Sample reports include the following:
  - ***Executive Summary Report:*** Provides Customer network information while summarizing the PCI scan results. If the Customer meets all of the requirements set forth in the PCI procedures and/or requirements, the executive summary will contain a statement of compliance. If the Customer fails to meet those requirements, the executive summary will reflect non-compliance.
  - ***Detailed Vulnerability Report:*** Provides a detailed and technical view of the scan results and includes a section that categorizes discovered vulnerabilities according to the PCI procedures.
  - ***Attestation of Scan Compliance Report:*** Provides a summary of Customer's network and its PCI compliance (pass or fail) assertions by Customer and the Approved Scanning Vendor (ASV) that the scan complies with the PCI Council requirements.
- **PCI Portal** – The PCI Portal is separate from both the Secureworks portal and the Qualys Vulnerability Management portal. Hence requiring a separate individual logon to enable access. This will be supplied during implementation. Depending on the type of PCI Scanning Service purchased, Customer will be provided with access to the PCI Portal which provides automated workflow support, results storage and report generation for the PCI scanning process. The reports and information generated with the PCI Service are restricted by the requirements of the PCI DSS. For example, scan results must be less than 30 days old to be considered recent and valid for PCI reporting.
- **PCI False Positive Exception Handling** – The ASV will review false positive submissions submitted by the Customer. Customers are required to submit these submissions and any supporting documentation or evidence as requested by the ASV. Evidence may include logs, screenshots,

configuration information, etc. The ASV will determine acceptance or non-acceptance of the submission and will note this on the appropriate PCI reports.

- **Policy Compliance:** Secureworks will provide Customer with access to the Scanning Portal to execute reports. Compliance Dashboard, Policy Summary Reports, Policy Compliance Reports, Authentication Reports, Policy reports, Compliance Scorecard reports, Control Pass/Fail reports, and Individual Host Compliance Reports are examples of policy compliance reports that are available with an applicable Policy Compliance add-on module. Report capabilities are restricted to the capabilities of the scanning platform and it is Customer's responsibility to generate reports.

  This add-on module automates the process of assessing server and application configuration compliance with desired policy. It is most useful for organizations subject to compliance mandates (e.g., PCI, HIPAA) that impose specific constraints on server or application configurations. Policy Compliance delivers configuration compliance scanning, remediation tracking workflow, and reporting of Customer's environment. If Customer purchases Cloud Agent to use with Policy Compliance, then endpoints can also be assessed for compliance.

  For Customers purchasing VMS with Qualys, it is Customer's responsibility to do the following:

  - Complete Asset Identification SAP to identify groupings of Assets
  - Define scan schedules, scan frequency and approved scanning times
  - Fill out Scan Schedule SAP
  - Monitor scans for errors and completion
  - Retrieve policy compliance scan results from Customer scanning subscription
  - Identify any anomalies, errors, or network impacts regarding scan results and adjust scan (e.g., adjust option profile) as necessary
  - Review scan result and report output for accuracy
  - Customer must ensure staying within their license restrictions
  - Develop and monitor KPIs to measure success of the compliance service
  - Remediate failures
  - Identifying and applying any patches to be applied
  - Ignoring failures or granting exceptions
  - Managing workflow for ignoring failures or granted exceptions
  - Create and manage authentication records for authenticated scanning
  - Address any issues with authentication failures within Customer environment
  - Build/Import any policies (where technology applicable) as necessary to measure compliance
  - Build any custom controls (where technology applicable) necessary to measure compliance
  - Validate success of policies and controls within the Customer's environment
  - Customize control/plugin values to match Customer defined policy

  For Customers purchasing VMS Platinum, see the RACI table ("Customer and Secureworks Responsibilities") in the **VMS Platinum SD**.

  Secureworks will submit requests to vendor for feature enhancements and bug identification. If Customer wants Secureworks to configure Asset Groups and/or scan schedules within Customer's scanning subscription, then Customer will complete and return the necessary Secureworks-provided forms; otherwise, Customer will configure Asset Groups and/or scan schedules.

  - **Compliance Policy Definition** – Compliance policy creation or definition may be added pursuant to a SOW through Secureworks Security Consulting. A consultant will work with Customer to create one or more new compliance policies that Customer will import or build within the Policy Compliance Portal and apply to specified Assets.

- **Asset View:** Cloud-based solution for a continuously updated inventory of all Customer's Assets (also known as Host Assets), regardless of where they reside. ***Note:*** This module is bundled into the Service, and is supported by a community; Customer can interact with others, similar to a forum. The community includes CMDB Sync (SYN) for synchronizing Asset information from Qualys into the ServiceNow CMDB.