

Service Description

Managed Protection Service for Desktop Firewalls – Standard

1. Scope of Services

The IBM Managed Protection Service for Desktop Firewalls – Standard (called “MPS for Desktop Firewalls - Standard” or “Service”) helps to provide protection for user desktops). The objective of the Service is to improve Customer’s security posture while simplifying the management and maintenance associated with the security implementation.

MPS for Desktop Firewalls – Standard supports IBM Proventia® Desktop Endpoint Security and IBM RealSecure® Desktop (called “Agent”). Such Agents are controlled and updated using the agent manager component of the IBM Proventia® Management SiteProtector™ system (called “Agent Manager”).

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

Definitions of Service-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 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 application designed to allow or deny access requests based on a set security policy. Many firewalls include a full set of networking features (for example, routing capabilities and address and port rewriting).
- c. antivirus
Using behavioral techniques, desktop antivirus actively monitors activity on each Host. This level of analysis helps block unknown worms, viruses, and other malware, and helps prevent damage.

MPS for Desktop Firewalls – Standard will provide the following services in support of the product features previously listed:

- d. 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”).
- e. policy management
Agents only help to protect Hosts when configured correctly for their network environment. IBM provides policy management services to help Customer keep Agents configured with a valid security policy, and retain records of all changes.
- f. device management
IBM will maintain the Agents and management infrastructure by monitoring system health and Agent Manager availability, and applying vendor updates to the Agents using the Agent Manager.
- g. vulnerability management
Vulnerabilities are weaknesses in the Hosts in Customer’s environment. IBM will provide limited vulnerability management services to help identify and remediate such vulnerabilities.
- h. X-Force Threat Analysis Service
IBM will provide security intelligence to the Customer based on such things as original research completed by the IBM Internet Security Systems™ 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.

i. Virtual-SOC

The Virtual-SOC is a Web-based interface designed to enable delivery of key Service details and on-demand protection solutions.

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

Table 1 - Product Features

Product Feature	MPS for Desktop Firewalls - Standard
Ideal for:	Desktop implementations ranging from 500 to 100,000 workstations.
Supported operating systems	Specific Microsoft Windows operating systems supported by the Proventia Desktop and RealSecure Desktop Agents
Supported policy features	Includes IPS, IDS, virus prevention system (“VPS”), buffer overflow exploit protection (“BOEP”), inbound/outbound firewall rules, adaptive/static policies, and antivirus compliance
Intrusion Prevention configuration	X-Force Certified Attack List protection with event viewing via the Virtual-SOC
Intrusion Detection configuration	Attack identification with event viewing via the Virtual-SOC
Supported infrastructure options	<ul style="list-style-type: none"> • IBM-hosted SiteProtector™ system with Customer-provided IBM-managed Agent Managers on-site at one or more Customer locations • Agent Manager stacking

The following table provides an overview of MPS for Desktop Firewalls - Standard Service provided in support of the product features previously listed.

Table 2 - Services

Services	MPS for Desktop Firewalls - Standard
Project kickoff	Included
Policy management	Unlimited policy changes
Policy configuration	Up to 4 custom policy configurations provided for the first 10,000 desktops. One additional custom policy may be added for each additional block of up to 10,000 desktops (for example, a 15,000 desktop deployment will receive 5 custom policies).
Customer-requested policy changes	Changes accepted by IBM to control both inbound and outbound desktop access
Device management	24 x 7 device health and availability monitoring and maintenance of Agent Manager infrastructure and maintenance of Security Content for Agents
Security Content updates	Updates made within 72 hours of release of new Security Content
Vulnerability management	Quarterly scan of up to 5 IPs
X-Force Threat Analysis Service	Available to 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/RealSecure Desktop Agents and the Agent Manager component of the SiteProtector system will be managed as part of MPS for Desktop Firewalls – Standard.

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;
- set expectations; 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 virtual private network (“VPN”) may be used, if appropriate.

2.1.2 Assessment

Data Gathering

IBM will provide a form for the 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 to help determine the layout of the Customer network, Hosts on the network, and desired security policies. A portion of the requested data will reflect the 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.

Existing Agent Manager Assessment

If IBM will be taking over management of an existing Agent Manager, IBM must assess the Agent Manager to be sure it meets then-current SiteProtector system requirements. IBM may require the Agent Manager hardware and operating system 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 Agent Managers deployed through IBM at the time of purchase, much of the configuration and policy setting will take place at IBM facilities. For existing Agent Managers already in use, Customer will have the option to ship the Agent Manager to IBM for configuration at IBM facilities.

Installation

While physical installation and cabling are a Customer responsibility, IBM will provide 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 an IBM deployment specialist.

At Customer’s request and for an additional fee, IBM will provide physical installation services.

Remote Configuration

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

All Agent Managers will require some remote configuration, which may include registration of the Agent with the 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 Customer with the option of viewing 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 Customer. At this time, the ongoing management and support phase of the Service officially begins. Typically, IBM will introduce 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

The number of policies and groups available for Customer use is determined by the size of the managed deployment. Up to four custom policy configurations are provided for the first 10,000 desktops. One additional custom policy may be added for each additional block of up to 10,000 desktops (for example, a 15,000 desktop deployment will receive five custom policies).

Additional policies and groups may be purchased for an additional monthly fee.

Adaptive and Static Policies

MPS for Desktop Firewalls – Standard supports policies in an adaptive configuration, a static configuration, or a combination of the two.

Adaptive policies are dynamic and automatically adjust the outbound access capabilities of a given Host, depending on the source Internet Protocol (“IP”) address and means of connectivity when it communicates with a desktop controller infrastructure component.

Static policies are constant, regardless of the source IP address in use by the Host when a connection to the Agent Manager is established. Static policies provide a predictable, rules-based approach to security policy application.

Policy Changes

The Service provides an unlimited number of changes per month. All policy changes and modifications will be completed by IBM. Completed and verified changes will be pushed from the SOC to the Customer’s Agent Manager. As each Proventia Desktop Agent checks in with the Agent Manager, the new policy is downloaded and applied to the applicable Agents.

Proventia Desktop Agents may be installed on mobile computers, or devices that may not be running each and every day. Therefore, it may take several days (or longer in some instances) for all Agents to check in with the Agent Manager and download the latest policy version.

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.

X-Force Certified Attack List

IBM will configure the Agent, based on a 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. The Agent will be monitored 24 hours/day by 7 days/week.

2.2.2 Device Management

Health and Availability Monitoring

The health and performance of the Agent Managers for MPS for Desktop Firewalls – Standard are monitored by using a Host-based monitoring Agent. The devices are regularly polled by the SOC, keeping IBM security analysts informed of potential problems as they develop. Key metrics analyzed by the monitoring Agent include:

- hard disk capacity;
- CPU utilization;
- memory utilization; and
- process availability.

In addition to the above metrics, IBM will monitor device uptime and 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 and Security Content Updates

Periodically, it will be necessary for IBM to install application patches and updates to the managed infrastructure, and provide required software and configurations that enable desktop Agents to update themselves with the latest Security Content. Such patches and updates may improve performance and security, enable additional functionality, and resolve potential application problems.

Application patches and updates may require infrastructure downtime or Customer assistance to implement. IBM will notify Customer of a maintenance window in advance of any performance-impacting updates. All maintenance notifications will clearly state the impacts of scheduled maintenance in addition to any specific Customer security contact requirements.

Log Storage

X-Force® Protection System (“XPS”) serves as a data warehouse for event and log data. 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.

The Customer must specify exact retention periods on a “per Agent Manager” basis in one year increments, with a maximum of seven years. All specified retention times assume an active Service contract has been maintained for each Agent Manager and log source.

Security Event and Log Delivery

IBM will retrieve Customer data, at Customer’s request from the IBM Managed Security Services Infrastructure and store it 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 the Customer’s requested format.

Management Platforms

For Proventia and RealSecure products, IBM will use the SiteProtector system to control Agent policy and configuration, to push updates to the Agent, and to securely receive data from the Agent using a SiteProtector Agent Manager.

The Agent Manager serves as a centralized point of communication for desktop Agents to send event data, download updated policies, and receive Security Content updates. IBM will manage and maintain a limited number of Agent Managers in support of the Customer implementation.

In some cases, Customer may already use the SiteProtector system, and may elect to connect desktop Agents to an existing Agent Manager on Customer’s premises. Customer’s Agent Manager 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 responsible for management of Customer premises SiteProtector software, hardware, and associated operating systems. IBM will require login credentials to the Customer-managed SiteProtector application server for the purpose of managing Agent policy, application of Agent updates, and Agent troubleshooting. Customer will not under any circumstances modify the Agent policy or configuration once the SOC has taken over management of the Agent configurations.

Agent Managers must be deployed on dedicated devices at Customer premises, in proportion to the size of the desktop deployment. A properly sized Agent Manager can accommodate approximately 20,000-25,000 individual Hosts. The number of required Agent Managers for a given implementation may vary depending on the implementation size, specifications of the Agent Manager platform, and the usage of adaptive policies.

The following table defines the number of Agent Managers IBM will manage as part of the Services.

Deployment Size (# of Hosts)	Includes Management of X Number of Agent Managers
1 – 20,000	1
20,001 – 40,000	2
40,001 – 60,000	3
60,001 – 80,000	4
80,001 – 100,000	5
100,001 and above	1 additional Agent Manager for each 20,000 Hosts

Troubleshooting

IBM analysts will work directly with Customer and IBM product technical support to resolve IBM issues impacting a significant portion of the installed user base. Isolated IBM issues impacting individual Hosts will be evaluated, but such issues may require resolution by Customer or in conjunction with IBM product technical support. The Service does not provide direct support to desktop Agent users.

Troubleshooting may consist of an offline analysis by the IBM analyst, or an active troubleshooting session driven by IBM in conjunction with Customer security contacts. IBM will attempt to resolve IBM technical issues as quickly as possible. In the event IBM-managed devices are eliminated as the potential source of a given problem, no further troubleshooting will be performed by IBM analysts.

Out-of-Band Access

Out-of-band (“OOB”) access to the Agent Manager is a highly recommended feature that assists the SOC in the diagnosis of potential device issues. Implementing OOB requires that Customer purchase an IBM-supported OOB device and provide 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 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 Firewalls

The desktop Agent firewall is designed to provide protection against unwanted and malicious traffic. By utilizing stateful packet inspection and bi-directional policies, the firewall helps to prevent unwanted traffic from entering or leaving each individual desktop.

Policy

Firewall policies support rules that restrict inbound and outbound traffic based on port number and protocol type. During deployment of the Service, IBM will work with Customer’s authorized security and deployment contacts to collect the data required for IBM to configure customized security policies. A limited number of custom policies may be implemented, based on the size of the desktop deployment. Policies will be developed based on Customer requirements, and assigned to groups of desktop users whose desktop Agents will receive and enforce such security settings.

Firewall Policy 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 more than five network or IP objects, or the manipulation of more than one rule, 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.

2.2.4 Intrusion Prevention and Intrusion Detection

Traffic processed by the desktop Agent will be examined for malicious activity. Traffic deemed harmful will be prevented from affecting the target system whenever possible.

IDS/IPS Policy Changes

The Service deploys the desktop Agents with maximum blocking capabilities enabled. If legitimate traffic is inadvertently blocked by multiple desktop Agents, Customer may submit a policy change request through the Virtual-SOC requesting such traffic be allowed to pass through all devices belonging to the group in which the affected Agents reside.

Intrusion Detection System (“IDS”) data is collected by IBM for statistical reference and reporting. As such, all desktop Agents will leverage an identical IDS configuration which ensures that key events are delivered to and displayed through the Virtual-SOC.

Intrusion Prevention and Blocking

The Service enables all attack detection and blocking capabilities of Proventia Desktop. This enablement is designed to block active attacks. Attacks not blocked by Proventia Desktop will be visible through the Virtual-SOC.

Configurations that do not have active blocking enabled are not supported by the Service.

2.2.5 X-Force Threat Analysis Service

X-Force Threat Analysis Service provides proactive security management through 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.

Each authorized security contact will receive access to the X-Force Threat Analysis Service for the duration of the contract.

2.2.6 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 and 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

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

- a. number of service level agreements (“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.

Service Tickets

Service tickets are created when an IBM issue is worked within the SOC for a specific security platform or Customer. Each service ticket captures the data relevant to the specific IBM issue, including but not limited to:

- issue description;
- issue type and priority;

- relevant dates/times;
- relevant IP addresses and ports; and
- detailed worklog of all actions taken.

Service tickets are available, through the Virtual-SOC, for one year following their creation.

3. Customer Responsibilities

While IBM will work with Customer to deploy and implement the Agent Manager, and IBM will manage the Agent Manager, 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 Manager or begin management of an existing Agent Manager, 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 security policies to be deployed across the desktop Agent Hosts. 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 desktop Agent meets then current SiteProtector system requirements, 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 Manager, IBM may require the Agent Manager 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 actual installation and some testing of all desktop Agents, unless such service is provided as part of an IBM PSS consulting project.

3.2 Ongoing Management and Support

3.2.1 Agent Manager Management

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 Manager is Internet-accessible via a dedicated, static IP address. Internet access service and telecommunications transport circuits are solely the Customer's responsibility.

Customer is solely responsible for procuring and making available the required hardware for Agent Manager devices. Customer is responsible for maintaining current hardware and software maintenance contracts.

3.2.2 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, the Customer is ultimately responsible for its own network security strategy, including incident response procedures.

3.2.3 Physical Environment

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

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

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

3.2.4 Hardware Replacement

If a Customer premises Agent Manager experiences a hardware failure requiring an RMA, IBM analysts will work with the Customer to provide required data to allow the Customer to escalate the occurrence to

the appropriate hardware vendor or provider. IBM analysts will not be responsible for escalating hardware failures directly to the vendor on the Customer's behalf. The time required for a replacement device to arrive on-site is determined by the type of maintenance agreement in place between the Customer and the respective hardware vendor or provider.

When replacement hardware arrives, the Customer security contact or Customer's vendor must complete a series of steps (for example, operating system installation, network configuration, activation of terminal services, and establishment of a login account) to allow IBM to remotely connect to the device and return it to normal operation. At the Customer's request, physical installation may be provided by IBM PSS for an additional fee.

3.2.5 Management Platforms

Customers hosting their own SiteProtector infrastructure:

- a. must set up an event stream to IBM, via the Internet;
- b. must ensure their Agent Managers have unique, routable IP addresses to forward events to IBM;
- c. must have an Agent Manager dedicated to the devices IBM will be monitoring on behalf of the Customer. Such Agent Manager may not receive events from devices for which Customer has not contracted with IBM 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.

3.2.6 Data Compilation

Customer consents to IBM 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 Service. 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 Definitions

Group Move Request - any authorized request for modification of a single policy group's contents for up to five Hosts by an X-Force® Security Operations Analyst within a single request submission. Any change request that requires the modification of six or more Hosts within a single group, or the altering of multiple policy group contents will be counted as two or more Group Move Requests.

4.2 SLA Guarantees

The SLA guarantees described below comprise the measured metrics for delivery of the Service. Unless explicitly stated below, no additional guarantees or warranties of any kind shall apply to the Service 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 desktops that are running a supported version of Proventia Desktop or RealSecure Desktop. For a claim against this SLA to be considered valid:
 - (1) the affected desktop device must have reported in to the desktop controller/Agent Manager within the past five days from the time of compromise, and
 - (2) Customer's total number of reporting desktop Agents must be within the number purchased for the active MPS for Desktop Firewalls – Standard contract.

- 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 Customer security contact in accordance with established procedures.
- c. Policy change request implementation guarantee –Customer policy change requests will be implemented within eight 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 Customer security contact in accordance with established procedures.
- d. Emergency policy change request implementation guarantee – IBM will implement Customer emergency policy change requests within two hours of Customer’s declaration of emergency (by telephone) following change submission through the Virtual-SOC.
This guarantee is only available for policy change requests submitted by a valid Customer security contact in accordance with established procedures. Further, this guarantee is based on actual time of implementation, and not on the time Customer was notified the request was completed..
IBM will promptly notify Customer upon implementation of a policy change request by telephone, e-mail, fax, pager, or electronic response via the Virtual-SOC and will continue attempting to contact the designated Customer contact until a contact is reached or all escalation contacts have been exhausted.
No more than two emergency policy change requests may be declared per calendar month.
- e. Group Move Request guarantee - Customer Group Move Requests will be implemented within four 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 Customer security contact in accordance with established procedures.
- f. Proactive system monitoring guarantee – IBM will notify Customer within 30 minutes after IBM determines that Customer’s desktop Agent is unreachable via standard in-band connectivity.
IBM will contact the designated Customer contact by a method elected by IBM. During an outage escalation, IBM will continue attempting to contact the designated Customer contact until such contact is reached or all escalation contacts have been exhausted.
- g. 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 is published for general availability by the vendor.

SLA Summary

Service Level Agreement	MPS for Desktop Firewalls - Standard
Security Incident prevention guarantee	Applicable
Policy change request acknowledgement guarantee	Acknowledgement within 2 hours of receipt
Policy change request implementation guarantee	Implementation within 8 hours of receipt
Emergency policy change request implementation guarantee	Implementation within 2 hours of declaration of emergency
Group Move Request guarantee	Implementation within 4 hours of receipt
Proactive system monitoring guarantee	Notification within 30 minutes
Proactive Security Content update guarantee	Begin updates within 72 hours

4.3 SLA Remedies

IBM will issue a credit 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 (U.S.), or the equivalent in local currency, 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 Desktop Firewalls – Standard for the initial Security Incident that was not prevented.
- b. Policy change request acknowledgement, policy change request implementation, emergency policy change implementation, Group Move request, 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 – Select
Security Incident prevention guarantee	Credit of 1 month fee for MPS for Desktop Firewalls – Standard
Policy change request acknowledgement guarantee	Credit of 1 day’s fee for MPS for Desktop Firewalls – Standard
Policy change request implementation guarantee	
Emergency policy change request implementation guarantee	
Group Move Request guarantee	
Proactive system monitoring guarantee	
Proactive Security Content update guarantee	

4.4 Scheduled and Emergency Portal Maintenance

Scheduled maintenance shall mean any maintenance:

- a. of which Customer is notified at least five days in advance; or
- b. that is performed during the standard monthly maintenance window on the first 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.

4.5 SLA Exclusions and Stipulations

4.5.1 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.

4.5.2 Customer Network/Server Change Notifications

The 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.

4.5.3 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.

4.5.4 SLA Compliance and Reporting

SLA compliance and the associated remedies are based on fully functional network environments, Internet and circuit connectivity, desktop Agents, and properly configured Agent Managers. If SLA compliance failure is caused by CPE hardware or software (including any and all Agents and the Hosts on which they reside), all SLA remedies are considered null and void.

4.5.5 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, device failures, 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.

4.5.6 Active Blocking Requirements

The MPS for Desktop offering requires active blocking of attacks as specified in the X-Force Certified Attack List. In the event Customer requests that active blocking be disabled for any signatures in the X-Force Certified Attack List, no Security Incident SLAs (i.e., Security Incident Prevention Guarantee, Security Incident Identification Guarantee, and Security Incident Response Guarantee) shall apply for those signatures not configured to actively block attacks.

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 its 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. During an Internet emergency, IBM will communicate all other priority level incidents 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.