Service Description

IBM Vulnerability Management Service

1. Service Overview

IBM Vulnerability Management Service (called "VMS") is designed to provide a comprehensive, Web-driven vulnerability management program that provides visibility into potential exposure areas within a distributed network environment.

The details of your order (e.g., the services you require, contract period, and charges) will be specified in the Order.

Definitions of service-specific terminology can be found at www.ibm.com/services/iss/wwcontracts

VMS has been designed to help provide you with the tools and capabilities required to implement an effective vulnerability management program. The service may be delivered as either an external or an internal solution. If delivered as an external solution, scanning will be provided which originates at the SOC. If delivered as an internal solution, a scanning agent (called "Agent") will be deployed into the Customer's internal network to provide vulnerability management of internal Hosts which may not be directly accessible by Hosts outside of the Customer's network.

The following features and capabilities are provided as part of the service.

a. Web-driven interface for scan scheduling, review, and reporting;

b. internal and external scanning;

c. accurate and detailed vulnerability results;

d. comprehensive lifecycle-based approach toward vulnerability management;

e. customizable views and dynamic access to vulnerability data;

f. ability to track individual assets, device criticality, and assignment of owners;

g. comprehensive tool-set for workflow management and remediation tracking;

h. productivity tracking of those responsible for vulnerability remediation; and

i. access to research needed to quickly identify effective remediation steps.

The IBM approach to vulnerability management includes six key components.

j. vulnerability discovery - provides a Web-driven interface that allows Customers to schedule and launch either internal or external scans of assets within their individual environments;

k. prioritization - catalogs each scanned device (i.e., asset) and allows Customers to assign business criticality ratings and match system owners to specific assets. Asset owners are notified when vulnerabilities are discovered, and are provided with a personalized view into overall program impacts on their security posture;

l. remediation – helps to identify vulnerabilities and assigns them to designated asset owners for review and remediation. Individual asset owners can use the Virtual-SOC to learn about a specific vulnerability and track its remediation within the enterprise. The service provides a detailed workflow, with visual queues and notifications to guide asset owners;

m. dynamic protection – integrates VMS with a Customer's existing IBM Managed Security Services (as applicable) to dynamically update server and network Intrusion Prevention policies with appropriate blocking responses. This capability enhances vulnerability management to provide vulnerability protection;

n. verification – permit the assignment to remain active until VMS verifies the patch has been effectively implemented and all attack vectors for a given vulnerability have been successfully eliminated; and

o. customized reporting - provides a results-oriented view of service performance and security posture.

The following table provides an overview of VMS service features.

Table 1 - Service Features

Service Features	External Scanning	Internal Scanning

Ideal for:	Identifying vulnerabilities within the network perimeter	Identifying vulnerabilities across the enterprise
Organization size	Any	Any
Number of available scans	Based on number of Internet protocols ("IPs") and frequency purchased	Unlimited scans of a specified set of IPs – within the constraints of the platform
Hardware platform required	No	Yes
Available policies	16	16
Scans external IPs	Yes	Yes
Scans internal IPs	No	Yes
Ranking of discovered assets	Yes	
Assignment of administrators to discovered assets	Yes	
Assign vulnerabilities for remediation	Yes	
Dynamic IBM Virtual Patch® technology	Yes	
Full vulnerability remediation workflow	Yes	
Historical trending of vulnerability data	Yes	
Industry and vertical comparisons	Yes	
Verification of resolved vulnerabilities	Yes	
Integration with IBM Managed Security Services and IBM Managed Protection Services	Yes	

2. IBM Responsibilities

2.1 Deployment and Initiation

During deployment and initiation of internal VMS, IBM will either work with the Customer to deploy a new internal scanning Agent or begin management of an existing Agent.

For external VMS, IBM will work with the Customer to enable scanning of their externally facing Hosts.

2.1.1 Project Kickoff

IBM will send the Customer a welcome e-mail and conduct a kickoff call to:

- introduce the Customer contacts to the assigned IBM deployment specialist;
- set expectations; and
- begin to assess the Customer requirements and environment, if an internal scanning Agent will be deployed.

To enable deployment of internal VMS, IBM will provide a document called "Network Access Requirements", detailing how IBM will connect remotely to the Customer's network, and any specific technical requirements to enable such access. Typically, IBM will connect via standard access methods through the Internet; however, a site-to-site VPN may be used, if appropriate.

External VMS requires only a short deployment session between the Customer and the IBM deployment specialist.

2.1.2 Assessment

Data Gathering

IBM will work with the Customer to help configure the Customer's profile within the Virtual-SOC. This configuration may include setup of accounts and valid IP addresses that may be scanned.

Environment Assessment

This section applies only to Customers who have purchased the internal scanning option of VMS.

Using the provided information, IBM will work with the Customer to understand the existing Customer environment, and build a configuration for the Agent. During this assessment, IBM may make recommendations to adjust the layout of the network to improve scanning capability or otherwise enhance security.

Existing Agent Assessment

This section applies only to Customers who have purchased the internal scanning option of VMS.

If IBM will be taking over management of an existing Agent, IBM must assess the Agent to be sure it meets certain specifications. IBM may require the Agent software or Security Content to be reinstalled, or upgraded to the most current versions in order to provide the service. Other required criteria may include the addition or removal of applications and user accounts.

2.1.3 Implementation

This section applies only to Customers who have purchased the internal scanning option of VMS.

Configuration at IBM

For Agents purchased through IBM at the time of deployment, much of the configuration and policy setting will take place at IBM facilities. For existing Agents already in use, the Customer will have the option to ship the Agent to IBM for configuration at IBM facilities.

Installation

While physical installation and cabling are a Customer responsibility, IBM will provide live support, via phone and e-mail, and will assist the Customer with location of vendor documents detailing the installation procedure for the Agent. Such support must be scheduled in advance to ensure availability of a deployment specialist.

At the Customer's request, physical installation may be provided by IBM Professional Security Services ("PSS") for an additional fee.

Remote Configuration

When taking over management of an existing Agent, IBM will typically perform the configuration remotely. The Customer may be required to physically load media.

All managed Agents will require some remote configuration, which may include the registration of the Agent with IBM Managed Security Services infrastructure.

2.1.4 Transition to SOC

Once the Agent is configured, physically installed and implemented, and connected to the IBM Managed Security Services infrastructure, IBM will provide the Customer with the option of having a demonstration of the Virtual-SOC capabilities and performance of common tasks.

The final step of services deployment is when the Security Operations Center ("SOC") takes over management and support of the Agent and the relationship with the Customer. At this time, the ongoing management and support phase of the services officially begins. Typically, IBM will introduce the Customer via phone to the SOC personnel.

2.2 Ongoing Management and Support

2.2.1 Vulnerability Management

VMS is an electronic service that regularly and automatically scans Customer devices for known vulnerabilities. Each scan results in comprehensive reports that are designed to identify potential weaknesses, assess relative network risk, and provide recommendations to manage identified vulnerabilities.

External VMS consists of remotely delivered scans which originate from IBM facilities. IBM will require the Customer to validate they are the owner of the IP address range to be scanned, prior to the initial scan of such IP address range being performed. Using this configuration, IBM can only scan static IP addresses belonging to the Customer that are publicly routable.

Internal VMS provides all the benefits of vulnerability management, but is delivered by an Agent deployed inside the Customer's internal network. IBM will provide a licensed copy of IBM Internet Scanner® software for the duration of the internal VMS contract.

2.2.2 Virtual-SOC

The Virtual-SOC is a Web-based interface designed to enable delivery of key service details and on-demand protection solutions. The Virtual-SOC is structured to deliver a consolidated view of the Customer's overall security posture. The portal is capable of merging data from multiple geographies or technologies into a common interface, allowing for comprehensive analysis, alerting, remediation, and reporting.

The Virtual-SOC provides real-time access for communications including ticket creation, security event handling, incident response, data presentation, report generation, and trend analysis.

Reporting

VMS is designed to provide reports that focus on the status of vulnerabilities within your enterprise, protection measures employed, security activities, security scorecard, subordinate activities and service summaries. Many of the available reports can be generated using customizable data sets and user-defined reporting periods with varying views.

Users of the System

The service is designed to help organizations manage vulnerability exposures across the enterprise by providing multiple individuals, from different levels within the organization, with varying levels of access to the system.

a. Authorized Security Contacts

   Users classified as Customer security contacts will be the primary users of VMS and will have full access to the system including the ability to execute scans, generate reports, assign vulnerabilities for remediation, and apply virtual patches. IBM SOC analysts will only accept phone calls from authorized Customer security contacts. Customers may identify up to three authorized security contacts for VMS.

b. Subordinates/System Administrators

   Users classified at this level will receive limited access to the VMS system. Subordinates/system administrators are identified by authorized Customer security contacts, and are then assigned specific devices for which they may have access. Vulnerabilities can then be assigned to these individuals for remediation once identified during the discovery process. Subsequently, subordinates/system administrators may login to the system, review and research assigned vulnerabilities and document any remediation efforts. Users at this level do not have the authority to review data or make changes outside of devices assigned directly to them. Customers may identify an unlimited number of subordinates/system administrators for the VMS service (within the constraints of the platform).

c. Manager/Read Only

   This level of access provides managers, and those with executive oversight, full access to the VMS and its reporting components, but does not allow them to make changes to any configurations, scheduled scans, or vulnerability assignments. This profile is designed for non-technical program stakeholders.

Dashboard

In addition to vulnerabilities, VMS provides an overview "at a glance" (called "Dashboard") to deliver a snapshot of the Customer's state of security as it relates to vulnerabilities. The Dashboard provides administrators with a comprehensive overview of the threat level, current scan results, pending scan jobs, top vulnerable Hosts (i.e., assets) and other information relevant to the Customer's vulnerability management program. The Dashboard provides a single view of current program status and serves as a launch pad to other VMS features, including:

- scan scheduling;
- asset inventories;
- virtual patch application;
- customized reporting;

- security activity logs; and
- service configuration.

Authorized Customer security contacts will have access to the entire Dashboard and all service features and functionality. Other Customer users (e.g., system administrators) will receive a more focused view that outlines vulnerabilities or assets to which they have been assigned.

2.2.3 Scanning

VMS identifies network assets (e.g., servers and network devices), recording and cataloging each item, and building an association between assets and their respective vulnerabilities. VMS provides a Web-driven interface that controls scan initiation, identification of assets to be scanned, and types of scans to be conducted. After a scan is completed, electronic notifications will be delivered to the authorized Customer security contacts informing them that results are pending review.

VMS provides the Customer with two distinct types of scanning which can be employed together or separately:

External Scanning

External scanning provides the Customer with a potential hacker's view of the network perimeter and is designed to highlight those risk exposures open to the general Internet community. External scans will identify and assess only devices with routable IP addresses. Non-routable IP addresses behind closed firewalls will not be scanned. Scans are scheduled through the Virtual-SOC and launched from the IBM secure data center environment. External scans do not require CPE, setup, or hardware/software investment. External scanning is delivered based on the number of IPs and the frequency of scanning.

External scanning is purchased based on the number of IPs to be scanned over a given period of time. The Customer may purchase any number of IPs to be scanned on a weekly, monthly or quarterly basis. Each scan will subtract from the available pool of IPs regardless of whether the same or unique systems are being assessed during each scan. Available IPs will automatically refresh, based on the purchased frequency. IPs which are unused at the close of the allotted time period will be forfeited.

Internal Scanning

Internal scanning helps to allow the Customer to accurately assess the state of vulnerabilities within their enterprise. This type of assessment is important as a large percentage of network-based attacks (e.g., mass-propagating worms) often originate unknowingly from inside a protected or private network. Internal scans can be launched from a scanning Agent located at the Customer's premises and require the Customer to provide the appropriate hardware and operating system. An unlimited number of scans may be launched from the internal scanning Agent, based on the size of the environment and the number of IPs purchased. Internal scanning Agents can process up to 10,000 unique IPs per device.

When both scanning types are used together, they help the Customer delineate which vulnerabilities are identifiable only from the outside, only from the inside, or from both locations. This information can help the Customer prioritize the vulnerabilities to be addressed.

2.2.4 Scan Policies

To provide flexibility for each scheduled scan, a total of 16 different policies are available for both internal and external scanning. These 16 policies allow the Customer to assess vulnerabilities and exposures that exist across a variety of device types with varying degrees of intrusiveness. An example of such a policy is one tailored specifically for conducting assessment scans, to identify vulnerabilities on assets such as servers, desktops, routers, and switches.

2.2.5 Scheduling of Scans

Scan scheduling can be accomplished 24 hours/day by 7 days/week through the Virtual-SOC. You may schedule a scan by providing the following parameters:

- scan name – a brief alias for the scan;
- scan date and time – scans can be executed each hour;
- scan retry interval – number of hours before a failed scan starts again;
- policy – any of the outlined policies can be selected; and
- scan target – a predefined target range of IPs or a user-specific range.

Pending scans will be displayed directly on the Dashboard, and scans may be canceled using the "Cancel a Scan" option from the Dashboard interface. Scans may be canceled at any time prior to their scheduled start date, and no penalties will apply.

2.2.6 Scan Results

Scan results are available immediately following the successful completion of a scheduled scan. Results of each separate scan can be viewed independently through the "Scan History" option of the Dashboard. Cumulative changes in asset inventories and discovered vulnerabilities can be reviewed through their respective sections of the VMS system.

This distributed manner of archiving and storing scan data allows authorized Customer security contacts to quickly review the results of a single scan, while also reviewing the overall state of assets and their respective vulnerabilities across the enterprise. Scan results typically include some or all of the following information:

- discovered assets (IPs);
- available services;
- available ports;
- banner information;
- operating systems identified; and
- vulnerabilities with associated severity.

2.2.7 Asset Identification and Grouping

As indicated above, discovered assets will be automatically identified and cataloged into VMS. Authorized Customer security contacts will have the option to create logical groupings into which assets may be placed (e.g., Web server farm, enterprise resource planning ("ERP") systems, and routers). Assets may exist within an unlimited number of groups to ensure that systems serving multiple functions can be organized accordingly. These groups can be used as scan targets and report datasets.

Some systems have multiple IP addresses, or are referenced using a dedicated, private IP or a translated routable IP. For organizations with such systems and configurations, VMS will establish relational linkages between assets and multiple IP addresses to help ensure multiple assets are not created for devices that might be referenced by more than one IP. Linkages can be established by authorized Customer security contacts within the VMS configuration.

2.3 Prioritization and Vulnerability Assignment

One of the challenges of vulnerability management is properly prioritizing which vulnerabilities should be remediated first, and tracking and recording the prioritization. VMS automatically sorts and displays vulnerable systems based on the severity of identified vulnerabilities and the business criticality of the impacted assets. The available information makes prioritizing vulnerabilities more manageable. Vulnerabilities can be assigned electronically to the appropriate subordinate/system administrator for remediation.

2.3.1 Asset Criticality

VMS provides authorized Customer security contacts with the ability to assign a numeric business criticality ranking to each discovered asset. Rankings can be assigned to single or multiple assets at one time. Assigning a criticality ranking to each discovered asset allows prioritization for which vulnerabilities should be remediated first. Business criticality ratings will be stored in the VMS system and can be modified by authorized Customer security contacts at any time.

2.3.2 Assigning Vulnerabilities for Remediation

VMS allows the Customer to track and distribute workload by assigning vulnerabilities directly to those responsible for fixing them. Authorized Customer security contacts can define subordinate/system administrators in the system. Defining these individuals will automatically create the appropriate logins and electronically notify the user they have been added to the system. This provides subordinate/system administrators the ability to log directly into the system to receive assigned workload (vulnerabilities). If user maintenance is required, an authorized Customer security contact will have the authority to modify login credentials, and add or delete accounts.

After the appropriate users have been entered into the system, they can be assigned directly to discovered assets for which they hold remediation responsibility. As vulnerabilities are discovered,

having system administrators associated with specific assets will help to speed the vulnerability assignment process.

2.3.3 Tracking Assigned Vulnerabilities

Using the Dashboard, authorized Customer security contacts can review a summary of system administrators and their assigned vulnerabilities. For additional details regarding current assignments and historical trending, authorized Customer security contacts may also visit the "View and Assign Vulnerabilities" section of the VMS system. A variety of reporting options is available to allow authorized Customer security contacts to generate reports on subordinate/system administrator activity. These reports can help identify which individuals have been most productive and where additional effort may be required.

2.4 Dynamic Virtual Patching

By combining VMS with the IBM Proventia® Network Intrusion Prevention System ("IPS"), VMS can provide you with dynamic virtual patching capabilities. Authorized Customer security contacts can configure their service implementation to automatically or selectively request the deployment of virtual patches to Proventia Intrusion Prevention devices on networks and servers. Virtual patching helps protect vulnerable systems from attack while system administrators are applying vendor-supplied patches.

Virtual patching capabilities are supported on Proventia IPS Appliances and RealSecure® Server software. For virtual patching to occur, the Intrusion Prevention devices must be under full management by IBM Managed Security Services which are available for an additional fee. Virtual patching of unmanaged or third party Intrusion Prevention technology is not supported.

2.5 Vulnerability Remediation

When subordinate/system administrators have been electronically notified of vulnerability assignments, these individuals will be prompted to log directly into the Virtual-SOC to review their assigned workload. Following review, users may begin researching and documenting efforts as they work towards a resolution. As progress is made, authorized Customer security contacts can follow along using the real-time review capabilities provided through the Virtual-SOC. Significant changes in vulnerability status will result in an electronic push of information to the authorized Customer security contacts.

2.5.1 Reviewing/Researching Vulnerabilities

As subordinate/system administrators login to the Virtual-SOC, they will be provided with a detailed list of vulnerabilities pending review. The vulnerabilities can be reviewed in detail, including asset properties, vulnerability severity, description, impacts and required remediation steps.

VMS provides the user with information required to understand specific vulnerabilities and appropriate remediation steps. Extensive reading and outside research is not required to formulate a plan for resolving a specific issue.

2.5.2 Remediation Workflow

VMS provides you with a workflow designed to guide you through the remediation process. Each discovered vulnerability is designated a security lifecycle graphic that updates in real-time as remediation progress is completed. Using this tool, a subordinate/system administrator will be provided with the next step to resolve a specific vulnerability.

The workflow is primarily driven by the status of the vulnerability. Such status indicates where a given vulnerability resides in the remediation lifecycle, at a given point in time. For example, the following status may be used during the remediation process:

- not assigned – initial status, set automatically following discovery of a vulnerability;
- ignored – indicates a given vulnerability should be ignored for the time being. This status is set manually and is not recommended;
- notified – indicates a vulnerability has been assigned for remediation. This status is set automatically;
- reviewed –indicates the system administrator has reviewed the vulnerability. This status is set automatically;
- pending – indicates the vulnerability has been reviewed and the remediation is in progress. This item is set manually.

- resolved pending confirmation – indicates the vulnerability is believed to be resolved and a follow-up scan is necessary to confirm. This status is set manually; and
- resolved – indicates the vulnerability has been confirmed to no longer exist. This status is set automatically following a verification scan.

The above status indicators are provided for example purposes only. Actual status indicators in the service may be modified based on your feedback or technical necessity.

Vulnerability remediation typically requires disabling vulnerable services or applying software patches. Because it may be difficult to determine if a patch was applied successfully, or if a given vulnerability was resolved, VMS does not allow users to set a vulnerability status to "resolved". Rather, VMS allows users to set status to "resolved pending confirmation". Vulnerabilities will remain in this status until a follow-up scan is launched and the vulnerability is confirmed to no longer exist. At this point, the system will automatically set the vulnerability to "resolved".

2.5.3 Managed Security and Protection Services Integration

VMS provides additional capability when used in conjunction with other IBM Managed Security Services. This combination helps blend the gathered data to provide a comprehensive view of vulnerabilities as they relate to Security Incidents and escalations under the IBM Managed Intrusion Detection Service and IBM Managed Protection Services.

2.5.4 Management of Scanning Agents

If Agent licenses are provided as part internal scanning of the VMS implementation, IBM will provide full management of the Agents. Management of the Agents will be facilitated through the use of Windows Terminal Services with encryption enabled. Under this configuration, IBM will retain sole administrator level access to the device. Any and all changes to the scanning application or underlying operating system will be the sole responsibility of IBM security operations analysts.

The Customer may perform management of internal scanning Agents provided the Customer owns or purchases an applicable license for the Agent. The Customer must receive approval from IBM prior to making any changes to the Agent or the operating system. If approval is not received, IBM will not be held responsible for service failures related to improper scanning Agent functionality.

Health and Availability Monitoring

The health and performance of VMS is monitored by using a Host-based monitoring Agent (when possible) or SNMP. The devices are regularly polled by the SOC, keeping IBM security analysts informed of some potential problems as they develop. Key metrics analyzed by the monitoring Agent include:

- hard disk capacity (if applicable);
- CPU utilization;
- memory utilization; and
- process availability.

In addition to system health metrics, IBM will monitor device availability. If contact with a managed device is lost, additional time-based checks will be initiated to verify a valid outage has been identified.

In the event system health problems or an outage has been confirmed, a trouble ticket will be created and an IBM security analyst will be notified to begin research and investigation. The status of all system health tickets is available through the Virtual-SOC.

Outage Notification

If the Agent is not reachable through standard in-band means, the Customer will be notified via telephone using a predetermined escalation procedure. Following telephone escalation, IBM will begin investigating problems related to the configuration or functionality of the managed device.

Application Updates

Periodically, it will be necessary for IBM to install patches and software updates to improve device performance, enable additional functionality, and resolve potential application problems. The application of such patches and updates may require platform downtime or Customer assistance to complete. If required, IBM will declare a maintenance window in advance of any such updates, and the notification will clearly state the impacts of the scheduled maintenance and any Customer-specific requirements.

Security Content Updates

To help ensure that the most current threats are properly identified, IBM will update security platforms with the most current Security Content. Such Security Content, delivered in the form of new checks or signatures for the vulnerability scanner, enhances the Agent's detection capabilities.

At the discretion of IBM, Security Content updates may be downloaded and installed onto the security platform at any time. Such an operation is transparent to users.

Scanning Agent Troubleshooting

If a scanning Agent does not perform as expected, or is identified as the potential source of a network or server-related problem, IBM will examine the Agent configuration and functionality for potential issues. Troubleshooting may consist of an offline analysis by IBM, or an active troubleshooting session between IBM and the Customer. IBM will attempt to resolve any technical issues as expediently as feasible. If the Agent is eliminated as the source of a given problem, no further troubleshooting will be performed by IBM.

Data Retention and Restoration

During the course of service delivery, the scanning Agent will generate a large amount of data related to discovered vulnerabilities within the customer environment. This data will be stored within the Virtual-SOC and will remain accessible online for a period of one year from the time the data enters the system.

Following display on the Virtual-SOC, logs are migrated to a physical backup media such as tape or DVD. Backup media is archived in a secure, environmentally controlled facility. Archived data will be available for up to seven years from the date of log creation.

At the Customer's request, IBM will submit a request for media location and retrieval. Hourly consulting fees will apply for all time spent restoring and preparing data in the Customer's requested format.

All specified retention times assume an active VMS contract has been maintained for each unique event / log source. Cancellation of the service for a given event/log source, or cancellation of VMS will require IBM to delete all collected data from the affected event/log sources.

3. Customer Responsibilities

While IBM will work with internal scanning Customers to deploy and implement the Agent, and IBM will manage the Agent, the Customer will be required to work with IBM in good faith and assist IBM in certain situations as requested by IBM.

3.1 Deployment and Initiation

During deployment, the Customer will work with IBM to deploy a new Agent or begin management of an existing Agent, as applicable.

The Customer will be required to provide and validate ownership of any IP address ranges to be scanned and must work with IBM in good faith to accurately assess the Customer's network and environment. The Customer must provide contacts within the organization, and specify an escalation path through the organization in the event that IBM must contact the Customer.

The Customer must ensure that any existing Agent meets IBM specifications, and must work to meet recommendations concerning the Customer's network and network access requirements, if changes are required to ensure workable protection strategies.

If IBM will be taking over management of an existing Agent, IBM may require the Agent software or Security Content to be reinstalled or upgraded to the most current versions in order to provide the service. Other required criteria may include the addition or removal of applications and user accounts. Such upgrades, additions, or removals will be the sole responsibility of the Customer.

The Customer will work with IBM in good faith to bring internal scanning Agents "live" within committed timeframes.

The Customer is responsible for assisting IBM in gaining remote access to the internal scanning Agent by configuring terminal services, as requested by the IBM deployment specialist.

3.2 Ongoing Management and Support

3.2.1 Configuration / Change Management

The Customer acknowledges that IBM is the sole party authorized to make direct system changes to the Agent when such Agent is managed by IBM.

The Customer agrees to work in good faith to allow IBM to upgrade internal scanning Agents as new releases of the Internet scanner application become available.

The Customer is required to provide advance notice of any scheduled system reboots, maintenance, or power tests that may result in temporary inaccessibility of the internal scanning Agent.

In the case of hardware or OS failure of the internal scanning Agent, the Customer is responsible for all activities associated with resolution of the failure.

The Customer may be required to assist in patching or upgrading of the internal scanning Agent application.

3.2.2 Server Environment / Requirements

Servers with the internal scanning Agent installed must meet the most current application minimum system requirements as outlined in the vendor's product documentation.

The Customer is responsible for taking appropriate measures to ensure the network in which the internal scanning Agent is installed is secure, using firewall configurations and following appropriate security practices.

The Customer must provide a secure, physically controlled environment for servers on which the internal scanning Agent resides.

The Customer will ensure that access control points within their respective networks allow scanning Agents to pass traffic through them in order to properly assess for vulnerabilities.

The Customer will ensure the internal scanning Agent is Internet-accessible via a static IP address.

3.2.3 Software Maintenance

The Customer is responsible for ensuring that valid support and maintenance are maintained for any client provided instances of Internet scanner and for any hardware platforms on which the application resides.

4. Service Level Agreements

IBM SLAs establish response time objectives and countermeasures for Security Incidents resulting from VMS. The SLAs become effective when the deployment process has been completed, the device has been set to "live", and support and management of the device have been successfully transitioned to the SOC.

The SLA remedies are available provided the Customer meets its obligations as defined in this Service Description.

4.1 SLA Guarantees

The SLA guarantees described below comprise the measured metrics for delivery of VMS. Unless explicitly stated below, no additional guarantees or warranties of any kind shall apply to services delivered under VMS. The remedies for failure to meet the SLA guarantees are specified in the section entitled "SLA Remedies", below.

a. Vulnerability scanning execution guarantee – IBM will begin execution of a scheduled vulnerability assessment within one hour (plus or minus) of the time scheduled by the Customer (or by IBM on behalf of the Customer) and all scans will be completed without failure. This guarantee applies only to correctly configured scan requests, for devices and networks covered by a current subscription to VMS.

b. Virtual Patch application guarantee – IBM will implement Virtual Patch requests, received through the Virtual-SOC, within two hours of the request being entered into the system. This guarantee is based on actual time of implementation; not on the time the Customer was notified that the request was completed. This guarantee is only applicable when the requested implementation applies to a valid managed Intrusion Prevention technology under a current subscription for IBM Managed Security Services.

c. Proactive system monitoring guarantee - the Customer will be notified within 15 minutes after IBM determines the Customer's managed internal scanning Agent is unreachable via standard in-band connectivity.

d. Proactive Security Content update guarantee – IBM will apply all new Security Content updates to the Customer's managed security platform within 72 hours from the time the Security Content update was published for general availability by the vendor.

SLA	External Scanning	Internal Scanning
Vulnerability scanning execution guarantee	Available	Available
Virtual Patch application guarantee	Available	Available
Proactive system monitoring guarantee	Not available	Available
Proactive Security Content update guarantee	Not available	Available

4.2 SLA Remedies

As the sole remedy for failure to meet any of the guarantees described in the section entitled "SLA Guarantees", IBM will credit the Customer's account if IBM fails to meet the SLA guarantees described in the section entitled "SLA Guarantees" during any given calendar month. For all SLAs, the Customer may obtain no more than one credit for each SLA per day, not to exceed a total for all SLAs of $25,000 (U.S.), or the equivalent in local currency, in a given calendar month, as stated in the section entitled "SLA Exclusions and Stipulations" below. Specific SLA remedies are listed below:

a. Vulnerability scanning execution remedy – if IBM fails to meet this guarantee, the Customer account will be credited as follows:

   (1) External scans – one additional (i.e., in addition to the original) scheduled scan of equal or lesser value, at no charge; or

   (2) Internal scans – one day of the total invoiced VMS monthly fee.

b. Virtual patch application remedy – if IBM fails to meet this guarantee, the Customer account will be credited for one day of the total VMS monthly fee.

c. Proactive system monitoring and proactive Security Content update remedies - if IBM fails to meet either of these guarantees, the Customer account will be credited for one day of the total VMS monthly fee.

Table 3 - SLAs and Remedies Summary

	Remedies for VMS	
Service Level Agreements	**External Scans**	**Internal Scans**
Vulnerability scanning execution guarantee	Credit of 1 additional scan, or 1 day of the monthly fee for VMS, as applicable.	Credit of 1 day of the monthly fee for VMS
Virtual Patch application guarantee	Credit of 1 day of the monthly fee for VMS	
Proactive system monitoring guarantee	Not available	
Proactive Security Content update guarantee	Not available	

4.3 SLA Exclusions and Stipulations

4.3.1 Customer Contact Information

Multiple SLAs require IBM to provide notification to the designated Customer contact after certain events occur. In the case of such an event, the Customer is solely responsible for providing IBM with accurate and current contact information for the designated contact(s). The current contact information on record is available to authorized contacts through the Virtual-SOC. IBM will be relieved of its obligations under these SLAs if IBM contact information is out of date or inaccurate due to Customer action or omission.

4.3.2 Customer Network/Server Change Notifications

The Customer is responsible for providing IBM advance notice regarding any network or server changes to the firewall environment. If the event advance notice cannot be provided, the Customer is required to provide IBM with notification of changes within seven calendar days of said network or server changes. Notification is completed by the submission or update of a critical server ticket through the Virtual-SOC. If the Customer fails to notify IBM as stated above, all SLA remedies are considered null and void.

4.3.3 Maximum Penalties/Remedies Payable to Customer

The total SLA credits (called "remedies") provided by VMS, described in the sections entitled "SLA Guarantees" and "SLA Remedies" above, will not exceed the service fees for one calendar month.

4.3.4 Network Traffic Applicable to SLAs

Certain SLAs focus on the prevention, identification and escalation of Security Incidents. These SLAs assume that traffic has successfully reached the firewall and therefore the firewall has the ability to process the traffic against the installed policy and generate a logged event. Traffic that does not logically or electronically pass through a firewall, or that does not generate a logged event, is not covered under these SLAs.

4.3.5 SLA Compliance and Reporting

SLA compliance and the associated remedies are based on fully functional network environments, Internet and circuit connectivity, firewalls, and properly configured servers. If SLA compliance failure is caused by CPE hardware or software (including any and all Agents), all SLA remedies are considered null and void. IBM will provide SLA compliance reporting through the Virtual-SOC.

4.3.6 Testing of Monitoring and Response Capabilities

The Customer may test IBM monitoring and response capabilities by staging simulated or actual reconnaissance activity, system or network attacks, and/or system compromises. These activities may be initiated directly by the Customer or by a contracted third party with no advance notice to IBM. SLAs will not apply during the period of such staged activities, and remedies will not be payable if the associated guarantee(s) are not met.

5. Service Level Objectives

IBM service level objectives (called "SLOs") establish nonbinding objectives for the provision of certain features of MPS for Networks – Select. The SLOs become effective when the deployment process has been completed, the device has been set to "live", and support and management of the device have been successfully transitioned to the SOC. IBM reserves the right to modify these SLOs with 30 days prior written notice.

a. Virtual-SOC – IBM will provide a 99.9% accessibility objective for the Virtual-SOC outside of the times detailed in the section entitled "Scheduled and Emergency Portal Maintenance".

b. Internet Emergency – In the event IBM declares an Internet emergency, it is IBM's objective to notify the Customer's specified points of contact via e-mail within 15 minutes of emergency declaration. This notification will include an incident tracking number, telephone bridge number, and the time that IBM will conduct a situation briefing.

   During declared Internet emergencies, IBM will provide a live telephone-conference situation briefing and summarized e-mail designed to provide information that the Customer can use to protect their organization. Situation briefings following the onset of an Internet emergency will supersede any requirement for IBM to provide Customer-specific escalations for events directly related to the declared Internet emergency. IBM will communicate all other priority level incidents, during an Internet emergency, via automated systems such as e-mail, pager and voice mail.

   Standard escalation practices will resume upon conclusion of the stated Internet emergency. Termination of an emergency state is marked by a decrease in the AlertCon level to AlertCon 2, or an e-mail notification delivered to an authorized Customer security contact.

6. Other Terms and Conditions

IBM reserves the right to modify the terms of this Service Description, including the SLAs, with 30 days prior written notice.