

## Descriptif de Services

---

### Managed Protection Service for Desktop Firewalls – Standard

#### 1. Objet

IBM Managed Protection Service for Desktop Firewalls – Standard (le « Service MPS for Desktop Firewalls – Standard ») offre une protection à chaque niveau de l'infrastructure réseau du Client (réseau, serveur et postes de travail utilisateur). Ce service a pour objet d'améliorer le positionnement du Client en matière de sécurité, tout en simplifiant les procédures d'administration et de maintenance associées à l'implémentation d'une solution de sécurité.

Le Service MPS for Desktop Firewalls – Standard prend en charge IBM Proventia® Desktop Endpoint Security et IBM RealSecure® Desktop (les « Agents »). Ces Agents sont gérés et mis à jour via le gestionnaire d'agent de la plate-forme IBM Proventia® Management SiteProtector™ (le « Gestionnaire d'Agent »).

Les détails de votre commande (les services dont vous avez besoin, la durée de validité du contrat et le prix, par exemple) seront indiqués sur le Bon de commande.

Les définitions des termes spécifiques aux services figurent dans le Glossaire disponible sur le site [www.ibm.com/services/iss/wwcontracts](http://www.ibm.com/services/iss/wwcontracts)

IBM prendra en charge tout ou partie des fonctionnalités suivantes :

- a. Systèmes de détection et de prévention d'intrusion (« IDS/IPS »)  
IDS/IPS est un système de gestion de la sécurité des ordinateurs et réseaux qui permet de collecter et d'analyser des informations en provenance de diverses zones de l'ordinateur ou du réseau pour identifier et bloquer les éventuelles violations de la sécurité, c'est-à-dire les intrusions (attaques provenant de l'extérieur de l'entreprise) et les utilisations abusives (attaques de l'intérieur de l'entreprise).
- b. Pare-feu  
Un pare-feu est un ensemble de programmes associés implanté sur un serveur de passerelle réseau qui permet ou interdit à certains Systèmes hôtes ou réseaux de communiquer entre eux en fonction de règles de sécurité établies. De nombreux pare-feu comprennent un ensemble complet de fonctions réseau (fonctions d'acheminement et de réécriture d'adresses et de ports, par exemple).
- c. Antivirus  
Utilisant des méthodes d'analyse comportementale, les antivirus pour poste de travail surveillent efficacement l'activité de chaque Système hôte. Ce niveau d'analyse permet de bloquer les vers, les virus informatiques et autres programmes malveillants, contribuant ainsi à prévenir d'éventuels dommages.

Le Service MPS for Desktop Firewalls – Standard offrira les services suivants à l'appui des fonctionnalités énumérées ci-dessus :

- d. lancement, évaluation et implémentation du projet  
Lors du déploiement du Service MPS for Desktop Firewalls, IBM travaillera en collaboration avec le Client afin de définir les procédures de sécurité adéquates, d'aider le Client à installer et à configurer le ou les Agents et de vérifier le bon fonctionnement du système avant de transférer la gestion du ou des Agents sur le SOC.
- e. gestion des stratégies de sécurité  
Les Agents ne sont en mesure de protéger efficacement les Systèmes hôtes que s'ils sont configurés correctement pour leur environnement réseau. IBM fournit des services de gestion des stratégies de sécurité afin d'aider le Client à configurer les Agents via une stratégie de sécurité adéquate et à garder trace de toutes les modifications effectuées.
- f. gestion des systèmes  
IBM assurera la maintenance des Agents et de leur infrastructure de gestion en surveillant l'état de santé de chaque système et la disponibilité du Gestionnaire d'Agent, et en appliquant aux Agents des mises à jour fournisseur par le biais du Gestionnaire d'Agent.

g. gestion des vulnérabilités

Les vulnérabilités constituent les points faibles des Systèmes hôtes au sein de l'environnement du Client. IBM fournira des services de gestion des vulnérabilités pour permettre d'identifier ces vulnérabilités et d'y remédier.

h. XFTAS

IBM fournira au Client des services de veille sécuritaire basés sur les recherches menées par l'équipe de Recherche & Développement IBM Internet Security Systems™ X-Force®, sur le bilan des activités mondiales en termes de menaces qui a été établi par IBM Global Threat Operations Center, et sur les études complémentaires réalisées par des organismes publics ou privés.

i. Virtual-SOC

Le Virtual-SOC est un portail Web qui permet au Client d'accéder à une somme d'informations sur la gestion des Agents, les alertes, les fichiers journaux, les rapports, les demandes de modification de procédure, et à d'autres types de tickets de service.

Le tableau suivant présente les fonctionnalités produit de du service MPS for Desktop Firewalls - Standard.

**Tableau 1 – Fonctionnalités produit**

Fonctionnalité produit	MPS for Desktop Firewalls - Standard
Idéal pour :	Les environnements poste de travail composés de 500 à 100 000 postes de travail.
Systèmes d'exploitation pris en charge	Tous les systèmes d'exploitation pris en charge par Proventia Desktop et RealSecure Desktop.
Fonctions de sécurité prises en charge	Inclut une option d'interface utilisateur, un système IPS/IDS, un système de prévention contre les nouveaux virus (« VPS »), un système de prévention de l'exploitation de la mémoire tampon (« BOEP »), des règles de pare-feu applicables au trafic entrant/sortant, des stratégies de configuration dynamique, des outils de conformité et des antivirus.
Configuration du système de prévention d'intrusion	Offre une protection contre les attaques répertoriées dans la liste X-Force Certified Attack List (XFCAL), en permettant de visualiser les événements avec Virtual-SOC.
Configuration du système de détection d'intrusion	Associe des fonctions d'identification au processus de visualisation d'événements via le Virtual-SOC.
Options d'infrastructure prises en charge	Utilisation conjointe de la plate-forme SiteProtector, implantée dans les locaux d'IBM, avec des contrôleurs de poste de travail gérés par IBM sur un ou plusieurs des sites du Client.

Le tableau suivant présente les services MPS for Desktop Firewalls - Standard fournis à l'appui des fonctionnalités produit énumérées ci-dessus.

**Tableau 2 - Services**

Services	MPS for Desktop Firewalls - Standard
Lancement du projet	inclus
Gestion de la politique de sécurité	Nombre illimité de modifications des règles de sécurité
Configuration de la politique de sécurité	Possibilité de configurer jusqu'à 4 politiques personnalisées pour les 10 000 premiers postes de travail. Il est possible d'ajouter une politique personnalisée supplémentaire pour tout groupe additionnel de 10 000 postes maximum (dans le cadre du déploiement de 15 000 postes de travail, par exemple, il est possible de configurer 5 politiques

	personnalisées).
Modifications de règles de sécurité demandées par le Client	Modifications acceptées par IBM afin de contrôler à la fois les accès entrants et sortants aux postes de travail.
Gestion des systèmes	Surveillance, 24 heures sur 24, 7 jours sur 7, de l'état de santé et de la disponibilité des systèmes, et maintenance de l'infrastructure de gestion et du Contenu de sécurité des Agents.
Mises à jour du Contenu de sécurité	Application des mises à jour dans les 72 heures suivant la publication du nouveau Contenu de sécurité.
Gestion des vulnérabilités	Scan trimestriel de 5 adresses IP maximum
XFTAS	1 abonnement pour une personne au service de veille sécuritaire XFTAS
Virtual-SOC	Offre un accès en temps réel pour les communications

## 2. Responsabilités d'IBM

### 2.1 Déploiement et initialisation

Lors de la phase de déploiement et d'initialisation, IBM travaillera en collaboration avec le Client pour déployer un nouvel Agent ou commencer à gérer un Agent existant. Le Service MPS for Desktop Firewalls – Standard prend uniquement en charge les Agents Proventia Desktop et le Gestionnaire d'Agent de la plate-forme SiteProtector.

#### 2.1.1 Lancement du projet

IBM enverra au client un courriel d'accueil et organisera une conférence téléphonique initiale afin de :

- présenter les points de contact Client au spécialiste du déploiement IBM ;
- définir les attentes vis-à-vis du projet ;
- commencer à évaluer les besoins et l'environnement du Client.

IBM fournira un document intitulé « Spécifications d'accès au réseau », qui décrit la façon dont IBM se connectera à distance au réseau du Client, ainsi que les spécifications techniques requises pour permettre ce type d'accès. En règle générale, IBM se connectera via Internet, à l'aide de méthodes d'accès standard ; toutefois, une connexion VPN de site à site pourra être utilisée, le cas échéant.

#### 2.1.2 Évaluation

##### Collecte de données

IBM remettra un formulaire au Client afin qu'il fournisse les informations détaillées nécessaires pour le paramétrage initial de l'Agent et des fonctionnalités des services associés. La plupart des questions sont d'ordre technique et permettront de déterminer la configuration du réseau du Client, les Systèmes hôte connectés au réseau et les règles de sécurité souhaitées. Certaines des informations demandées concernent l'entreprise du Client, notamment les contacts pour les questions de sécurité et la procédure d'escalade pour signaler les problèmes.

##### Évaluation de l'environnement

Sur la base des informations fournies, IBM travaillera avec le Client afin de comprendre l'environnement existant et de déterminer la configuration ainsi que la politique de sécurité de l'Agent. En cas de migration d'un Agent existant vers un Agent plus récent, IBM utilisera la configuration et la politique de l'Agent existant.

Dans tous les cas de figure, IBM pourra préconiser un ajustement de la stratégie en vigueur en réponse aux menaces les plus actives à l'échelle mondiale (telles qu'elles sont définies par IBM Global Threat Operations Center) et en vue de réduire le nombre d'alertes erronées, le cas échéant.

Lors de cette évaluation, IBM pourra être appelé à formuler des recommandations sur la manière d'ajuster la stratégie applicable à l'Agent afin d'optimiser la sécurité.

##### Évaluation du Gestionnaire d'Agent existant

S'il reprend la gestion d'un Gestionnaire d'Agent existant, IBM devra évaluer ce dernier afin de s'assurer qu'il répond à certaines spécifications. IBM pourra exiger la mise à niveau de ce Gestionnaire d'Agent pour pouvoir assurer le service. IBM pourra en outre imposer comme autres conditions l'ajout ou la suppression d'un certain nombre d'applications et de comptes utilisateurs.

### **2.1.3 Implémentation**

#### **Configuration chez IBM**

En ce qui concerne les Gestionnaires d'Agent qui sont déployés à l'achat par le biais d'IBM, la plupart des tâches de configuration et de développement de stratégie seront exécutées dans les locaux d'IBM. Quant aux Gestionnaires d'Agent existants et déjà opérationnels, le Client aura la possibilité de les expédier à IBM pour qu'ils soient configurés dans les locaux d'IBM.

#### **Installation**

Bien que les procédures d'installation et de câblage physiques relèvent de la responsabilité du Client, IBM fournira une assistance permanente, par téléphone et messagerie électronique, et aidera le Client à se procurer la documentation fournisseur décrivant la procédure d'installation de l'Agent. Ce type d'assistance devra être planifié à l'avance pour permettre à IBM de garantir la disponibilité d'un spécialiste du déploiement.

À la demande du Client, l'installation physique pourra être assurée par IBM Professional Security Services (« PSS »), moyennant un surcoût.

#### **Configuration à distance**

S'il reprend la gestion d'un Gestionnaire d'Agent existant, IBM exécute généralement la procédure de configuration à distance. La présence du Client peut toutefois s'avérer indispensable pour charger physiquement les supports.

Tous les Gestionnaires d'Agent nécessitent certaines opérations de configuration à distance, telles que l'enregistrement de l'Agent au sein de l'infrastructure IBM Managed Security Services (MSS).

### **2.1.4 Transfert sur le SOC**

Une fois l'Agent configuré, physiquement installé, implémenté et connecté à l'infrastructure IBM MSS, IBM offrira au Client la possibilité d'assister à une démonstration des fonctionnalités du Virtual-SOC et de l'exécution des tâches les plus courantes.

L'étape finale du déploiement des services consiste à transférer sur le SOC la gestion et le support de l'Agent et de la relation Client. C'est à ce moment-là que débute officiellement la phase de gestion et de support permanent des services. En règle générale, IBM présente le Client par téléphone au personnel du SOC.

## **2.2 Gestion et support permanent**

Une fois l'environnement en place et pendant toute période ultérieure de reconduction du contrat, IBM fournira les Services MPS for Desktop Firewalls – Standard sur la base de prestations de type 24 heures sur 24, 7 jours sur 7.

### **2.2.1 Gestion des stratégies**

Le nombre de groupes et de stratégies de sécurité pouvant être implémentés par le Client dépend de l'ampleur du processus de déploiement géré. Quatre stratégies personnalisées sont disponibles pour les 10 000 premiers postes de travail. Il est possible d'ajouter une stratégie personnalisée supplémentaire pour tout groupe additionnel de 10 000 postes maximum (dans le cadre du déploiement de 15 000 postes de travail, par exemple, il est possible de configurer cinq stratégies personnalisées).

Il est possible d'acheter des groupes et stratégies de sécurité supplémentaires moyennant une redevance mensuelle additionnelle.

#### **Stratégies de configuration dynamique et statique**

Le Service MPS for Desktop Firewalls – Standard prend en charge les stratégies de configuration dynamique et statique, ou une combinaison des deux.

Les stratégies de configuration dynamique ajustent automatiquement les possibilités d'accès sortant d'un Système hôte donné en fonction de son adresse IP d'origine et de ses moyens de connexion lorsqu'il communique avec l'un des composants d'infrastructure du contrôleur de poste de travail.

Les stratégies de configuration statique sont constantes, quelle que soit l'adresse IP d'origine utilisée par le Système hôte pour se connecter au Gestionnaire d'Agent. Elles offrent une approche prévisible, basée sur des règles, de l'implémentation des stratégies de sécurité.

### **Modifications de procédure**

Le Service MPS for Desktop Firewalls – Standard prend en charge un nombre illimité de modifications de procédure par mois. Toutes les modifications de procédure seront effectuées par IBM. Une fois terminées et validées, ces modifications seront envoyées en mode « push » du SOC au Gestionnaire d'Agent du Client. Lorsque chaque Agent Proventia Desktop s'enregistrera auprès du Gestionnaire d'Agent, la nouvelle procédure sera téléchargée et appliquée aux Agents concernés.

Les Agents Proventia Desktop peuvent être installés sur des ordinateurs portables ou des appareils qui ne sont pas nécessairement utilisés de façon quotidienne. Par conséquent, plusieurs jours (voire plus, dans certains cas) peuvent être nécessaires pour que tous les Agents s'enregistrent auprès du Gestionnaire d'Agent et téléchargent la dernière version de la procédure.

Les demandes de modification de procédure sont soumises à l'approbation d'IBM, qui s'engage à fournir une réponse dans un délai raisonnable. La demande pourra toutefois être rejetée, entre autres, si la modification de procédure a pour effet de générer un grand nombre d'alertes erronées.

### **X-Force Certified Attack List (XFCAL)**

IBM configurera l'Agent à partir d'une liste prédéfinie d'attaques, personnalisée en fonction de l'environnement réseau du Client. Chaque Agent sera implémenté avec l'option XFCAL activée. Cette option est conçue pour fournir une protection contre les attaques les plus sérieuses qui menacent actuellement les entreprises.

La liste XFCAL est gérée et mise à jour une fois par trimestre sur le Virtual-SOC. Elle répertorie de nombreux types d'attaque, telles que les portes dérobées, les chevaux de Troie et les vers informatiques.

IBM mettra à jour la configuration de l'Agent à mesure que les conditions de menace évolueront. L'Agent sera surveillé 24 heures sur 24, 7 jours sur 7.

## **2.2.2 Gestion des systèmes**

### **Surveillance de l'état de santé et de la disponibilité des systèmes**

L'état de santé et les performances des Gestionnaires d'Agent utilisés par le Service MPS for Desktop Firewalls – Standard sont surveillés via un Agent de surveillance résidant sur le Système hôte. Les systèmes sont interrogés régulièrement par le SOC afin de tenir les analystes de la sécurité IBM informés des problèmes potentiels à mesure qu'ils évoluent. Les principaux indicateurs de performances analysés par l'Agent de surveillance sont :

- la capacité de disque dur (s'il y a lieu) ;
- le taux d'utilisation processeur ;
- le taux d'utilisation mémoire ;
- la disponibilité des processus.

Outre l'état de santé proprement dit, IBM contrôlera la disponibilité des systèmes. En cas de perte de contact avec un système géré, des procédures de vérification additionnelles relatives aux temps seront lancées pour s'assurer qu'un motif valable d'interruption de service a été identifié.

En cas de confirmation d'une interruption de service ou de problèmes liés à l'état de santé des systèmes, un ticket d'incident sera créé et un message de notification sera adressé à un analyste de la sécurité IBM pour lui permettre de lancer une procédure de recherche et d'investigation. L'état de tous les tickets de santé du système est disponible par le biais du Virtual-SOC.

### **Notification relative aux interruptions de service**

Si l'Agent n'est pas accessible à l'aide des processus de connexion intrabande standard, le Client en sera informé par téléphone selon un processus d'escalade prédéfini. À la suite de ce processus téléphonique, IBM commencera à effectuer des recherches sur les problèmes liés à la configuration ou aux fonctionnalités du système géré.

### **Mise à jour des applications et du Contenu de sécurité**

IBM sera amené périodiquement à installer des correctifs et des mises à jour d'applications au sein de l'infrastructure gérée, et à fournir les configurations et les logiciels requis pour permettre aux Agents de poste de travail de procéder à leur propre mise à jour à l'aide du Contenu de sécurité le plus récent. Ces

correctifs et mises à jour peuvent contribuer à améliorer les performances et la sécurité, à étendre les fonctionnalités existantes et à résoudre les problèmes applicatifs potentiels.

L'application de ces correctifs et mises à jour pourra nécessiter l'immobilisation de l'infrastructure ou l'assistance du Client. IBM annoncera, si nécessaire, une fenêtre de maintenance avant l'application de ces mises à jours, et tiendra le Client clairement informé de l'impact des opérations de maintenance planifiée, en tenant compte des impératifs éventuels de chacun des points de contact de sécurité du Client.

### **Stockage des fichiers journaux**

X-Force® Protection System sert d'entrepôt de données pour les données d'événement émanant de différentes ressources de sécurité, applications et plates-formes. Après avoir été visualisés sur le Virtual-SOC, les fichiers journaux sont transférés sur un support de sauvegarde physique, tel qu'une bande ou un DVD. Les supports de sauvegarde sont archivés sur un site sécurisé présentant un environnement contrôlé. Les données archivées seront disponibles pendant un laps de temps défini par l'utilisateur, dans la limite de sept ans à compter de la date de création du journal.

À la demande du Client, IBM soumettra une demande de recherche et d'extraction de support. Des frais de consultation seront appliqués sur une base horaire pour l'ensemble du temps passé à restaurer et à présenter les données au format requis par le Client.

### **Plates-formes d'administration**

Pour gérer des Agents multifournisseur, IBM utilisera une plate-forme d'administration implantée dans ses propres locaux.

En ce qui concerne les produits Proventia, IBM utilisera en principe la plate-forme SiteProtector pour gérer la stratégie et la configuration de l'Agent, pour envoyer les mises à jour en mode « push » à l'Agent et pour recevoir de façon sécurisée les données émanant de ce dernier via un collecteur d'événements SiteProtector (le « Collecteur d'événements »).

Il se peut que le Client utilise déjà la plate-forme SiteProtector ; dans ce cas, il pourra choisir de connecter l'Agent au Collecteur d'événements au sein de ses propres locaux. Le Collecteur d'événements du Client sera alors connecté à la plate-forme SiteProtector implantée dans les locaux d'IBM. Cette configuration est généralement appelée « empilage ». Tout Client qui choisit d'utiliser une configuration SiteProtector empilée s'expose à des responsabilités supplémentaires.

IBM utilisera en principe un Gestionnaire d'Agent pour gérer les Agents de poste de travail. Le Gestionnaire d'Agent sert de plate-forme de communication centralisée permettant aux Agents de poste de travail d'envoyer des données d'événement, de télécharger les modifications de procédure et de recevoir les mises à jour du Contenu de sécurité. IBM assure la gestion et la mise à jour d'un nombre limité de Gestionnaires d'Agent dans le cadre du processus d'implémentation Client.

Les Gestionnaires d'Agent doivent être déployés sur des systèmes dédiés dans les locaux du Client, proportionnellement au nombre de postes de travail. Un Gestionnaire d'Agent correctement dimensionné peut prendre en charge de 20 000 à 25 000 Systèmes hôtes individuels environ. Le nombre de Gestionnaires d'Agent requis dans le cadre d'un processus d'implémentation donné peut varier en fonction de l'ampleur de ce processus, des spécifications de la plate-forme sur laquelle ils résident et de l'utilisation ou non de stratégies de configuration dynamique.

Le tableau suivant indique le nombre de Gestionnaires d'Agent pris en charge par IBM dans le cadre du Service MPS for Desktop Firewalls – Standard.

<b>Ampleur du processus de déploiement (en nombre de Systèmes hôtes)</b>	<b>Nombre de Gestionnaires d'Agent pris en charge par IBM</b>
De 1 à 20 000	1
De 20 001 à 40 000	2
De 40 001 à 60 000	3
De 60 001 à 80 000	4

De 80 001 à 100 000	5
100 001 et plus	1 Gestionnaire d'Agent supplémentaire pour tout groupe additionnel de 20 000 Systèmes hôtes

### Résolution des incidents

Les analystes IBM travailleront directement avec le Client et les membres du support technique produit IBM pour résoudre les problèmes liés à IBM qui affectent une part significative du parc d'utilisateurs. Les problèmes ponctuels liés à IBM qui affectent des Systèmes hôtes spécifiques seront analysés, mais il appartiendra au Client de les résoudre, avec le soutien éventuel des membres du support technique produit IBM. Le Service MPS for Desktop Firewalls - Standard ne fournit pas d'assistance directe aux utilisateurs des Agents de poste de travail.

La procédure de dépannage peut consister en une analyse hors connexion effectuée par IBM ou en une session de résolution d'incidents en ligne entre IBM et les points de contact de sécurité du Client. IBM s'efforcera de résoudre tous les problèmes techniques aussi convenablement que possible. Si les systèmes gérés par IBM sont hors de cause, IBM mettra fin à la procédure de résolution d'incidents.

### Gestion des accès hors bande

La gestion des accès hors bande (« OOB ») est une fonction optionnelle du Gestionnaire d'Agent, destinée à aider le SOC à diagnostiquer les incidents potentiels qui affectent les systèmes. Pour pouvoir implémenter cette fonction, le Client devra acquérir un équipement OOB pris en charge par IBM et prévoir une ligne analogique dédiée pour la connexion.

Si le Client dispose déjà d'une solution OOB, celle-ci sera utilisée par IBM pour accéder aux systèmes gérés, sous réserve que :

- cette solution ne permette pas à IBM d'accéder à des systèmes non gérés ;
- l'utilisation de cette solution ne nécessite pas l'installation d'un logiciel spécialisé ;
- le Client fournisse des instructions détaillées sur la manière d'accéder aux systèmes gérés par IBM ;
- le Client assume l'entière responsabilité de la gestion de la solution OOB.

### 2.2.3 Pare-feu

Le pare-feu associé aux Agents de poste de travail est conçu pour fournir une protection contre le trafic indésirable et malveillant. Via un mode d'inspection dynamique des paquets et des stratégies bidirectionnelles, ce pare-feu contribue à bloquer tout accès entrant ou sortant vers ou depuis les postes de travail pour le trafic indésirable.

#### Stratégie

Les stratégies de pare-feu prennent en charge la définition de règles visant à limiter le trafic entrant et sortant en fonction du numéro de port et du type de protocole. Lors de la phase de déploiement du Service MPS for Desktop Firewalls - Standard, IBM collaborera avec les points de contact autorisés du Client en charge de la sécurité et du déploiement afin de collecter les données dont il a besoin pour configurer des stratégies de sécurité personnalisées. Il est possible d'implémenter un nombre limité de stratégies personnalisées sur la base du nombre de postes de travail déployés. Ces stratégies seront développées en fonction des besoins du Client et affectées à des groupes d'utilisateurs de postes de travail spécifiques, dont les Agents seront chargés de réceptionner et d'implémenter ces paramètres de sécurité.

#### **Modification de la stratégie de pare-feu**

Toute modification de la configuration ou de la stratégie de pare-feu doit être soumise à une demande d'ajout ou de modification d'une règle unique, à raison de cinq objets IP ou réseau maximum par demande. Toute demande de modification impliquant l'ajout d'au moins six objets IP ou réseau, ou la manipulation d'au moins deux règles, sera comptabilisée comme deux demandes ou plus. Si la demande porte sur des modifications qui n'entrent pas dans le cadre de la stratégie de pare-feu basée sur un jeu de règles, chaque demande soumise sera considérée comme une demande de modification unique, dans les limites du raisonnable.

#### **2.2.4 Prévention et détection des intrusions**

Le trafic traité par l'Agent de poste de travail sera examiné dans le but de détecter d'éventuelles activités malveillantes. Tout trafic jugé préjudiciable se verra interdire, dans la mesure du possible, l'accès au système cible.

##### **Modification des procédures de détection et de prévention d'intrusion**

Le Service MPS for Desktop Firewalls – Standard déploie les Agents de poste de travail avec un maximum de fonctions de blocage activées. Si le trafic légitime se trouve bloqué par inadvertance par plusieurs Agents de poste de travail, le Client peut soumettre, via le Virtual-SOC, une demande de modification de procédure pour solliciter l'autorisation de laisser ce trafic transiter par tous les systèmes appartenant au groupe dans lequel résident les Agents concernés.

Les données IDS (« Intrusion Detection System ») sont collectées par IBM à des fins de référence statistique et de création de rapports. À ce titre, tous les Agents de poste de travail présenteront une configuration IDS identique afin de garantir la diffusion et l'affichage des événements importants via le Virtual-SOC.

##### **Prévention et blocage des intrusions**

Le Service MPS for Desktop Firewalls – Standard active toutes les fonctions de détection et de blocage d'attaques de Proventia Desktop afin de bloquer les attaques actives. Les attaques non bloquées par Proventia Desktop seront visibles via le Virtual-SOC.

Le Service MPS for Desktop Firewalls – Standard ne prend pas en charge les configurations au sein desquelles la fonction de blocage des attaques actives n'est pas activée.

#### **2.2.5 X-Force Threat Analysis Service (XFTAS)**

Le service XFTAS permet de gérer la sécurité de façon proactive via une évaluation complète de l'état global des menaces en ligne, ainsi que des analyses détaillées.

Ce service fournit des informations sur les menaces collectées auprès des SOC, ainsi que des données fiables en matière de veille sécuritaire émanant de l'équipe de Recherche & Développement de la X-Force. Le recoupement de toutes ces informations permet d'identifier la nature et le degré de gravité des menaces Internet externes.

Pour chaque Agent acheté, le Client se verra proposer un abonnement pour une personne au service XFTAS, pendant toute la durée de validité du contrat.

#### **2.2.6 Virtual-SOC**

Le Virtual-SOC est un portail Web conçu pour fournir des informations clés sur les services et les solutions de protection à la demande. Le Virtual-SOC est structuré de façon à offrir une vue unifiée de la situation globale du Client au regard de la sécurité. Il est capable d'intégrer, au sein d'une même interface, des données émanant de plusieurs secteurs géographiques ou se rapportant à diverses technologies, offrant ainsi un jeu complet de fonctions d'analyse, d'alerte, de résolution d'incidents et de production de rapports.

Le Virtual-SOC offre un accès en temps réel pour les communications concernant, par exemple, la création de tickets d'incident, la gestion d'événements, la résolution d'incidents, la présentation des données, la production de rapports et l'analyse de tendances.

##### **Production de rapports**

Via le Virtual-SOC, le Client pourra accéder à tout moment à un jeu complet d'informations sur les services afin de consulter la liste des tickets de service et des Incidents de sécurité. Une fois par mois, IBM fournira un rapport de synthèse indiquant :

- a. le nombre d'Accords sur le niveau de service (SLA) invoqués et honorés ;
- b. le nombre et le type de demandes de service ;
- c. la liste et le récapitulatif des tickets de service ;
- d. le nombre d'Incidents de sécurité détectés, ainsi que leur statut et leur degré de priorité ;
- e. la liste et le récapitulatif des Incidents de sécurité.

### **Création de tickets de service**

Un ticket de service est généré chaque fois qu'un incident lié à IBM est traité au sein du SOC pour une plate-forme de sécurité ou un Client spécifique. Tout ticket d'incident contient, de façon non limitative, les informations suivantes :

- description de l'incident ;
- type et degré de priorité de l'incident ;
- date et heure de l'incident ;
- adresses IP et ports concernés ;
- journal détaillé des actions mises en œuvre.

Les tickets d'incident sont disponibles, via le Virtual-SOC, pendant un an à compter de leur date de création.

## **3. Responsabilités du Client**

Tandis qu'IBM travaillera avec le Client au déploiement et à l'implémentation du Gestionnaire d'Agent et qu'il gèrera ce dernier, le Client sera tenu de collaborer en toute bonne foi et d'assister IBM, à la demande de celui-ci, dans certaines circonstances.

### **3.1 Déploiement et initialisation**

Lors de la phase de déploiement, le Client travaillera en collaboration avec IBM pour déployer un nouveau Gestionnaire d'Agent ou commencer à gérer un Gestionnaire d'Agent existant, selon le cas.

Le Client participera à une conférence initiale planifiée afin de présenter les membres de l'équipe, de définir les attentes vis-à-vis du projet et de lancer le processus d'évaluation.

Le Client sera tenu de remplir un formulaire afin de fournir des informations détaillées sur les stratégies de sécurité à déployer sur les Systèmes hôtes sur lesquels résident les Agents de poste de travail. Le Client devra fournir une liste de points de contact et définir un processus d'escalade au sein de l'entreprise pour le cas où IBM aurait besoin de le contacter.

Le Client devra s'assurer que tout Agent de poste de travail existant répond aux spécifications d'IBM et se conformer aux recommandations relatives à son réseau et à ses besoins d'accès réseau, si des modifications sont nécessaires pour garantir des stratégies de protection efficaces.

S'il reprend la gestion d'un Gestionnaire d'Agent existant, IBM pourra exiger la mise à niveau de ce Gestionnaire d'Agent ou du Contenu de sécurité existant pour pouvoir assurer le service. IBM pourra en outre imposer comme autres conditions l'ajout ou la suppression d'un certain nombre d'applications et de comptes utilisateurs. Le Client assumera l'entière responsabilité de ces mises à niveau, ajouts ou suppressions.

Alors qu'IBM fournira conseils et assistance, le Client sera responsable de l'installation physique et de certaines des procédures de test des Agents de poste de travail, à moins que ce service ne soit assuré dans le cadre d'un projet d'expertise conseil IBM PSS.

### **3.2 Gestion et support permanent**

#### **3.2.1 Gestion du Gestionnaire d'Agent**

Il appartient au Client d'apporter les modifications convenues à l'environnement réseau, sur la base des recommandations d'IBM.

Le Client est tenu de maintenir à tout moment une connexion Internet active et pleinement opérationnelle, et de veiller à ce que le Gestionnaire d'Agent soit accessible par Internet via une adresse IP statique dédiée.

Il relève de la seule responsabilité du Client de se procurer le matériel requis par les systèmes Gestionnaire d'Agent et de le rendre disponible à ceux-ci. Le Client est responsable de la gestion des contrats de maintenance matériel et logiciel en cours de validité.

#### **3.2.2 Gestion des stratégies**

Le Client reconnaît qu'IBM est la seule partie responsable de et ayant le pouvoir de modifier la stratégie et/ou la configuration de l'Agent.

#### **3.2.3 Environnement physique**

Le Client doit fournir un environnement physique contrôlé et sécurisé au Gestionnaire d'Agent.

Les Clients qui décident de ne pas déployer de solution OOB peuvent être tenus de fournir une assistance pratique concernant le Gestionnaire d'Agent, afin de résoudre et/ou diagnostiquer les problèmes techniques éventuels.

Le Client convient de collaborer avec IBM sur une base annuelle afin de passer en revue la configuration matérielle courante des systèmes gérés et d'identifier les mises à jour requises. Ces mises à jour seront fondées sur l'évolution des fonctionnalités du système d'exploitation et des besoins applicatifs.

### **3.2.4 Remplacement de matériel**

Si un Gestionnaire d'Agent résidant sur un équipement privé d'abonné est affecté par une panne de matériel nécessitant une autorisation de retour d'article (RMA), les analystes IBM collaboreront avec le Client afin de lui fournir les données requises pour lui permettre de faire remonter l'incident jusqu'au fournisseur du matériel concerné. Toutefois, il ne relève pas de la responsabilité des analystes IBM de faire remonter, de la part du Client, les pannes de matériel directement jusqu'au fournisseur. Le délai nécessaire à l'acheminement sur site d'un équipement de rechange peut varier en fonction du type de contrat de maintenance en vigueur entre le Client et le fournisseur du matériel concerné.

À l'arrivée de l'équipement de rechange, le point de contact de sécurité du Client sera invité à effectuer une série d'opérations (installation du système d'exploitation, configuration du réseau, activation de services de terminaux et création d'un compte utilisateur, par exemple) pour permettre à IBM de se connecter à distance au système et d'en rétablir le fonctionnement normal. À la demande du Client, l'installation physique pourra être assurée par IBM Professional Security Services (« PSS »), moyennant un surcoût.

### **3.2.5 Plate-formes d'administration**

Les Clients qui hébergent leur propre infrastructure SiteProtector :

- a. doivent configurer un flux d'événements à transmettre à IBM via Internet ;
- b. doivent veiller à ce que chaque Collecteur d'événements dispose d'une adresse IP acheminable unique pour la transmission des événements à IBM ;
- c. doivent disposer d'un Collecteur d'événements dédié aux systèmes qu'IBM est appelé à surveiller au nom du Client. Ce Collecteur d'événements ne devra pas recevoir d'événements émanant de systèmes autres que ceux pour lesquels le Client a souscrit un contrat de gestion ou de surveillance ;
- d. doivent fournir à IBM des droits d'accès administrateur exclusifs au serveur d'applications de la plate-forme SiteProtector, par le biais de la console système SiteProtector, pour lui permettre d'envoyer des mises à jour en mode « push » et de superviser la stratégie ;
- e. peuvent être appelés à mettre leur infrastructure SiteProtector à niveau pour permettre le transfert de données vers l'infrastructure IBM MSS ;
- f. ne doivent pas modifier la stratégie ou la configuration de l'Agent en dehors du cadre du processus de demande de modification de procédure qui a été établi.

## **4. Accords sur le niveau de service**

Les Accords sur le niveau de service (SLA) IBM établissent des objectifs en termes de temps de réponse et des contre-mesures destinées à remédier aux Incidents de sécurité liés au Service MPS for Desktop Firewalls – Standard. Les Accords sur le niveau de service prennent effet une fois que le processus de déploiement est terminé, que le système a été activé et que le support et la gestion du système ont été transférés sur le SOC.

Les recours sont applicables sous réserve que le Client remplisse ses obligations, telles qu'elles sont définies dans le présent Descriptif de Services.

### **4.1 Définitions**

Demande de modification de groupe – toute demande autorisée de modification du contenu d'un groupe unique de stratégies portant sur un maximum de cinq Systèmes hôtes et émise, via une procédure de soumission unique, par un analyste des opérations de sécurité de la X-Force®. Toute demande de modification portant sur six Systèmes hôtes ou plus au sein d'un même groupe ou affectant le contenu de plusieurs groupes de stratégies sera comptabilisée comme deux Demandes de modification de groupe ou plus.

## 4.2 Garanties de niveau de service

Les garanties de niveau de service décrites ci-dessous englobent les mesures de performances applicables au Service MPS for Desktop Firewalls – Standard. Sauf si cela est expressément stipulé ci-dessous, aucune garantie supplémentaire d'aucune sorte ne saurait s'appliquer au Service MPS for Desktop Firewalls – Standard. Les seuls recours applicables en cas de non respect des garanties de niveau de service sont décrits dans la section « Recours » ci-dessous.

- a. Garantie de prévention des Incidents de sécurité – tous les Incidents de sécurité XFCAL seront bloqués sur les postes de travail du Client qui exécutent une version prise en charge de Proventia Desktop ou de RealSecure Desktop. Pour qu'une réclamation au titre du présent Accord sur le niveau de service soit considérée comme valide :
  - (1) le poste de travail concerné doit avoir rendu compte de l'Incident de sécurité au contrôleur de poste de travail/ Gestionnaire d'Agent dans les cinq jours suivant l'incident ;
  - (2) le nombre total d'Agents de poste de travail déclarants du Client ne doit pas excéder le nombre d'Agents achetés dans le cadre du contrat MPS for Desktop Firewalls – Standard en vigueur.
- b. Garantie d'accusé de réception des demandes de modification de procédure – IBM accusera réception des demandes de modification de procédure émanant du Client dans un délai de deux heures à compter de leur réception par IBM. Cette garantie s'applique uniquement aux demandes de modification de procédure soumises par un point de contact de sécurité dûment autorisé, conformément aux procédures établies.
- c. Garantie de mise en œuvre des demandes de modification de procédure – les demandes de modification de procédure émanant du Client seront mises en œuvre dans un délai de huit heures à compter de leur réception par IBM, à moins qu'elles n'aient été mises en attente en raison du manque d'informations requises pour pouvoir les mettre en œuvre.

Cette garantie s'applique uniquement aux demandes de modification de procédure soumises par un point de contact de sécurité dûment autorisé, conformément aux procédures établies.
- d. Garantie de mise en œuvre des modifications d'urgence demandées – IBM mettra en œuvre les demandes de modification d'urgence émanant du Client dans un délai de deux heures à compter de la déclaration d'urgence (par téléphone) du Client qui fait suite à la demande de modification soumise par le biais du Virtual-SOC.

Cette garantie s'applique uniquement aux demandes de modification de procédure soumises par un point de contact de sécurité dûment autorisé du Client, conformément aux procédures établies. De plus, cette garantie repose sur l'heure de mise en œuvre effective, et non sur l'heure à laquelle le Client a été informé du fait que la demande a été traitée.

Après la mise en œuvre d'une demande de modification, IBM en informera le Client dans les plus brefs délais par téléphone, messagerie électronique, télécopie, radiomessagerie ou via le Virtual-SOC, et s'efforcera de se mettre en relation avec le point de contact désigné du Client jusqu'à ce qu'il ait réussi à joindre un interlocuteur ou qu'il soit parvenu à la fin de la liste des personnes à contacter dans le cadre du processus d'escalade.

Le Client ne doit pas déposer plus de deux demandes de modification d'urgence par mois calendaire.
- e. Garantie de mise en œuvre des Demandes de modification de groupe – les Demandes de modification de groupe seront mises en œuvre dans un délai de quatre heures à compter de leur réception par IBM, à moins qu'elles n'aient été mises en attente en raison du manque d'informations requises pour pouvoir les mettre en œuvre.

Cette garantie s'applique uniquement aux demandes de modification de procédure soumises par un point de contact de sécurité dûment autorisé, conformément aux procédures établies.
- f. Garantie de surveillance proactive du système – le Client sera informé dans un délai de 30 minutes après qu'IBM aura détecté que l'Agent de poste de travail du Client est inaccessible au moyen des processus de connexion intrabande standard.

IBM contactera le point de contact désigné du Client via la méthode de son choix. Lors du processus d'escalade afférent à une interruption de service, IBM s'efforcera de se mettre en relation avec le contact client désigné jusqu'à ce qu'il ait réussi à joindre un interlocuteur ou qu'il soit parvenu à la fin de la liste des personnes à contacter.

- g. Garantie de mise à jour proactive du Contenu de sécurité – IBM installera toute nouvelle mise à jour du Contenu de sécurité sur la plate-forme de sécurité gérée du Client dans les 72 heures qui suivront leur mise à disposition par le fournisseur.

**Récapitulatif des garanties de niveau de service**

Garantie de niveau de service	MPS for Desktop Firewalls - Standard
Prévention des Incidents de sécurité	Oui
Accusé de réception des demandes de modification de procédure	Oui, dans un délai de 2 heures après réception
Mise en œuvre des demandes de modification de procédure	Oui, dans un délai de 8 heures après réception
Mise en œuvre des modifications d'urgence demandées	Oui, dans un délai de 2 heures après déclaration
Mise en œuvre des Demandes de modification de groupe	Oui, dans un délai de 4 heures après réception
Surveillance proactive du système	Oui, notification dans un délai de 30 minutes
Mise à jour proactive du Contenu de sécurité	Oui, lancement du processus de mise à jour dans un délai de 72 heures

**4.3 Recours**

*NOTE AU RESPONSABLE LOCAL DES CONTRATS & NÉGOCIATIONS : Veuillez remplacer « \$25 000 (U.S.) » par son équivalent dans votre devise locale (l'euro, par exemple).*

En cas de non respect, au cours d'un mois calendaire donné, de n'importe laquelle des garanties décrites dans la section intitulée « Garanties de niveau de service », IBM prévoit comme unique recours de créditer le compte du Client. Le Client ne pourra bénéficier que d'un seul crédit par jour pour chaque Accord sur le niveau de service, dans la limite de \$25 000 (U.S.) par mois calendaire pour l'ensemble des Accords sur le niveau de service, conformément aux dispositions de la section ci-dessous intitulée « Responsabilités et limitation de responsabilité ». Les recours applicables sont répertoriés ci-dessous :

- Prévention des Incidents de sécurité – si la garantie de prévention des Incidents de sécurité n'est pas remplie pendant un mois calendaire donné, le compte du Client sera crédité d'un montant équivalent à celui de la redevance mensuelle due au titre du Service MPS for Desktop Firewalls – Standard pour le premier Incident de sécurité n'ayant pas été évité ;
- Accusé de réception des demandes de modification de procédure, mise en œuvre des demandes de modification de procédure et des demandes de modification de groupe, surveillance proactive du système et mise à jour proactive du Contenu de sécurité – si IBM ne remplit pas l'une de ces garanties, le Client se verra octroyer un crédit d'une journée sur le montant de la redevance mensuelle due au titre de la surveillance de la plate-forme touchée et, le cas échéant, de la plate-forme de sécurité gérée pour laquelle la garantie en question n'a pas été remplie.

**Tableau 3 - Récapitulatif des garanties de niveau de service et des recours**

Garantie de niveau de service	Recours applicable
Prévention des Incidents de sécurité	Octroi d'un crédit correspondant au montant de la redevance mensuelle due au titre du Service MPS for Desktop Firewalls – Standard
Accusé de réception des demandes de modification de procédure	
Mise en œuvre des demandes de modification de procédure	

Mise en œuvre des modifications d'urgence demandées	Octroi d'un crédit d'une journée sur le montant de la redevance mensuelle due au titre du Service MPS for Desktop Firewalls – Standard
Mise en œuvre des Demandes de modification de groupe	
Surveillance proactive du système	
Mise à jour proactive du Contenu de sécurité	

#### 4.4 Maintenance planifiée et dépannage d'urgence du portail

La maintenance planifiée couvre toutes les opérations de maintenance :

a. dont le Client est informé au moins cinq jours à l'avance ; ou

*NOTE AU RESPONSABLE LOCAL DES CONTRATS & NÉGOCIATIONS : Veuillez remplacer la mention « 8:00 a.m. – 4:00 p.m., heure des Etats-Unis de l'Est et du Canada » par votre équivalent local.*

b. qui sont effectuées durant la fenêtre de maintenance mensuelle standard, le deuxième samedi de chaque mois, de 8:00 a.m. à 4:00 p.m., heure des Etats-Unis de l'Est et du Canada. Le point de contact désigné du Client sera averti de ces opérations de maintenance.

Aucune des dispositions de la section intitulée « Accords sur le niveau de service » ne saurait empêcher IBM d'effectuer des opérations de dépannage d'urgence en fonction des besoins. Le point de contact principal du Client qui aura été désigné sera averti dans un délai préalable de 30 minutes du démarrage et de l'achèvement de toute opération de dépannage d'urgence.

#### 4.5 Responsabilités et limitation de responsabilité

##### 4.5.1 Devoir d'information envers le point de contact du Client

Plusieurs Accords sur le niveau de service imposent à IBM d'informer le point de contact désigné du Client lorsque des événements spécifiques se produisent. Pour le cas où ce type d'événement se produirait, il relève de la responsabilité exclusive du Client de fournir à IBM des informations précises et actualisées concernant le(s) point(s) de contact désigné(s). Une fois enregistrées, ces informations seront mises à la disposition de points de contact dûment autorisés par le biais du Virtual-SOC. IBM sera déchargé de ses obligations dans le cadre des présents Accords sur le niveau de service si les informations qui lui sont fournies sont périmées ou inexactes par suite d'un manquement ou d'une omission de la part du client.

##### 4.5.2 Obligation de notification des modifications réseau ou serveur de la part du Client

Le Client est tenu d'informer IBM par avance de toute modification réseau ou serveur susceptible d'affecter l'environnement de l'Agent. Si aucune notification préalable ne peut être fournie, le Client est tenu d'informer IBM des modifications survenues dans les sept jours calendaires suivant lesdites modifications. La procédure de notification s'effectue par la soumission ou la mise à jour d'un ticket de serveur critique via le Virtual-SOC. Si le Client omet d'informer IBM conformément à la procédure ci-dessus, tous les recours applicables au titre des Accords sur le niveau de service seront considérés comme nuls et non avenue.

##### 4.5.3 Montant maximal des pénalités/indemnités payables au Client

Le montant total des crédits (« indemnités ») pouvant être octroyés en cas de non respect des garanties de niveau de service dans le cadre de l'offre MPS for Desktop Firewalls – Standard, tels qu'ils sont décrits dans les sections ci-dessus intitulées « Garanties de niveau de service » et « Recours », ne saurait excéder le montant de la redevance mensuelle associée aux services.

##### 4.5.4 Trafic réseau couvert par les Accords sur le niveau de service

Certains Accords sur le niveau de service mettent l'accent sur la prévention, l'identification et l'escalade des Incidents de sécurité. Or, ces Accords sur le niveau de service présupposent que le trafic a correctement atteint l'Agent et que, par conséquent, ce dernier est en mesure de le gérer conformément à la stratégie en vigueur et de déclencher un événement journalisé. Le trafic qui ne transite pas par un Agent par voie logique ou électronique ou qui n'entraîne pas le déclenchement d'un événement journalisé n'est pas couvert par les présents Accords sur le niveau de service.

#### **4.5.5 Conformité et rapports de conformité vis-à-vis des Accords sur le niveau de service**

La conformité vis-à-vis des Accords sur le niveau de service et les recours applicables en cas de non respect de ces Accords supposent que les environnements réseau, les connexions réseau et Internet et les Agents de poste de travail soient pleinement opérationnels, et que les Gestionnaires d'Agent soient configurés de façon adéquate. Si la non conformité vis-à-vis des Accords sur le niveau de service est due à des problèmes matériels ou logiciels inhérents aux équipements privés d'abonné (tous Agents compris, ainsi que les Systèmes hôtes sur lesquels ils résident), tous les recours seront considérés comme nuls et non avenue.

#### **4.5.6 Test de la capacité de surveillance et de réactivité**

Le Client a la possibilité de tester la capacité de surveillance et de réactivité d'IBM en lançant périodiquement des opérations de reconnaissance, des attaques système ou réseau, des pannes système et/ou des tentatives de compromission système réelles ou simulées. Ces opérations peuvent être menées directement par le Client ou par un tiers sous contrat, sans qu'IBM en ait été préalablement averti. Les Accords sur le niveau de service ne seront pas applicables pendant la durée d'exécution de ces opérations, et aucune indemnité ne sera due à titre de recours en cas de non respect de la ou des garanties qui leur sont associées.

### **5. Objectifs de niveau de service**

Les Objectifs de niveau de service (« SLO ») IBM sont des objectifs non contractuels liés à la fourniture de fonctionnalités spécifiques dans le cadre de l'offre MPS for Desktop Firewalls – Standard. Les Objectifs de niveau de service prennent effet une fois que le processus de déploiement est terminé, que le système a été activé et que le support et la gestion du système ont été transférés sur le SOC. IBM se réserve le droit de modifier ces Objectifs de niveau de service dans un délai de 30 jours à compter de l'envoi d'un préavis écrit.

- a. Virtual-SOC – IBM fournira un objectif d'accessibilité de 99,9 % en dehors des heures spécifiées dans la section « Maintenance planifiée et dépannage d'urgence du portail ».
- b. Incident Internet d'urgence – Dans le cas où il serait appelé à effectuer une déclaration d'urgence liée à un incident Internet, IBM s'est fixé pour objectif d'en informer par courriel les points de contact désignés du Client dans les 15 minutes qui suivent cette déclaration. Cette notification comportera un numéro de suivi d'incident et un numéro téléphonique d'urgence, et indiquera l'heure à laquelle IBM entend organiser une conférence téléphonique pour faire le point de la situation.

Lors des incidents Internet d'urgence ayant fait l'objet d'une déclaration, IBM organisera une conférence téléphonique en direct pour faire le point de la situation et enverra au Client des courriels récapitulatifs pour permettre à ce dernier de protéger son entreprise. Les séances d'information destinées à faire le point de la situation suite à l'émergence d'un incident Internet d'urgence se substitueront à toute obligation de la part d'IBM de se conformer aux processus d'escalade spécifiques au Client en ce qui concerne les événements directement liés à l'Incident Internet d'urgence qui aura été déclaré. Lors d'un incident Internet d'urgence, IBM tiendra le Client informé de tout autre incident présentant un niveau de priorité quelconque par le biais de systèmes automatisés du type messagerie électronique, radiomessagerie et messagerie vocale.

Les processus d'escalade standard reprendront leur cours normal au terme de l'incident Internet d'urgence. La fin de l'état d'urgence est marquée par le passage de la condition d'alerte au niveau AlertCon 2 ou par l'envoi d'un courriel de notification au contact de sécurité dûment autorisé du Client.

### **6. Autres clauses**

IBM se réserve le droit de modifier les termes du présent Descriptif de Services, y compris les Accords sur le niveau de service, dans un délai de 30 jours à compter de l'envoi d'un préavis écrit.