

Service Description

Managed Protection Services for Networks - Standard

1. Scope of Services

IBM Managed Protection Services for Networks – Standard (called “MPS for Networks – Standard” or “Service”) is designed to provide a comprehensive solution for network monitoring and a high level of security protection from external and internal threats.

The Service provides managed, inline protection of network segments using one of the Proventia MX appliances (called “Agents”). The Proventia MX is an all-in-one appliance which includes a wide range of common security functions.

The details of Customer’s order (for example, the services requested, contract period, and charges) will be specified in an Order.

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

IBM will support the following product features, as applicable:

- a. Intrusion Detection and Intrusion Prevention Systems (called “IDS/IPS”)
IDS/IPS is a security management system for computers and networks that is designed to gather and analyze information from various areas within a computer or a network, to help identify and block possible security breaches (i.e., intrusions (attacks from outside the organization) and misuse (attacks from within the organization)).
- b. firewall
A firewall is an appliance that is designed to allow or deny access requests based on a set security policy, and provides routing capabilities to direct network traffic. Many firewalls include a full set of networking features (for example, address and port rewriting).
- c. Virtual Private Networks (“VPNs”)
A VPN utilizes public telecommunications networks to conduct private data communications using encryption. Most implementations use the Internet as the public infrastructure and a variety of specialized protocols to support private communications through the Internet.
- d. antispam
Antispam technology is designed to minimize the volume of spam e-mail to user mail boxes. Spam filters utilize spam signatures, detection algorithms, and heuristic analysis to reduce the volume of unwanted e-mail and help remove objectionable content.
- e. Web filtering
Web filtering helps the Customer to block objectionable content, mitigate Web-borne threats, and govern Web viewing behavior of personnel behind the managed Agent.
- f. antivirus
Gateway antivirus systems scan many kinds of file transfers (such as Web pages, e-mail traffic, and file transfer protocol (“FTP”) exchanges) for worms, viruses, and other forms of malware.
- g. high availability
To help protect against hardware failure and provide high availability, two Agents may be configured and deployed; one fully operational and the other waiting as a backup to take over should the first Agent fail. Some Agents can also be deployed as clusters, such that one Agent is active and the other Agent is in passive mode.

MPS for Networks – Standard will provide the following services in support of the product features listed above:

- h. project kickoff, assessment, and implementation
During deployment of the Service, IBM will work with Customer to help define appropriate security policies, assist with installation and configuration of the Agent(s), and verify proper device operation prior to transition of the Agent(s) to the Security Operations Center (“SOC”).

- i. policy management
Agents only protect Hosts when configured correctly for their network environment. IBM provides policy management services to help the Customer keep Agents configured with a valid security policy, and retain records of all changes.
- j. device management
IBM will maintain the Agent by monitoring availability and applying vendor updates to the Agent.
- k. vulnerability management
Vulnerabilities are weaknesses in Hosts in the Customer's environment. IBM will provide vulnerability management services to help identify and remediate such vulnerabilities.
- l. IBM Internet Security Systems™ X-Force® Threat Analysis Service
IBM will provide security intelligence to the Customer based on such things as original research completed by the IBM X-Force research and development team, worldwide threat activity as identified by the IBM Global Threat Operations Center, and secondary research from other public and private resources.
- m. Virtual-SOC
The Virtual-SOC is a Web interface which serves as the Customer's interface to management of the Agent, alerts, logs, reports, policy change requests, and other types of service tickets.

The following table provides an overview of MPS for Networks - Standard product features.

Table 1 - Product Features

Product Features	Proventia MX 100x	Proventia MX 300x	Proventia MX 50xx
Supported users	5 – 50	50 – 250	250 – 500
IDS/IPS	Support for help in blocking attacks in X-Force Certified Attack List, and alerting of high-, medium-, and low-severity incidents		
Firewall	Custom firewall policy		
VPN:	Support for site-to-site, client and SSL VPNs		
Antispam	Filtering, tagging, and deletion of Web-based spam content		
Web filtering	Web filtering with support for filter override, site blacklisting and source white listing		
Antivirus	Virus protection; reports and notification through the Virtual-SOC		
High availability	Support for active/active or active/passive Agents		
Out-of-Band ("OOB")	Optional		

The following table provides an overview of MPS for Networks - Standard services provided in support of the product features listed above.

Table 2 - Services

Services	Proventia MX 100x	Proventia MX 300x	Proventia MX 50xx
Project kickoff, assessment, and implementation	Included		
Policy management	By IBM only; 2 policy change requests per month	By IBM only; 4 policy change requests per month	By IBM only; 6 policy change requests per month

Device management	24x7 device health and availability monitoring, and maintenance of Agent software and Security Content
Vulnerability management	Quarterly scan of 5 IPs
X-Force Threat Analysis Service	1 seat for the X-Force Threat Analysis Service security intelligence service for each authorized security contact
Virtual-SOC	Provides real-time access for communications

2. IBM Responsibilities

2.1 Deployment and Initiation

During deployment, IBM will either work with Customer to deploy a new Agent or begin management of an existing Agent. Only Proventia MX Agents can be managed as part of the Service.

2.1.1 Project Kickoff

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

- introduce Customer contacts to the assigned IBM deployment specialist;
- review IBM and Customer responsibilities; and
- begin to assess Customer requirements and environment.

IBM will provide a document called “Network Access Requirements”, detailing how IBM will connect remotely to 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.

2.1.2 Assessment

Data Gathering

IBM will provide a form for Customer to document detailed information for the initial setup of the Agent and associated Service features. Most of the questions will be technical in nature and help determine the layout of Customer network, Hosts on the network, and desired security policies. A portion of the requested data will reflect Customer organization, and will include security contacts and escalation paths.

Environment Assessment

Using the provided information, IBM will work with Customer to understand the existing Customer environment, and build a configuration and security policy for the Agent. If migrating from an existing Agent to a newer Agent, IBM will use the configuration and policy on the existing Agent. In each case, IBM may recommend policy adjustments in response to the most active worldwide threats (as determined by the IBM Global Threat Operations Center), and may tune the policy to reduce the number of erroneous alarms, if required.

During this assessment, IBM may make recommendations to adjust the policy of the Agent or the layout of the network to enhance security. If an Agent does not include firewall capabilities, or is implemented with firewall capabilities disabled, IBM recommends that the Agent be deployed behind a firewall. Placement outside the firewall may require policy tuning to eliminate high volumes of false alarms and may limit IBM’s ability to implement certain protection strategies.

If Customer chooses to deploy the Agent in a passive mode, the protection provided by the Agent and associated service level agreements (“SLAs”) will be substantially decreased. Should Customer choose to transition to an inline deployment at a later date, this transition will require advance notice due to the extra effort that will be required.

Existing Agent Assessment

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 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

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, Customer will have the option to ship the Agent to IBM for configuration at IBM facilities.

Installation

While physical installation and cabling are Customer's responsibility, IBM will provide live support, via phone and e-mail, and will assist 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 Customer's request and for an additional fee, IBM will provide physical installation services.

If Customer chooses to deploy the client VPN functionality of the Proventia MX, IBM will support the deployment of client VPN software through an enablement model, as described in the section entitled "VPN Support", subsection "Client VPNs", of this Service Description.

Remote Configuration

When taking over management of an existing Agent, IBM will typically perform the configuration remotely, including registration of the Agent with IBM Managed Security Services infrastructure. Customer may be required to physically load media.

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 Service deployment is when the 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. IBM will introduce the Customer via phone to the SOC personnel.

2.2 Ongoing Management and Support

After the Service environment has been established, and during any renewal contract period, IBM will provide the Service on a 24 hours/day by 7 days/week basis.

2.2.1 Policy Management

Changes

A single firewall policy/configuration change is defined as any authorized request for the addition or modification of one rule with five or fewer network or IP objects in a single request. Any change request requiring the addition of six or more network or IP objects, or the manipulation of two or more rules, will be counted as two or more requests. If the request applies to changes outside of the rule-based firewall policy, each submitted request will be considered a single change, within reasonable limits.

All policy and configuration changes will be completed by IBM. MPS for Networks – Standard Customers may process changes to the firewall platform security policy/configuration as follows:

- a. Proventia MX 100x - two changes per calendar month by submitting a policy change request through the Virtual-SOC;
- b. Proventia MX 300x – four changes per calendar month by submitting a policy change request through the Virtual-SOC;
- c. Proventia MX 50xx – six changes per calendar month by submitting a policy change request through the Virtual-SOC.

Additional policy changes can be provided for an additional fee. Following the closure of a calendar month, unused changes are considered void and may not be rolled over to the following month.

For Customer-requested Agent policy changes, IBM will target to:

- investigate policy change requests; and
- update the Agent policy configuration.

Policy change requests are subject to approval by IBM. Such approval will not be unreasonably withheld; however, among other reasons, a request will be denied if the policy change would result in a large number of false alarms.

Ongoing Policy Maintenance

IBM will work with Customer to maintain protection strategies, including types of automatic blocking behavior in the case of Agents deployed inline.

Once a quarter, Customer may request IBM to review with them all Agents under management and identify recommended changes to the network protection strategy.

Authentication Accounts

Specific firewall functionality often allows for authentication of user accounts to enable access through application proxies or for usage of specific protocols. IBM will support the enablement of such functionality; however, user account management is the responsibility of Customer. Customer may wish to integrate a third party authentication server with the firewall. Such a server will be managed by Customer and provide additional options for user administration. IBM issues surrounding authentication of protocols and application proxies also extend to client and Secure Sockets Layer (“SSL”) VPN capabilities.

Notifications and Alerts

Certain Agents allow e-mails and/or SNMP traps to be generated and sent from the device when certain events occur. By following the standard change request procedure, Customer may request that IBM configure the Agent to deliver e-mails to a designated address.

Such a configuration is subject to approval by IBM, which will not be unreasonably withheld. However, among other reasons, a request will be denied if the configuration will have an adverse impact on the ability of the platform to protect the network environment. As with other device configurations, changes to the platform notification and alerting settings will be considered a policy change request.

X-Force Certified Attack List

IBM will configure the Agent, based on a comprehensive predefined list of attacks, tailored to Customer’s network environment. Each Agent will be implemented with X-Force Certified Attack List activated. X-Force Certified Attack List is designed to provide protection against high-risk attacks currently threatening organizations.

The X-Force Certified Attack List is maintained and updated quarterly on the Virtual-SOC. This list contains many types of attacks including backdoors, Trojans, and worms.

IBM will update the Agent configuration as threats change.

2.2.2 Device Management

IBM will be the sole provider of software-level device management for the Agent. With root/super-user/administrator level access to the device, along with an out-of-band system and an Agent installed on the device, IBM will maintain system status awareness, apply operating system patches and upgrades, troubleshoot problems on the device, and work with Customer to help ensure the device remains up and available. IBM will monitor for availability of the Agent, notify Customer when certain utilization thresholds have been met, and monitor the device 24 hours/day by 7 days/week.

Regular, automatic updates will be provided for the software and firmware.

At Customer’s request and for an additional fee, IBM will provide on-site assistance.

Management Connectivity

All security logs, events and management data travel between the SOC and the managed Agent via the Internet. Data traveling across the Internet is encrypted using industry-standard strong encryption algorithms whenever possible.

Requests for connectivity through alternate means (for example, private data circuit and/or VPN) will be addressed on a case-by-case basis. Additional monthly fees may apply to accommodate connection requirements outside of the standard in-band connectivity.

Management Platforms

For Agents from many vendors, IBM will use a management platform on IBM premises to manage the Agent.

For Proventia products, IBM will typically use the IBM SiteProtector™ management infrastructure to control Agent policy and configuration, to push updates to the Agent, and to securely receive data from the Agent using a SiteProtector event collector (called “Event Collector”).

In some cases, Customer may already use SiteProtector, and may elect to connect the Agent to the Event Collector on Customer’s premises. Customer’s Event Collector will then connect to the SiteProtector infrastructure at IBM. This configuration is commonly known as “stacking”. Any Customer choosing to use a stacked SiteProtector configuration will be subject to additional responsibilities.

Log Storage

X-Force® Protection System serves as a data warehouse for event data from a variety of security devices, applications, and platforms. The infrastructure maintains safeguards required for the logical separation of data by device and by Customer. Security events and logs are stored natively in a compressed format, preserving the original raw data. As each security event and log is written to disk, a unique hash is automatically generated to verify the integrity of the data. At the close of each 24 hour period, a checksum of all hashes generated over the course of the day is created, serving as a snapshot of the previous day’s activity.

The Customer must specify exact retention periods on a “per device” basis in one year increments. All specified retention times assume an active MSS for Security Event and Log Management contract has been maintained for each unique security event and log source.

Security Event and Log Delivery

At Customer’s request, IBM will retrieve Customer data from the IBM Managed Security Services infrastructure and store such data on encrypted media for delivery to a specified location. IBM will charge then-current consulting fees or pre-negotiated fees for all time and materials utilized to restore and prepare data in Customer’s requested format.

Health and Availability Monitoring

IBM will monitor availability of the Agent using a set of checks. For some platforms, IBM will monitor the data stream coming from the Agent, and poll administrative interfaces on the Agent. If contact with a managed device is lost, additional time-based checks will be initiated to validate the outage.

For many platforms, IBM will install monitoring software on the Agent that monitors system health and performance. For these deployments, IBM will analyze and respond to key metrics, including:

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

In the event these checks confirm an outage or system health problems, 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, Customer will be notified using a predetermined escalation procedure. Following telephone escalation, IBM will begin investigating problems related to the configuration or functionality of the managed device.

Application/Operating System 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. Security Content, delivered in the form of new checks or signatures for the IPS, antispam and antivirus modules, and new URL listings for the Web filtering module, enhances the Agent's security 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.

Device Troubleshooting

If the Agent does not perform as expected, or is identified as the potential source of a network-related problem, IBM will examine the device configuration and functionality for potential issues. Troubleshooting may consist of an offline analysis by IBM, or an active troubleshooting session between IBM and 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.

Out-of-Band Access

Out-of-band ("OOB") access is a highly recommended feature that assists the SOC in the diagnosis of potential device issues. Implementing OOB requires Customer purchase an IBM-supported OOB device and provides a dedicated analog phone line for connectivity.

If Customer has an existing OOB solution, IBM will use this solution for OOB access to managed devices, provided:

- the solution is approved by IBM;
- the solution does not allow IBM access to any non-managed devices;
- using the solution does not require installation of any specialized software;
- Customer provides detailed instructions for accessing IBM-managed devices; and
- Customer is responsible for all aspects of managing the OOB solution.

2.2.3 Vulnerability Management Service

The Vulnerability Management Service ("VMS") is a remotely delivered, electronic service that regularly and automatically scans Customer's in-scope Internet perimeter devices for known vulnerabilities. Each scan results in several comprehensive reports that are designed to identify potential weaknesses, assess relative network risk, and provide recommendations to manage identified vulnerabilities. IBM will require Customer to validate it is the owner of all IP addresses to be scanned, prior to the initial scan of such IP addresses being performed. For each Agent purchased, Customer will receive quarterly remote vulnerability assessment scanning for up to five IP addresses.

Details of VMS can be found in the Service Description entitled "IBM Vulnerability Management Service", document number BELUX-7817-xx, which can be found at www.ibm.com/services/iss/wwcontracts.

2.2.4 X-Force Threat Analysis Service

X-Force Threat Analysis Service provides proactive security management through comprehensive evaluation of global online threat conditions and detailed analyses.

The service provides threat information collected from the SOCs, and trusted security intelligence from the X-Force research and development team. This combination helps to identify the nature and severity of external Internet threats.

For each authorized security contact, Customer will receive one seat for the X-Force Threat Analysis Service for the duration of the contract.

2.2.5 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 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, event handling, incident response, data presentation, report generation, and trend analysis.

Reporting

Customer will have access to comprehensive Service information, through the Virtual-SOC, to review service tickets and Security Incidents at any time. One time per month, IBM will produce a summary report that includes:

- a. number of SLAs invoked and met;
- b. number and type of service requests;
- c. list and summary of service tickets;
- d. number of Security Incidents detected, priority and status; and
- e. list and summary of Security Incidents.

2.2.6 VPN Support

The VPN feature allows supported server-based or client-based VPNs to be connected to the Agent and helps to enable secure transmission of data across untrusted networks, via site-to-site communication. The default configuration of this feature activates this capability on the managed Agent and includes the initial configuration of up to two remote sites. After the initial configuration, each setup of a site-to-site VPN is considered a policy change.

IBM will support static authentication methods for both site-to-site and client VPN configurations. Static authentication also includes the use of Customer's existing radius authentication server implementation. Certificate-based authentication is not currently supported as a part of the VPN service configuration.

Site-to-Site VPNs

A site-to-site VPN is defined as a VPN created between the Agent and another supported encryption device. Site-to-site VPNs provide help to secure connectivity for entire networks by building a tunnel between the managed firewall platform and another compatible VPN endpoint. Site-to-site VPNs can be established between:

- two IBM-managed VPN-capable Agents, or
- an IBM-managed endpoint and a non-IBM-managed endpoint. A one-time fee will be charged for the initial configuration of a managed to unmanaged endpoint.

In the event problems with the VPN tunnel arise after setup, IBM will work with Customer and vendor contacts to identify, diagnose, and resolve performance and IBM-related issues

Client VPNs

Client VPNs help to provide secure connectivity into a protected network, from a single workstation with the appropriate client VPN software and access credentials. Client VPNs help to enable remote workers to access internal network resources without the risk of eavesdropping or data compromise.

IBM supports client VPN implementations through an enablement model. IBM will work with Customer to configure and test the first five client VPN users. Following successful connectivity for these five users, it will be Customer's responsibility to perform user administration for individuals requiring a client VPN connection. IBM will provide Customer with a demonstration of the user management capabilities of the deployed firewall platform (if applicable), and help to provide the appropriate access levels and software required to complete the setup.

Client VPN solutions typically require the installation of a client VPN application onto the specific workstations participating in the secured tunnel. The deployed Agent is designed to determine the specific client VPN applications to be supported by the Services. Some client VPN applications may be available through their respective vendors at no additional cost, while others are licensed per seat. Customer is solely responsible for the acquisition, installation, and associated costs therein of any required client VPN software.

SSL VPNs

SSL VPNs help to offer secure connectivity into company resources from any Web-enabled personal computer ("PC"), without the need for a dedicated client VPN application. This allows remote workers to access company resources from an Internet-connected PC. In contrast to traditional Internet Protocol Security ("IPsec") VPNs, SSL VPNs do not require installation of specialized client software on users' computers.

IBM supports SSL VPN implementations through an enablement model. IBM will work with Customer to configure and test the first five SSL VPN users. Following successful connectivity for these five users, it will be Customer's responsibility to perform user administration for individuals requiring an SSL VPN connection. IBM will provide Customer with a demonstration of the user management capabilities of the deployed firewall platform (if applicable), and provide the appropriate access levels and software required to complete the setup.

2.2.7 Antispam

The integrated antispam capabilities of many Agents check inbound and outbound e-mail messages for known spam signatures, patterns, and behaviors. The Agent must be placed in a location where e-mail passes through the device prior to reaching the mail gateway. This helps prevent undesirable messages from impacting the performance and availability of the mail gateway. While the core function of antispam technology is to eliminate unsolicited advertisements, most antispam technology also filters phishing attempts (i.e., e-mails designed to fool users into releasing their private data). Typically, phishing e-mails claim to be from a legitimate service, but refer the user to a malicious Web site which collects the user's personal data.

The antispam policy can typically be configured to white list or blacklist specific e-mail addresses and domains, as desired. Such configurations are designed to allow for e-mail messages from these e-mail addresses and domains to always pass, or always be deleted by the antispam module, respectively. IBM will work directly with Customer to collect data required for IBM to construct customized white and blacklists tailored to the specific needs of Customer.

Enabling antispam functionality may require additional licensing from the Agent's vendor, which shall be the sole responsibility of Customer.

2.2.8 Web Filtering

Web filtering is designed to address potential objectionable Internet content. Using content analysis technology, the managed Agent can provide policy-based content control.

Enabling Web filtering may require additional licensing for the Agent which shall be the sole responsibility of Customer.

Configuration

In order for Web filtering to be effective, the Agent must be placed in a location where user Web traffic passes through the device(s) prior to reaching the intended destination. This allows the Web filtering module to compare the requested URL against the content database to validate the requested destination is authorized.

During the initial setup and deployment process, IBM will work with Customer to create a policy that is customized to the organization's specific needs.

2.2.9 Antivirus

Antivirus support is designed to minimize the risk of malicious code within the network data stream. Antivirus gateways can be configured to scan Web, e-mail, and file-transfer traffic, and are designed to block the transmission of files which contain any of a number of designated threats. Most antivirus scanners will also block common forms of spyware, as well as many types of network worms.

Enabling antivirus functionality may require additional licensing for the Agent, which shall be the sole responsibility of Customer.

Configuration

In order for antivirus implementations to be effective, the Agent must be placed in a location where user and inbound traffic passes through the device(s) prior to reaching its intended destination. This allows the Agent to compare monitored traffic against known virus signatures and/or behavior.

During the initial setup and deployment process, IBM will work with Customer to create a policy that is customized to the organization's specific needs.

2.2.10 High Availability

High availability ("HA") increases the reliability of the Service by supporting the implementation of redundant Agents into Customer's managed environment. Adding HA to the Service requires the purchase of a second Agent and on-going management fees. It may also require changes to the Agent,

software licensing, IP addressing requirements, or managed services fees. The Service does not support non-integrated, third party HA solutions.

Active/Passive Implementations

Active/passive implementations improve reliability of the Agent gateway solution through redundancy. In this configuration, a second Agent is configured as a hot-standby, ready to begin serving the network if the primary Agent experiences a critical hardware or software failure. In such a scenario, failover is designed to be automatic and nearly instantaneous. Active/passive configurations are recommended for mission critical environments with low to medium traffic loads.

Active/Active Implementations

Active/active clusters improve reliability and performance of the managed Agents by using both Agents to handle the network traffic simultaneously. In this configuration, each Agent handles a share of the network packets, determined by a load-balancing algorithm. If one Agent fails, the other Agent is designed to automatically handle all of the traffic until the failed Agent has been restored. Active/active configurations are recommended for mission critical environments with high traffic volumes and/or large fluctuations in network utilization.

3. Customer Responsibilities

While IBM will work with Customer to deploy and implement the Agent, and IBM will manage the Agent, 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, Customer will work with IBM to deploy a new Agent or begin management of an existing Agent, as applicable.

Customer will participate in a scheduled kickoff call to introduce team members, set expectations and begin the assessment process.

Customer will be required to complete a form to provide detailed information about the network configuration (including applications and services for the Hosts on the protected network) and must work with IBM in good faith to accurately assess the Customer's network and environment. Customer must provide contacts within the organization, and specify an escalation path through the organization in the event that IBM must contact Customer.

Customer must ensure that any existing Agent meets IBM specifications, and must work to meet recommendations concerning 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 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 Customer.

While IBM will provide support and guidance, Customer is responsible for the physical installation and cabling of all Agents, unless such service is provided as an IBM consulting project. If Customer chooses to deploy the client VPN functionality of the Proventia MX, Customer is responsible for the actual installation and some testing of the client VPN software, with IBM support. Customer is responsible for procuring any client VPN software directly from a vendor, although IBM may make recommendations and guide Customer to an appropriate vendor contact.

3.2 Ongoing Management and Support

3.2.1 Policy Management

Customer acknowledges that IBM is the sole party responsible for and possessing authority to change the Agent's policy and/or configuration.

While IBM may assist, Customer is ultimately responsible for its own network security strategy, including incident response procedures.

3.2.2 Device Management

If Customer wishes to enable the HA feature of the Service, Customer agrees to purchase a second Agent and pay for the ongoing management of such Agent.

Customer is responsible for maintaining current hardware and software maintenance contracts.

Physical Environment

Customer must provide a secure, physically controlled environment for the Agent.

Customers who choose not to deploy an OOB solution may be required to provide hands-on assistance with the Agent for the purposes of troubleshooting and/or diagnosing technical difficulties.

On an annual basis, Customer agrees to work with IBM to review the current hardware configuration of the managed devices and identify required updates. These updates will be based on identified changes to the operating system and application requirements.

Network Environment

Customer is responsible for making agreed-to changes to the network environment based upon IBM recommendations.

Customer is required to maintain an active and fully functional Internet connection at all times, and must ensure the Agent is Internet-accessible via a dedicated, static IP address. Internet access service and telecommunications transport circuits are solely the Customer's responsibility.

Customer is responsible for ensuring the desired network traffic and applicable segments are configured to route network traffic through the Agent.

Management Platforms

Customers hosting their own SiteProtector infrastructure:

- a. must set up an event stream to IBM, via the Internet;
- b. must ensure its Event Collectors have unique, routable IP addresses to forward events to IBM;
- c. must have an Event Collector dedicated to the devices IBM will be monitoring on behalf of Customer. Such Event Collector may not receive events from devices for which Customer has not contracted for management or monitoring;
- d. must provide IBM with full administrative access to the SiteProtector application server, via the SiteProtector console, for the purpose of pushing updates and controlling policy;
- e. may be required to upgrade their SiteProtector infrastructure in order to transfer data to the IBM Managed Security Services infrastructure; and
- f. must not alter the Agent's policy or configuration outside of the established policy change request procedure.

3.2.3 VPN Support

For VPN connections to sites that are not being managed by IBM, Customer must provide a completed "VPN Site Configuration" form. The VPN will be configured in accordance with the information provided. Troubleshooting of remote site connectivity is strictly limited to IBM managed sites.

3.2.4 Data Compilation

Customer consents to IBM collecting, gathering and compiling security event log data to look at trends, and real or potential threats. IBM may compile or otherwise combine this security event log data with similar data of other customers so long as such data is compiled or combined in a manner that will not in any way reveal the data as being attributable to Customer.

4. Service Level Agreements

IBM SLAs establish response time objectives and countermeasures for Security Incidents resulting from the Services. 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 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 the Services. Unless explicitly stated below, no additional guarantees or warranties of any kind shall apply to the Services delivered under this Service Description. The sole remedies for failure to meet the SLA guarantees are specified in the section entitled “SLA Remedies”, below.

- a. Security Incident prevention guarantee – all X-Force Certified Attack List Security Incidents will be successfully stopped on Customer network segments that are protected and monitored by an Agent.
- b. Policy change request acknowledgement guarantee – IBM will acknowledge receipt of Customer’s policy change request within two hours of receipt by IBM. This guarantee is only available for policy change requests submitted by a valid security contact in accordance with the provided procedures.
- c. Policy change request implementation guarantee – Customer policy change requests will be implemented within 24 hours of receipt by IBM unless the request has been placed in a “hold” status due to insufficient information required to implement the submitted policy change request.
This guarantee is only available for policy change requests submitted by a valid security contact in accordance with established procedures.
- d. Proactive system monitoring guarantee – Customer will be notified within 30 minutes after IBM determines Customer’s Agent is unreachable via standard in-band connectivity. During an outage escalation, IBM will continue attempting to contact the designated Customer contacts (in the advised priority order) until a designated contact is reached or until all contacts have been exhausted.
- e. Proactive Security Content update guarantee – IBM will apply all new Security Content updates to Customer’s managed security platform within 72 hours from the time the Security Content update was published for general availability by the vendor.

4.2 SLA Remedies

A credit will be issued as the sole remedy for failure to meet any of the guarantees described in the section entitled “SLA Guarantees” during any given calendar month. 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 (euros), in a given calendar month.

- a. Security Incident prevention remedy – if the Security Incident prevention guarantee is not met for any given calendar month, a credit will be issued for the applicable charges for one month’s fees for MPS for Networks – Standard for the initial Security Incident that was not prevented.
- b. Policy change request acknowledgement, policy change request implementation, proactive system monitoring and proactive Security Content update remedies – If IBM fails to meet any of these guarantees, a credit will be issued for the applicable charges for one day of the monthly monitoring fee for the affected device and, if applicable, the specific managed security platform for which the respective guarantee was not met.

Table 3 - Summary of Service Level Agreements and Remedies

Service Level Agreements	Remedies for MPS for Networks – Standard
Security Incident prevention guarantee	Credit of 1 month fee for MPS for Networks – Standard
Policy change request acknowledgement guarantee	Credit of 1 day of the monthly monitoring fee for the affected device
Policy change request implementation guarantee	
Proactive system monitoring guarantee	
Proactive Security Content update guarantee	

4.3 Scheduled and Emergency Portal Maintenance

Scheduled maintenance shall mean any maintenance:

- a. of which the Customer is notified at least five days in advance; or
- b. that is performed during the standard monthly maintenance window on the second Saturday of every month from 8:00 a.m. – 4:00 p.m. United States Eastern Time. Notice of scheduled maintenance will be provided to the designated Customer contact.

No statement in the section entitled “Service Level Agreements” shall prevent IBM from conducting emergency maintenance on an “as needed” basis. During such emergency maintenance, the affected Customer’s primary point of contact will receive notification within 30 minutes of initialization of the emergency maintenance and within 30 minutes of the completion of any emergency maintenance.

4.4 SLA Exclusions and Stipulations

4.4.1 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, 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.

4.4.2 Customer Network/Server Change Notifications

Customer is responsible for providing IBM advance notice regarding any network or server changes to the Agent environment. If the event advance notice cannot be provided, 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 Customer fails to notify IBM as stated above, all SLA remedies are considered null and void.

4.4.3 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 Agent and therefore the Agent 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 an Agent, or that does not generate a logged event, is not covered under these SLAs.

4.4.4 SLA Compliance and Reporting

SLA compliance and the associated remedies are based on fully functional network environments, Internet and circuit connectivity, Agents, 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.

4.4.5 Testing of Monitoring and Response Capabilities

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 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 (“SLOs”) establish nonbinding objectives for the provision of certain features of the Services. 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 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 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 at any time. Should such modification reduce the scope or level of the Service being delivered (for example, eliminating a previously provided Service or lengthening the Security Incident response time), IBM will provide a minimum of 30 days prior notice via the ISS Web portal or other electronic means.